

- **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 W1310R. 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 W1310R. 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"/>

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

4.3 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	bonalinx-W 1310R 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	bonalinx-W 1310R supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS	bonalinx-W 1310R supports dynamic DNS (DDNS) feature.

4.3.1 Network Address Translation

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](#)

4.3.2 Privilege List

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. W1310R allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking **Apply**.

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

Warning: Permitting specific IP addresses to have network access rights without going through standard authentication process at the 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. W1310R 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"/>

Warning: 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.

4.3.3 Monitor IP List

W1310R 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	

4.3.4 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"/>

4.3.5 Proxy Server Properties

W1310R 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 W1310R 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:** W1310R has a built-in proxy server. If this function is enabled, the end users will be forced to treat W1310R 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.**

4.3.6 Dynamic DNS

W1310R 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	<input type="text" value="DynDNS.org(Dynamic)"/>
Host name	<input type="text"/>
Username/E-mail	<input type="text"/>
Password/Key	<input type="text"/>

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

4.4 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 bonalinx-W1310R firmware.
Restart	Restart the system.

4.4.1 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 W1310R.

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"/>
<input type="button" value="✓ Apply"/> <input type="button" value="✗ Clear"/>	

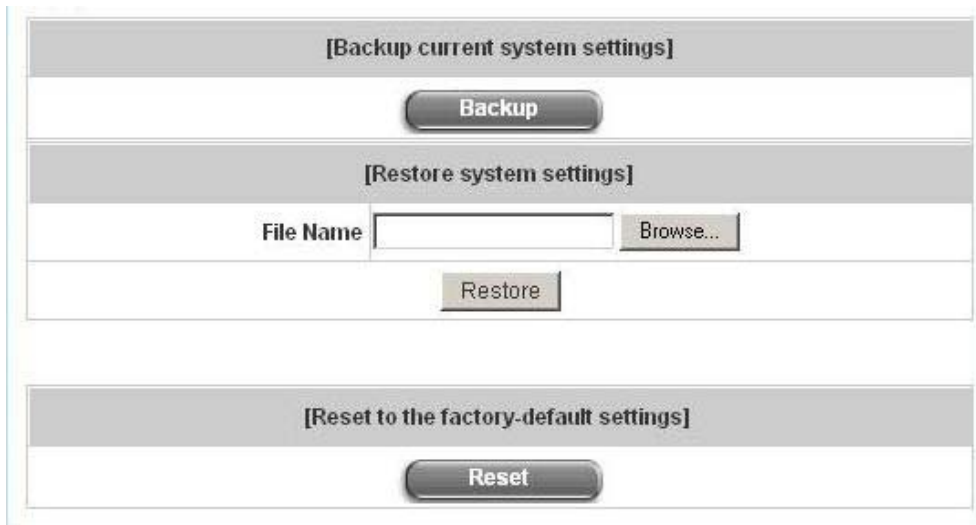
Change Manager Password	
Old Password	<input type="text"/>
New Password	<input type="text"/>
Verify Password	<input type="text"/>
<input type="button" value="✓ Apply"/> <input type="button" value="✗ Clear"/>	

Change Operator Password	
Old Password	<input type="text"/>
New Password	<input type="text"/>
Verify Password	<input type="text"/>
<input type="button" value="✓ Apply"/> <input type="button" value="✗ Clear"/>	

