LevelOne

AMG-2000

AP Management Gateway

User Manual

v2.0-0705

Table of Contents

Chapter 1. Before You Start

1.1 Preface

This manual is intended for the system or network administrators with the networking knowledge to complete the step by step instructions of this manual in order to use the AMG-2000 for a better management of network system and user data.

1.2 Document Convention

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

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

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

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

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

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

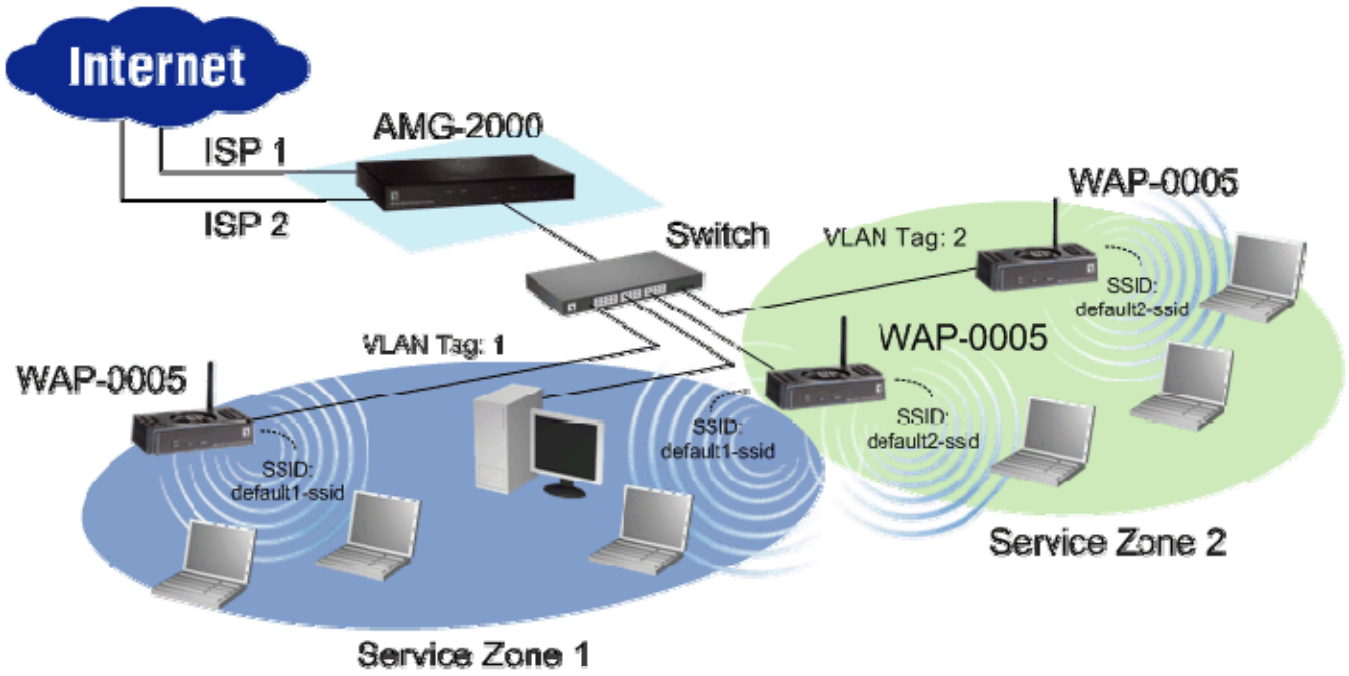
Chapter 2. System Overview

2.1 Introduction of AMG-2000

AMG-2000 is an AP Management Gateway dedicatedly designed for small to medium-sized network deployment and management, making it an ideal solution for easily creating and extending WLANs in SMB offices. With its user management features, administrators will be able to manage the whole process of wireless network access. In addition, Access Point (AP) management functions allow administrators to discover, configure, update, and monitor all managed APs from a single secured interface, and from there, gain full control of entire wireless network.

2.2 System Concept

When deployed by small businesses or service providers, AMG-2000's "Service Zone" based architecture allows administrators to logically separate wired and wireless networks by VLAN tags as well as SSIDs. Basically, a Service Zone can cover certain areas of wired and wireless networks, where users attempting to access the resources within the service zone will be controlled based on the access control profile of the service zone, such as authentication, security feature, wireless encryption method, traffic control, etc. As shown below is a typical network architecture to show how network users are separated and controlled by the two Service Zones, each of which is associated with its unique VLAN tag and SSID.



2.3 Specification

2.3.1 Hardware Specification

- **General**

  Form Factor: Mini-desktop

  Dimensions (W x D x H): 235 mm x 161.9 mm x 37.6 mm

  Weight: 1Kg

  Operating Temperature: 0 ~ 40°C

  Storage Temperature: 20 ~ 70°C

  Power: 100~240 VAC, 50/60 Hz

  Ethernet Interfaces: 7 x Fast Ethernet (10/100 Mbps)

- **Connectors & Display**

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

  Private Port: 1 x 10BASE-T/100BASE-TX RJ-45

  LAN Ports: 4 x 10BASE-T/100BASE-TX RJ-45

  Console Port: 1 x RJ-11

  LED Indicators: 1 x Power, 1 x Status, 2 x WAN, 1 x Private, 4 x LAN

2.3.2 Technical Specification

- **Networking**

  Supports Router, NAT mode

  Supports Static IP, DHCP, PPPoE on WAN interface

  Configurable LAN ports authentication

  Supports IP Plug and Play (IP PnP)

  Built-in DHCP server and supports DHCP relay

  Supports NAT:

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

  Supports static route

  Supports SMTP redirection

  Supports Walled Garden (free surfing zone)

  Supports MAC Address Pass-Through

  Supports HTTP Proxy

- **Security**

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

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

  Supports VPN Pass-through(IPSec and PPTP)

  Supports DoS attack protection

  Supports user Black List

  Allows user identity plus MAC address authentication for local accounts

- **User Management**

  Supports up to 120 concurrent users

  Provides 500 local accounts

  Provides 2000 on-demand accounts

  Provides guest accounts

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

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

  Customizable login and logout portal page

  User Session Management:

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

- **AP Management**

  Supports up to 12 manageable IEEE 802.11 compliant APs

  Centralized remote management via HTTP/SNMP interface

  Automatic discovery of managed APs and list of managed APs

  Allows administrators to add and delete APs from the device list

  Allows administrators to enable or disable managed APs

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

  Locally maintained configuration profiles of managed APs

  Single UI for upgrading and restoring managed APs' firmware

  System status monitoring of managed APs and associated client stations

  Automatic recovery of APs in case of system failure

  System alarms and status reports on managed APs

- **Monitoring and Reporting**

  Status monitoring of on-line users

  IP-based monitoring of network devices

  WAN connection failure alert

  Syslog support for diagnosing and troubleshooting

  User traffic history logging

- **Accounting and Billing**

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

  Built-in billing profiles for on-demand accounts

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

  Provides billing report on screen for on-demand accounts

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

  Traffic history report in an automatic email to administrator

- **System Administration**

  Multi-lingual, web-based management UI

  SSH remote management

  Remote firmware upgrade

  NTP time synchronization

  Backup and restore of system configuration

Chapter 3 Base Installation

3.1 Hardware Installation

3.1.1 System Requirements

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

3.1.2 Package Contents

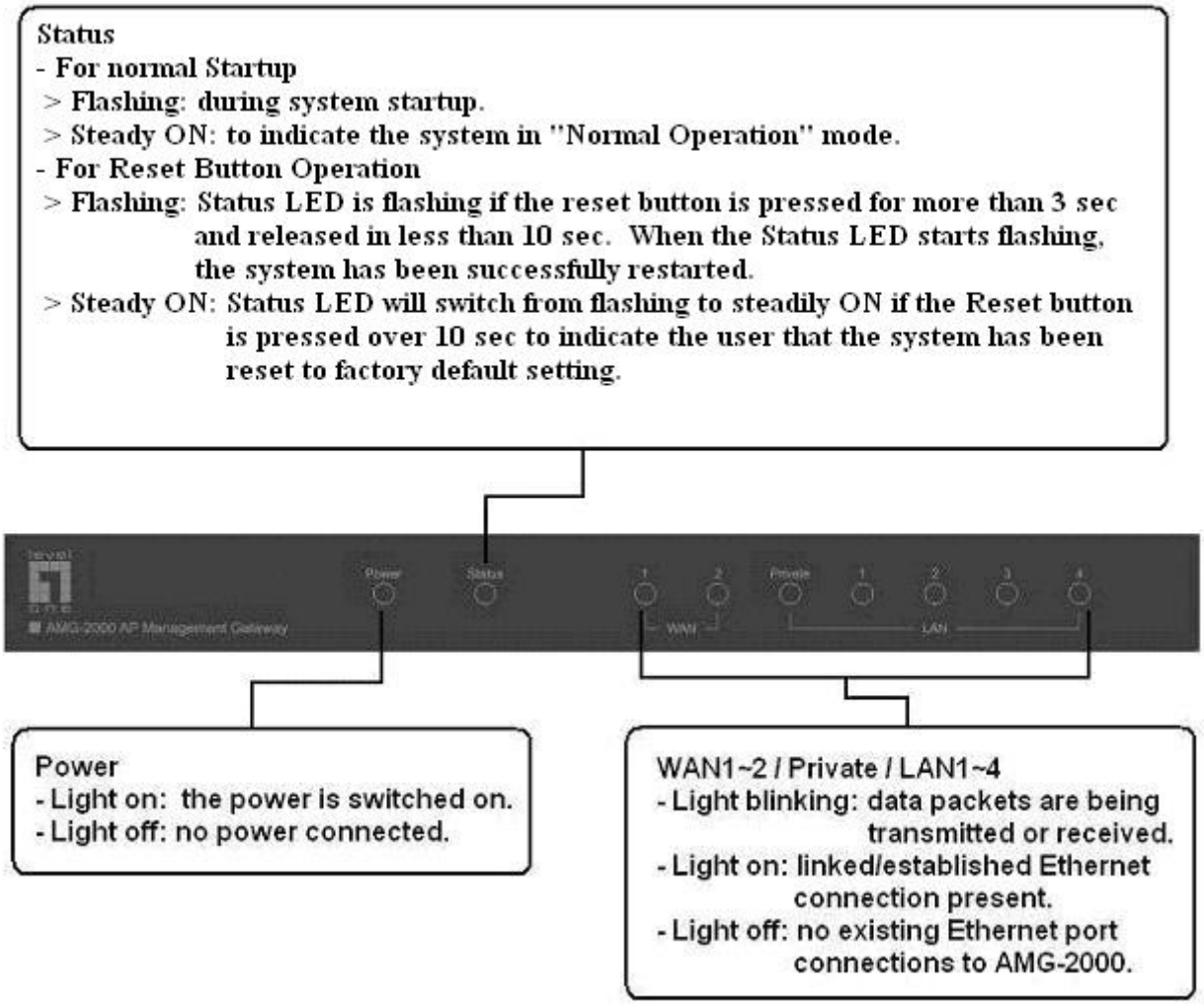
The standard package of AMG-2000 includes:

- AMG-2000 x 1
- CD-ROM x 1
- Quick Installation Guide x 1
- Power Adaptor x 1
- Straight-through Ethernet Cable x 1
- Console Cable x 1

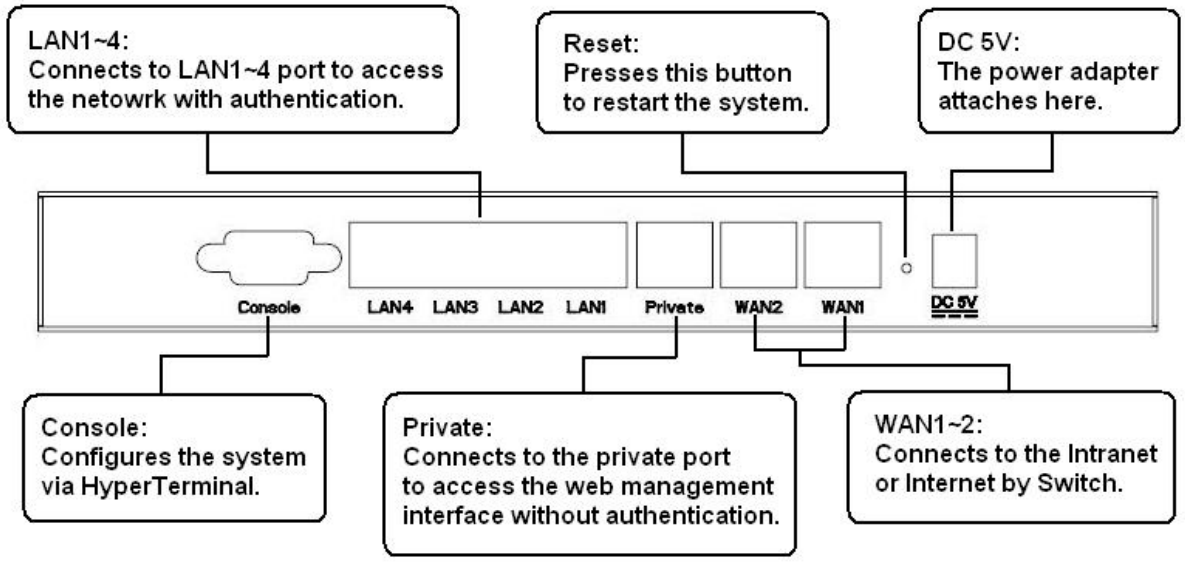
Warning: *Using a power supply with different voltage rating will damage this product.*

3.1.3 Panel Function Descriptions

Front Panel

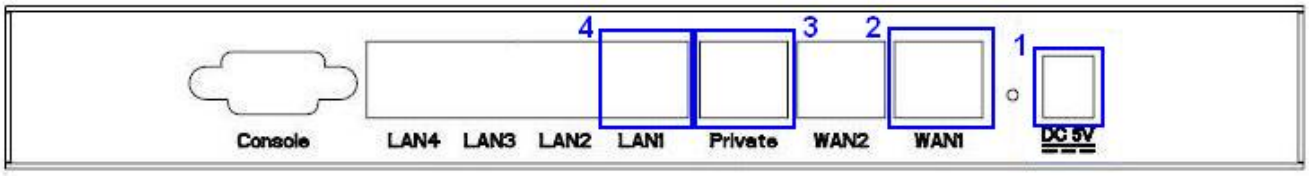


Rear Panel



3.1.4 Installation Steps

Please follow the following steps to install AMG-2000:



1. Connect the power adapter to the power socket on the rear panel. The Power LED should be on to indicate a proper connection.
2. Connect an Ethernet cable to the WAN1 Port on the rear panel. Connect the other end of the Ethernet cable to an ADSL modem, a cable modem or a switch/hub of the network. The LED of the WAN1 port should be on to indicate a proper connection.
3. Connect an Ethernet cable to Private Port on the rear panel. Connect the other end of the Ethernet cable to the user's PC. The LED of Private Port should be on to indicate a proper connection. (**Note:** No authentication is required for the users to access the network via Private Port and the administrator can enter the administrative user interface to perform configurations via Private Port.)
4. Connect an Ethernet cable to one of the LAN1~LAN4 Port on the rear panel. Connect the other end of the Ethernet cable to an AP or a switch. The LED of the LAN should be on to indicate a proper connection. (**Note:** Authentication is required for the clients to access the network via these LAN Ports.)

Attention: *Usually a straight-through cable could be applied when the AMG-2000 connects to an Access Point which supports automatic crossover. If after the AP hardware resets, the AMG-2000 could not be able to connect to the AP while connecting with a straight-through cable, the user have to pull out and plug-in the straight-through cable again. This scenario does NOT occur while using a crossover cable.*

After the hardware of AMG-2000 is installed completely, the system is ready to be configured in the following sections.

3.2 Software Configuration

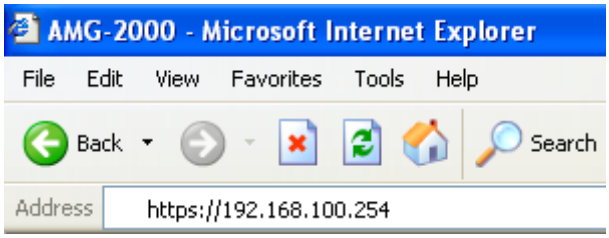
3.2.1 Quick Configuration

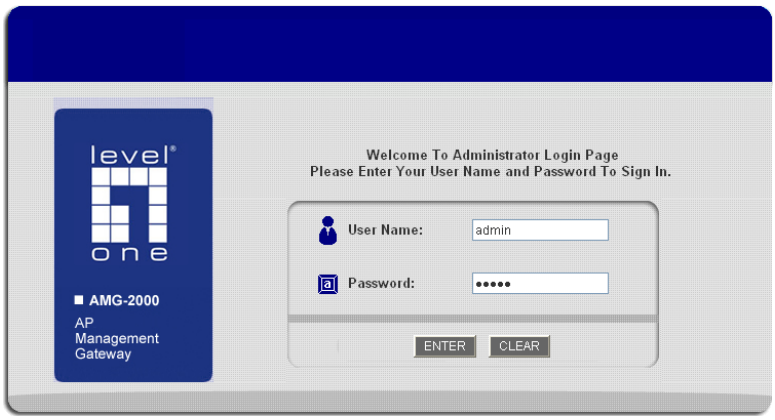
There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard provides a simple and easy way to guide you through the setup of AMG-2000 (for the AP configuration, you have to set it up in administrator interface). Follow the procedures and instructions given by the Wizard to enter the required information step by step. After saving and restarting AMG-2000, it is ready to use. There will be **6** steps as listed below:

1. Change Admin's Password
2. Choose System's Time Zone
3. Set System Information
4. Select the Connection Type for WAN Port
5. Add Local User Account (Optional)
6. Save and Restart AMG-2000

Please follow the following steps to complete the quick configuration.

1. Use the network cable of the 10/100BaseT to connect a PC to the LAN1~LAN4 port, and then start a browser (such as Microsoft IE or Firefox). Next, enter the gateway IP address as the web management interface's URL, the default is https://192.168.100.254. In the opened webpage, you will see the login screen. Enter ***"admin"***, the default username and password, in the User Name and Password column. Click ***Enter*** to log in.





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

AMG-2000 supports three accounts with different access privileges. You can log in as **admin**, **manager** or **operator**. The default password and access privilege for each account are as follows.

Admin: The administrator can access all area of the AMG-2000.

User Name: **admin**

Password: **admin**

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

User Name: **manager**

Password: **manager**

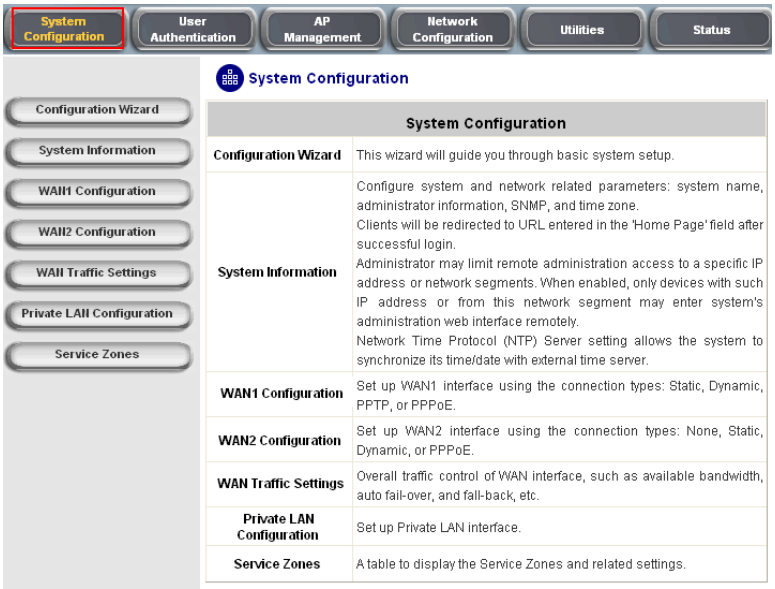
Operator: The operator can only access the area of ***Create On-demand User*** to create and print out the new on-demand user accounts.

User Name: **operator**

Password: **operator**

2. After successfully logging into AMG-2000, you can enter the web management interface and see the welcome screen. There is a ***Logout*** button on the upper right corner to log out the system when finished.

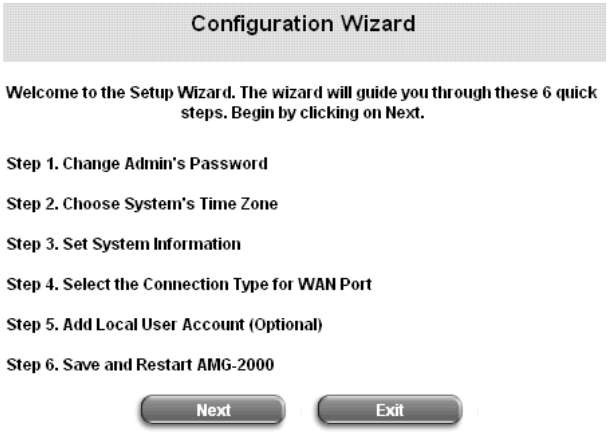
3. Then, run the configuration wizard to help you complete the configuration. Click ***System Configuration*** to the **System Configuration** homepage.



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

5. **Configuration Wizard**

First of all, you will see a welcome screen to briefly introduce the 6 steps. After a brief overview of the whole process, click ***Next*** to begin.



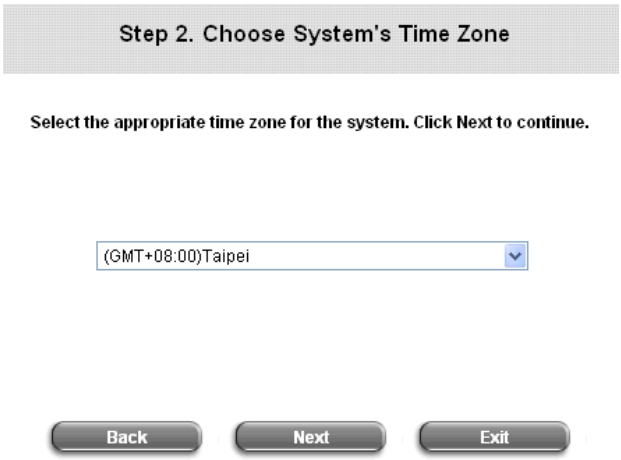
- **Step 1. Change Admin's Password**

  Enter a new password for the admin account and retype it in the verify password field (twenty-character maximum and no spaces). **The field with red asterisks is necessary to fill in.** Click ***Next*** to continue.

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

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

  Click ***Next*** to continue.



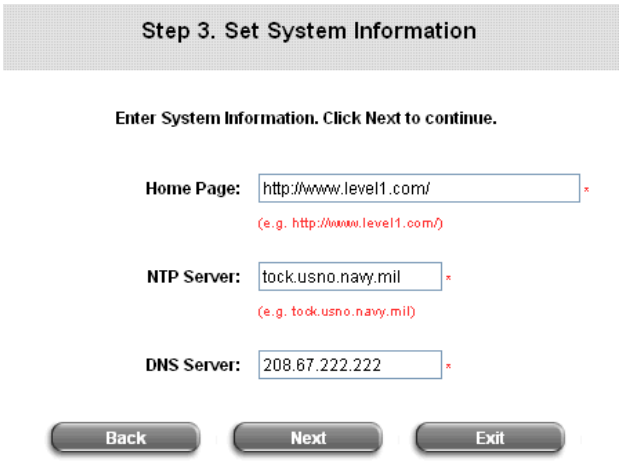
- **Step 3. Set System Information**

  Home Page: Enter the URL that users should be directed to when successfully authenticated or use the default.

  NTP Server: Enter the IP address or domain name of external time server for AMG-2000 time synchronization or use the default.

  DNS Server: Enter an IP address of DNS Server. Contact your network administrator if you are not sure of the DNS IP Address.

  Click ***Next*** to continue.



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

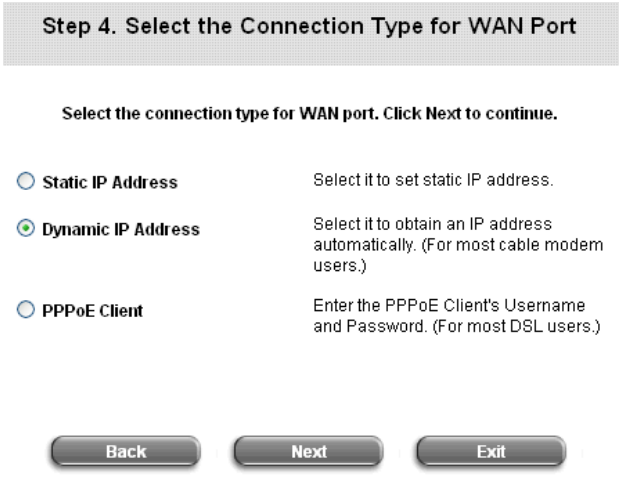
  There are three types of WAN1 port to select in wizard: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**.

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

  - **Dynamic IP Address**

    If this option is selected, AMG-2000 will obtain IP settings from an external DHCP server on network connected by WAN1 automatically.

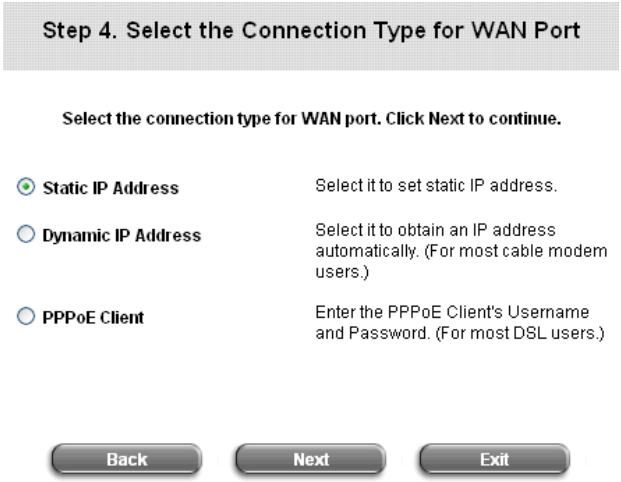
    Click ***Next*** to continue.

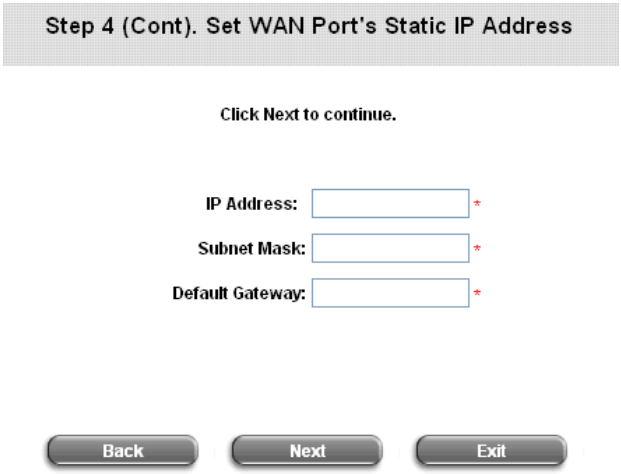


- **Static IP Address: Set WAN Port's Static IP Address**

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

  Click ***Next*** to continue.

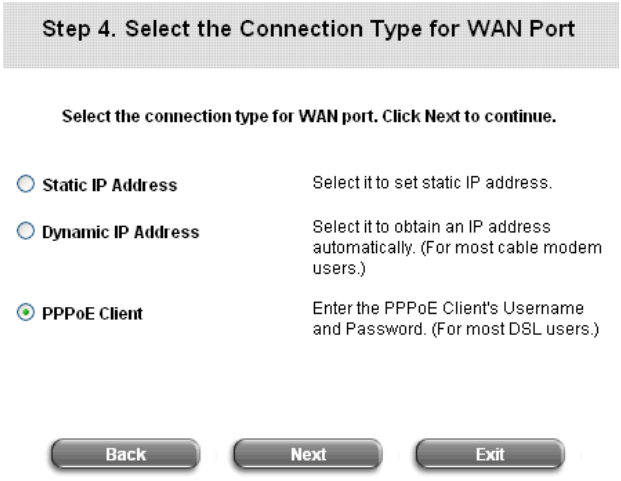


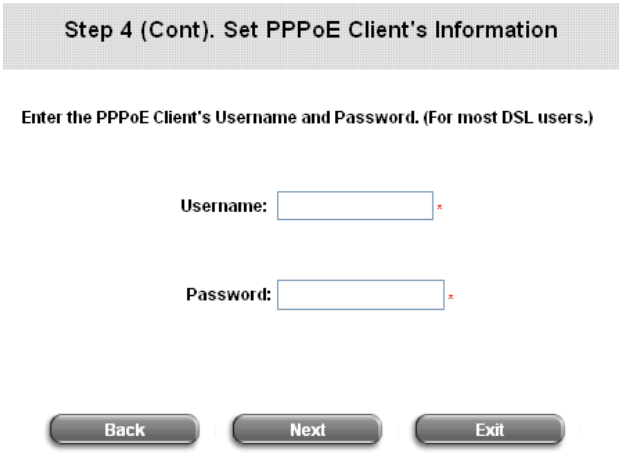


- **PPPoE Client: Set PPPoE Client's Information**

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

  Click ***Next*** to continue.

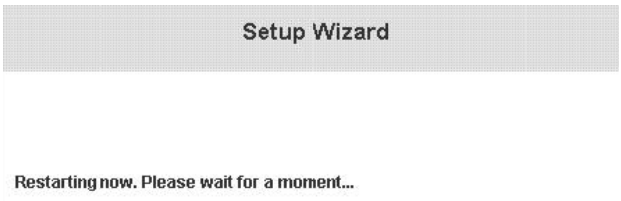




- Step 5. Add Local User Account (Optional)
  New user accounts can be added to the local user database. To add a user here, enter the ***Username*** (e.g. test), ***Password*** (e.g. test), ***MAC Address*** (optional) and assign a ***Policy*** to this account (or None), and press the ***Add Now*** button. More users can be added into the local user account database by clicking the ***Add Now*** button. Click ***Next*** to continue.

- **Step 6. Save and Restart AMG-2000**
  Click ***Restart*** to save the current settings and restart AMG-2000. The Setup Wizard is now completed.

- **Setup Wizard.**
  During AMG-2000 restarting, a **"Restarting now. Please wait for a moment..."** message will appear on the screen. Please do not interrupt AMG-2000 until the message has disappeared. This indicates that a complete and successful restart process has finished.



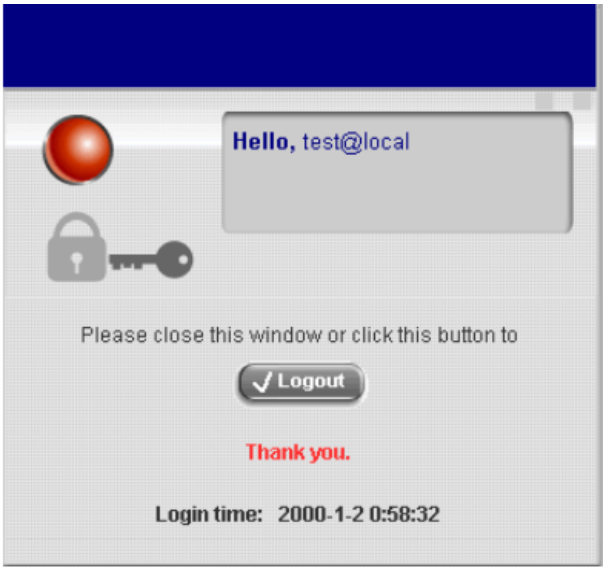
> ***Note:*** *During every step of the wizard, if you wish to go back to modify the settings, please click the* ***Back*** *button to go back to the previous step.*

3.2.2 User Login Portal Page

To login from the login portal page via the LAN1~LAN4 port, the user have to be identified the user name and password. The administrator also can verify the correctness of the configuration steps of AMG-2000.

1. First, connect a user-end device (for example, a PC) to the LAN1~LAN4 port of the AMG-2000, and set the device to obtain IP address automatically. After the user end obtains the network address, please open an Internet browser and the default login webpage will appear on the Internet browser.
   Typing in user information of a valid user account. Assumes local user database is chosen in the configuration wizard, key in the username and password created and then click ***Submit*** button (e.g. ***test@local*** for the username and ***test*** for the password).

2. Login success page appearing means AMG-2000 has been installed and configured successfully. Now, you can browse the network or surf the Internet!



3. But if you see the following screen with a sentence, **"Sorry, this feature is available for on-demand user only"**, it means you click the **"Remaining"** button by mistake. This button is only for on-demand users and if you are not an on-demand user, please just click the ***Submit*** button.

4. If you are an on-demand user, you can enter the username and password in the **"User Login Page"** and then click the ***Remaining*** button to know the remaining time or data quota of the account.

5. When an on-demand user logs in successfully, the following **Login Successfully** screen will appear and it is a little different from the normal user's login successfully screen. There is an extra line showing **"Remaining usage"** and a **"Redeem"** button.

- **Remaining usage:** Show the remaining time or data volume that the on-demand user can used to surf Internet.
- **Redeem:** When the remaining time or data size is insufficient, the user can buy additional account from the counter and add the quota to the current account. After clicking the ***Redeem*** button, you will see the following screen. Please enter the new username and password you got and click ***Enter*** button. Then you will see the total available use time and data size after adding credit.

Chapter 4 Web Interface Configuration

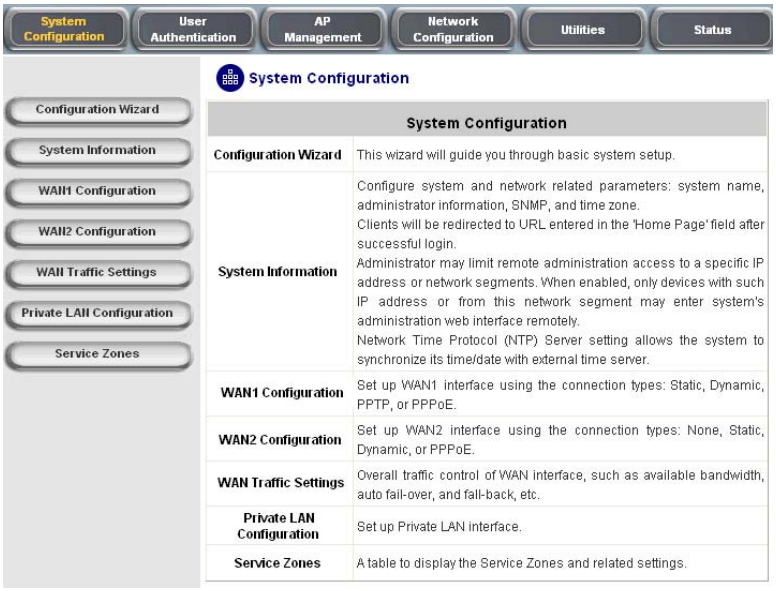
This chapter will guide you through further detailed settings. The following table is the UI and functions of the AMG-2000.

OPTION	System Configuration	User Authentication	AP Management	Network Configuration	Utilities	Status
FUNCTION	Configuration Wizard	Authentication Configuration	AP List	Network Address Translation	Change Password	System Status
	System Information	Black List Configuration	AP Discovery	Privilege List	Backup/Restore Settings	Interface Status
	WAN1 Configuration	Policy Configuration	Manual Configuration	Monitor IP List	Firmware Upgrade	Current Users
	WAN2 Configuration	Additional Configuration	Template Settings	Walled Garden List	Restart	Traffic History
	WAN Traffic Settings		Firmware Management	Proxy Server Properties	Wake On Lan	Notification Configuration
	Private LAN Configuration		AP Upgrade	Dynamic DNS		
	Service Zones			IP Mobility		
				VPN Configuration		

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

4.1 System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN1 Configuration**, **WAN2 Configuration**, **WAN Traffic Settings, Private LAN Configuration** and **Service Zones.**

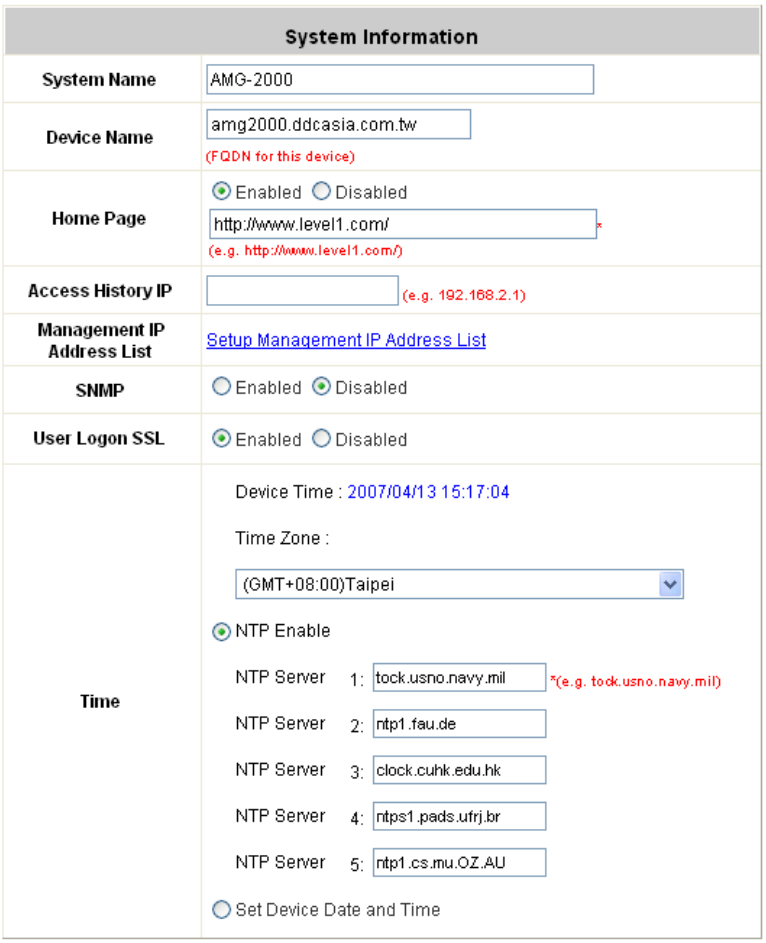


4.1.1 Configuration Wizard

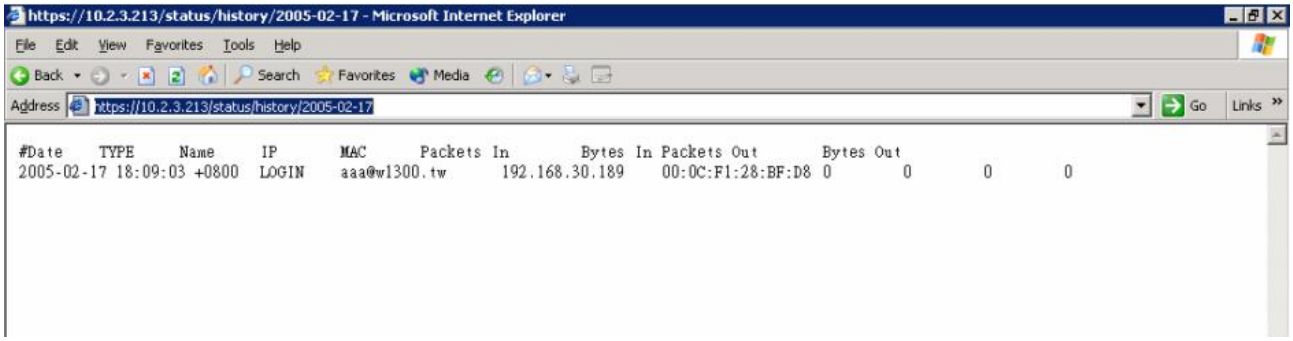
Please refer to **3.2.1 Quick Configuration** for the detail description of **Configuration Wizard**.

4.1.2 System Information

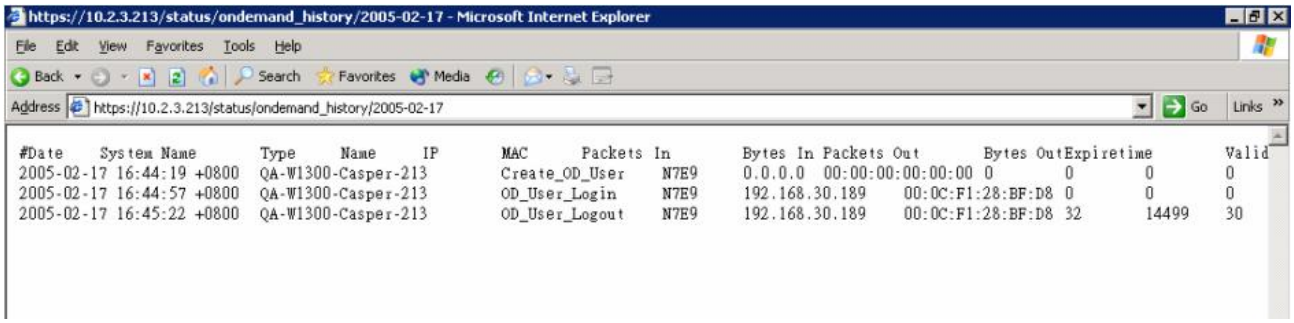
Most of the major system information about AMG-2000 can be set here. Please refer to the following description for each field:



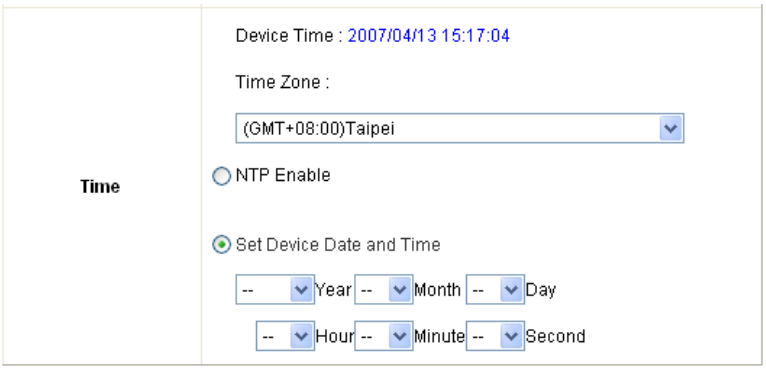
- **System Name:** Set the system's name or use the default.
- **Device Name:** FQDN (Fully-Qualified Domain Name). This is the domain name of the AMG-2000 as seen on client machines connected on LAN ports. A user on client machine can use this name to access AMG-2000 instead of its IP address.
- **Home Page:** Enter the website of a Web Server to be the homepage. When users log in successfully, they will be directed to the homepage set. Usually, the homepage is set to the company's website, such as http://www.leve1.com. If the home page function is disabled, the user will be directed to the URL she/he tries to connect originally.
- **Access History IP:** Specify an IP address of the administrator's computer or a billing system to get billing history information of AMG-2000 with the predefined URLs as the following:
  Traffic History：https://10.2.3.213/status/history/2005-02-17



On-demand History：https://10.2.3.213/status/ondemand_history/2005-02-17

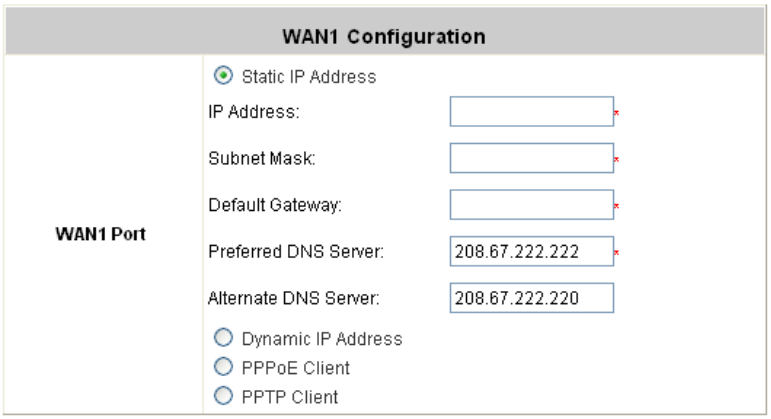


- **Management IP Address List:** Set the IP range which is able to connect to the web management interface via WAN and/or LAN1~LAN4 port. For example, 10.2.3.0/24 means that as long as you are within the IP address range of 10.2.3.0/24, you can reach the administration page of AMG-2000. If the IP range bit number is omitted, 32 is used which specify a single IP address.
- **SNMP:** AMG-2000 supports SNMPv2. If the function is enabled, you can assign the Manager IP address and the SNMP community name used to access the management information base (MIB) of the system. However, for the external system, SNMP is a read-only function.
- **User Logon SSL:** Enable to activate https (encryption) or disable to activate http (non encryption) login page.
- **Time:** AMG-2000 supports NTP communication protocol to synchronize the system time with remote time server. Please specify the local time zone and IP address of at least one server in the system configuration interface for adjusting the time automatically. (Universal Time is Greenwich Mean Time, GMT). You can also set the time manually when you select **"Set Device Date and Time (GMT)"**. Please enter the date and time for the corresponding fields.



4.1.3 WAN1 Configuration

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



- **Static IP Address:** Manually specifying the IP address of the WAN port. The red asterisk marks indicate required fields and have to be filled.

