



Hot Spot
Wireless Subscriber Gateway
WSG-404

User's Manual

Copyright

Copyright (C) 2007 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE mark Warning

The is a class B device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Trademarks

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

WEEE Warning



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 Hot Spot Wireless Subscriber Gateway

Model: WSG-404

Rev: 1.0

Part No.: EM-WSG404v1 (2081-B41070-000)

Table of Contents

1. Introduction	5
1.1 Package Contents	5
1.2 Features	6
1.3 Precautions	7
1.4 Outlook	7
1.4.1 Top Panel	7
1.4.2 Rear Panel	8
1.5 Technical Specifications	10
1.5.1 Hardware Specifications	10
1.5.2 Software Specifications	11
2. Installation	13
2.1 Installation Requirements	13
2.1.1 System Requirements	13
2.1.2 ISP Requirements	13
2.1.3 Your PC Requirements	14
2.2 Hardware Connection and Installation	15
2.2.1 Physical Installation	15
2.3 Software Configuration	16
2.3.1 Quick Configuration	16
2.3.2 External Network Access	24
3. Web Interface Configuration	27
3.1 System Configuration	28
3.1.1 Configuration Wizard	28
3.1.2 System Information	29
3.1.3 WAN Configuration	31
3.1.4 LAN1 & LAN2 Configuration	33
3.1.5 LAN3 & LAN4 Configuration	36
3.1.6 Wireless Configuration	39
3.2 User Authentication	45
3.2.1 Authentication Configuration	45
3.2.1.1 Authentication Method - Local User Setting	66
3.2.1.2 Authentication Method - POP3	71
3.2.1.3 Authentication Method - RADIUS	72
3.2.1.4 Authentication Method - LDAP	74
3.2.1.5 Authentication Method - NTDomain	75
3.2.2 Black List Configuration	76
3.2.3 Policy Configuration	78
3.2.4 Guest User Configuration	82
3.2.5 Additional Configuration	83
3.3 Network Configuration	100
3.3.1 Network Address Translate	100

3.3.2 Privilege Configuration	104
3.3.3 Monitor IP Configuration	105
3.3.4 Walled Garden List	107
3.3.5 Proxy Server Properties	108
3.3.6 Dynamic DNS	109
3.4 Utilities	110
3.4.1 Change Password	110
3.4.2 Backup/Restore Settings	112
3.4.3 Firmware Upgrade	113
3.4.4 Restart	113
3.5 Status.....	114
3.5.1 System Status.....	114
3.5.2 Interface Status.....	116
3.5.3 Concurrent Users.....	118
3.5.4 Traffic History.....	118
3.5.5 Notify Configuration	120
3.6 Help	121
4. Appendix A --- Console Interface	122
5. Appendix B --- Configuration on Authorize.Net	125
6. Appendix C --- Proxy Setting for Hotspot.....	130
7. Appendix D --- Proxy Setting for Enterprise.....	133
8. Appendix E --- Disclaimer for On-Demand Users	138

1. Introduction

The PLANET Wireless Subscriber Gateway WSG-404 is a compact intelligent gateway integrated with a four-port port-based switch. It provides Plug & Play Internet access, advanced security and network management.

The WSG-404 is designed for service providers, system integrator or hotspot venue operator without backend-RADIUS-Server to have integrated solution for rapid deployment, which can start hotspot service quickly and easily and enhance service performance.

The WSG-404 is an ideal solution for hotel lobbies, coffee bars, airport lounges, conference facilities and other sites that commonly host business travelers, and offers instant high-speed Internet connections. With its IP Plug and Play technology, it accepts any client configuration login, when client open browser the WSG-404 immediately recognizes new end-user and redirects their browser to customized Web pages. There's no need for end-user to change any of their default network (Static IP), e-mail (SMTP Server behind firewall), or browser settings (HTTP Proxy) or load any special software to access hotspot service. It's completely Plug' Play with any browser.

1.1 Package Contents

Please inspect your package. The following items should be included in the WSG-404 packages:

- 1x WSG-404 unit
- 1x Power Adapter
- 1x User's Manual CD
- 1x Quick Installation Guide
- 1x RJ-45 Cable
- 1x RS-232
- 2x Antenna

If any of the above items are damaged or missing, please contact your dealer immediately.

Optional Product that can co-work with WSG-404:

WSG-ACG4 Account Generator Printer

- 1x Power Adapter
- 1x RJ-11 Cable
- 1x Quick Installation Guide

This Account Generator is an optional device that can work with WSG-404. With this Account Generator it is much easier for operator to create the accounts for any guests. Without the Account Generator, all the account generation can be done through Administrator's Web management page. The demand of this Account Generator can vary on the install site

1.2 Features

- **Ideal Hot Spot solution**
Via the integrated 802.11g wireless interface, mobile users can establish high speed Internet access without any configuration.
- **Zero configuration (Plug-n-Play) Internet access**
WSG-404 translates proper IP address information for Internet access, all IP configurations, either DHCP, Private IP or Static IP information will be turned into Internet-ready configurations. Subscribers won't feel the difference, and no need to face to the inconvenience of IP reconfigurations.
- **Built-in proprietary AAA mechanism and billing system**
PLANET WSG-404 integrates Web-based Authentication (including subscriber SSL logon page), selective Web-based Accounting, and proprietary billing mechanism, which can help you to prepare a billing mechanism in a very short time and bring most convenience, the least efforts for billing applications.
- **RADIUS AAA support**
WSG-404 provides standard based Radius Client to communicate with any standard based Radius server, in order to support AAA (Authentication, Authorization and Accounting).
- **Exclusive Printer Accounting (Optional)**
Machine operators may customize the printout information for different billing application.
- **Security and Firewall**
With built-in 64/128-bit RC4 WEP Encryption, VLAN Security for Wireless, subscriber SSL Login Page / Admin Page, VPN (IPSec/PPTP) Pass through...various security features, PLANET WSG-404 bring you an ease-of-use and most comfort safe Internet access environment.
- **Ease-of-Use and Management**
The built-in web management interface in WSG-404 brings most convenience to system administrators or machine operators while configuring machine or setting up subscriber privileges in movements. With time increments, clerks or machine operators may print out, billing and other user information with time increments are conveniently printed on the button-operated printer included with the PLANET WSG-404. Time increments may be compiled simply by pressing the printer button multiple times. No computers or complex back-end subscriber management systems are required for deployment.
- **Virtual Server & DMZ Capability**
The standard and user-defined Virtual server gives the WSG-404 has the most flexibility to share local resources like Email, FTP or HTTP servers to the Internet in a more secure way. The DMZ (De-Militarized Zone) capability helps LAN users to act like an independent Internet node that communicates to the Internet in both directions while maintaining security for LAN users.

Note:

The "PnP" Function only can be used with TCP/IP-based Network.

1.3 Precautions

- Never remove or open the cover. You may suffer serious injury if you touch these parts.
- Never install the system in the wet locations.
- Use only the original fitting AC power adapter otherwise there is a danger of severe electrical shock.
- Avoid exposing the WSG-404 to direct sunlight or another heat source.
- Choose a well-ventilated area to position your WSG-404.

1.4 Outlook



Figure 1-1 WSG-404 Outlook

1.4.1 Top Panel

The top panel of the WSG-404 is shown below.

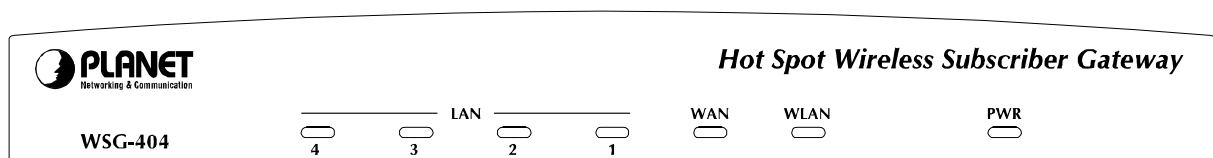


Figure 1-2 WSG-404 Top Panel

LEDs Indication

LED	Color	Status	Description
PWR	Green	Off	The device is turned off
		On	The device is turned on
WLAN	Green	Off	The wireless is not ready
		On	The wireless is ready
		Flashing	The wireless data transmission
WAN	Green	Off	The WAN is not connected
		On	The WAN has a successful (10/100Mbps) Ethernet connection
		Flashing	The WAN is sending or receiving packet
LAN 1~4	Green	Off	The LAN is not connected
		On	The LAN has a successful (10/100Mbps) Ethernet connection
		Flashing	The LAN is sending or receiving packet

Note:

1. Use only the bundled DC adapter for the power system, other power adapter could damage the device permantly.
2. During the firmware upgrade process, please do not power off the device, otherwise it could damage the device permantly.

1.4.2 Rear Panel

The rear panel of the WSG-404 is shown below.

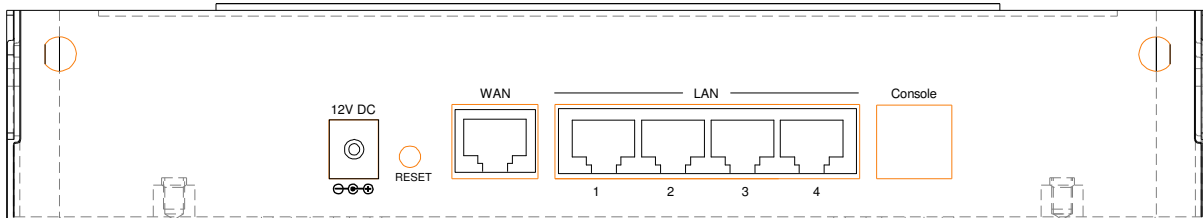


Figure 1-4 WSG-404 Rear Panel

Port Indication

	Power	Reset	WAN	LAN 1	LAN 2	LAN 3	LAN 4	Console
Printed on Housing	12V DC	RESET	WAN	1	2	3	4	Console
Interface	Power	Button	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45	RJ-11

POWER:

The power adaptor plugs here.

RESET:

Used for restarting the system.

WAN:

One RJ-45 port is used for connecting xDSL or Cable Mode to the Internet/Intranet.

LAN1~2:

Used for Connecting to the public LAN. It can be chosen to require authentication to access network resource and the Internet.

LAN3~4:

Used for Connecting to the private LAN. Authentication is not required to access the network resource from here.

Console:

Used for configuring the system via Hyper Terminal or connecting to the WSG-ACG4 (Ticket Printer).

1.5 Technical Specifications

1.5.1 Hardware Specifications

Ports	LAN	4 x RJ45 (10Base-T/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X) 1 x 802.11g wireless AP interface
	WAN	1 x RJ45 (10Base-T/100Base-TX, Auto-Negotiation)
	Console	1 x RJ11
Wireless Data rate		Up to 54Mbps with Auto fall back with 802.11b
Wireless Encryption		WEP 64/128 bit WPA with TKIP
Wireless Authentication		IEEE 802.1x (EAP-MD5, EAP-TLS, CHAP, PEAP) WPA-PSK
Wireless Antenna Type		2dBi (Max) Dual detachable diversity antenna with reverse SMA
Wireless Operating Range		Open Space: 100~300m Indoors: 35~100m
LED Indicators		1 x POWER LED 1 x WLAN Link/Activity LED 1 x WAN Link/Activity LED 4 x LAN Link/Activity LEDs
Environmental		Operating Temperature: 5 ~ 45 °C Relative Humidity: 10 ~ 80 % (non-condensing) Storage Temperature: - 25 ~ 55 °C Relative Humidity: 5 ~ 90 % (non-condensing)
Electrical		External Power Adaptor Power Input: 12V DC, 1.5A
Regulatory Compliance		FCC part 15 Class B CE Mark Class B
Dimension		230 x 150 x 45.5 mm (W x D x H)
Weight		1.4 Kg

1.5.2 Software Specifications

Network	<p>IEEE802.3 10BaseT Ethernet IEEE802.3u 100BaseTX Fast Ethernet IEEE802.11b 11Mbps IEEE802.11g 54Mbps Supports 50 Simultaneous Users IP Plug and Play (IP PnP) Supports External HTTP Proxy Servers; Built-in Proxy Server WEP Data Encryption 64/128 bit WPA with TKIP; Radius SMTP Server Redirection DHCP Server DHCP Relay NAT IP Routing Dynamic DNS Walled Garden: Up to 20 Session Number: Max. 16384 Supports NTP (Network Time Protocol)</p>
WAN Connection Type	<p>DHCP WAN Client PPPoE WAN Client PPTP WAN Client Static IP WAN Client</p>
AAA / Billing	<p>Built-in Authentication Exclusive Printer Accounting without PC operating Web-based Login Page Authentication Web-based Accounting Flexible Billing Profiles and Price Plan Flexible Billing Mechanism Flexible Time Mechanism (Time to Finish and Accumulation) External DB25 Support (WSG-ACG4) RADIUS Authentication Credit Card Support (Authorize.net, *PayPal) 10 Customizable Billing Profile Remaining Credit Reminder Accumulation Billing Account log *Future feature</p>
Security	<p>Layer 2 Isolation SSL Login Page SSL Administration VPN Pass through (IPSec/PPTP) Pass through Destination IP/URL Pass through Source IP/MAC Restricted Destination Filtering IP/URL Share LAN Resources Customize SSL Certificate DoS Attack Protection IEEE 802.1x (EAP-MD5, EAP-TLS, CHAP, PEAP)</p>
Management	<p>Supports Multiple Authentication Methods (Local and On-demand, LDAP, POP3(s), RADIUS, NT Domain)</p>

Supports Multiple Logins with One Single Account
SSL Protected Login Portal Page
Administrator/Manager/Operator Management Access
Local Account: Max. **500**
Supports Guest Accounts: Up to **10**
Customize Login/Logout Page
Remote Browser-based Configuration and Management
Policy-based Access Control
IP-based/MAC-based Privilege List
Friendly Notification E-mail
Backup/Restore/Factory Default Setting
Remote Firmware Upgrade
System Information Table
Per-user Traffic History Log
Support External Syslog Server
Billing Report Summary
Bandwidth Control
Session Idle Timer
Session/Account Expiration Control
Secure Remote via PPTP VPN
Supports SNMP V2
SSL Certificate Upload

2. Installation

The followings are instructions for setting up the WSG-404. Refer to the illustration and follow the simple steps below to quickly install your WSG-404.

2.1 Installation Requirements

Before installing the WSG-404, make sure your network meets the following requirements.

2.1.1 System Requirements

- Cable modem or DSL/ADSL modem.
- Network cables: Use standard 10/100Base-TX network (UTP) cables with RJ45 connectors.
- Subscriber PC installed with Wireless adapter that complied with 802.11b, or 802.11g.
- Workstations of subscribers running Windows 95/98/ME, NT4.0, 2000/XP, MAC OS9 or later, Linux, UNIX or other platform compatible with TCP/IP protocols.
- <Optional> Account generator (Model No.: WSG-ACG4).

2.1.2 ISP Requirements

Verify whether your ISP use fixed or dynamic IP. If it is a fixed IP, be sure to get the IP from your ISP. For dynamic IP, which is mostly used, the PC will get the IP automatically whenever it hooks up on the modem.

Dynamic IP

- Dynamic IP Setting

Fixed IP

- Your fixed IP address for the WSG-404
- Your subnet mask for the WSG-404
- Your default gateway IP address
- Your DNS IP address

PPPoE

- Your user name from your ISP
- Your password from your ISP

PPTP

- PPTP Server IP Address from your ISP
- PPTP Local IP address from your ISP
- PPTP Local IP subnet mask from your ISP
- Your user name from your ISP
- Your password from your ISP

2.1.3 Your PC Requirements

The Static IP settings for the PC

- Your PC's fixed IP address
- Your PC's subnet mask
- Your PC's default gateway IP address
- Your PC's primary DNS IP address

Note:

1. The gateway's default IP address setting is “**LAN1&LAN2: 192.168.2.254, LAN3&LAN4: 192.168.1.254**”
 2. The gateway's default subnet mask setting is “**255.255.255.0**”
-

The Dynamic IP settings for the PC

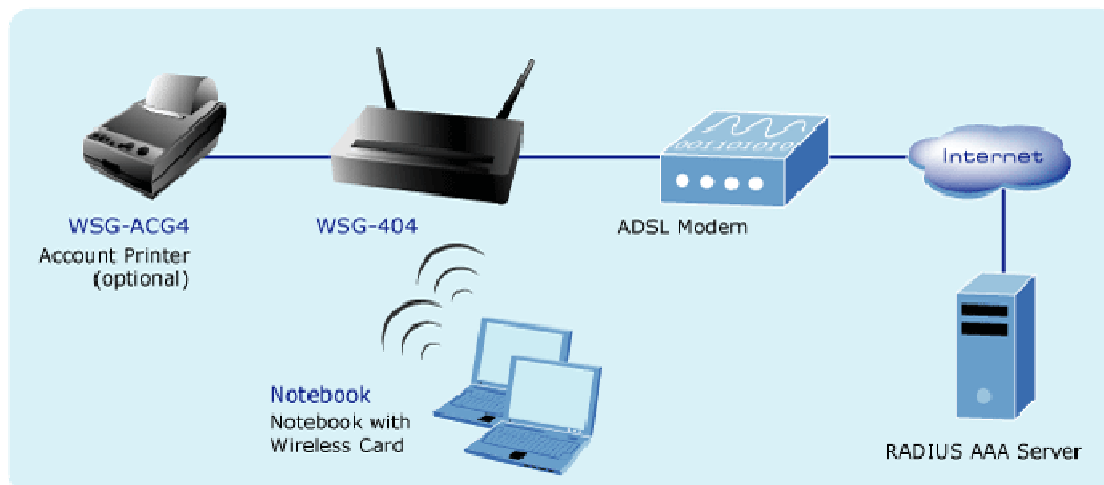
We recommend that you leave your IP settings as automatically assigned. By default, the WSG-404 is a DHCP server, and it will give your PC the necessary IP settings.

Note:

Before turn on the WSG-404, make sure there is no other DHCP server in the LAN network; otherwise it will influence the whole network operation.

2.2 Hardware Connection and Installation

2.2.1 Physical Installation



Physical connection of WSG-404

1. Ensure the WSG-404 and the Cable/DSL modem are powered OFF before commencing. Leave your Cable/DSL modem connected to its wall socket (phone line or cable input).
2. Use Ethernet cables to connect to the **LAN1/LAN2** port on the rear panel. Connect the other end of the Ethernet cable to an AP or Switch. (Note: Authentication is required for the clients to access the network via **LAN1/LAN2** port. The LAN port with authentication function is referred to as **Public LAN**).
3. Use Ethernet cables to connect to the **LAN3/LAN4** port on the rear panel. Connect the other end of the Ethernet cable to a PC. (Note: Authentication is **NOT** required for the clients to access the network via **LAN3/LAN4** port. The LAN port with authentication function is referred to as **Private LAN**).
4. Connect your Cable/DSL Modem to the **WAN** port on the rear panel. Use the cable supplied with your Cable/DSL modem. If no cable was supplied with your modem, use a standard network cable. Please make sure the connection is established (LED is on).
5. Connect the Power Adapter. Use only the unit provided.
6. Power ON. The **PWR** LED should stay on (If your network is connected, the WAN/WLAN/LAN LED will be on, too).
7. Power on the PC that connected to the WSG-404.