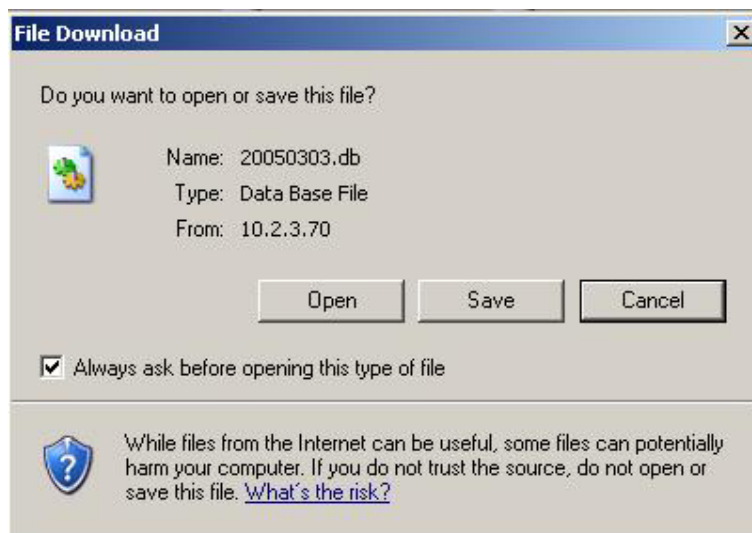
Caution: If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial port, console/printer port.

4.4.2 Backup/Restore Settings

This function is used to backup/restore the W1310R settings. Also, W1310R can be restored to the factory default settings here.




- **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 W1310R 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 W1310R.

4.4.3 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**

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

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

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

4.4.4 Restart

This function allows the administrator to safely restart W1310R and the process should take about three minutes. Click **YES** to restart W1310R; click **NO** to go back to the previous screen. If the power needs to be turned off, restarting W1310R first and then turning off the power after completing the restart process is highly recommended.

 **Restart**

Do you want to **Restart** bonalinx-W 1310R?

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

4.5 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.

4.5.1 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		bonalinx-W 1310R
Admin info		Sorry! The service is temporarily unavailable.
Home Page		http://www.cipherium.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:

<u>Item</u>		<u>Description</u>
Current Firmware Version		The present firmware version of W1310R
System Name		The system name. The default is W1310R
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.

4.5.2 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	00:4F:68:50:00:BE
	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	W1310R
	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	00:4F:68:50:00:5A
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
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	00:4F:68:50:00:5A
	IP Address	192.168.2.254
	Subnet Mask	255.255.255.0

The description of the table is as follows.

<u>Item</u>		<u>Description</u>
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.
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.

4.5.3 Current 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:D0:C9:60:01:04	12	10C8		
2		guest5	15	12E0	454	Logout
	192.168.1.100	00:D0:C9:60:01:05	15	12E0		
3		guest6	25	21C0	64	Logout
	192.168.1.131	00:D0:C9:60:01:06	25	21C0		
4		guest7	25	21C0	64	Logout
	192.168.1.165	00:D0:C9:60:01:07	25	21C0		



4.5.4 Traffic History

This function is used to check the history of W1310R. 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

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

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

- **Traffic History**

As shown in the following figure, each line is a traffic history record consisting of 9 fields, **Date**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, and **Bytes Out**, of user activities.

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

- **On-demand User Log**

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

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

4.5.5 Notify Configuration

The W1310R 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.

Notify Configuration	
Traffic History Email	Send From: <input type="text"/>
	Send To: <input type="text"/>
	Interval: <input type="text" value="1 Hour"/>
	SMTP Server: <input type="text"/>
	Auth Method: <input type="text" value="NONE"/>
	Send Test Email: <input type="button" value="Send"/>
Syslog Server	IP: <input type="text"/> Port: <input type="text"/>
Notify Configuration	
On-demand User Log History Email	Send From: <input type="text"/>
	Send To: <input type="text"/>
	Interval: <input type="text" value="1 Hour"/>
	SMTP Server: <input type="text"/>
	Auth Method: <input type="text" value="NONE"/>
	Send Test Email: <input type="button" value="Send"/>
Syslog Server	IP: <input type="text"/> Port: <input type="text"/>

- **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.