  IP address: the IP address of the WAN1 port.

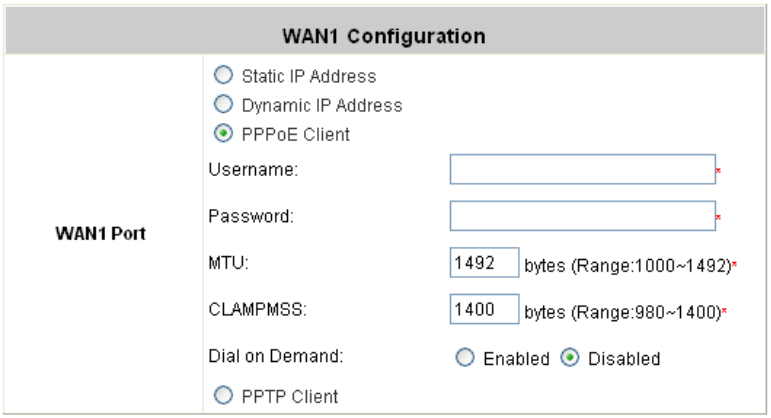
  Subnet mask: the subnet mask of the network WAN1 port connects to.

  Default gateway: a gateway of the network WAN1 port connects to.

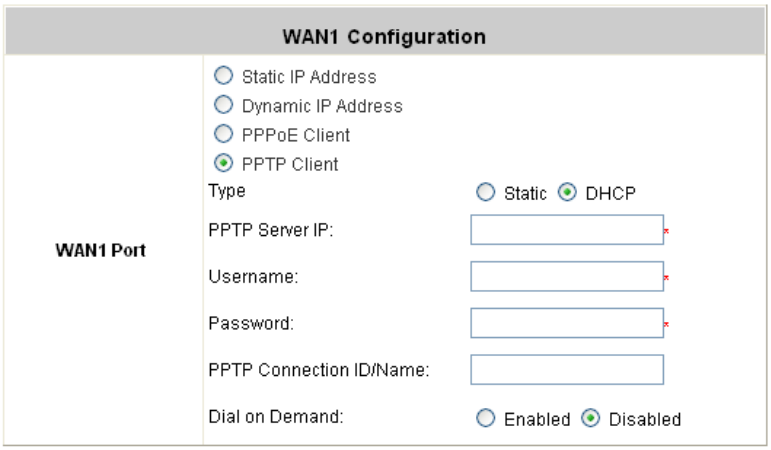
  Preferred DNS Server: The primary DNS server is used by the system.

  Alternate DNS Server: The substitute DNS server is used by the system. This is an optional field.
- **Dynamic IP address:** It is only applicable for the network environment where a DHCP server is available. Click the ***Renew*** button to get an IP address.

- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the **"User Name"**, **"Password"**, **"MTU"** and **"CLAMPMSS"**. There is a **Dial on demand** function under PPPoE. If this function is enabled, you can set a **Maximum Idle Time**. When the idle time is reached, the system will automatically disconnect itself.



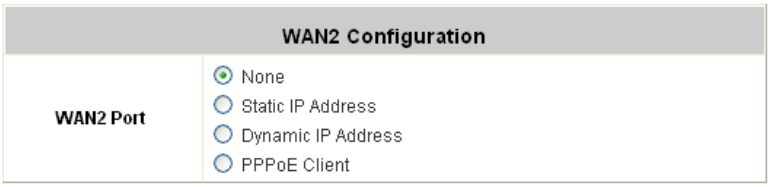
- **PPTP Client:** Set WAN1 port to connect to external PPTP server to establish PPTP VPN tunnel. You can select **Static** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red mark are required. Please fill in these fields. There is a **Dial on demand** function under PPTP. If this function is enabled, you can set a **Maximum Idle Time**. When the idle time is reached, the system will automatically disconnect itself.



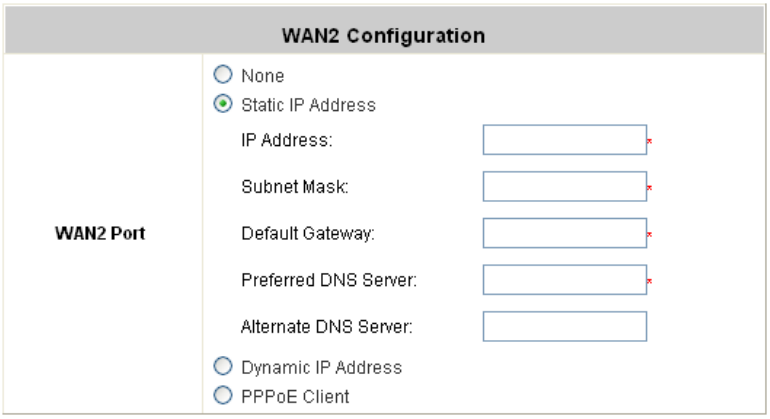
4.1.4 WAN2 Configuration

Except select **None** to disable this function, there are 3 connection types for the WAN2 port: **Static IP Address, Dynamic IP Address** and **PPPoE Client**.

- **None**: The WAN2 Port is disabled.

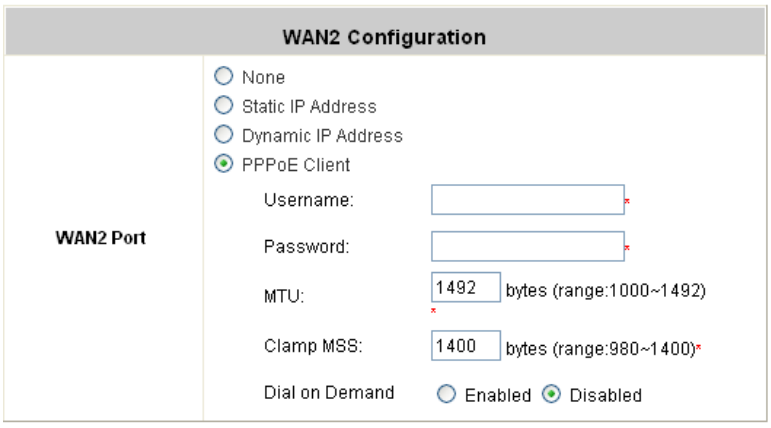


- **Static IP Address:** Specify the IP Address, Subnet Mask, Preferred DNS Server, and Default Gateway of WAN2 Port, which should be applicable for the network environment.



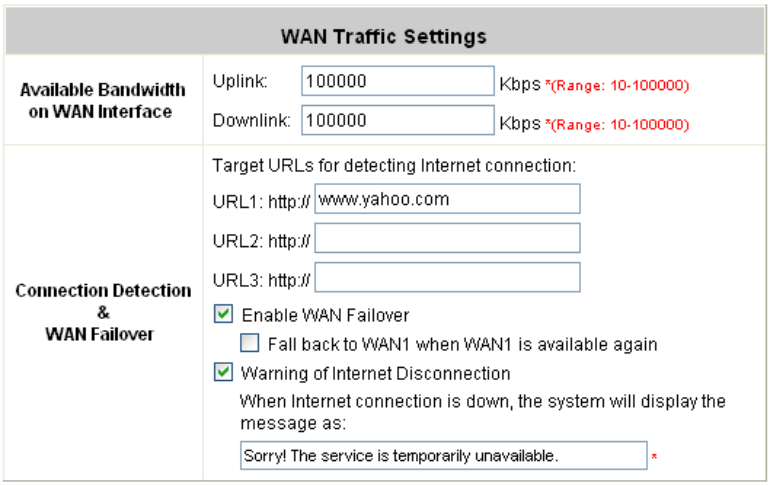
- **Dynamic IP Address:** Select this when WAN2 Port can obtain IP address automatically, such as a DHCP Server available from WAN2 Port.

- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the **"User Name"**, **"Password"**, **"MTU"** and **"CLAMPMSS"**. There is a **Dial on demand** function under PPPoE. If this function is enabled, you can set a **Maximum Idle Time**. When the idle time is reached, the system will automatically disconnect itself.



4.1.5 WAN Traffic Settings

The section is for administrator to configure the control over the entire system's traffic though the WAN interface (WAN1 and WAN2 ports).



Available Bandwidth on WAN Interface:

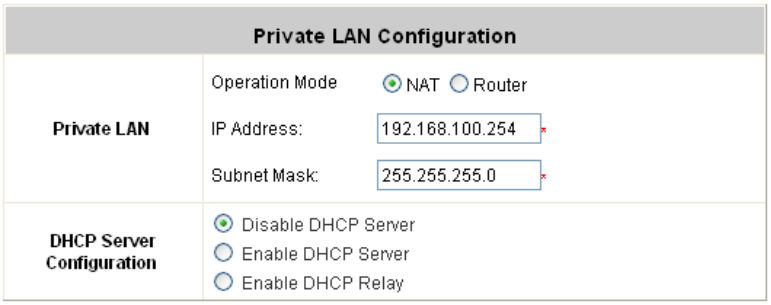
- **Uplink:** It specifies the maximum uplink bandwidth that can be shared by clients of the system.
- **Downlink:** It specifies the maximum downlink bandwidth that can be shared by clients of the system.

Connection Detection & WAN Failover:

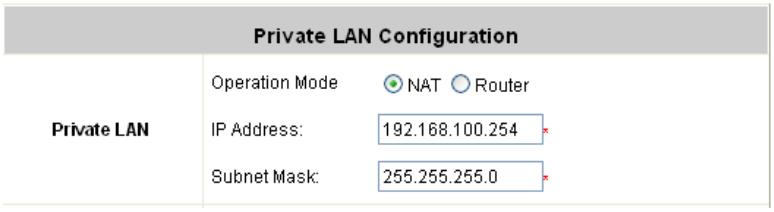
- **Target URLs for detecting Internet connection:** These URLs are used by the system as the targets to detect Internet connection, for the purpose of alert of Internet disconnection and WAN Failover. At least one URL is required to enable WAN Failover.
- **Enable WAN Failover:** Normally a Service Zone uses WAN1 as it primary WAN interface. When enabled and WAN2 is available, WAN1's traffic will be routed to WAN2 when WAN1 connection is down. On the other hand, a Service Zone's policy could also use WAN2 as its interface; in that case, if WAN2 is down, the WAN2's traffic under its policy will also be routed to WAN1.
- **Fall back to WAN1 when WAN1 is available again:** If WAN Failover is enabled, the traffic will be routed to WAN2 automatically when WAN1 connection fails. When enabled, the routed traffic will be back to WAN1 when WAN1 connection is recovered.
- **Warning of Internet Disconnection:** When enabled, the text box is for the administrator to enter an alert message in order to notify users that the Internet connection is down. The alert message will show up in the users' browser when they try to access any website on Internet.

4.1.6 Private LAN Configuration

When accessing the network through the Private LAN port, users are not required to be authenticated. In this section, you can set the related configuration for the private LAN port and DHCP server.



- **Private LAN Configuration**



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 private port.

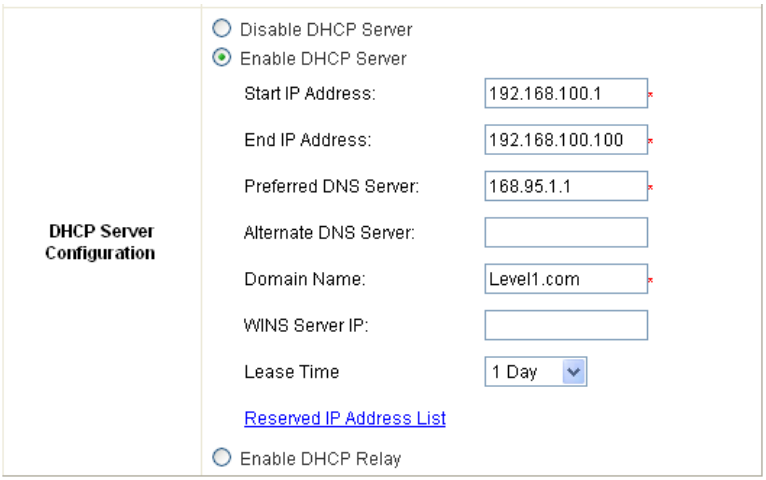
Subnet Mask: Enter the desired subnet mask for the private port.

- **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.

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



Enable DHCP Server—Start/End IP Address: 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 change the DHCP.

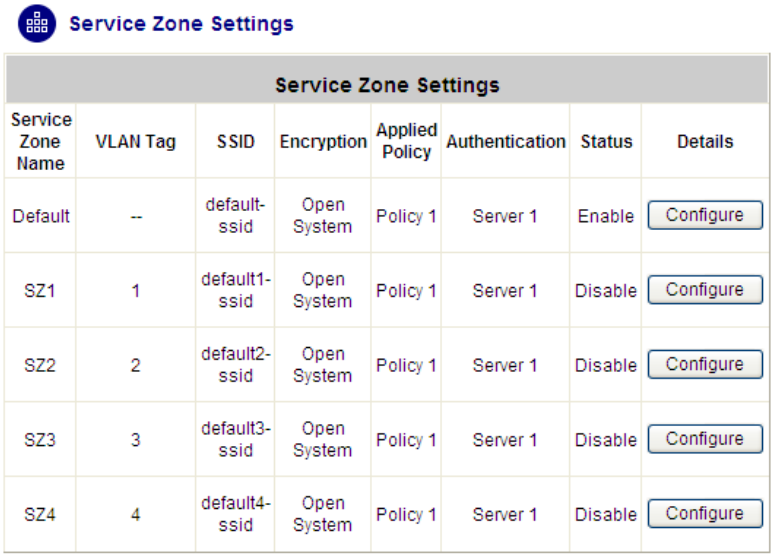
Reserved IP Address List: For reserved IP address settings in detail, please click the hyperlink of ***Reserved IP Address***. If you want to use the **Reserved IP Address List** function, click on the **Reserved IP Address List** on the management interface. Then, the setup of the Reserved IP Address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

3. **Enable DHCP Relay:** If you want to enable this function, you must specify other DHCP Server IP address. See the following figure. For more information about DHCP relay, please see ***Appendix H. DHCP Relay***.

4.1.7 Service Zones

A Service Zone is a logical network area to cover certain wired and wireless networks in an organization such as SMB or branch offices. By associating a unique VLAN Tag and SSID with a Service Zone, administrators can separate wired network and wireless network into different logical zones. Users attempting to access the resources within the Service Zone will be controlled based on the access control profile of the Service Zone, such as authentication, security feature, wireless encryption method, traffic control, etc. *For more information about Service Zone, please refer to* ***Appendix F*****.**

There are up to five Service Zones to be utilized; by default, they are named as: **Default, SZ1, SZ2, SZ3 and SZ4**, as shown in the table below.



Service Zone Settings

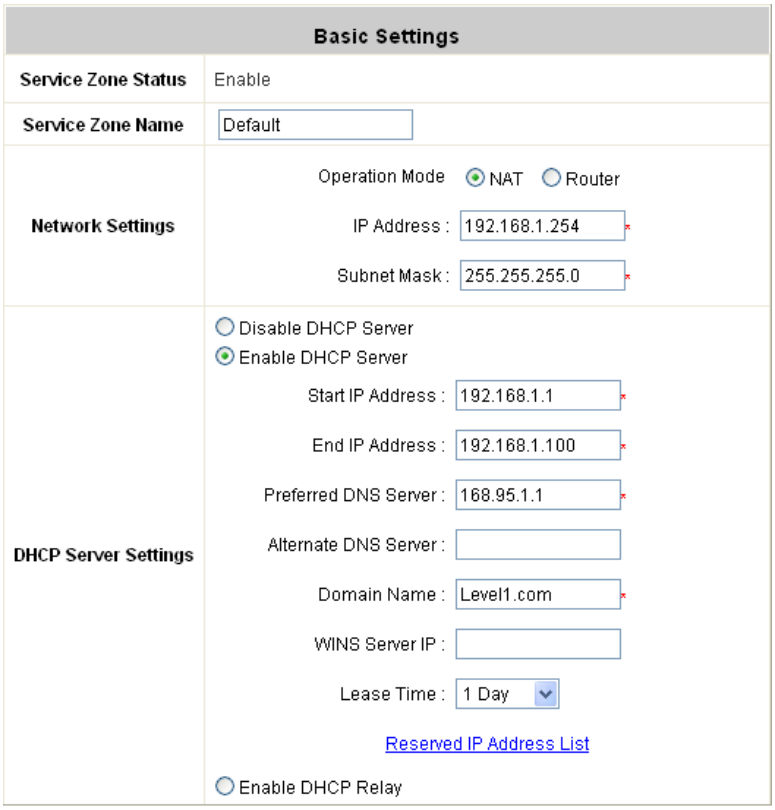
Service Zone Settings							
Service Zone Name	VLAN Tag	SSID	Encryption	Applied Policy	Authentication	Status	Details
Default	--	default-ssid	Open System	Policy 1	Server 1	Enable	Configure
SZ1	1	default1-ssid	Open System	Policy 1	Server 1	Disable	Configure
SZ2	2	default2-ssid	Open System	Policy 1	Server 1	Disable	Configure
SZ3	3	default3-ssid	Open System	Policy 1	Server 1	Disable	Configure
SZ4	4	default4-ssid	Open System	Policy 1	Server 1	Disable	Configure

- Service Zone Name: Mnemonic name of the Service Zone.
- VLAN Tag: The VLAN tag number that is mapped to the Service Zone.
- SSID: The SSID that is associated with the Service Zone.
- Encryption: Data encryption method for wireless networks within the Service Zone.
- Applied Policy: The policy that is applied to the Service Zone.
- Authentication: Default authentication method/server that is used within the Service Zone.
- Status: Each Service Zone can be enabled or disabled.
- Details: Configurable, detailed settings for each Service Zone.

Click ***Configure*** button to configure each Service Zone: **Basic Settings**, **Authentication Settings** and **Wireless Settings**.

1) *Service Zone Settings —Basic Settings*

The system supports three types of DHCP modes, **Disable DHCP Server**, **Enable DHCP server**, and **Enable DHCP relay**. Each service zone can have its own DHCP setting. Select the radio button of Disable DHCP Server to disable the built-in DHCP server when clients are assigned static IP addresses. Select the radio button of Enable DHCP Server to enable the built-in DHCP server. When the Enable DHCP server is chosen, the system will act as a DHCP server and assign IP addresses to its clients. Select the radio button of Enable DHCP Relay when a service zone is connected to an external DHCP server. When Enable DHCP Relay is chosen, the IP addresses of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this service zone.



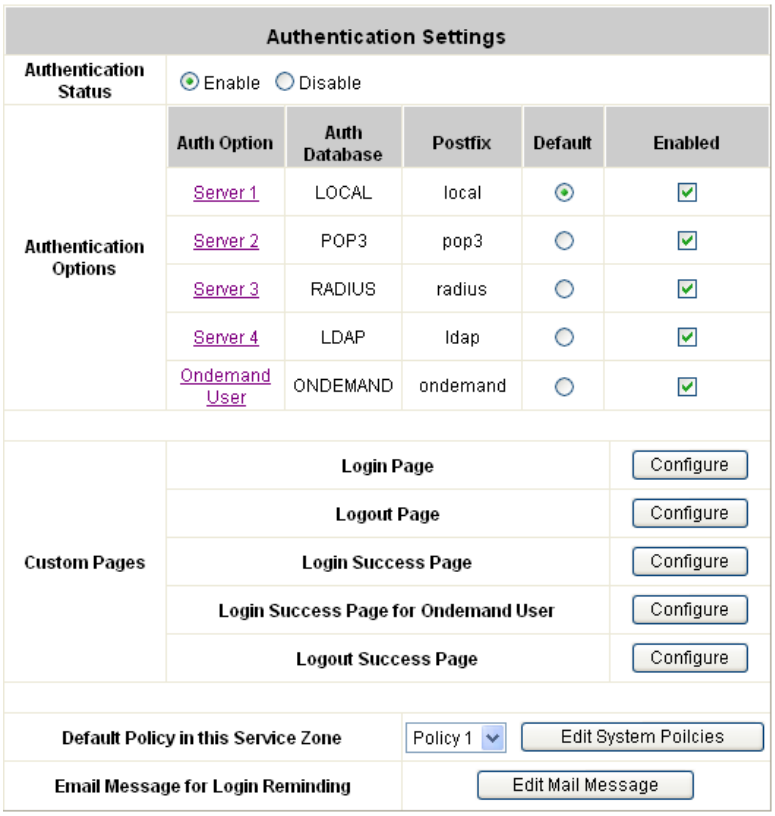
- **Service Zone Status:** Each service zone can be enabled or disabled except for the default service zone.
- **Service Zone Name:** The name of service zone could be input here.
- **Operation Mode:** Contains **NAT** mode and **Router** mode. When NAT mode is chosen, the service zone runs in NAT mode. When Router mode is chosen this service zone runs in Router mode.
- **IP address:** The IP Address of this service zone.
- **Subnet Mask:** The subnet Mask of this service zone.
- **DHCP Server:** Related information needed on setting up the DHCP Server is described as follows: DHCP pool Start IP Address, DHCP pool End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Server, Lease Time, and Reserved IP Address List.
- **WINS Server IP:** The IP address of the WINS (Windows Internet Naming Service) server that if WINS server is applicable to this service zone.
- **Lease Time:** This is the time period that the IP addresses issued from the DHCP server are valid and available.
- **Reserved IP Address List:** Each service zone can reserve up to 40 IP addresses from predefined DHCP

range to prevent the system from issuing these IP addresses to downstream clients. The administrator can reserve a specific IP address for a special device with certain MAC address.

- **Domain Name:** Enter the Windows domain name for this service zone.
- **Enable DHCP server:** This allows the enabling/disabling the built-in DHCP server.
- **Start IP Address / End IP Address:** A range of IP addresses that built-in DHCP server will assign to clients. Please change it accordingly at *System—General—Management IP Address* List to permit the administrator to login to the AMG-2000 admin page after the default IP address of Network Interface is changed.

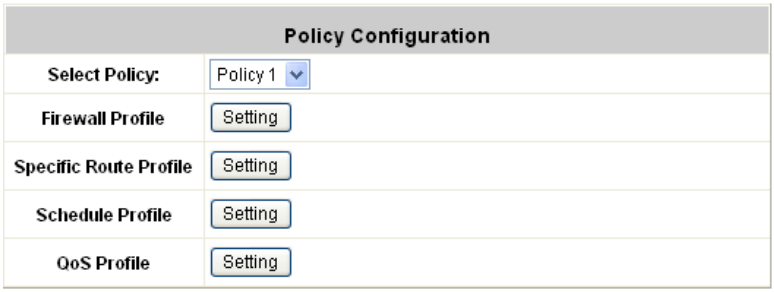
2) *Service Zone Settings —Authentication Settings*

The system supports five types of authentication database that are Local, POP3, RADIUS, LDAP, and NT Domain and provides up to four authentication options and one Guest Users authentication option. The administrator needs to activate and configure at least one of these authentication databases for an enabled service zone. Postfix is used to inform the system which type of authentication database to be used for authentication when multiple databases are concurrently in use. Each authentication option is distinguished by the postfix in clients' username such as "user1@postfix1". One of authentication database can be assigned as default for a service zone. Thus, for the authentication option being assigned as default, the postfix can be omitted while entering username.

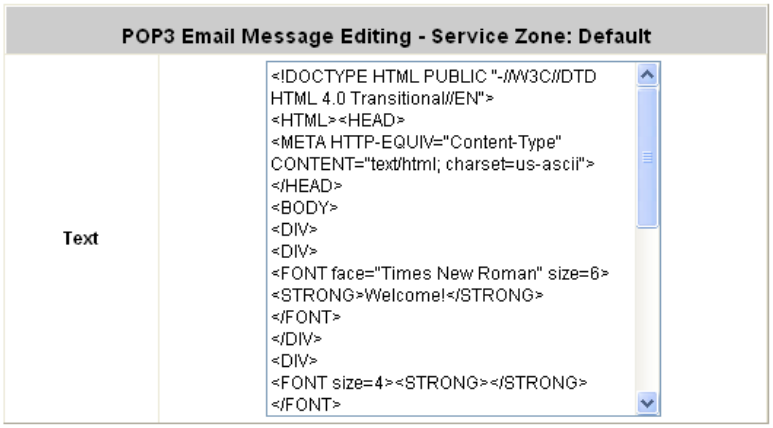


- **Custom Pages:** There are five users' login and logout pages that can be customized by administrators for each service zone.
- **Default Policy in this Service Zone:** There are one Global and eight sets of policy profiles in the system. Each policy consists of Firewall, Specific Route, Schedule, and QoS. Global policy only has Firewall and Specific Route profile. Policies can be defined in the policy tab. The administrator can select one of the defined policies to apply it to the specific service zone. Please refer to ***4.2.3 Policy Configuration*** for

complete description.



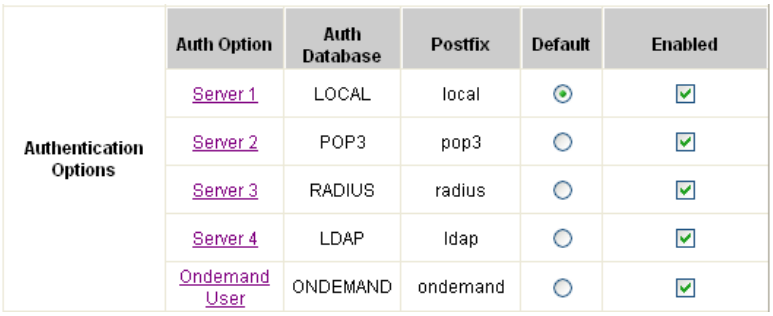
- **Email Message for Login Reminding:** Click ***Edit Mail Message*** to change the content for Login reminding words. Clients will receive an email with this reminding content when they access their mail servers before logging in the system.



2.1) Authentication Options

Click the hyperlink of **Auth Option**, the **Authentication option** page will appear, from **Server1~4** and **Guest Users.**

Click the button of ***Configure*** to have further configuration.



2.2) Custom Pages

There are five users' login and logout pages for each service zone that can be customized by administrators.

Click the button of ***Configure***, the **Login (Logout)** page will appear, including **Login page**, **Logout Page**, **Login Success Page**, **Login Success Page for Instant Account** and **Logout Success Page.**

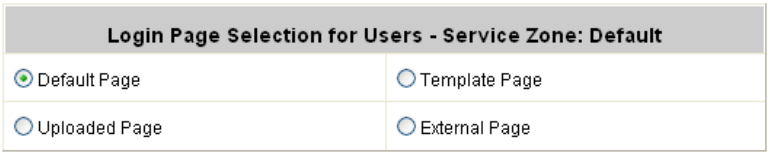
Click the radio button of page selections to have further configuration.

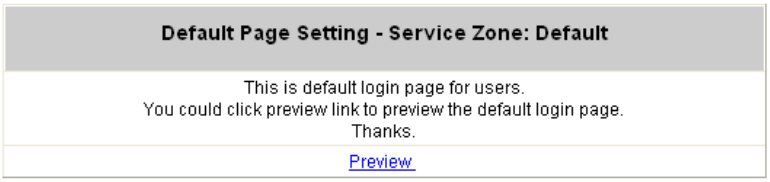
2.2.1) Custom Pages — **Login Page**

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.

- *Custom Pages — Login Page —* ***Default Page***

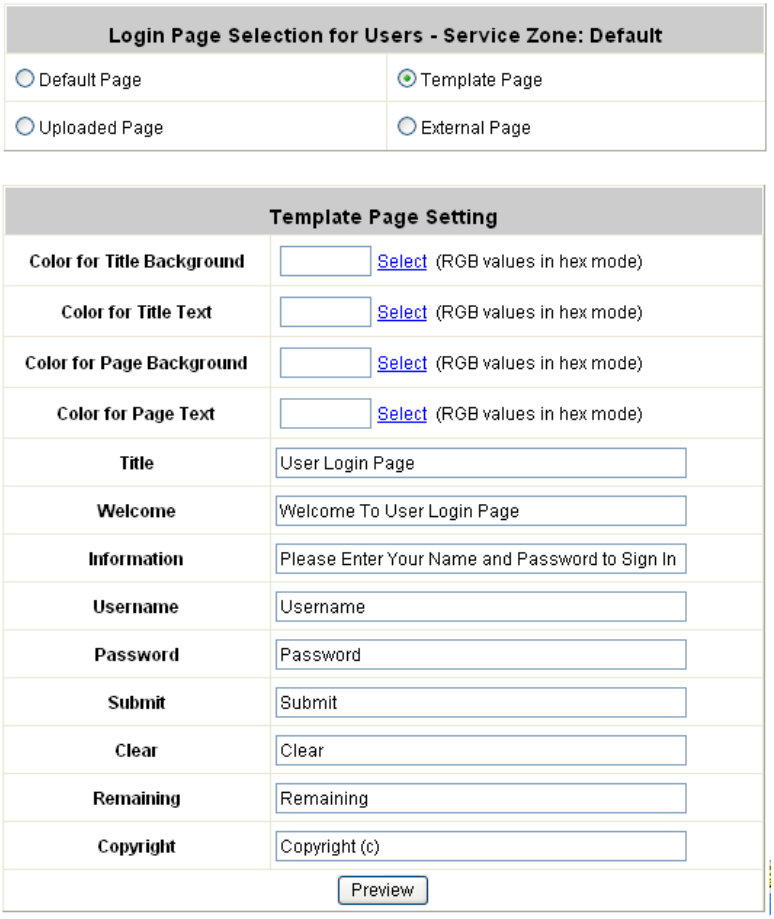
  Choose Default Page to use the default login page.





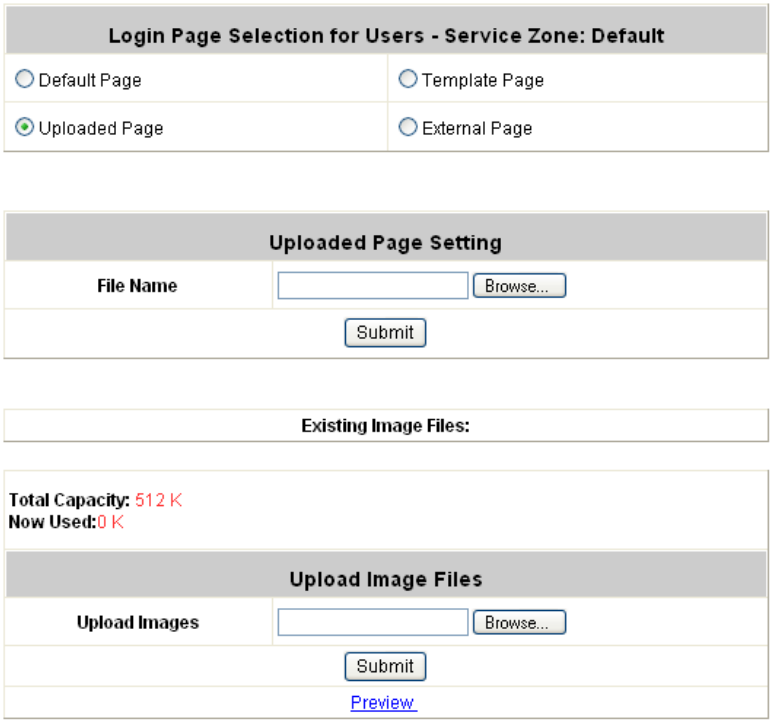
- *Custom Pages — Login Page —* ***Template Page***

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



- *Custom Pages — Login Page —* ***Uploaded Page***

  Choose Uploaded Page and upload a login page.



  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>
```

And 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.

Remote VPN : <img src=images/xx.jpg">
Default Service Zone: <img src=images0/xx.jpg">
Service Zone 1 : <img src=images1/xx.jpg">
Service Zone 2 : <img src=images2/xx.jpg">
Service Zone 3 : <img src=images3/xx.jpg">
Service Zone 4 : <img src=images4/xx.jpg">

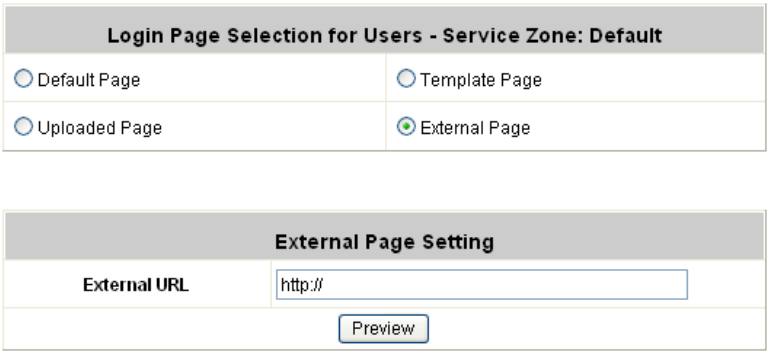
Click the ***Browse*** button to select the file to upload. Then click ***Submit*** to complete the upload process.

Next, 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.

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.

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

- *Custom Pages —Login Pages —**External Page***



Choose the ***External Page*** selection and get the login page from the specific website. In the External Page Setting, enter the URL of the external login page and then click ***Apply***.

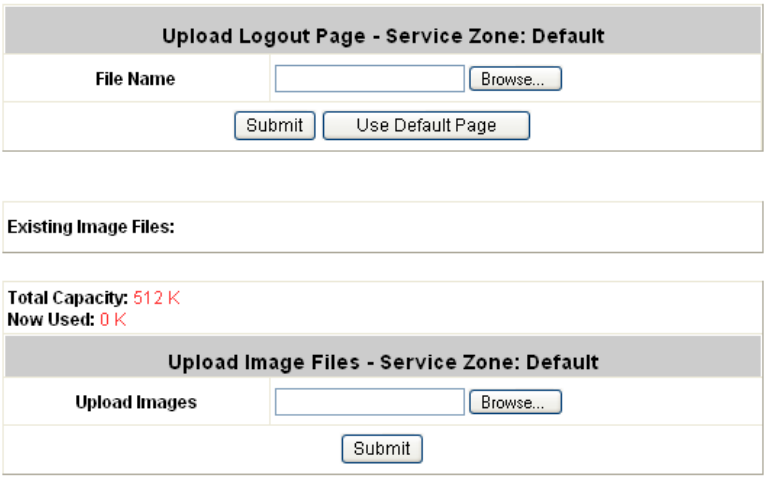
After applying the setting, the new login page can be previewed by clicking ***Preview*** button at the bottom of this page.

The user-defined logout 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>
```

2.2.2) Custom Pages — **Logout Page**

The administrator can apply their own logout page in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page—Uploaded Page" instructions for more details.



Note: 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 customized logout page can be previewed by clicking ***Preview*** at the bottom of this page. If restore to factory default setting is needed for the logout interface, click the "**Use Default Page"** button.

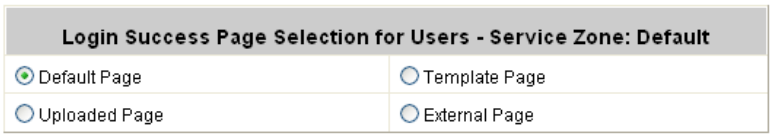
```
<form action="userlogout.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Logout">
<input type="reset" name="clear" value="Clear">
</form>
```

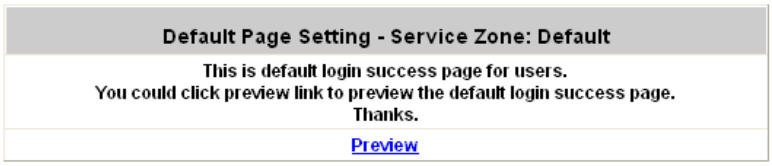
2.2.3) Custom Pages — **Login Success Page**

The users can apply their own Login Success page in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

- *Custom Pages — Login Success Page —* ***Default Page***

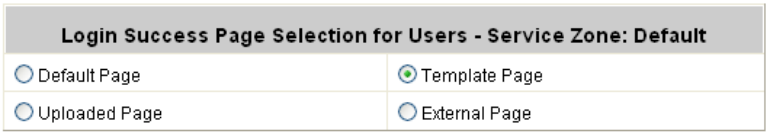
Choose Default Page to use the default login success page.

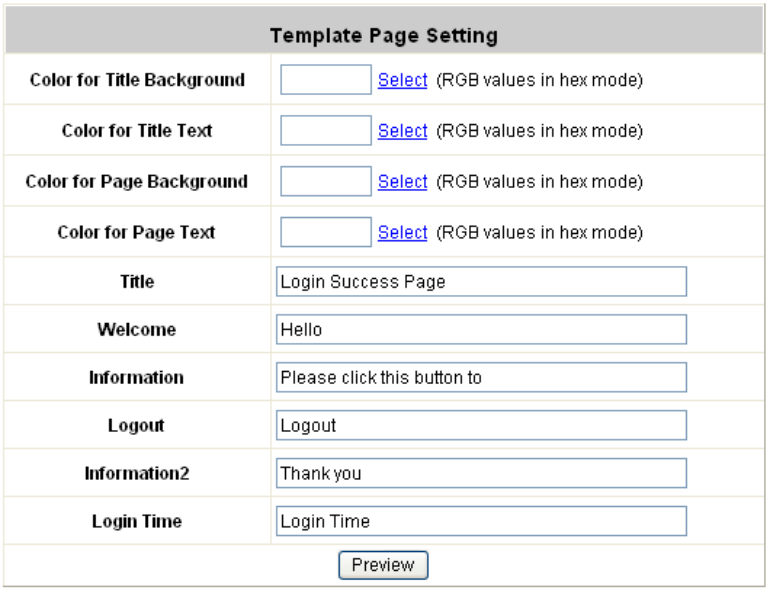




- *Custom Pages — Login Success Page —* ***Template Page***

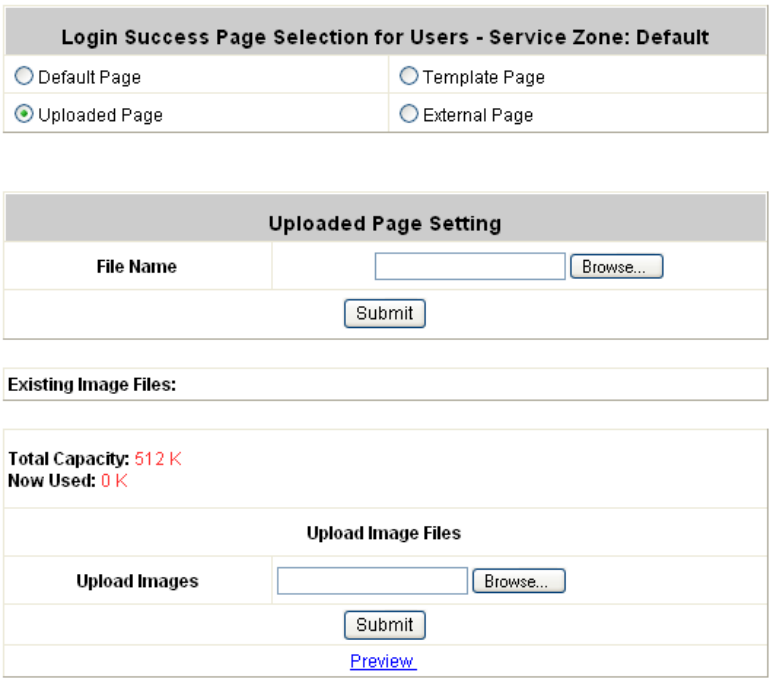
Choose Template Page to make a customized login success page. Click ***Selec***t to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.





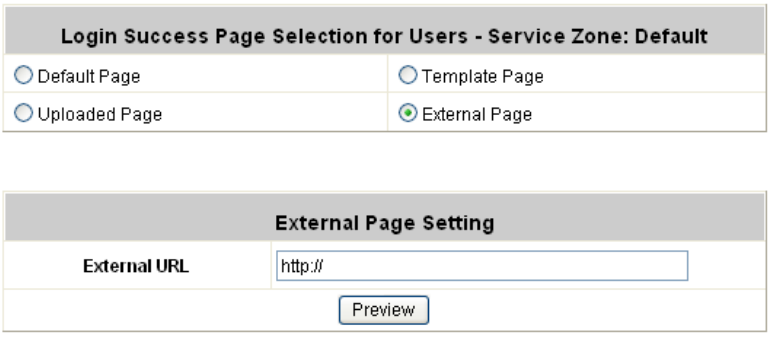
- *Custom Pages — Login Success Page—* ***Uploaded Page***

Choose Uploaded Page and get the login success page to upload. Click the Browse button to select the file for the login success page upload. Then click Submit to complete the upload process. After the upload process is completed and applied, the new login success page can be previewed by clicking Preview button at the bottom.



- *Custom Pages — Login Success Page —* ***External Page***

Choose the External Page selection and get the login success page from the specific website. In the External Page Setting, enter URL of the external login page and then click Apply. After applying the setting, the new login success page can be previewed by clicking Preview button at the bottom of this page

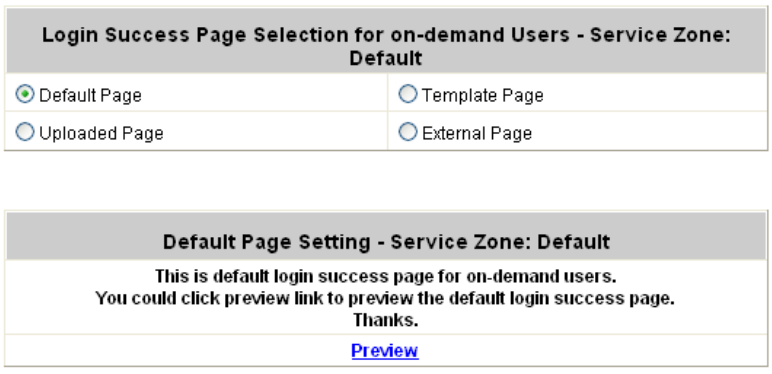


2.2.4) Custom Pages — Login Success Page for Instant Account

The users can apply their own Login Success page for Instant Users in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

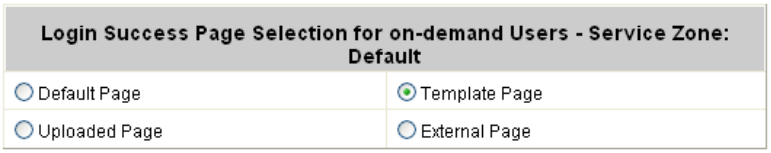
- *Custom Pages — Login Success Page for Instant Account —* ***Default Page***

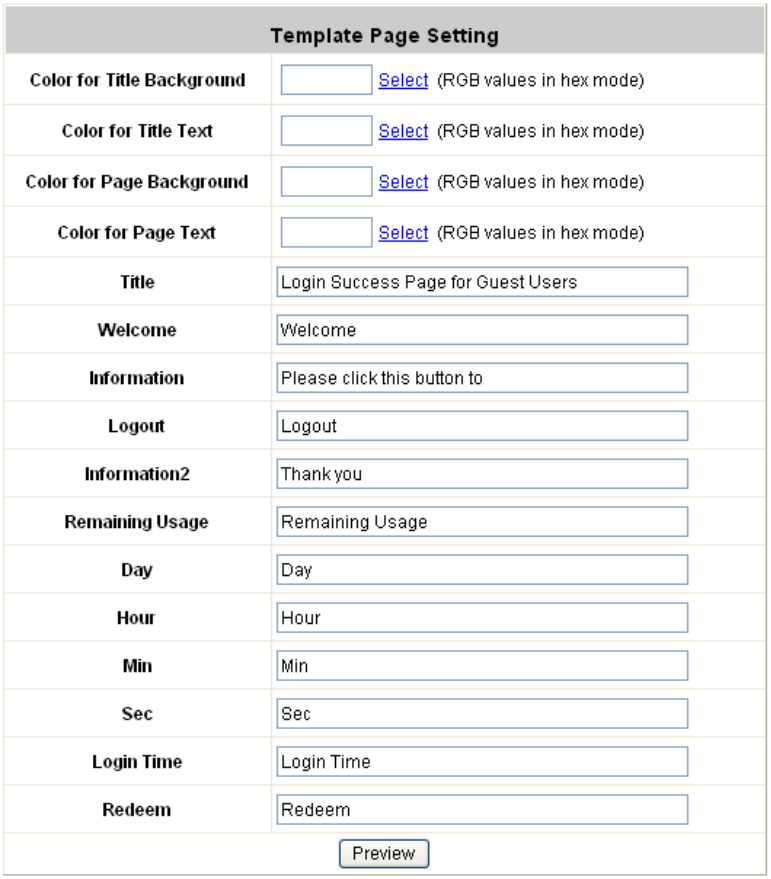
Choose Default Page to use the default login success page for Instant account



- *Custom Pages — Login Success Page for Instant Account — **Template Page***

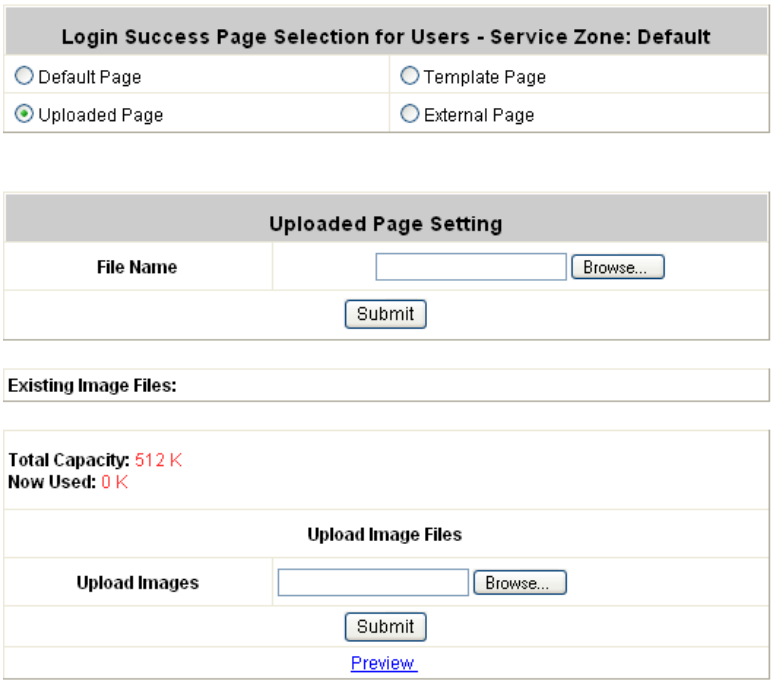
  Choose Template to make a customized login success for Instant account. Click *Select* to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result.





