



AMG-2000

AP Management Gateway

User Manual

Table of Contents

| | |
|---|-----------|
| 1. BEFORE YOU START | 1 |
| 1.1. PREFACE | 1 |
| 1.2. DOCUMENT CONVENTION | 1 |
| 2. SYSTEM OVERVIEW | 2 |
| 2.1. INTRODUCTION | 2 |
| 2.2. SYSTEM CONCEPT | 3 |
| 2.3. SPECIFICATION | 4 |
| 2.1.1 <i>Hardware Specification</i> | 4 |
| 2.1.2 <i>Technical Specification</i> | 4 |
| 3. BASE INSTALLATION | 7 |
| 3.1. HARDWARE INSTALLATION | 7 |
| 3.1.1 <i>System Requirements</i> | 7 |
| 3.1.2 <i>Package Contents</i> | 7 |
| 3.1.3 <i>Panel Function Descriptions</i> | 8 |
| 3.1.4 <i>Installation Steps</i> | 9 |
| 3.2. SOFTWARE CONFIGURATION | 10 |
| 3.2.1 <i>Quick Configuration</i> | 10 |
| 3.2.2 <i>User Login Portal Page</i> | 18 |
| 4. WEB INTERFACE CONFIGURATION | 20 |
| 4.1. SYSTEM CONFIGURATION | 21 |
| 4.1.1 <i>Configuration Wizard</i> | 21 |
| 4.1.2 <i>System Information</i> | 22 |
| 4.1.3 <i>WAN1 Configuration</i> | 23 |
| 4.1.4 <i>WAN2 & Failover</i> | 26 |
| 4.1.5 <i>LAN1~4 Configuration</i> | 28 |
| 4.1.6 <i>Private LAN Configuration</i> | 31 |
| 4.2. USER AUTHENTICATION | 34 |
| 4.2.1 <i>Authentication Configuration</i> | 34 |
| 4.2.2 <i>Black List Configuration</i> | 50 |
| 4.2.3 <i>Policy Configuration</i> | 52 |
| 4.2.4 <i>Additional Configuration</i> | 60 |
| 4.3. AP MANAGEMENT | 85 |
| 4.3.1 <i>AP List</i> | 85 |
| 4.3.2 <i>AP Discovery</i> | 95 |
| 4.3.3 <i>Manual Configuration</i> | 98 |

| | | |
|--------|---|-----|
| 4.3.4. | <i>Template Settings</i> | 98 |
| 4.3.5. | <i>Firmware Management</i> | 100 |
| 4.3.6. | <i>AP Upgrade</i> | 101 |
| 4.4. | NETWORK CONFIGURATION | 102 |
| 4.4.1. | <i>Network Address Translation</i> | 102 |
| 4.4.2. | <i>Privilege List</i> | 105 |
| 4.4.3. | <i>Monitor IP List</i> | 106 |
| 4.4.4. | <i>Walled Garden List</i> | 108 |
| 4.4.5. | <i>Proxy Server Properties</i> | 109 |
| 4.4.6. | <i>Dynamic DNS</i> | 110 |
| 4.4.7. | <i>IP Mobility</i> | 110 |
| 4.5. | UTILITIES | 111 |
| 4.5.1. | <i>Change Password</i> | 111 |
| 4.5.2. | <i>Backup/Restore Settings</i> | 113 |
| 4.5.3. | <i>Firmware Upgrade</i> | 114 |
| 4.5.4. | <i>Restart</i> | 114 |
| 4.6. | STATUS | 115 |
| 4.6.1. | <i>System Status</i> | 115 |
| 4.6.2. | <i>Interface Status</i> | 117 |
| 4.6.3. | <i>Current Users</i> | 119 |
| 4.6.4. | <i>Traffic History</i> | 119 |
| 4.6.5. | <i>Notify Configuration</i> | 121 |
| 4.7. | HELP | 124 |
| 5. | APPENDIX A -- CONSOLE INTERFACE | 125 |
| 6. | APPENDIX B -- NETWORK CONFIGURATION ON PC | 128 |
| 7. | APPENDIX C - WINDOWS SERVER 2000/2003 AD | 137 |
| 8. | APPENDIX D - PROXY SETTING FOR HOTSPOT | 141 |
| 9. | APPENDIX E - PROXY SETTING FOR ENTERPRISES | 144 |
| 10. | APPENDIX E - GLOSSARY | 148 |

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.



Apply

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



Clear

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

2. System Overview

2.1. Introduction

AMG-2000 is a network access controller, 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, upgrade, and monitor all managed APs from a single secured interface, and from there, gain full control of entire wireless network.

- **Simplified Deployment and Administration**

- Ease of integration into existing wireless and wired network

- No configuration change is required on client devices

- Customizable login portal page to control the authentication process

- Ability to manage the entire wireless network from a single point

- **Comprehensive Security Features**

- Integrated user authentication based on industry standards

- Authorized end-to-end communication for both wireless and wired networks

- Standards-based encryption capabilities ensure data privacy to user's device

- Protection against DoS attack and unauthorized access points

- **Effective User Management**

- Simultaneous support for internal and external user authentication options

- Policy-based control approach enhances the management of multiple categories of users

- On-line user list monitors real-time status of each individual user

- Provides detailed per-user traffic history log for analysis and record keeping

- **Centralized AP Management**

- Centralized remote control of managed APs avoids the need to individually configure each device

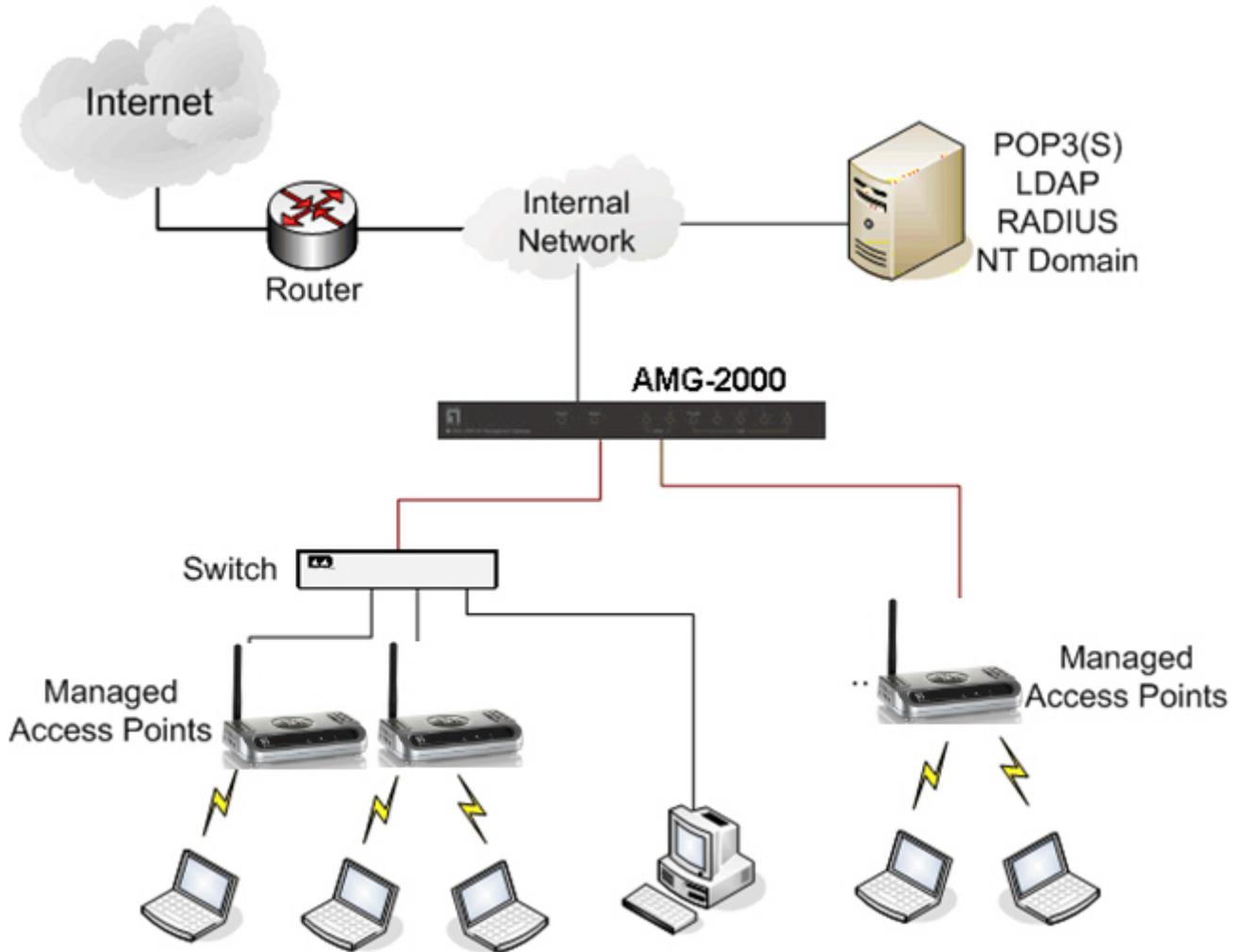
- Automatic discovery of APs to identify and enroll managed APs to the device list

- Remote status monitoring of managed APs and associated client stations ensures efficient network resource utilization

- Provides system alarms and statistics reports on managed APs

2.2. System Concept

AMG-2000 is responsible for user authentication, authorization and management. The user account information is stored in the local database or a specified external databases server. The user authentication is processed via the SSL encrypted web interface. This interface is compatible to most desktop devices and palm computers. The following figure is an example of AMG-2000 set to control a part of the company's intranet. The whole managed network includes the cable network users and the wireless network users.



2.3. Specification

2.1.1 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

2.1.2 Technical Specification

- **Networking**

Supports Router, NAT mode

Supports Static IP, DHCP, PPPoE on WAN interface

Configurable LAN ports authentication

Supports IP Plug and Play (IP PnP)

Built-in DHCP server and supports DHCP relay

Supports NAT:

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

Supports static route

Supports SMTP redirection

Supports Walled Garden (free surfing zone)

Supports MAC Address Pass-Through

Supports HTTP Proxy

- **Security**

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

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

Supports VPN Pass-through (IPSec and PPTP)

Supports DoS attack protection

Supports user Black List

Allows user identity plus MAC address authentication for local accounts

- **User Management**

Supports up to 120 concurrent users

Provides 500 local accounts

Provides 2000 on-demand accounts

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

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

Customizable login and logout portal page

User Session Management:

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

- **AP Management**

Supports up to 12 manageable IEEE 802.11 compliant APs

Centralized remote management via HTTP/SNMP interface

Automatic discovery of managed APs and list of managed APs

Allows administrators to add and delete APs from the device list

Allows administrators to enable or disable managed APs

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

Locally maintained configuration profiles of managed APs

Single UI for upgrading and restoring managed APs' firmware

System status monitoring of managed APs and associated client stations

Automatic recovery of APs in case of system failure

System alarms and status reports on managed APs

- **Monitoring and Reporting**

Status monitoring of on-line users

IP-based monitoring of network devices

WAN connection failure alert

Syslog support for diagnosing and troubleshooting

User traffic history logging

- **Accounting and Billing**

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

Built-in billing profiles for on-demand accounts

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

Provides billing report on screen for on-demand accounts

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

Traffic history report in an automatic email to administrator

- **System Administration**

Multi-lingual, web-based management UI

SSH remote management

Remote firmware upgrade

NTP time synchronization

Backup and restore of system configuration

3. Base Installation

3.1. Hardware Installation

3.1.1. System Requirements

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

3.1.2. Package Contents

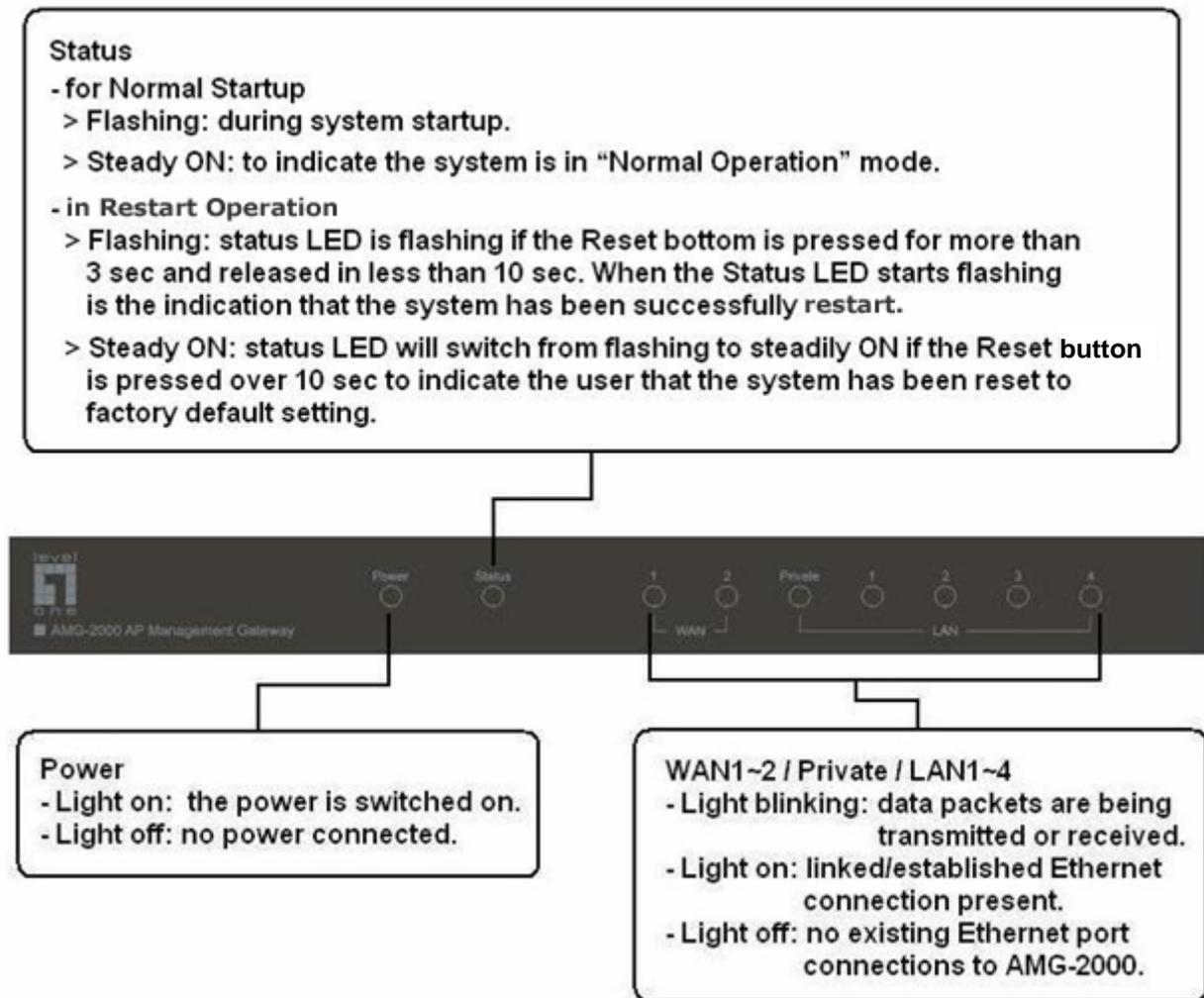
The standard package of AMG-2000 includes:

- AMG-2000 x 1
- CD-ROM x 1
- Quick Installation Guide x 1
- Power Adaptor (DC 5V) x 1
- Cross Over Ethernet Cable x 1
- Straight-through Ethernet Cable x 1
- Console Cable x 1

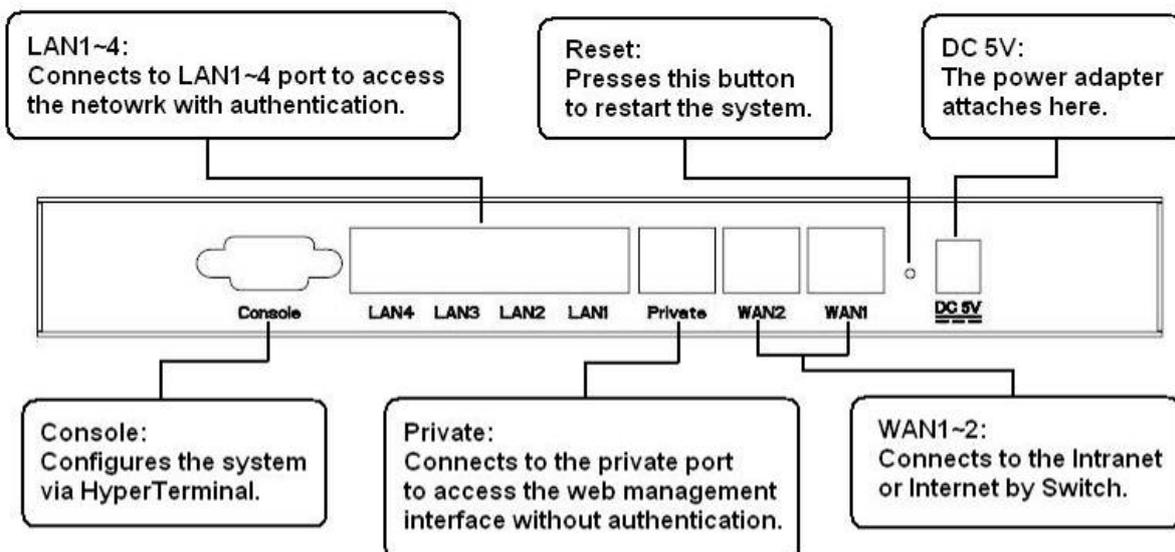
Warning: *Using a power supply with different voltage rating will damage this product.*

3.1.3. Panel Function Descriptions

Front Panel

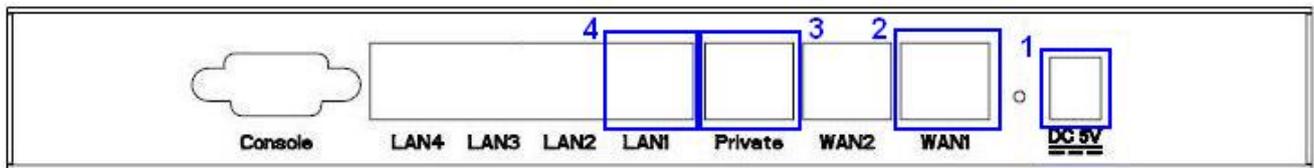


Rear Panel



3.1.4. Installation Steps

Please follow the following steps to install AMG-2000:



1. Connect the DC power adapter to the power connector socket on the rear panel. The Power LED should be on to indicate a proper connection.
2. Connect an Ethernet cable to the WAN1 Port on the rear panel. Connect the other end of the Ethernet cable to ADSL modem, cable modem or a switch/hub of the internal network. The LED of WAN1 Port should be on to indicate a proper connection.
3. Connect an Ethernet cable to Private Port on the rear panel. Connect the other end of the Ethernet cable to a client'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 web management 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 switch. The LED of the LAN Port should be on to indicate a proper connection. (**Note:** Authentication is required for the users 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

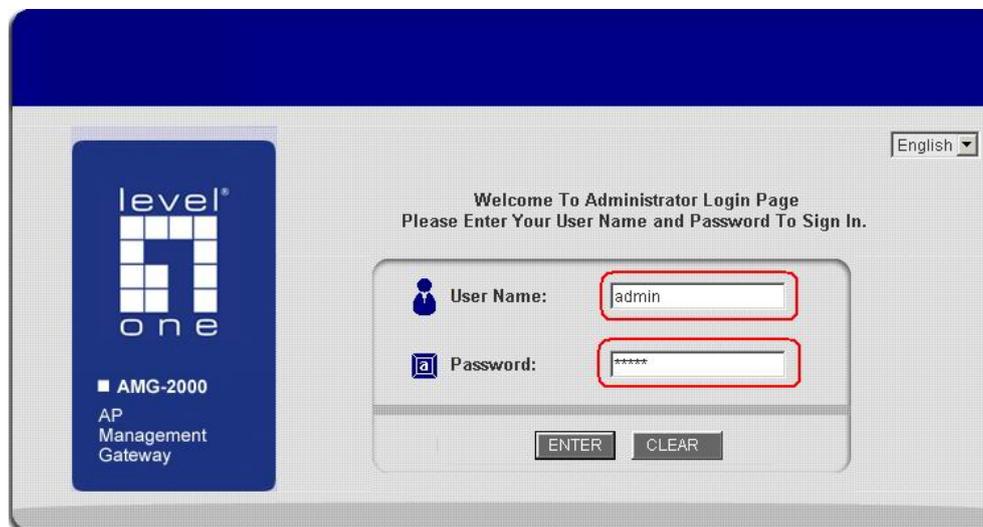
3.2.1. Quick Configuration

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). You just need to 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. Set Authentication Methods
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 one of 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://192.168.2.254>. In the opened webpage, you will see the login screen. Enter "**admin**", the default username and password, in the User Name and Password column. Click **Enter** to log in.



Caution: If you can't get the login screen, the reasons may be: 1. The PC 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 **6. 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**

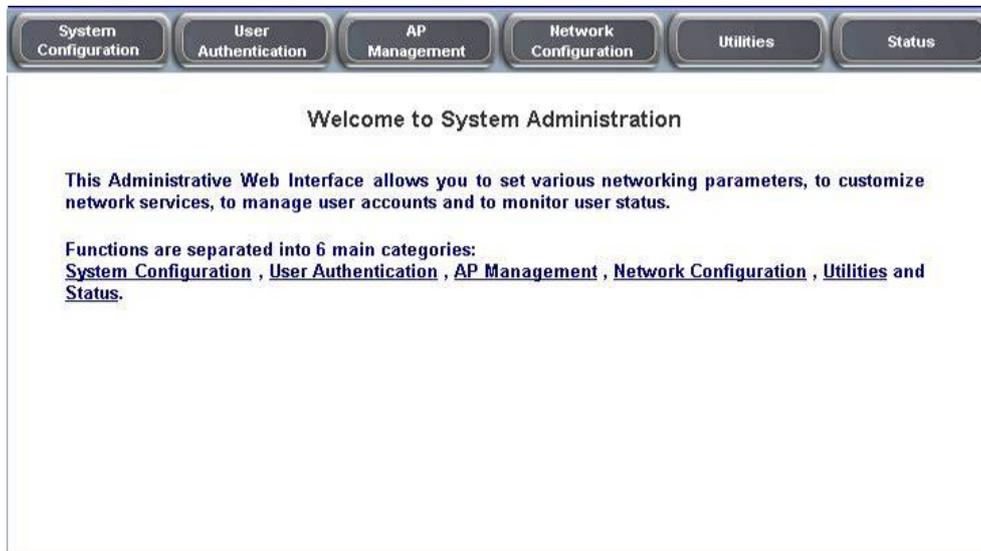
Password: **manager**

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

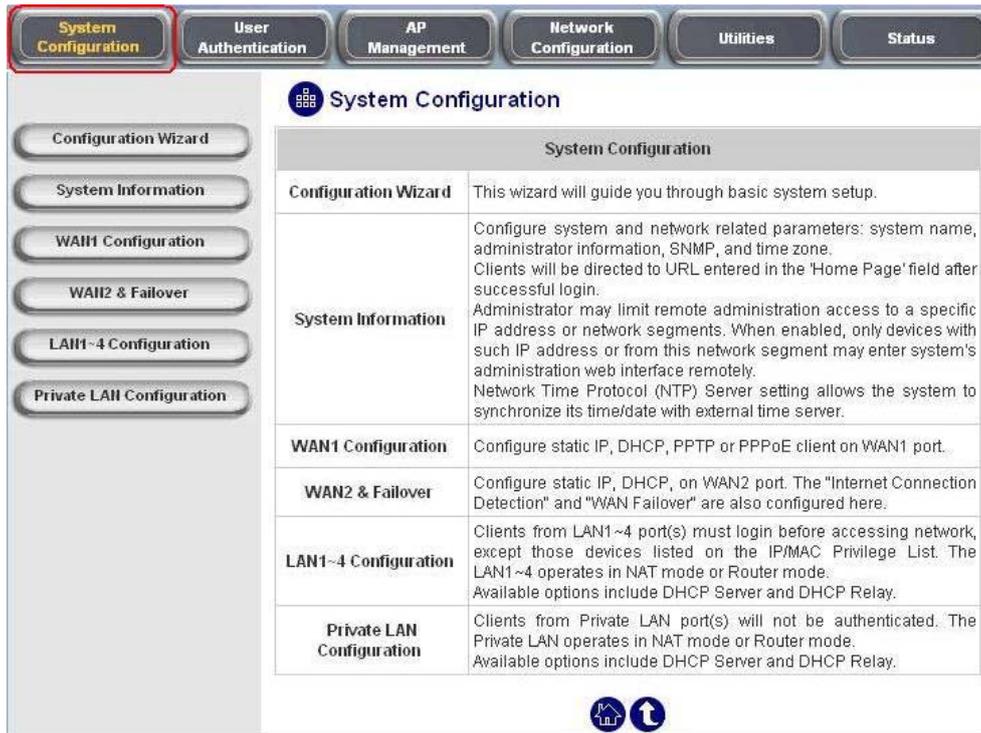
User Name: **operator**

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.