4.6 Help

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

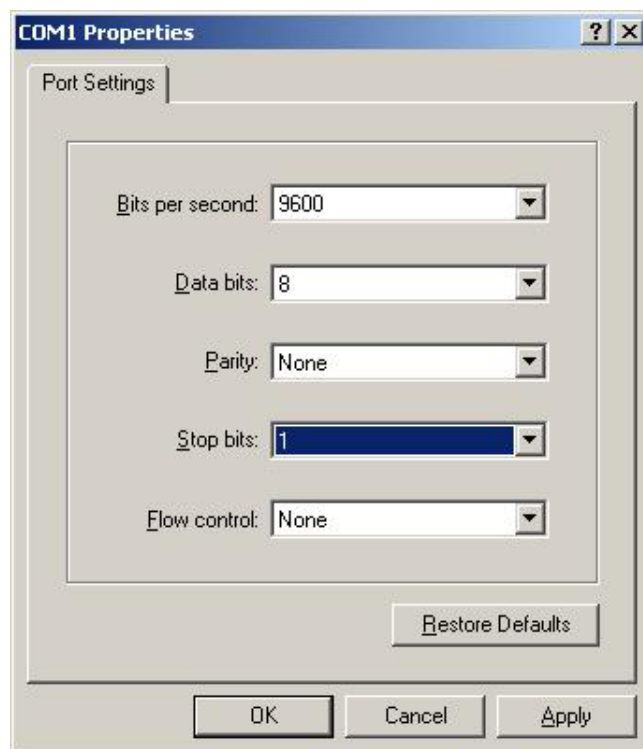
Click **Help** to the **Online Help** window and then click the hyperlink of the items to get the information.



5. Appendix A -- Console Interface

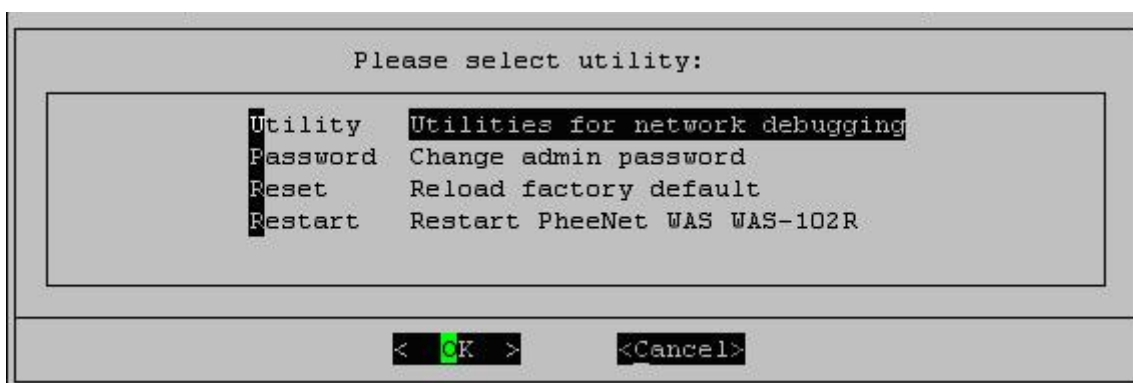
Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. In order to connect to the console port of W1310R, 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**.