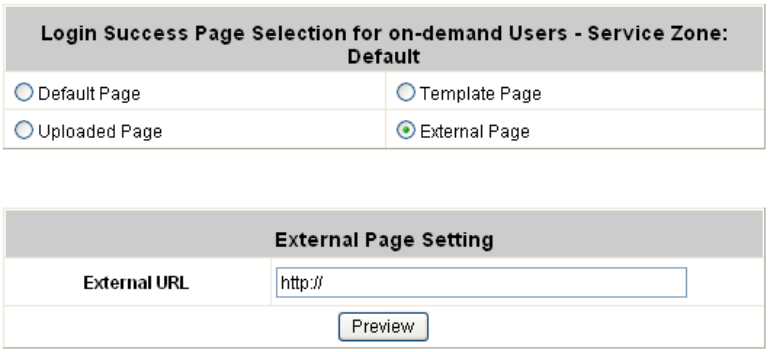
- *Custom Pages — Login Success Pages for Instant Account — **Uploaded Page***

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



- *Custom Pages —Login Success Pages for Instant Account —* ***External Page***

  Choose the External Page selection and get the login success page from the specific website. In the External Page Setting, enter URL of the external login page and then click Apply. After applying the setting, the new login success page can be previewed by clicking Preview button at the bottom of this page.

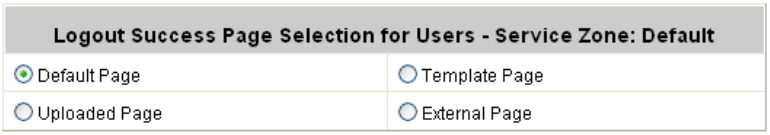


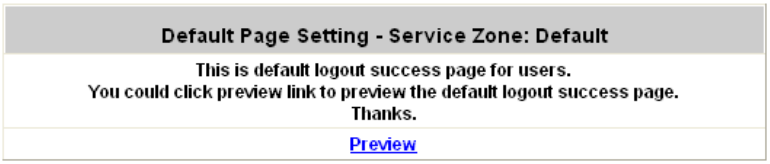
2.2.5) Custom Pages — **Logout Success Page**

The administrator can apply their own Logout Success page for Users in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

- *Custom Pages — Logout Success Page —* ***Default Page***

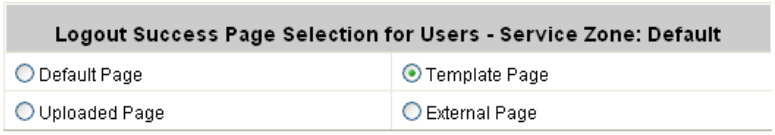
  Choose ***Default Page*** to use the default logout success page.

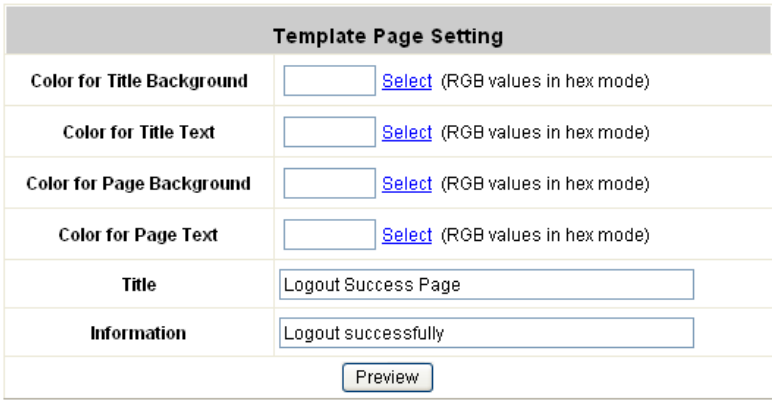




- *Custom Pages — Logout Success Page —* ***Template Page***

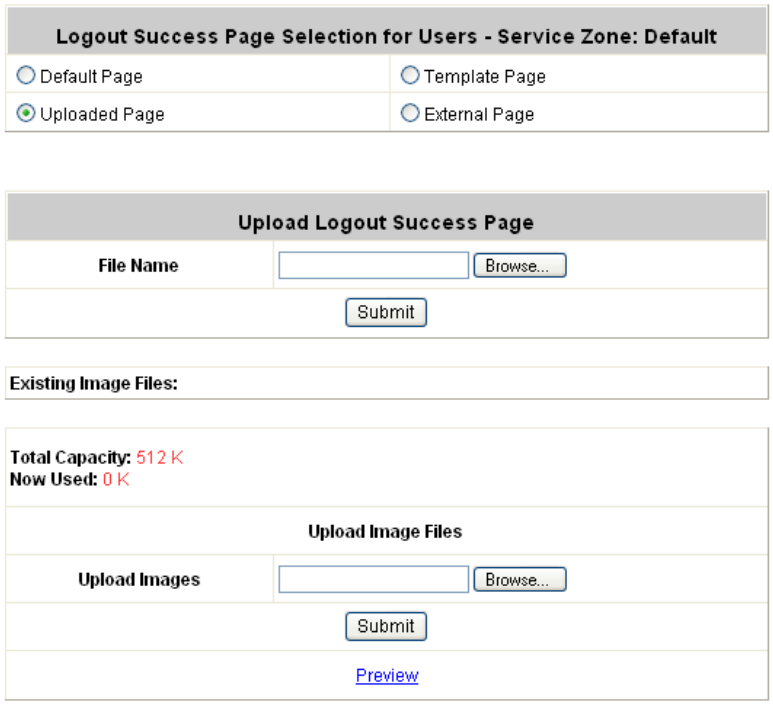
  Choose Template Page to make a customized logout success page. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.





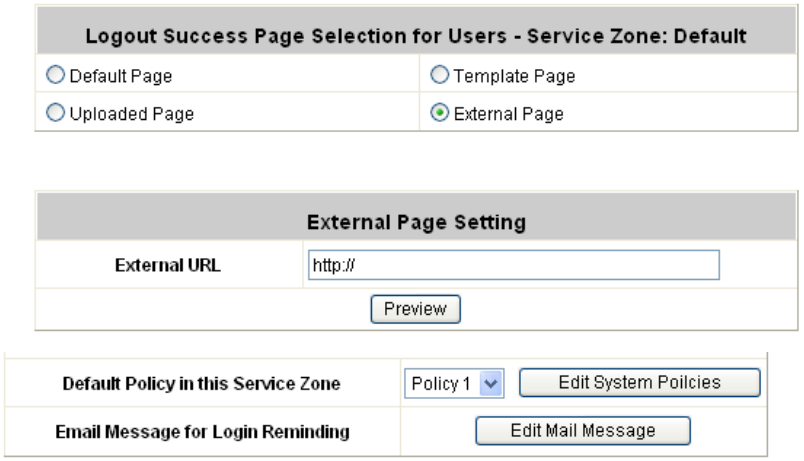
- *Custom Pages — Logout Success Page —* ***Uploaded Page***

  Choose Uploaded Page and get the logout success page to upload. Click the ***Browse*** button to select the file for the logout success page upload. Then click ***Submit*** to complete the upload process. After the upload process is completed and applied, the new logout success page can be previewed by clicking ***Preview*** button at the bottom.

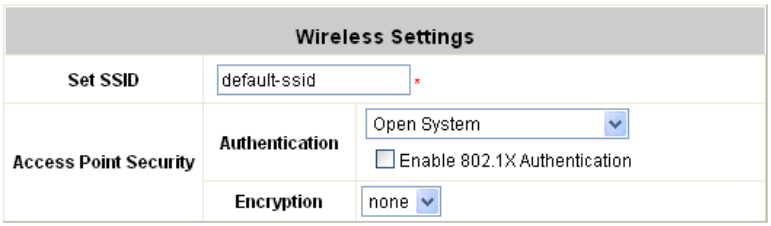


- *Custom Pages —Logout Success Page —**External Page***

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



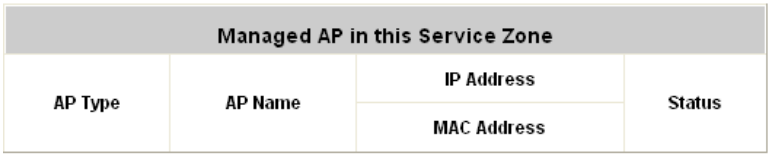
3) Service Zone Settings —Wireless Settings



- **Set SSID:** Each service zone must setup its own SSID.
- **Access Point Security:** Each service zone can setup its own **Authentication** and **Encryption** support. Authentication support: WPA-PSK, IEEE 802.1X (EAP-MD5, EAP-TLS, CHAP, PEAP); and encryption support: WEP (64/128bit), WPA and WPA2.

4) Service Zone Settings —Managed AP in the service Zone

- **Managed AP in this Service Zone:** List all APs belonging to this service zone.

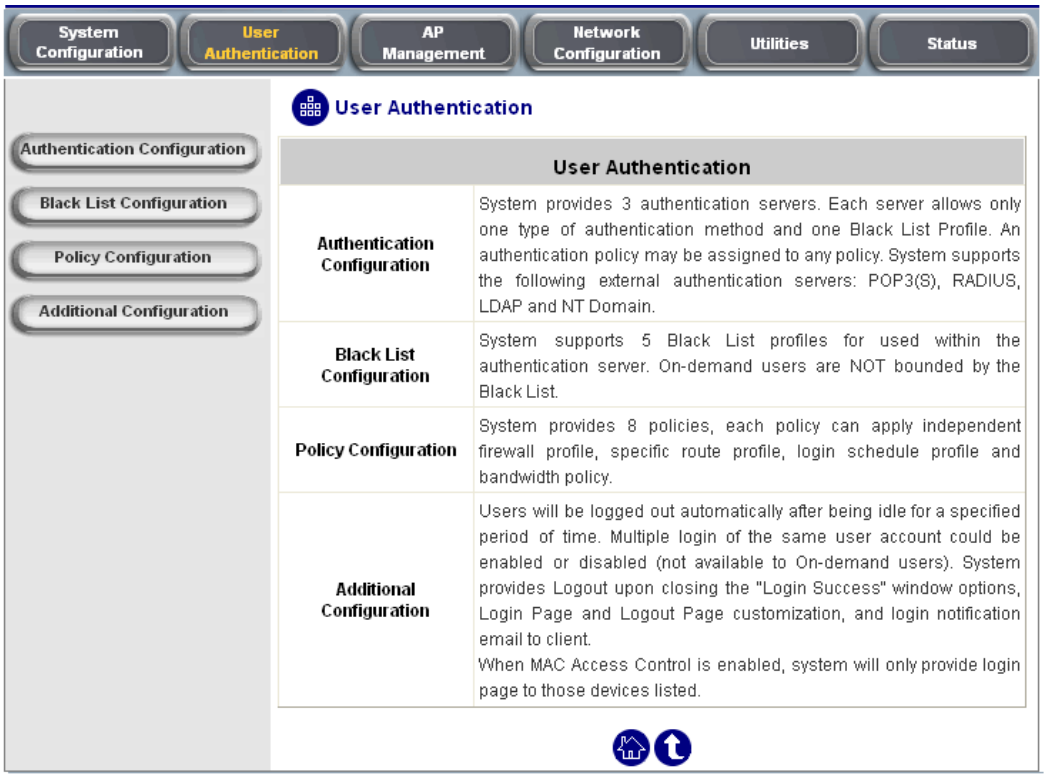


Note: Limitation on WAP-0005 AP (AP Type: LevelOne_Adv-AP) deployment

Because Default Service Zone (system default name: Default) does not support VLAN Tag, network administrators must pay attention to the limitation when deploying WAP-0005 AP. WAP-0005 supports two modes: (1) ***Non-VLAN*** *mode – in this mode, WAP-0005 can only be associated with the Default Service Zone (system default name: Default) or (2)* ***VLAN*** *mode – in this mode, WAP-0005 can only be associated with other Service Zones (system default names: SZ1, SZ2, SZ3, or SZ4).*

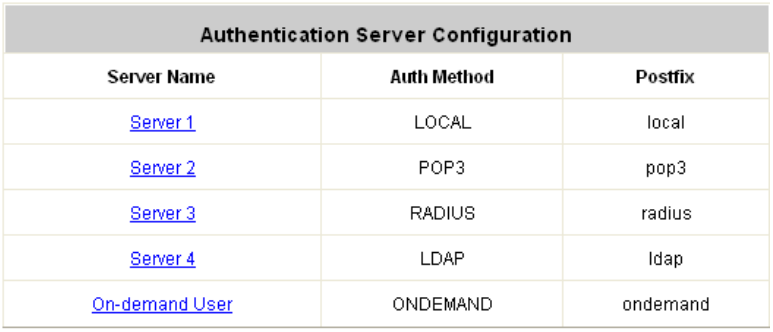
4.2 User Authentication

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



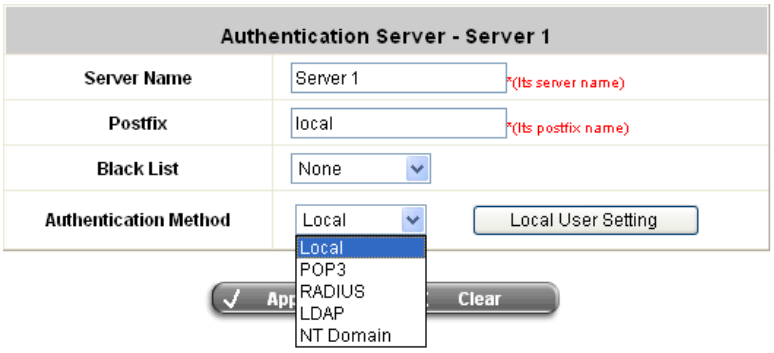
4.2.1 Authentication Configuration

This section is for administrator to pre-configure authentication servers for the entire system's Service Zones. For a particular Service Zone, administrator should enable all the authentication servers which will be used and also specify a default authentication server in the page of Service Zones Settings. Up to four servers which can be selected and pre-configured here from the authentication databases (Local database, POP3, RADIUS, LDAP, and NT Domain Server) and one default server for on-demand users can also be pre-configured here for setting up Service Zones later. (for the Service Zone Authentication Settings, please see **4.1.7 Service Zones**)



Authentication Server Configuration		
Server Name	**Auth Method**	**Postfix**
Server 1	LOCAL	local
Server 2	POP3	pop3
Server 3	RADIUS	radius
Server 4	LDAP	ldap
On-demand User	ONDEMAND	ondemand

- **Server 1~4:** There are 5 kinds of authentication methods/databases (Local, POP3, RADIUS, LDAP and NT Domain) to choose from.



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.

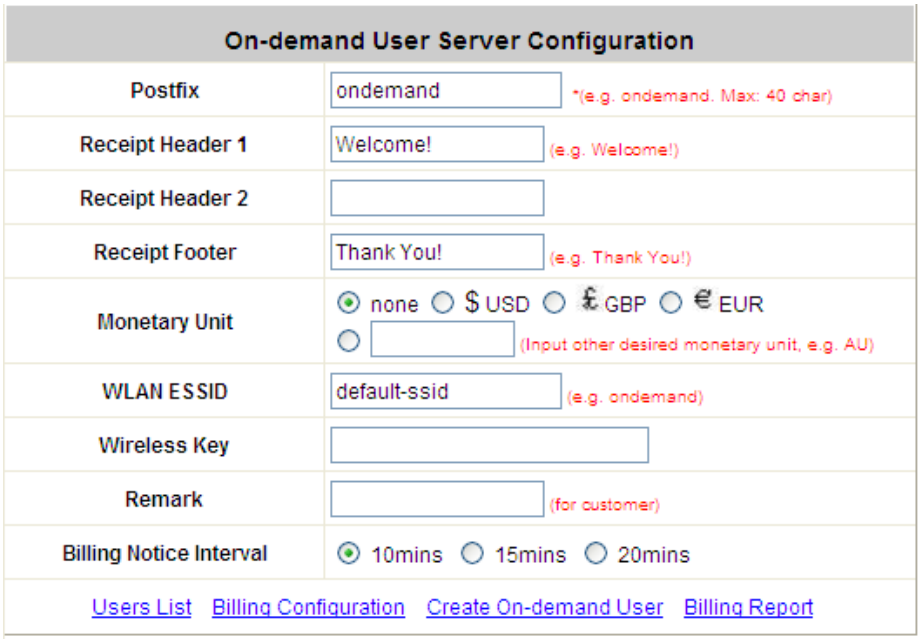
Postfix: Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

Black List: There are 5 sets of black lists. You can select one of them or choose **"None"**. Please refer to **4.2.2 Black List Configuration** for more information.

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

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

- **On-demand User:** This is the default authentication server for on-demand or guest users.



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 your own receipt header message or use the default.

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

Monetary Unit: Select or enter the desired monetary unit for your region.

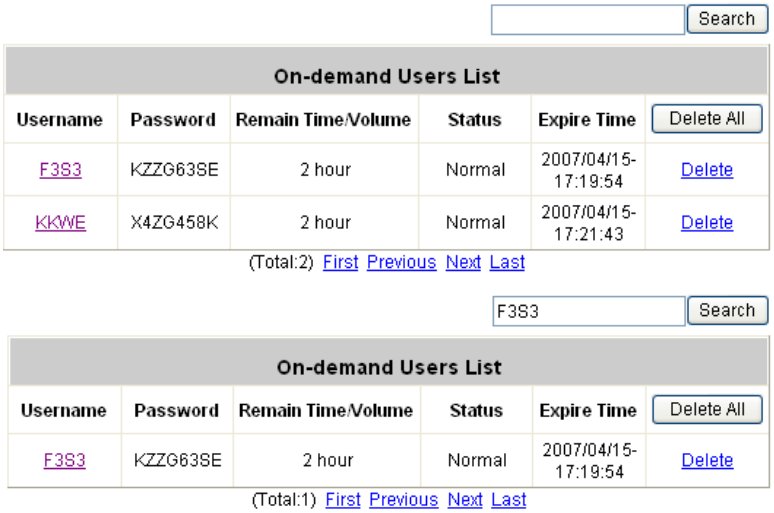
WLAN ESSID: Enter the ESSID of the AP.

Wireless Key: Enter the WEP key of the AP.

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

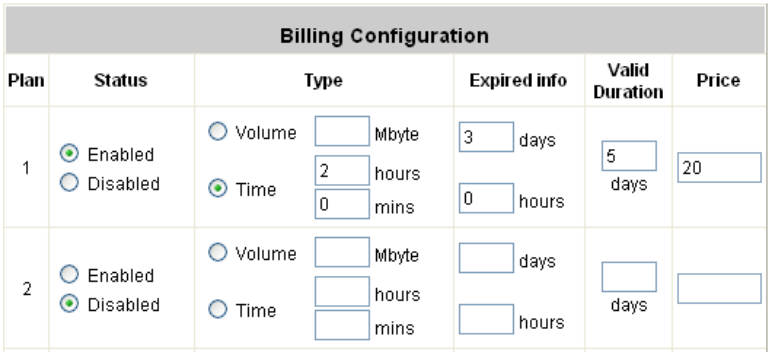
Billing Notice Interval: While a volume type on-demand user is still logged in, the system will update the billing notice of the login successful page by the time interval defined here.

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



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

Billing Configuration: Click the hyperlink of **Billing Configuration** to enter the **Billing Configuration** page. In the **Billing Configuration** page, the administrator may configure up to 10 billing plans.



Billing Configuration

Plan	Status	Type	Expired info	Valid Duration	Price
1	Enabled / Disabled	Volume: Mbyte; Time: 2 hours 0 mins	3 days 0 hours	5 days	20
2	Enabled / Disabled	Volume: Mbyte; Time: hours mins	days hours	days	

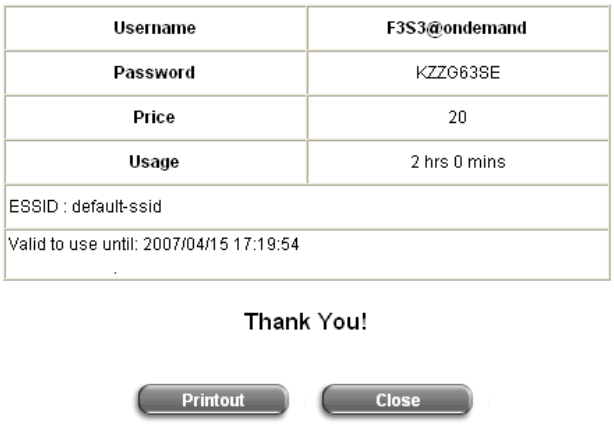
- **Status:** Select to enable or disable this billing plan.
- **Type:** Set the billing plan by **"Volume"** (the maximum volume allowed is 9999999 Mbyte) or **"Time"** (the maximum time allowed is 999 hours and 59 minutes).
- **Expired Info:** This is the duration of time that the user needs to activate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

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

Pressing the ***Create*** button for the desired rule, an On-demand user will be created, then click ***Printout*** to print a receipt which will contain this on-demand user's information. There are 500 On-demand user accounts available.



Username	F3S3@ondemand
Password	KZZG63SE
Price	20
Usage	2 hrs 0 mins
ESSID : default-ssid	
Valid to use until: 2007/04/15 17:19:54	

Thank You!

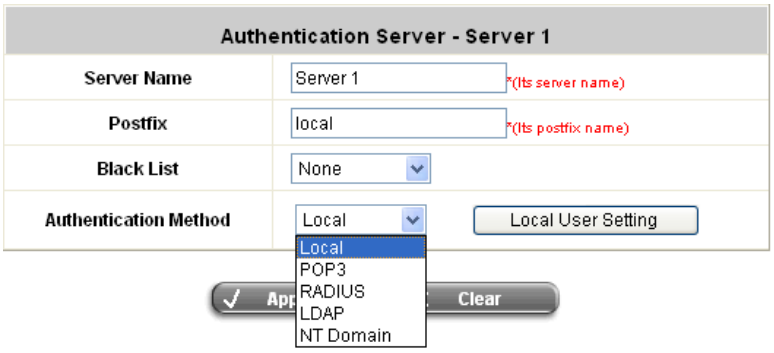
Printout Close

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

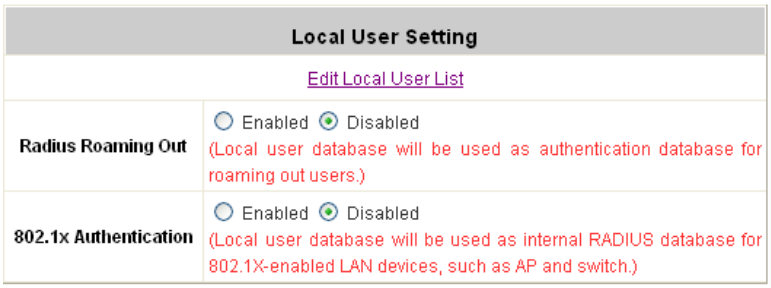
- **Report All:** Click this to get a complete report including all the on-demand records. This report shows the total expenses and individual accounting of each plan for all plans available.
- **Search:** Select a time period to get a period report. The report tells the total expenses and individual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

- **Authentication Method – Local User Setting**

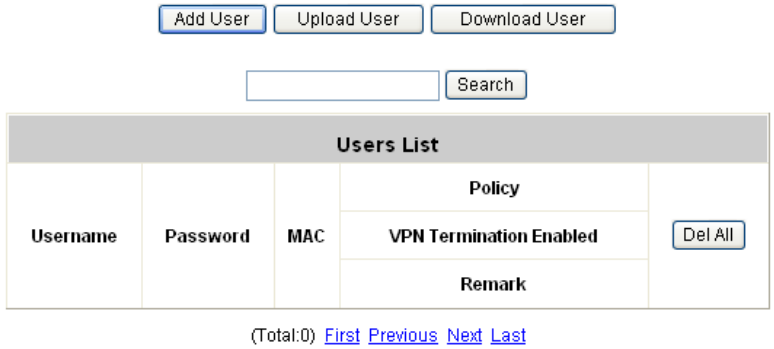
  Choose **"Local User"** in the **Authentication Method** field, the hyperlink besides the pull-down menu will become **"Local User Setting"**.



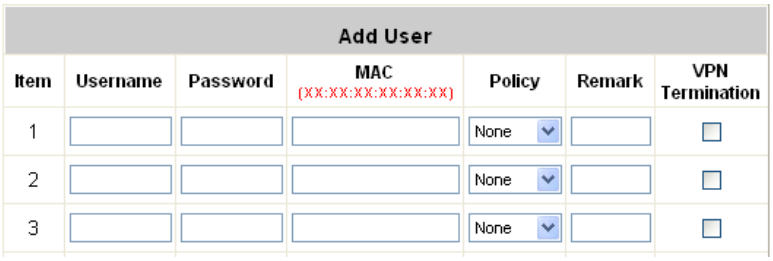
Click the hyperlink to get in for further configuration.



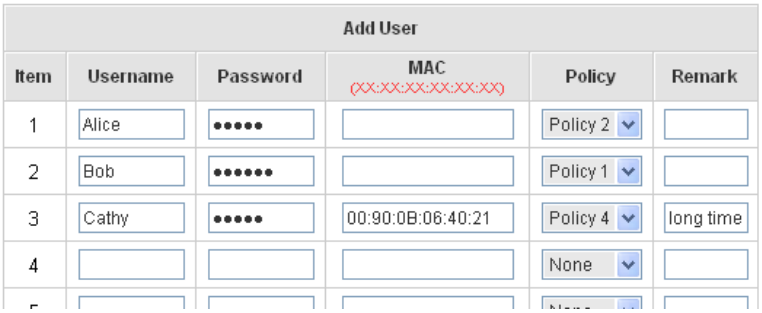
Edit Local User List: Click this to enter the **"Local User List"** screen.



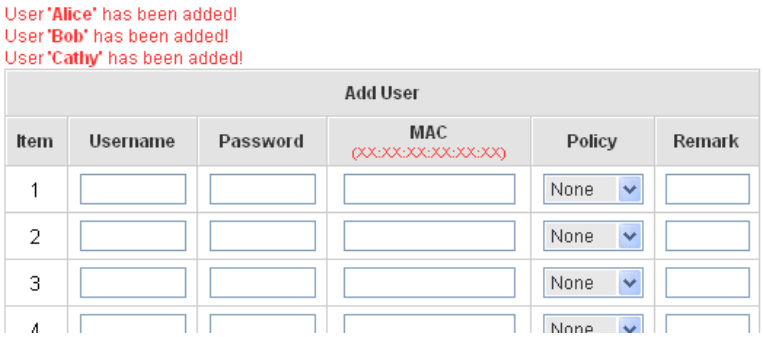
Add User: Click ***Add User*** to enter the **Add User** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC"** (optional) and **"Remark"** (optional). Notice that username cannot start with "guest" if guest user is enabled. Then, select a desired **Policy** and click ***Apply*** to complete adding the user or users.



Add some users:



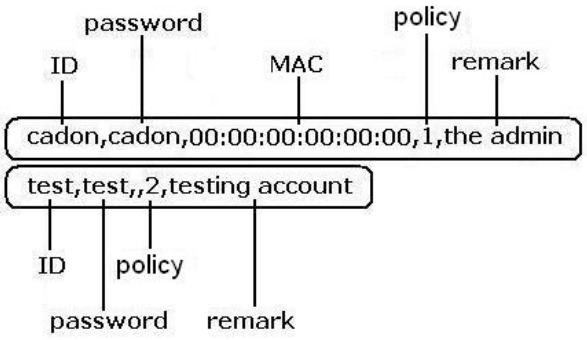
Click "Apply" to save the settings.



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.

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. The Group field indicates policy number to use. When adding user

accounts by uploading a file, the existing accounts in the embedded database will not be replaced by new ones.



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

Users List			
Username	Password	MAC	Policy Remark
Alice	alice		2
Bob	123bbb		1
Cathy	41380	00:90:0B:06:40:21	4 long time

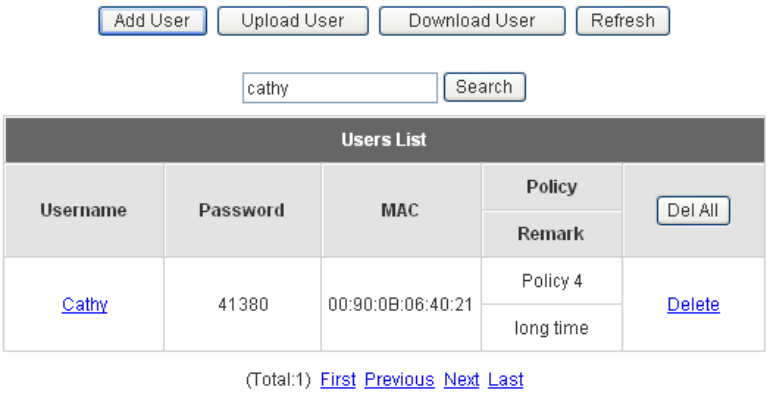
Download

Refresh: Click this to renew the user list.

Users List				
Username	Password	MAC	Policy Remark	Del All
Alice	alice		Policy 2	Delete
Bob	123bbb		Policy 1	Delete
Cathy	41380	00:90:0B:06:40:21	Policy 4 long time	Delete
Allen	apple		Policy 1 night shift	Delete

(Total:4) First Previous Next Last

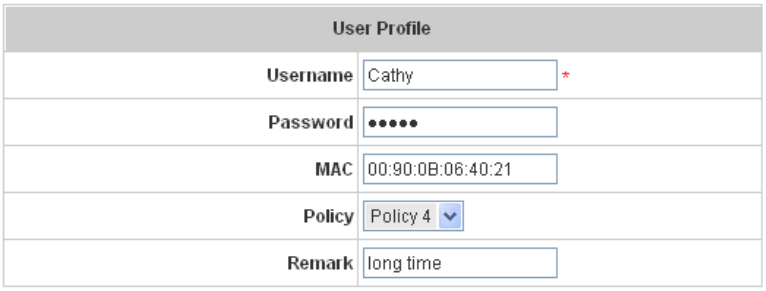
Search: Enter a keyword of a username that you wish to search in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.



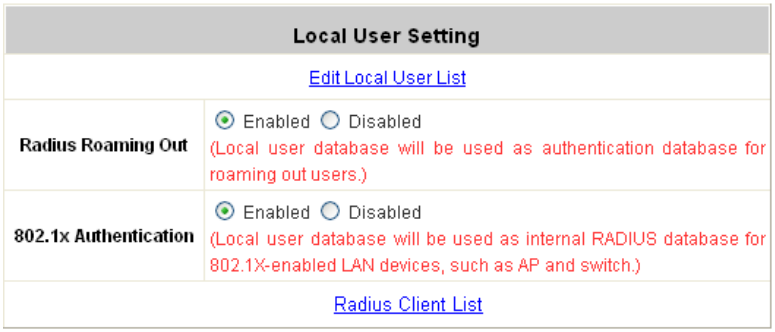
Del All: This will delete all the users at once.

Delete: This will delete the users individually.

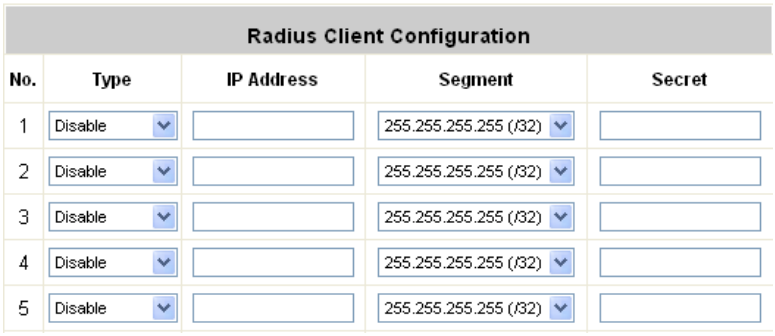
Edit User: If you want to edit the content of individual user account, click the username of the desired user account to enter the **Edit User** Interface for that particular user, and then modify or add any desired information such as **"Username"**, **"Password"**, **"MAC"** and **"Remark"** (optional).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



Radius Roaming Out / 802.1x Authentication: Enable the two function separately and the hyperlink of ***Radius Client List***.



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

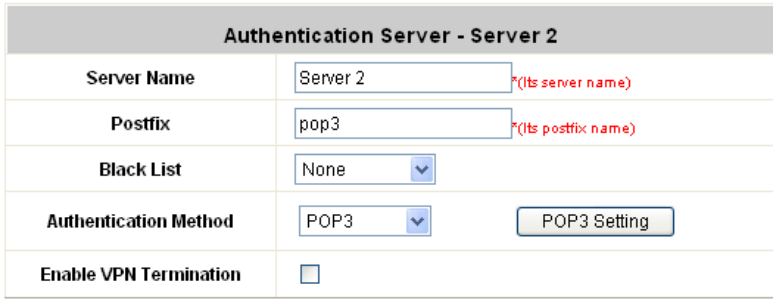


Roaming Out: This is the Radius Roaming Out function that our company cooperates with III (Institute for Information Industry). When you select **"Roaming Out"**, the local user can login from other site.

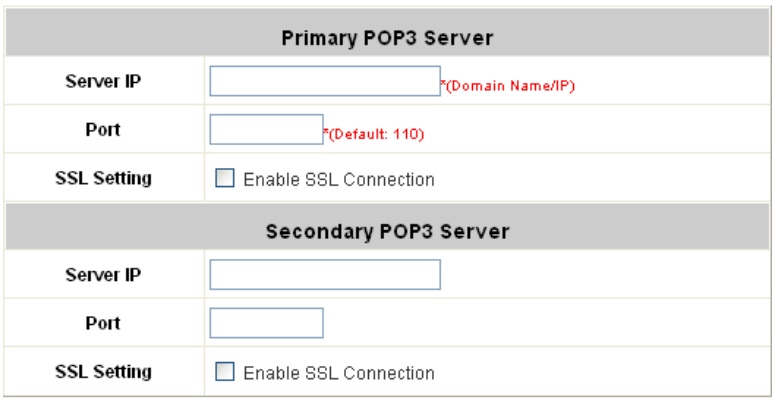
802.1x: This system support **PEAP** (**P**rotracted **E**xtensible **A**uthentication **P**rotocol) function. When selecting 802.1x, the system is provided with this function. 802.1x function must be used in LAN.

- **Authentication Method – POP3**

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



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.



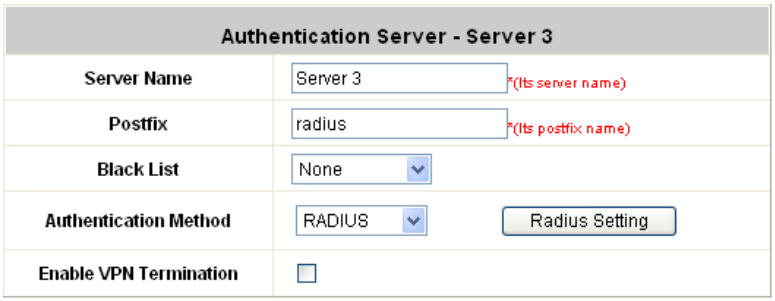
Server IP: Enter the IP address/domain name given by your ISP.

Port: Enter the Port given by your ISP. The default value is 110.

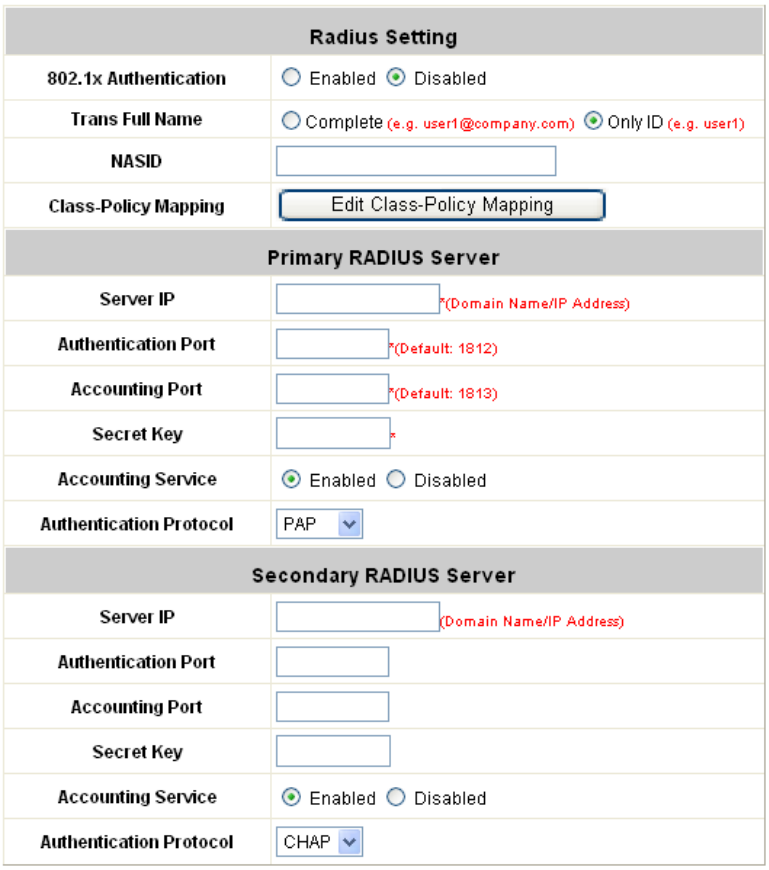
SSL Connection: If this option is enabled, the POP3s protocol will be used to encrypt the authentication.

- **Authentication Method – RADIUS**

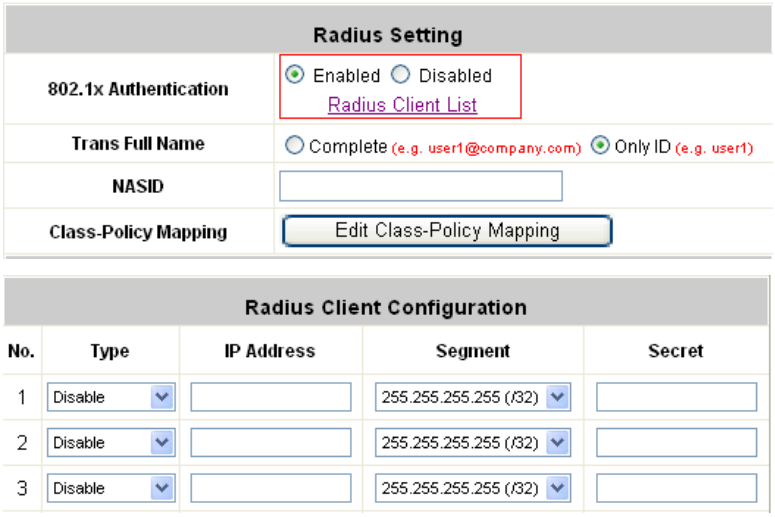
  Choose **"RADIUS"** in the **Authentication Method** field, the hyperlink beside the pull-down menu will become **"Radius Setting"** and there is a hyperlink of **"Edit Policy Mapping"** shows beside Policy.



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.



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. AMG-2000 will forward the authentication request from these clients to the configured Radius Servers.



Trans Full Name: When enabled, the ID and postfix will be sent to the RADIUS server for authentication. When disabled, only the ID will be sent to RADIUS server for authentication.

NASID: Enter a line of characters, for example "meeting-room", for identifying AMG-2000 itself to the RADIUS server. Please use numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.), and all other letters are not allowed.

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.

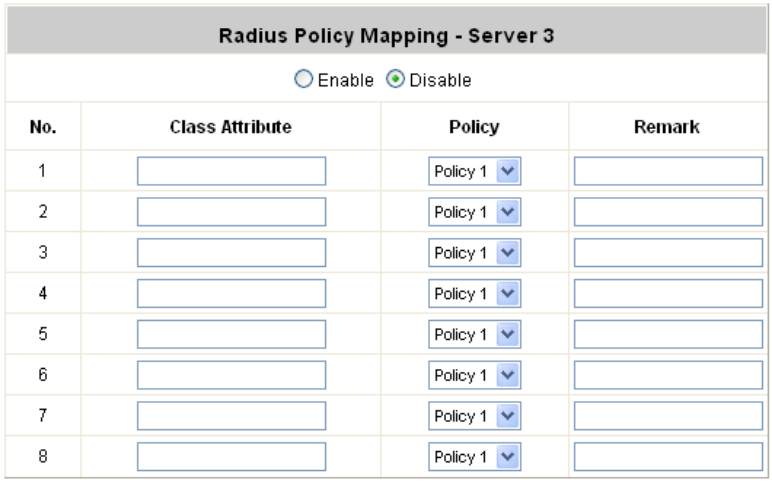
Accounting Port: Enter the accounting port of the RADIUS server and the default value is 1813.

Secret Key: Enter the key for encryption and decryption.

Accounting Service: Select this to enable or disable the **"Accounting Service"** for accounting capabilities.

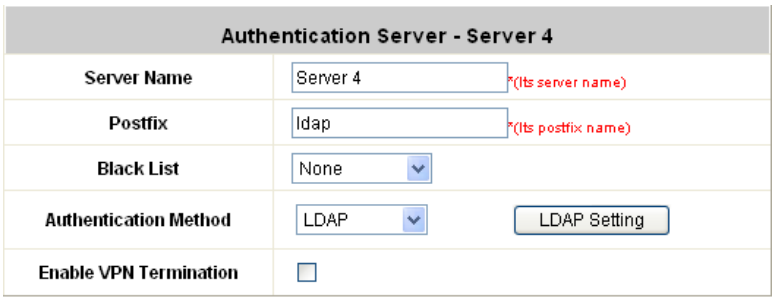
Authentication Protocol: There are two methods, CHAP and PAP for selection.

Click the hyperlink of **Edit Policy Mapping** for further configuration. In Class Attribute filed, enter the class attribute according to the setting of Radius server and assign a policy. The class attribute could be a character string using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.), all other letters are not allowed. These settings will become effective immediately after clicking the ***Apply*** button.

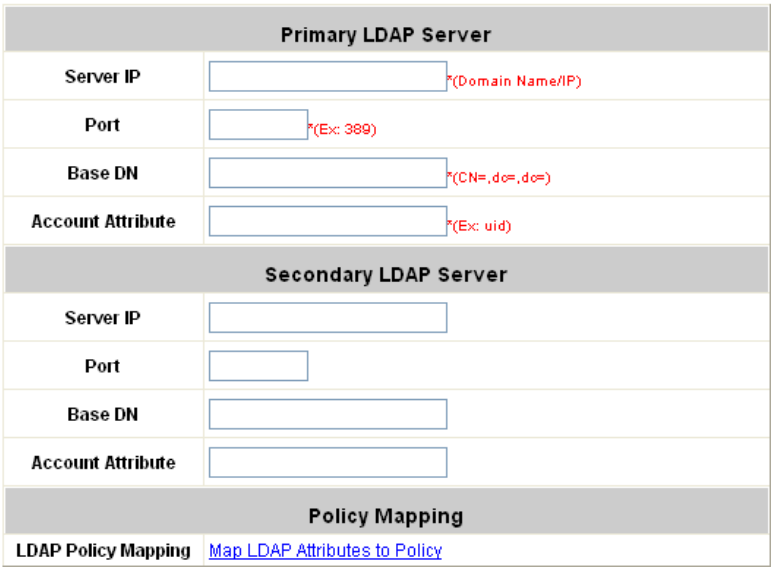


- **Authentication Method – LDAP**

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



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.



Server IP: Enter the IP address or domain name of the LDAP server.

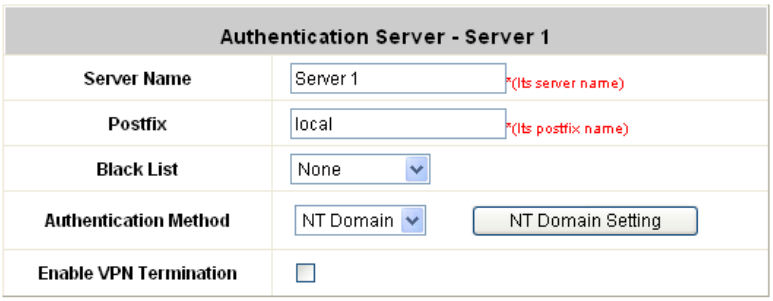
Port: Enter the Port of the LDAP server, and the default value is 389.