2.3 Software Configuration

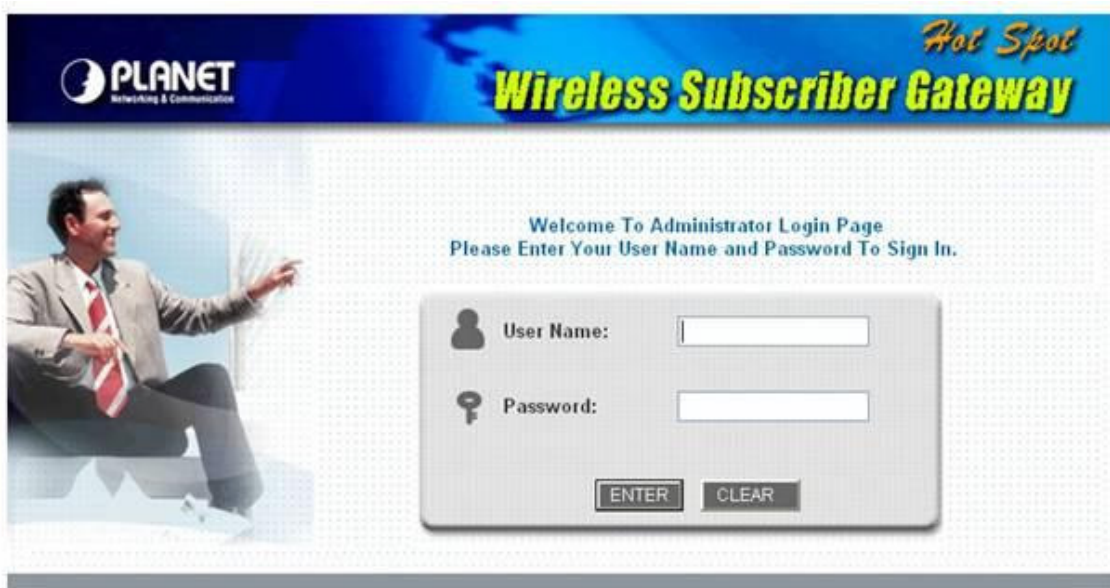
2.3.1 Quick Configuration

There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard has 7 steps providing a simple and easy way to guide you through the setup of PLANET WSG-404. Follow the procedures and instructions given by the Wizard to enter the required information step by step. After saving and restarting PLANET WSG-404, it is ready to use. There will be 7 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. **Set Wireless – Access Point Connection**
7. **Save and Restart PLANET WSG-404**

To access the web management interface, connect the PC and WSG-404 in advance via the Private Port of WSG-404. Then, launch the web browser and enter the IP address of the gateway for that port in the address field then pres **Enter**. Default IP address of the default gateway of the Private Port is <https://192.168.2.254> (Note: **https** is used for a secured connection).

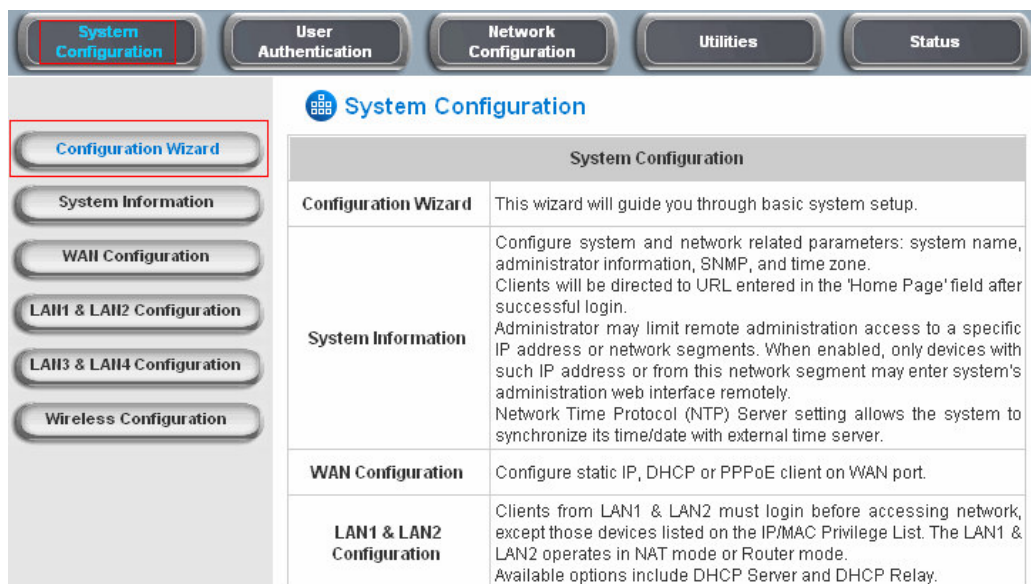
The administrator login page will appear. Enter **default username “admin” & default password “admin”** in the User Name and Password fields. Click **Enter** to login.



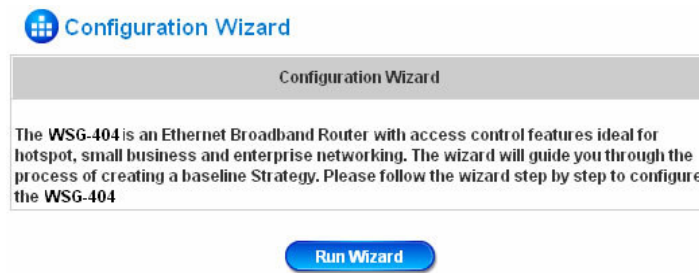
After successfully logging into WSG-404, a web management interface with a welcome message will appear.



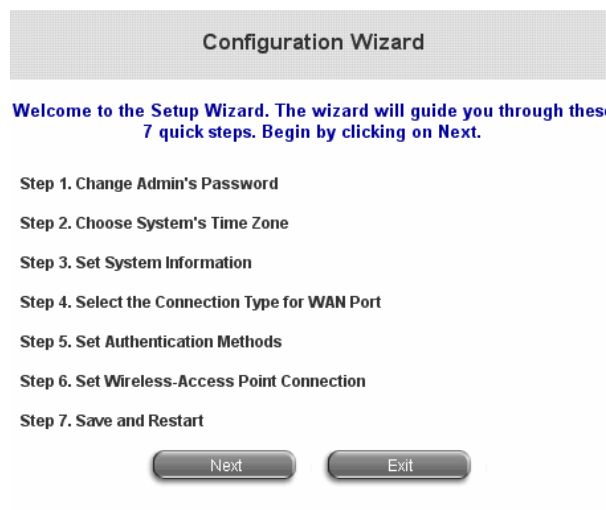
Click **System Configuration** to the System Configuration screen and run the **Configuration Wizard** to help you complete the configuration.



Click **Run Wizard** to begin the **Configuration Wizard**



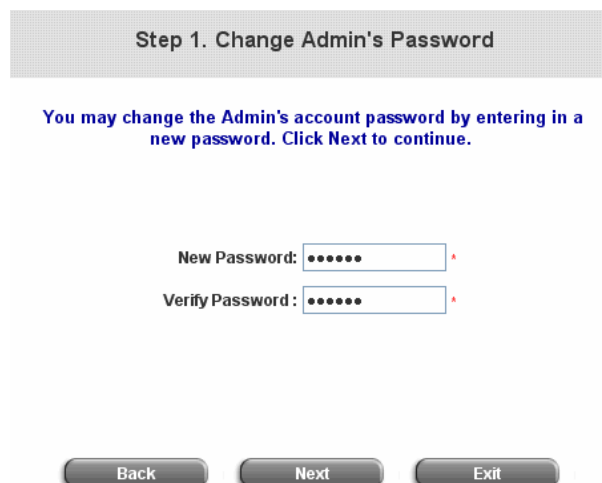
After clicking **Run Wizard**, the **Configuration Wizard** will appear in a pop-up browser window. Click "**Next**" to begin.



Step 1: Change Admin's Password

Enter a new password for the admin account and retype it in the verify password field (Twenty characters maximum and no spaces allowed).

Click "**Next**" to continue.



Step 2: Choose System's Time Zone

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

Click **“Next”** to continue.

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

Step 3: Set System Information

Home Page: Enter the URL that users should be initially directed to when successfully authenticated to the network.

NTP Server: Enter the URL of external time server for WSG-404 time synchronization or use the default server.

DNS Server: Enter a DNS Server provided by your ISP. Contact the ISP if the DNS IP Address is unknown.

Click **“Next”** to continue.

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

Step 4: Select the Connection Type for WAN Port

There are three types of WAN port to select from: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**. Select a proper Internet connection type.

Click “**Next**” to continue.

Step 4. Select the Connection Type for WAN Port

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

<input checked="" type="radio"/> Static IP Address	Choose it to set static IP address.
<input type="radio"/> Dynamic IP Address	Choose it to obtain an IP address automatically. (For most cable modem users.)
<input type="radio"/> PPPoE Client	Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)

Step 4(Cont): Set Static IP Address Information

Enter the **IP Address**, **Subnet Mask** and **Default Gateway** as the examples provided by the ISP.

Click “**Next**” to continue.

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

Click Next to continue.

IP Address:	<input type="text" value="210.66.155.73"/>	*
Subnet Mask:	<input type="text" value="255.255.255.224"/>	*
Default Gateway:	<input type="text" value="210.66.155.94"/>	*

Step 4(Cont): Set PPPoE Client's Information after selecting PPPoE Client

Enter the **Username** and **Password** provided by the ISP.

Click "**Next**" to continue.

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

Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)

Username: *

Password: *

Step 5: Select Authentication Methods

Please specify the policy name for this authentication method. The Postfix field (e.g. Local) will be used as the postfix name (e.g. username@Local). An authentication method has to be selected from one of the five options appeared in this window (Local User is selected for this setup example). Local User is an authentication method that uses the built-in user account database supported by WSG-404.

Click "**Next**" to continue.

Step 5. Set Authentication Methods

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

Postfix: *

(Is postfix name.)

Policy: ▼

Local User LDAP

POP3 NT Domain

RADIUS

Step 5(Cont.): 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) and **MAC** (optional) and assign a policy to this particular user (or use the default). Upon completing adding a user, more users can be added to this authentication method by clicking the ADD bottom.

Click **“Next”** to continue.

Step 5 (Cont). Add User

Click **“ADD”** button to add Local User. Click **Next** to continue.

Username:

Password:

MAC: (XXXXXXXXXX)

Policy: None

Step 6: Set Wireless Access-Point Connection

SSID: Enter a SSID (Up to 32 characters) for the system. The default is **WSG-404**. SSID is a unique identifier used for the wireless users’ devices to associate with WSG-404.

Transmission Mode: WSG-404 supports two transmission modes, 802.11b and 802.11(b+g). Select the appropriate transmission mode to work with the wireless clients in the network.

Channel: If the default channel used by many other APs, it is necessary to select another channel form the Channel field for a better performance.

Click **“Next”** to continue.

Step 6. Set Wireless Access-Point Connection

Enter the SSID name and channel number to be used for the Wireless Access-Point. Click **Next** to continue.

SSID:

Transmission Mode: 802.11(b+g)

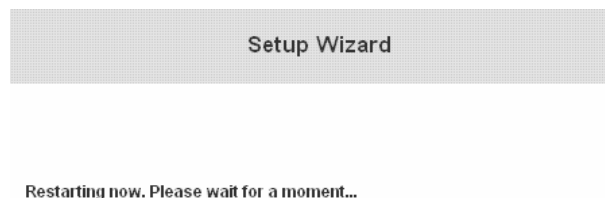
Channel: 1

Step 7: Save and Restart WSG-404

Click **Restart** to save the current settings and restart WSG-404. The Setup Wizard is now completed.



During PLANET WSG-404 restart, a “**Restarting now. Please wait for a moment...**” message will appear on the screen. Please do not interrupt PLANET WSG-404 until the **Configuration Wizard** window has disappeared. This indicates that the restart process has completed



Note:

If you wish go back to modify the setting during every steps of the wizard. Please click the **Back** button to go back to the previous step.

2.3.2 External Network Access

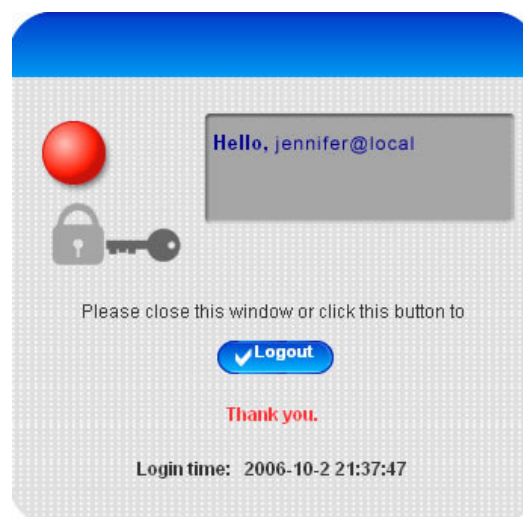
If all the steps are set properly, PLANET WSG-404 can be further connected to the managed network to experience the controlled network access environment. Firstly, connect an end-user device to the network at PLANET WSG-404's LAN1/LAN2 and set to obtain an IP address automatically. After the network address is obtained at the user end, open an Internet browser and link to any website. Then, the default logon webpage will appear in the Internet browser.

1. First, connect a user-end device to LAN1/LAN2 port of the PLANET WSG-404, and set the dynamical access network. After the user end obtains the network address, please open an Internet browser and the default login webpage will appear on the Internet browser. Key in the username and password created in the local user account or the on-demand user account in the interface and then click **Submit** button. Here, we key in the local user account (e.g. **test@Local** for the username and **test** for the password) to connect the network.



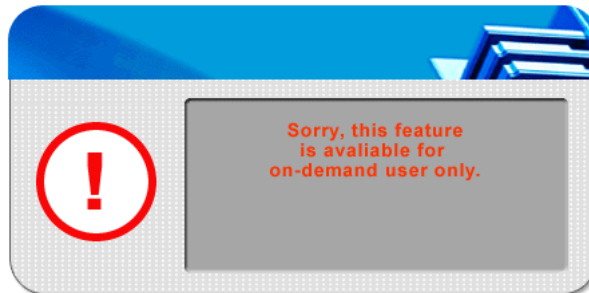
The screenshot shows a web browser window titled "User Login Page". The page has a blue header with the title. Below the header, it says "Welcome To User Login Page!" and "Please Enter Your User Name and Password To Sign In.". There are two input fields: "User Name:" with the value "jennifer@local" and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

2. Login page appearing means PLANET WSG-404 has been installed and configured successfully. Now, the user can browse the network or surf the Internet.

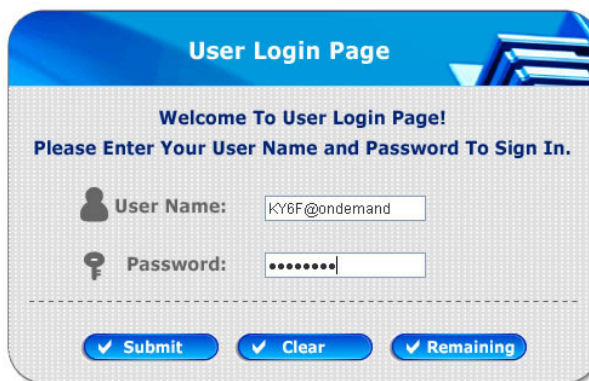


The screenshot shows a web browser window with a blue header. On the left, there is a red circle and a padlock icon. On the right, a grey box contains the text "Hello, jennifer@local". Below this, it says "Please close this window or click this button to" followed by a "Logout" button. At the bottom, it says "Thank you." and "Login time: 2006-10-2 21:37:47".

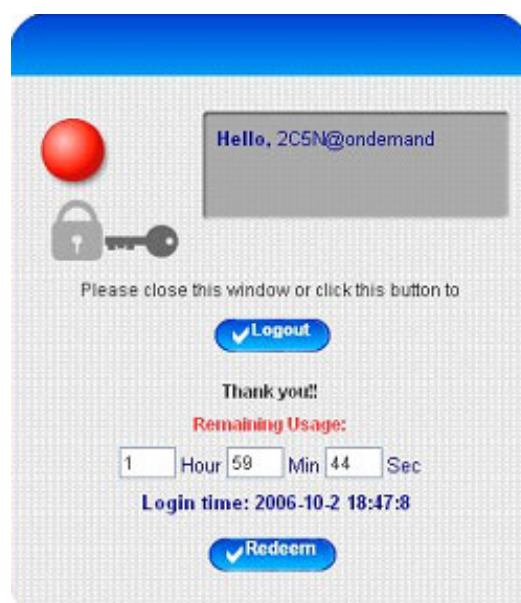
3. If the screen shows “**Sorry, this feature is available for on-demand user only**”, the “**Remaining**” button has been clicked. This button is only for on-demand users. For users other than on-demand users, please click the **Submit** button.



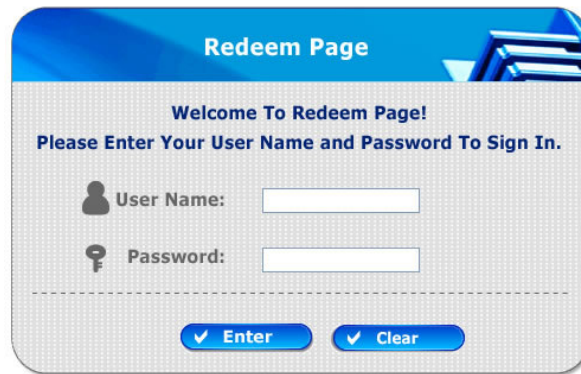
4. An on-demand user can enter the username and password in the “**User Login Page**” and click the **Remaining** button to view the remaining time the account.



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 rest of use time that the on-demand user can surf Internet.
- **Redeem:** When the remaining time or data size is insufficient, the user has to pay for adding credit at the counter, and then, the user 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.



The image shows a screenshot of a web page titled "Redeem Page". The page has a blue header with the title. Below the header, there is a welcome message: "Welcome To Redeem Page!" followed by "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 two buttons: "Enter" and "Clear".

Note:

The system will automatically reject the redeem process when the redeem amount exceeds the maximum time/data volume provided by PLANET WSG-404.

3. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table shows all the functions of PLANET WSG-404.



OPTION	System Configuration	User Authentication	Network Configuration	Utilities	Status
FUNCTION	Configuration Wizard	Authentication Configuration	Network Address Translation	Change Password	System Status
	System Information	Black List Configuration	Privilege List	Backup/Restore Settings	Interface Status
	WAN Configuration	Policy Configuration	Monitor IP List	Firmware Upgrade	Current Users
	LAN1 & LAN2 Configuration	Guest User Configuration	Walled Garden List	Restart	Traffic History
	LAN3 & LAN4 Configuration	Additional Configuration	Proxy Server Properties		Notify Configuration
	Wireless Configuration		Dynamic DNS		

3.1 System Configuration

This section includes the following functions:

Configuration Wizard, System Information, WAN Configuration, LAN1 & LAN2 Configuration, LAN3 & LAN4 Configuration and Wireless 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.
WAN Configuration	Configure static IP, DHCP or PPPoE client on WAN port.

3.1.1 Configuration Wizard

There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard has 7 steps providing a simple and easy way to go through the basic setups of PLANET WSG-404 and is served as **Quick Configuration**. Please refer to **2.3.1 Quick Configuration** for the introduction and description of **Configuration Wizard**.