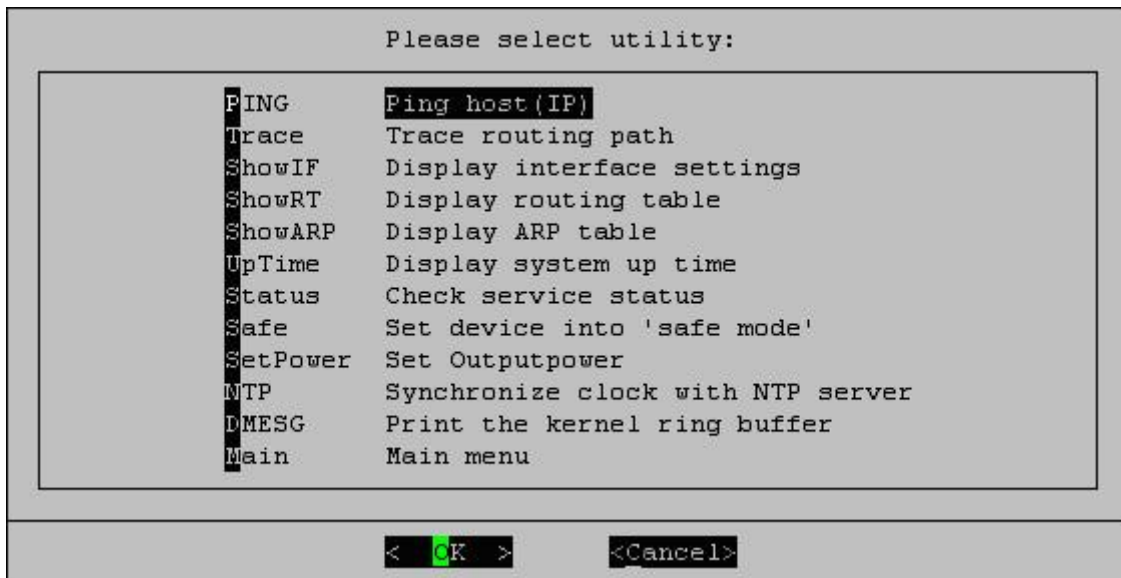
Caution: the main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the **Enter** key to make selection or confirm what you enter.

3. Once the console port of W1310R 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 AMG-2000 into safe mode, then administrator can management this device with browser again.
- Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.
- Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their bootup messages instead of copying the messages by hand.
- Main menu: Go back to the main menu.

- **Change admin password**

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

The username is "admin" and the default password is also "admin", which is the same as for the web management interface. 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.

Caution: *Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the W1310R Admin username and password after logging in the system for the first time.*

- **Reload factory default**

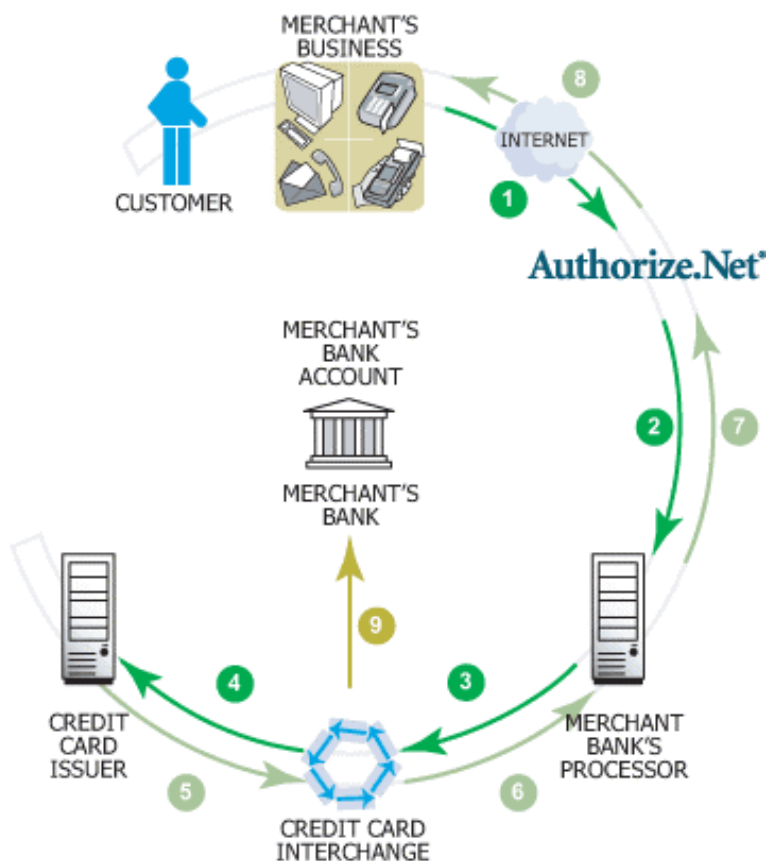
Choosing this option will reset the system configuration to the factory defaults.