Base DN: Enter the distinguished name of the LDAP server.

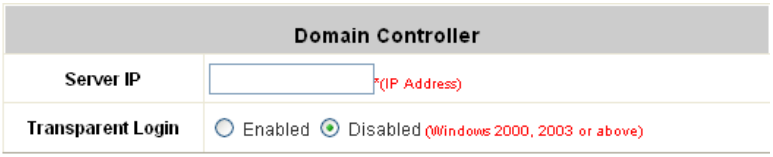
Account Attribute: Enter the account attribute of the LDAP server.

- **Authentication Method – NT Domain**

  Choose **"NTDomain"** in the **Authentication Method** field, the hyperlink beside the pull-down menu will become **"NT Domain Setting"**.



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.

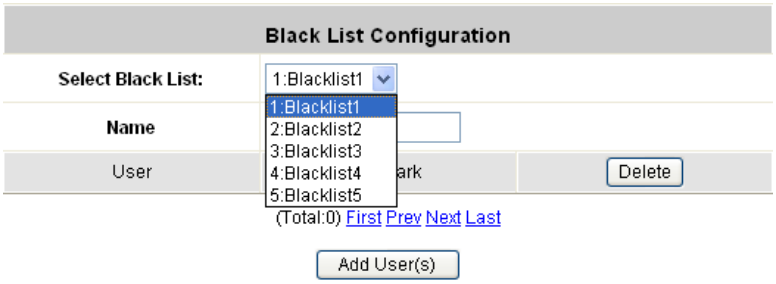


Server IP address: Enter the server IP address of the domain controller.

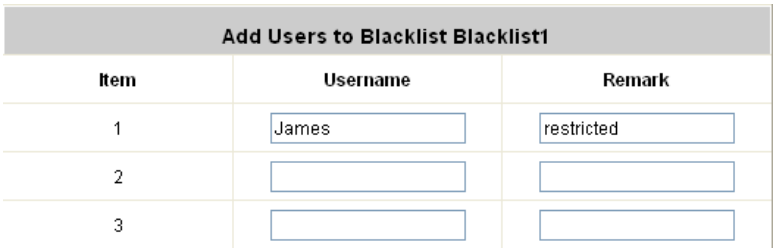
Transparent Login: If the function is enabled, when users log into the Windows domain, they will log into AMG-2000 automatically.

4.2.2 Black List Configuration

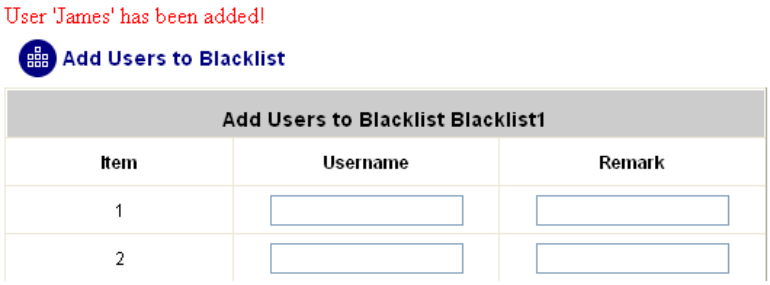
The administrator can add, delete, or edit the black list for user access control. Each black list can include 40 users at most. If a user in the black list wants to log into the system, the user's access will be denied. The administrator can use the pull-down menu to select the desired black list.



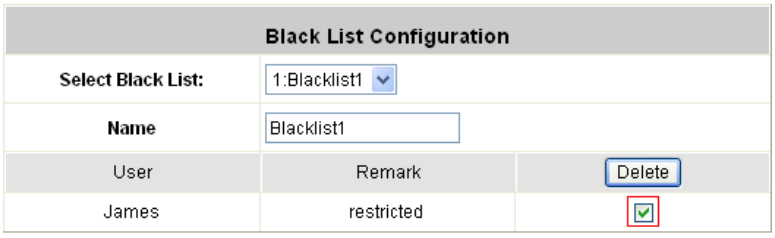
- **Select Black List:** There are 5 lists to select from for the desired black list.
- **Name:** Set the black list name and it will show on the pull-down menu above.
- **Add Users:** Click the hyperlink to add users to the selected black list.



After entering the usernames in the **"Username"** blanks and the related information in the **"Remark"** blank (not required), click ***Apply*** to add the users.



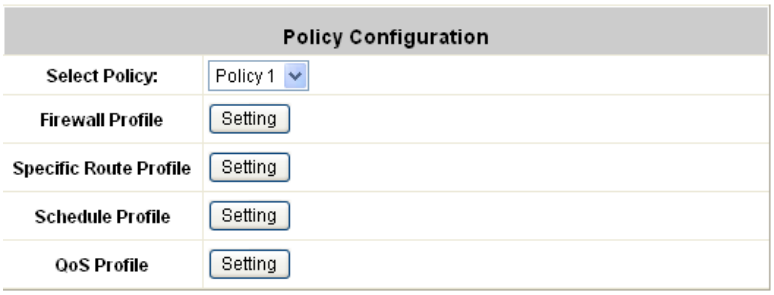
If the administrator wants to remove a user from the black list, just select the user's **"Delete"** check box and then click the ***Delete*** button to remove that user from the black list.



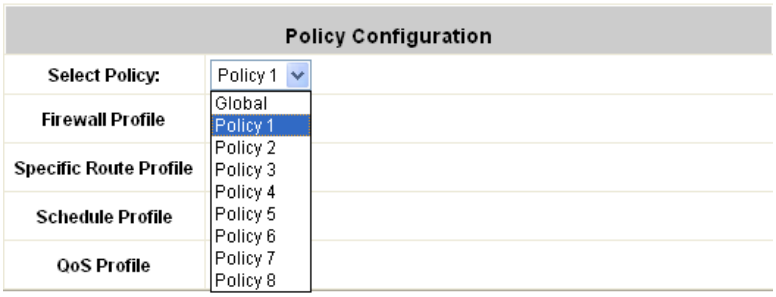
4.2.3 Policy Configuration

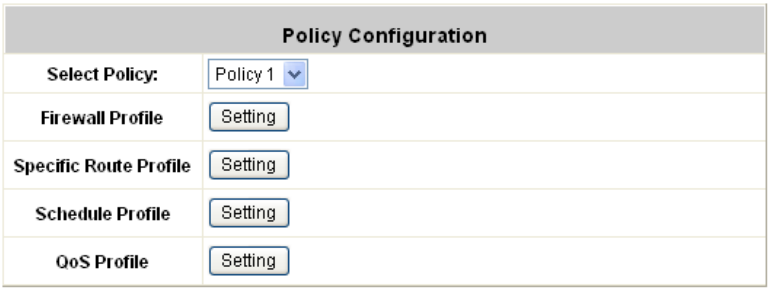
There are 8 policies and one Global Policy in Policy Configuration. Except Global Policy, every Policy has three profiles, **Firewall Profile**, **Specific Route Profile**, and **Schedule Profile** as well as **Total Bandwidth**, **Individual Maximum Bandwidth** and **Individual Request Bandwidth** setting for that policy.

- **Policy 1~8**



➢ **Select Policy:** Select **Policy 1 ~ Policy 8**.





➢ **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.

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

Policy 1 - Firewall Rules

No.	Active	Action	Name	Source / Destination	IPSec Encrypted	Service	Schedule
1	☐	Block		ANY / ANY		ALL	Always
2	☐	Block		ANY / ANY		ALL	Always

Policy 1 - Edit Filter Rule

Rule Item: 1		Rule Name:	
Source		Destination	
Interface	ALL	Interface	ALL
IP Address		IP Address	
Subnet Mask	255.255.255.255 (/32)	Subnet Mask	255.255.255.255 (/32)
MACAddress			
IPSec Traffic	☐	IPSec Traffic	☐
Service	ALL		
Schedule	◉ Always ○ Recurring ○ One Time		
Action	◉ Block ○ Pass		

Rule Item: This is the rule that you have selected.

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

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

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

Source/Destination — Interface: There are four interfaces to choose, **WAN1**, **WAN2**, **LAN1~LAN4 Port** and **Private Port**.

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

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

- **Specific Route Profile**

Click the hyperlink of ***Setting*** for **Specific Route Profile**, the Specific Route Profile list will appear.

Policy 1 - Specific Default Route

Enable ☐ Default Gateway: IP Address

Policy 1 - Specific Route Profile

Route Item	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1		255.255.255.255 (/32)	
2		255.255.255.255 (/32)	

Profile Name: The profile name can be changed here.

Default Gateway: Choose an appropriate default gateway from the drop-down menu, or enter IP address manually into the blank. Check the "Enable" box to enable this function.

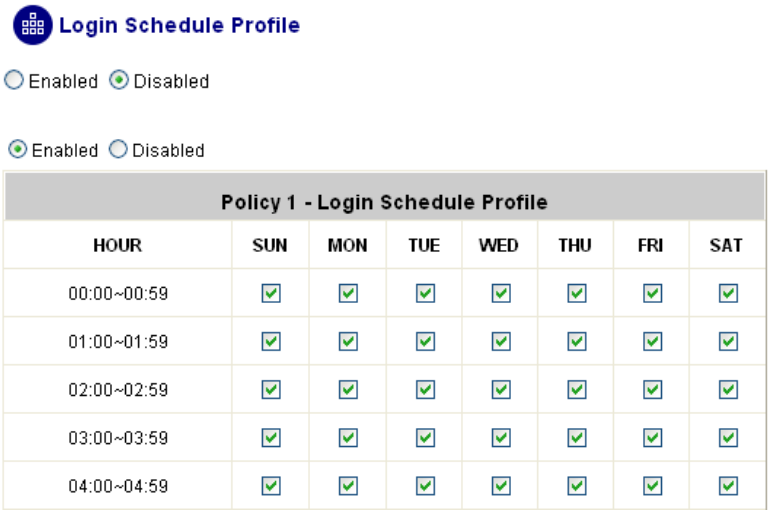
IP Address: The destination IP address of the host or the network.

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.

- **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.



Policy 1 - Login Schedule Profile							
HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
00:00~00:59	☑	☑	☑	☑	☑	☑	☑
01:00~01:59	☑	☑	☑	☑	☑	☑	☑
02:00~02:59	☑	☑	☑	☑	☑	☑	☑
03:00~03:59	☑	☑	☑	☑	☑	☑	☑
04:00~04:59	☑	☑	☑	☑	☑	☑	☑

- **QoS Profile**

Click the button of ***Setting*** for **QoS Profile** to enter the Traffic Configuration. Choose one **Traffic Class** for that particular policy.

Policy 1 - Traffic Configuration	
Traffic Class	Best Effort
Total Downlink	Unlimited
Individual Maximum Downlink	Unlimited
Individual Request Downlink	None
Total Uplink	Unlimited
Individual Maximum Uplink	Unlimited
Individual Request Uplink	None

Traffic Class: Define allowed class and choose among **Voice**, **Video**, **Best Effort** and **Background**.

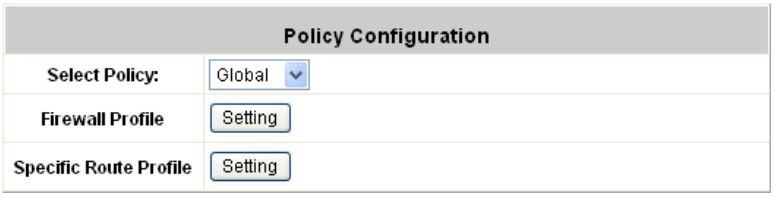
Total Downlink/Uplink: Define maximum downlink and uplink allowed of the total bandwidth shared by users within the same policy.

Individual Maximum Downlink/Uplink: Define maximum downlink and uplink allowed for individual user; the individual maximum bandwidth can not exceed the value of total downlink / uplink.

Individual Request Downlink/Uplink: Define the guaranteed minimum downlink and uplink for individual user; the minimum bandwidth can not exceed the setting value of total downlink and uplink and

individual maximum downlink/uplink.

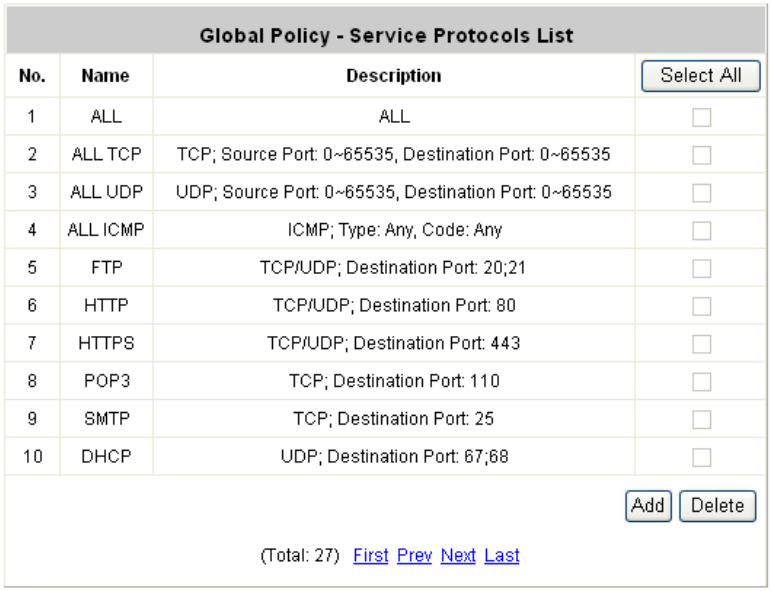
- **Global Policy**
  - **Select Policy:** Select **Global** to set the **Firewall Profile** and **Specific Route Profile**.



Policy Configuration	
Select Policy:	Global
Firewall Profile	Setting
Specific Route Profile	Setting

  - **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.

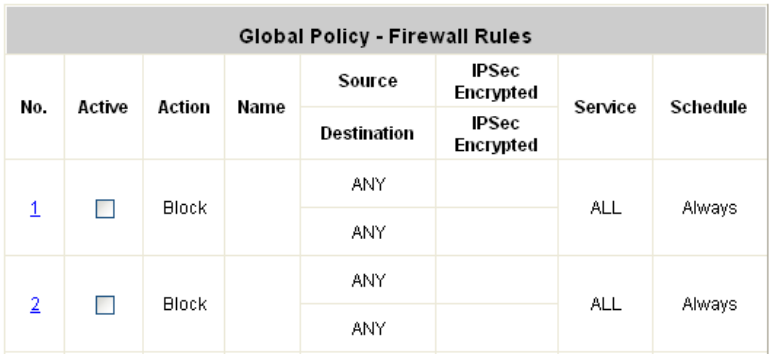
Global Policy - Firewall Configuration
Predefined and Custom Service Protocols
Firewall Rules



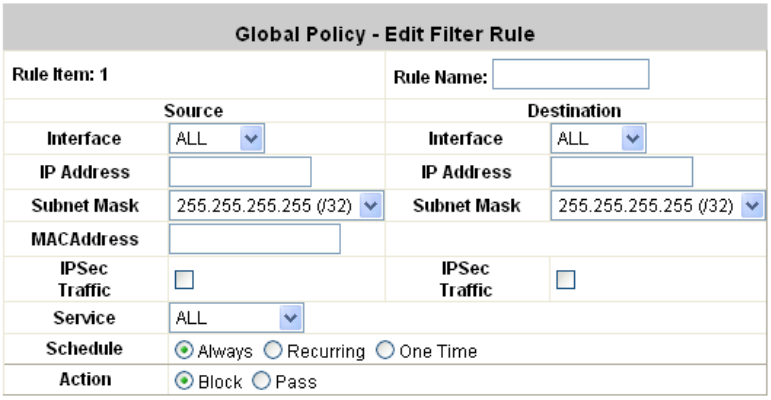
Global Policy - Service Protocols List			
No.	Name	Description	Select All
1	ALL	ALL	
2	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	
3	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	
4	ALL ICMP	ICMP; Type: Any, Code: Any	
5	FTP	TCP/UDP; Destination Port: 20;21	
6	HTTP	TCP/UDP; Destination Port: 80	
7	HTTPS	TCP/UDP; Destination Port: 443	
8	POP3	TCP; Destination Port: 110	
9	SMTP	TCP; Destination Port: 25	
10	DHCP	UDP; Destination Port: 67;68	

Add Delete

(Total: 27) First Prev Next Last



Global Policy - Firewall Rules							
No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1		Block		ANY		ALL	Always
				ANY			
2		Block		ANY		ALL	Always
				ANY			



Rule Item: This is the rule that you have selected.

Rule Name: The rule name can be changed here.

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

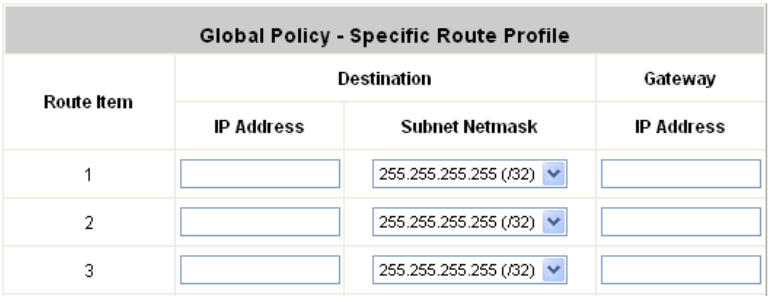
Source —MAC Address: The MAC address of the source IP address. This is for specific MAC address filter.

Source/Destination —Interface: There are four interfaces to choose, **WAN1**, **WAN2**, **LAN1** and **LAN2**.

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

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

- **Specific Route Profile:** Click the hyperlink of ***Setting*** for **Specific Route Profile**, the Specific Route Profile list will appear.

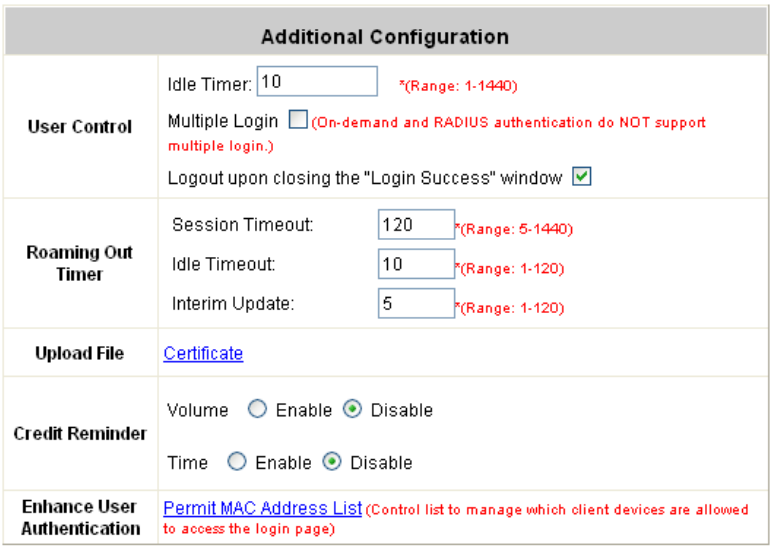


IP Address (Destination): The destination IP address of the host or the network.

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

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

4.2.4 Additional Configuration



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

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

  Multiple Login: When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users and RADIUS accounting.)

  Logout upon closing the login Success window: When a user logs into the network, a small window will appear to show the user's information and there is a logout button for the logout. If enabled. When the users try to close the small window, there will be a new popup window to confirm the logout in case the users click the logout button by accident.

- **Roaming Out Timer**

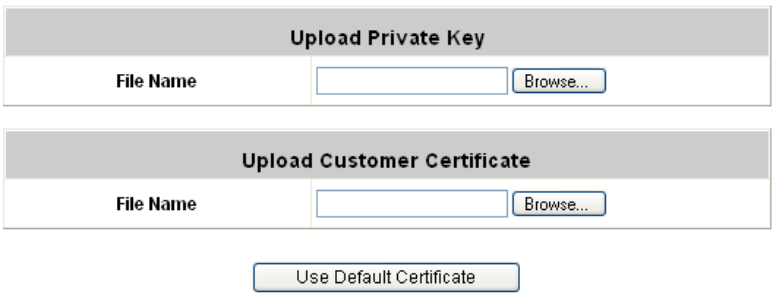
  Session Timeout: The time that the user can access the network while roaming. When the time is up, the user will be kicked out automatically.

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

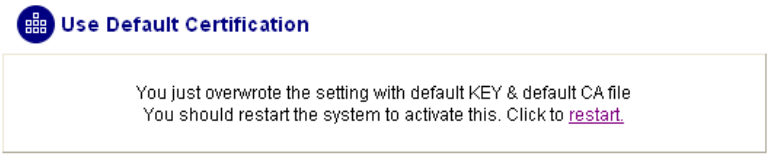
  Interim Update: The system will update the users' current status and usage according to this periodically.

- **Upload File**

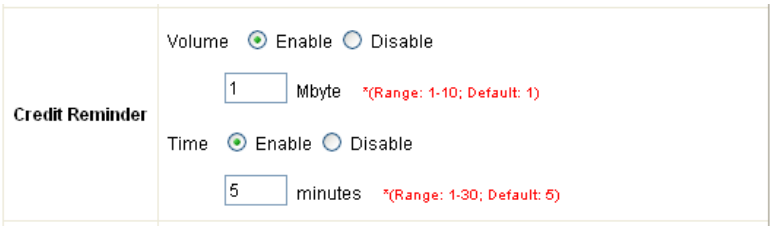
  1. **Certificate:** The administrator can upload new private key and customer certificate. Click the ***Browse*** button to select the file for the certificate upload. Then click ***Submit*** to complete the upload process.



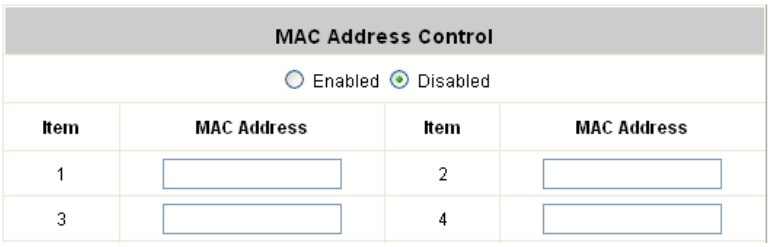
Click ***Use Default Certificate*** to use the default certificate and key.



- **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.



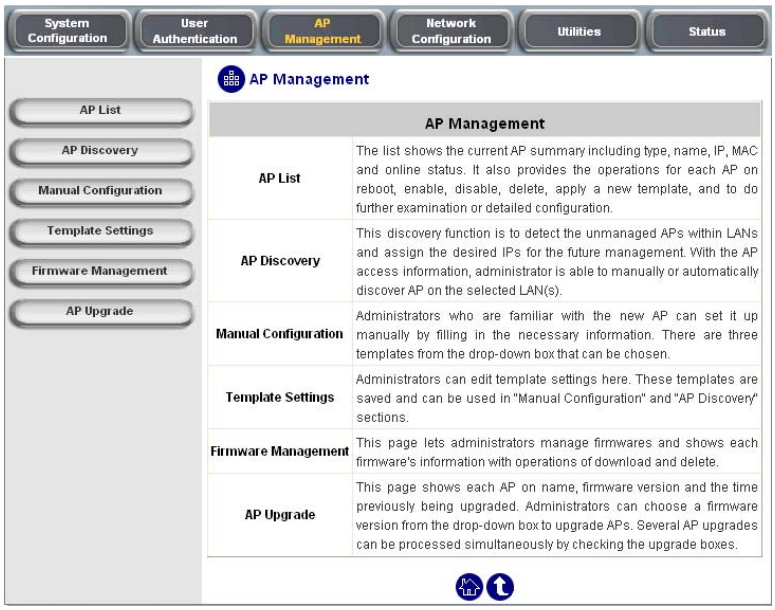
- **MAC Address Control:** With this function, only the users with their MAC addresses in this list can log into AMG-2000. There will only be 40 users allowed in this MAC address list. User authentication is still required for these users. Please enter the **MAC Address List** to fill in these MAC addresses, select **Enable**, and then click ***Apply***.



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

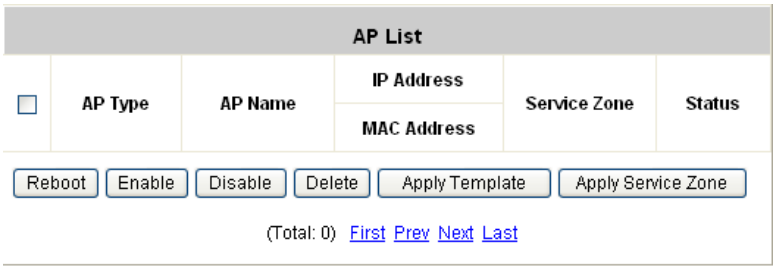
4.3 AP Management

AMG-2000 supports to manage up to 12 access points (AP), and they can be configured in this section. This section includes the following functions: **AP List**, **AP Discovery**, **Manual Configuration**, **Template Settings**, **Firmware Management** and **AP Upgrade**.

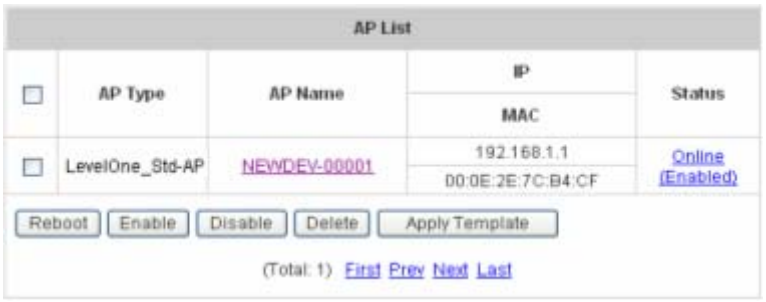


4.3.1 AP List

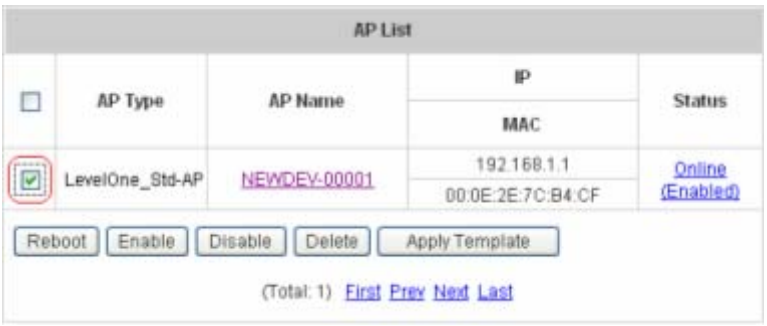
All of the AP under the management of AMG-2000 will be shown in the list. The AP can be edited by clicking the hyperlink of ***AP Name*** and the AP status can be got by clicking the hyperlink of ***Status***.



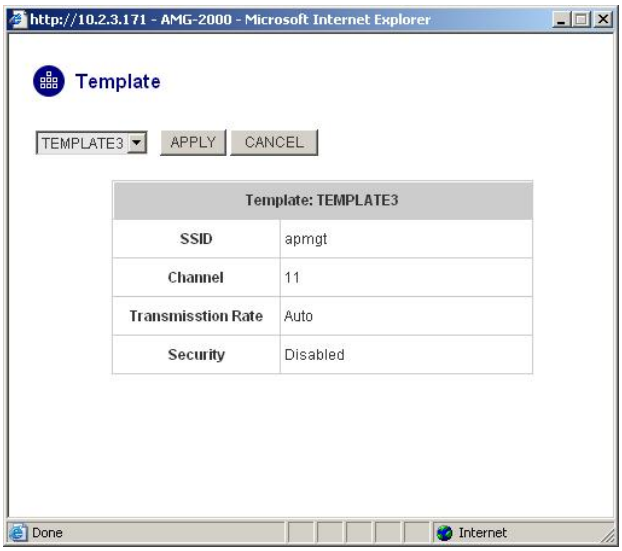
After adding 1 AP:



You can check any AP and then click the button below to **Reboot**, **Enable**, **Disable** and **Delete** the checked AP.



Click **Apply Template** to select one template to apply to the AP.



- **AP Name**

  Click ***AP Name*** and enter the interface about related settings. There four kinds of settings, **General Settings**, **LAN Interface Setting**, **Wireless Interface Setting** and **Access Control Setting**. Click the hyperlink to go on the configuration.

General Settings		
Setting	Name	NEWDEV-00001
	Remark	None
	Firmware	1.20

LAN Interface Setting		
LAN	IP	192.168.2.2
	Mode	Static IP

Wireless Interface Setting		
Wireless LAN	SSID	apmgt
	Channel	11
	Security Type	Disabled

Access Control Setting		
Access Control	Status	Disabled
	Mode	Allowed
	Number of MAC Addresses	0

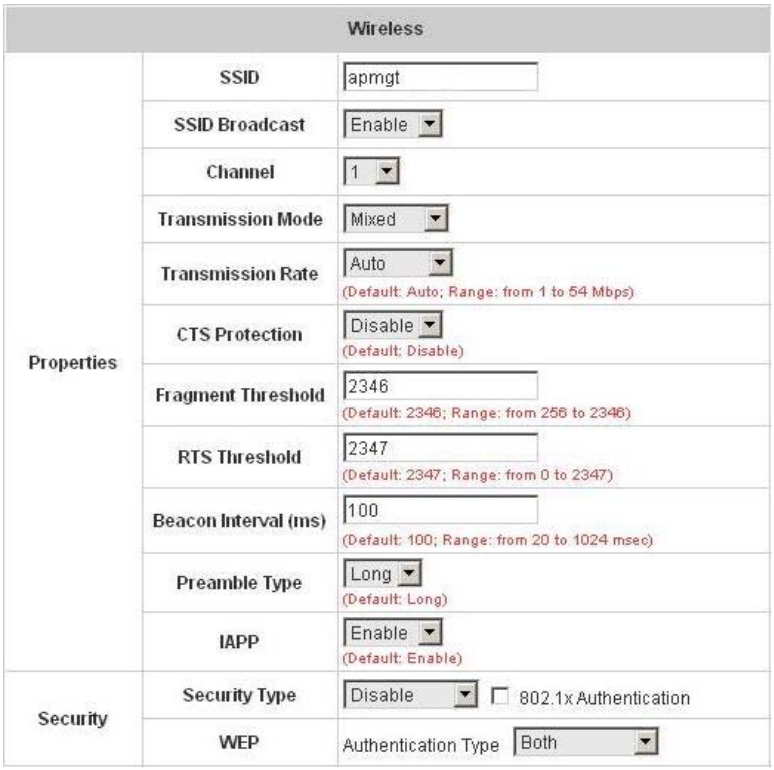
  - **General Setting:** Click ***Setting*** to enter the **General Setting** interface. You can revise the AP **Name**, **Admin Password** and **Remark**. Besides, you can see the firmware information here.

General Settings	
Name	NEWDEV-00001
Admin Password	1234
Remark	
Firmware	1.23

  - **LAN Setting:** Click ***LAN*** to enter the **LAN Setting** interface. Input the data of LAN including **IP address**, **Subnet Mask** and **Default Gateway** of AP.

LAN Settings	
IP Address	192.168.2.2 *
Subnet Mask	255.255.255.0 *
Default Gateway	0.0.0.0 *

- **Wireless LAN:** Click ***Wireless LAN*** to enter the **Wireless** interface. The data of Properties and Security need to be filled.



Properties

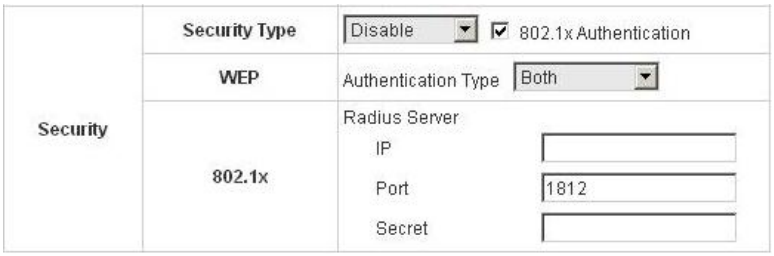
- **SSID:** The SSID is the unique name shared among all APs in a wireless network. The SSID must be the same for all APs in the wireless network. It is case sensitive and has a maximum length of 32 bytes.
- **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, you may want to enable this function, but make sure to disable it when you finished. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to your network. With this disabled to increase network security and prevent the SSID from being seen on networked.
- **Channel:** Select the appropriate channel from the list to correspond with your network settings; for example, 1 to 11 channels are suitable for the North America area.
- **Transmission Mode:** There are 3 modes to select, **802.11b** (2.4G, 1~11Mbps)**, 802.11g** (2.4G, 54Mbps) and **Mix mode** (b and g).
- **Transmission Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speed or you can keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **CTS Protection:** The default value is **Disable**. When select **"Enable"**, a protection mechanism will decrease collision probability when many 802.11g APs exist simultaneously. However, performance of your 802.11g APs may decrease.
- **Fragment Threshold:** Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds.

The entered time means how often the beacon signal transmission between the access point and the wireless network.

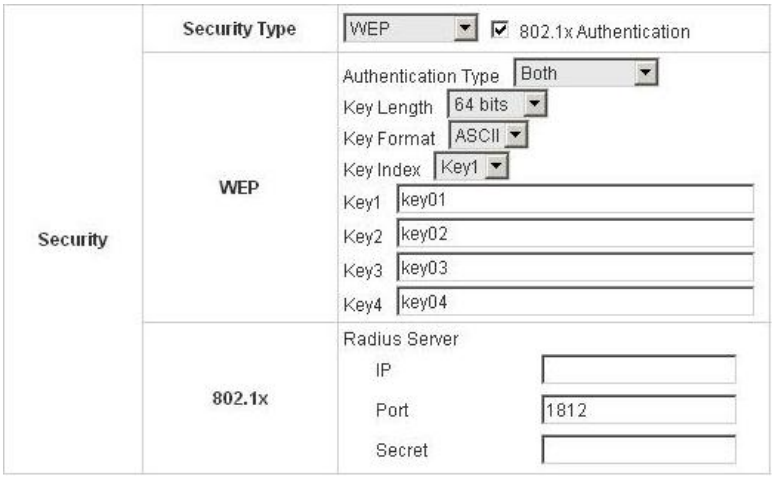
- **Preamble Type:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. You can select either Short Preamble or Long Preamble.
- **IAPP:** Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period.

Security: There are four kinds of security type, **WEP**, **WPA**, **WPA2** and**WPA2 Mixed** for selection.

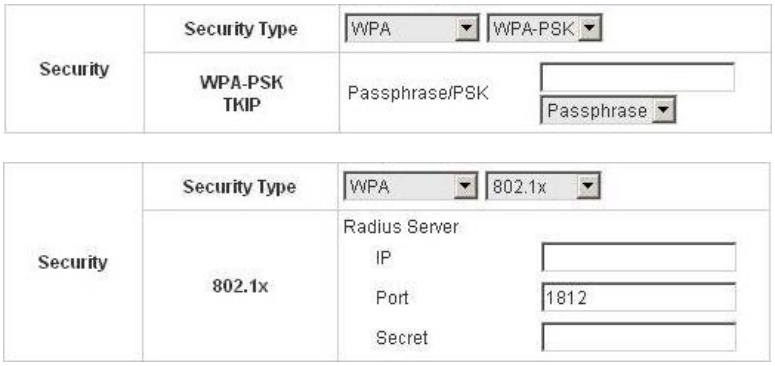
- **Disable:** Choose this type, there is no any encryption used but **802.1x Authentication** and **Authentication Type**. For Authentication Type, you can choose **Open System**, **Shared Key** or **Both** according to the settings of the AP and Client. Check **802.1x Authentication** to enable this function and enter the related data, if necessary.



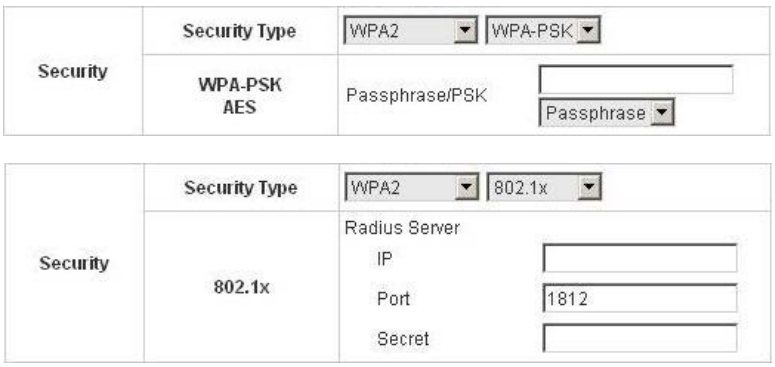
- **WEP:** WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read. Select **Authentication Type** (Open System, Shared Key or Both), **Key Length** (64 bits or 128 bits), **Key Index** (Key1~Key4) and then input the **Key**. Check **802.1x Authentication** to enable this function and enter the related data, if necessary.



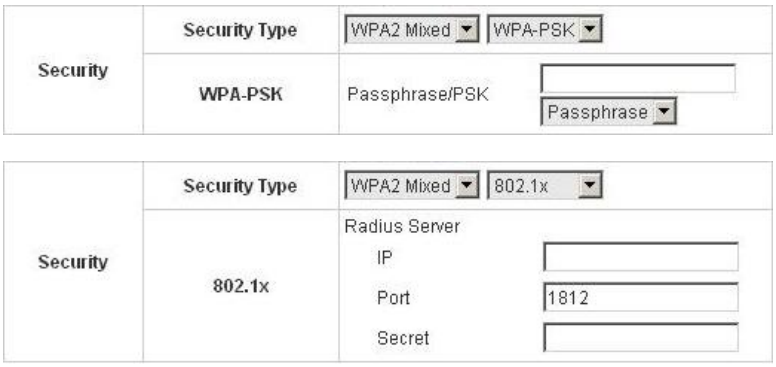
- **WPA:** WPA is Wi-Fi's encryption method that protects unauthorized network access by verifying network users through a server. Select 802.1x or WPA-PSK security type and enter the related information below.



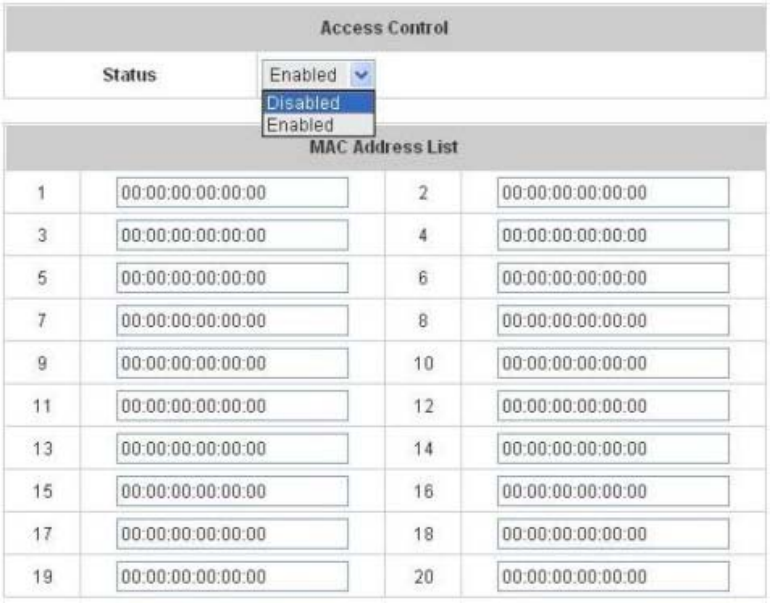
- **WPA2**: Wi-Fi Protected Access version 2. The follow on security method to WPA for Wi-Fi networks that provides stronger data protection and network access control. Select 802.1x or WPA-PSK security type and enter the related information below. WPA2 only can use AES encryption type.



- **WPA Mixed:** If you want to use TKIP and AES encryption type at the same time, you can choose this security type. Select 802.1x or WPA-PSK security type and enter the related information below.

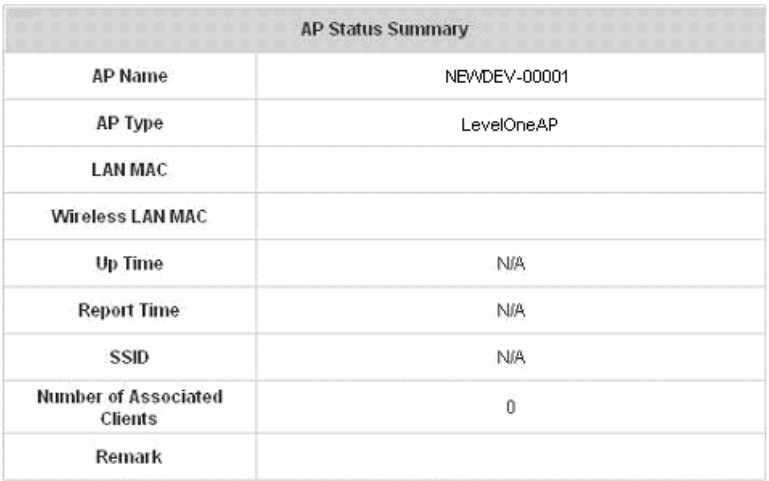


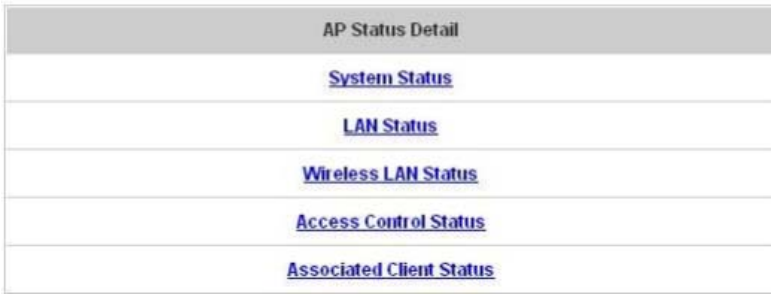
- **Access Control:** In this function, when the status is **"Enabled"**, only these clients which MAC addresses are listed in the list can be allowed to connect AMG-2000. When **"Disabled"** is selected, all clients can connect AMG-2000. The default is **Disabled**.



- **Status**

After clicking the hyperlink of Status, you can see the basic information of the AP including **AP Name**, **AP Type**, **LAN MAC**, **LAN MAC**, **Wireless LAN MAC**, **Up Time**, **Report Time**, **SSID**, **Number of Associated Clients** and **Remark**. In the below of the **AP Status Detail**, there are the related detailed information, **System Status**, **LAN Status**, **Wireless LAN Status**, **Access Control Status** and **Associated Client Status**.





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

System Information	
AP Name	NEWDEV-00001
AP Status	Online
Last Reporting Time	2006-06-28 10:27:37

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

LAN Interface	
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Gateway	0.0.0.0

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

Wireless Interface	
Up Time	0day:0h:4m:32s
SSID	apmgt
Beacon Interval (ms)	100
RTS Threshold	2347
Channel	11
Transmission Rate	Auto
Preamble Type	Long Preamble
IAPP	Enabled
Security	WEP

- **Access Control:** The table shows the status of MAC of clients under the control of the AP.

Access Control	
Status	Disabled

Access Control	
Status	Enabled

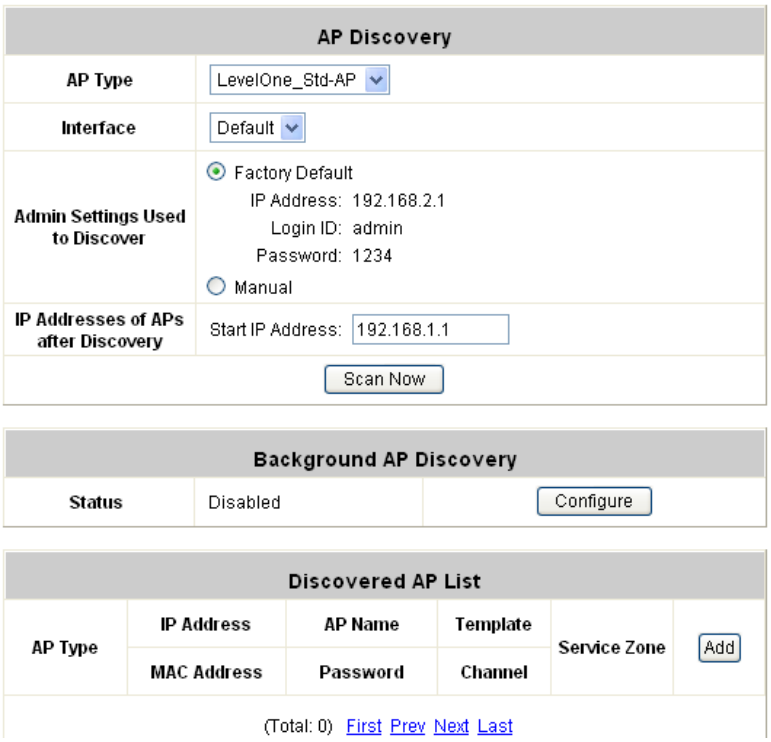
Control List	
00:00:00:00:00:01	00:00:00:00:00:02
00:00:00:00:00:03	00:00:00:00:00:04
00:00:00:00:00:05	00:00:00:00:00:06
00:00:00:00:00:07	00:00:00:00:00:08
00:00:00:00:00:09	00:00:00:00:00:10
00:00:00:00:00:11	00:00:00:00:00:12
00:00:00:00:00:13	00:00:00:00:00:14
00:00:00:00:00:15	00:00:00:00:00:16
00:00:00:00:00:17	00:00:00:00:00:18
00:00:00:00:00:19	00:40:96:A1:AF:dd

- **Client List:** The table shows the clients connecting to the AP and the related information of the client.