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



- 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 star 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 for 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.

Step 1. Change Admin's Password

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

New Password: ***** *

Verify Password: ***** *

Back Next Exit

Step 2. Choose System's Time Zone

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

(GMT+08:00)Taipei

Back Next Exit

Step 3. Set System Information

Enter System Information. Click Next to continue.

Home Page: http://global.level1.comf *
(e.g. http://global.level1.comf)

NTP Server: tock.usno.navy.mil *
(e.g. tock.usno.navy.mil)

DNS Server: 188.95.1.1 *

Back Next Exit

Step 4. Select the Connection Type for WAN Port

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

Static IP Address Choose it to set static IP address.

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

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

Back Next Exit

➤ **Dynamic IP Address**

If this option is selected, AMG-2000 will obtain IP settings from 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 network administrator.

Click **Next** to continue.

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

Click Next to continue.

IP Address: *

Subnet Mask: *

Default Gateway: *

Back Next Exit

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

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

Click **Next** to continue.

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

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

Username: *

Password: *

Back Next Exit

• **Step 5. Set Authentication Methods**

Set the user's information in advance. Enter an easily identified name as the postfix name in the **Postfix** field (e.g. Local), select a policy to assign to (you can configure the policy routes, firewall rules and login schedule for each policy later, for now just use the default), and choose an authentication method.

Click **Next** to continue. Different information has to be provided for each kind of authentication method:

Step 5. Set Authentication Methods

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

Postfix: *
(Its postfix name.)

Policy

Local User LDAP

POP3 NT Domain

RADIUS

Back Next Exit

➤ **Local User: Add User**

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

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

Step 5 (Cont). Add User

Click "ADD" button to add Local User. Click Next to continue.

Username:

Password:

MAC: (XXXXXXXXXXXX)

Policy:

➤ **POP3 User: POP3**

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

Click **Next** to continue.

Step 5 (Cont). POP3

Configure POP3 Server information. Click Next to continue.

POP3 Server: *(Domain Name/IP)

Server Port: *(Default: 110)

Enable SSL

➤ **RADIUS User: RADIUS**

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

Click **Next** to continue.

Step 5 (Cont). RADIUS

Configure RADIUS Server information. Click Next to continue.

RADIUS Server: *(Domain Name/IP)

Authentication Port: *(Default: 1812)

Accounting Port: *(Default: 1813)

Secret Key: *

Accounting Service: *

Authentication Method: *

➤ **LDAP User: LDAP**

You can configure external LDAP user data base here. Enter the “**LDAP Server**”, “**Server Port**”, “**Base DN**” and “**Account Attribute**”.

Click **Next** to continue.

Step 5 (Cont). LDAP

Configure LDAP Server information. Click **Next** to continue.

LDAP Server: * (Domain Name/IP)

Server Port: * (Default: 389)

Base DN: * (CN=,dc=,dc=)

Account Attribute: * (Default: uid)

➤ **NT Domain User: NT Domain**

When NT Domain is selected, enter the information for “**Server IP Address**”, and enable/disable “**Transparent Login**” (used to login AMG-2000 automatically when login to NT domain. This option normally requires extra configuration to work, we suggest you NOT to enable it at initial configuration).

Click **Next** to continue.

Step 5 (Cont). NT Domain

Configure NT Domain Server information. Click **Next** to continue.

Server IP Address: *

Transparent Login

• **Step 6. Save and Restart AMG-2000**

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

Step 6. Save and Restart AMG-2000

The Setup Wizard has completed. Click on **Back** to review or modify settings. Click **Restart** to save the settings and restart the system to have the current settings take effect.

- **Setup Wizard.**

During AMG-2000 restart, a “**Restarting now. Please wait for a while.**” 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.



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

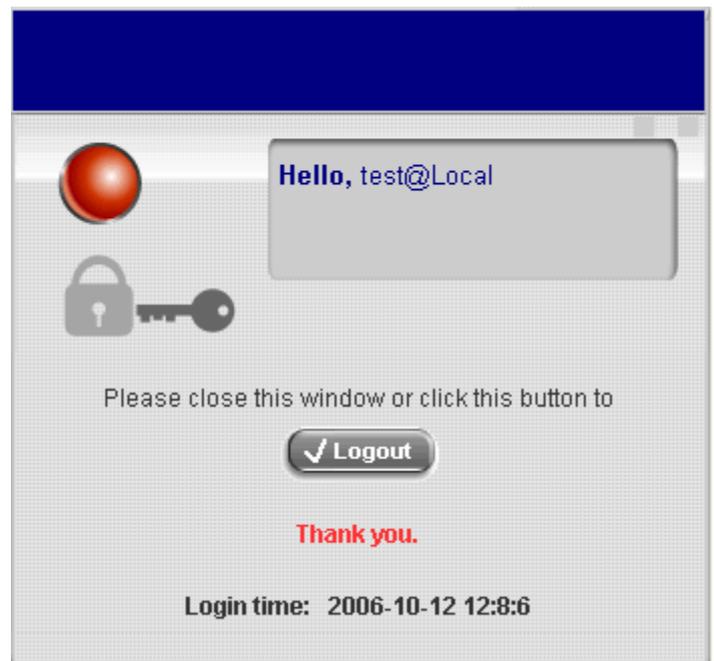
3.2.2. User Login Portal Page

To login from the login portal page via the 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.

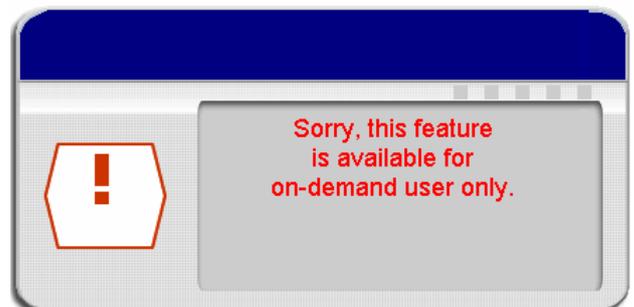
1. First, connect a user-end device (for example, a PC) to one of the LAN1~LAN4 port of the AMG-2000, and set the device to obtain IP address automatically. After the user end obtains the IP address, please open an Internet browser and the default user login webpage will appear on the Internet browser. Type 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!



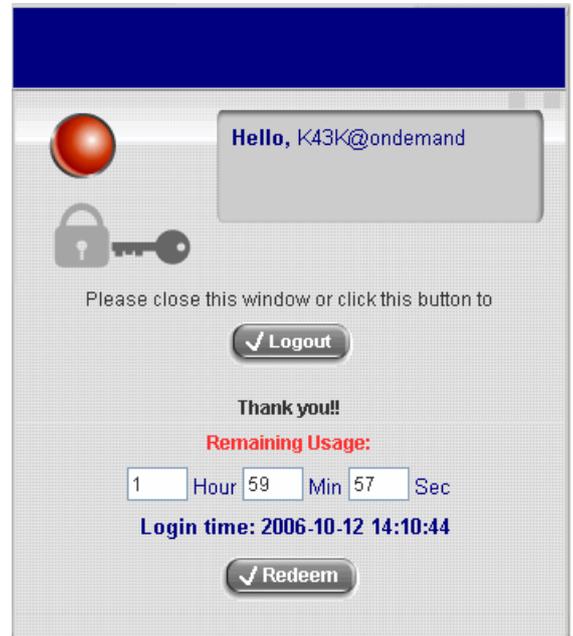
3. But if you see the following screen with a sentence, **“Sorry, this feature is available for on-demand user only”**, it means you click the **“Remaining”** button by mistake. This button is only for on-demand users and if you are not an on-demand user, please just click the **Submit** button.



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.



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 & Failover | Additional Configuration | Template Settings | Walled Garden List | Restart | Traffic History |
| | LAN1~4 Configuration | | Firmware Management | Proxy Server Properties | | Notification Configuration |
| | Private LAN Configuration | | AP Upgrade | Dynamic DNS | | |
| | | | | IP Mobility | | |

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 & Failover**, **LAN1~4 Configuration** and **Private LAN Configuration**.

| System Configuration | |
|---------------------------|---|
| Configuration Wizard | This wizard will guide you through basic system setup. |
| System Information | Configure system and network related parameters: system name, administrator information, SNMP, and time zone. Clients will be directed to URL entered in the 'Home Page' field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely. Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server. |
| WAN1 Configuration | Configure static IP, DHCP, PPTP or PPPoE client on WAN1 port. |
| WAN2 & Failover | Configure static IP, DHCP, on WAN2 port. The "Internet Connection Detection" and "WAN Failover" are also configured here. |
| LAN1~4 Configuration | Clients from LAN1~4 port(s) must login before accessing network, except those devices listed on the IP/MAC Privilege List. The LAN1~4 operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay. |
| Private LAN Configuration | Clients from Private LAN port(s) will not be authenticated. The Private LAN operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay. |

4.1.1. Configuration Wizard

Please refer to **3.2.2 User Login Portal Page** for the detail description of **Configuration Wizard**.

Configuration Wizard

AMG-2000 is a Network Access Controller with access control features ideal for hotspot, small and medium business networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure AMG-2000.

Run 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 Information | |
|--------------------------|--|
| System Name | <input type="text" value="AP Management Gateway"/> |
| Device Name | <input type="text"/> (FQDN for this device) |
| Home Page | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="text" value="http://www.level1.com/"/> * (e.g. http://www.level1.com/) |
| Access History IP | <input type="text"/> (e.g. 192.168.2.1) |
| Remote Manage IP | <input type="text"/> (e.g. 192.168.3.1 or 192.168.3.0/24) |
| SNMP | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| User Logon SSL | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Time | Device Time : 2006/10/12 14:21:35 Time Zone : <input type="text" value="(GMT+08:00)Taipei"/> <input checked="" type="radio"/> NTP Enable NTP Server 1: <input type="text" value="tock.usno.navy.mil"/> *(e.g. tock.usno.navy.mil) NTP Server 2: <input type="text" value="ntp1.fau.de"/> NTP Server 3: <input type="text" value="clock.cuhk.edu.hk"/> NTP Server 4: <input type="text" value="ntps1.pads.ufrj.br"/> NTP Server 5: <input type="text" value="ntp1.cs.mu.OZ.AU"/> <input type="radio"/> Set Device Date and Time |

- **System Name:** Set the system's name or use the default.
- **Device Name:** 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.level1.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>

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

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

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

- **Remote Manage IP:** Set the IP range which is able to connect to the web management interface via WAN 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.

| | |
|-------------|--|
| Time | Device Time : 2007/01/05 14:03:03 <input type="radio"/> NTP Enable <input checked="" type="radio"/> Set Device Date and Time (GMT) -- Year -- Month -- Day -- Hour -- Minute -- Second |
|-------------|--|

4.1.3.WAN1 Configuration

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

| WAN1 Configuration | |
|--|---|
| WAN1 Port | <input checked="" type="radio"/> Static IP Address |
| | IP Address: <input type="text" value="10.2.3.197"/> * |
| | Subnet Mask: <input type="text" value="255.255.255.0"/> * |
| | Default Gateway: <input type="text" value="10.2.3.254"/> * |
| | Preferred DNS Server: <input type="text" value="168.95.1.1"/> * |
| | Alternate DNS Server: <input type="text"/> |
| <input type="radio"/> Dynamic IP Address | |
| <input type="radio"/> PPPoE Client | |
| <input type="radio"/> PPTP Client | |

- **Static IP Address:** Manually specifying the IP address of the WAN1 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.