- **Restart W1310R**

Choosing this option will restart W1310R.

6. Appendix B -- Configuration on Authorize.Net

Before the "Credit Card" and related functions can be managed appropriately, W1310R requires the merchant owners to have a valid **Authorize.Net** (www.authorize.net) account, since Authorize.Net is the on-line payment gateway that W1310R 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.



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	W1310R 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 W1310R
CONNECTION METHOD	W1310R will take care of the communication with the Authorize.Net

Therefore, to set up W1310R 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 W1310R and Authorize.Net.

1.2 Configure W1310R using an Authorize.Net account

Please log in W1310R. 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 W1310R

Settings of the merchant account on Authorize.Net should be matched with the configuration of W1310R:

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 W1310R, 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 W1310R and Authorize.Net, please log in W1310R. 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 W1310R.

2.1 Void A Transaction and Remove the On-demand Account Generate on W1310R

Sometimes, a transaction may need to be canceled as well as the related user account on W1310R 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 W1310R, please log in W1310R. 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 W1310R

- 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 W1310R, please log in W1310R. 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, W1310R 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 W1310R. 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 W1310R, the way to distinguish transactions from different locations is to make the invoice numbers different. To change the invoice setting, please log in W1310R. 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.

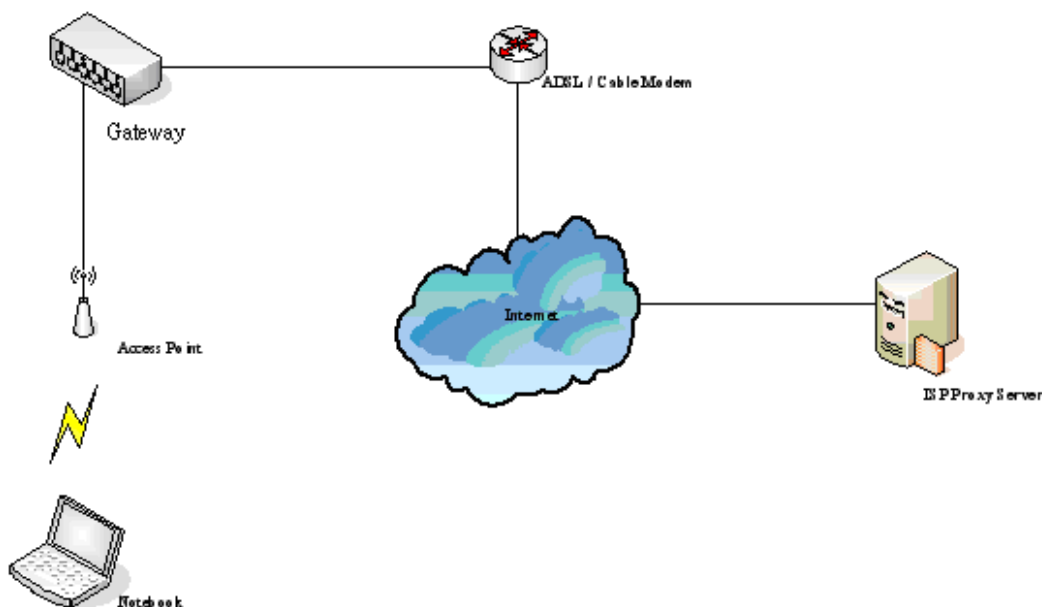
3.3 Search for The Transaction Details for A Specific Customer

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.

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

7. Appendix C -- Proxy Setting for Hotspot

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



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

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. The top navigation bar includes System Configuration, User Authentication, Network Configuration (highlighted with a red box), Utilities, and Status. The main content area shows the Network Configuration page with a sidebar of options and a table of configuration details.

Network Configuration	
Network Address Translation	bonalinx-W 1310R 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	bonalinx-W 1310R supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS	bonalinx-W 1310R 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.