Configuration Wizard

The WSG-404 is an Ethernet Broadband Router with access control features ideal for hotspot, small business and enterprise networking. The wizard will guide you through the process of creating a baseline Strategy. Please follow the wizard step by step to configure the WSG-404

Run Wizard

3.1.2 System Information

These are some main information about PLANET WSG-404. Please refer to the following description for these blanks:

System Information	
System Name	<input type="text" value="WSG-404"/>
Administrator Info	<input type="text" value="Sorry! The service is temporarily unavailable."/> <small>(Fill appear when Internet connection fails.)</small>
Device Name	<input type="text"/> <small>(FQDN for this device)</small>
Home Page	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="http://www.planet.com.tw"/>
Access History IP	<input type="text"/> <small>(e.g. 192.168.2.1)</small>
Remote Manage IP	<input type="text"/> <small>(e.g. 192.168.3.1 or 192.168.3.0/24)</small>
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
User Logon SSL	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time	Device Time : 2006/11/06 13:07:59 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"/> <small>*e.g. tock.usno.navy.mil</small> 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.ufjf.br"/> NTP Server 5: <input type="text" value="ntp1.cs.mu.OZAU"/> <input type="radio"/> Set Device Date and Time

- **System Name:** Set the system's name or use the default.
- **Administrator Info:** Enter the Administrator's information here, such as administrator's name, telephone number, e-mail address, etc. If users encountered problems in the connection of the WAN port to the system, this information will appear on the user's login screen.
- **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, 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 WSG-404. An example is provided as follows and "10.2.3.213" is the WAN IP of PLANET WSG-404.

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

#Date	System Name	Type	Name	IP	MAC	Packets In	Bytes In	Packets Out	Bytes Out	Expiration	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
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
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	30

- **Remote Manage IP:** Set the IP block with a system which is able to connect to the web management interface via the authenticated 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 WSG-404.
- **SNMP:** PLANET WSG-404 supports SNMPv2. If the function is enabled, administrators can 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 WSG-404 supports NTP communication protocol to synchronize the network time. Please specify the IP address of a server in the system configuration interface for adjusting the time automatically. (Universal Time is Greenwich Mean Time, GMT). Time can be set manually by selecting “**Set Device Date and Time**”. Please enter the date and time for these fields.

Device Time : 2006/11/06 13:07:59

Time Zone:

(GMT+08:00)Taipei

NTP Enable

Set Device Date and Time

-- Year -- Month -- Day

-- Hour -- Minute -- Second

3.1.3 WAN Configuration

There are 4 methods of obtaining IP address for the WAN Port: **Static IP Address**, **Dynamic IP Address**, **PPPoE** and **PPTP Client**.

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

WAN Configuration	
WAN Port	<input checked="" type="radio"/> Static IP Address
	IP Address: <input type="text" value="10.2.3.26"/> *
	Subnet Mask: <input type="text" value="255.255.255.0"/> *
	Default Gateway: <input type="text" value="10.2.3.254"/> *
	Preferred DNS Server: <input type="text" value="168.95.1.1"/> *
	Alternate DNS Server: <input type="text"/>
<input type="radio"/> Dynamic IP Address	
<input type="radio"/> PPPoE Client	
<input type="radio"/> PPTP Client	

IP address: the IP address of the WAN port.

Subnet mask: the subnet mask of the WAN port.

Default gateway: the gateway of the WAN port.

Preferred DNS Server: the primary DNS Server of the WAN port.

Alternate DNS Server: The substitute DNS Server of the WAN 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.

WAN Configuration	
WAN Port	<input type="radio"/> Static IP Address
	<input checked="" type="radio"/> Dynamic IP Address <input type="button" value="Renew"/>
	<input type="radio"/> PPPoE Client
	<input type="radio"/> PPTP Client

- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the “**User Name**”, “**Password**”, “**MTU**” and “**CLAMP MSS**”. 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.

WAN Configuration	
WAN Port	<input type="radio"/> Static IP Address <input type="radio"/> Dynamic IP Address <input checked="" type="radio"/> PPPoE Client <input type="radio"/> PPTP Client
	Username: <input type="text" value="admin"/> *
	Password: <input type="password" value="*****"/> *
	MTU: <input type="text" value="1492"/> bytes (Range:1000~1492)*
	CLAMP MSS: <input type="text" value="1400"/> bytes (Range:980~1400)*
	Dial on Demand: <input type="radio"/> Enable <input checked="" type="radio"/> Disable

- **PPTP Client:** 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 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.

WAN Configuration	
WAN 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"/> *
	Preferred DNS Server: <input type="text"/> *
	Alternate DNS Server: <input type="text"/>
	PPTP Server IP: <input type="text"/> *
	Username: <input type="text"/> *
	Password: <input type="password"/> *
PPTP Connection ID/Name: <input type="text"/>	
Dial on Demand: <input type="radio"/> Enable <input checked="" type="radio"/> Disable	

WAN Configuration	
WAN 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"/>
	Dial on Demand: <input type="radio"/> Enable <input checked="" type="radio"/> Disable

3.1.4 LAN1 & LAN2 Configuration

User authentication for the two LAN ports can be enabled or disabled.

LAN1 & LAN2 Configuration	
LAN1 & LAN2	IP PNP <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	User Authentication <input checked="" type="radio"/> Enable <input type="radio"/> Disable
	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

- LAN1 & LAN2 Port

LAN1 & LAN2 Port	IP PNP <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	User Authentication <input checked="" type="radio"/> Enable <input type="radio"/> Disable
	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"/>

IP PNP: Users can use static IP address to connect to the system. Regardless of what the IP address at the user end is, users can still be authenticated through PLANET WSG-404 and access the network.

User Authentication: Choose to enable or disable this function. If “**User Authentication**” is disabled, users can access Internet without being authenticated.

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 LAN1 & LAN2 port.

Subnet Mask: Enter the desired subnet mask for the LAN1 & LAN2 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 asterisks are required to be filled in.

DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server DHCP Scope Start IP Address: <input type="text" value="192.168.1.1"/> * End IP Address: <input type="text" value="192.168.1.100"/> * Preferred DNS Server: <input type="text" value="168.95.1.1"/> * Alternate DNS Server: <input type="text"/> Domain Name: <input type="text" value="planet.com.tw"/> * WINS Server IP: <input type="text"/> Lease Time: <input type="text" value="1 Day"/> <input type="button" value="v"/> Reserved IP Address List <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 Public 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 IP Address: 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 for IP address outside the DHCP range 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 mandatory). Click **Apply** to complete the setup.

Reserved IP Address List - LAN1 & LAN2			
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) First Prev Next Last			

3. **Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. 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"/> *
----------------------------------	--

3.1.5 LAN3 & LAN4 Configuration

In this section, set the related configuration for LAN3/LAN4 port and DHCP server.

LAN3 & LAN4 Configuration	
LAN3 & LAN4	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 type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server
	DHCP Scope
	Start IP Address: <input type="text" value="192.168.2.1"/>
	End IP Address: <input type="text" value="192.168.2.100"/>
	Preferred DNS Server: <input type="text" value="168.95.1.1"/>
	Alternate DNS Server: <input type="text"/>
	Domain Name: <input type="text" value="planet.com.tw"/>
	WINS Server IP: <input type="text"/>
	Lease Time: <input type="text" value="1 Day"/>
	Reserved IP Address List
<input type="radio"/> Enable DHCP Relay	

- LAN3 & LAN4 Port

LAN3 & LAN4 Port	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"/>

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

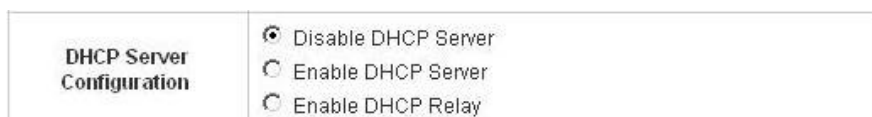
IP Address: Enter the desired IP address for the LAN3 & LAN4 port.

Subnet Mask: Enter the desired subnet mask for the LAN3 & LAN4 port.

• DHCP Server Configuration

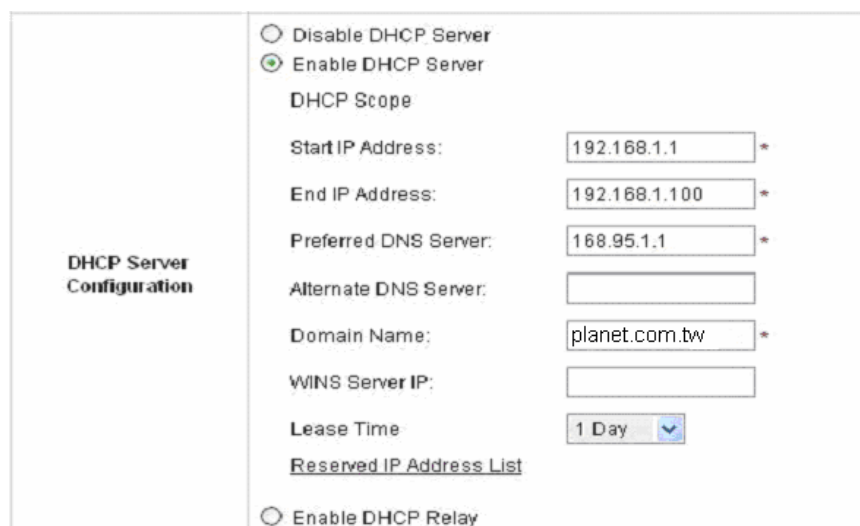
There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

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



The screenshot shows the 'DHCP Server Configuration' section with three radio button options: 'Disable DHCP Server' (selected), 'Enable DHCP Server', and '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 asterisks are required to be filled in.



The screenshot shows the 'DHCP Server Configuration' section with 'Enable DHCP Server' selected. The 'DHCP Scope' section includes the following fields: 'Start IP Address' (192.168.1.1), 'End IP Address' (192.168.1.100), 'Preferred DNS Server' (168.95.1.1), 'Alternate DNS Server' (empty), 'Domain Name' (planet.com.tw), and 'WINS Server IP' (empty). The 'Lease Time' is set to '1 Day'. A red asterisk is present next to the Start IP Address, End IP Address, Preferred DNS Server, and Domain Name fields. A hyperlink for 'Reserved IP Address List' is visible below the Lease Time field. The 'Enable DHCP Relay' option is also present at the bottom.

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 IP Address: Enter the IP address of WINS.

Lease Time: Choose the time to update 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 for IP address outside the DHCP range is desired, click the **Reserved IP Address List** on the management interface. 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 mandatory). Click **Apply** to complete the setup.

Reserved IP Address List - LAN3 & LAN4			
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) First Prev Next Last			

3. **Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. 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"/> *
----------------------------------	--

3.1.6 Wireless Configuration

This section is for setting related configurations for the wireless port.

Wireless Configuration	
Basic Configuration	SSID: <input type="text" value="WSG-404"/> *
	<input checked="" type="checkbox"/> Sync To Ticket
	Transmission Mode: <input type="text" value="802.11(b+g)"/> ▼
	Channel: <input type="text" value="1"/> ▼
	SSID Broadcast: <input checked="" type="checkbox"/>
	Layer2 Client Isolation: <input checked="" type="checkbox"/>
Security Advance	
Wireless Port	IP PNP: <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	User Authentication: <input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Operation Mode: <input type="text" value="NAT"/> ▼
	IP Address: <input type="text" value="192.168.3.254"/> *
	Subnet Mask: <input type="text" value="255.255.255.0"/> *
DHCP Server Configuration	<input type="radio"/> Disable DHCP Server
	<input checked="" type="radio"/> Enable DHCP Server
	DHCP Scope
	Start IP Address: <input type="text" value="192.168.3.100"/> *
	End IP Address: <input type="text" value="192.168.3.200"/> *
	Preferred DNS Server: <input type="text" value="168.95.1.1"/> *
	Alternate DNS Server: <input type="text"/>
	Domain Name: <input type="text" value="planet.com.tw"/> *
	WINS Server IP: <input type="text"/>
	Lease Time: <input type="text" value="1 Day"/> ▼
Reserved IP Address List	
WDS Configuration	<input type="radio"/> Enable DHCP Relay
	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply

Clear

• Basic Configuration

Basic Configuration	SSID	WSG-404 *
		<input checked="" type="checkbox"/> Sync To Ticket
	Transmission Mode	802.11(b+g) v
	Channel	1 v
	SSID Broadcast	<input checked="" type="checkbox"/>
	Layer2 Client Isolation	<input checked="" type="checkbox"/>
	Security Advance	

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, must not exceed 32 characters and may be any character on the keyboard. Administrators can give a new name in this field or use the default name.

Sync to Ticket: Synchronize the SSID of ticket with this system.

Channel: Select the appropriate channel from the list to correspond to the network settings; for example, 1 to 11 channels are suitable for the North America area. All points in the wireless network must use the same channel in order to make sure correct connection.

Transmission Mode: There are 2 modes to select from, **802.11b** (2.4G, 1~11Mbps) and **802.11 (b+g)** (2.4G, 1~11Mbps and 2.4G, 54Mbps).

SSID Broadcast: Select to enable the SSID broadcast in the network. When configuring the network, this function may be enabled but should be disabled when configuration is finished. Since when SSID Broadcast is enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to the network.

Layer2 Client Isolation: This function can be enabled to isolate any client from each other.

Security: For security settings in detail, please click the hyperlink **Security** to go into the **Security** page. Choose “**Enable**” to configure the setting.

Security	
WEP Key	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Security	
WEP Key	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WEP Key Encryption	<input checked="" type="radio"/> 64bits <input type="radio"/> 128bits
Mode	HEX ▾
	<input checked="" type="radio"/> 1. <input type="text"/>
	<input type="radio"/> 2. <input type="text"/>
	<input type="radio"/> 3. <input type="text"/>
	<input type="radio"/> 4. <input type="text"/>

1. **WEP Key: Wired Equivalent Privacy.** If using this function is desired, please choose “Enable”.
2. **WEP Key Encryption:** This is a data privacy mechanism based on a 64-bit or 128-bits shared key algorithm.
3. **Mode:** There are two types of encryption, **HEX** and **ASCII**. After selecting one of them, please enter the related information in the blanks below.

Advance: For advance settings in detail, please click the hyperlink **Advance** to go into the **Advance** page.

Advance	
Authentication Type	Auto ▾ (Default : Auto)
Transmission Rates	Auto ▾ (Default : Auto)
CTS Protection Mode	Disable ▾ (Default : Disable)
Basic Rates	Set1 ▾ (Default : Set1)
Beacon Interval	100 <input type="text"/> (Default : 100, Milliseconds, Range : 20-1000)
RTS Threshold	OFF ▾ (Default : OFF, Range : 256-2346)
Fragmentation Threshold	OFF ▾ (Default : OFF, Range : 256-2346)
DTIM Interval	20 <input type="text"/> (Default : 20, Range : 1-255)

1. **Authentication Type:** The default value is **Auto**. When “**Auto**” is selected, it will auto-detect to authenticate by **Shared Key** type or **Open System** type. **Shared Key** is used such that both the sender and the recipient share a WEP key for authentication. **Open Key** is that the sender and the recipient do not share a WEP key for authentication. All points on the network must use the same authentication type.
2. **Transmission Rates:** The default value is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of this particular wireless network. Select from a range of transmission speeds or keep the default setting, **Auto**, to make the Access Point use the fastest possible data rate automatically.

3. **CTS Protection Mode:** The default value is **Disable**. When enabled, a protection mechanism will ensure that the 802.11b devices can connect to Access Point and not be affected by many other 802.11g devices existing at the same time. However, the performance of this 802.11g devices may decrease.
4. **Basic Rate:** The basic rate offers three options, **All**, **Set1** and **Set2** and the default value is **Set1**. Depending on the wireless mode selected, PLANET WSG-404 will deliver a pre-defined data rate. Select “**All**” to activate all transmission rates to be compatible with the majority of the devices.
5. **Beacon Interval:** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the signal transmission occurs between the access point and the wireless network.
6. **RTS Threshold: Ready To Send** threshold. The range is from 256 to 2346 and the default is **OFF**. The administrator could set the value which is the time to wait before sending another packet. It is recommended that the value remains in the range of 256 to 2346.
7. **Fragmentation Threshold:** The range is from 256 to 2346 and the default is **OFF**. The value specifies the maximum size of packet allowed before data is fragmented into multiple packets. It should be remained in the range of 256 to 2346. A smaller value results smaller packets but with a larger numbers of packets in transmission.
8. **DTIM Interval:** This function indicates the interval of the **Delivery Traffic Indication Message** (DTIM). DTIM is a countdown function to inform clients to listen to broadcast and multicast messages. When an Access Point has buffered broadcast or multicast message from an associated client, it sends the next DTIM at this interval rate (from 1~255), the client will hear the beacons.

• Wireless Port

Wireless Port	IP PNP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	User Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Operation Mode	NAT <input type="button" value="v"/>
	IP Address:	192.168.3.254 *
	Subnet Mask:	255.255.255.0 *

IP PNP: Use any IP address to connect to the system. Regardless of what the IP address at the users end is, they can still be authenticated through PLANET WSG-404 and access the network.

User Authentication: If “**User Authentication**” is disabled, “**Specific Route Profile**” needs to be specified for the users to access Internet.

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

IP Address: Enter desired IP address for the wireless port.

Subnet Mask: Enter desired subnet mask for the wireless 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 the 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 asterisks are required to be filled in.

DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server DHCP Scope Start IP Address: <input type="text" value="192.168.3.100"/> * End IP Address: <input type="text" value="192.168.3.200"/> * Preferred DNS Server: <input type="text" value="168.95.1.1"/> * Alternate DNS Server: <input type="text"/> Domain Name: <input type="text" value="planet.com.tw"/> * WINS Server IP: <input type="text"/> Lease Time: <input type="text" value="1 Day"/> ▾ Reserved IP Address List <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 Wireless 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 IP Address: 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 for IP address outside the DHCP range is desired, click on the **Reserved IP Address List** on the management interface. 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 mandatory). Click **Apply** to complete the setup.

Reserved IP Address List -- Wireless			
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"/>

- Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. 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"/> *
----------------------------------	--

- **WDS configuration**

This function can extend the range of accessing the network. It has to work with a repeater. A repeater is a peripheral device supporting PLANET WSG-404 to extend the wireless access by receiving requests from APs or clients and passing the requests to PLANET WSG-404 to obtain authentication.

WDS Configuration	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
--------------------------	---

When “Enable” is clicked, there will be a warning box showing up.



If this function is enabled, please enter the MAC address of repeater in the blanks. A maximum of three repeaters are supported.

WDS Configuration	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
	Item	WDS Client MAC Address
	1	<input type="text"/>
	2	<input type="text"/>
3	<input type="text"/>	

3.2 User Authentication

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

User Authentication	
Authentication Configuration	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.
Black List Configuration	System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List.
Policy Configuration	System provides 3 policies, each policy can apply independent firewall profile, specific route profile, login schedule profile and bandwidth policy.

3.2.1 Authentication Configuration

This function is to configure the settings for 802.1x authentication, authentication server, and on-demand user authentication.

802.1x Authentication Configuration					
802.1x Authentication Configuration					<input type="checkbox"/>
Authentication Server Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enabled
Server 1	LOCAL	Postfix1	Policy A	<input type="radio"/>	<input type="checkbox"/>
Server 2	POP3	Postfix2	Policy A	<input type="radio"/>	<input type="checkbox"/>
Server 3	LDAP	Postfix3	Policy A	<input type="radio"/>	<input type="checkbox"/>
On-demand User	ONDEMAND	bonalinx	Policy A	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>

• **802.1x Authentication Configuration**

802.1x Authentication Configuration	
802.1x Authentication Configuration	<input checked="" type="checkbox"/>

There are two kinds of 802.1x authentication methods and one encryption mechanism: **802.1x**, **WPA w/ 802.1x** and **WPA-PSK**. Click the hyperlink **802.1x Authentication Configuration** to set the related configurations. After completing and clicking **Apply** to save the settings, go back to the previous page to check the item box next to **802.1x Authentication Configuration** to enable this function. When using 802.1x authentications, the RADIUS attributes such as idle timeout or session timeout have no effect.