Client List							
No	MAC	User ID	TX Packet (s)	RX Packet (s)	Rate	Power Saving	Expiration countdown
1	00:02:8a:f3:aa:a4	N/A	2	6	11	No	300

4.3.2 AP Discovery

When manageable APs are to be deployed in the wireless network, it is convenient to discover all the APs from a single interface.



- **AP Discovery Settings**

  By pre-defining the settings of those APs in this AP Discovery interface, administrator will be able to discover (by clicking on the ***Scan Now*** button) all manageable APs under AMG-2000 at once. After these APs are discovered, administrator can apply the template of AP setting and add to the AP List for later maintenance.

  - **AP Type**: The type of manageable APs to be discovered: **LevelOne_Std-AP and LevelOne_Adv-AP**.
  - **Interface**: The default Service Zone to which the APs are connected.
  - **Admin Settings Used to Discover:** This is the setting of web-based Administration UI of the specific AP. If the APs are not reset to "Factory Default" values, administrator can select ***Manual*** to manually enter the current IP address range, Login ID and Password of the APs.

Note: Limitation on WAP-0005 AP (AP Type: LevelOne_Adv-AP) Discovery

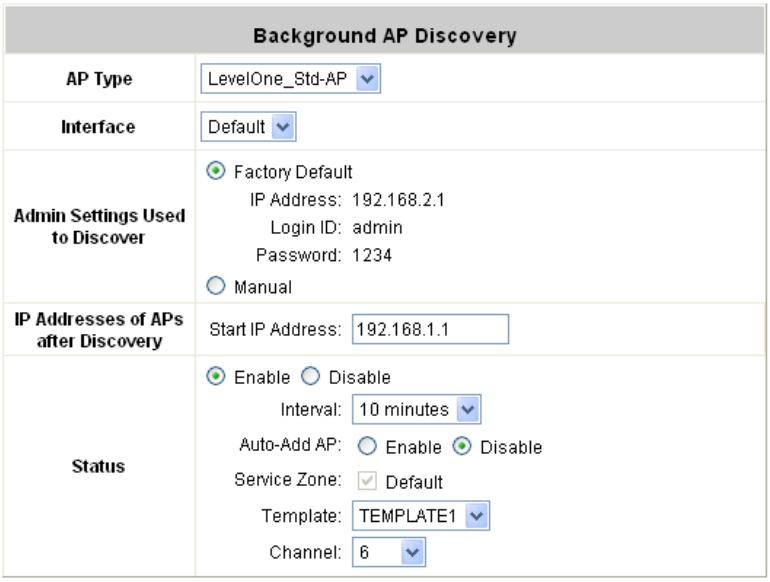
Under default mode (DHCP Client) of WAP-0005 AP, the AP will be assigned an IP address automatically when the AP can reach a DHCP server on the network, such as the built-in DHCP server of AMG-2000. As a result, the system will NOT be able to discover WAP-0005 using the ***Factory Default*** *setting. The workaround is to connect the AP to the network only after the timeout of its DHCP request.*

  - **IP Addresses of APs after Discovery**: The start IP address of IP address range to be assigned to the discovered APs.

- **Scan Now:** Click this button to start the discovery. All discovered APs will be shown in the ***Discovered AP List***. If any IP address to be assigned to a specific AP is used, there will be a warning message showing up. If so, please change the **IP Addresses of APs after Discovery** and then click ***Scan Now*** again.

- **Background AP Discovery:**

The system can be set up to discover APs periodically in background

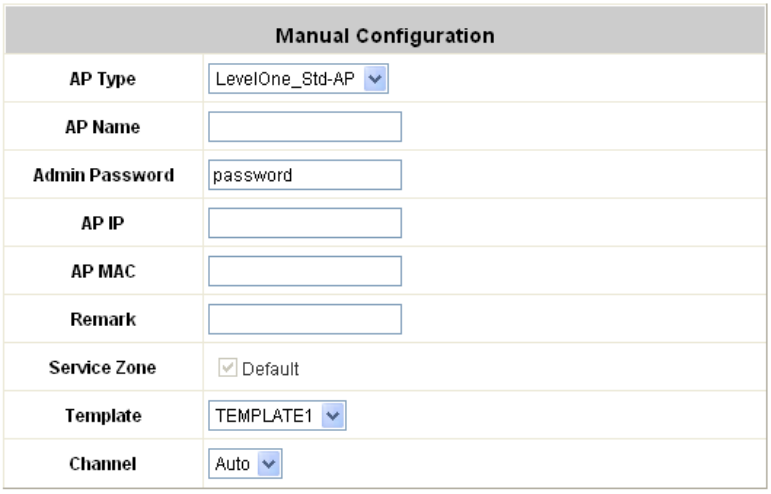


Settings of ***Background AP Discovery*** are the same as the in the ***AP Discovery*** settings mentioned above. For the ***Status***, when enabled, the system will discover APs in background at the time interval (Default: 10 minutes). If any AP is discovered and "Auto-Add AP" enabled, the system will add the discovered APs into the ***AP List*** table automatically, apply the selected ***Template*** of AP setting to the APs, and assign available IP addresses to the APs.

Discovered AP List: Administrator can click ***Add*** button to register the APs to the ***AP List*** for management. The Service Zone to which the APs will belong is specified here. By clicking **Add** button, the current management page is directed to ***AP List***, where the newly added APs will show up with a status of "configuring". It may take a couple of minutes to see the status of the newly added AP to change from "configuring" to "online" or "offline".

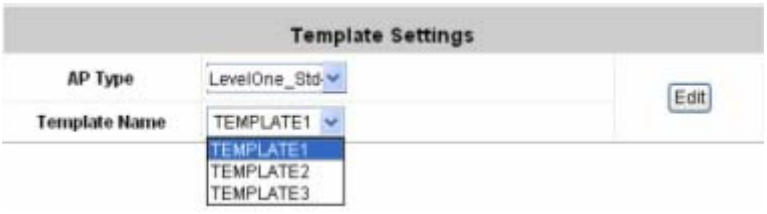
4.3.3 Manual Configuration

Manageable APs can also be added to ***AP List*** manually. Input the related data of the AP and select a Template. Then click ***Add***, the AP will be added to the ***AP List***.

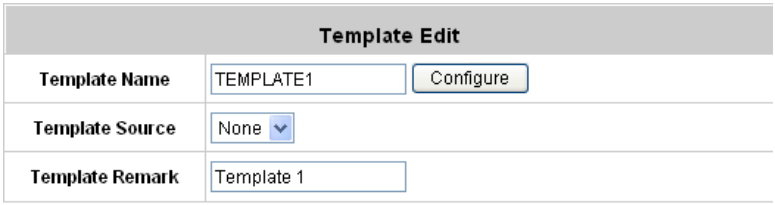


4.3.4 Template Settings

Template is a completed configuration of AP that you can copy it to an AP, thus not necessary to configure the AP individually. There are three templates provided by AMG-2000 and click ***Edit*** to go on configuration.



Before configuring the template, you can copy the configuration of an AP to the template by selecting a **Template AP**, and you don't have to configure the template from the beginning and can just revise some settings for demand. If you don't want to copy, please select **NONE**. Input the **Template Name** and **Template Remark** and click the hyperlink of ***Configure*** to go on configuration.



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

Reset

General	
Subnet Mask	255.255.255.0 *
Default Gateway	192.168.1.254 *

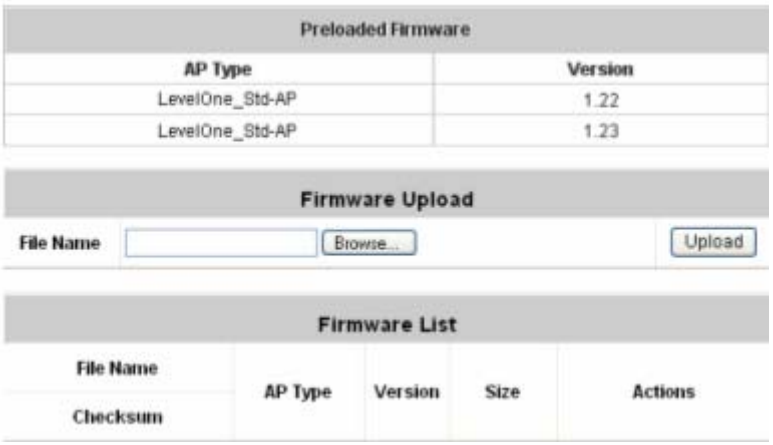
Wireless		
Properties	SSID Broadcast	Enable
	Transmission Mode	Mixed
	Transmission Rate	Auto (Default: Auto; Range: from 1 to 54 Mbps)
	CTS Protection	Disable (Default: Disable)
	Fragment Threshold	2346 (Default: 2346; Range: from 256 to 2346)
	RTS Threshold	2347 (Default: 2347; Range: from 0 to 2347)
	Beacon Interval (ms)	100 (Default: 100; Range: from 20 to 1024 msec)
	Preamble Type	Long (Default: Long)
	IAPP	Enable (Default: Enable)

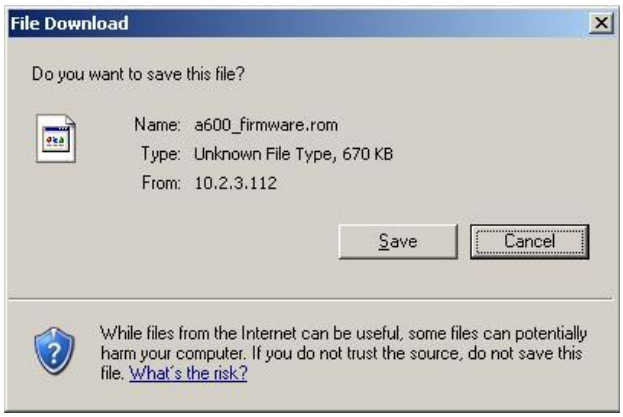
Access Control	
Status	Disabled

MAC Address List			
1	00:00:00:00:00:00	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00
5	00:00:00:00:00:00	6	00:00:00:00:00:00
7	00:00:00:00:00:00	8	00:00:00:00:00:00
9	00:00:00:00:00:00	10	00:00:00:00:00:00
11	00:00:00:00:00:00	12	00:00:00:00:00:00
13	00:00:00:00:00:00	14	00:00:00:00:00:00
15	00:00:00:00:00:00	16	00:00:00:00:00:00
17	00:00:00:00:00:00	18	00:00:00:00:00:00
19	00:00:00:00:00:00	20	00:00:00:00:00:00

4.3.5 Firmware Management

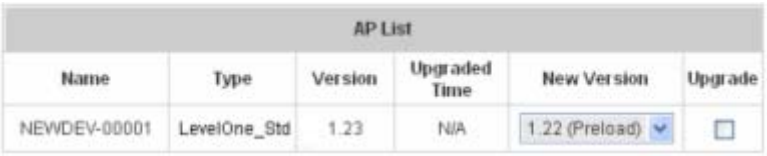
In this function, you can upload the AP's firmware to AMG-2000 and also can download the present firmware to the local or delete it.





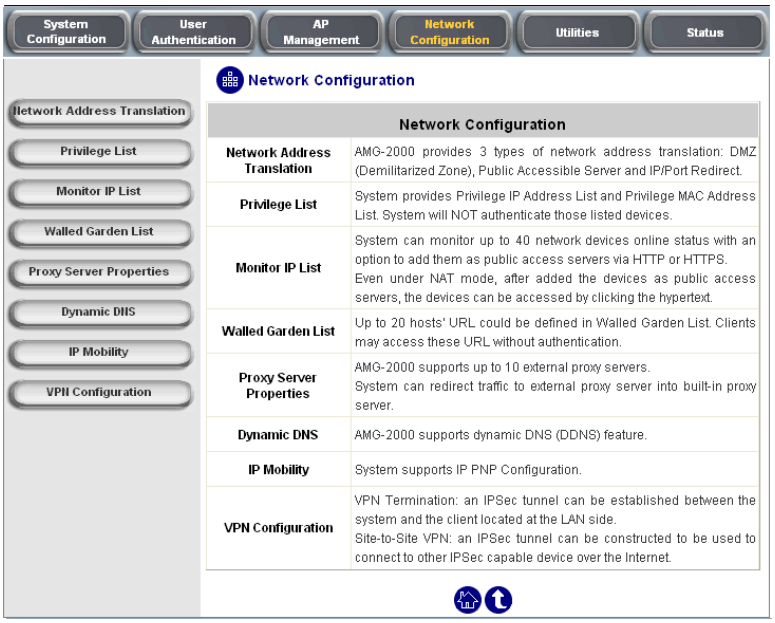
4.3.6 AP Upgrade

Check the APs which need to be upgraded and select the upgrade version of firmware, and then click ***Apply*** to upgrade firmware.



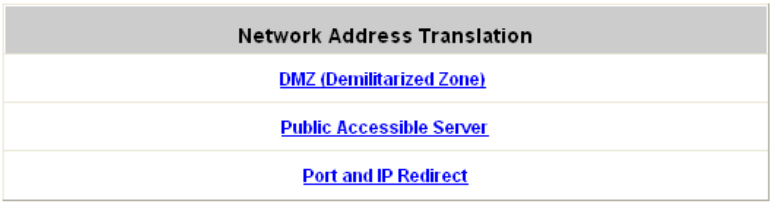
4.4 Network Configuration

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



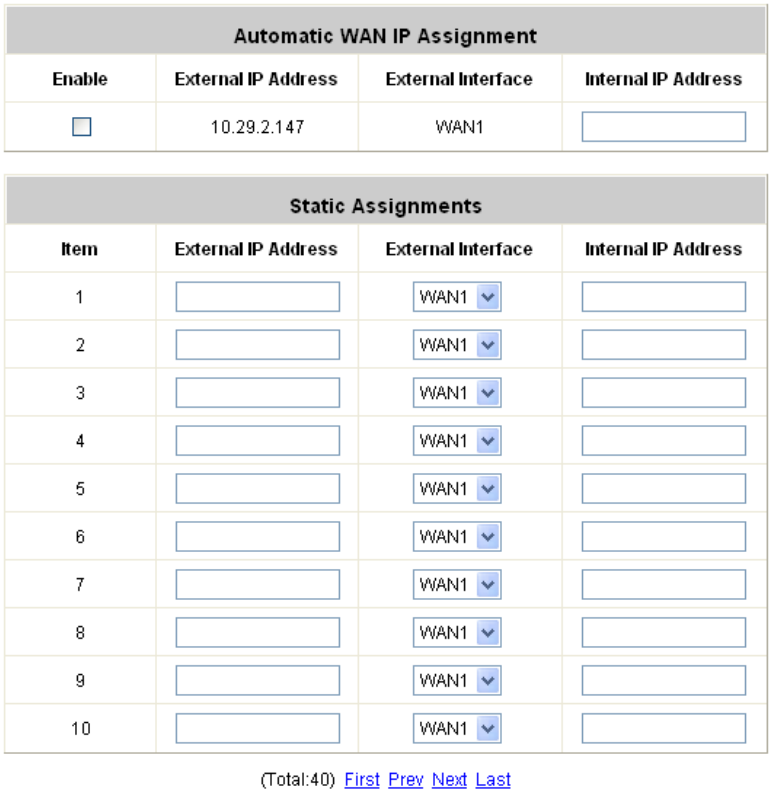
4.4.1 Network Address Translation

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



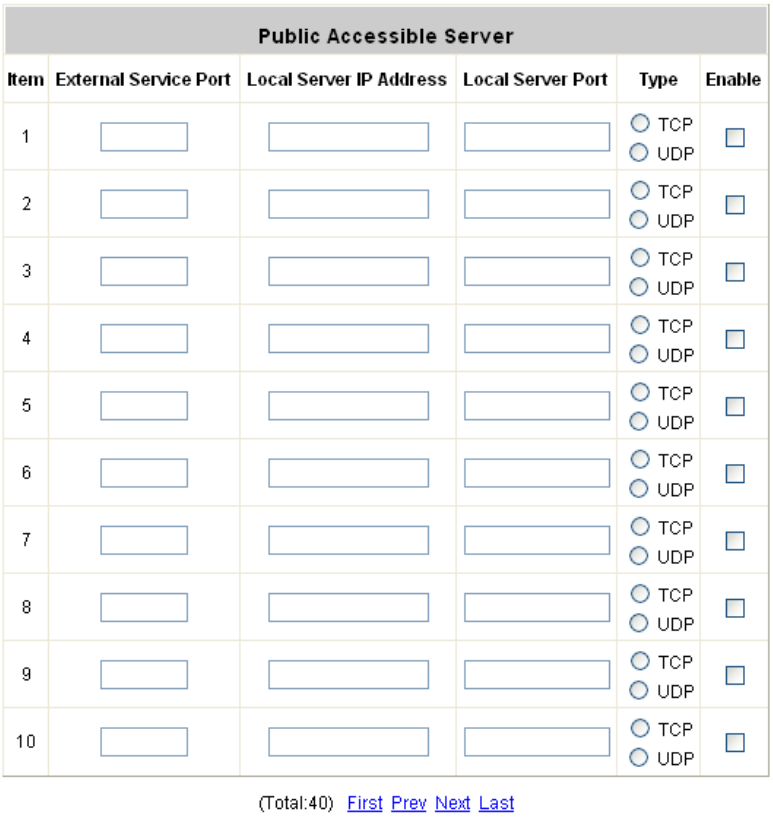
- **DMZ (Demilitarized Zone)**

  DMZ allows administrators to define mandatory external to internal IP mapping, hence a user on WAN side network can access the private machine via the external IP (similar to DMZ usage in firewall product). There are 40 sets of static **Internal IP Address** and **External IP Address** available. If a host needs a static IP address to access the network through WAN port, set a static IP for the host. First choose whether to enable Internal IP Address by checking the box and inputting an Internal IP Address under Automatic WAN IP Assignment. Then input Internal IP Address and corresponding External IP Address under Static Assignments, and choose an External Interface from the drop-down menu. These settings will become effective immediately after clicking the ***Apply*** button.



- **Public Accessible Server**

  This function allows the administrator to set 40 virtual servers at most, so that the computers not belonging to the managed network can access the servers in the managed network via WAN port IP of AMG-2000. 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.

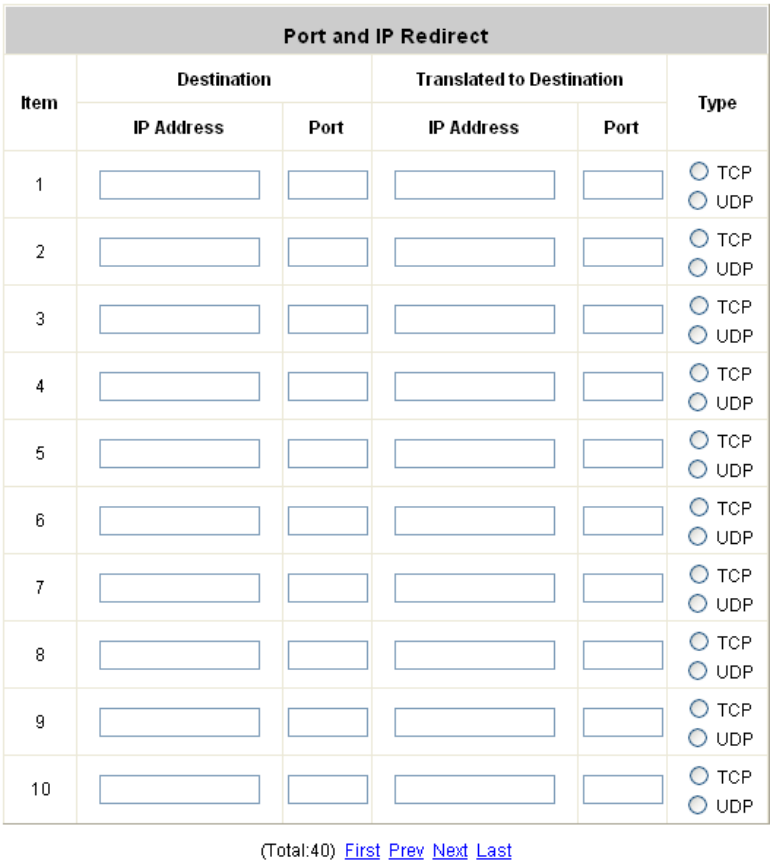


Public Accessible Server					
Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				TCP UDP	
2				TCP UDP	
3				TCP UDP	
4				TCP UDP	
5				TCP UDP	
6				TCP UDP	
7				TCP UDP	
8				TCP UDP	
9				TCP UDP	
10				TCP UDP	

(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***.



Port and IP Redirect					
Item	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1					TCP UDP
2					TCP UDP
3					TCP UDP
4					TCP UDP
5					TCP UDP
6					TCP UDP
7					TCP UDP
8					TCP UDP
9					TCP UDP
10					TCP UDP

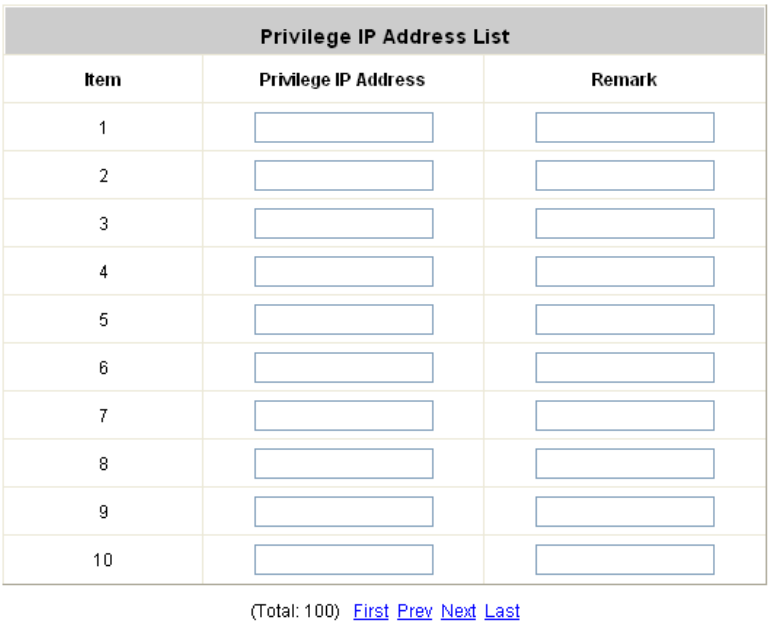
(Total:40) First Prev Next Last

4.4.2 Privilege List

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

- **Privilege 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. AMG-2000 allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking ***Apply***.

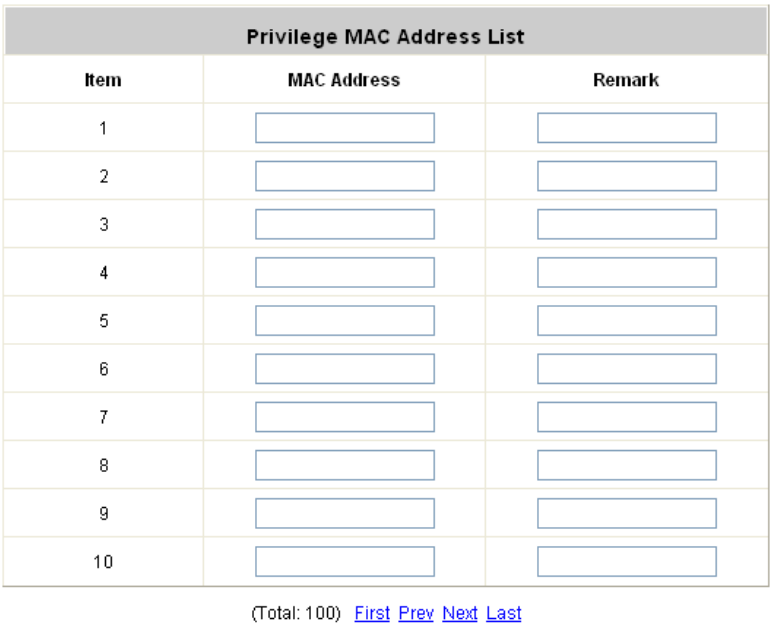


Warning: *Permitting specific IP addresses to have network access rights without going through standard authentication process at the LAN1~LAN4 port may cause security problems.*

- **Privilege MAC Address List**

  In addition to the IP address, you can also set the MAC address of the workstations that need to access the network without authentication in this list. AMG-2000 allows 100 privilege MAC addresses at most.

  List can be created manually-- 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		
2		
3		
4		
5		
6		
7		
8		
9		
10		

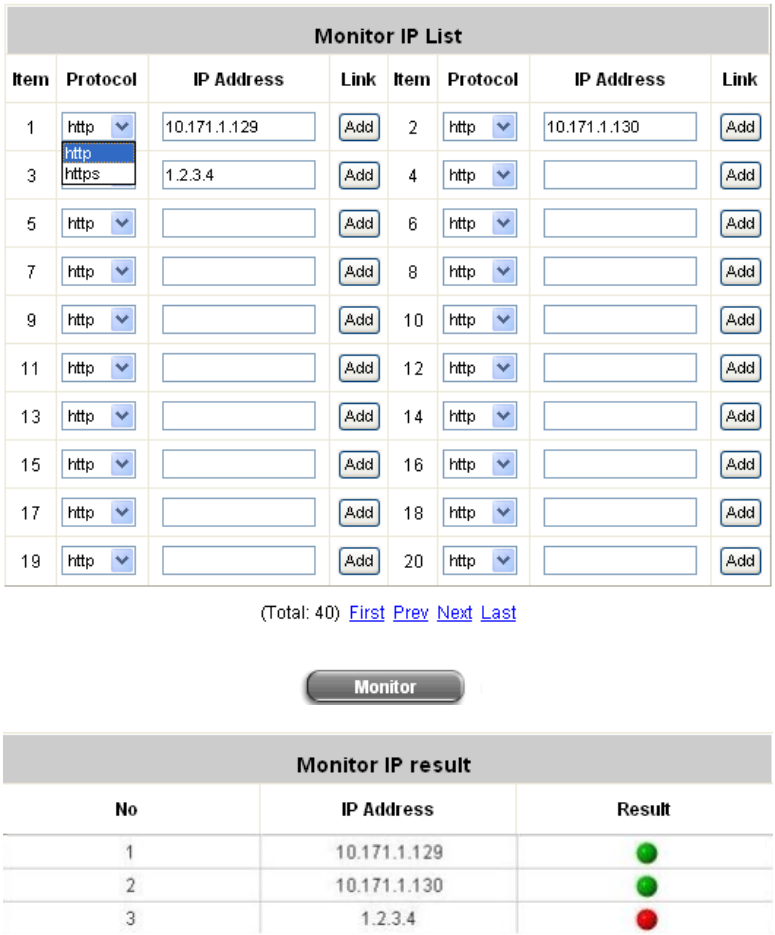
(Total: 100) First Prev Next Last

Warning: *Permitting specific MAC addresses to have network access rights without going through standard authentication process at the LAN1~LAN4 port may cause security problems.*

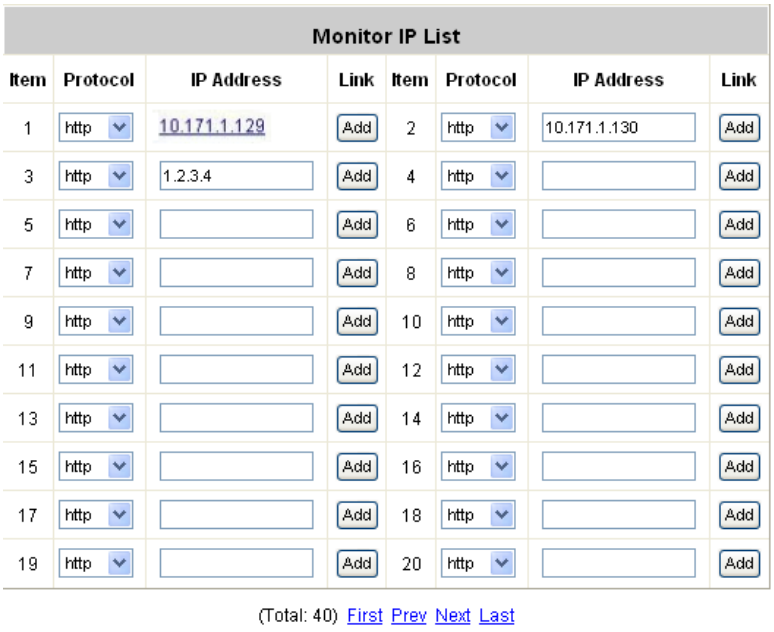
4.4.3 Monitor IP List

AMG-2000 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.

Enter an **IP Address**, then 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 at most on the **"Monitor IP List"**.



On each monitored device with a WEB server running, you may add a link for the easy access by selecting a protocol, http or https, and click the **Add** button. After clicking Add button, the IP address will become a hyperlink, and then you can easily access the host by clicking the hyperlink. Click the **Del** button to remove the setting.



Monitor IP List

Item	Protocol	IP Address	Link	Item	Protocol	IP Address	Link
1	http	10.171.1.129	Add	2	http	10.171.1.130	Add
3	http	1.2.3.4	Add	4	http		Add
5	http		Add	6	http		Add
7	http		Add	8	http		Add
9	http		Add	10	http		Add
11	http		Add	12	http		Add
13	http		Add	14	http		Add
15	http		Add	16	http		Add
17	http		Add	18	http		Add
19	http		Add	20	http		Add

(Total: 40) First Prev Next Last

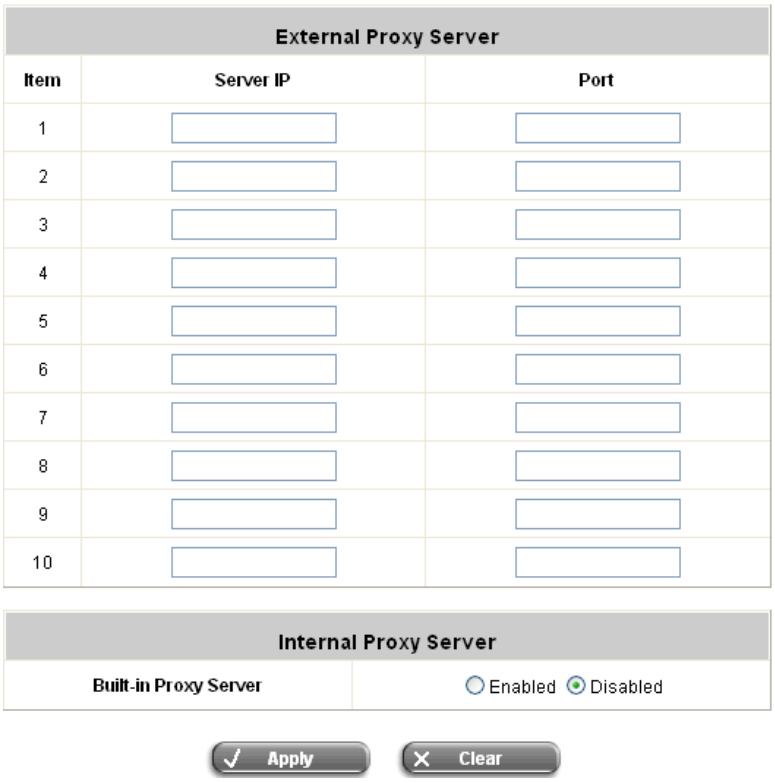
4.4.4 Walled Garden List

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

Caution: *To use the domain name, the AMG-2000 has to connect to DNS server first or this function will not work.*

4.4.5 Proxy Server Properties

AMG-2000 supports Internal Proxy Server and External Proxy Server functions.

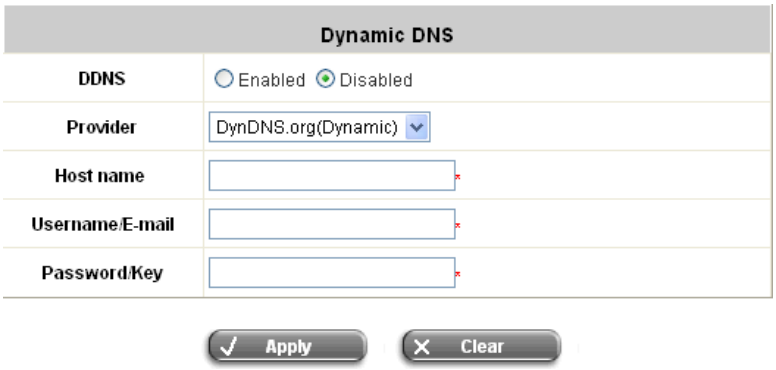


- **External Proxy Server:** Under the AMG-2000 security management, the system will match the External Proxy Server list to the end-users' proxy setting. If there isn't a matching, then the end-users will no be able to reach the login page and thus unable to access the network. If there is a matching, then the end-users will be directed to the system first for authentication. After a successful authentication, the end-users will be redirected back to the desired proxy servers depending on various situations.
- **Internal Proxy Server:** AMG-2000 has a built-in proxy server. If this function is enabled, the end users will be forced to treat AMG-2000 as the proxy server regardless of the end-users' original proxy settings.

Note: To see more details about setting up proxy servers, please read ***Appendix D. Proxy Setting for Hotspot*** and ***Appendix E. Proxy Setting for Enterprise***.

4.4.6 Dynamic DNS

AMG-2000 provides a convenient DNS function to translate a domain name to the IP address of WAN port that helps the administrator memorize and connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to the DNS server. These settings will become effective immediately after clicking ***Apply***.



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

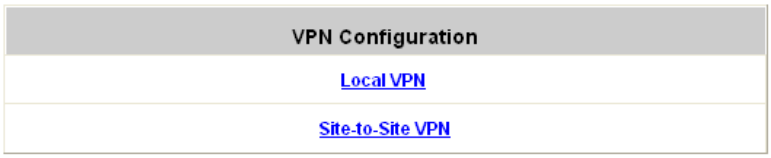
4.4.7 IP Mobility

AMG-2000 supports IP PNP function.

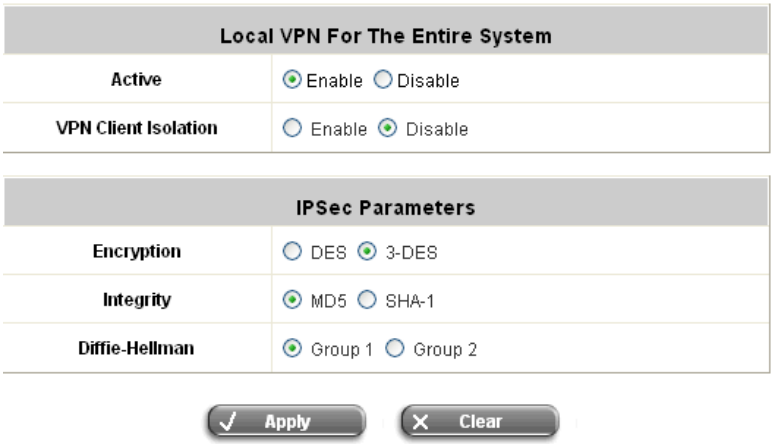
At the user end, you can use any IP address to connect to the system. Regardless of what the IP address at the user end is, you can still authenticate through AMG-2000 and access the network.

4.4.8 VPN Configuration

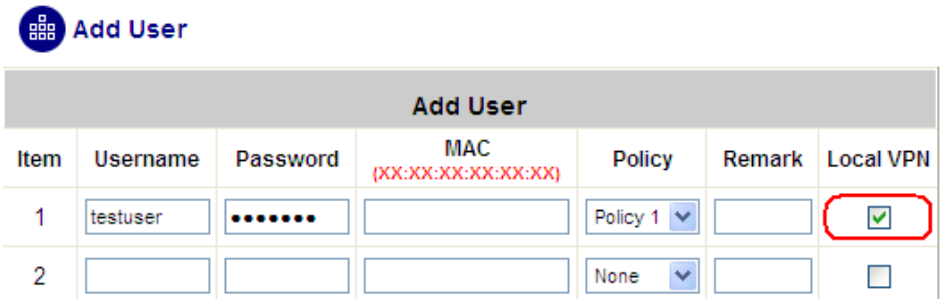
VPN (Virtual Private Network) a type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POPS. VPN creates a private encrypted tunnel from the end user's computer, through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



- **Local VPN:** It allows to create the VPN tunnel between a user's device and AMG-2000, to encrypt the data transmission. Only when this function is enabled (***Active***) here do users of the entire system are able to use Local VPN. In addition, Local VPN users can be isolated from each other when ***VPN Client Isolation*** is enabled. For more information about Local VPN, please see ***Appendix G. Local VPN User Configuration***.

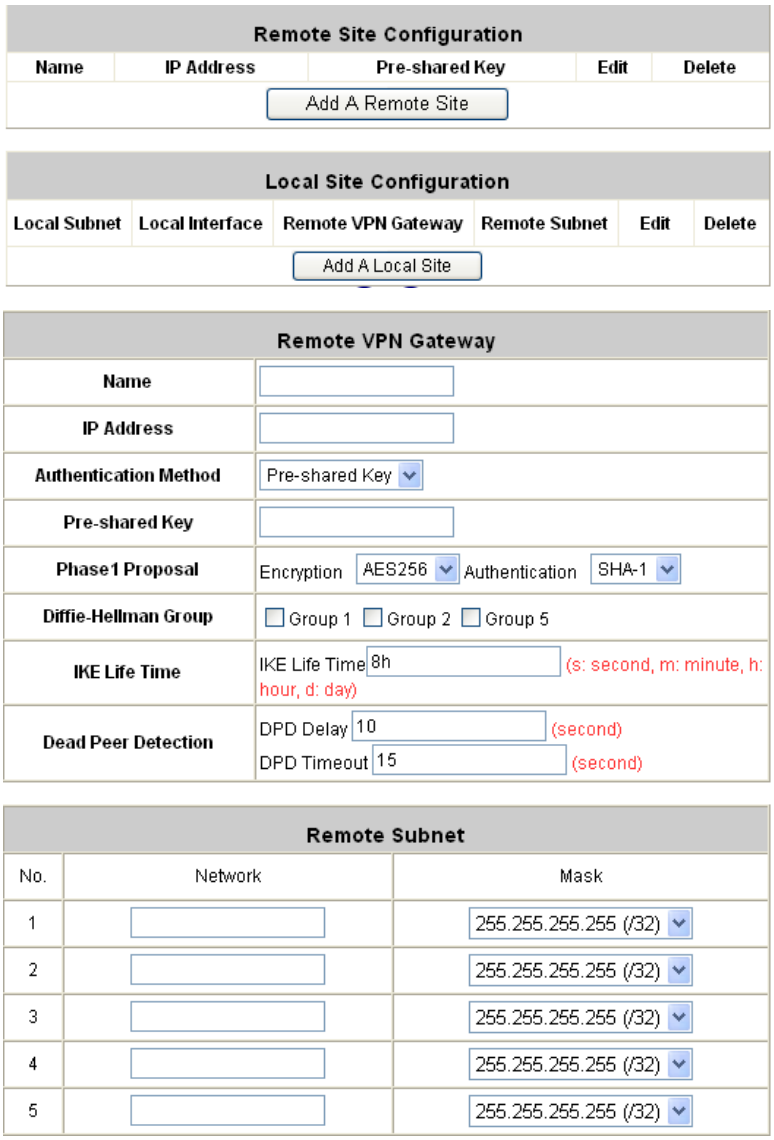


Note: *When users are required to use Local VPN for data security, their user accounts have to be configured properly to do so. For example, when adding a user account (e.g. testuser) into the* ***Local User*** *Database, administrator should check the "****Local VPN****" box:*



- **Site-to-Site VPN:** It allows the system to create the VPN tunnels from the system WAN ports to the remote sites, such as branch offices.

  Click ***Add A Remote Site*** button to enter the **Remote VPN Gateway** page for further configuration.



Click ***Add a Local Site*** button to enter the **Local Site Information** page for further configuration.

Click ***Add a New Host*** button to enter the screen of **Remote VPN Gateway**.

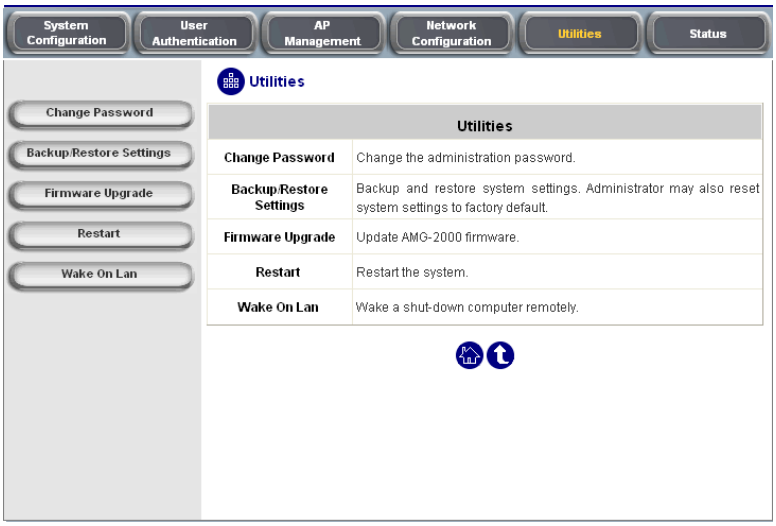
Local Site Information	
Local Interface	WAN1
Remote Gateway IP Address	Edit Host / Add a New Host
Local Subnet	(in prefix notation: x.x.x.x/yy)
Remote Subnet	
Phase2 Proposal	Encryption AES256 Authentication SHA-1
Key Life Time	Key Life Time 24h (s:second, m:minute, h:hour, d:day)
Rekey	Enable Rekey Rekey Margin 9m (second)
Perfect Forward Secrecy	Enable PFS PFS GroupMODP1024 Group 2

Remote VPN Gateway	
Name	
IP Address	
Authentication Method	Pre-shared Key
Pre-shared Key	
Phase1 Proposal	Encryption AES256 Authentication SHA-1
Diffie-Hellman Group	Group 1 Group 2 Group 5
IKE Life Time	IKE Life Time 8h (s: second, m: minute, h: hour, d: day)
Dead Peer Detection	DPD Delay 10 (second) DPD Timeout 15 (second)

Remote Subnet		
No.	Network	Mask
1		255.255.255.255 (/32)
2		255.255.255.255 (/32)
3		255.255.255.255 (/32)
4		255.255.255.255 (/32)
5		255.255.255.255 (/32)

4.5 Utilities

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



4.5.1 Change Password

AMG-2000 supports three accounts with different access privileges. You can log in as **admin**, **manager** or **operator**. The default password and access privilege for each account are as follow:

Admin: The administrator can access all configuration pages of the AMG-2000.

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**

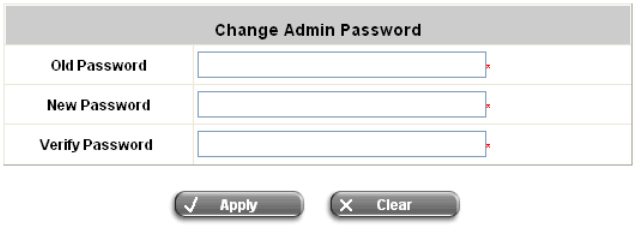
Password: **manager**

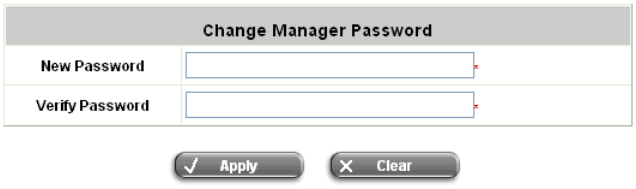
Operator: The operator can only access the configuration page of ***Create On-demand User*** to create and print out the new on-demand user accounts.

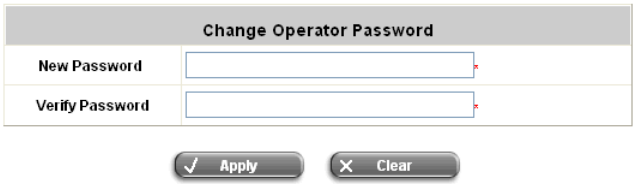
User Name: **operator**

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.