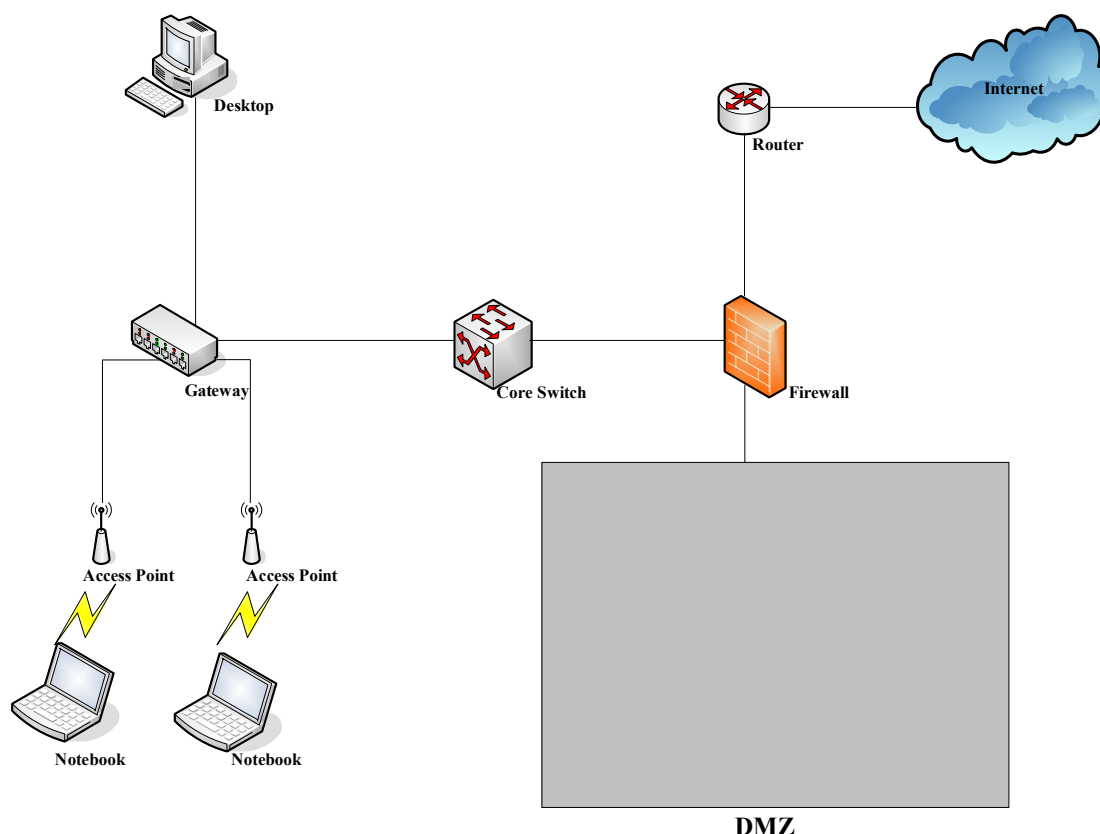
External Proxy Server		
Item	Server IP	Port
1	<input type="text" value="10.2.3.203"/>	<input type="text" value="6588"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input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

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

8. 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.

Caution : 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.

System Configuration User Authentication **Network Configuration** Utilities Status

Network Configuration

Network Address Translation
Privilege List
Monitor IP List
Walled Garden List
Proxy Server Properties
Dynamic DNS

Network Configuration	
Network Address Translation	bonalinx-W 1310R 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	bonalinx-W 1310R supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS	bonalinx-W 1310R 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