1. **802.1x**: Enable the 802.1x authentication method. The fields with red asterisks are required to be filled in.

802.1x Authentication Configuration	
<input checked="" type="radio"/> 802.1x <input type="radio"/> WPA w/ 802.1x <input type="radio"/> WPA-PSK	
Authentication Server IP:	<input type="text"/> *
Authentication Port:	<input type="text" value="1812"/> *(Default: 1812)
Secret Key:	<input type="text"/> *
Accounting Server IP:	<input type="text"/> *
Accounting Port:	<input type="text"/> *(Default: 1813)
Secret Key:	<input type="text"/> *
Accounting Service	<input type="text" value="Enabled"/>
Policy	<input type="text" value="Policy A"/>

Authentication Server IP: The IP address or domain name of the Authentication server.

Authentication Port: The port of the authentication server. The default value is 1812.

Secret Key: The secret key of the authentication sever for encryption and decryption.

Accounting Server IP: The IP address or domain name of the accounting server.

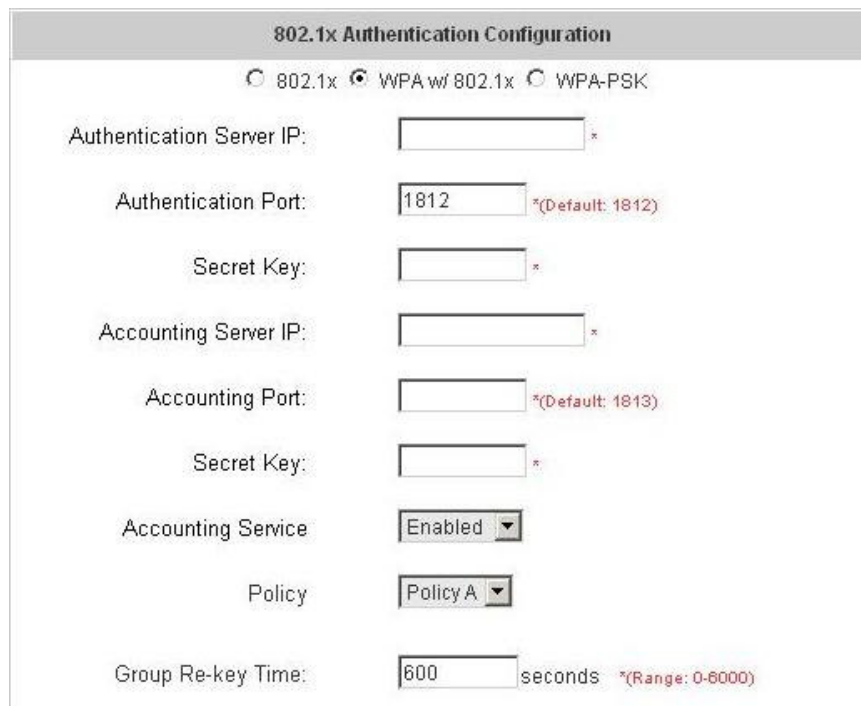
Account Port: The port of the accounting server. The default value is 1813.

Secret Key: The secret key of the accounting sever for encryption and decryption.

Accounting Service: Enable or disable accounting service.

Policy: There are three policies to select from.

2. **WPA x/802.1x:** Enable the supported WPA-Enterprise, Wireless Protection Access with 802.1x.



802.1x Authentication Configuration

802.1x WPA w/ 802.1x WPA-PSK

Authentication Server IP: *

Authentication Port: *(Default: 1812)

Secret Key: *

Accounting Server IP: *

Accounting Port: *(Default: 1813)

Secret Key: *

Accounting Service: ▼

Policy: ▼

Group Re-key Time: seconds *(Range: 0-6000)

Authentication Server IP: The IP address or domain name of the Authentication server.

Authentication Port: The port of the authentication server. The default value is 1812.

Secret Key: The secret key of the authentication sever for encryption and decryption.

Accounting Server IP: The IP address or domain name of the accounting server.

Account Port: The port of the accounting server. The default value is 1813.

Secret Key: The secret key of the accounting sever for encryption and decryption.

Accounting Service: Enable or disable accounting service.

Policy: There are three policies to select from.

Group Re-key Time: Time interval for re-keying broadcast/multicast keys in seconds. The maximum is 6000 sec.

3. **WPA-PSK: Wireless Protection Access-PreShared Key**, a kind of encryption mechanism supporting WPA-SOHO. When using WPA-PSK, there is no user authentication required.

802.1x Authentication Configuration

802.1x
 WPA w/802.1x
 WPA-PSK

Group Re-key Time: sec (0~6000)

PSK:

Passphrase:

Group Re-key Time: Time interval for re-keying broadcast/multicast keys in seconds. The maximum is 6000 sec.

PSK: The **Pre-Shared Key** uses 64 hexadecimal.

Passphrase: A kind of password using 8 to 63 ASCII characters.

Note:

After clicking **Apply**, there will be a restart message. You must click **Restart** to apply the settings.

• **Authentication Server Configuration**

The system provides 3 servers and one on-demand server that the administrator can apply with different policy. Click on the server name to set the related configurations for that particular server. After completing and clicking **Apply** to save the settings, go back to the previous page to choose a server to be the default server and enable or disable any server on the list. Users can log into the default server without the postfix to allow faster login process.

802.1x Authentication Configuration					
802.1x Authentication Configuration					<input type="checkbox"/>
Authentication Server Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enabled
Server 1	LOCAL	Postfix1	Policy A	<input type="radio"/>	<input type="checkbox"/>
Server 2	LOCAL	Postfix2	Policy A	<input type="radio"/>	<input type="checkbox"/>
Server 3	LOCAL	Postfix3	Policy A	<input type="radio"/>	<input type="checkbox"/>
On-demand User	ONDEMAND	pheenet	Policy A	<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	<input type="text" value="Server 1"/> <small>*(Its server name)</small>
Server Status	Enabled
Postfix	<input type="text" value="Postfix1"/> <small>*(Its postfix name)</small>
Black List	<input type="text" value="None"/>
Authentication Method	<input type="text" value="Local User"/> Local User Setting
Policy	<input type="text" value="Policy A"/>

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.

Note:

The Policy Name cannot contain these words: MAC and IP.

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

Authentication Methods: There are 5 authentication methods, **Local**, **POP3**, **RADIUS**, **LDAP** and **NT Domain** to configure from. Select the desired method and 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**.

Note:

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.

1. **On-demand User:** This is for the customer's need in a store environment. 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	Disabled
Postfix	planet (e.g. planet Max: 40 char)
Receipt Header 1	Welcome! (e.g. Welcome!)
Receipt Header 2	
Receipt Footer	Thank You! (e.g. Thank You!)
Printer Baud Rate	9600
Monetary Unit	<input checked="" type="radio"/> none <input type="radio"/> \$ USD <input type="radio"/> £ GBP <input type="radio"/> € EUR <input type="radio"/> (Input other desired monetary unit, e.g. AU)
WLAN ESSID	WSG-404 (e.g. planet)
Wireless Key	
Remark	(for customer)
Billing Notice Interval	<input checked="" type="radio"/> 10mins <input type="radio"/> 15mins <input type="radio"/> 20mins
Twin Ticket	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

[Users List](#)
[Billing Configuration](#)
[Create On-demand User](#)
[Billing Report](#)
[CreditCard](#)

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.

Printer Baud Rate: Select the desired transmission baud rate. The default value is 9600.

Monetary Unit: Select the desired monetary unit.

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

WLAN ESSID: Enter the ESSID of the AP. Administrators can supply a new name or use the default name.

Wireless Key: Enter the Wireless key of the AP such as WEP or WPA.

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

Billing Notice Interval: While the 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.

Twin Ticket: Enable this function to print duplicate receipts.

Users List: Click to enter the **On-demand Users List** page. In the **On-demand Users List**, detailed information will be documented here. By default, the On-demand user database is empty.

On-demand Users List					
Username	Password	Remaining Time/Volume	Status	Expiration Time	Delete All
Q2FX	93NH7WYK	Out of Qouta	Not available	2006/05/04-10:22:59	Delete
64MM	V8UF3967	2 hour	Normal	2006/05/05-10:12:15	Delete
N77X	86N99T4E	Out of Qouta	Not available	2006/05/03-10:35:44	Delete
8Y89	5352P766	Redeemed before	Not available	2006/05/03-11:02:02	Delete
8N6X	788VZ9B8	10 min	Expire	2006/05/02-11:15:16	Delete
2797	NW4679S4	10 min	Normal	2006/05/02-11:56:09	Delete
2XD4	7R9S2RR2	2 hour	Normal	2006/05/05-10:56:16	Delete
4HC4	R888S37X	1 hour 59 min 42 sec	Normal	2006/05/07-11:10:16	Delete
2TP4	ZUF7XE5A	10 min	Normal	2006/05/02-12:06:51	Delete

(Total:9) [First](#) [Previous](#) [Next](#) [Last](#)

- **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 1:The format of each line is "ID (Username), Password, Type, Status, Available Data transfer or Session length, Activation deadline (Date), Expired Date, Validity duration, Plan, Price, Total Data transfer or Session length when bought, Generated Date, First Login Date, Last Logout Date, Logout Cause" without the quotes. The separator between two columns in a line is a comma. When uploading a file, any format error or duplicated username will terminate the uploading process. No account will be uploaded. Please correct the format in the uploading file or delete the duplicated user account in the database, then try again.

Note 2:The unit of data transfer is byte. The unit of session length is second. ID (Username) and Password must be given in upper case.

Upload On-demand User Account

File Name

The uploading file should be a text file and the format of each line is " **ID (Username), Password, Type, Status, Available Data transfer or Session length, Activation deadline (Date), Expired Date, Validity duration, Plan, Price, Total Data transfer or Session length when bought, Generated Date, First Login Date, Last Logout Date, Logout Cause**" without the quotes. The separator between two columns in a line is a comma. When uploading a file, any format error or duplicated username will terminate the uploading process and no account will be uploaded. Please correct the format in the uploading file or delete the duplicated user account in the database, then try again. The unit of data transfer is byte. The unit of session length is second. ID (Username) and Password must be given in upper case.

Example1: For Session Length type

The **Type** must be written as **TIME**, Set Status must be set as **0**. Set **Session Length** in seconds. **Activation Deadline** must be in the format of yyyy/mm/dd hh:mm:ss. Set **Validity Duration** as **1**, and give a **Plan** that's already been generated and enabled from **Billing Configuration** page. Provide a price in any monetary unit defined in **On-demand User Server Configuration** page. Finally, set **Session Length when bought** the same as **Session Length**. Leave other fields blank.

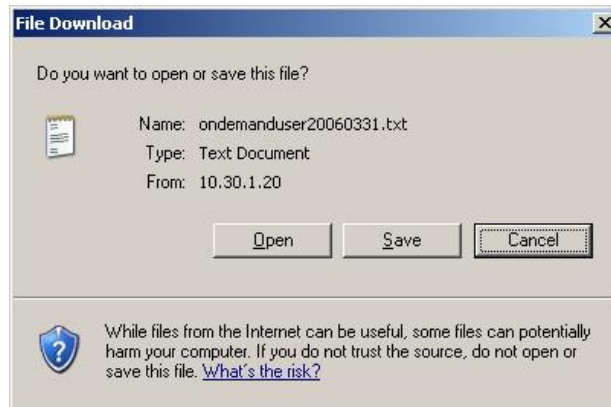
User Name	Type	Session Length	Validity Duration	Price
USER1,PASSWORD1	TIME,0	120	2006/09/13 11:35:43,1	3,22,120
USER2,PASSWORD2	TIME,0	120	2006/09/13 11:35:43,1	3,22,120
	Password	Status	Activation Deadline	Plan Session Length when bought

Example2: For Total Data Transfer type

The **Type** must be written as **DATA**, Set Status must be set as **0**. Set **Total Data Transfer** in bytes. **Activation Deadline** must be in the format of yyyy/mm/dd hh:mm:ss. Set **Validity Duration** as **1**, and give a **Plan** that's already been generated and enabled from **Billing Configuration** page. Provide a price in any monetary unit defined in **On-demand User Server Configuration** page. Finally, set **Total Data Transfer when bought** the same as **Session Length**. Leave other fields blank.

User Name	Type	Total Data Transfer	Validity Duration	Price
USER1,PASSWORD1	DATA,0	2097152	2006/09/13 11:35:43,1	2,11,2097152
USER2,PASSWORD2	DATA,0	2097152	2006/09/13 11:35:43,1	2,11,2097152
	Password	Status	Activation Deadline	Plan Total Data Transfer when bought

- **Download User:** Click this to create a .txt file and then save it on disk.



- **Search:** Enter a keyword of a username that needs 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.
- **Remaining 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.
- **Expiration Time:** The expiration time of the account.
- **Del 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		Expiration Time	Valid Duration	Policy Name	Price
1	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> Data <input checked="" type="radio"/> Time	<input type="text"/> Mbyte <input type="text"/> hrs <input type="text"/> mins	<input type="text"/> 3 days <input type="text"/> 0 hours	<input type="text"/> 5 days	Policy A ▾	<input type="text"/> 20
2	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Data <input type="radio"/> Time	<input type="text"/> 100 Mbyte <input type="text"/> hrs <input type="text"/> mins	<input type="text"/> 5 days <input type="text"/> 12 hours	<input type="text"/> 7 days	Policy B ▾	<input type="text"/> 10
3	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> Data <input checked="" type="radio"/> Time	<input type="text"/> Mbyte <input type="text"/> 4 hrs <input type="text"/> 0 mins	<input type="text"/> 10 days <input type="text"/> 0 hours	<input type="text"/> 10 days	None ▾	<input type="text"/> 20
4	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Data <input type="radio"/> Time	<input type="text"/> 5000 Mbyte <input type="text"/> hrs <input type="text"/> mins	<input type="text"/> 20 days <input type="text"/> 0 hours	<input type="text"/> 30 days	Policy A ▾	<input type="text"/> 50
5	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> Data <input type="radio"/> Time	<input type="text"/> Mbyte <input type="text"/> hrs <input type="text"/> mins	<input type="text"/> days <input type="text"/> hours	<input type="text"/> days	None ▾	<input type="text"/>

- **Status:** Select to enable or disable this billing plan.
- **Type:** Set the billing plan by “Data” (the maximum volume allowed is 9,999,999 Mbyte) or “Time” (the maximum days allowed is 999 days).
- **Expiration time:** This is the duration of time that the account has to be activated after 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 Internet after 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 that will contain this on-demand user's information.

 **Welcome!**

Username	6Q97@planet
Password	7CAM3ZV8
Price	20
Usage	2 hrs 0 mins

ESSID : WSG-404

Wireless Key:

Valid to use until: 2006/09/16 18:08:34

Thank You!

[Printout](#) [Close](#)

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

The screenshot shows a web interface for generating a report. At the top left is a button labeled 'Report All'. Below it are two rows of date selection controls. The first row is labeled 'From' and includes dropdown menus for 'year', 'month', and 'day'. The second row is labeled 'To' and includes dropdown menus for 'year', 'month', and 'day'. To the right of the 'To' row is a 'Search' button.

- **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

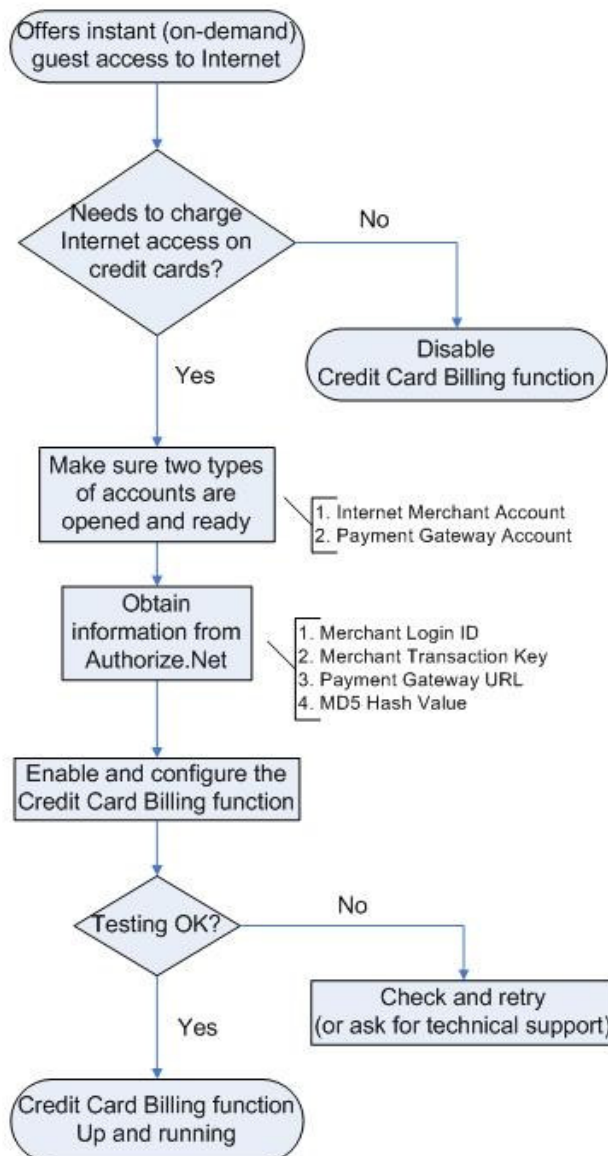
- **Search:** Select a time period to get a period report. The report tells the total expenses and individual accounting of each plan for all plans available for that period of time.

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

Credit Card: Click this to enter the **Credit Card Configuration** page. This section is about how independent HotSpot owners can enable the credit card billing function, making the HotSpot an e-commerce environment for end users to pay for and get Internet access using their credit cards. Before the “Credit Card” and related functions can be managed appropriately, PLANET WSG-404 requires the merchant owners to have a valid **Authorize.Net** (www.authorize.net) account, since Authorize.Net is the on-line payment gateway that PLANET WSG-404 supports now. Please see **Appendix B. The Configuration on Authorize.Net** to setup an Aurtherize.Net account and other necessary information.

Note:

A payment gateway “Paypal” will be supported in the future.



After getting an Authorize.Net account, set the following configuration in Credit Card Configuration of PLANET WSG-404.

Credit Card General Configuration	
Credit Card Payment	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Credit Card Payment Page Configuration	
Merchant Login ID	<input type="text" value="cnpdev1421"/> *
Merchant Transaction Key	<input type="text" value="fAE8bX3Seh1Ys9ul"/> *
Payment Gateway URL	<input type="text" value="https://test.authorize.net/gateway/transact.dll"/> *
Verify SSL Certificate	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Test Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="button" value="Try Test"/> *
MD5 Hash	<input checked="" type="radio"/> Enable <input type="radio"/> Disable MD5 Hash Value: <input type="text"/> * If MD5 Hash is enabled and an error occurs due to the current transaction: <input checked="" type="radio"/> Cancel the current transaction and disable credit card payment option. <input type="radio"/> Cancel the current transaction but still leave credit card payment option available.

➤ **Credit Card General Configuration**

Credit Card Payment: Click Enable to turn on this function or click Disable to turn off this function.

➤ **Credit Card Payment Page Configuration**

Merchant ID: The merchant ID is similar to a username and is used by the Payment Gateway to authenticate transactions.

Merchant Transaction Key: The merchant transaction key is similar to a password and is used by the Payment Gateway to authenticate transactions.

Payment Gateway URL: The Payment Gateway verifies the URL specified in the post string against the URLs in this field.