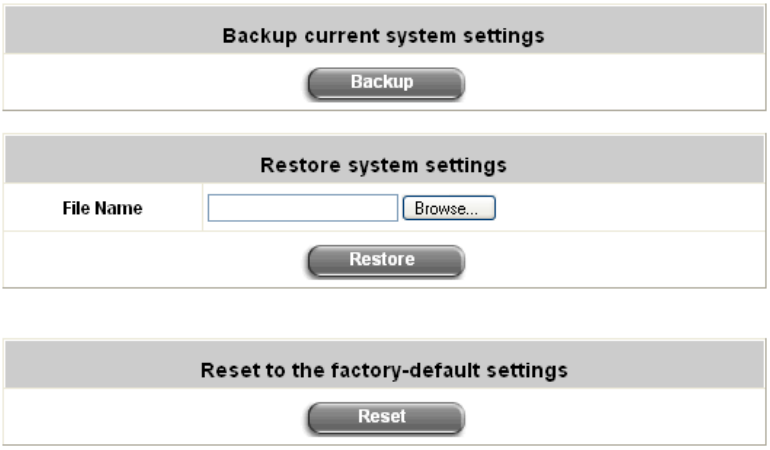




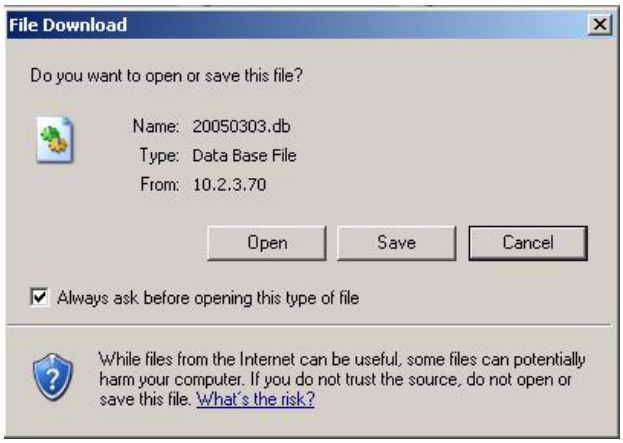
Caution: *If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial port, console/printer port.*

4.5.2 Backup/Restore Setting

This function is used to backup/restore the AMG-2000 settings. Also, AMG-2000 can be restored to the factory default settings here.



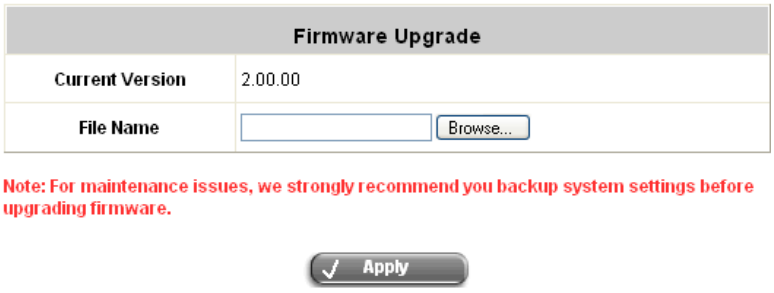
- **Backup current system setting:** Click ***Backup*** to create a .db database backup file and save it on disk.



- **Restore system setting:** Click ***Browse*** to search for a .db database backup file created by AMG-2000 and click ***Restore*** to restore to the same settings at the time the backup file was created.
- **Reset to the factory-default settings:** Click ***Reset*** to load the factory default settings of AMG-2000.

4.5.3 Firmware Upgrade

The administrator can download the latest firmware from website and upgrade the system here. Click ***Browse*** to search for the firmware file and click ***Apply*** to go on with the firmware upgrade process. It might be a few minutes before the upgrade process completes and the system needs to be restarted afterwards to make the new firmware effective.

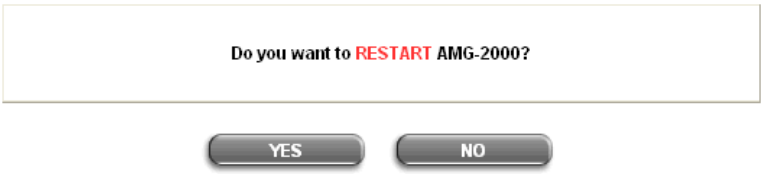


Warning: *1. Firmware upgrade may cause the loss of some of the data. Please refer to the release notes for the limitation before upgrading the firmware.*

2. Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or the restart process. It may damage the system and cause it to malfunction.

4.5.4 Restart

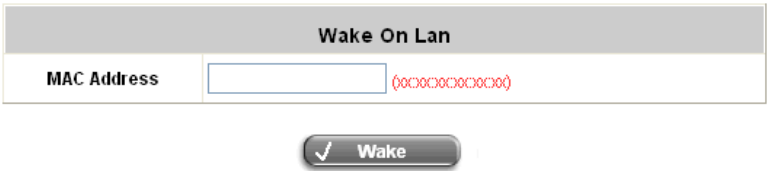
This function allows the administrator to safely restart AMG-2000 and the process should take about 100 seconds. Click ***YES*** to restart AMG-2000; click ***NO*** to go back to the previous screen. If you need to turn off the power, we recommend you to restart AMG-2000 first and then turn off the power after completing the restart process.



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

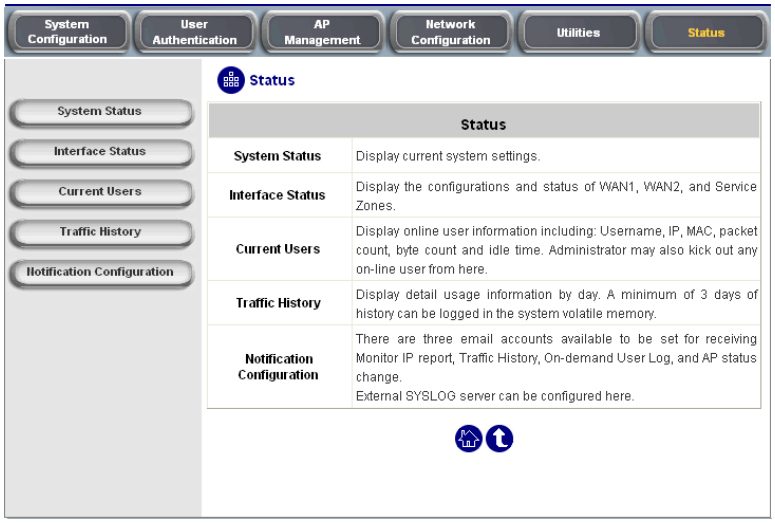
4.5.5 Wake On Lan

The **Wake On Lan** function supports to boot up a power-down computer (supporting Wake-on-LAN) connected on the LAN side remotely from the system. Enter the **MAC Address** of the desired device and click ***Wake*** to execute this function.



4.6 Status

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



4.6.1 System Status

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

System Status		
Current Firmware Version		2.00.00
Build		00100
System Name		AMG-2000
Home Page		http://www.level1.com/
Syslog server-Traffic History		N/A:N/A
Syslog server-On demand User log		N/A:N/A
Proxy Server		Disabled
Logout upon closing the "Login Success" window		Enabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
SNMP		Disabled
History	Retained Days	3 days
	Email To	N/A
		N/A
		N/A
Time	NTP Server	tock.usno.navy.mil
	Date Time	2007/04/12 15:37:16 +0800
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	208.67.222.222
	Alternate DNS Server	208.67.222.220

The description of the table is as follows:

Item		***Description***
Current Firmware Version		The present firmware version of AMG-2000
System Name		The system name. The default is AMG-2000
Home Page		The page the users are directed to after initial login success.
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.
Logout upon closing the Login Success window		Enabled/disabled stands for the setting of hiding/displaying an extra confirmation window when users click the logout button.
Warning of Internet Disconnection		Enabled/Disabled stands for the connection at WAN is normal or abnormal (**Warning of Internet Disconnection**) and all online users are allowed/disallowed to log in the network.
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.
	Email To	The email address that the traffic history information will be sent to.
Time	**NTP Server**	The network time server that the system is set to align.
	Date Time	The system time is shown as the local time.
User	**Idle Timer**	The number of 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.
DNS	**Preferred DNS Server**	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

4.6.2 Interface Status

This section provides an overview of the interface for the administrator including **WAN1**, **WAN2**, **LAN1~LAN4 Port** and **Private Port**.

Interface Status		
WAN1	MAC Address	00:06:78:AA:AA:AC
	IP Address	10.29.2.147
	Subnet Mask	255.255.0.0
WAN2	Disabled	
Service Zone - Default	Mode	NAT
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
Service Zone - Default 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)
Service Zone - SZ1	Disabled	
Service Zone - SZ2	Disabled	
Service Zone - SZ3	Disabled	
Service Zone - SZ4	Disabled	

The description of the table is as follows.

Item		***Description***
WAN1	**MAC Address**	The MAC address of the WAN1 port.
	IP Address	The IP address of the WAN1 port.
	Subnet Mask	The Subnet Mask of the WAN1 port.
Service Zone	**Mode**	The mode of the LAN1~4 port.
	MAC Address	The MAC address of the LAN1~4 port.
	IP Address	The IP address of the LAN1~4 port.
	Subnet Mask	The Subnet Mask of the LAN1~4 port.
Service Zone DHCP Server	**Status**	Enable/disable stands for status of the DHCP server on the LAN1~4 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.

4.6.3 Current Users

In this function, each online user's information including **Username**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Idle**, **Source AP** and **Kick Out** will be shown. Administrator can force out a specific online user by clicking the hyperlink of ***"Logout"***,, and check the user access AP status by click the hyperlink of the AP name for "Source AP". . Click ***Refresh*** is to update the current users list.

Current Users List

Item	Username		Pkts In	Bytes In	Idle	Location
	IP	MAC	Pkts Out	Bytes Out		Kick Out
1	07@s1		787	339553	72	AAF6-129
	10.171.1.249	00:40:96:A1:AF:DD	733	79373		Logout

Refresh

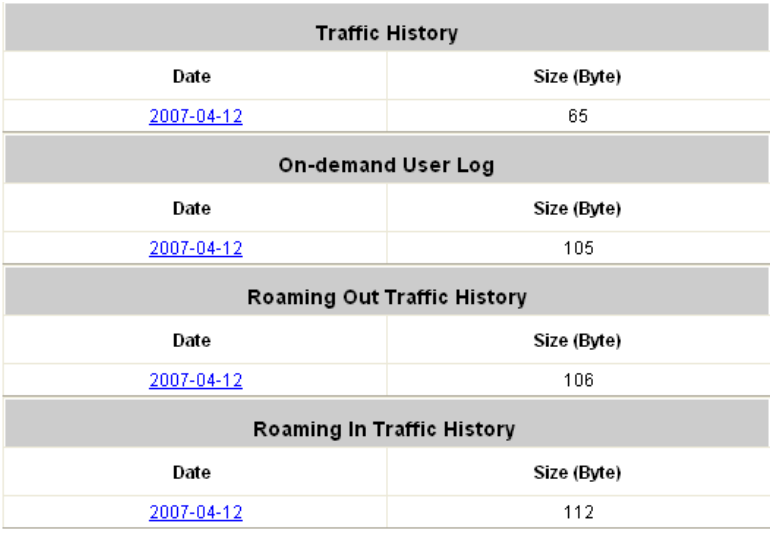
Click the Source AP to get the information of all associated client of the source AP.

Client List

No	MAC	User ID	TX Packet (s)	RX Packet (s)	Rate	Power Saving	Expiration countdown
1	00:40:96:a1:af:dd	02@s1	138	422	54	Yes	266

4.6.4 Traffic History

This function is used to check the history of AMG-2000. The history of each day will be saved separately in the DRAM for at least3 days.



Traffic History	
Date	Size (Byte)
2007-04-12	65
On-demand User Log	
Date	Size (Byte)
2007-04-12	105
Roaming Out Traffic History	
Date	Size (Byte)
2007-04-12	106
Roaming In Traffic History	
Date	Size (Byte)
2007-04-12	112

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

If the **History Email** has been entered under the **Notification 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**, **Validation** and **Remark**, of user activities.

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

- **Roaming Out Traffic History**

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

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

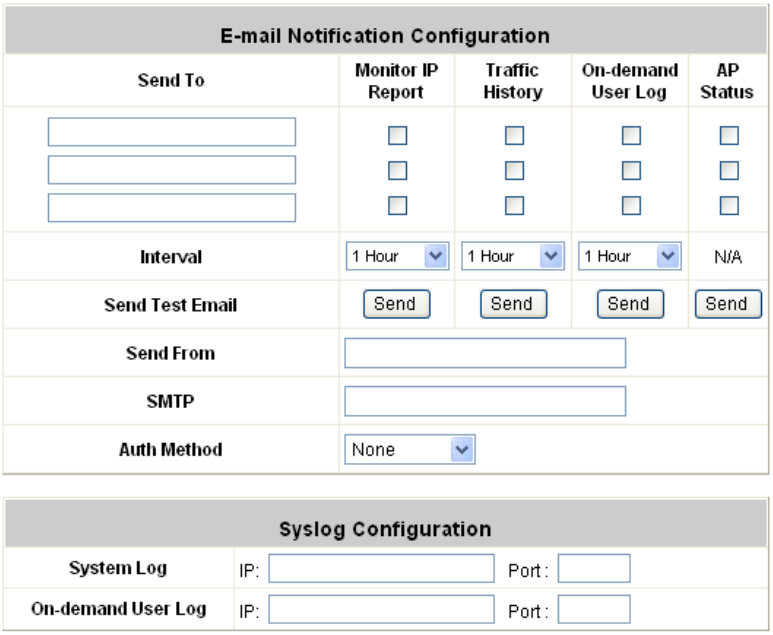
- **Roaming In Traffic History**

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

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

4.6.5 Notify Configuration

AMG-2000 can automatically send the notification of **Monitor IP Report**, **Traffic History**, **On-demand User Log** and **AP status** to up to 3 particular e-mail address. Enter the related information and select the desired items and then apply the settings.

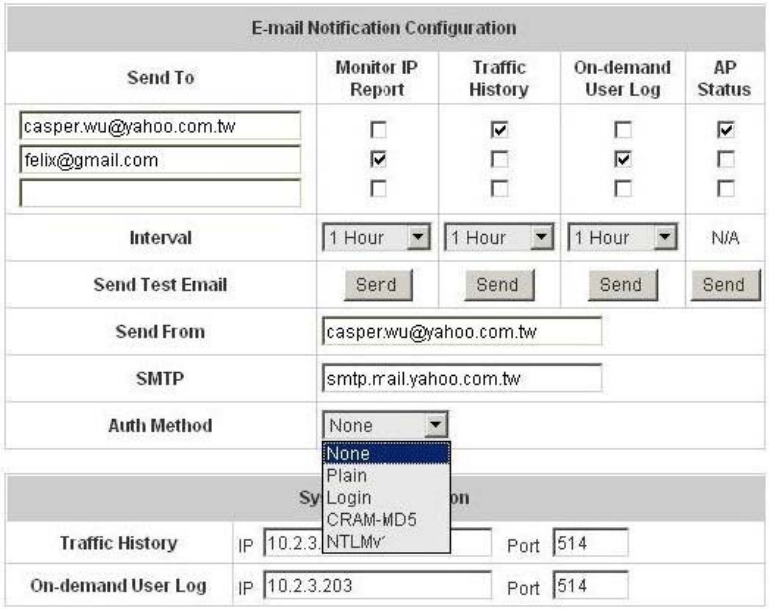


- **Send To:** You can set up to 3 e-mail address to receive the notification. These are the receiver's e-mail addresses. There are four kinds of notification to selection -- Monitor IP Report, Traffic History, On-demand User Log and AP Status, check which notification you want to receive.
- **Interval:** The time interval to send the e-mail report.
- **Send Test Email:** To test the settings immediately.
- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **SMTP:** The IP address of the sender's SMTP server.
- **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method you select, you have to enter the **Account Name**, **Password** and **Domain**.

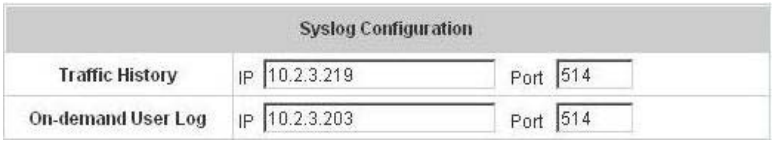
  NTLMv1 is not currently available for general use.

  Plain and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use the UNIX login password. Netscape uses **Plain**. Outlook and Outlook express uses **Login** as default, although they can be set to use **NTLMv1**.

  Pegasus uses **CRAM-MD5** or **Login** but you are not able to configure which method to use.



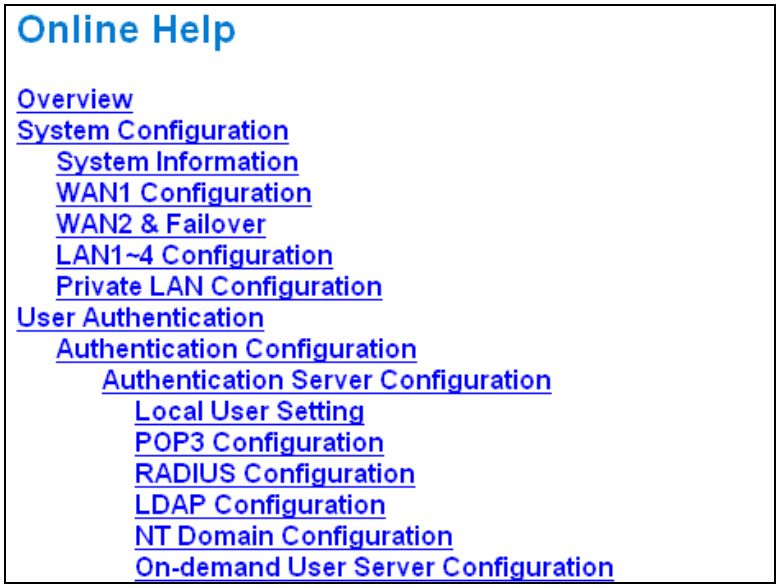
- **Syslog Configuration:** Enter the IPs and Ports of the Syslog server to receive system events including Traffic History and On-demand User Log.



4.7 Help

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

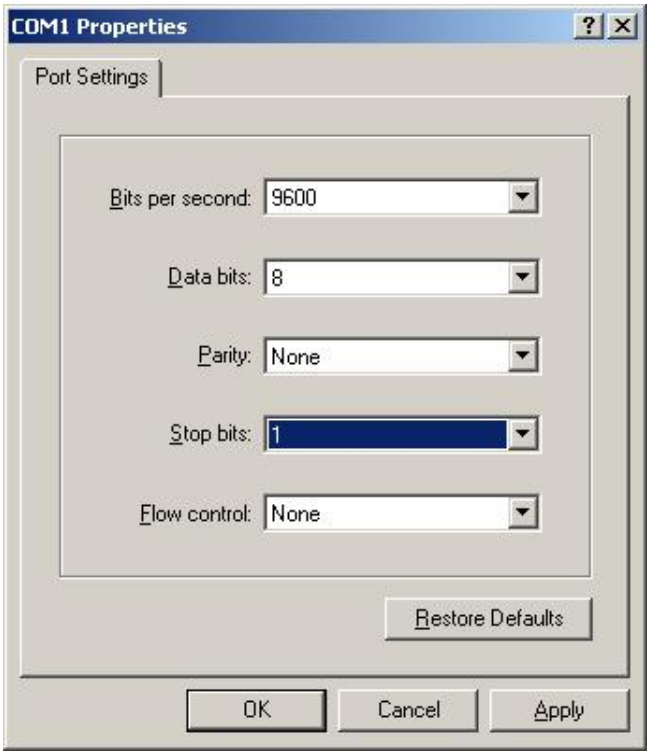
Click ***Help*** to the **Online Help** window and then click the hyperlink of the items to get the information.



Appendix A. Console Interface

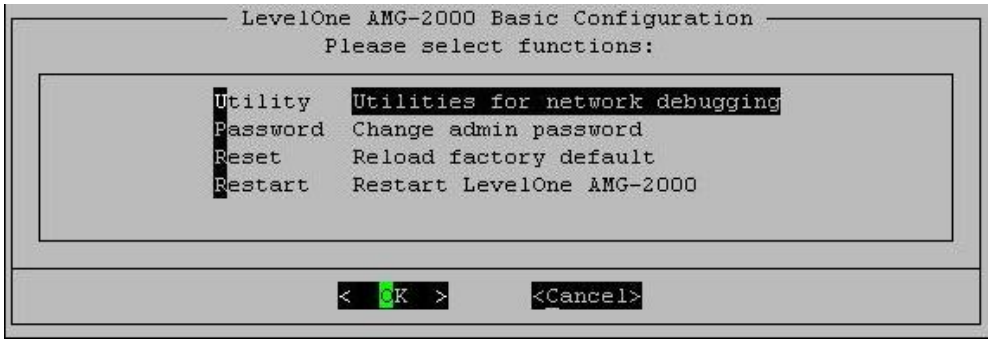
Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. To connect the console port of AMG-2000, you need a console, modem cable and a terminal simulation program, such as the Hyper Terminal.
2. If you use Hyper Terminal, please set the parameters as **9600,8,n,1**.



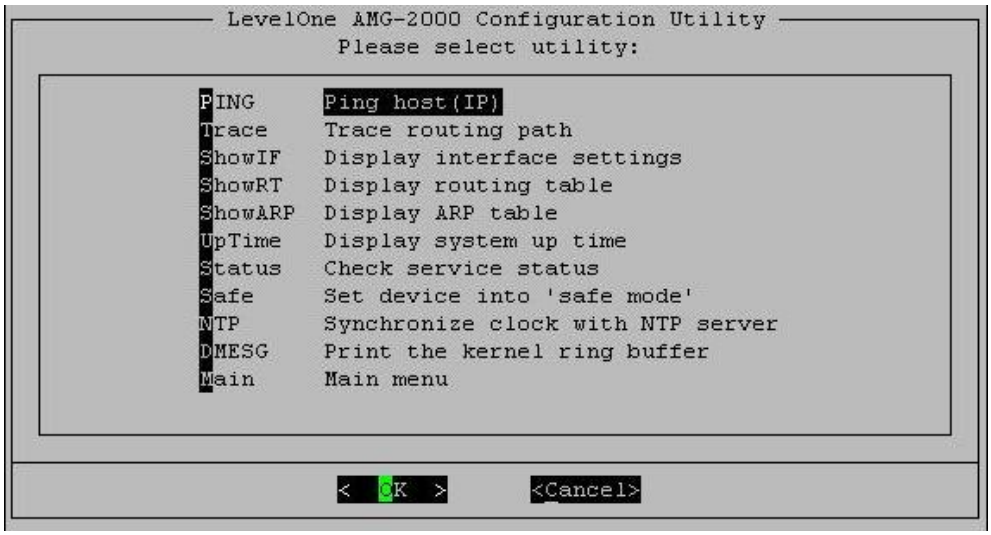
Caution: *the main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the* ***Enter*** *key to make selection or confirm what you enter.*

3. Once the console port of AMG-2000 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages to the system and the welcome screen or the main menu should appear. If you are still unable to see the welcome screen or the main menu of the console, please check the connection of the cables and the settings of the terminal simulation program.



- **Utilities for network debugging**

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



  - Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
  - Trace routing path: Trace and inquire the routing path to a specific target.
  - Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.
  - Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
  - Display ARP table: The internal ARP table of the system is displayed.
  - Display system up time: The system live time (time for system being turn on) is displayed.
  - Check service status: Check and display the status of the system.
  - Set device into "safe mode": If administrator is unable to use Web Management Interface via the browser for the system failed inexplicitly. Administrator can choose this utility and set 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. You can use this option to change the administrator's password. Even if you forgot the password and are unable to log in the management interface from the web or the remote end of the SSH, you can still use the null modem to connect the console management interface and set the administrator's password again.

Caution: *Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the AMG-2000 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 AMG-2000**
  Choosing this option will restart AMG-2000.

Appendix B. Network Configuration on PC

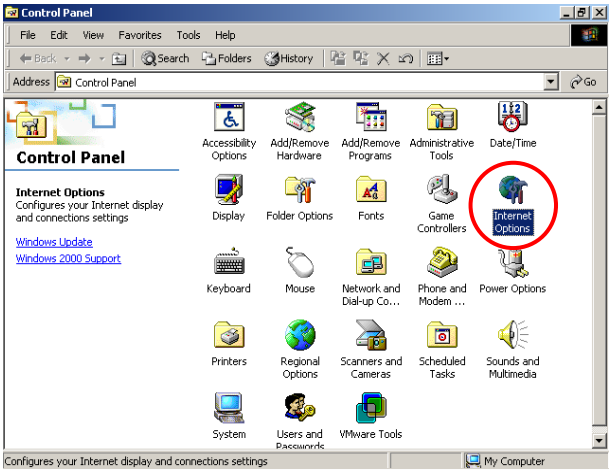
After AMG-2000 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**

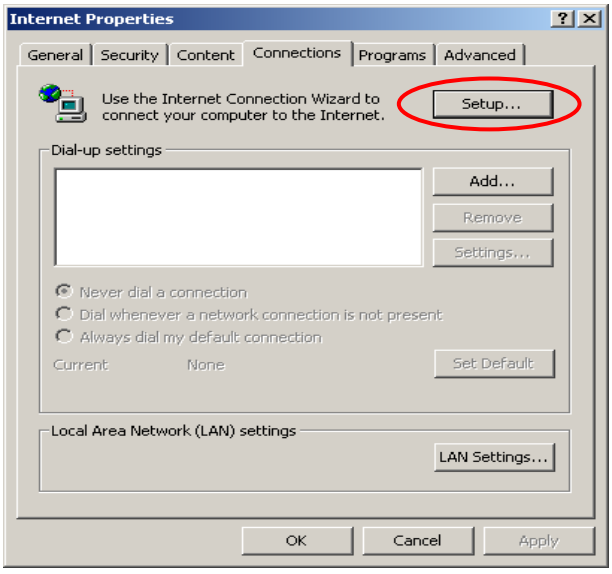
  If the Internet Connection of this client PC has been configured as use local area network already, you can skip this setup.

  ◆ **Windows 9x/2000**

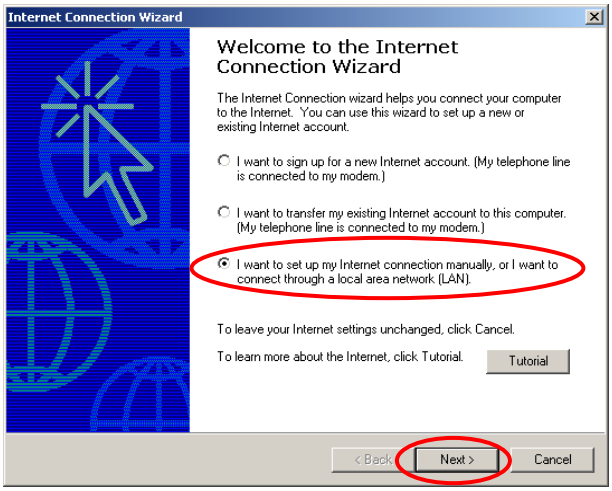
  1. Choose **Start** > **Control Panel** > **Internet Options**.



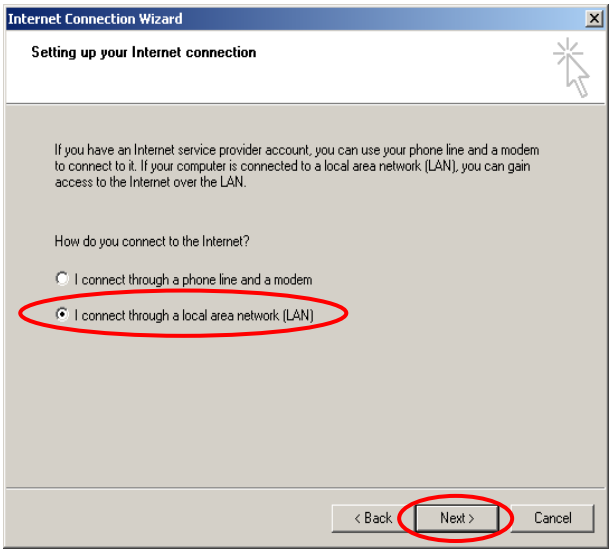
  2. Choose the **"Connections"** label, and then click ***Setup***.



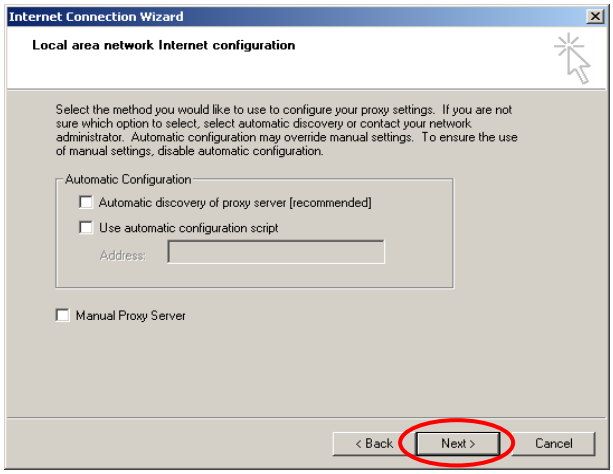
3. Choose **"I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)"**, and then click ***Next***.



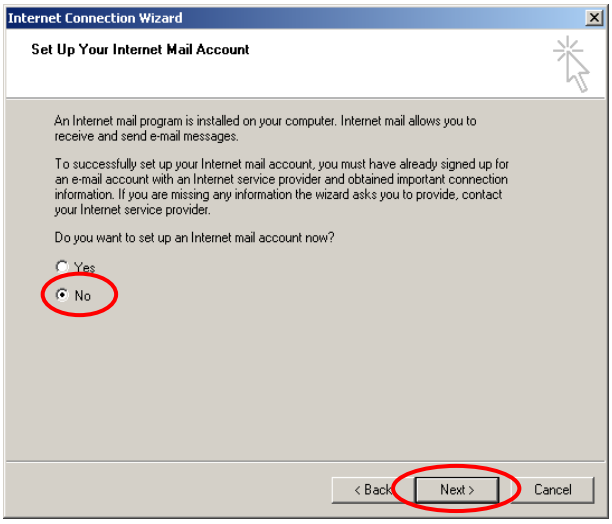
4. Choose **"I connect through a local area network (LAN)"** and click ***Next***.



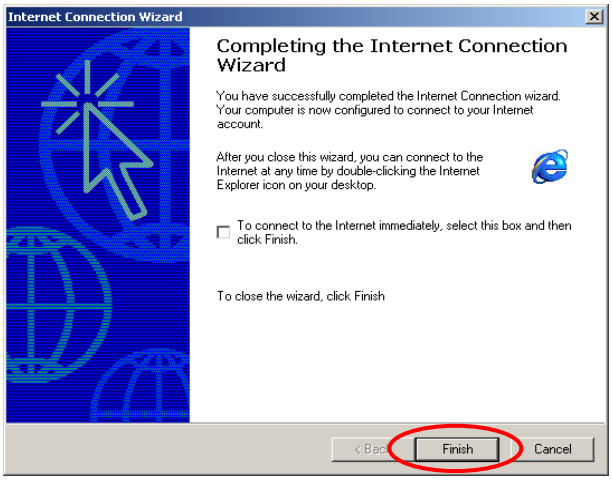
5. **DO NOT** choose any option in the following LAN window for Internet configuration, and just click ***Next***.



6. Choose **"No"**, and click ***Next***.

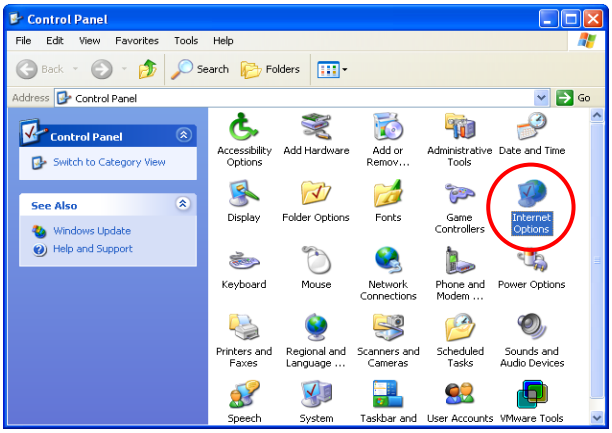


7. Finally, click ***Finish*** to exit the **Internet Connection Wizard**. Now, the set up has been completed.

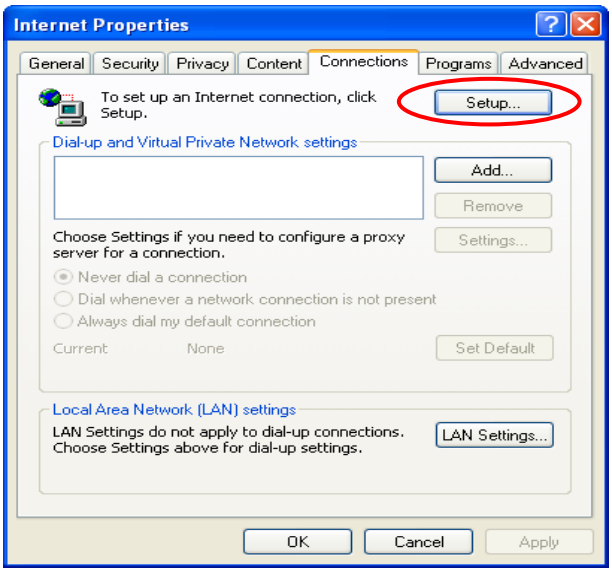


◆ **Windows XP**

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

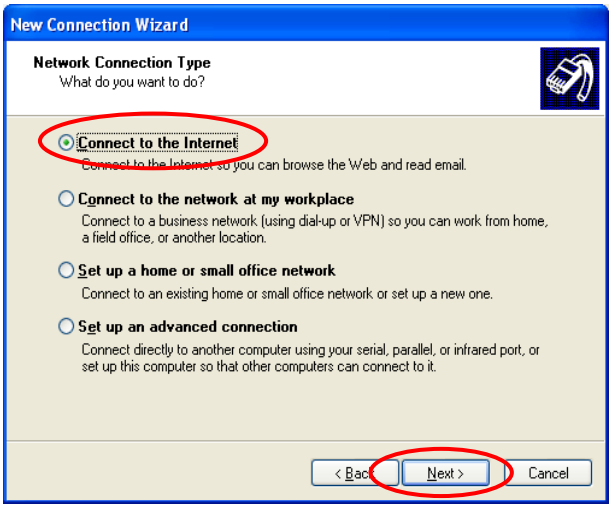


2. Choose the **"Connections"** label, and then click ***Setup***.

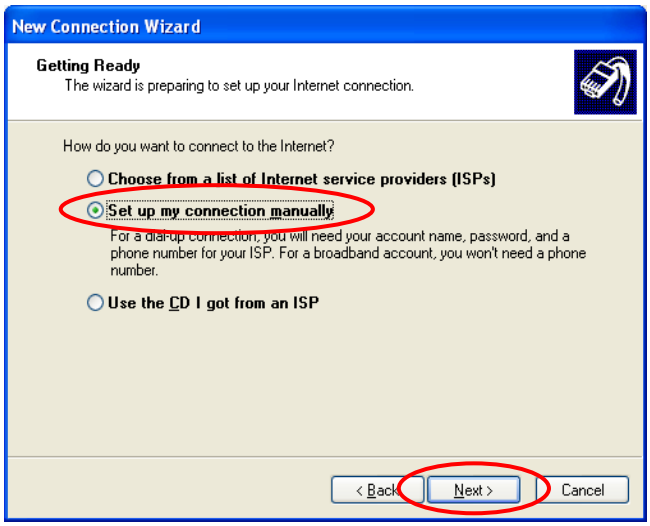


3. Click ***Next*** when **Welcome to the New Connection Wizard** screen appears.

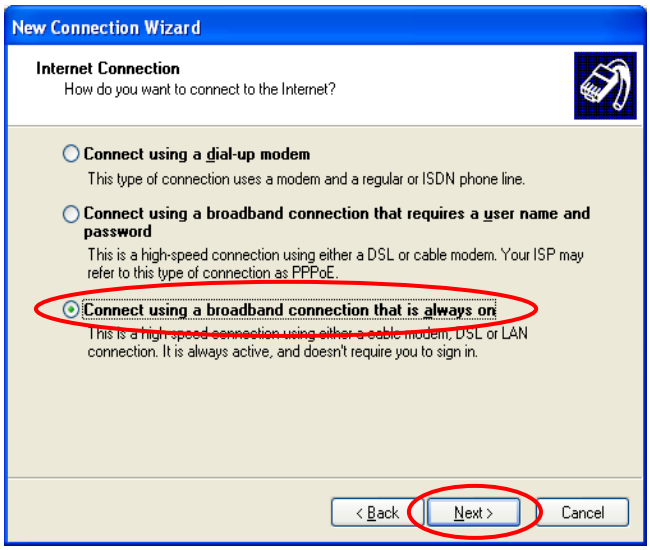
4. Choose **"Connect to the Internet"** and then click ***Next***.



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



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



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

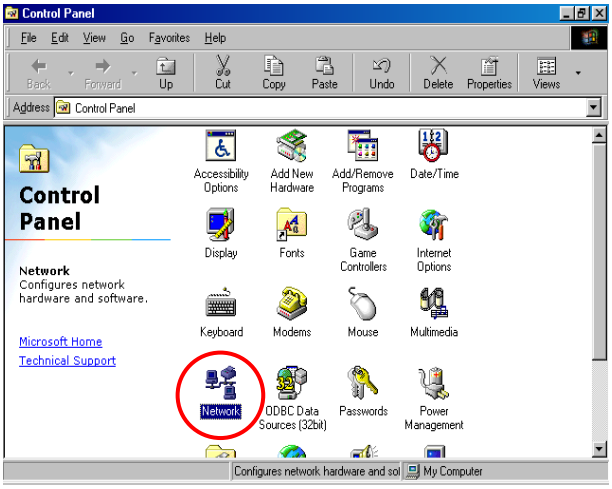
- **TCP/IP Network Setup**

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

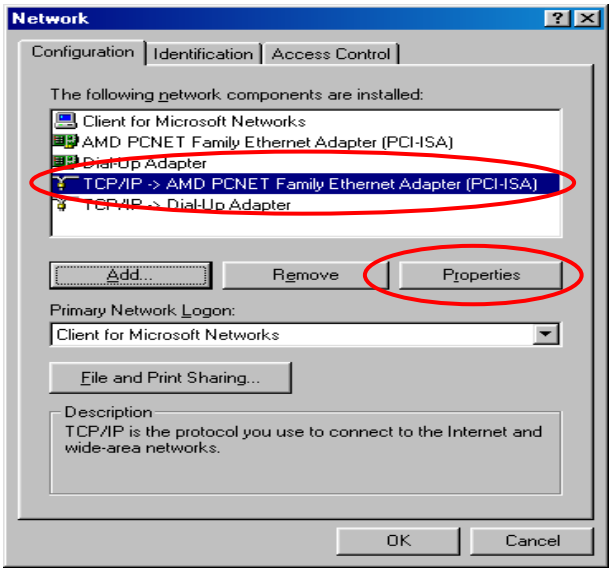
  If you want to check the TCP/IP setup or use a static IP to connect to AMG-2000 LAN port, please follow the following steps:

  ◆ **Check the TCP/IP Setup of Window 9x/ME**

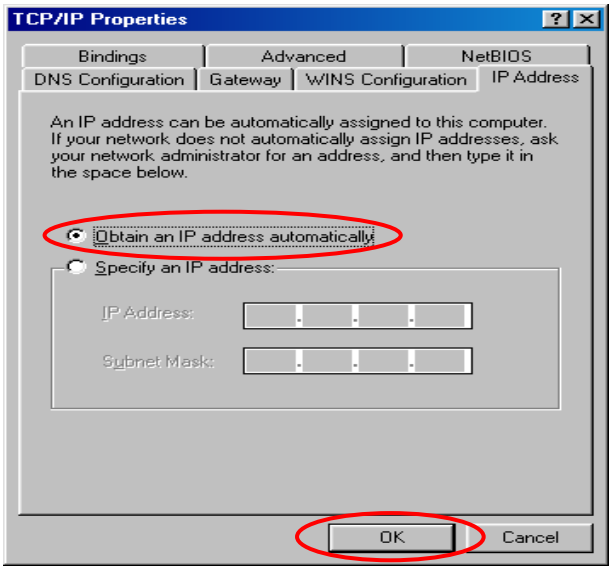
  1. Choose **Start > Control Panel > Network**.



  2. Choose **"Configuration"** label and select **"TCP/IP > AMD PCNET Family Ethernet Adapter (PCI-ISA)"**, and then click ***Properties***. Now, you can choose to use **DHCP** or **specific IP address**.

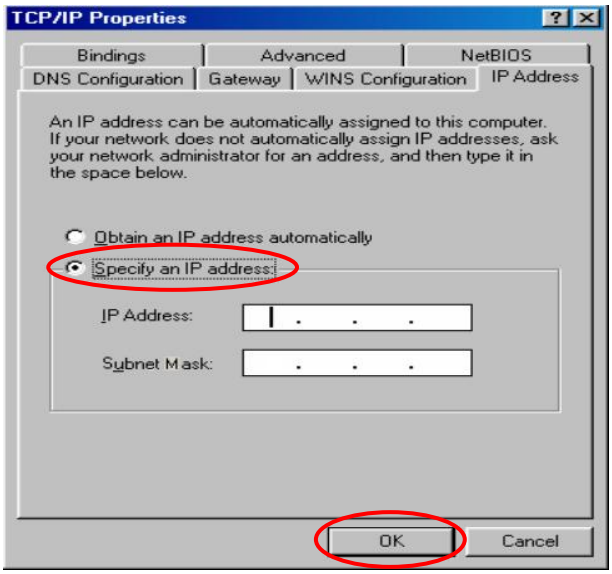


3-1. **Using DHCP:** If you want to use DHCP, please choose **"Obtain an IP address automatically"** on the **"IP Address"** label and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AMG-2000.

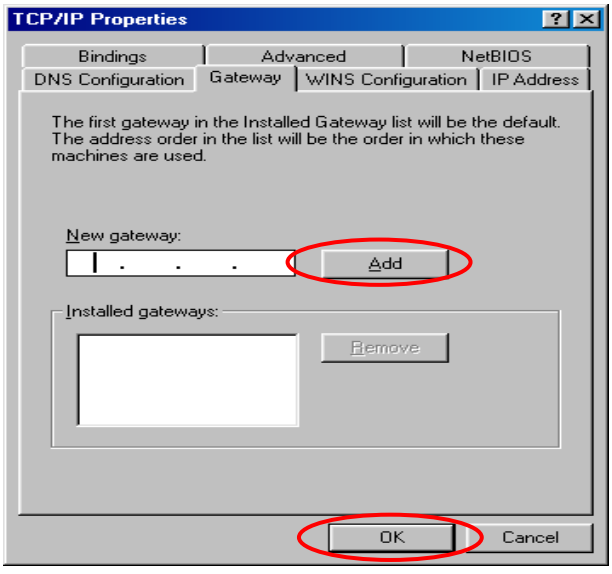


3-2. **Using Specific IP Address:** If you want to use specific IP address, you have to ask the network administrator for the information of AMG-2000: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.

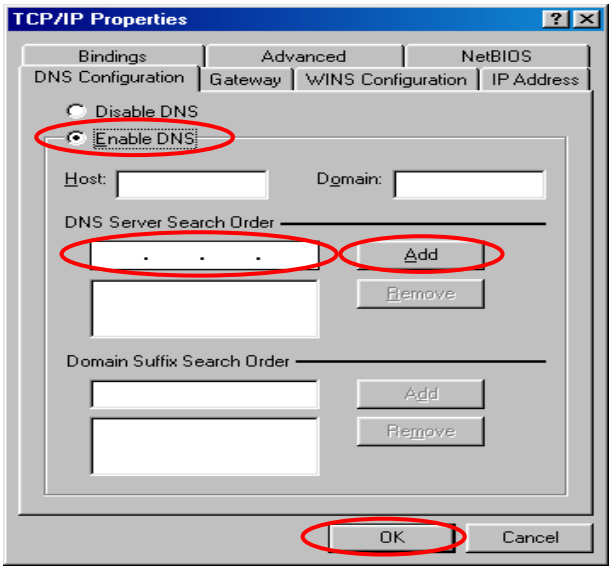
- Please choose **"Specify an IP address"** and enter the information given by the network administrator in **"IP Address"** and **"Subnet Mask"** on the **"IP Address"** label and then click ***OK***.



- Choose **"Gateway"** label and enter the gateway address of AMG-2000 in the **"New gateway:"** and then click ***Add*** and ***OK***.

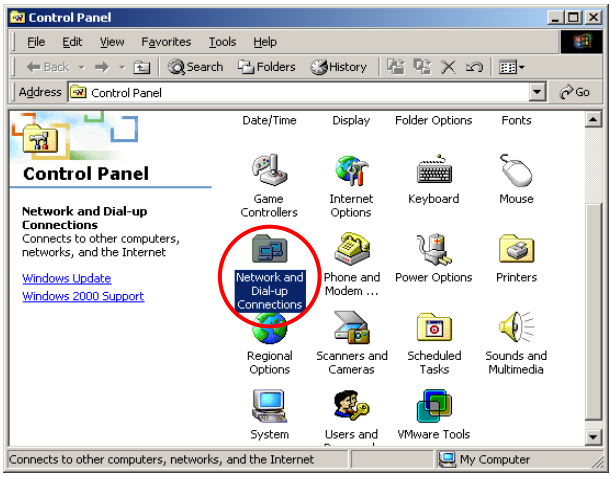


- Choose **"DNS Configuration"** label. If the DNS Server column is blank, please click ***Enable DNS*** and then enter the DNS address(es) provided by your network administrator. Then, click ***Add*** and click ***OK***.