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

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

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

- 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.

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

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

4.1.4.WAN2 & Failover

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

- **None**: The WAN2 Port is disabled. You can still enter up to three URLs and check “**Warning of Internet Disconnection**” to detect the WAN1 port connection status.

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

- **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. You can enter up to three URLs and check “**Warning of Internet Disconnection**” to work with the WAN **Failover** function.

| WAN2 & Failover | |
|------------------|--|
| WAN2 Port | <input type="radio"/> None <input checked="" type="radio"/> Static IP Address IP Address: <input type="text"/> * Subnet Mask: <input type="text"/> * Default Gateway: <input type="text"/> * Preferred DNS Server: <input type="text"/> * Alternate DNS Server: <input type="text"/> <input type="radio"/> Dynamic IP Address |
| Failover | Probe Target URL1: http:// <input type="text"/> URL2: http:// <input type="text"/> URL3: http:// <input type="text"/> <input type="checkbox"/> WAN Failover <input type="checkbox"/> Warning of Internet Disconnection |

If **WAN Failover** function is enabled, when WAN1 connection fails, the traffic will be routed to WAN2 automatically. If **Failback to WAN1 when possible** function is enabled, when WAN1 connection is recovered, the routed traffic will be back to WAN1.

| | |
|-----------------|---|
| Failover | Probe Target URL1: http:// <input type="text" value="www.google.com"/> URL2: http:// <input type="text"/> URL3: http:// <input type="text"/> <input checked="" type="checkbox"/> WAN Failover <input checked="" type="checkbox"/> Failback to WAN1 when possible <input type="checkbox"/> Warning of Internet Disconnection |
|-----------------|---|

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

| WAN2 & Failover | |
|------------------|---|
| WAN2 Port | <input type="radio"/> None <input type="radio"/> Static IP Address <input checked="" type="radio"/> Dynamic IP Address <input type="button" value="Renew"/> |
| Failover | Probe Target URL1: http:// <input type="text"/> URL2: http:// <input type="text"/> URL3: http:// <input type="text"/> <input type="checkbox"/> WAN Failover <input type="checkbox"/> Warning of Internet Disconnection |

For Dynamic IP Address, **WAN Failover** and **Fallback to WAN1 when possible** also can be enabled like as the function for **Static IP Address**.

| WAN2 & Failover | |
|------------------|---|
| WAN2 Port | <input type="radio"/> None <input type="radio"/> Static IP Address <input checked="" type="radio"/> Dynamic IP Address <input type="button" value="Renew"/> |
| Failover | Probe Target URL1: http:// <input type="text" value="www.google.com"/> URL2: http:// <input type="text"/> URL3: http:// <input type="text"/> <input checked="" type="checkbox"/> WAN Failover <input checked="" type="checkbox"/> Fallback to WAN1 when possible <input type="checkbox"/> Warning of Internet Disconnection |

4.1.5.LAN1~4 Configuration

Clients access the network through LAN1~4 ports must log in for authentication first. In this section, you can set the related configuration for LAN1~4 ports and DHCP server.

| LAN1~4 Configuration | |
|----------------------------------|---|
| LAN1~4 | Operation Mode <input type="text" value="NAT"/> <input type="button" value="v"/> IP Address: <input type="text" value="192.168.1.254"/> * Subnet Mask: <input type="text" value="255.255.255.0"/> * |
| DHCP Server Configuration | <input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay |

- LAN1~4

| LAN1~4 Configuration | |
|----------------------|---|
| LAN1~4 | Operation Mode: <input type="text" value="NAT"/> |
| | IP Address: <input type="text" value="192.168.1.254"/> * |
| | Subnet Mask: <input type="text" value="255.255.255.0"/> * |

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

IP Address: Enter the desired IP address for the LAN1~LAN4 port.

Subnet Mask: Enter the desired subnet mask for the LAN1~LAN4 port.

- DHCP Server Configuration**

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

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

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

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

| | |
|---|--|
| DHCP Server Configuration | <input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server |
| | DHCP Scope |
| | Start IP Address: <input type="text" value="192.168.1.1"/> * |
| | End IP Address: <input type="text" value="192.168.1.100"/> * |
| | Preferred DNS Server: <input type="text" value="168.95.1.1"/> * |
| | Alternate DNS Server: <input type="text"/> |
| | Domain Name: <input type="text" value="Level1.com"/> * |
| | WINS Server IP: <input type="text"/> |
| | Lease Time: <input type="text" value="1 Day"/> |
| | Reserved IP Address List |
| <input type="radio"/> Enable DHCP Relay | |

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

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

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

Domain Name: Enter the domain name.

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

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.

| Reserved IP Address List - LAN1~4 | | | |
|---|----------------------|----------------------|----------------------|
| Item | Reserved IP Address | MAC | Description |
| 1 | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 2 | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 3 | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 4 | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 5 | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 6 | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 7 | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 8 | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 9 | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 10 | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| (Total:40) First Prev Next Last | | | |

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

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

4.1.6. Private LAN Configuration

To access the network through the private LAN port doesn't have to authenticate before logging in. In this section, you can set the related configuration for the private LAN port and DHCP server.

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

- Private LAN

| Private LAN Configuration | |
|---------------------------|---|
| Private LAN | Operation Mode: <input type="text" value="NAT"/> |
| | IP Address: <input type="text" value="192.168.2.254"/> * |
| | Subnet Mask: <input type="text" value="255.255.255.0"/> * |

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

IP Address: Enter the desired IP address for the 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.

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

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

| | |
|--|---|
| DHCP Server Configuration | <input type="radio"/> Disable DHCP Server |
| | <input checked="" type="radio"/> Enable DHCP Server: |
| | DHCP Scope: |
| | Start IP Address: <input type="text" value="192.168.2.1"/> * |
| | End IP Address: <input type="text" value="192.168.2.100"/> * |
| | Preferred DNS Server: <input type="text" value="168.95.1.1"/> * |
| | Alternate DNS Server: <input type="text"/> |
| | Domain Name: <input type="text" value="Level1.com"/> * |
| | WINS Server IP: <input type="text"/> |
| | Lease Time: <input type="text" value="1 Day"/> ▼ |
| Reserved IP Address List | |
| <input type="radio"/> Enable DHCP Relay | |

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

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

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

Domain Name: Enter the domain name.

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

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.

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

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

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

4.2. User Authentication

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

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

4.2.1. Authentication Configuration

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

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

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

| Authentication Server - Server 1 | |
|----------------------------------|---|
| Server Name | Server 1 <small>*(Its server name)</small> |
| Server Status | Enabled |
| Postfix | Postfix1 <small>*(Its postfix name)</small> |
| Black List | None ▼ |
| Authentication Method | Local User ▼ Local User Setting |
| Policy | Policy 1 ▼ |

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

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

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

Black List: There are 5 sets of black lists. 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 **NTDomain** to configure from. Select the desired method and then click the link beside the pull-down menu for more advanced configuration. For more details, please refer to **4.2.1 Authentication Configuration**.

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

Policy: There are 8 policies to choose from to apply to this particular server.

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

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

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.

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

WLAN ESSID: Enter the ESSID of the AP.

Wireless Key: Enter the wireless key of the AP.

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

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

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

| On-demand Users List | | | | | |
|----------------------|----------|--------------------|--------|---------------------|------------------------|
| Username | Password | Remain Time/Volume | Status | Expire Time | Delete All |
| DH3P | ER4S43FE | 2 hour | 2 hour | 2005/06/02-17:23:39 | Delete |
| 97UU | V7B23947 | 2 hour | 2 hour | 2005/06/05-11:45:26 | Delete |

(Total:2) [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.
- **Username:** The login name of the on-demand user.
- **Password:** The login password of the on-demand user.
- **Remain Time/Volume:** The total time/Volume that the user can use currently.
- **Status:** The status of the account. Normal indicates that the account is not in-use and not overdue. Online indicates that the account is in-use and not overdue. Expire indicates that the account is overdue and cannot be used.
- **Expire Time:** The expiration time of the account.
- **Delete All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.

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

| Billing Configuration | | | | | | |
|-----------------------|--|--|---|---------------------------------------|--------------------------------|-------|
| Plan | Status | Type | | Expired info | Valid Duration | Price |
| 1 | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled | <input type="radio"/> Volume <input type="text" value="999"/> Mbyte <input checked="" type="radio"/> Time <input type="text" value="999"/> hours <input type="text" value="59"/> mins | <input type="text" value="999"/> days <input type="text" value="999"/> hours | <input type="text" value="999"/> days | <input type="text" value="0"/> | |
| 2 | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled | <input type="radio"/> Volume <input type="text"/> Mbyte <input type="radio"/> Time <input type="text"/> hours <input type="text"/> mins | <input type="text"/> days <input type="text"/> hours | <input type="text"/> days | <input type="text"/> | |
| 3 | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled | <input type="radio"/> Volume <input type="text"/> Mbyte <input type="radio"/> Time <input type="text"/> hours <input type="text"/> mins | <input type="text"/> days <input type="text"/> hours | <input type="text"/> days | <input type="text"/> | |
| 4 | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled | <input type="radio"/> Volume <input type="text"/> Mbyte <input type="radio"/> Time <input type="text"/> hours <input type="text"/> mins | <input type="text"/> days <input type="text"/> hours | <input type="text"/> days | <input type="text"/> | |

- **Status:** Select to enable or disable this billing rule.

- **Type:** Set the billing rule 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 | 8 hrs 0 mins | 80 | Enabled | Create |
| 3 | 40 hrs 0 mins | 200 | Enabled | Create |
| 4 | 9999999 Mbyte | 9999999 | Enabled | Create |
| 5 | N/A | N/A | Disabled | Create |
| 6 | N/A | N/A | Disabled | Create |

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

 **Welcome!**

| | |
|---|----------------------|
| Username | 788X@ondemand |
| Password | SF6W2HKK |
| Price | 20 |
| Usage | 2 hrs 0 mins |
| ESSID : | |
| Share WEP Keys: | |
| Valid to use until: 2007/01/08 14:22:30 | |

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

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

To year: -- month: -- day: -- Search

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

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

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

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

- **Authentication Method – Local User Setting**

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

| Authentication Server - Server 1 | |
|----------------------------------|---|
| Server Name | Server 1 <small>*(Its server name)</small> |
| Server Status | Enabled |
| Postfix | Postfix1 <small>*(Its postfix name)</small> |
| Black List | None |
| Authentication Method | Local User Local User Setting |
| Policy | |

Click the hyperlink to get in for further configuration.

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

Edit Local User List: Click this to enter the “Local User List” screen and click the individual **Username** to edit that account.

| Users List | | | | |
|--------------------------|----------|-----|--------|--|
| Username | Password | MAC | Policy | <input type="button" value="Del All"/> |
| | | | Remark | |
| Anderson | A123 | | None | Delete |
| Mary | 94001 | | None | Delete |

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

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). Then, select a desired **Policy** and click **Apply** to complete adding the user or users.

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

User **Anderson** has been added!
 User **Mary** has been added!