Verify SSL Certificate: **Secure Sockets Layer**, a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

Test Mode: It is possible to submit a test transaction to the payment gateway. Transactions that are submitted while Test Mode is enabled are NOT actually processed. The example as follows:

Wireless Internet Access

Rate Plan	Price
<input type="radio"/> 2 hrs 0 mins	\$ 5.00
<input checked="" type="radio"/> 6 hrs 0 mins	\$ 8.00
<input type="radio"/> 12 hrs 0 mins	\$ 12.00
<input type="radio"/> 600 Mbyte	\$ 5.00
<input type="radio"/> 1000 Mbyte	\$ 8.00
<input type="radio"/> 2000 Mbyte	\$ 12.00

Credit Card & Contact Information

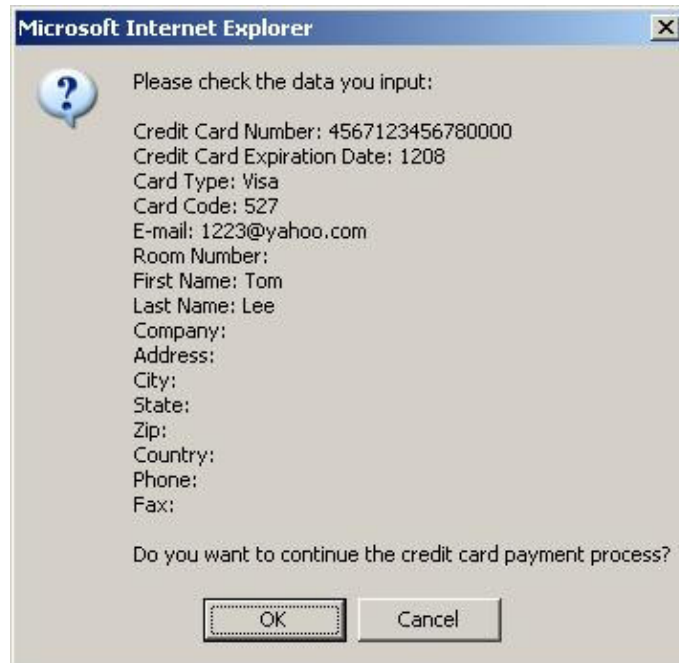
Credit Card Number	<input type="text" value="4567123456780000"/> *
Credit Card Expiration Date	<input type="text" value="1208"/> *(MMYY)
Card Type	<input type="text" value="Visa"/> *
Card Code	<input type="text" value="527"/> *
E-mail	<input type="text" value="tlee1223@yahoo.com"/> *
First Name	<input type="text" value="Tom"/> *
Last Name	<input type="text" value="Lee"/> *
Company	<input type="text"/>
Address	<input type="text"/>
City	<input type="text"/>
State	<input type="text"/>
Zip	<input type="text"/>
Country	<input type="text"/>
Phone	<input type="text"/>
Fax	<input type="text"/>

Fields denoted by an asterisk(*) are required.

Note:

You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If you choose to enter your e-mail address, you will receive a confirmation letter for your own reference.

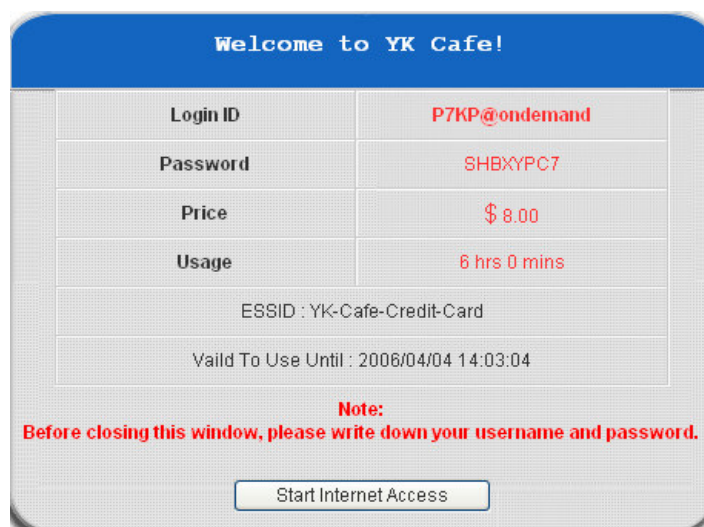
Click **Submit** to send out this transaction. There will be a confirm dialog box showing up. Check the data again and the click **OK** to go on the transaction or click **Cancel** to revise the data or cancel this transaction.



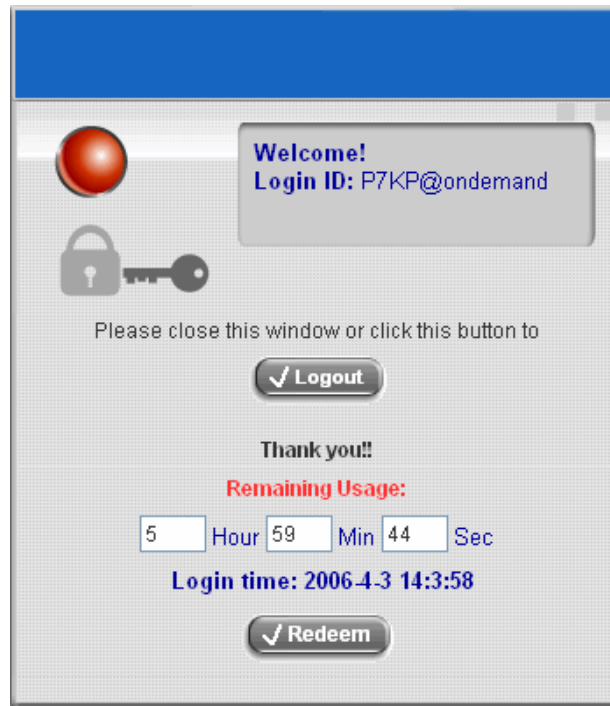
After clicking OK, there will be another dialog box showing up to confirm this transaction again. Click **OK** to complete the process or click **Cancel** to revise the data or cancel this transaction.



Click **OK** to complete the transaction and a welcome screen will show up.



Click **Start Internet Access** to begin to use the Internet.



MD5 Hash: If transaction responses need to be encrypted by the Payment Gateway, enter and confirm a MD5 Hash Value and select a reactive mode. The MD5 Hash security feature enables merchants to verify that the results of a transaction, or transaction response, received by their server were actually sent from the Payment Gateway.

Service Disclaimer Content	
We may collect and store the following personal information: email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.	<input type="text"/> <input type="text"/> <input type="text"/>

Credit Card Payment Page Billing Configuration				
Plan	Enable/Disable		Quota	Price
1	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	2 hrs 0 mins	5.00
2	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	6 hrs 0 mins	8.00
3	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	12 hrs 0 mins	12.00
4	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	600 Mbyte	5.00
5	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	1000 Mbyte	8.00
6	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	2000 Mbyte	12.00
7	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
8	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
9	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
10	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		

Client's Purchasing Record	
Invoice Number	<input type="text" value="YK-Cafe-"/> - <input type="text" value="00000049"/> * <input type="checkbox"/> Reset
Description	<input type="text" value="Wireless Internet Acces"/> *
E-mail Header	<input type="text" value="Thank you very much fo"/> *

➤ **Service Disclaimer Content**

View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.

➤ **Credit Card Payment Page Billing Configuration**

These 10 plans are the plans in **Billing Configuration**, and desired plan can be enabled.

➤ **Client's Purchasing Record**

Invoice Number: An invoice number may be provided as additional information against a transaction. This is a reference field that may contain any format of information.

Description: Narrative text entered by a user to describe the nature of a transaction.

Email Header: Enter the information that should appear in the header of the invoice.

Credit Card Payment Page Fields Configuration		
Item	Displayed Text	Required
<input checked="" type="checkbox"/> Credit Card Number	Credit Card Number *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Credit Card Expiration Date	Credit Card Expiration Date *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Card Type	Card Type * <input checked="" type="checkbox"/> Visa <input checked="" type="checkbox"/> American Express <input checked="" type="checkbox"/> Master Card <input checked="" type="checkbox"/> Discover	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Card Code	Card Code *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> E-mail	E-mail *	<input checked="" type="checkbox"/>
<input type="checkbox"/> Customer ID	Room Number *	<input type="checkbox"/>
<input checked="" type="checkbox"/> First Name	First Name *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Last Name	Last Name *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Company	Company *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Address	Address *	<input type="checkbox"/>
<input checked="" type="checkbox"/> City	City *	<input type="checkbox"/>
<input checked="" type="checkbox"/> State	State *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Zip	Zip *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Country	Country *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Phone	Phone *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Fax	Fax *	<input type="checkbox"/>

*Displayed text fields must be filled.

Credit Card Payment Page Remark Content	
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If	<input type="text"/> <input type="text"/> <input type="text"/>

➤ **Credit Card Payment Page Fields Configuration**

Display: Check the box to show this item on the customer’s payment interface.

Displayed Text: Enter what needs to be shown for this field.

Mandatory: Check the box to indicate this item as a required field.

Credit Card Number: Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.

Credit Card Expiration Date: Month and year expiration date of the credit card. This should be entered in the format of MMY. For example, an expiration date of July 2005 should be entered as 0705.

Card Type: This value indicates the level of match between the Card Code entered on a transaction and the value that is on file with a customer’s credit card company. A code and narrative description are provided indicating the results returned by the processor.

Card Code: The three- or four-digit code assigned to a customer’s credit card number (found either on the front of the card at the end of the credit card number or on the back of the card).

Email: An email address may be provided along with the billing information of a transaction. This is the customer’s email address and should contain an @ symbol.

Customer ID: This is an internal identifier for a customer that may be associated with the billing information of a transaction. This field may contain any format of information.

First Name: The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's name.

Last Name: The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's name.

Company: The name of the company associated with the billing or shipping information entered on a given transaction.

Address: The address entered either in the billing or shipping information of a given transaction.

City: The city is associated with either the billing address or shipping address of a transaction.

State: A state is associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.

Zip: The ZIP code represents the five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits and four digits.

Country: The country is associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full value.

Phone: A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all number or it may include parentheses or dashes to separate the area code and number.

Fax: A fax number may be associated with the billing information of a transaction. This number may be entered as all number or contain parentheses and dashes to separate the area code and number.

➤ **Credit Card Payment Page Remark Content**

Enter additional details for the transaction such as Tax, Freight and Duty Amounts, Tax Exempt status, and a Purchase Order Number, if applicable.

3.2.1.1 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**”.

Configure Authentication Server 1	
Server Name	Server 1 <small>*(It's server name)</small>
Server Status	Disabled
Postfix	Local <small>*(It's postfix name)</small>
Black List	None
Authentication Method	Local User Local User Setting
Policy Name	

Apply Clear

Click the hyperlink for further configuration.

Local User Setting

[Edit Local User List](#)

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

Add User Upload User Download User Refresh

Search

Users List					
Username	Password	MAC	Policy	Remark	Del All

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

Add User: Click the hyperlink of Add User to enter the **Add User** interface. Fill in the necessary information such as “**Username**”, “**Password**”, “**MAC**” (optional) and “**Remark**” (optional). Then, select a desired **Policy** and click **Apply** to complete adding the user or users.

Add User					
Item	Username	Password	MAC (xx:xx:xx:xx:xx:xx)	Policy	Remark
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>

Input the users and enter the necessary information.

Add User					
Item	Username	Password	MAC (xx:xx:xx:xx:xx:xx)	Policy	Remark
1	Tony	asti234	<input type="text"/>	Policy A <input type="button" value="v"/>	<input type="text"/>
2	Larry	1deTg5	00:01:23:3F:6D:7E	Policy A <input type="button" value="v"/>	<input type="text"/>
3	Judy	fish258	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
4	Oksana	oklova	<input type="text"/>	Policy B <input type="button" value="v"/>	long term
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>

After inputting the users and all the information desired, click **Apply**.

User **Tony** has been added!
 User **Larry** has been added!
 User **Judy** has been added!
 User **Oksana** has been added!

Add User					
Item	Username	Password	MAC (xx:xx:xx:xx:xx:xx)	Policy	Remark
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>	<input type="text"/>

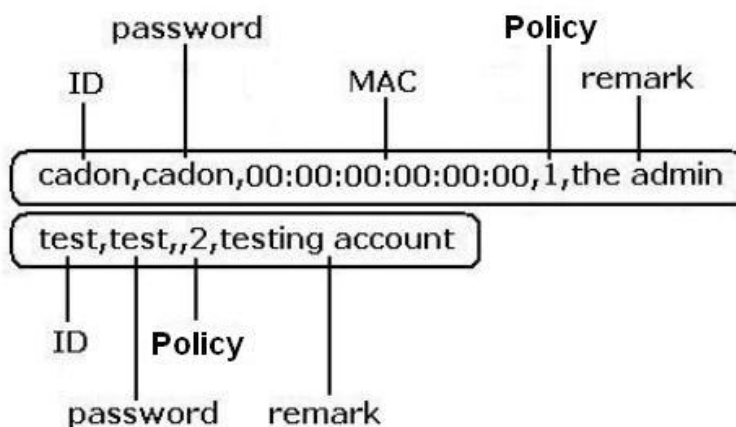
Upload User: Click this to enter the **Upload User** interface. Click the **Browse** button to select the text file for the user account upload. Then click **Submit** to complete the upload process.

Note: The format of each line is "ID, Password, MAC, Policy, Remark" 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.

Upload User Account

File Name

The uploading file should be a text file and the format of each line is "**ID, Password, MAC, Policy, Remark**" 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. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by new ones.



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	<input type="button" value="Del All"/>
			Remark	
Tony	asti234		Policy A	Delete
Larry	1deTg5	00:01:23:3F:6D:7E	Policy A	Delete
Judy	fish258		None	Delete
Oksana	oklova		Policy B	Delete
			long term	

(Total:4) [First](#) [Previous](#) [Next](#) [Last](#)

Refresh: Click this to renew the user list.

Users List				
Username	Password	MAC	Policy	Del All
			Remark	
Tony	asti234		Policy A	Delete
Larry	1deTg5	00:01:23:3F:6D:7E	Policy A	Delete
Judy	fish258		None	Delete
Oksana	oklova		Policy B	Delete
			long term	
Laura	kitty2166		Policy C	Delete
			new	

(Total:5) [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.

Users List				
Username	Password	MAC	Policy	Del All
			Remark	
Oksana	oklova		Policy B	Delete
			long term	

(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 editing the content of individual user account is desired, click the username of the desired user account to enter the **Edit User** Interface for that particular user, and then modify or add any desired information such as **“Username”**, **“Password”**, **“MAC”** (optional) and **“Remark”** (optional). Then, click **Apply** to complete the modification.

Edit User	
Username	Oksana *
Password	oklova *
MAC	00:01:33:7C:2D:1F
Group	Policy C
Remark	permanent

3.2.1.2 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	Server 1 <small>*(Its server name)</small>
Server Status	Enabled
Postfix	Postfix1 <small>*(Its postfix name)</small>
Black List	None
Authentication Method	POP3 POP3 Setting
Policy	Local User POP3 Radius LDAP NTDomain

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"/> *(Domain Name /IP)
Port	<input type="text"/> *(Default:110)
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 POP3 protocol will perform the authentication.

3.2.1.3 Authentication Method - RADIUS

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

Authentication Server - Server 1	
Server Name	<input type="text" value="Server 1"/> *(its server name)
Server Status	Enabled
Postfix	<input type="text" value="Postfix1"/> *(its postfix name)
Black List	None
Authentication Method	Radius Radius Setting
Policy	<div style="border: 1px solid black; padding: 2px;"> Local User POP3 Radius LDAP NTDomain </div>

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 checked="" type="radio"/> Enable <input type="radio"/> Disable Radius Client List
Trans Full Name	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
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"/> Enable <input type="radio"/> Disable
Authentication Protocol	PAP ▾
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"/> Enable <input type="radio"/> Disable
Authentication Protocol	CHAP ▾

- **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** table, the clients, which are using 802.1X as the authentication method, shall be put into this table. PLANET WSG-404 will forward the authentication request from these clients to the configured Radius Servers.

Radius Client Configuration				
No.	Type	IP Address	Segment	Secret
1	802.1x ▾	192.168.1.0	255.255.255.0 (/24) ▾	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) ▾	
6	Disable ▾		255.255.255.255 (/32) ▾	
7	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 the PLANET WSG-404 for the external RADIUS authentication 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.

3.2.1.4 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	Enabled
Postfix	Postfix1 <small>*(Its postfix name)</small>
Black List	None
Authentication Method	LDAP LDAP Setting
Policy	<div style="border: 1px solid gray; padding: 2px;"> Local User POP3 Radius LDAP NTDomain </div>

Apply Clear

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

3.2.1.5 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	<input type="text" value="Server 1"/> *(Its server name)
Server Status	Enabled
Postfix	<input type="text" value="Postfix1"/> *(Its postfix name)
Black List	None <input type="button" value="v"/>
Authentication Method	NTDomain <input type="button" value="v"/> NT Domain Setting
Policy	<input type="button" value="v"/> Local User <input type="button" value="v"/> POP3 <input type="button" value="v"/> Radius <input type="button" value="v"/> LDAP <input type="button" value="v"/> NTDomain <input type="button" value="v"/> Clear

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, users will log into PLANET WSG-404 automatically when they log into the Windows domain.

3.2.2 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	<input type="text" value="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="John"/>	<input type="text" value="computer hacker"/>
2	<input type="text" value="Nancy"/>	<input type="text"/>
3	<input type="text" value="Kaleen"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>

Click **Apply** to add the users.

User 'John' has been added!
 User 'Nancy' has been added!
 User 'Kaleen' 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"/>

If removing a user from the black list is desired, 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
John	computer hacker	<input type="checkbox"/>
Nancy		<input type="checkbox"/>
Kaleen		<input checked="" type="checkbox"/>

(Total:3) [First](#) [Prev](#) [Next](#) [Last](#)

[Add User to List](#)

3.2.3 Policy Configuration

Every Policy has three profiles, **Firewall Profile**, **Specific Route Profile**, and **Schedule Profile** as well as one **Bandwidth** setting for that policy.

Policy Configuration	
Policy A ▾	
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
Bandwidth	Unlimited ▾

- **Firewall Profile**

Click the hyperlink of **Setting** for **Firewall Profile**, the Firewall Profiles list 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.

Profile Name:

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

Edit Filter Rule						
Rule Item: 1						
Rule Name: <input type="text"/>				<input type="checkbox"/> Enable this Rule		
Action : <input type="text" value="Block"/>			Protocol <input type="text" value="ALL"/>			
Source MAC Address: <input type="text"/>				(For Specific MAC Address Filter)		
	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.

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 five interfaces to choose, **ALL**, **WAN**, **Wireless**, **Public LAN (LAN1/LAN2)** and **Private LAN (LAN3/LAN4)**.

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 Route Profile list will appear.

Profile Name:

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

Profile Name: The profile name can be changed here.

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

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

IP Address: The IP address of the next router to the destination.

Default: Check this option to apply the default value.

- **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: Enable Disable

Profile Name: Enable Disable

Login Schedule Profile							
HOURL	SUN	MON	TUE	WED	THU	FRI	SAT
0	<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"/>
1	<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"/>
2	<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"/>
3	<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"/>
4	<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"/>
5	<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"/>
6	<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"/>
7	<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"/>
8	<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"/>
9	<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	<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"/>

- **Bandwidth**

Choose one bandwidth limit for that particular policy.