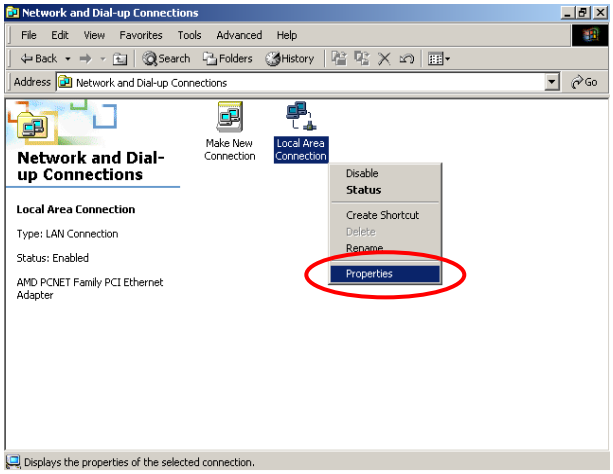


◆ **Check the TCP/IP Setup of Window 2000**

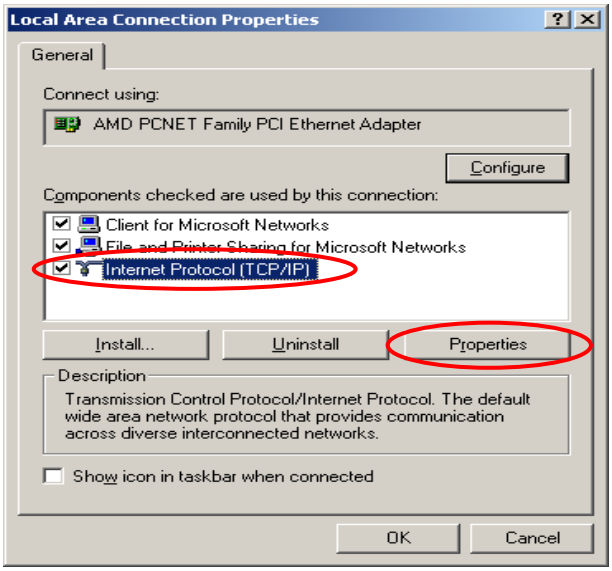
1. Select **Start > Control Panel > Network and Dial-up Connections**.



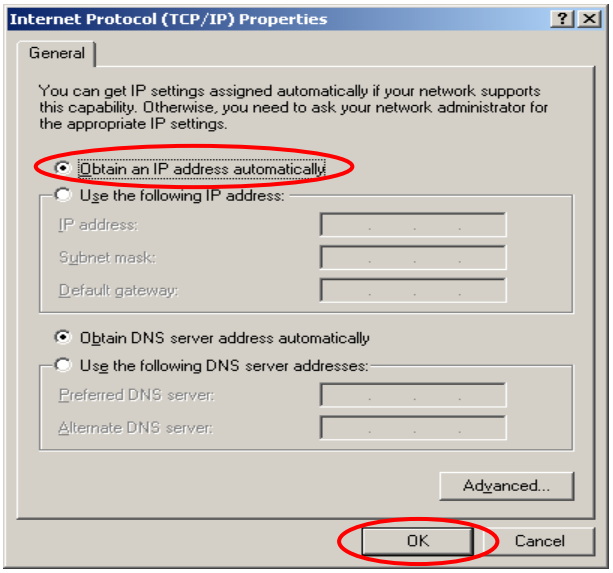
2. Click the right button of the mouse on **"Local Area Connection"** icon and then select **"Properties"**.



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

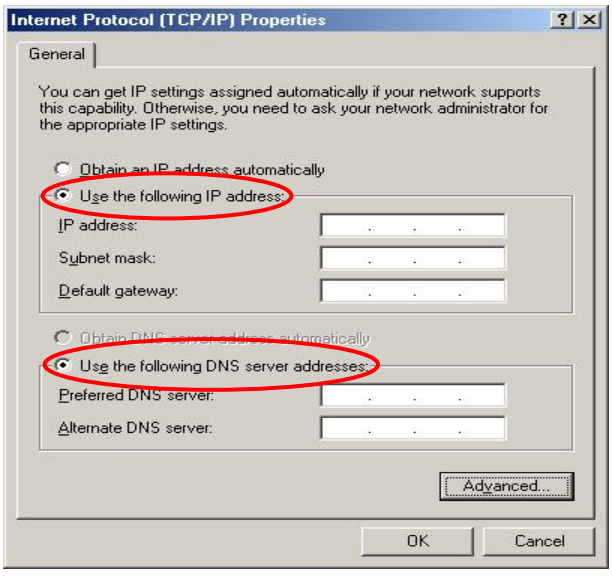


4-1. **Using DHCP:** If want to use DHCP, please choose **"Obtain an IP address automatically"** and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AMG-2000.



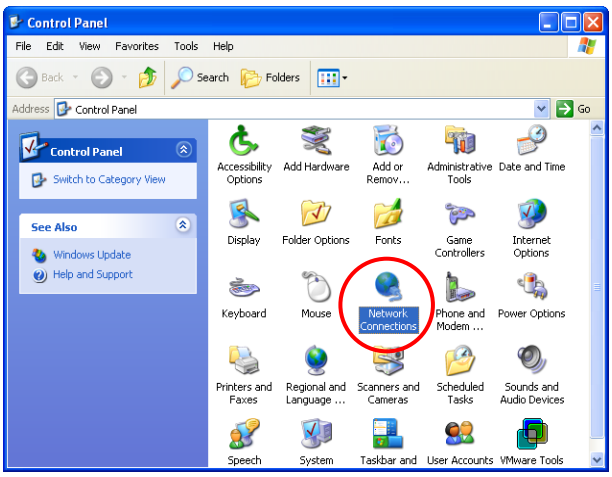
4-2. **Using Specific IP Address:** If you want to use specific IP address, you have to ask the network administrator for the information of the AMG-2000: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.

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

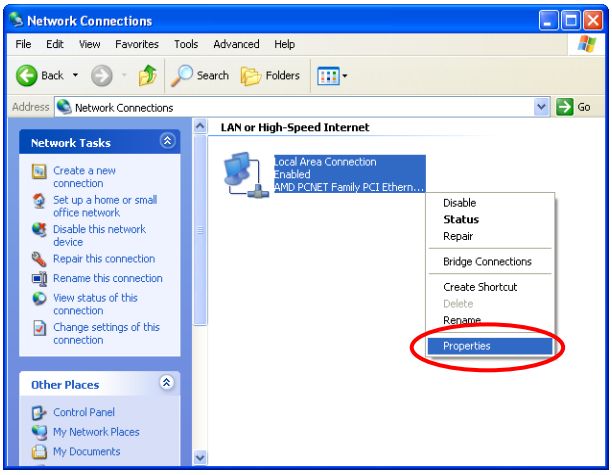


◆ **Check the TCP/IP Setup of Window XP**

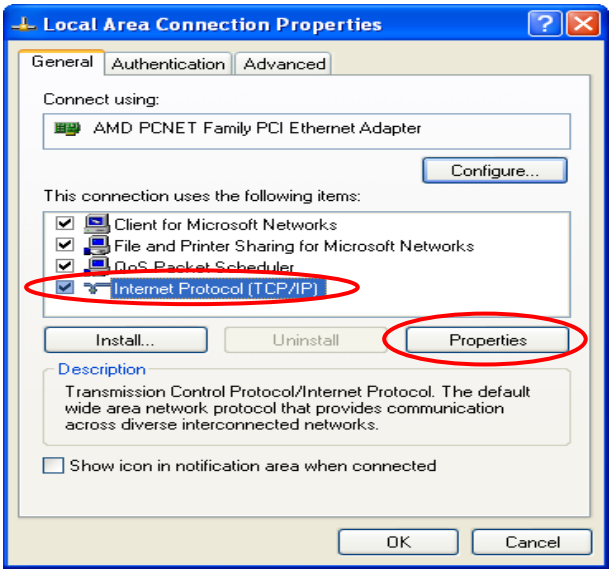
1. Select **Start > Control Panel > Network Connection**.



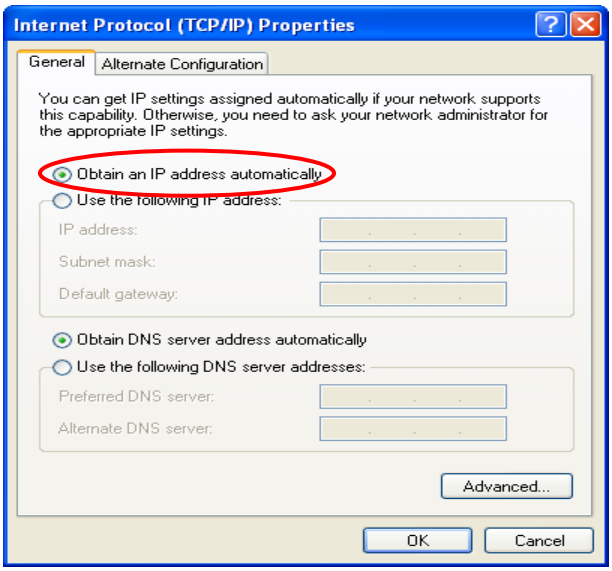
2. Click the right button of the mouse on the **"Local Area Connection"** icon and select **"Properties"**



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

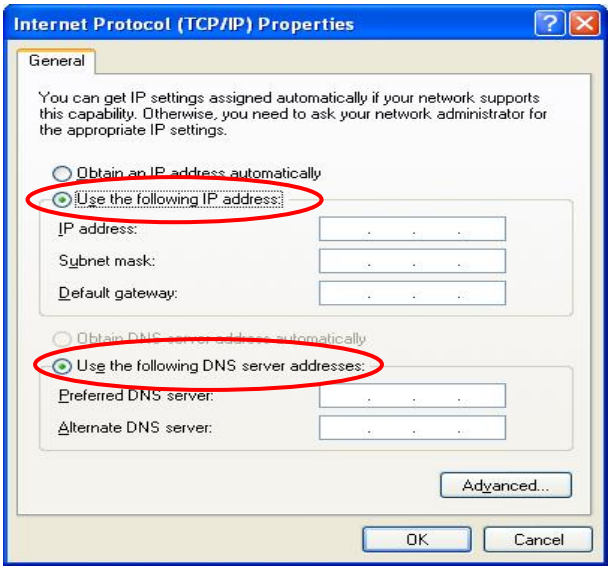


3-1. **Using DHCP:** If want to use DHCP, please choose **"Obtain an IP address automatically"** and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AMG-2000.



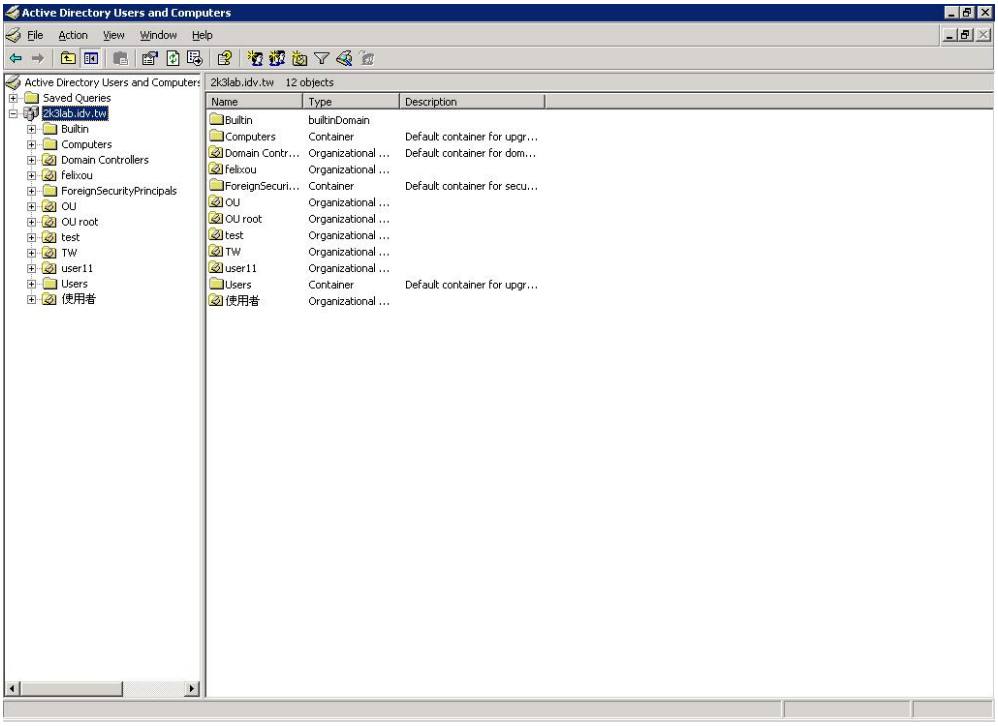
3-2. **Using Specific IP Address:** If want to use specific IP address, you have to ask the network administrator for the information of the AMG-2000: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.

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

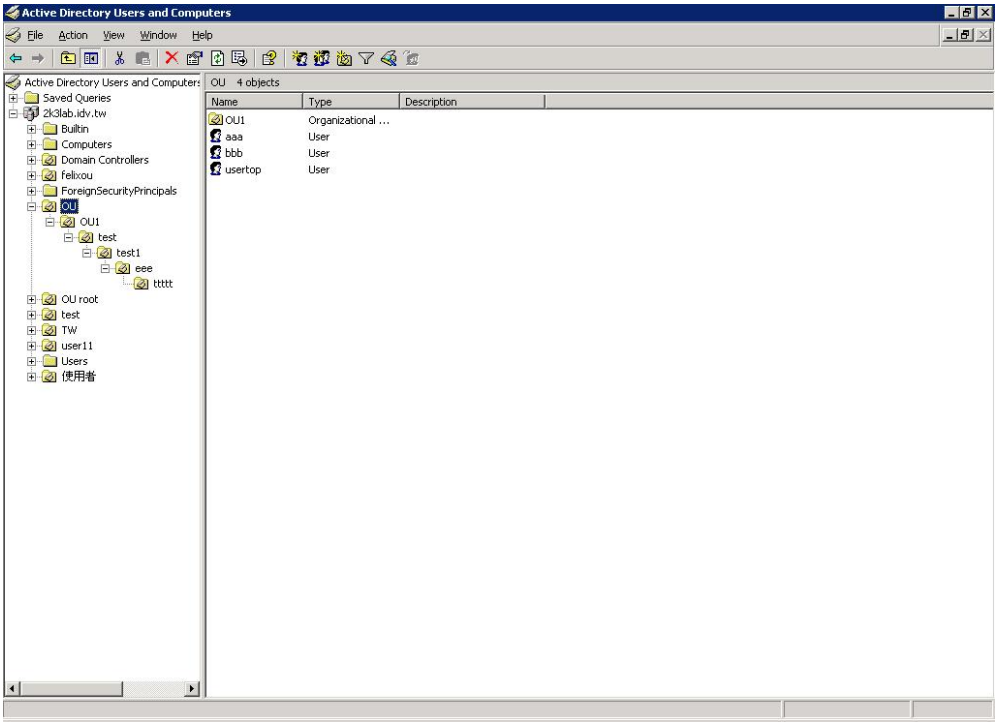


Appendix C. Windows Server

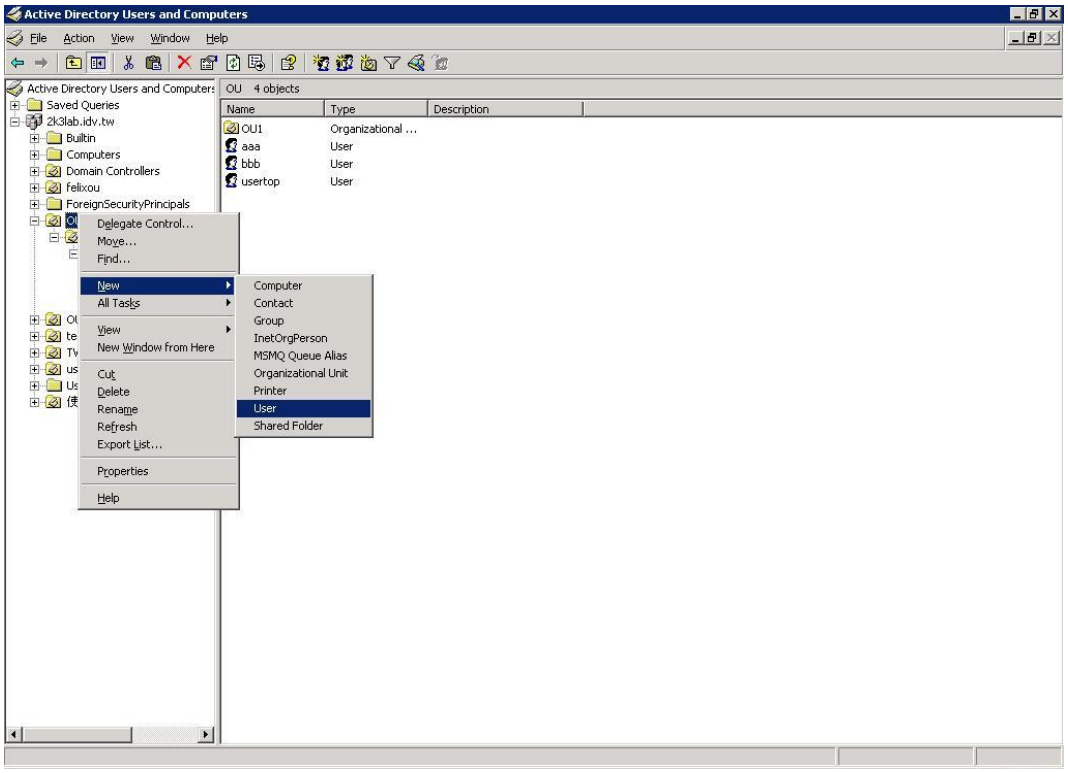
AD environment mode can be supported by AMG-2000. For example, the domain, 2k3lab.idv.tw, is controlled by Window 2000/2003 sever and please make sure you have enabled the Active directory Service on the Windows Server.



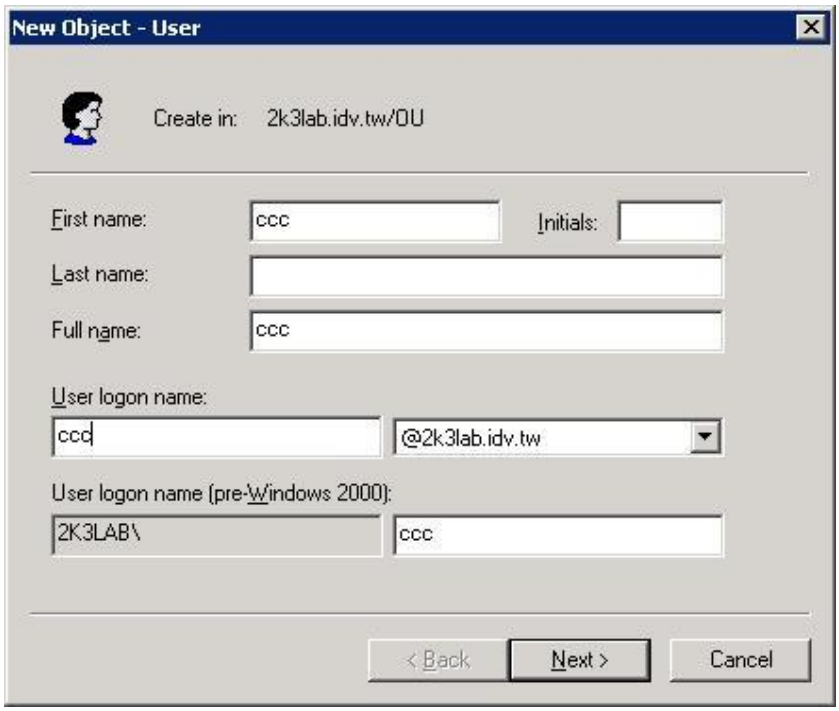
When the AMG-2000 is set up, Windows Server should be also ready by the MIS in your company. Then, you can add new user and group under the OU.



Right-click on the OU to add a new user. ***OU→New→User***.

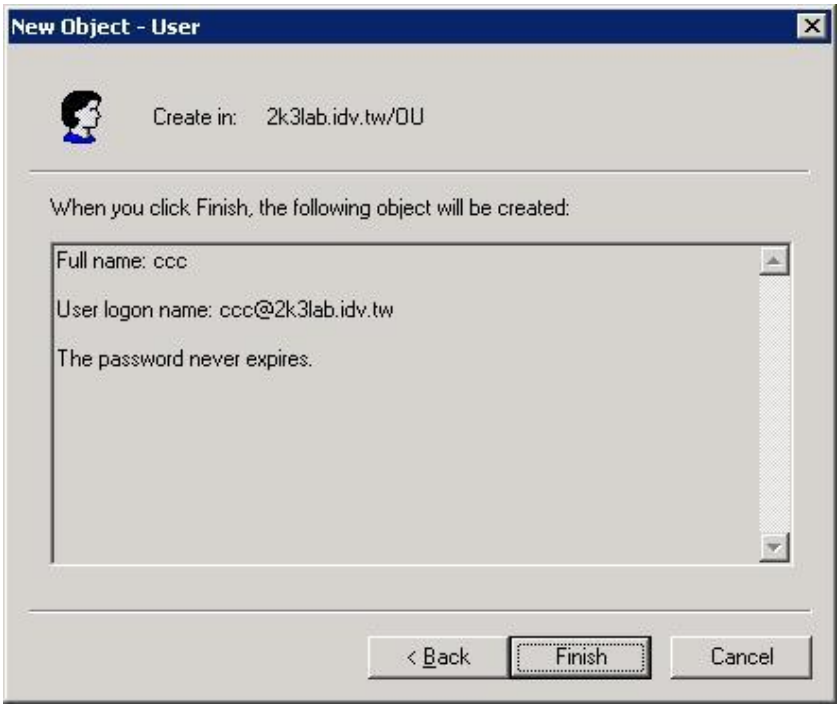


Enter the user name in the necessary fields, ***"First name"*** and "***User logon name"***, and click ***Next***.

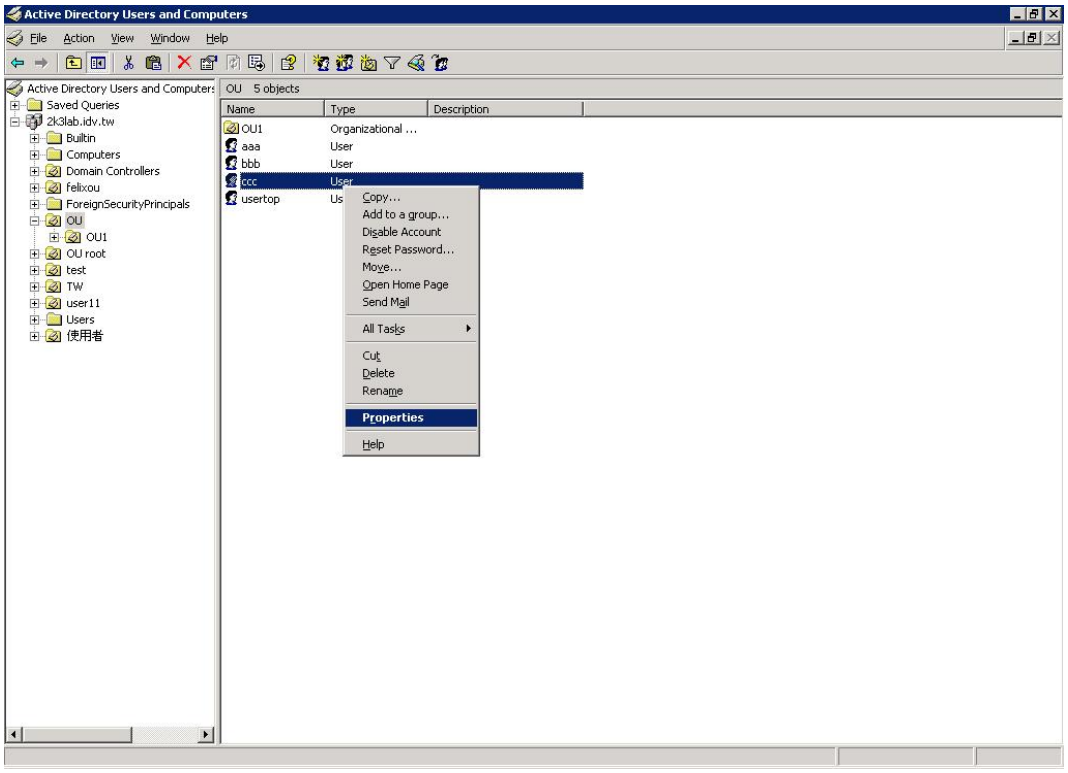


Enter the Password and enter it again for confirmation. The password must be six characters or more. Depend on the request to check the four selections below. .Then, click the ***Next***.

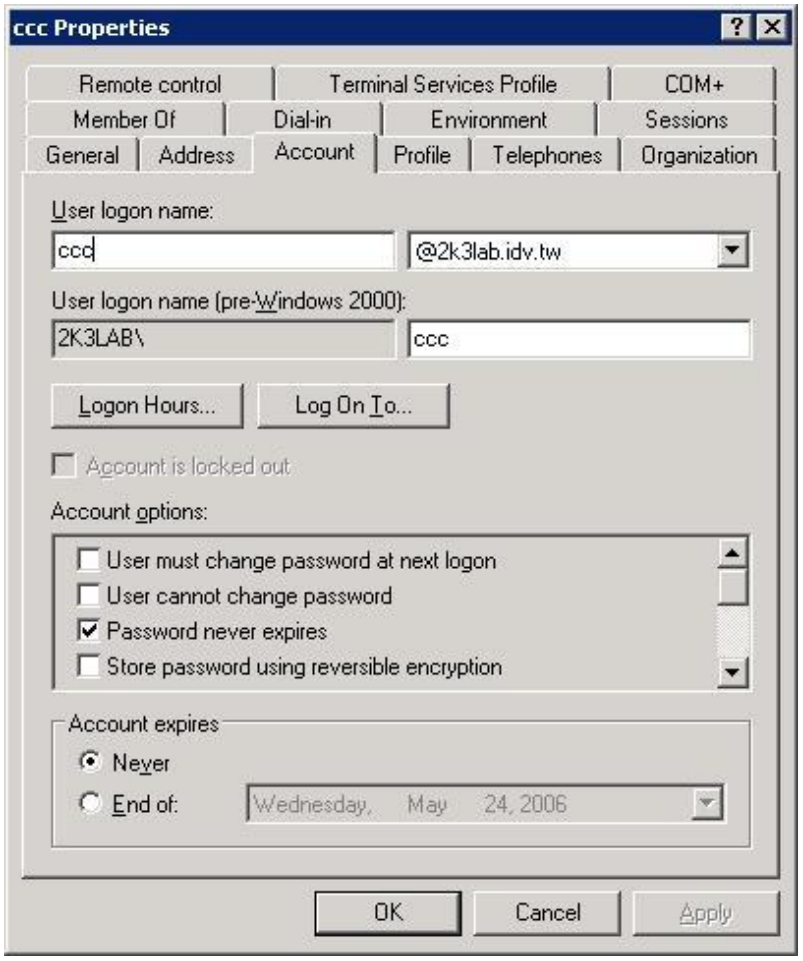
The new user, ***ccc***, is created successfully under the OU.



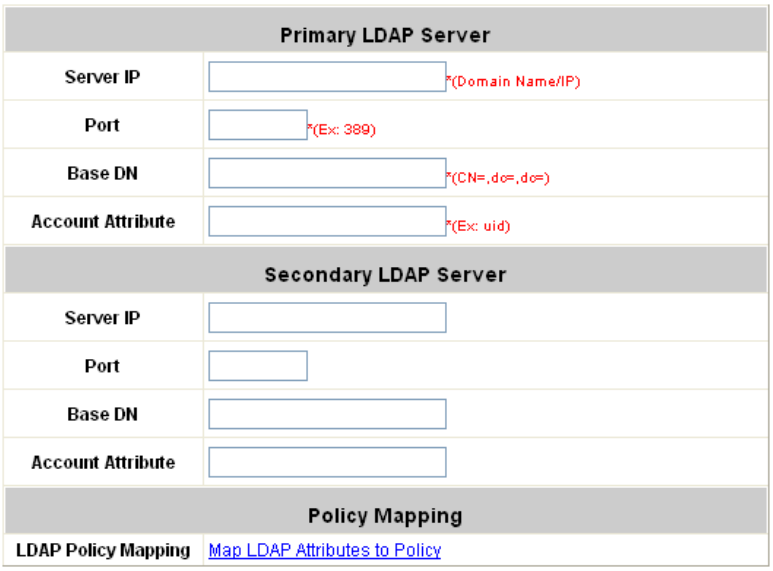
Right-click on ccc to view the properties. ***ccc→Properties***.



Click the ***Account*** label and you will see the account information about ccc.



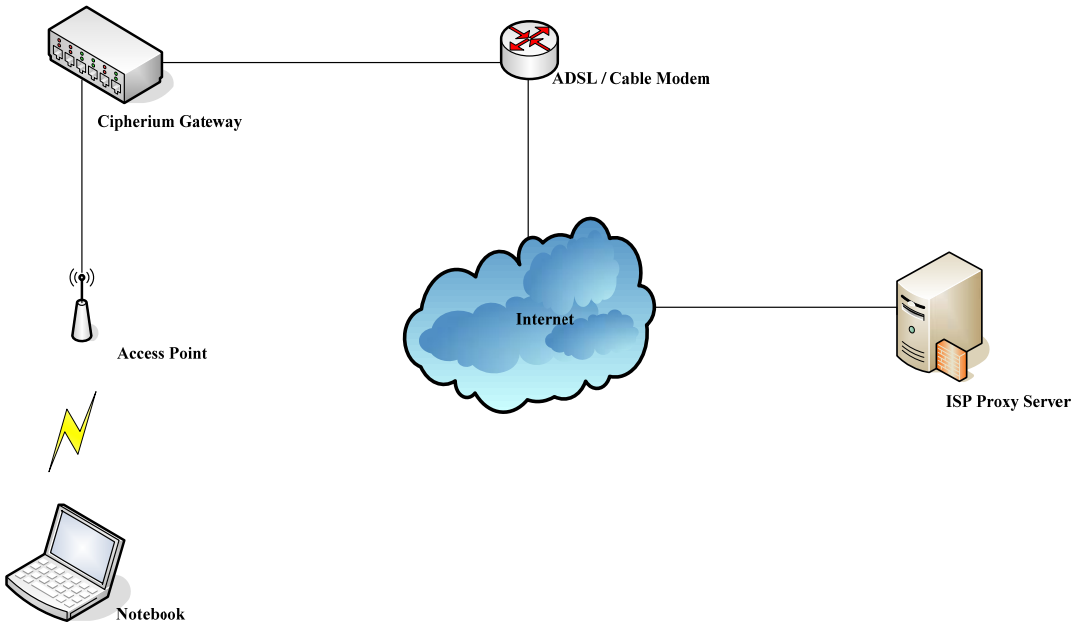
Then, you can get the information to fill in the fields of LDAP Server. For example, ***Server IP: www.2k3lab.idv.tw***; ***Port: 389***; ***Base DN: ou=OU,dc=2k3lab,dc=idv,dc=tw***; ***Account Attribute: CN***



Note: *Usually, the users are created under the* ***CN=users****, and the Base DN will be* ***"CN=users,dc=2k3lab,dc=idv,dc=tw"****. The Account Attribute of Windows Server will only be* ***CN*** *and that of Linux could be* ***CN*** *or* ***uid****.*

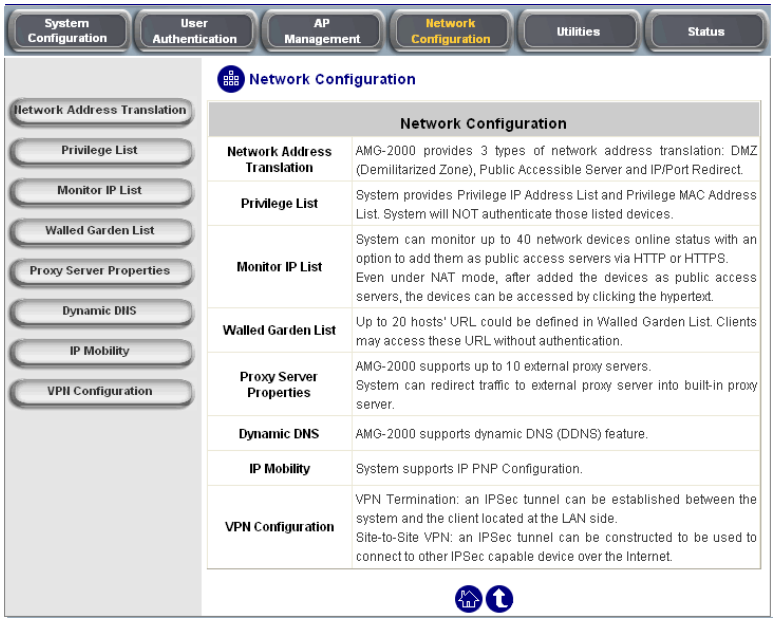
Appendix D. Proxy Setting for Hotspot

HotSpot is a place such as coffee shops, hotels, or other public areas where provide Wi-Fi service for mobility users. HotSpot is usually implemented without complex network architecture and using some proxy server which provide by Internet Service Providers.

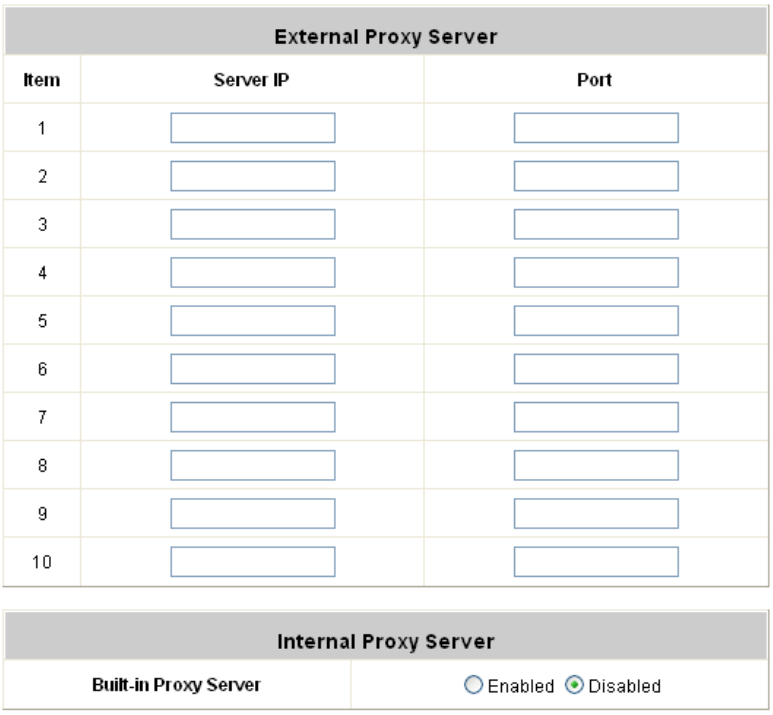


In Hotspots, mobility users usually enable their proxy setting of the browsers such as IE, Firefox, or the others, so we need to set some proxy configuration in the Gateway. Please follow the steps to complete the proxy configuration：

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



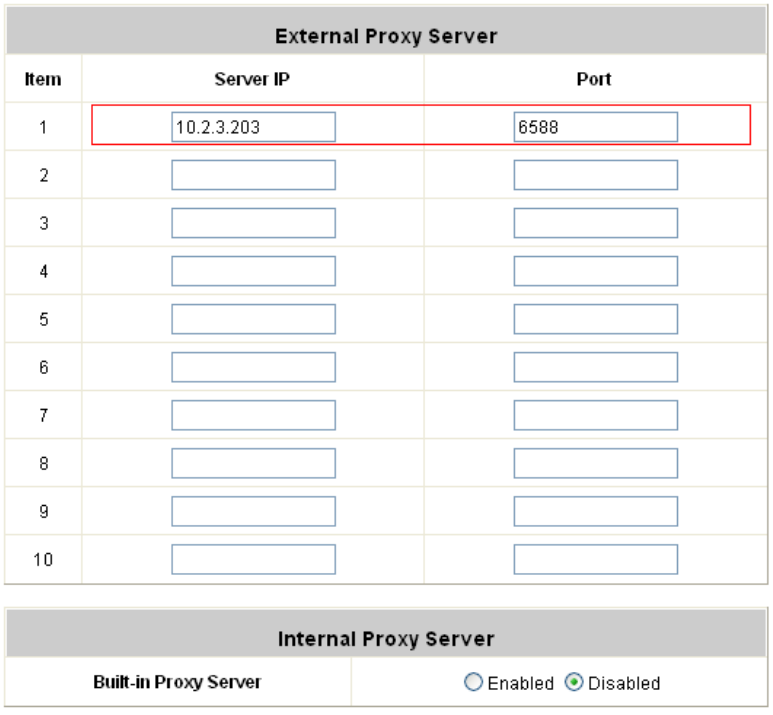
3) Click the ***Proxy Server Properties*** from left menu and the homepage of the **Proxy Server Properties** will appear.



External Proxy Server		
Item	Server IP	Port
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server	
Built-in Proxy Server	○ Enabled ◉ Disabled

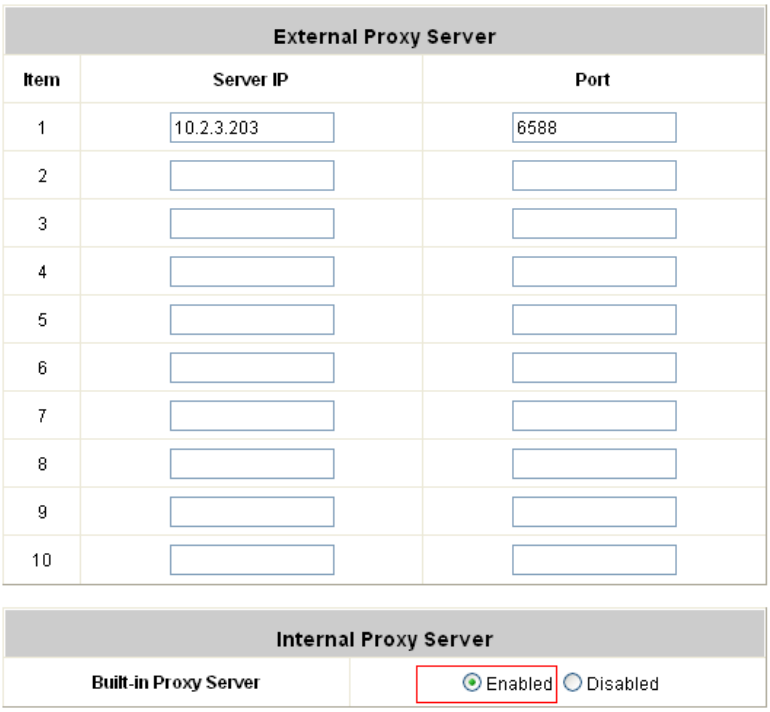
4) Add your ISP's proxy Server IP and Port into ***External Proxy Server*** Setting.



External Proxy Server		
Item	Server IP	Port
1	10.2.3.203	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server	
Built-in Proxy Server	○ Enabled ◉ Disabled

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



External Proxy Server

Item	Server IP	Port
1	10.2.3.203	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		

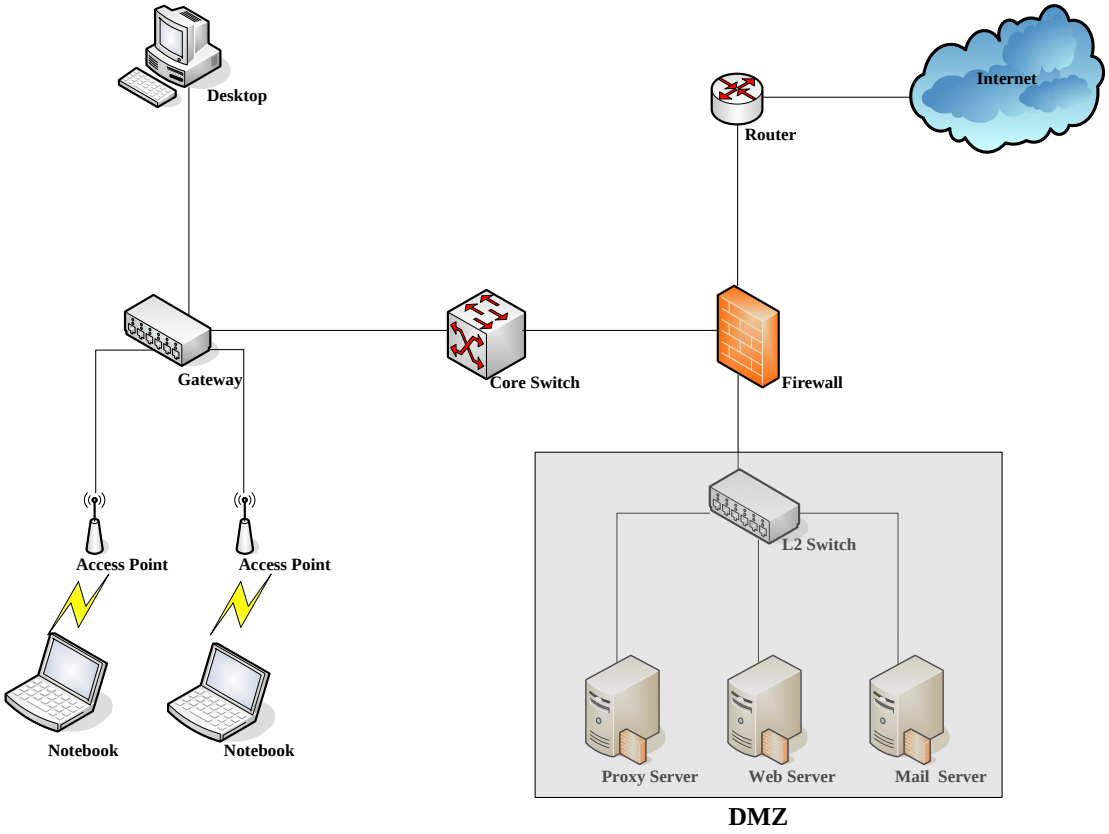
Internal Proxy Server

Built-in Proxy Server	(•) Enabled ( ) Disabled

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

Appendix E. Proxy Setting for Enterprise

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



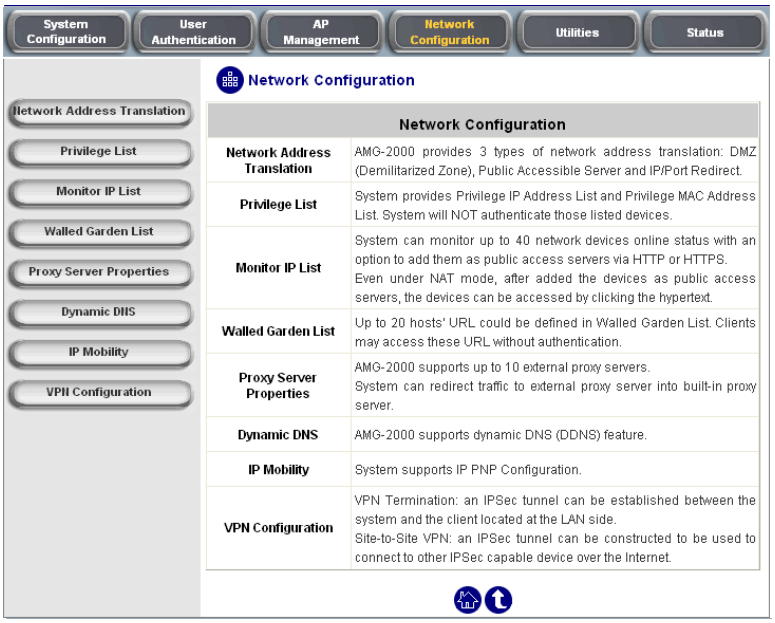
In enterprises, network manager or MIS maybe usually ask their users to enable their proxy setting of the browsers such as IE, Firefox, or others to reduce the internet access loading, so we need to set some proxy configuration in the Gateway.

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 proxy setting of browsers, and you don't need to set any proxy configuration in the Gateway.