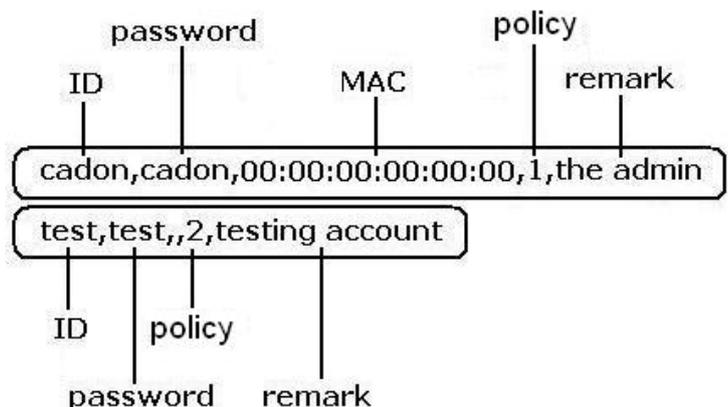
| Add User | | | | | |
|----------|----------------------|----------------------|----------------------------|--------|----------------------|
| Item | Username | Password | MAC (xx:xx:xx:xx:xx:xx) | Policy | Remark |
| 1 | <input type="text"/> | <input type="text"/> | <input type="text"/> | None ▾ | <input type="text"/> |
| 2 | <input type="text"/> | <input type="text"/> | <input type="text"/> | None ▾ | <input type="text"/> |
| 3 | <input type="text"/> | <input type="text"/> | <input type="text"/> | None ▾ | <input type="text"/> |

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

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

Upload User Account

File Name



The uploading file should be a text file and the format of each line is "ID, Password, MAC, Policy, Remark" without the quotes. There

must be no spaces between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. 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 |
| Anderson | A123 | | 0 |
| | | | |
| Mary | 94001 | | 0 |
| | | | |

[Download](#)

Refresh: Click this to renew the user list.

| Users List | | | | |
|--------------------------|----------|-----|--------|--|
| Username | Password | MAC | Policy | <input type="button" value="Del All"/> |
| | | | Remark | |
| Anderson | A123 | | None | Delete |
| | | | | |
| Mary | 94001 | | None | Delete |
| | | | | |

(Total:2) [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.

| Users List | | | | |
|----------------------|----------|-----|--------|--|
| Username | Password | MAC | Policy | <input type="button" value="Del All"/> |
| | | | Remark | |
| Mary | 94001 | | None | Delete |
| | | | | |

(Total:1) [First](#) [Previous](#) [Next](#) [Last](#)

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

Delete: This will delete the users individually.

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

| User Profile | |
|--------------|---------|
| Username | Mary * |
| Password | ***** * |
| MAC | |
| Policy | None ▾ |
| Remark | |

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

| Local User Setting | |
|--------------------------------------|---|
| Edit Local User List | |
| Radius Roaming Out | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| 802.1x Authentication | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| 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.

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

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 (Protracted Extensible Authentication Protocol)** 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**”.

- **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.

| Authentication Server - Server 1 | |
|----------------------------------|--|
| Server Name | Server 1 <small>*(its server name)</small> |
| Server Status | Enabled |
| Postfix | Postfix1 <small>*(its postfix name)</small> |
| Black List | None |
| Authentication Method | Radius Radius Setting |
| Policy | Local User POP3 Radius LDAP NTDomain Edit Policy Mapping |

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 asterisks are necessary information. These settings will become effective immediately after clicking the **Apply** button.

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

802.1X Authentication: Enable this function and the hyperlink of **Radius Client List** will appear. Click the

hyperlink to get into the Radius Client Configuration list for further configuration. In the **Radius Client Configuration** table, the clients, which are using 802.1X as the authentication method, shall be put into this table. AMG-2000 will forward the authentication request from these clients to the configured Radius Servers.

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

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

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

- Authentication Method – LDAP**

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

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

Click the hyperlink for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red star are necessary information. These settings will become effective immediately after clicking the **Apply** button.

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

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

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

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

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

- Authentication Method – NT Domain**

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

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

Click the hyperlink for further configuration. Enter the server IP address and enable/disable the transparent login function. These settings will become effective immediately after clicking the **Apply** button.

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

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

Transparent Login: If the function is enabled, 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.

| Black List Configuration | | |
|----------------------------------|------------|--------------------------|
| Select Black List : 1:Blacklist1 | | |
| Name | Blacklist1 | |
| User | Remark | Delete |
| aaa | | <input type="checkbox"/> |

(Total:1) [First](#) [Prev](#) [Next](#) [Last](#)

[Add User to List](#)

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

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

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

User '1234' has been added!



Add Users to Blacklist

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

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

| Black List Configuration | | |
|--------------------------|--------------|---------------------------------------|
| Select Black List : | 1:Blacklist1 | |
| Name | Blacklist1 | |
| User | Remark | <input type="button" value="Delete"/> |
| 12345 | | <input checked="" type="checkbox"/> |

(Total:1) [First](#) [Prev](#) [Next](#) [Last](#)

[Add User to List](#)

4.2.3. Policy Configuration

There are 8 policies and one Global Policy in Policy Configuration. Except Global Policy, each 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

| Policy Configuration | |
|------------------------------|-------------------------|
| Select Policy: | Policy 1 ▾ |
| Firewall Profile | Setting |
| Specific Route Profile | Setting |
| Schedule Profile | Setting |
| Total Bandwidth | Unlimited ▾ |
| Individual Maximum Bandwidth | Unlimited ▾ |
| Individual Request Bandwidth | None ▾ |

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

| Policy Configuration | |
|------------------------------|-------------------------|
| Select Policy: | Policy 1 ▾ |
| Firewall Profile | Setting |
| Specific Route Profile | Setting |
| Schedule Profile | Setting |
| Total Bandwidth | Unlimited ▾ |
| Individual Maximum Bandwidth | Unlimited ▾ |
| Individual Request Bandwidth | None ▾ |

- **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 Name:

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

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

Rule Item: This is the rule 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.

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

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

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

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

Source/Destination Interface: There are four interfaces to choose, **All**, **WAN1**, **WAN2**, **LAN1~4** and

Private LAN.

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

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

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

➤ **Specific Route Profile**

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

Profile Name:

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

Profile Name: The profile name can be changed here.

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

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

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

Gateway IP Address: The IP address of the 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.

Profile Name: Enabled Disabled

Profile Name: Enabled Disabled

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

➤ **Total Bandwidth**

Choose one bandwidth limit for that particular policy.

| Policy Configuration | |
|------------------------------|---|
| Select Policy: | Policy 1 ▾ |
| Firewall Profile | Setting |
| Specific Route Profile | Setting |
| Schedule Profile | Setting |
| Total Bandwidth | Unlimited ▾ |
| Individual Maximum Bandwidth | <div style="border: 1px solid gray; padding: 2px;"> Unlimited 16 Kbps 32 Kbps 64 Kbps 128 Kbps 256 Kbps 512 Kbps 1 Mbps 2 Mbps 3 Mbps 5 Mbps </div> |
| Individual Request Bandwidth | |

✓ Apply ✗ Clear




➤ **Individual Maximum Bandwidth:**

Choose a bandwidth for the maximum bandwidth of an individual user.

| Policy Configuration | |
|------------------------------|---|
| Select Policy: | Policy 1 ▾ |
| Firewall Profile | Setting |
| Specific Route Profile | Setting |
| Schedule Profile | Setting |
| Total Bandwidth | Unlimited ▾ |
| Individual Maximum Bandwidth | <div style="border: 1px solid gray; padding: 2px;"> Unlimited 16 Kbps 32 Kbps 64 Kbps 128 Kbps 256 Kbps 512 Kbps 1 Mbps 2 Mbps 3 Mbps 5 Mbps </div> |
| Individual Request Bandwidth | |

✓ Apply ✗ Clear



➤ **Individual Request Bandwidth:**

Choose a bandwidth for the minimum bandwidth of an individual user.

| Policy Configuration | |
|------------------------------|---|
| Select Policy: | Policy 1 ▾ |
| Firewall Profile | Setting |
| Specific Route Profile | Setting |
| Schedule Profile | Setting |
| Total Bandwidth | Unlimited ▾ |
| Individual Maximum Bandwidth | Unlimited ▾ |
| Individual Request Bandwidth | None ▾ None 16 Kbps 32 Kbps 64 Kbps 128 Kbps 256 Kbps 512 Kbps 1 Mbps 2 Mbps 3 Mbps 5 Mbps |

• **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.

Policy Name:

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

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

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

Rule Name: The rule name can be changed here.

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

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

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

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

Source/Destination Interface: There are four interfaces to choose, **ALL**, **WAN1**, **WAN2**, **LAN1~4** and **Private LAN**.

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

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

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

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

Profile Name:

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

Profile Name: The profile name can be changed here.

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

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

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

4.2.4. Additional Configuration

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

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

Idle Timer: If a user has been idled with no network activities, 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 authentication method)

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

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

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

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

| Upload Private Key | |
|--------------------|---|
| File Name | <input type="text"/> <input type="button" value="Browse..."/> |

| Upload Customer Certificate | |
|-----------------------------|---|
| File Name | <input type="text"/> <input type="button" value="Browse..."/> |

| |
|--|
| <input type="button" value="Use Default Certificate"/> |
|--|

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

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

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

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

| Default Page Setting |
|--|
| <p>This is default login page for users. You could click preview link to preview the default login page. Thanks.</p> <p style="text-align: center;">Preview</p> |

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

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

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

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

Login Page Selection for Users

Default Page Template Page
 Uploaded Page External Page

Uploaded Page Setting

File Name:

Existing Image Files:

Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

Upload Images:

[Preview](#)

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

User Login Page

Welcome To User Login Page!

Please Enter Your User Name and Password To Sign In .

 User Name:

 Password:

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

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

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

```

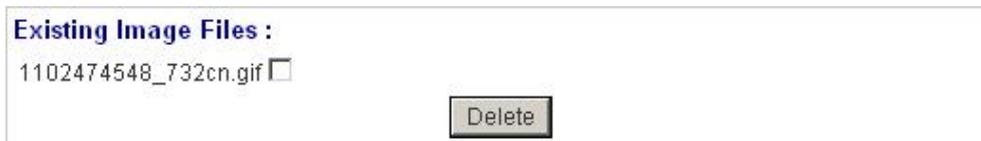
```

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



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

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



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

In AMG-2000, the end user first gets a login page when she/he opens its web browser right after associating with an access point. However, in some situations, the hotspot owners or MIS staff may want to display "terms of use" or announcement information before the login page. Hotspot owners or MIS staff can design a new disclaimer/announcement page and save the page in their local server. After the agreement shown on the page is read, users are asked whether they agree or disagree with the disclaimer. By clicking I agree, users are able to log in. If users choose to decline, they will get a popup window saying they are unable to log in. The basic design is to have the disclaimer and login function in the same page but with the login function hidden until users agree with the disclaimer.

Here we will supply the codes for this page. Please note that the blue part is for the login feature, the red part is

the disclaimer, and the green part can be modified freely by administrators to suit the situation better. Now the default is set to "I disagree" with the disclaimer. Administrators can change the purple part to set "agree" as the default or set no default. These codes should be saved in local storage with a name followed by .html, such as login_with_disclaimer.html.