Policy Configuration

Policy A ▾

Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
Bandwidth	<input type="text" value="Unlimited"/> ▾ <ul style="list-style-type: none"> Unlimited 16 Kbps 32 Kbps 64 Kbps 128 Kbps 256 Kbps 512 Kbps 1 Mbps 2 Mbps 3 Mbps 5 Mbps

3.2.4 Guest User Configuration

This function can permit guests to log into the system. Select “**Enable Guest User**” and click **Apply** to save the settings.

Guest User Configuration

Enable Guest User Disable Guest User

[Guest User List](#)

Policy:

Session Length: hours

Idle Timer: minutes *(Range: 1-1440)

- **Guest User List:** PLANET WSG-404 offers 10 guest users for log in. To activate a guest user, just enter the password in the corresponding “**Password**” text field for that guest account. Guest accounts with blank password will not be activated.

Guest Users List		
Item	Username	Password
1	guest1	<input type="text" value="13RD69"/>
2	guest2	<input type="text" value="q7800FT"/>
3	guest3	<input type="text"/>
4	guest4	<input type="text"/>
5	guest5	<input type="text"/>
6	guest6	<input type="text"/>

- **Policy:** Select one policy to apply to.
- **Session Length:** This restricts the connection time of the guest users. The default session length is 6 hours and the available session time ranges from 1 to 12 hours or unlimited.
- **Idle Timer:** If a guest user has been idled with no network activities at all, the system will automatically kick out the user. The Idle timer can be set in the range of 1~1440 minutes, and the default idle timer is 10 minutes.

3.2.5 Additional Configuration

Additional Configuration	
User Control	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"/>
Internet Connection Detection	http:// <input type="text"/>
Upload File	Certificate Login Page Logout Page Login Succeed Page Login Succeed Page for On-Demand Logout Succeed Page
Credit Reminder	Volume <input type="radio"/> Enabled <input checked="" type="radio"/> Disable Time <input type="radio"/> Enabled <input checked="" type="radio"/> Disable
POP3 Message	Edit Mail Message
Enhance User Authenticate	Permit MAC Address List

- **User Control:** Functions under this section applies for all general users.
- **Idle Timer:** If a user has been idled with no network activities at all, the system will automatically kick out the user. The Idle timer can be set in the range of 1~1440 minutes, and the default Idle timer is 10 minutes.
- **Multiple Login:** When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users and RADIUS authentication method.)
- **Friendly Logout:** When a user logs into the system, a small window will appear to show the user's information and there is a logout button for users to logout. If enabled. When the users try to close the small window, there will be a new popup window to confirm the action in case the users close the login succeed page by accident.
- **Internet Connection Detection:** Enter a specific URL or IP address and PLANET WSG-404 will try to detect the network connection by sending packets directly to that specific URL or IP address. If there is a problem in the connection of the WAN port of the system such that the URL or IP address specified cannot be reached, there will be a message showing that can be set in the Administrator Info in System Information section on the users' screen.
- **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 'Browse...' button. The bottom section is titled 'Upload Customer Certificate' and also contains a 'File Name' label, an empty text input field, and a '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 overwrite 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, 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' (which is 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 blue underlined link labeled 'Preview'.

- 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"/> Select (RGB values in hex mode)
Color for Title Text	<input type="text"/> Select (RGB values in hex mode)
Color for Page Background	<input type="text"/> Select (RGB values in hex mode)
Color for Page Text	<input type="text"/> Select (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** to upload new login page. Click the **Browse** button to select the file for the login page upload. Then click **Submit** to complete the upload process.

Login Page Selection for Users

Default Page Template Page
 Uploaded Page External Page

Uploaded Page Setting

File Name

Existing Image Files:

Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

Upload Images

[Preview](#)

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

User Login Page

Welcome To User Login Page!

Please Enter Your User Name and Password To Sign In .

 User Name:

 Password:

[Click here to purchase by Credit Card Online.](#)

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 to be uploaded.

```

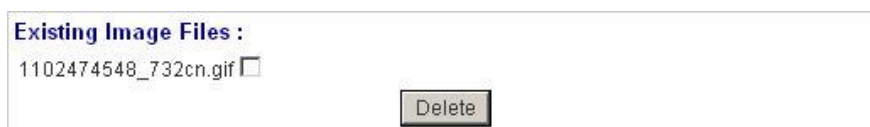
```

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.



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"/>	

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.



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

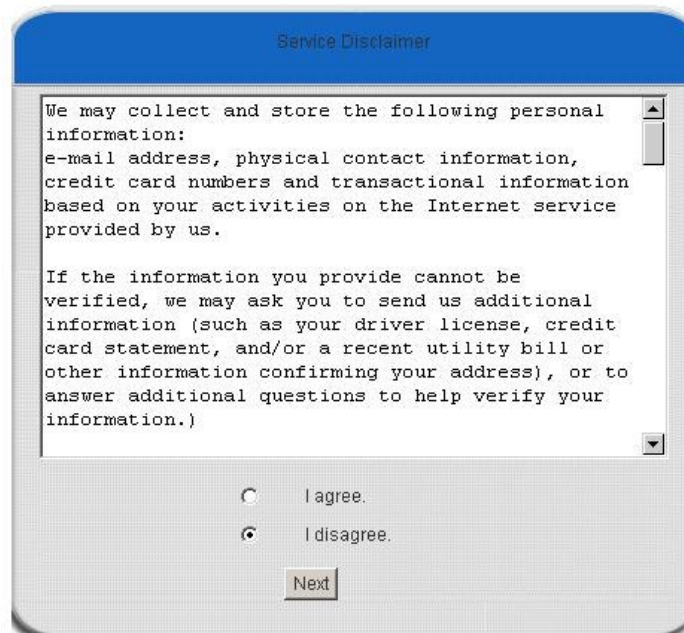
In PLANET WSG-404, the end user first gets a login page when she/he opens its web browser right after associating with an access point. However, in some situations, the hotspot owners or MIS staff may want to display “terms of use” or announcement information before the login page. Hotspot owners or 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 E.

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



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



[Click here to purchase by Credit Card Online.](#)

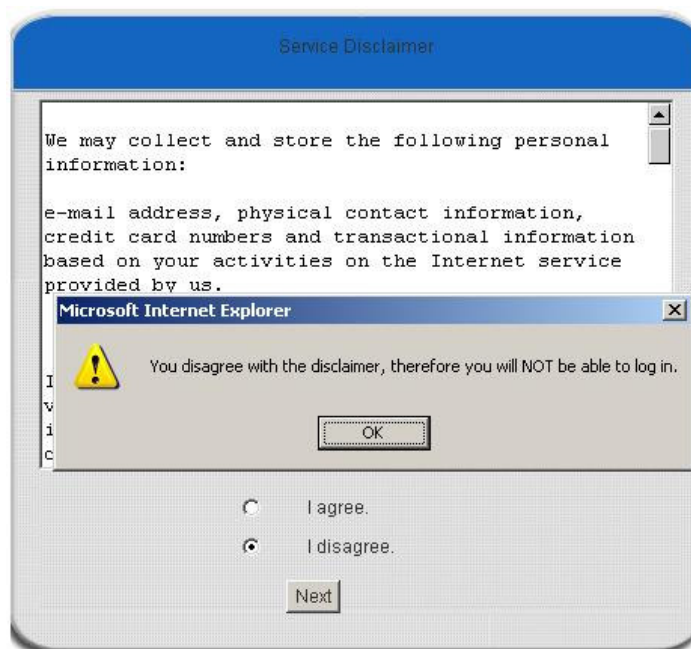
If user checks “**I agree**” and clicks **Next**, then he/she is prompted to fill in the login name and password.



The screenshot shows a web form titled "User Login Page". At the top, it says "Welcome To User Login Page!" and "Please Enter Your User Name and Password To Sign In .". Below this are two input fields: "User Name:" with a person icon and "Password:" with a key icon. At the bottom, there are three buttons: "Submit", "Clear", and "Remaining", each with a checkmark icon.

[Click here to purchase by Credit Card Online.](#)

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



The screenshot shows a "Service Disclaimer" window with a text area containing the following text: "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." Below the text area are two radio buttons: "I agree." (unselected) and "I disagree." (selected). A "Next" button is located below the radio buttons. A "Microsoft Internet Explorer" error dialog box is overlaid on top, displaying a yellow warning triangle icon and the message: "You disagree with the disclaimer, therefore you will NOT be able to log in." with an "OK" button.

- 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"/>	

The **External Page** prepared to be loaded here needs to have the following code as well to let the system work properly

```
<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>
```

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



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

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.

4. **Login Succeed Page:** The administrator can use the default login succeed page or get the customized login succeed page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click **Preview** to see the login succeed page.
- a. Choose **Default Page** to use the default login succeed page.

- b. Choose **Template Page** to make a customized login succeed 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 Succeed 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"/> Select (RGB values in hex mode)
Color for Title Text	<input type="text"/> Select (RGB values in hex mode)
Color for Page Background	<input type="text"/> Select (RGB values in hex mode)
Color for Page Text	<input type="text"/> Select (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 upload the login succeed page. Click the **Browse** button to select the file for the login succeed page upload. Then click **Submit** to complete the upload process.

Login Succeed 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"/>	
Preview	

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

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 succeed page, click the **Use Default Page** button to restore it to default.



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.



- d. Choose the **External Page** selection and get the login succeed 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 login succeed page can be previewed by clicking **Preview** button at the bottom of this page.



5. **Login Succeed Page for On-Demand:** The administrator can use the default login succeed page for On-Demand or get the customized login succeed page for On-Demand by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click **Preview** to see the login succeed page for On-Demand.

- a. Choose **Default Page** to use the default login succeed page for On-Demand.

Login Succeed 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>This is default succeed login page for on-demand users. You could click preview link to preview the default succeed login page. Thanks.</p> <p style="text-align: center;">Preview</p>

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

Login Succeed 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"/> Select (RGB values in hex mode)
Color for Title Text	<input type="text"/> Select (RGB values in hex mode)
Color for Page Background	<input type="text"/> Select (RGB values in hex mode)
Color for Page Text	<input type="text"/> Select (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 click the **Browse** button to select the file for the login succeed page for On-Demand upload. Then click **Submit** to complete the upload process.

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

If the user-defined login succeed page for On-Demand includes an image file, the image file path in the HTML code must be the image file to be uploaded.

``

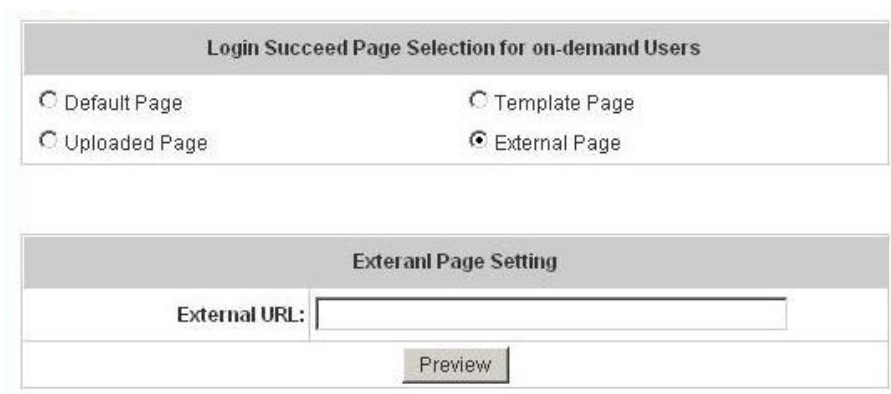
Enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click **Submit**. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login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

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.



Existing Image Files :
1102474548_732cn.gif

- d. Choose the **External Page** selection and get the login succeed 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 succeed page for On-Demand can be previewed by clicking **Preview** button at the bottom of this page.



Login Succeed Page Selection for on-demand Users

Default Page Template Page
 Uploaded Page External Page

External Page Setting

External URL:

6. **Logout Succeed Page:** The administrator can use the default logout succeed page or get the customized login succeed page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click **Preview** to see the logout succeed page.
- a. Choose **Default Page** to use the default logout succeed page.



Logout Succeed Page Selection for Users

Default Page Template Page
 Uploaded Page External Page

Default Page Setting

This is default logout succeed page for users.
You could click preview link to preview the default logout succeed page.
Thanks.
[Preview](#)

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

Logout Succeed 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"/> Select (RGB values in hex mode)
Color for Title Text	<input type="text"/> Select (RGB values in hex mode)
Color for Page Background	<input type="text"/> Select (RGB values in hex mode)
Color for Page Text	<input type="text"/> Select (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 click the **Browse** button to select the file for the logout succeed page upload. Then click **Submit** to complete the upload process.

Logout Succeed 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 Succeed Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/> <input type="button" value="Use Default Page"/>	

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"/>	
Preview	

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

If the user-defined logout succeed page includes an image file, the image file path in the HTML code must be the image file to be uploaded.

``

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 succeed page, click the **Use Default Page** button to restore it to default.



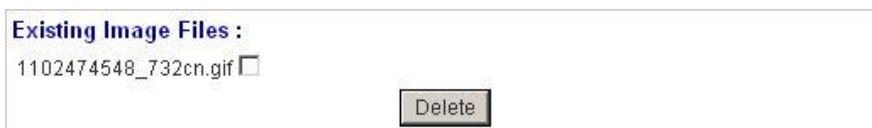
Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

Upload Images Browse...

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.

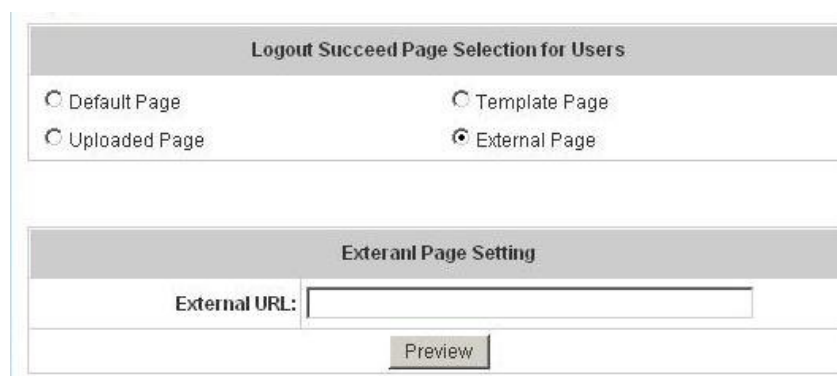


Existing Image Files :

1102474548_732cn.gif

Delete

- d. Choose the **External Page** selection and get the logout succeed 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 succeed page can be previewed by clicking **Preview** button at the bottom of this page.



Logout Succeed Page Selection for Users

Default Page Template Page
 Uploaded Page External Page

External Page Setting

External URL:

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 (1~10;default 1 Mbyte)
	Time	<input checked="" type="radio"/> Enabled <input type="radio"/> Disable
		<input type="text" value="5"/> mins (1~30;default 5 mins)

- **POP3 Message:** Before the users log into the network with their usernames and passwords, the users will receive a welcome mail from PLANET WSG-404. The administrator can edit the contents.

Edit Mail Message	
Text	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"> <HTML><HEAD> <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ascii"> </HEAD> <BODY> <DIV> <DIV> Welcome! </DIV> <DIV> </pre>

- **Enhance User Authentication:** With this function, only the users with their MAC addresses in this list can log into PLANET WSG-404. However, user authentication is still required for these users. Please enter the **MAC Address** to fill in these MAC addresses, select **Enable**, and then click **Apply**.

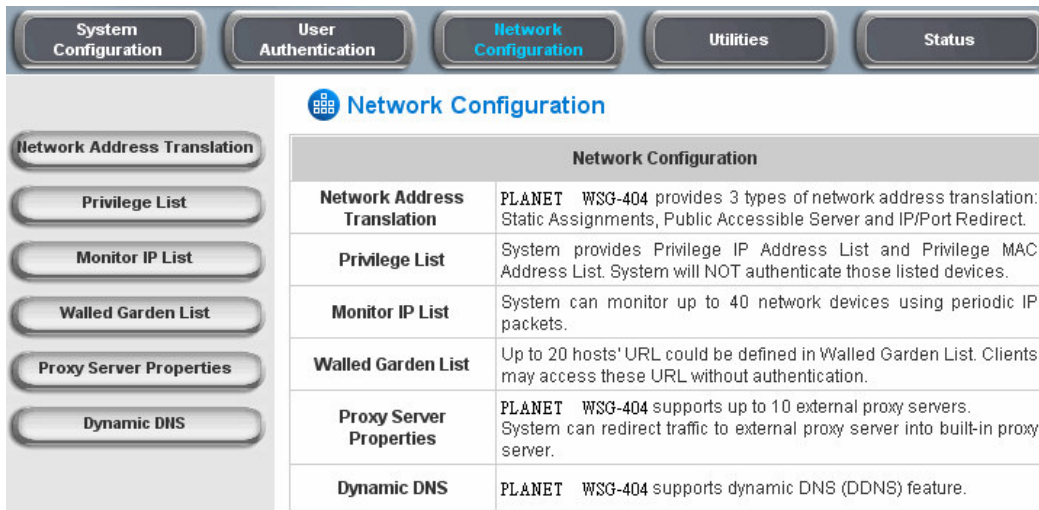
MAC Address Control			
<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Item	MAC Address	Item	MAC Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>

Note:

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

3.3 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**.



Network Configuration	
Network Address Translation	PLANET WSG-404 provides 3 types of network address translation: Static Assignments, 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 using periodic IP packets.
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 WSG-404 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS	PLANET WSG-404 supports dynamic DNS (DDNS) feature.

3.3.1 Network Address Translate

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

Network Address Translate
Static Assignments
Public Accessible Server
Port and IP Redirect

- **Static Assignments**

A computer within the Static Assignment list is unprotected by firewall and typically all port accesses are routed through to that computer. A router will forward all traffic to the computer specified in the Static Assignment list if it does not otherwise have a rule for how to forward traffic on a given port. There are 40 sets of static **Internal IP Address** and **External IP Address** available. These static IP addresses can be set to the any host which itself needs a static IP address to access the network through WAN port. These settings will become effective immediately after clicking the **Apply** button.

Static Assignments		
Item	Internal IP Address	External IP Address
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"/>

(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. 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](#)

3.3.2 Privilege Configuration

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

Privilege List	
Privilege IP Address List	
Privilege MAC Address List	

- **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 WSG-404 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"/>

Note:

Permitting specific IP addresses to have network access rights without going through standard authentication process at the Public LAN (LAN1/LAN2) may cause security problems.

• Privilege MAC Address List

In addition to the IP address, the MAC address of the workstations that need to access the network without authentication can also be set in this list. PLANET WSG-404 allows 100 privilege MAC addresses at most.

When manually creating 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"/>

Note:

Permitting specific MAC addresses to have network access rights without going through standard authentication process at the Public LAN (LAN1/LAN2) may cause security problems.

3.3.3 Monitor IP Configuration



PLANET WSG-404 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. Click **Monitor** to check the current status of all the monitored IP. The system provides 40 IP addresses for the “**Monitor IP List**”.

Admin Email	
Send From	<input type="text"/>
Send To	<input type="text"/>
Interval	1 Hour <input type="button" value="v"/>
SMTP	<input type="text"/>
Auth Method	NONE <input type="button" value="v"/>
Send Test Email	<input type="button" value="Send"/>

Monitor IP List			
Item	IP Address	Item	IP 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"/>

(Total40) [First](#) [Prev](#) [Next](#) [Last](#)

- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Send To:** The e-mail address of the person whom the monitoring result is for. This will be the receiver's e-mail.
- **Interval:** The time interval to send the e-mail report.
- **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 selected, enter the **Account Name**, **Password** and **Domain**.
- **Send Test Email:** To test the settings correct or not.
- **Monitor IP Address:** The IP addresses under monitoring.