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

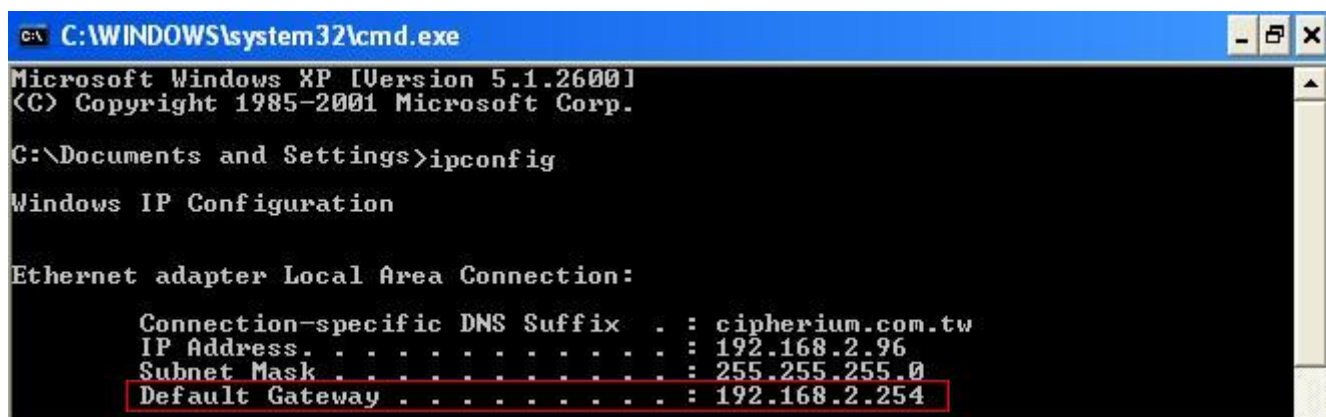
6. Click **Apply** to save the settings.

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

■ Client setting

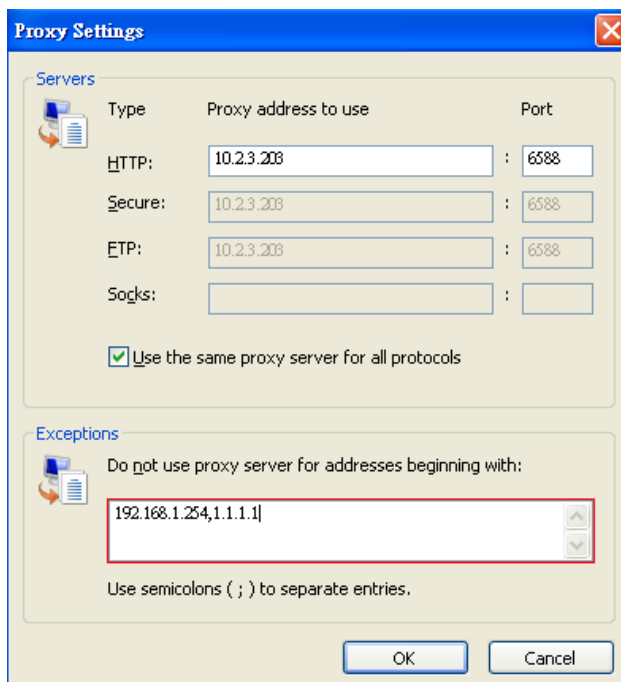
It is necessary for clients to add default gateway IP address into proxy exception information so the user login successful page can show up normally.