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

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

    function getCookie(name)
    {
        name += "="; // append '=' to name string
        var i = 0; // index of first name=value pair
        while (i < pham.length) {
            var offset = i + name.length; // end of section to compare name string
            if (pham.substring(i, offset) == name) { // if string matches
                var endstr = pham.indexOf(";", offset); //end of name=value pair
                if (endstr == -1) endstr = pham.length;
                return unescape(pham.substring(offset, endstr));
            }
            // return cookie value section
        }
        i = pham.indexOf(" ", i) + 1; // move i to next name=value pair
        if (i == 0) break; // no more values in cookie string
    }
    return null; // cookie not found
}

function CodeCookie(str)
{
    var strRtn="";

    for (var i=str.length-1;i>=0;i--)
    {
```

```

    strRtn+=str.charCodeAt(i);
    if (i) strRtn+="a";
}
return strRtn;
}
function DecodeCookie(str)
{
var strArr;
var strRtn="";

strArr=str.split("a");

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

return strRtn;

}

```

```

function MM_swapImgRestore() { //v3.0
var i,x,a=document.MM_sr; for(i=0;a&&i<a.length&&(x=a[i])&&x.oSrc;i++) x.src=x.oSrc;
}

```

```

function MM_preloadImages() { //v3.0
var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();
var i,j=d.MM_p.length,a=MM_preloadImages.arguments; for(i=0; i<a.length; i++)
if (a[i].indexOf("#")!=0){ d.MM_p[j]=new Image; d.MM_p[j++].src=a[i];}}
}

```

```

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

```

```

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

```

```

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

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

}

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

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

        return false;
    }

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

```

```

        disableButton=true;
        return true;
    }
    return true;
}
function reminder_onclick(form)
{
    Reminder.myusername.value = form.myusername.value;
    Reminder.mypassword.value = form.mypassword.value;
    Reminder.submit();
}
function cancel_onclick(form)
{
    form.reset();
}

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

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

    return true;
}

```

</script>

</head>

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

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

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

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

</ilayer>

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

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

We may collect and store the following personal information:

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

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

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

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

We may also share your personal information with:

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

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

personal information. If your personal information will be used contrary to this policy, you will receive prior notice.)

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

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

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

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

```

        </table></td>
    </tr>
    <tr>
        <td height="20">&nbsp;</td>
    </tr>
</table>

<div align="center">
<table name="login" id="login" width="497" height="328" border="0" align="center" cellpadding="2" cellspacing="0"
background="../images/userlogin.gif">
    <tr>
        <td height="146" colspan="2">&nbsp;</td>
    </tr>
    <tr>
        <td width="43%" height="53">&nbsp;</td>
        <td><input type="text" name="myusername" size="20"></td>
    </tr>
    <tr>
        <td height="42">&nbsp;</td>
        <td><input type="password" name="mypassword" size="20"></td>
    </tr>
    <tr>
        <td colspan="2">
            <div align="center">
                <a onclick="javascript:if(Before_Submit(Enter)){Enter.submit();}" onMouseOut="MM_swapImgRestore()"
onMouseOver="MM_swapImage('Image3','../images/submit0.gif',1)">
                    
                </a>
                <a onclick="cancel_onclick(Enter)" onMouseOut="MM_swapImgRestore()"
onMouseOver="MM_swapImage('Image5','../images/clear0.gif',1)">
                    
                </a>
                <a onclick="javascript:if(Before_Submit(Enter)){reminder_onclick(Enter);}"
onMouseOut="MM_swapImgRestore()" onMouseOver="MM_swapImage('Image4','../images/remaining0.gif',1)">
                    
                </a>
            </div>
        </td>
    </tr>
</table>

```

```

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

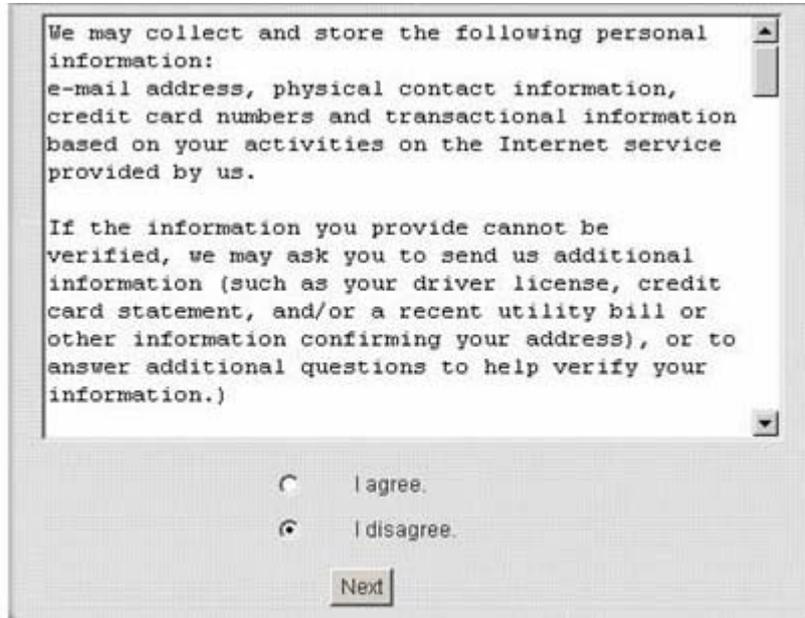
</div>
</form>
<form action="reminder.shtml" method="post" name="Reminder">
<input type="hidden" name="myusername" value="">
<input type="hidden" name="mypassword" value="">
</form>
<br>
<div align="center">
<table>
<tr>
<td width="100%">
<font color="#808080" size="2"><script language="JavaScript">document.write(copyright);</script></font></td>
</tr>
</table>
</div>
</body>
</html>

```

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



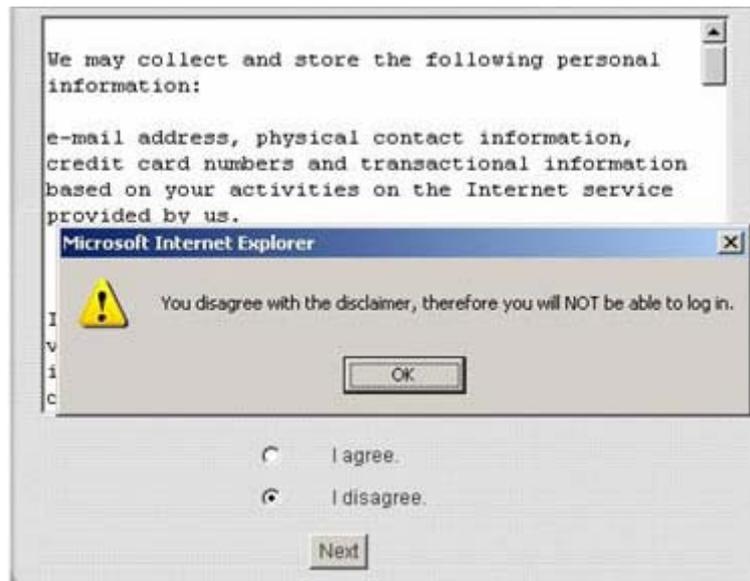
“Preview” can be clicked to see the uploaded page.



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



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



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

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

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

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



Please not that:

```
<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>
```

is needed in your HTML code to make sure the page works correctly.

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



The different part is the HTML code of the user-defined logout interface must include the following HTML

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

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

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

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

| Default Page Setting |
|---|
| <p style="text-align: center;">This is default login success page for users. You could click preview link to preview the default login success page. Thanks.</p> |
| Preview |

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

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

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

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

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

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

Existing Image Files:

| |
|------------------------------|
| Total Capacity: 512 K |
| Now Used: 0 K |

| Upload Image Files | |
|---------------------------------------|---|
| Upload Images | <input type="text"/> <input type="button" value="Browse..."/> |
| <input type="button" value="Submit"/> | |
| Preview | |

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

button at the bottom.

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



Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

Upload Images Browse...

Submit

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

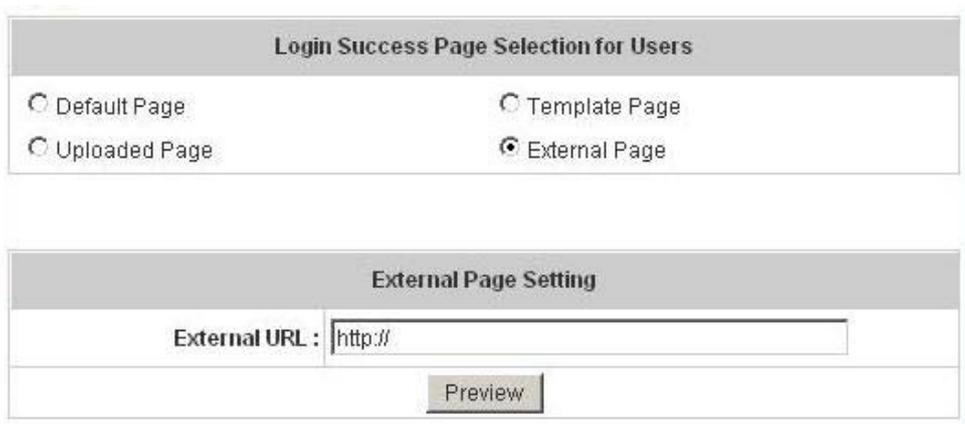


Existing Image Files :

1102474548_732cn.gif

Delete

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



Login Success Page Selection for Users

Default Page Template Page
 Uploaded Page External Page

External Page Setting

External URL :

Preview

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

- a. Choose **Default Page** to use the default login success page for on-demand.

Login Success Page Selection for on-demand Users

Default Page Template Page
 Uploaded Page External Page

Default Page Setting

This is default login success page for on-demand users.
 You could click preview link to preview the default login success page.
 Thanks.

[Preview](#)

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

Login Success Page Selection for on-demand Users

Default Page Template Page
 Uploaded Page External Page

Template Page Setting

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

- c. Choose **Uploaded Page** and you can get the login success page for on-demand by uploading. Click the

Browse button to select the file for the login success page for on-demand upload. Then click **Submit** to complete the upload process.

Login Success Page Selection for on-demand Users

Default Page Template Page
 Uploaded Page External Page

Upload Login Success Page for on-demand

File Name

Existing Image Files:

Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

Upload Images

[Preview](#)

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

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

Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

Upload Images

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

Existing Image Files :

1102474548_732cn.gif

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

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

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

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

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

| Default Page Setting | |
|--|--|
| This is default logout success page for users. You could click preview link to preview the default logout success page. Thanks. | |
| Preview | |

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

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

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

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

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

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

Existing Image Files:

| |
|------------------------------|
| Total Capacity: 512 K |
| Now Used: 0 K |

| Upload Image Files | |
|---------------------------------------|---|
| Upload Images | <input type="text"/> <input type="button" value="Browse..."/> |
| <input type="button" value="Submit"/> | |
| Preview | |

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

button at the bottom.

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

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

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

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

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

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

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

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

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

- **POP3 Message:** If a user tries to retrieve mail from POP3 mail server before login, the users will receive a welcome mail from AMG-2000. The administrator can edit the content of this welcome mail.

Edit Mail Message

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

- **Enhance User Authentication:** With this function, only the users with their MAC addresses in this list can log into 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 **Permit MAC Address List** to fill in these MAC addresses, select **Enable**, and then click **Apply**.

MAC Address Control

Enabled Disabled

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

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

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

4.3. AP Management

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**.

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

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

4.3.1. AP List

All of the 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**.

| AP List | | | | |
|--------------------------|----------|------------------------------|-------------------|----------------------------------|
| <input type="checkbox"/> | AP Type | AP Name | IP | Status |
| | | | MAC | |
| <input type="checkbox"/> | WAP-0006 | NEWDEV-00002 | 10.171.1.129 | Online (Enabled) |
| | | | 00:0E:2E:7C:AA:F6 | |
| <input type="checkbox"/> | WAP-0006 | NEWDEV-00003 | 10.171.1.130 | Online (Enabled) |
| | | | 00:0E:2E:7C:B5:1A | |

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

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

| AP List | | | | |
|-------------------------------------|----------|------------------------------|-------------------|---------------------|
| <input type="checkbox"/> | AP Type | AP Name | IP | Status |
| | | | MAC | |
| <input checked="" type="checkbox"/> | WAP-0006 | NEWDEV-00002 | 10.171.1.129 | Online (Enabled) |
| | | | 00:0E:2E:7C:AA:F6 | |
| <input type="checkbox"/> | WAP-0006 | NEWDEV-00003 | 10.171.1.130 | Online (Enabled) |
| | | | 00:0E:2E:7C:B5:1A | |

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

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

Template

TEMPLATE3

| Template: TEMPLATE3 | |
|---------------------|----------|
| SSID | apmgt |
| Channel | 11 |
| Transmission Rate | Auto |
| Security | Disabled |

Done Internet

- **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-00002 |
| | 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 | <input type="text" value="NEWDEV-00002"/> |
| Admin Password | <input type="text" value="1234"/> |
| Remark | <input type="text"/> |
| Firmware | 1.20 |

- **LAN Interface Setting:** Click **LAN** to enter the **LAN Settings** page. Input the data of LAN including **IP Address**, **Subnet Mask** and **Default Gateway** of the AP.

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

- **Wireless Interface Setting:** Click **Wireless LAN** to enter the **Wireless Interface Setting** page. The data of Properties and Security need to be filled in.

| Wireless | | |
|------------|----------------------|--|
| Properties | SSID | apmgt |
| | SSID Broadcast | Enable ▾ |
| | Channel | 1 ▾ |
| | Transmission Mode | Mixed ▾ |
| | Transmission Rate | Auto ▾ <small>(Default: Auto; Range: from 1 to 54 Mbps)</small> |
| | CTS Protection | Disable ▾ <small>(Default: Disable)</small> |
| | Fragment Threshold | 2346 <small>(Default: 2346; Range: from 256 to 2346)</small> |
| | RTS Threshold | 2347 <small>(Default: 2347; Range: from 0 to 2347)</small> |
| | Beacon Interval (ms) | 100 <small>(Default: 100; Range: from 20 to 1024 msec)</small> |
| | Preamble Type | Long ▾ <small>(Default: Long)</small> |
| | IAPP | Enable ▾ <small>(Default: Enable)</small> |
| Security | Security Type | Disable ▾ <input type="checkbox"/> 802.1x Authentication |
| | WEP | Authentication Type Both ▾ |

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.

| | | | |
|----------|---------------|---------------------|--|
| Security | Security Type | Disable | <input type="checkbox"/> 802.1x Authentication |
| | WEP | Authentication Type | Both |

| | | | |
|----------|---------------|---------------------|---|
| Security | Security Type | Disable | <input checked="" type="checkbox"/> 802.1x Authentication |
| | WEP | Authentication Type | Both |
| | 802.1x | Radius Server | |
| | | IP | <input type="text"/> |
| | | Port | <input type="text" value="1812"/> |
| | | Secret | <input type="text"/> |

- **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.

| | | |
|-----------------|----------------------|--|
| Security | Security Type | WEP <input type="button" value="v"/> <input checked="" type="checkbox"/> 802.1x Authentication |
| | WEP | Authentication Type <input type="button" value="v"/> Both Key Length <input type="button" value="v"/> 64 bits Key Format <input type="button" value="v"/> ASCII Key Index <input type="button" value="v"/> Key1 Key1 <input type="text" value="key01"/> Key2 <input type="text" value="key02"/> Key3 <input type="text" value="key03"/> Key4 <input type="text" value="key04"/> |
| | 802.1x | Radius Server IP <input type="text"/> Port <input type="text" value="1812"/> Secret <input type="text"/> |

- 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.

| | | |
|-----------------|----------------------|--|
| Security | Security Type | WPA <input type="button" value="v"/> WPA-PSK <input type="button" value="v"/> |
| | WPA-PSK TKIP | Passphrase/PSK <input type="text"/> <input type="button" value="v"/> Passphrase |

| | | |
|-----------------|----------------------|---|
| Security | Security Type | WPA <input type="button" value="v"/> 802.1x <input type="button" value="v"/> |
| | 802.1x | Radius Server IP <input type="text"/> Port <input type="text" value="1812"/> Secret <input type="text"/> |

- 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.

| | | | |
|----------|----------------|----------------|------------------------------------|
| Security | Security Type | WPA2 | WPA-PSK |
| | WPA-PSK AES | Passphrase/PSK | <input type="text"/> Passphrase |

| | | | |
|----------|---------------|---------------|--|
| Security | Security Type | WPA2 | 802.1x |
| | 802.1x | Radius Server | IP <input type="text"/> Port <input type="text" value="1812"/> Secret <input type="text"/> |

- 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.

| | | | |
|----------|---------------|----------------|------------------------------------|
| Security | Security Type | WPA2 Mixed | WPA-PSK |
| | WPA-PSK | Passphrase/PSK | <input type="text"/> Passphrase |

| | | | |
|----------|---------------|---------------|--|
| Security | Security Type | WPA2 Mixed | 802.1x |
| | 802.1x | Radius Server | IP <input type="text"/> Port <input type="text" value="1812"/> Secret <input type="text"/> |

- **Access Control Setting:** 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**.

| Access Control | | | |
|------------------|--|---|--|
| Status | | Enabled <input type="button" value="v"/> Disabled Enabled | |
| MAC Address List | | | |
| 1 | <input type="text" value="00:00:00:00:00:00"/> | 2 | <input type="text" value="00:00:00:00:00:00"/> |
| 3 | <input type="text" value="00:00:00:00:00:00"/> | 4 | <input type="text" value="00:00:00:00:00:00"/> |
| 5 | <input type="text" value="00:00:00:00:00:00"/> | 6 | <input type="text" value="00:00:00:00:00:00"/> |
| 7 | <input type="text" value="00:00:00:00:00:00"/> | 8 | <input type="text" value="00:00:00:00:00:00"/> |
| 9 | <input type="text" value="00:00:00:00:00:00"/> | 10 | <input type="text" value="00:00:00:00:00:00"/> |
| 11 | <input type="text" value="00:00:00:00:00:00"/> | 12 | <input type="text" value="00:00:00:00:00:00"/> |
| 13 | <input type="text" value="00:00:00:00:00:00"/> | 14 | <input type="text" value="00:00:00:00:00:00"/> |
| 15 | <input type="text" value="00:00:00:00:00:00"/> | 16 | <input type="text" value="00:00:00:00:00:00"/> |
| 17 | <input type="text" value="00:00:00:00:00:00"/> | 18 | <input type="text" value="00:00:00:00:00:00"/> |
| 19 | <input type="text" value="00:00:00:00:00:00"/> | 20 | <input type="text" value="00:00:00:00:00:00"/> |

- **Status**

After clicking the hyperlink of Status, you can see the basic information of the AP including **AP Name**, **AP Type**, **LAN MAC**, **Wireless LAN MAC**, **Up Time**, **Report Time**, **SSID**, **Number of Associated Clients** and **Remark**. In the 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**.

| AP Status Summary | |
|------------------------------|--------------|
| AP Name | NEWDEV-00002 |
| AP Type | WAP-0006 |
| LAN MAC | |
| Wireless LAN MAC | |
| Up Time | N/A |
| Report Time | N/A |
| SSID | N/A |
| Number of Associated Clients | 0 |
| Remark | |

| AP Status Detail |
|--|
| System Status |
| LAN Status |
| Wireless LAN Status |
| Access Control Status |
| Associated Client Status |

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

| System Information | |
|---------------------|---------------------|
| AP Name | NEWDEV-00002 |
| AP Status | Online |
| Last Reporting Time | 2006-06-28 10:27:37 |

- **LAN Status:** 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 LAN Status:** 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 Status:** 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 |

- **Associated Client Status:** 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

Use this function to detect and manage all of the APs in the network segments.

| AP Discovery | | | | |
|----------------|--------------------------------------|----------|-------------|--------------|
| Interface | Private LAN <input type="checkbox"/> | Base IP | 192.168.2.1 | Pool Size 12 |
| | LAN1~4 <input type="checkbox"/> | Base IP | 192.168.1.1 | Pool Size 12 |
| AP Access | AP Type | | WAP-0006 | |
| | IP Address Range | Start IP | 192.168.2.1 | |
| | | End IP | 192.168.2.1 | |
| | ID | | admin | |
| Password | | 1234 | | |
| Auto-Discovery | Status | Disabled | | Discover |
| Configure | | | | |

| Discovered AP List | | | | | |
|---|------|------------|----------|----------|-----|
| MAC Address | Name | IP Address | Password | Template | Add |
| (Total: 0) First Prev Next Last | | | | | |

- To discover AP manually, please fill in the required data.