Monitor IP result		
No	IP Address	Result
1	192.168.1.200	
2	192.168.1.100	

3.3.4 Walled Garden List

This function provides some free services to the users to access websites listed here 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"/>

3.3.5 Proxy Server Properties

PLANET WSG-404 supports Internal Proxy Server and External Proxy Server functions. Please select an **Access Gateway** and then perform the necessary configurations.

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 the PLANET WSG-404 security management, the system will match the External Proxy Server list to the end-users' proxy setting. If there isn't a match, then the end-users will no be able to reach the login page and thus unable to access the network. If there is a match, 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 WSG-404 has a built-in proxy server. If this function is enabled, the end users will be forced to treat PLANET WSG-404 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 C and Appendix D.

3.3.6 Dynamic DNS

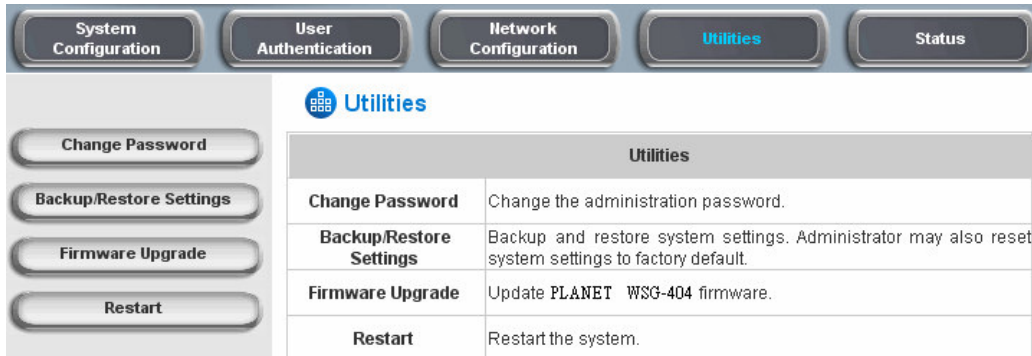
PLANET WSG-404 provides a convenient DNS function to translate the IP address of WAN port to a domain name that helps the administrator memorize and connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to the DNS server. These settings will become effective immediately after clicking **Apply**.

Dynamic DNS	
DDNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Provider	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.

3.4 Utilities

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



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 WSG-404 firmware.
Restart	Restart the system.

3.4.1 Change Password

There are three levels of authorities to use: **admin**, **manager** or **operator**. The default usernames and passwords are as follow:

Admin: The administrator can access all configuration pages of the PLANET WSG-404.

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 the current password and then enter the new password twice to verify. Click **Apply** to activate this new password.

Change Admin Password	
Old Password	<input type="text"/>
New Password	<input type="text"/>
Verify Password	<input type="text"/>

Change Manager Password	
Old Password	<input type="text"/>
New Password	<input type="text"/>
Verify Password	<input type="text"/>

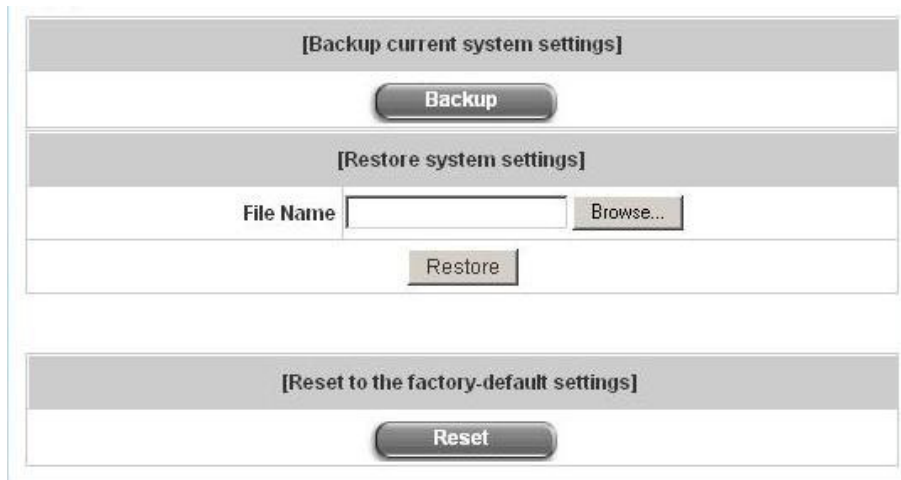
Change Operator Password	
Old Password	<input type="text"/>
New Password	<input type="text"/>
Verify Password	<input type="text"/>

Note:

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.

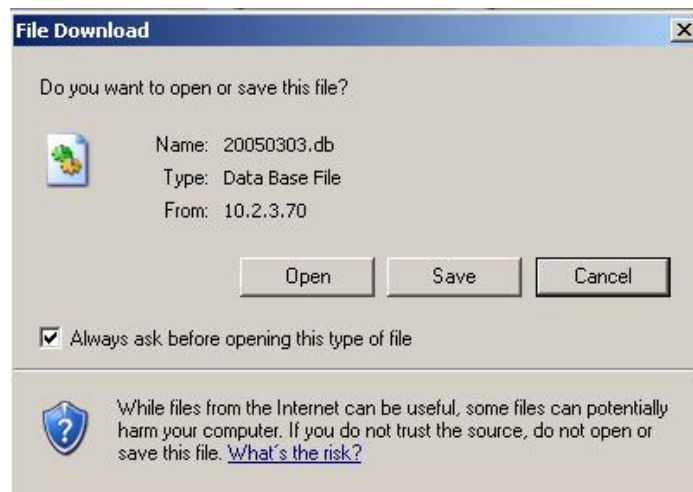
3.4.2 Backup/Restore Settings

This function is used to backup/restore the PLANET WSG-404 settings. Also, PLANET WSG-404 can be restored to the factory default settings here.



The screenshot shows a web-based interface for system settings. It is divided into three main sections, each with a grey header bar. The first section is titled "[Backup current system settings]" and contains a single "Backup" button. The second section is titled "[Restore system settings]" and includes a "File Name" text input field, a "Browse..." button to the right of the input, and a "Restore" button centered below the input field. The third section is titled "[Reset to the factory-default settings]" and contains a single "Reset" button.

- **Backup Current System Setting:** Click **Backup** to create a .db database backup file and save it on disk.



- **Restore System Setting:** Click **Browse** to search for a .db database backup file created by PLANET WSG-404 and click **Restore** to restore to the same settings at the time the backup file was created.
- **Resetting to the Factory-Default configuration:** Click **Reset** to load the factory default settings of PLANET WSG-404.

3.4.3 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 be a few minutes before the upgrade process completes and the system needs to be restarted afterwards to make the new firmware effective.

Firmware Upgrade	
Current Version	1.00.01-EN-E
File Name	<input type="text"/> <input type="button" value="Browse..."/>

Note:

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.
-

3.4.4 Restart

This function allows the administrator to safely restart PLANET WSG-404 and the process should take about three minutes. Click “**YES**” to restart PLANET WSG-404; click “**NO**” to go back to the previous screen. If the power needs to be turned off, restarting PLANET WSG-404 first and then turning off the power after completing the restart process is highly recommended.

Restart

Do you want to **Restart** PLANET WSG-404 ?

Note:

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

3.5 Status

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

Status	
System Status	Display current system settings.
Interface Status	Display WAN, LAN1 & LAN2, LAN3 & LAN4 and Wireless LAN configurations and status.
Current Users	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.
Traffic History	Display detail usage information by day. A minimum of 3 days of history can be logged in the system volatile memory.
Notify Configuration	Historical usage log can be sent automatically to a specific e-mail address defined here. External syslog server can be configured here.

3.5.1 System Status

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

System Status		
Current Firmware Version		1.00.01-EN-E
System Name		PLANET WSG-404
Admin info		Sorry! The service is temporarily unavailable.
Home Page		http://www.planet.com.tw
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	N/A
	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	2006/11/06 10:14:10 +0800
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
	Guest Account	Disabled
DNS	Preferred DNS Server	10.2.3.203
	Alternate DNS Server	168.95.1.1

The description of the table is as follows:

Item		Description
Current Firmware Version		The present firmware version of PLANET WSG-404
System Name		The system name. The default is PLANET WSG-404
Admin Info		The information to be shown on the login screen when a user has a connection problem.
Home Page		The page to which the users are directed after successful login.
Syslog server-Traffic History		The IP address and port number of the external Syslog Server. N/A means that it is not configured.
Syslog server-On demand User log		The IP address and port number of the external Syslog Server. N/A means that it is not configured.
Proxy Server		Enabled/disabled stands for that the system is currently using the proxy server or not.
Friendly Logout		Enabled/disabled stands for the setting of hiding/displaying an extra confirmation window when users close the login succeed page.
Internet Connection Detection		Enabled/Disabled stands for the connection at WAN is normal or abnormal (Internet Connection Detection) and all online users are allowed/disallowed to log in the network.
Management	Remote Management IP	The IP or IPs that is allowed for accessing the management interface.
	SNMP	Enabled/disabled stands for the current status of the SNMP management function.
History	Retained Days	The maximum number of days for the system to retain the users' information.
	Traffic log Email To	The email address to which that the traffic history information will be sent.
	On-demand log Email To	The email address to which the history information about on-demand users is sent.
Time	NTP Server	The network time server that the system is set to align.
	Date Time(GMT+0:00)	The system time is shown as the local time.
User	Idle Timer	The minutes allowed for the users to be inactive.
	Multiple Login	Enabled/disabled stands for the current setting to allow/disallow multiple logins form the same account.
	Guest Account	Enabled/disabled stands for the current status of allowing Guest Accounts to log in.
DNS	Preferred DNS Server	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

3.5.2 Interface Status

This section provides an overview of the interface for the administrator including **WAN**, **LAN1 & LAN2**, **LAN3 & LAN4**, and **Wireless Port**.

Interface Status		
WAN	MAC Address	00:30:4P:50:00:8B
	IP Address	10.30.1.149
	Subnet Mask	255.255.255.0
Wireless	Operation Mode	NAT
	MAC Address	N/A
	IP Address	192.168.3.254
	Subnet Mask	255.255.255.0
	SSID	WSG-404
	Channel	0
	Encryption Function	Disabled
Wireless DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.3.100
	End IP Address	192.168.3.200
	Lease Time	1440 Min(s)
LAN1 & LAN2	Mode	NAT
	MAC Address	00:30:4P:50:00:5A
	IP Address	192.168.1.254
LAN1 & LAN2 DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.1
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
LAN3 & LAN4	Mode	NAT
	MAC Address	00:30:4P:50:00:5A
	IP Address	192.168.2.254
	Subnet Mask	255.255.255.0

The description of the table is as follows.

Item		Description
WAN	MAC Address	The MAC address of the WAN port.
	IP Address	The IP address of the WAN port.
	Subnet Mask	The Subnet Mask of the WAN port.
Wireless	Operation Mode	The mode of the wireless port.
	MAC Address	The MAC address of the wireless port.
	IP Address	The IP address of the wireless port.
	Subnet Mask	The Subnet Mask of the wireless port.
	SSID	The ESSID of the wireless port.
	Channel	The assigned Channel of the Wireless port.

	Encryption Function	Enabled/disabled stands for the status of the encryption function of the wireless port.
Wireless DHCP Server	Status	Enable/disable stands for status of the DHCP server on the Wireless port.
	WINS IP Address	The WINS server IP on DHCP server. N/A means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.
LAN1 & LAN2	Mode	The mode of the LAN1 & LAN2 port.
	MAC Address	The MAC address of the LAN1 & LAN2.
	IP Address	The IP address of the LAN1 & LAN2.
	Subnet Mask	The Subnet Mask of the LAN1 & LAN2.
LAN1 & LAN2 DHCP Server	Status	Enable/disable stands for status of the DHCP server on the LAN1 & LAN2.
	WINS IP Address	The WINS server IP on DHCP server. N/A means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.
LAN3 & LAN4	Mode	The mode of the LAN3 & LAN4.
	MAC Address	The MAC address of the LAN3 & LAN4.
	IP Address	The IP address of the LAN3 & LAN4.
	Subnet Mask	The Subnet Mask of the LAN3 & LAN4.
LAN3 & LAN4 DHCP Server	Status	Enable/disable stands for status of the DHCP server on the LAN3 & LAN4 port
	WINS IP Address	The WINS server IP on DHCP server. N/A means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP Address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.

3.5.3 Concurrent Users

In this function, each online user's information including **Username**, **IP Address**, **MAC Address**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Idle** and **kick Out** can be obtained. Administrator can use this function to force a specific online user to log out. Click the hyperlink of **Logout** 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	Kick Out
	IP	MAC	Pkts Out	Bytes Out		
1		guest4	12	10C8	454	Logout
	192.168.1.107	00:30:4F:60:01:04	12	10C8		
2		guest5	15	12E0	454	Logout
	192.168.1.100	00:30:4F:60:01:05	15	12E0		
3		guest6	25	21C0	64	Logout
	192.168.1.131	00:30:4F:60:01:06	25	21C0		
4		guest7	25	21C0	64	Logout
	192.168.1.165	00:30:4F:60:01:07	25	21C0		



3.5.4 Traffic History

This function is used to check the history of PLANET WSG-404. The history of each day will be saved separately in the DRAM for 3 days.

Traffic History	
Date	Size (Byte)
2005-06-17	411

On-demand User Log	
Date	Size (Byte)
2005-06-17	411

Note:

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

3.5.5 Notify Configuration

The PLANET WSG-404 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.

The image displays two identical web interface panels for configuring email notifications. Each panel is titled 'Notify Configuration' and contains the following fields:

- Traffic History Email / On-demand User Log History Email:**
 - Send From:
 - Send To:
 - Interval:
 - SMTP Server:
 - Auth Method:
 - Send Test Email:
- Syslog Server:**
 - IP:
 - Port:

- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Send To:** The e-mail address of the person whom the history email is for. This will be the receiver's e-mail.
- **Interval:** The time interval to send the e-mail report.
- **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 selected, 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 use **LOGIN** as default, although they can be set to use **NTLMv1**.

Pegasus uses **CRAM-MD5** or **LOGIN** but administrators can not configure which method to be used.

- **Send Test Email:** To test the settings correct or not.
- **Syslog Server:** It specifies the IP and Port of the Syslog server.

3.6 Help

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

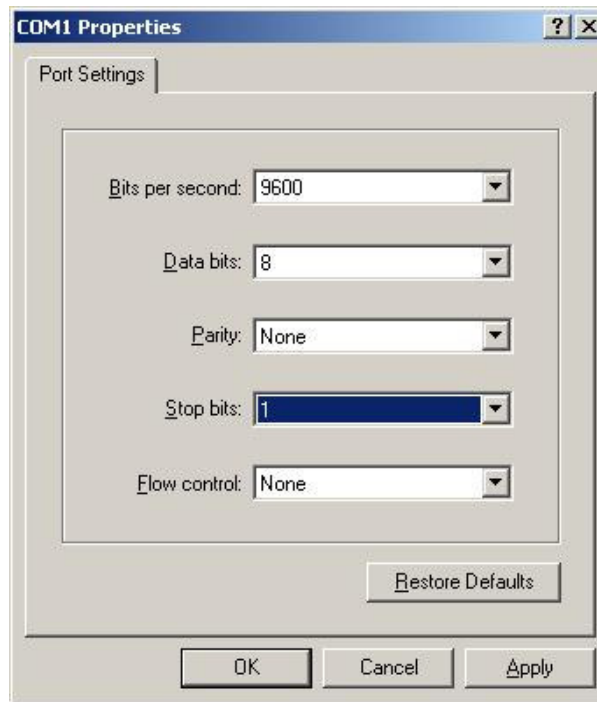
Click **Help** to the **Online Help** window and then click the hyperlink of the items to get the information.



4. Appendix A --- Console Interface

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

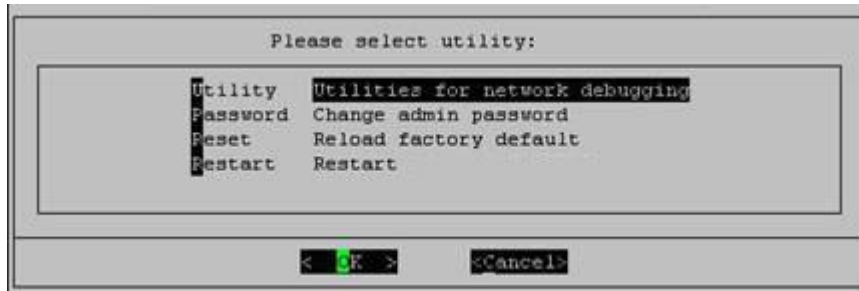
1. In order to connect to the console port of PLANET WSG-404, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are needed.
2. If a Hyper Terminal is used, please set the parameters as **9600, 8, n, 1**.



Note:

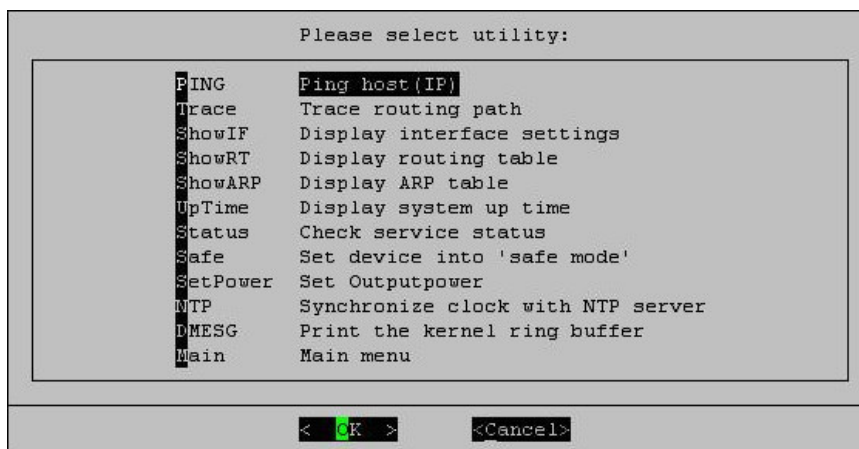
The main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the **Enter** key to make selection or confirm what you enter.

3. Once the console port of PLANET WSG-404 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 the welcome screen or the main menu of the console still can not show up, 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 WSG-404 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 boot up 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. Password can also be changed here. If administrators forget the password and are unable to log in the management interface from the web or the remote end of the SSH, they can still use the null modem to connect the console management interface and set the administrator’s password again.

Note:

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 the PLANET WSG-404 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 PLANET WSG-404**

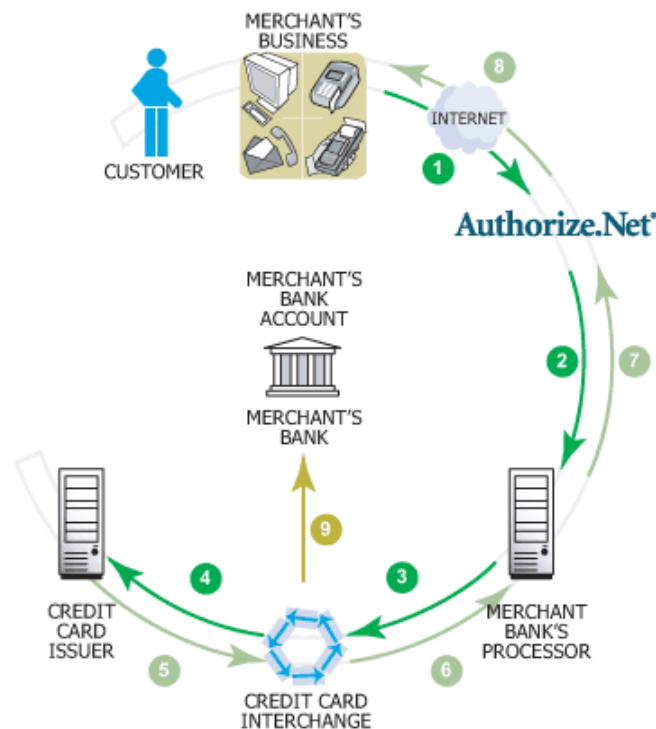
Choosing this option will restart PLANET WSG-404.