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

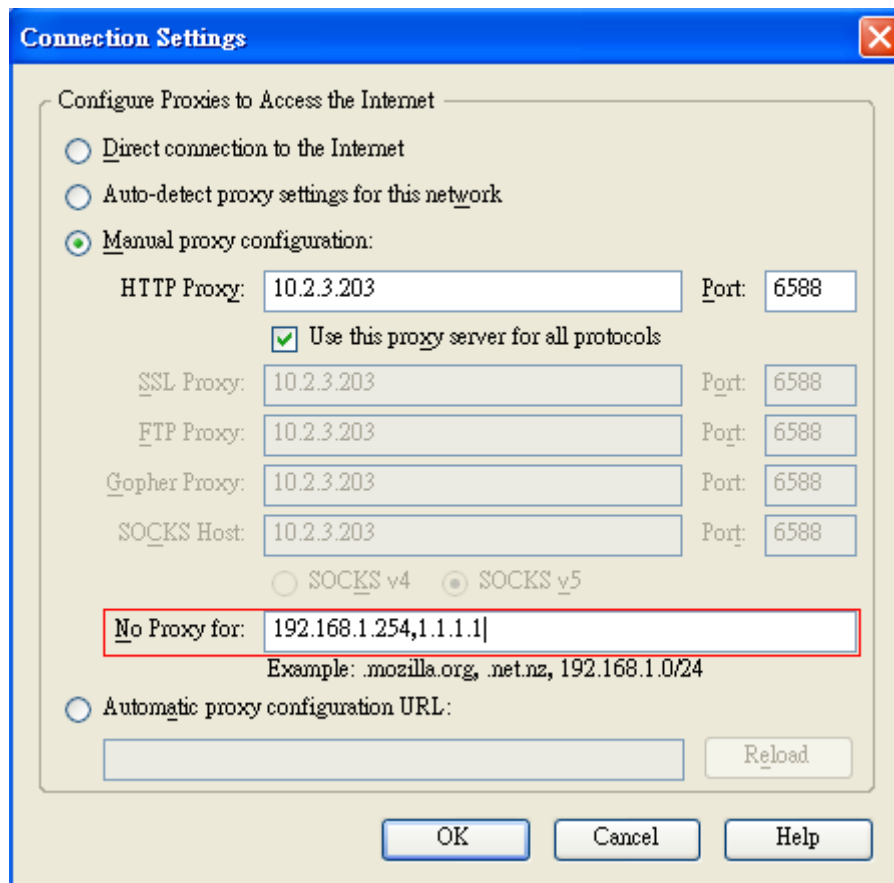


2. Open browser to add **default gateway IP address (e.g. 192.168.1.254)** and **logout page IP address "1.1.1.1"** into proxy exception information.

- For I.E



- For firefox



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

In W1310R, 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.

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/remaining0.gif')">
    <ilayer width={marquee_width}; height={marquee_height}; name="cmarquee01">
    <layer name="cmarquee02" width={marquee_width}; height={marquee_height};></layer>
    </ilayer>

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

<table name="disclaimer" id="disclaimer" width="460" height="430" border="0" align="center"
background="../images/agreement.gif">
    <tr>
        <td height="50" align="center" valign="middle"><div align="center" class="style5">Service
Disclaimer</div></td>
    </tr>
    <tr>
        <td height="260" align="center" valign="middle"><table width="370" height="260" border="0" align="center">
            <tr>
                <td>
                    <textarea name="textarea" cols="50" rows="15" align="center" readonly>

```

We may collect and store the following personal information:

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

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

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

information for accuracy, and verify it with third parties.

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

We may also share your personal information with:

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

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

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

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

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

```
</textarea>
</td>
</tr>
</table></td>
</tr>
```

```

<tr>
  <td height="40"><table width="170" height="20" border="0" align="center" cellpadding="2">
    <tr>
      <td align="left"><input name="selection" value="1" type="radio"></td>
      <td><span class="style4">I agree.</span></td>
    </tr>
    <tr>
      <td align="left"><input name="selection" value="2" checked type="radio"></td>
      <td><span class="style4">I disagree.</span></td>
    </tr>
  </table></td>
</tr>
<tr>
  <td height="30"><table width="110" height="20" border="0" align="center" cellpadding="2">
    <tr>
      <td width="45" align="center" valign="middle"><input name="next_button" type="button" value="Next"
onclick="javascript:check_agree(Enter)"></td>
    </tr>
  </table></td>
</tr>
<tr>
  <td height="20">&nbsp;</td>
</tr>
</table>

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

```

```

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

```

```

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

```

```

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

```

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

P/N: V10020061101