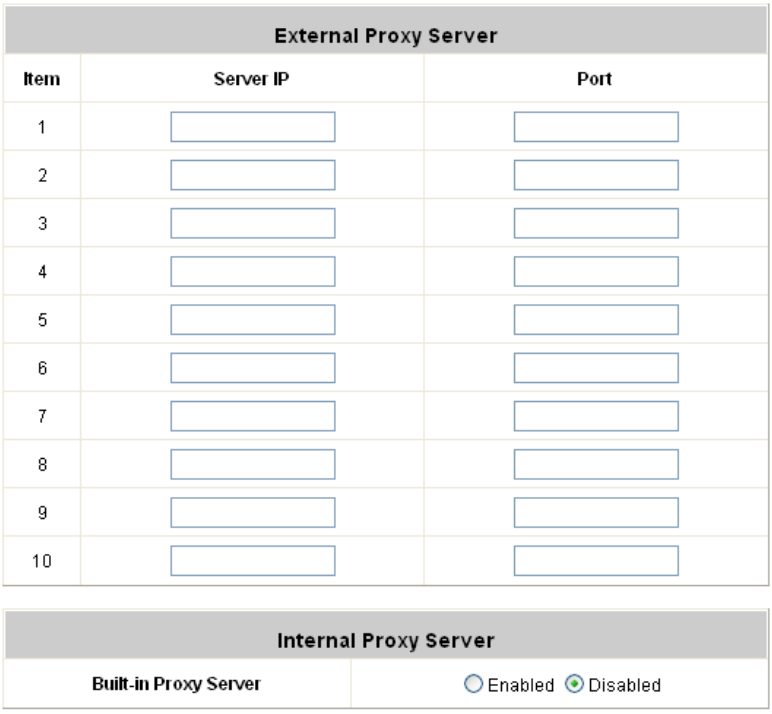
Please follow the steps to complete the proxy configuration：

1. Gateway setting

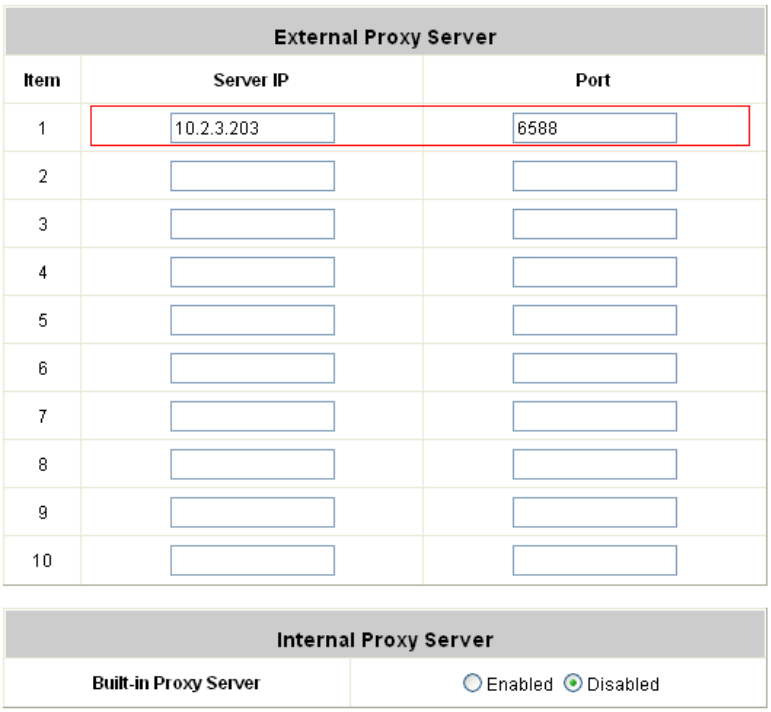
1) Login Gateway by using "***admin***".
2) Click the ***Network Configuration from top menu*** and the homepage of the ***Network Configuration*** will appear.



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



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



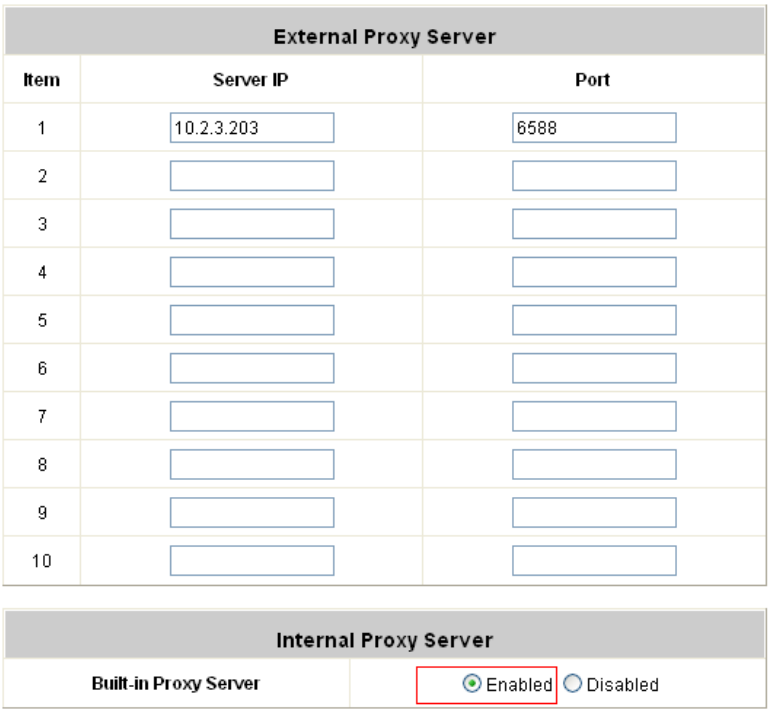
External Proxy Server

Item	Server IP	Port
1	10.2.3.203	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server

Built-in Proxy Server	○ Enabled ◉ Disabled

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



External Proxy Server

Item	Server IP	Port
1	10.2.3.203	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server

Built-in Proxy Server	◉ Enabled ○ Disabled

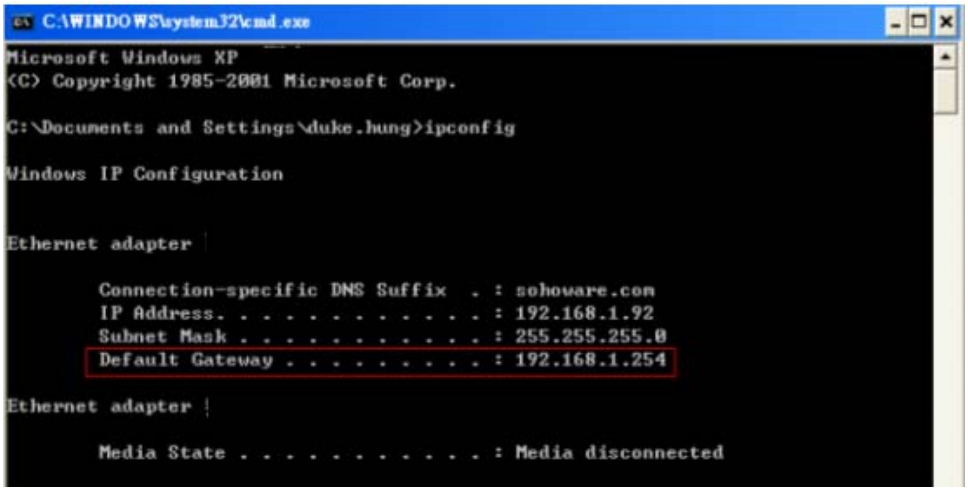
6) Click ***Apply*** to save the settings***.***

Warning：If your proxy server is down, 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.

2. Client setting

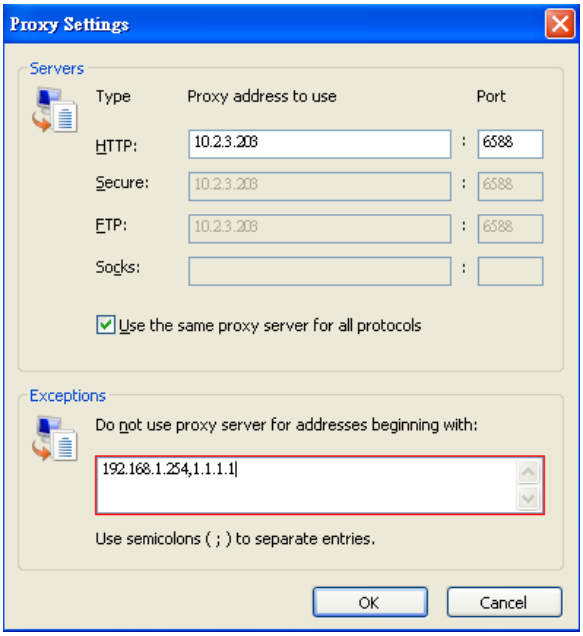
It is necessary for clients to add default gateway IP address into proxy exception information. By the way, user login successful page will appear normally.

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

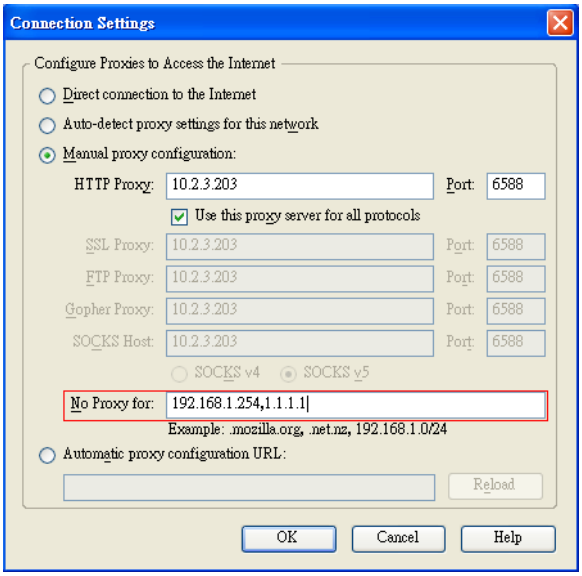


2) Open browser to add ***default gateway IP address (e.g. 192.168.1.254)*** and ***logout page IP address "1.1.1.1"*** into proxy exception information.

- **For IE**



- **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

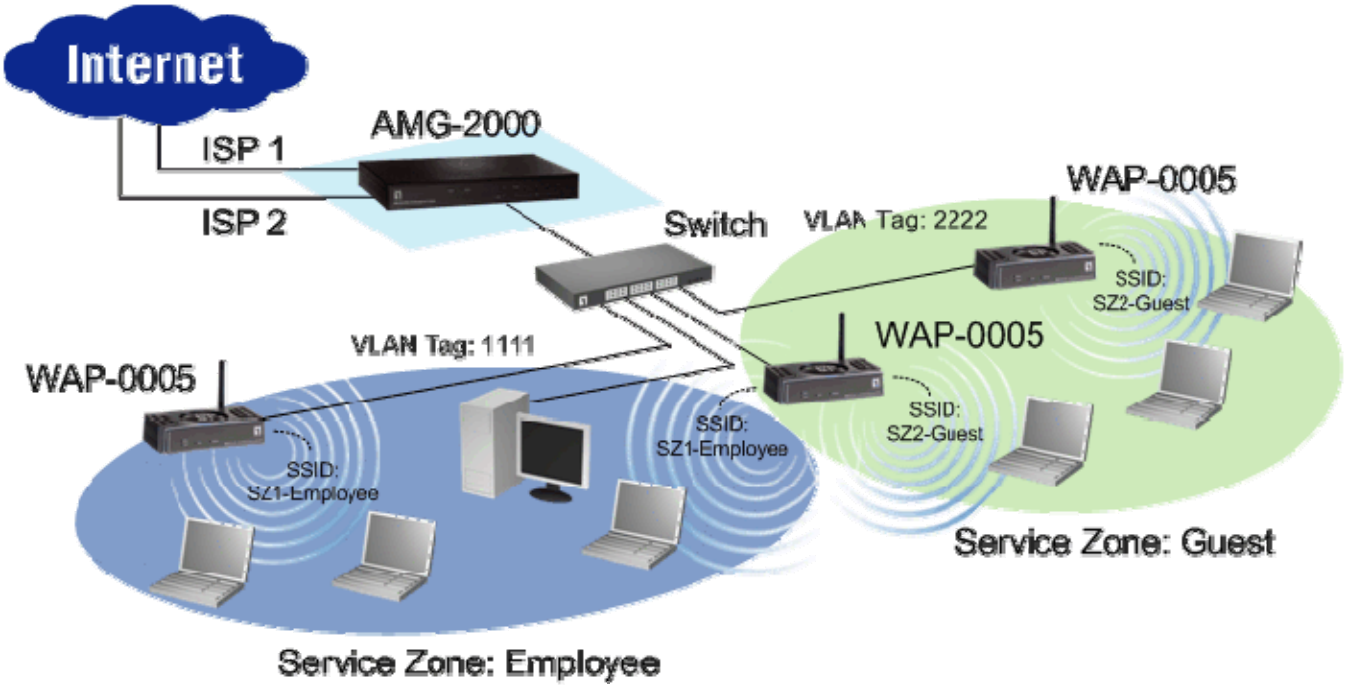
Appendix F. Service Zones – A Deployment Example

- **Typical Application Scenario: Employee vs. Guest**

  In this scenario, users are separated into **Employee** and **Guest** for the purpose of different levels of access control.

- **Application Network Diagram**

  One Service Zone (associated with VLAN tag: 1111 and SSID: SZ1-Employee) is set up for employees while the other Service Zone (associated with VLAN tag: 2222 and SSID: SZ1-Guest) is set up for guests.

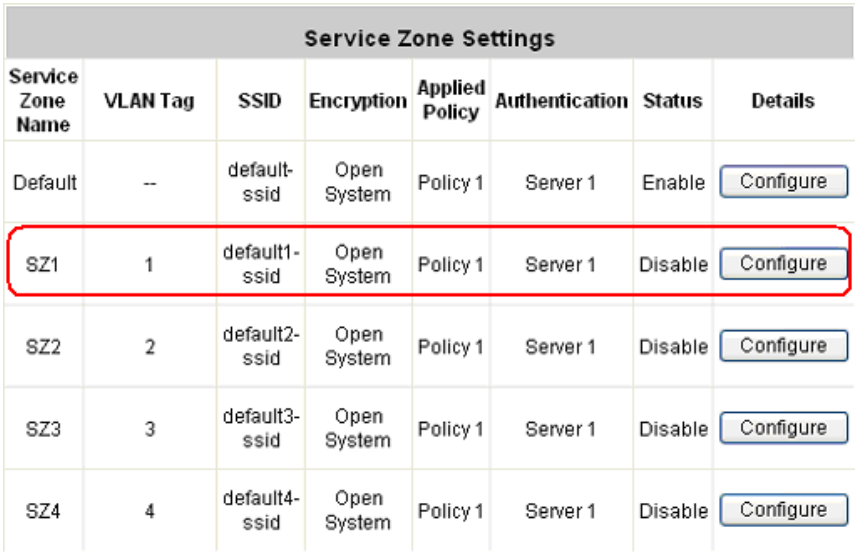


- **Requirements for the Application Scenario**

  1. No matter where they stay in the office, all users should be divided into two groups (**Employee** and **Guest**).
  2. Each Service Zone must setup its own **SSID** to let users to access the wireless network using the specific SSID. The system will give a unique Session ID to authenticated users when they start new sessions.
  3. Both groups of **Employee** and **Guest** will be redirected to different login portal pages and will be authenticated against different authentication database.
  4. Apply different access control policies to seperated groups **Employee** and **Guest**.

▪ Solution and Configuration in AMG-2000

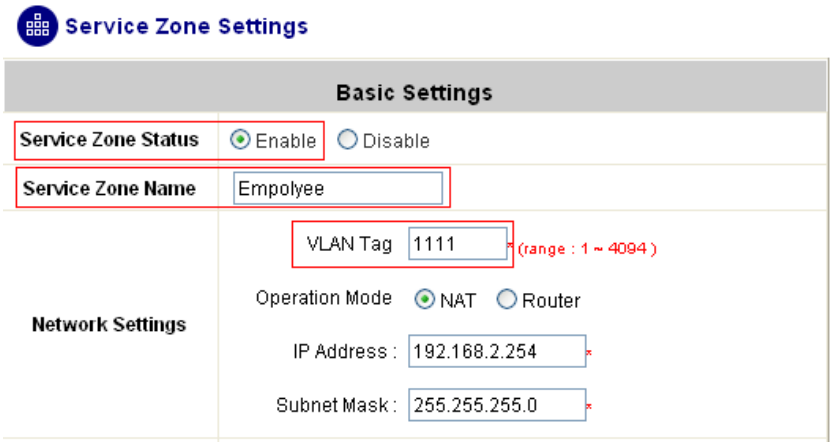
1) Choose the SZ1 for the **Employee** group (Take **Employee** for an example of Service Zone configuration)



Service Zone Settings

Service Zone Name	VLAN Tag	SSID	Encryption	Applied Policy	Authentication	Status	Details
Default	--	default-ssid	Open System	Policy 1	Server 1	Enable	Configure
SZ1	1	default1-ssid	Open System	Policy 1	Server 1	Disable	Configure
SZ2	2	default2-ssid	Open System	Policy 1	Server 1	Disable	Configure
SZ3	3	default3-ssid	Open System	Policy 1	Server 1	Disable	Configure
SZ4	4	default4-ssid	Open System	Policy 1	Server 1	Disable	Configure

2) Enable the **Service Zone** and set up other basic information

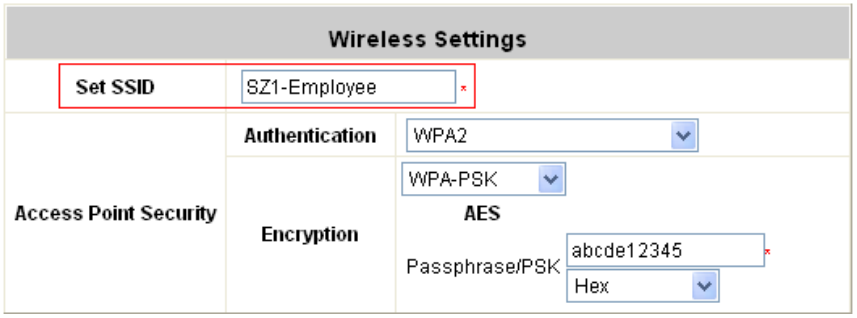


Service Zone Settings

Basic Settings

Service Zone Status	Enable / Disable
Service Zone Name	Empolyee
Network Settings	VLAN Tag 1111 * (range : 1 ~ 4094)
	Operation Mode NAT / Router
	IP Address : 192.168.2.254 *
	Subnet Mask : 255.255.255.0 *

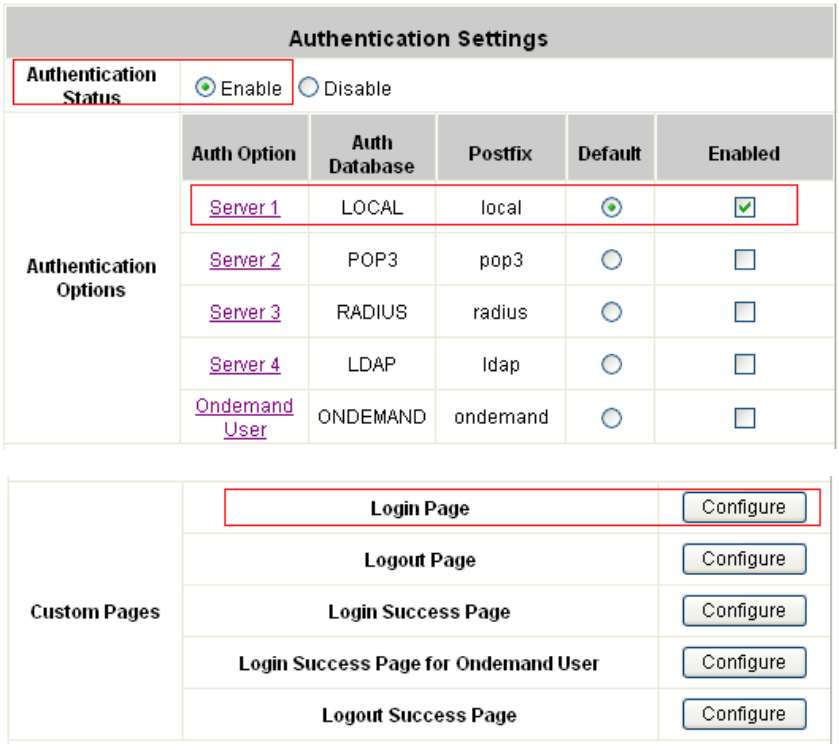
3) Configure the **SSID** and other settings which will be applied to the managed APs in this Service Zone



Wireless Settings

Set SSID	SZ1-Employee *	
Access Point Security	Authentication	WPA2
	Encryption	WPA-PSK AES Passphrase/PSK abcde12345 * Hex

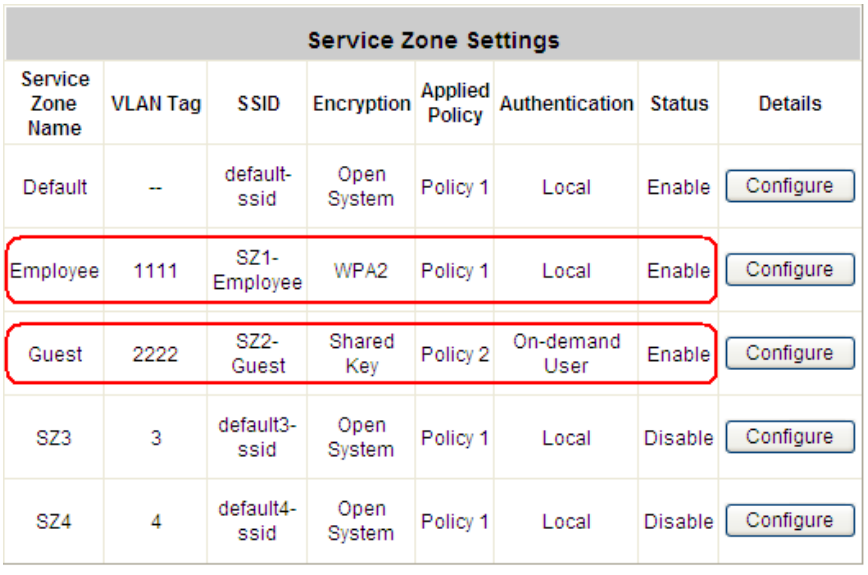
4) Enable the Authentication Status, select the Default Authentication Option and configure the login page



5) Choose the appropriate Policy which will be applied to this **Service Zone**

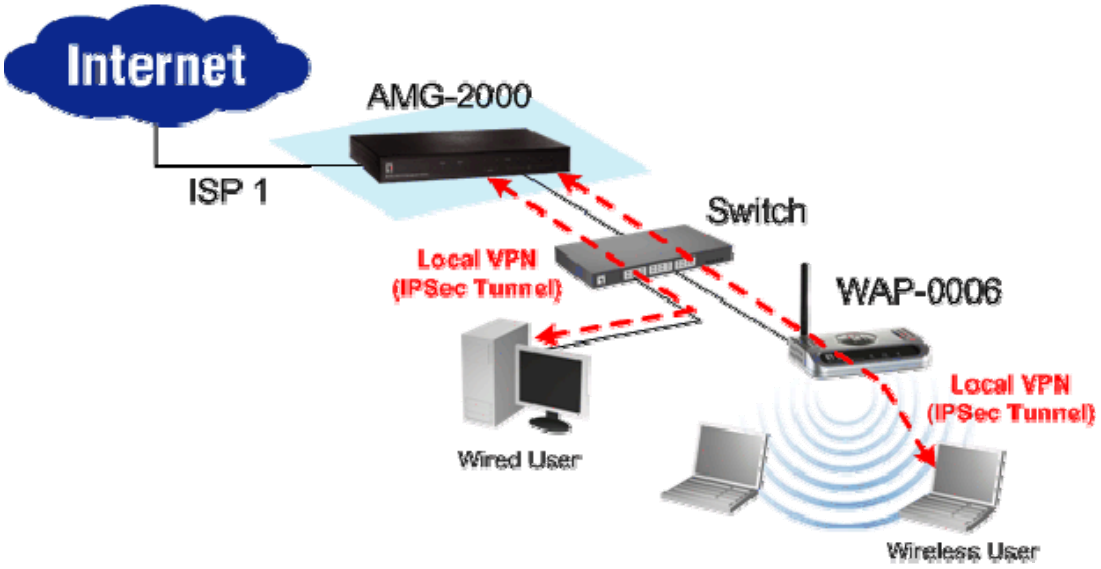
- **Finished Configuration – Service Zone Settings**

The table will summarize the current configuration and status for each Service Zone:



Appendix G. Local VPN User Configuration

AMG-2000 has the ability to establish IPSec VPN tunnels between local user's Windows devices (on local wired or wireless network) and AMG-2000 itself, for the purpose of traffic protection on local networks. By pushing down ActiveX Control to the user's browser from AMG-2000, the system will be able to install a so-called "clientless" IPSec VPN.

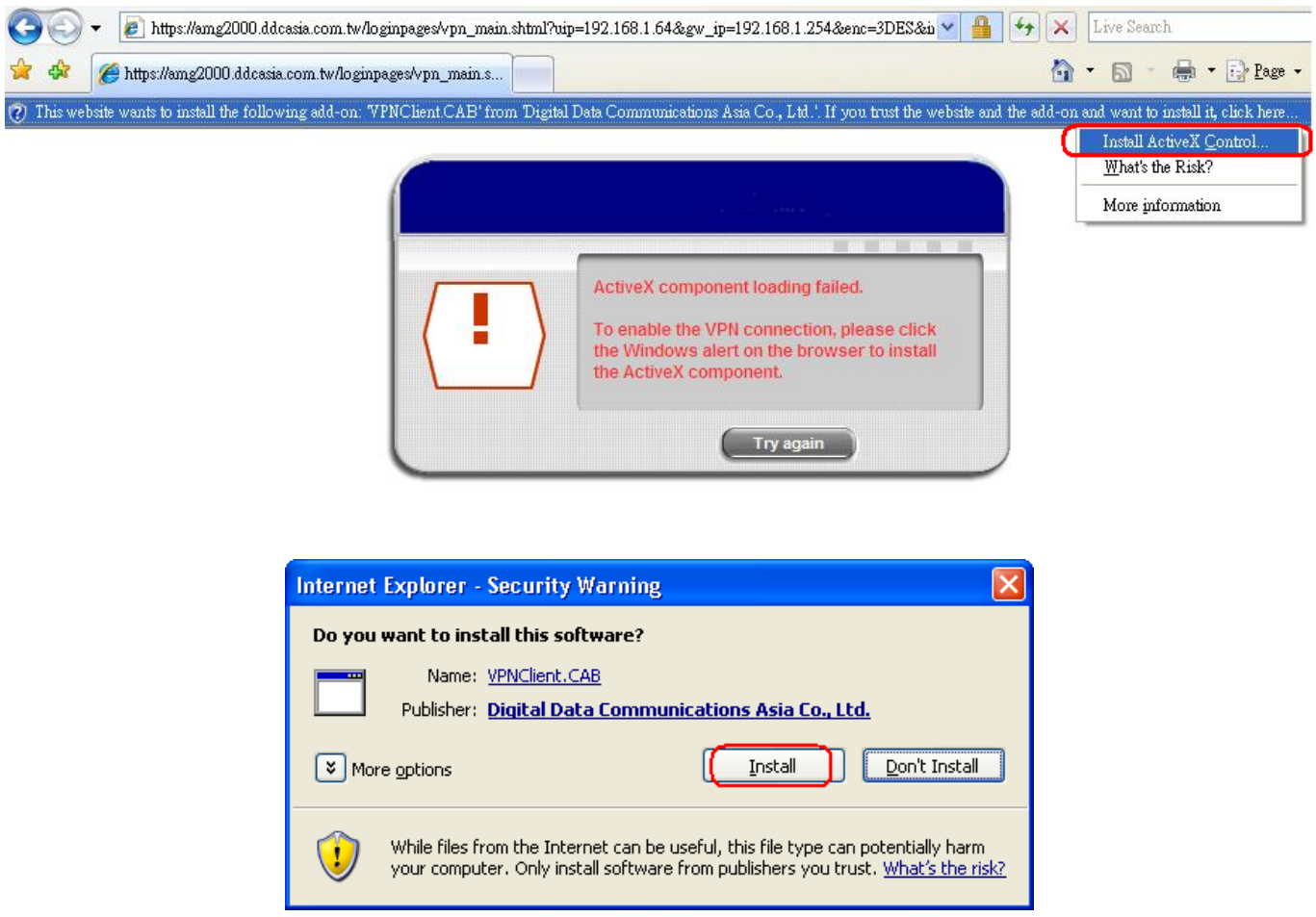


1. User Operation Flow

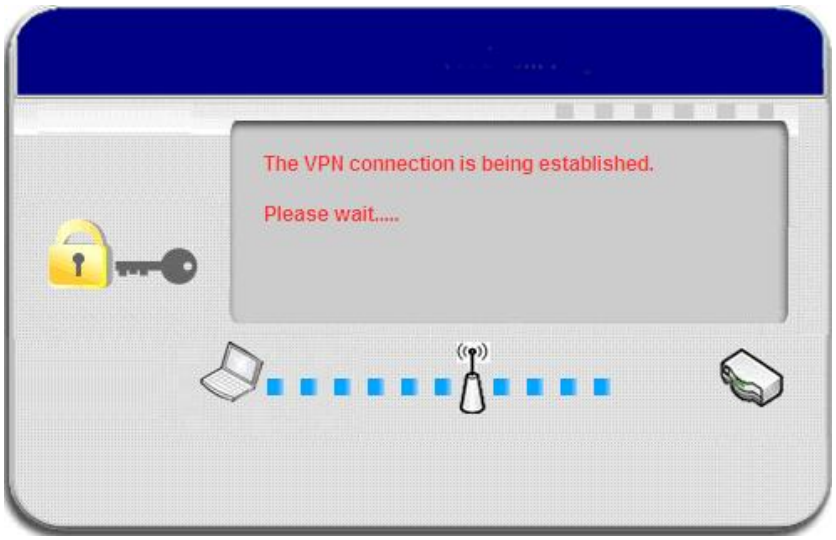
1) As usual, type in username and password in the User Login Page

2) For the first time, if the user has never used Local VPN feature, Windows IE browser (6.0 or above) will display an alert message to ask the user whether she or he wants to install the "add-on" software.

3) Click on the alert message and then choose the "Install ActiveX Control" to install the software.



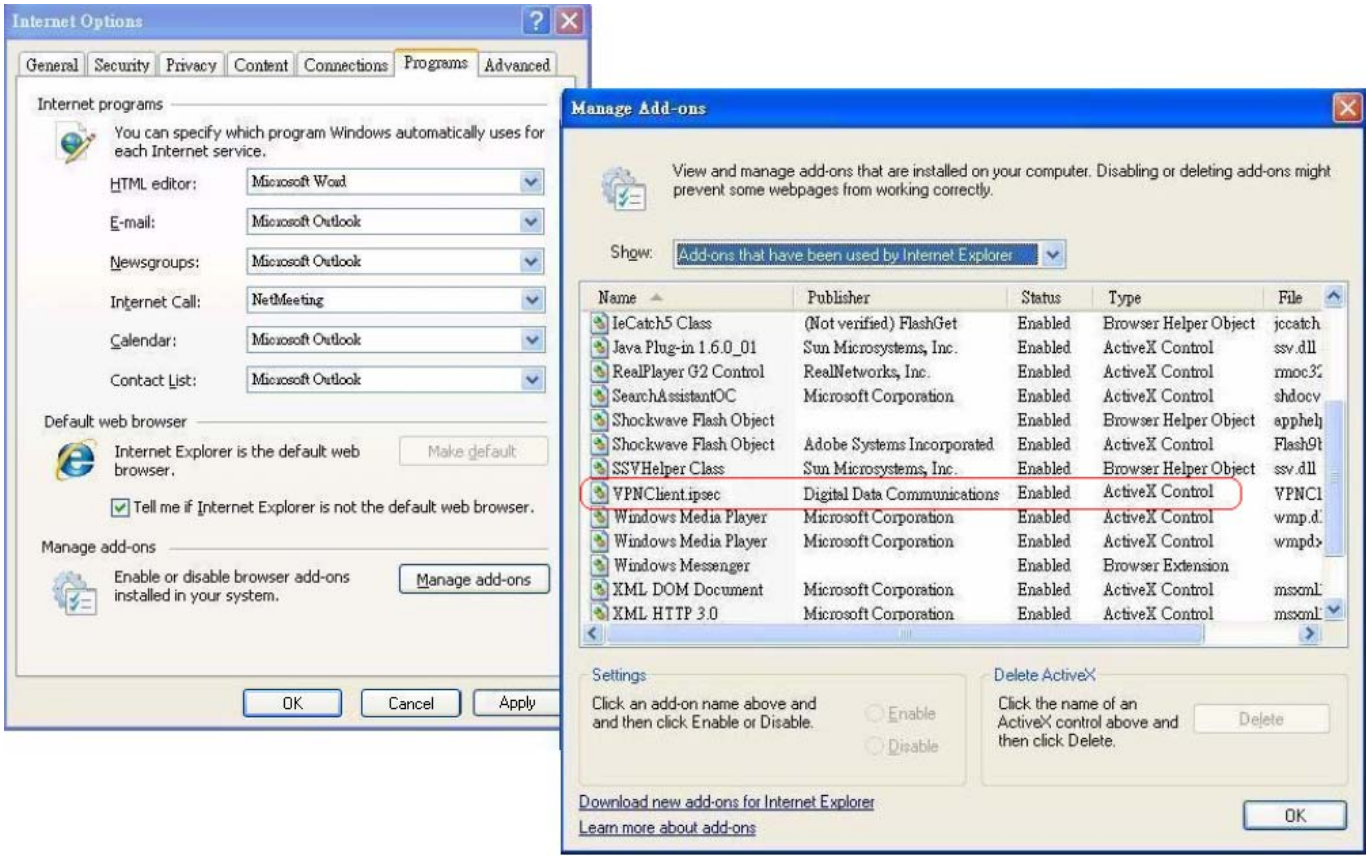
4) After the software is installed well, the system will try to establish the IPSec VPN tunnel for the user automatically.



5) Once the IPSec VPN tunnel is established, the user has successfully logged in and the connection is secured by IPSec VPN.

2. ActiveX Control component

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



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

3. Limitations

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

a. Internet Connection Firewall of Windows XP or Windows XP SP1 is not compatible with IPSec protocol. It shall be turned off to allow IPSec packets to pass through.

b. Without Windows patch KB889527, ICMP (Ping) and PORT command of FTP cannot work in Windows XP SP2.

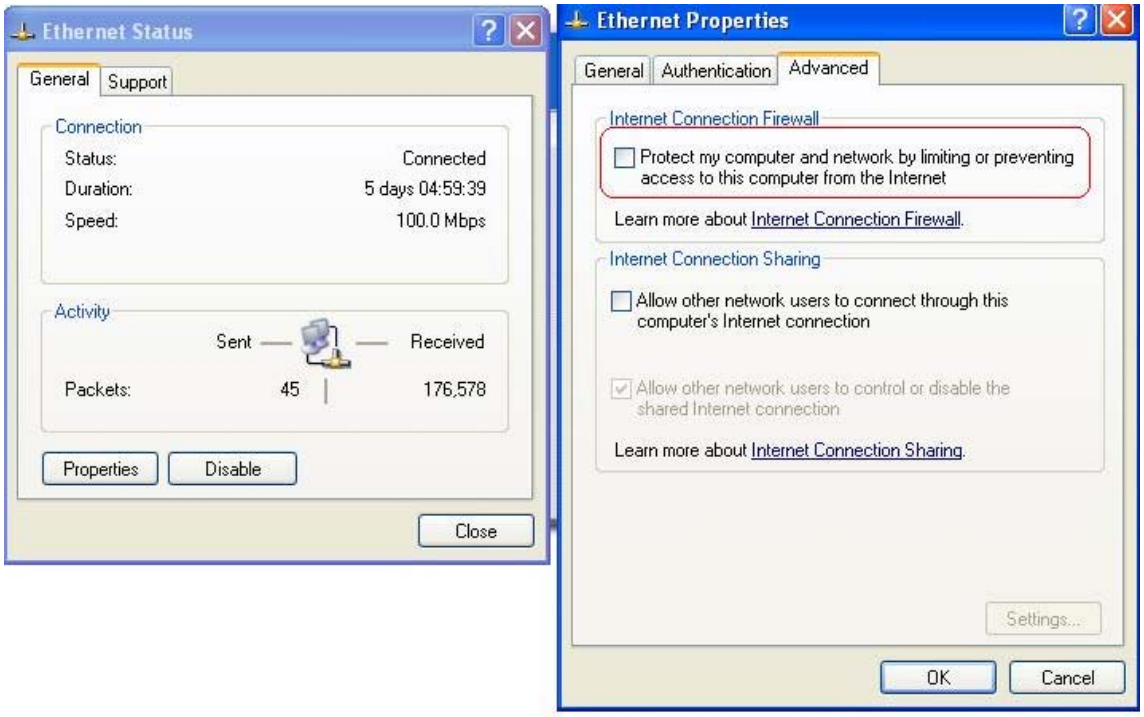
c. The forced termination (through CTRL+ALT+DEL or Task Manager) of the Internet Explorer will stop the running of ActiveX. It causes IPSec tunnel can't be cleared properly at client's device. In this case, a reboot of client's device is needed to clear the IPSec tunnel.

d. The crash of Windows Internet Explorer may cause the same result.

e. There are some OS and browser which may not support Local VPN.

a) Internet Connection Firewall

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



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

b) ICMP and Active Mode FTP

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

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

c) The Termination of ActiveX

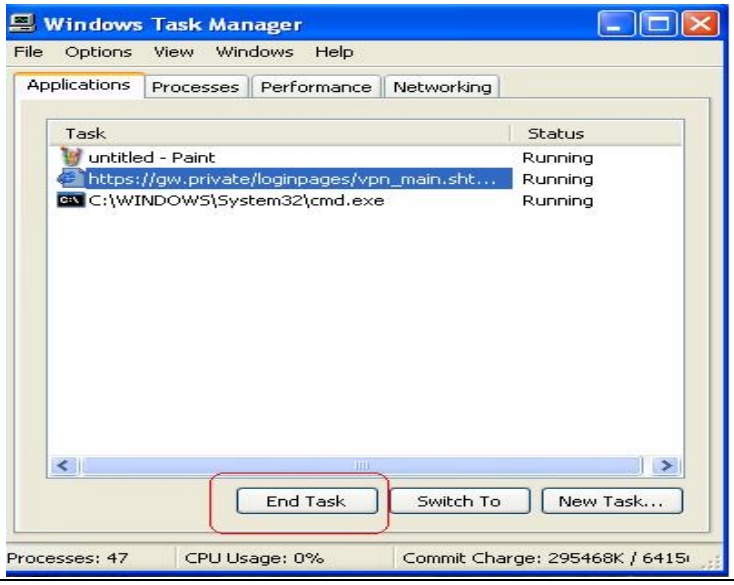
The ActiveX component for IPSec VPN is running paralleled with the web page of "Login Success". Unless user decides to close the session and to disconnect with AMG-2000, the following conditions or behaviors of using browser shall be avoided in order to maintain the built IPSec VPN tunnel always alive.

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

The crash of Internet Explorer on running ActiveX

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

Terminate the Internet Explorer Task from Windows Task Manager



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

There are some cases of Windows messages by which AMG-2000 will warn current user to:

(1) Close the Windows Internet Explorer,

(2) Click "logout" button on "login success" page,

(3) Click "back" or "refresh" of the same Internet Explorer,

(4) Enter new URL in the same Internet Explorer,

(5) Open a URL from the other application (e.g. email of Outlook) that occupies this existing Internet Explorer.

That shall all cause the termination of IPSec VPN tunneling if user chooses to click "Yes". The user has

to log in again to regain the network access.

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

e) Non-supported OS and Browser

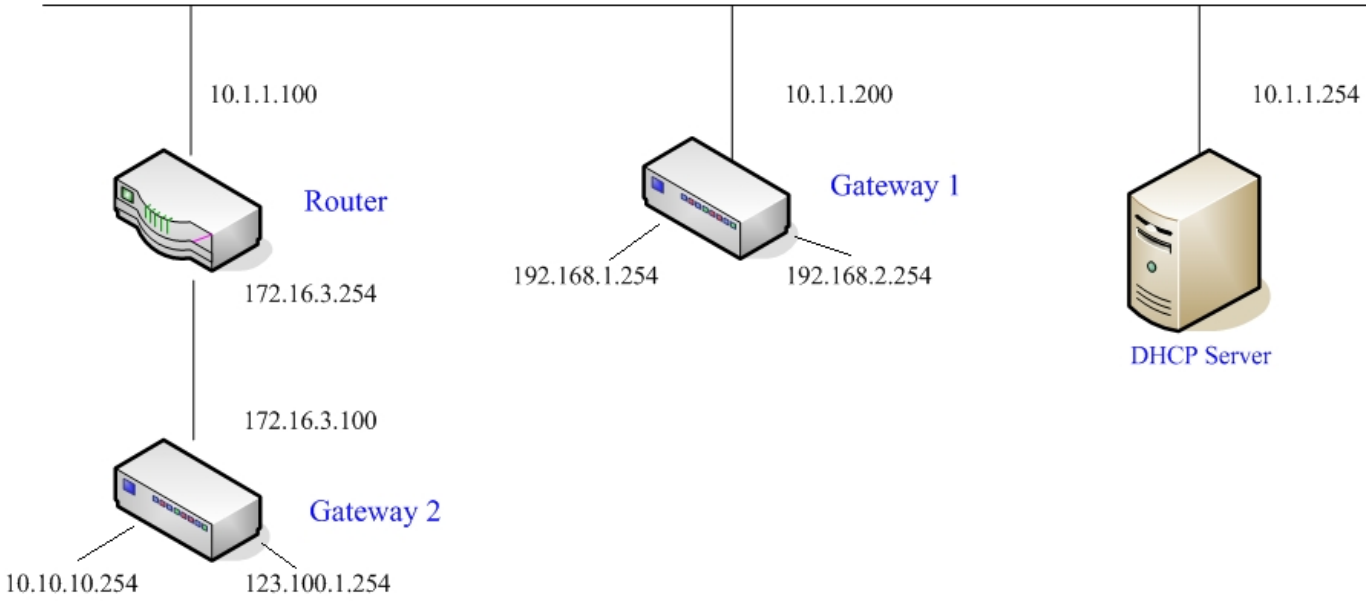
In current version, Windows Internet Explorer (6.0 or above) is the only browser supported by AMG-2000.

Windows XP and Windows 2000 are the only two supported OS along with this release.

Appendix H. DHCP Relay

AMG-2000 supports DHCP Relay defined according to RFC 3046 . For scaling reasons, it is advantageous to set up an external DHCP server other than having the internal DHCP server implemented in AMG-2000 to assign an IP. When forwarding client-originated DHCP packets to a DHCP server, a new option called the "Relay Agent Information option" is inserted by the DHCP relay agent. External DHCP servers that recognize the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies. The external DHCP server then echoes the option back to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

A graphic example of connecting 2 gateways with an external DHCP server:



Please note that the Router and Gateway 1 connected to the DHCP Server have to be under the same network segment as DHCP Server.

When a client requests IP address from Gateway 1 Public LAN through the build-in DHCP relay agent of AMG-2000, the DHCP server will receive a DHCP REQUEST packet with Option 82 (a code defined in RFC 3046). Also a Circuit ID will be sent by AMG-2000 when DHCP relay is enabled to define where the packet is sent from, and this Circuit ID should have a format of MAC_IP, such as 00:E0:22:DF:AC:DF_192.168.1.254. Therefore, when the external DHCP server gets the request packet, it knows where to reply to and which IP to assign.

Here is an example of configuration file of the DHCP server:

```
class "g1_public_lan" {
        match if option agent.circuit-id = "00:90:0B:07:60:91_192.168.1.254";
}

class "g1_private_lan" {
        match if option agent.circuit-id = "00:90:0B:07:60:92_192.168.2.254";
}

class "g2_public_lan" {
        match if option agent.circuit-id = "00:12:43:AD:32:F2_10.10.10.254";
}

class "g2_private_lan" {
        match if option agent.circuit-id = "00:12:43:AD:32:F2_123.100.1.254";
}

subnet 0.0.0.0 netmask 0.0.0.0 {

        option domain-name-servers      168.95.1.1;

        pool {
                allow members of "g1_public_lan";
                range 192.168.1.30 192.168.1.50;
                option routers 192.168.1.254;
                option subnet-mask 255.255.255.0;
        }

        pool {
                allow members of "g1_private_lan";
                range 192.168.2.30 192.168.2.50;
                option routers 192.168.2.254;
                option subnet-mask 255.255.255.0;
        }
```

From the file, client that connects to AMG-2000 sends out a DHCP request. DHCP relay function in AMG-2000 is enabled and sending a Circuit ID 00:90:0B:07:60:91_192.168.1.254 to the external DHCP server. When DHCP server gets the Circuit ID, it recognizes that the request is sent from g1_public_lan and thus assigns the client a DNS server of 169.95.1.1, an IP that can be in the range of 192.168.1.30 and 192.168.1.50, a default gateway of 192.168.1.254, and a subnet-mask of 255.255.255.0.

P/N: V20020070430