5. Appendix B --- Configuration on Authorize.Net

Before the “Credit Card” and related functions can be managed appropriately, PLANET WSG-404 requires the merchant owners to have a valid **Authorize.Net** (www.authorize.net) account, since Authorize.Net is the on-line payment gateway that PLANET WSG-404 supports now. The figure below shows the process of the credit card billing and we will introduce some important procedures for configurations on Authorize.Net.

Note:

A payment gateway “Paypal” will be supported in the future.



1. Setting Up

1.1 Open Accounts

As shown in the above figure, four elements are needed to begin an on-line business:

Element	Description
E-COMMERCE WEB SITE	PLANET WSG-404 has built-in web pages to present to end users to use credit cards
INTERNET MERCHANT ACCOUNT	A type of bank account that allows a business to accept Internet credit card
PAYMENT GATEWAY ACCOUNT	An Authorize.Net account is the type of account that is supported by PLANET WSG-404
CONNECTION METHOD	PLANET WSG-404 will take care of the communication with the Authorize.Net

Therefore, to set up PLANET WSG-404 to process credit card billing, the merchant owner will need two accounts (Internet Merchant account and Authorize.Net account). If you are looking for a merchant account or Internet payment gateway to process transactions, you can fill out the Inquiry Form on <http://www.authorize.net/solutions/merchantsolutions/merchantinquiryform/>. When the four elements are prepared, start configuring the settings on PLANET WSG-404 and Authorize.Net.

1.2 Configure PLANET WSG-404 using an Authorize.Net account

Please log in PLANET WSG-404. User Authentication → Authentication Configuration → Click the server **On-demand User** → **On-demand User Server Configuration** → Click **Credit Card** → **Credit Card Configuration**

Some major fields are required:

Setting	Description
Merchant Login ID	This is the "Login ID" that comes with the Authorize.Net account.
Merchant Transaction Key	To get a new key, please log in Authorize.Net → Click Settings and Profile → Go to the " Security " section → Click Obtain Transaction Key → Enter " Secret Answer " → Click Submit .
Payment Gateway URL	https://secure.authorize.net/gateway/transact.dll (default payment gateway)
MD5 Hash	To enhance the transaction security, merchant owner can choose to enable this function and enter a value in the text box: " MD5 Hash Value ".

Note:

For detailed description, please see P64 – Credit Card.

1.3 Configure the Authorize.Net Merchant Account to Match the Configuration of PLANET WSG-404

Settings of the merchant account on Authorize.Net should be matched with the configuration of PLANET WSG-404:

Setting	Description
MD5 Hash	To configure " MD5 Hash Value ", please log in Authorize.Net → Click Settings and Profile → Go to the " Security " section → click MD5 Hash → Enter " New Hash Value " & " Confirm Hash Value " → Click Submit .
Required Card Code	If the " Card Code " is set up as a required field, please log in Authorize.Net → Click Settings and Profile → Go to the " Security " section → click Card Code Verification → Check the Does NOT Match (N) box → Click Submit .

Required Address Fields	After setting up the required address fields on the “ Credit Card Payment Page Fields Configuration ” section of PLANET WSG-404, the same requirements must be set on Authorize.Net. To do so, please log in Authorize.Net → Click Settings and Profile → Go to the “ Security ” section → click Address Verification System (AVS) → Check the boxes accordingly → Click Submit .
--------------------------------	--

1.4 Test The Credit Card Payment via Authorize.Net

To test the connection between PLANET WSG-404 and Authorize.Net, please log in PLANET WSG-404. User Authentication → Authentication Configuration → Click the server **On-demand User** → **On-demand User Server Configuration** → **Credit Card** → **Credit Card Configuration** → Go to “**Credit Card Payment Page Configuration**” section → Enable the “**Test Mode**” → Click **Try Test** and follow the instructions

2. Basic Maintenance

In order to maintain the operation, merchant owners will have to manage the accounts and transactions via Authorize.Net as well as PLANET WSG-404.

2.1 Void A Transaction and Remove the On-demand Account Generate on PLANET WSG-404

Sometimes, a transaction may need to be canceled as well as the related user account on PLANET WSG-404 before it has been settled with the bank.

- a. To void an unsettled transaction, please log in Authorize.Net. Click **Unsettled Transactions** → Try to locate the specific transaction record on the “**List of Unsettled Transactions**” → Click the **Trans ID** number → Confirm and click **Void**.

Note:

To find the on-demand account name, click **Show Itemized Order Information** in the “**Order Information**” section → Username can be found in the “**Item Description**”.

- b. To remove the specific account from PLANET WSG-404, please log in PLANET WSG-404. User Authentication → Authentication Configuration → Click the server **On-demand User** → **On-demand User Server Configuration** → **Users List** → Click **Delete** on the record with the account name.

2.2 Refund A Settled Transaction and Remove The On-demand Account Generated on PLANET WSG-404

- a. To refund a credit card, please log in Authorize.Net. Click **Virtual Terminal** → Select Payment Method → Click **Refund a Credit Card** → Payment/Authorization Information → Type information in at least three fields: Card Number, Expiration Date, and Amount → Confirm and click **Submit**.
- b. To remove the specific account from PLANET WSG-404, please log in PLANET WSG-404. User Authentication → Authentication Configuration → Click the server **On-demand User** → **On-demand User Server Configuration** → **Users List** → Click **Delete** on the record with the account name.

2.3 Find the Username and Password for A Specific Customer

Please log in Authorize.Net. Click **Unsettled Transactions** → Try to locate the specific transaction record on the “**List of Unsettled Transactions**” → Click the **Trans ID** number → Click **Show Itemized Order Information** in the “**Order Information**” section → Username and Password can be found in the “**Item Description**”.

2.4 Send An Email Receipt to A Customer

If a valid email address is provided, PLANET WSG-404 will automatically send the customer an email receipt for each successful transaction via Authorize.Net. To change the information on the receipt for customer, please log in PLANET WSG-404. User Authentication → Authentication Configuration → Click the server **On-demand User** → **On-demand User Server Configuration** → **Credit Card** → **Credit Card Configuration** → **Client's Purchasing Record** → Type in information in the text boxes: “**E-mail Header and Description**” → Confirm and click **Apply**.

2.5 Send An Email Receipt for Each Transaction to The Merchant Owner

To configure the contact person who will receive a receipt for each transaction, please log in Authorize.Net. Click **Settings and Profile** → Go to the “**General**” section → click **Manage Contacts** → click **Add New Contact** to → Enter necessary contact information on this page → Check the “**Transaction Receipt**” box → Click **Submit**.

3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

3.1 Transaction Statistics by Credit Card Type during A Period

Please log in Authorize.Net. Click **Reports** → Check “**Statistics by Settlement Date**” radio button → Select “**Transaction Type**”, “**Start Date**”, and “**End Date**” as the criteria → Click **Run Report**

3.2 Transaction Statistics by Different Location

- a. To deploy more than one PLANET WSG-404, the way to distinguish transactions from different locations is to make the invoice numbers different. To change the invoice setting, please log in PLANET WSG-404. User Authentication → Authentication Configuration → Click the server **On-demand User** → On-demand User Server Configuration → Credit Card → Credit Card Configuration → Go to “**Client's Purchasing Record**” section → Check the “**Reset**” box → A location-specific ID (for example, Hotspot-A) can be used as the first part of “**Invoice Number**” → Confirm and click **Apply**.
- b. Please log in Authorize.Net → Click **Search and Download** → Specify the transaction period (or ALL Settled, Unsettled) in “**Settlement Date**” section → Go to “**Transaction**” section → Enter the first part of invoice number plus an asterisk character (for example, Hotspot-A*) in the “**Invoice #**” text box → Click **Search** → If transaction records can be found, the number of accounts sold is the number of search results → Or, click **Download To File** to download records and then use MS Excel to generate more detailed reports.

3.3 Search for The Transaction Details for A Specific Customer

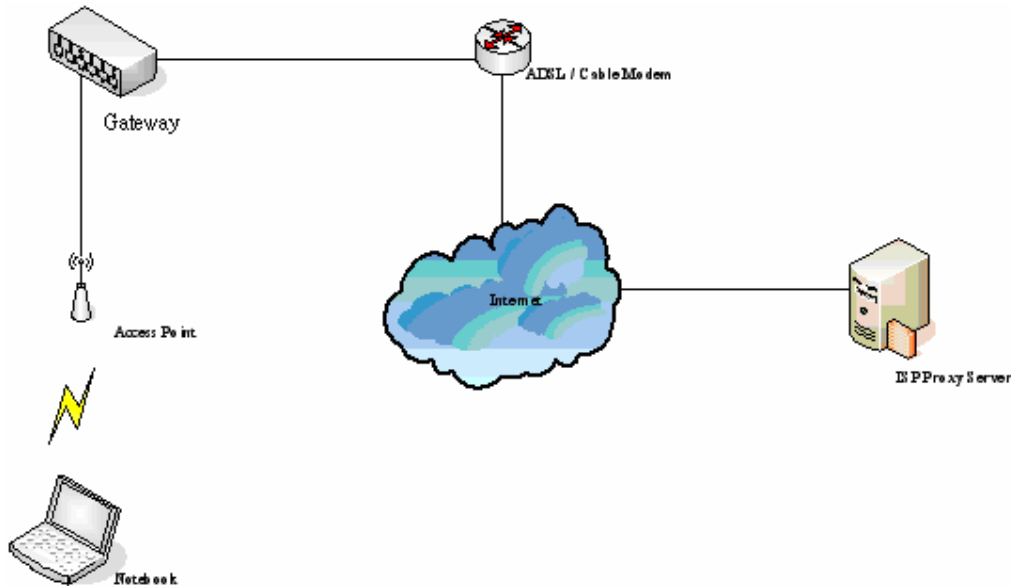
Please log in Authorize.Net. Click **Search and Download** → Enter the information for a specific customer as
criteria → Click **Search** → Click the **Trans ID** number to view the transaction details.

Note:

For more information about Authorize.Net, please see www.authorize.net.

6. Appendix C --- Proxy Setting for Hotspot

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



In Hot spots, 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 :

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' web interface. At the top, there are navigation buttons for 'System Configuration', 'User Authentication', 'Network Configuration' (highlighted), 'Utilities', and 'Status'. Below these, there is a sidebar with buttons for 'Network Address Translation', 'Privilege List', 'Monitor IP List', 'Walled Garden List', 'Proxy Server Properties', and 'Dynamic DNS'. The main content area is titled 'Network Configuration' and contains a table with the following data:

Network Configuration	
Network Address Translation	PLANET WSG-404 provides 3 types of network address translation: Static Assignments, 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 using periodic IP packets.
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 WSG-404 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS	PLANET WSG-404 supports dynamic DNS (DDNS) feature.

- 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"/> Enable <input checked="" type="radio"/> Disable

- 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"/> Enable <input checked="" type="radio"/> Disable

5. Enable Built-in Proxy Server in Internal Proxy Server Setting.

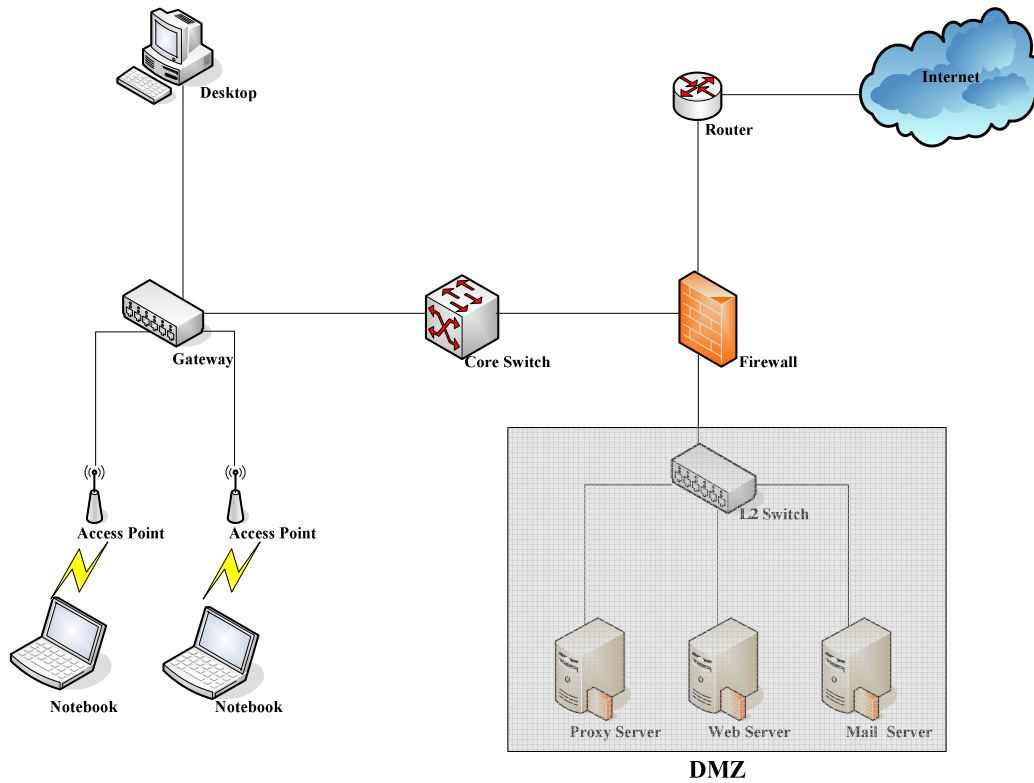
External Proxy Server		
Item	Server IP	Port
1	<input type="text" value="10.2.3.203"/>	<input type="text" value="6588"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input 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	
Built-in Proxy Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

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

7. Appendix D --- 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.

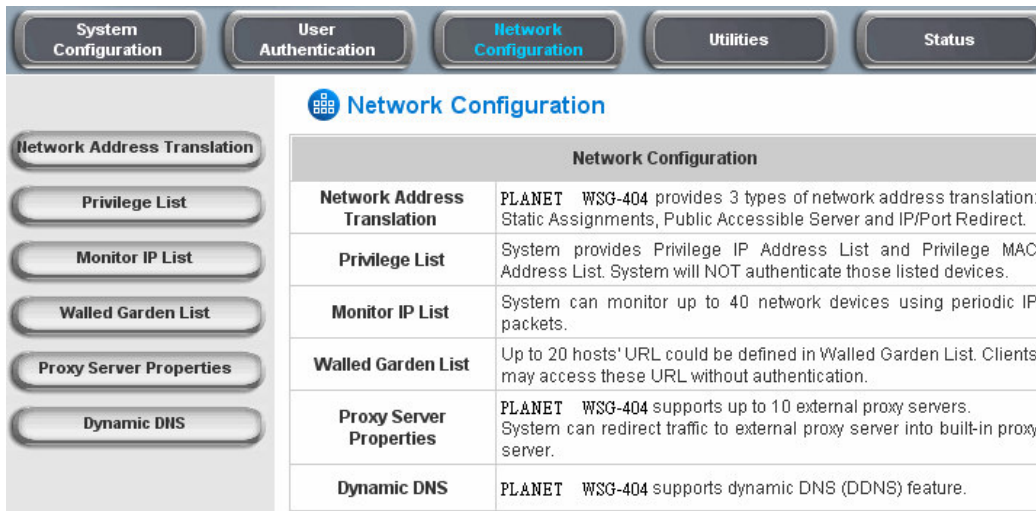
Note:

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.



3. 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"/> Enable <input checked="" type="radio"/> Disable

4. 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"/> Enable <input checked="" type="radio"/> Disable

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"/> Enable <input checked="" type="radio"/> Disable

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

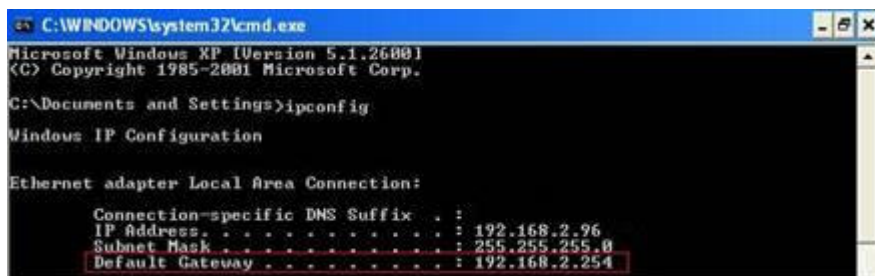
Note:

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**

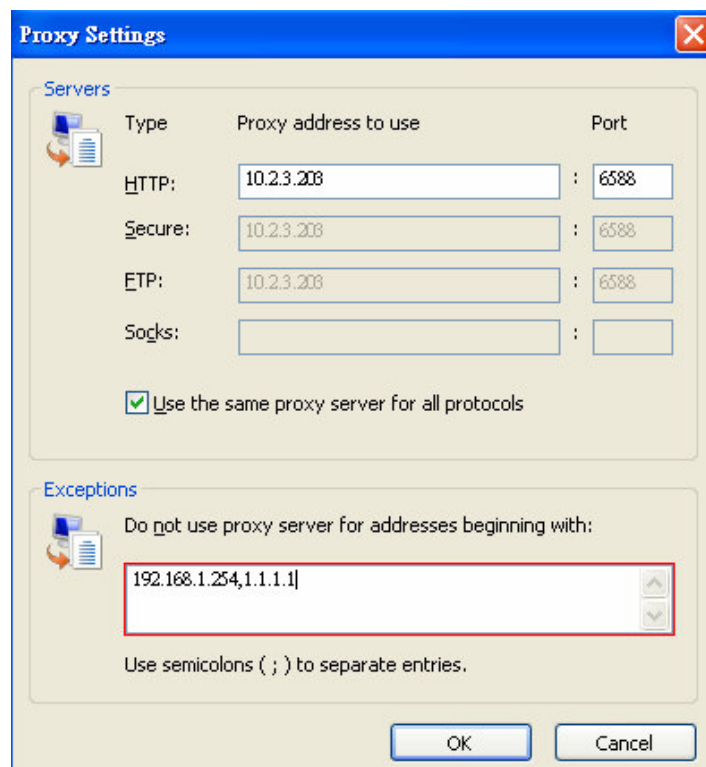
It is necessary for clients to add default gateway IP address into proxy exception information so the user login successful page can show up normally.

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: 10.2.3.203 Port: 6588

Use this proxy server for all protocols

SSL Proxy: 10.2.3.203 Port: 6588

FTP Proxy: 10.2.3.203 Port: 6588

Gopher Proxy: 10.2.3.203 Port: 6588

SOCKS Host: 10.2.3.203 Port: 6588

SOCKS v4 SOCKS v5

No Proxy for: 192.168.1.254,1.1.1.1

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

Automatic proxy configuration URL:

Reload

OK Cancel Help

8. Appendix E --- Disclaimer for On-Demand Users

In PLANET WSG-404, 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 hot spot owners or MIS staff may want to display “terms of use” or announcement information before the login page. Hot spot 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 += name.length + 1;
        }
    }
</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/remai
ning0.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>

```