 - **Interface:** Check **Private LAN** or/and **LAN1~4** and enter the **Base IP** and **Pool Size** (the discovered APs will be configured to use IP address among the pool).
 - **AP Access:** Input the **IP Address Range** (the default is 192.168.2.1/192.168.2.1), **ID** (the default is admin) and **Password** (the default is 1234) of the AP.

Then click the **Discover** button and the APs match the given settings will show in the list below. If the IP address you set is used, there will be a warning message showing up, please change the IP range on Base IP or Pool Size and then click **Discover** again. For the desired AP, input the desired Name and password, if changed for AP admin, select one template, check it and then click **Add** to add it under the managed list. (About the template, please see 4.3.4 Template Settings).

| AP Discovery | | | | |
|----------------|---|----------|-------------|--------------|
| Interface | LAN1~4 <input type="checkbox"/> | Base IP | 192.168.1.1 | Pool Size 12 |
| | Private LAN <input checked="" type="checkbox"/> | Base IP | 192.168.2.1 | Pool Size 12 |
| AP Access | AP Type | | WAP-0006 | |
| | IP Address Range | Start IP | 192.168.2.1 | |
| | | End IP | 192.168.2.1 | |
| | ID | | admin | |
| Password | | 1234 | | |
| Auto-Discovery | Status | Disabled | | Discover |
| Configure | | | | |

| Unavailable IP range. The following IP addresses have been used. Please change the IP range on Base IP or Pool Size. | | |
|--|-------------|-------------------|
| Interface | IP Address | MAC Address |
| Private LAN | 192.168.2.1 | 00:11:6B:30:85:63 |

| AP List | | | | | |
|---|------|------------|----------|----------|-----|
| MAC Address | Name | IP Address | Password | Template | Add |
| (Total: 0) First Prev Next Last | | | | | |

When the matched AP is discovered, it will show up in the list below and be given a new IP address as you set (ex: 192.168.2.2). Check the Add box to add the AP and it will be listed to the AP list.

| AP Discovery | | | | | | |
|----------------|------------------|-------------------------------------|--|--|--|---|
| Interface | LAN1~4 | <input type="checkbox"/> | Base IP | <input type="text" value="192.168.1.1"/> | Pool Size | <input type="text" value="12"/> |
| | Private LAN | <input checked="" type="checkbox"/> | Base IP | <input type="text" value="192.168.2.2"/> | Pool Size | <input type="text" value="12"/> |
| AP Access | AP Type | | WAP-0006 | | | <input type="button" value="Discover"/> |
| | IP Address Range | Start IP | <input type="text" value="192.168.2.1"/> | | | |
| | | End IP | <input type="text" value="192.168.2.1"/> | | | |
| | ID | | <input type="text" value="admin"/> | | | |
| Password | | <input type="text" value="1234"/> | | | | |
| Auto-Discovery | Status | Disabled | | | <input type="button" value="Configure"/> | |

| AP List | | | | | |
|---|---|-------------|-----------------------------------|--|--------------------------|
| MAC Address | Name | IP Address | Password | Template | Add |
| 00:11:6B:30:85:63 | <input type="text" value="NEWDEV-000"/> | 192.168.2.2 | <input type="text" value="1234"/> | <input type="text" value="TEMPLATE1"/> | <input type="checkbox"/> |
| (Total: 1) First Prev Next Last | | | | | |
| Last discovery was at 2006 June 28, 13:49:40. | | | | | |

Click Configuring to go on the related configuration. For the details, please refer to **4.3.1 AP List**.

| AP List | | | | |
|--|----------|------------------------------|-------------------|-----------------------------|
| <input type="checkbox"/> | AP Type | AP Name | IP | Status |
| | | | MAC | |
| <input checked="" type="checkbox"/> | WAP-0006 | NEWDEV-00001 | 192.168.2.2 | Configuring |
| | | | 00:11:6B:30:85:63 | |
| <input type="button" value="Reboot"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/> <input type="button" value="Apply Template"/> | | | | |
| (Total: 1) First Prev Next Last | | | | |

- **Auto-Discovery:** click Configure to enter Auto-Discovery interface to go on related configuration.

| AP Discovery | | | |
|-----------------------|--------------------------------------|---|---|
| Interface | Private LAN <input type="checkbox"/> | Base IP | 192.168.2.1 Pool Size 12 |
| | LAN1~4 <input type="checkbox"/> | Base IP | 192.168.1.1 Pool Size 12 |
| AP Access | AP Type | | WAP-0006 |
| | IP Address Range | Start IP | 192.168.2.1 |
| | | End IP | 192.168.2.1 |
| | ID | | admin |
| Password | | 1234 | |
| | | | <input type="button" value="Discover"/> |
| Auto-Discovery | Status | Disabled <input type="button" value="Configure"/> | |

The **Interface** and **AP Access** configuration is the same as the settings mentioned above. For the Auto-Discovery Status, when you enable this function, the system will scan once every 10 minutes or the time you set. If any AP is discovered and “Auto-Add AP” enabled, it will be assigned an available IP from the IP pool set within the interfaces and applied with the selected template.

| Auto-Discovery | | | |
|-----------------------|--------------------------------------|---|--------------------------|
| Interface | Private LAN <input type="checkbox"/> | Base IP | 192.168.2.1 Pool Size 12 |
| | LAN1~4 <input type="checkbox"/> | Base IP | 192.168.1.1 Pool Size 12 |
| AP Access | AP Type | | WAP-0006 |
| | IP Address Range | Start IP | 192.168.2.1 |
| | | End IP | 192.168.2.1 |
| | ID | | admin |
| Password | | 1234 | |
| Auto-Discovery | Status | <input checked="" type="radio"/> Enable <input type="radio"/> Disable Interval 10 minutes Auto-Add AP <input type="radio"/> Enable <input checked="" type="radio"/> Disable Template TEMPLATE1 | |

4.3.3. Manual Configuration

The AP also can be added manually. Input the related data of the AP and select a Template. Then click **ADD**, the AP will be added to the managed list.

| Manual Configuration | |
|----------------------|--|
| AP Type | WAP-0006 |
| AP Name | <input type="text"/> |
| Admin Password | <input type="text" value="1234"/> |
| AP IP | <input type="text" value="192.168.2.1"/> |
| AP MAC | <input type="text"/> |
| Remark | <input type="text"/> |
| Template | TEMPLATE3 ▾ |

4.3.4. Template Settings

Template is a model that you can copy it to every AP and not necessary to configure the AP individually. There are three templates provided and click **Edit** to go on configuration.

| Template Settings | |
|-------------------------------------|--|
| AP Type | WAP-0006 |
| Template Settings | TEMPLATE1 ▾ TEMPLATE1 TEMPLATE2 TEMPLATE3 |
| <input type="button" value="Edit"/> | |

Before configure the template, you can copy the configuration mode of a AP to the template by selecting a **Source 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 **Template ID** to go on configuration.

| Template Edit | |
|-----------------|---|
| Template ID | 1 |
| Template Name | <input type="text" value="TEMPLATE1"/> |
| Source AP | None ▾ |
| Template Remark | <input type="text" value="Template 1"/> |

| Template Edit | |
|-----------------|----------------------|
| Template ID | 1 |
| Template Name | TEMPLATE1 |
| Source AP | None |
| Template Remark | None NEWDEV-00001 |

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**.

| General | |
|-----------------|-----------------|
| Subnet Mask | 255.255.255.0 * |
| Default Gateway | 0.0.0.0 * |

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

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

4.3.5. Firmware Management

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

| Preloaded Firmware | |
|--------------------|---------|
| AP Type | Version |
| WAP-0006 | 1.22 |

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

| Firmware List | | | |
|---------------|---------|------|----------|
| File Name | Version | Size | Download |
| Checksum | | | Delete |



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.

| AP List | | | | |
|----------|-----------------|---------------------|-----------------|--------------------------|
| AP Name | Current Version | Last Upgrading Time | Upgrade Version | Upgrade |
| AAF6-129 | 1.20 | N/A | | <input type="checkbox"/> |
| B51A-130 | 1.20 | N/A | | <input type="checkbox"/> |

4.4. Network Configuration

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

| Network Configuration | |
|-----------------------------|--|
| Network Address Translation | AMG-2000 provides 3 types of network address translation: Static Assignments, Public Accessible Server and IP/Port Redirect. |
| Privilege List | System provides Privilege IP Address List and Privilege MAC Address List. System will NOT authenticate those listed devices. |
| Monitor IP List | System can monitor up to 40 network devices online status with an option to add them as public access servers via HTTP or HTTPS. Even under NAT mode, after added the devices as public access servers, the devices can be accessed by clicking the hypertext. |
| Walled Garden List | Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication. |
| Proxy Server Properties | AMG-2000 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server. |
| Dynamic DNS | AMG-2000 supports dynamic DNS (DDNS) feature. |
| IP Mobility | System supports IP PNP Configuration. |

4.4.1. Network Address Translation

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

| Network Address Translation |
|--|
| DMZ (Demilitarized Zone) |
| Public Accessible Server |
| Port and IP Redirect |

- **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.

| Automatic WAN IP Assignment | | | |
|-----------------------------|----------------------|---------------------|--------------------|
| Enable | Internal IP Address | External IP Address | External Interface |
| <input type="checkbox"/> | <input type="text"/> | 10.2.3.174 | WAN1 |

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

- **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 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="radio"/> TCP <input type="radio"/> UDP | <input type="checkbox"/> |
| 2 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="radio"/> TCP <input type="radio"/> UDP | <input type="checkbox"/> |
| 3 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="radio"/> TCP <input type="radio"/> UDP | <input type="checkbox"/> |
| 4 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="radio"/> TCP <input type="radio"/> UDP | <input type="checkbox"/> |
| 5 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="radio"/> TCP <input type="radio"/> UDP | <input type="checkbox"/> |
| 6 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="radio"/> TCP <input type="radio"/> UDP | <input type="checkbox"/> |
| 7 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="radio"/> TCP <input type="radio"/> UDP | <input type="checkbox"/> |
| 8 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="radio"/> TCP <input type="radio"/> UDP | <input type="checkbox"/> |
| 9 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="radio"/> TCP <input type="radio"/> UDP | <input type="checkbox"/> |
| 10 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="radio"/> TCP <input type="radio"/> UDP | <input type="checkbox"/> |

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

- **Port and IP Redirect**

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

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

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

4.4.2.Privilege List

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

| Privilege List |
|--|
| Privilege IP Address List |
| Privilege MAC Address List |

- Privilege IP Address List**

If there are some workstations belonging to the managed server that need to access the network without authentication, enter the IP addresses of these workstations in this list. The **“Remark”** blank is not necessary but is useful to keep track. AMG-2000 allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking **Apply**.

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

Warning: Permitting specific IP addresses to have network access rights without going through standard authentication process at the 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 | <input type="text"/> | <input type="text"/> |
| 2 | <input type="text"/> | <input type="text"/> |
| 3 | <input type="text"/> | <input type="text"/> |
| 4 | <input type="text"/> | <input type="text"/> |
| 5 | <input type="text"/> | <input type="text"/> |

Warning: Permitting specific MAC addresses to have network access rights without going through standard authentication process at the 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**”.

| 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 https | 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 |

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

Monitor

Click **Monitor** to monitor the IP addresses listed in the **Monitor IP List**. The **Monitor IP result** page shown as below will appear. In the **Result** column, green light means the IP address is alive and reachable. On the other hand, red light means the IP address is not reachable now. The administrator can understand the some networking devices by this feature.

| Monitor IP result | | |
|-------------------|--------------|---|
| No | IP Address | Result |
| 1 | 10.171.1.129 |  |
| 2 | 10.171.1.130 |  |
| 3 | 1.2.3.4 |  |

On each monitored item 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 the administrator can easily access the host when the administrator is from WAN interface and the system is running in NAT mode by clicking the hyperlink. Click the **Del** button to remove this link setting.

| Monitor IP List | | | | | | | |
|-----------------|----------|--------------|------|------|----------|--------------|------|
| Item | Protocol | IP Address | Link | Item | Protocol | IP Address | Link |
| 1 | http | 10.171.1.129 | Del | 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 |

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

Monitor

4.4.4.Walled Garden List

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

| Walled Garden List | | | |
|--------------------|---------|------|---------|
| Item | Address | Item | Address |
| 1 | | 2 | |
| 3 | | 4 | |
| 5 | | 6 | |
| 7 | | 8 | |
| 9 | | 10 | |
| 11 | | 12 | |
| 13 | | 14 | |
| 15 | | 16 | |
| 17 | | 18 | |
| 19 | | 20 | |

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

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

- **External Proxy Server:** Under the 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 not 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 8** and **Appendix 9**.

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**.

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

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

4.4.7. IP Mobility

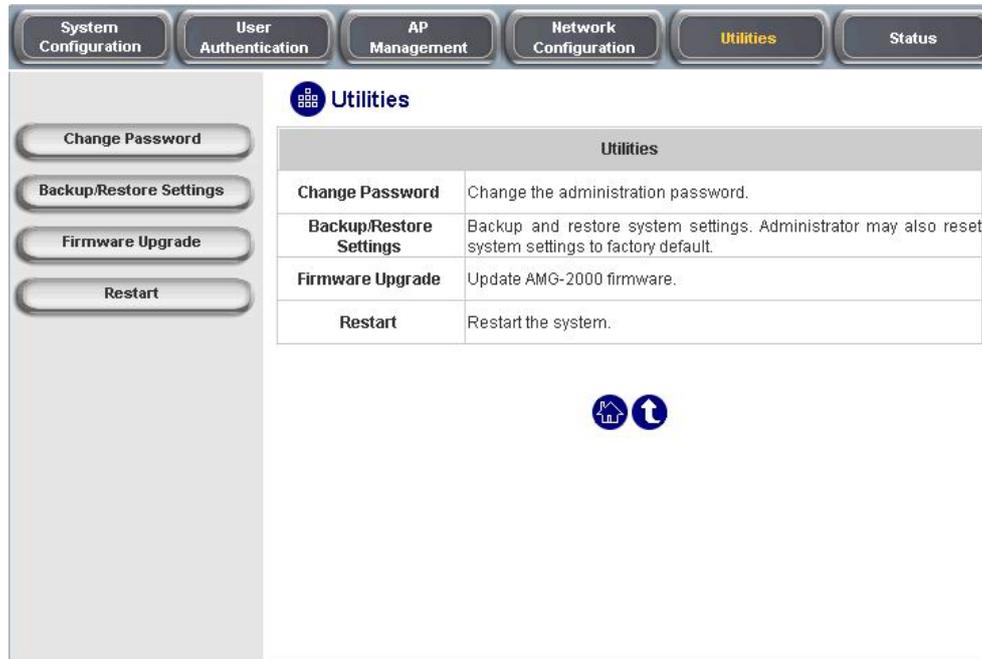
AMG-2000 supports IP PNP function.

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

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.

4.5. Utilities

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



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.

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

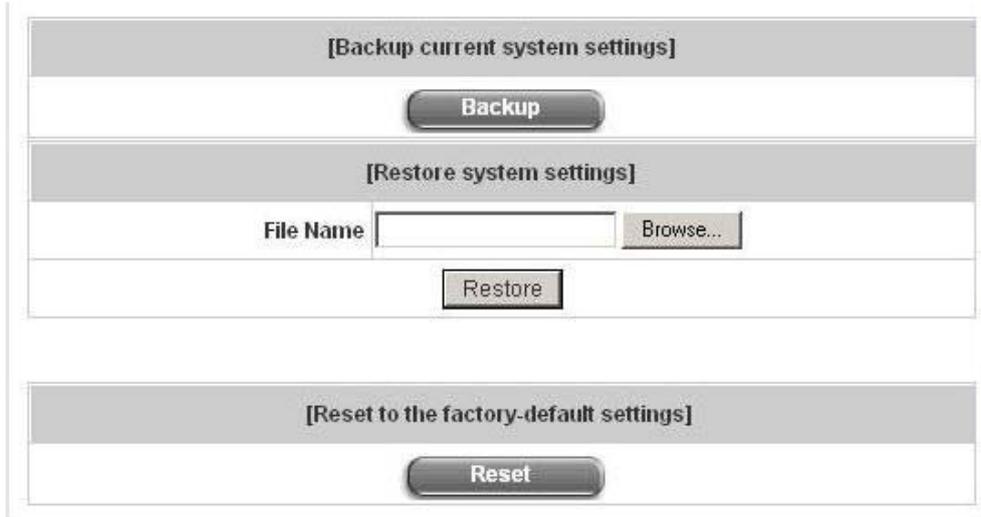
| Change Manager Password | |
|-------------------------|----------------------|
| New Password | <input type="text"/> |
| Verify Password | <input type="text"/> |

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

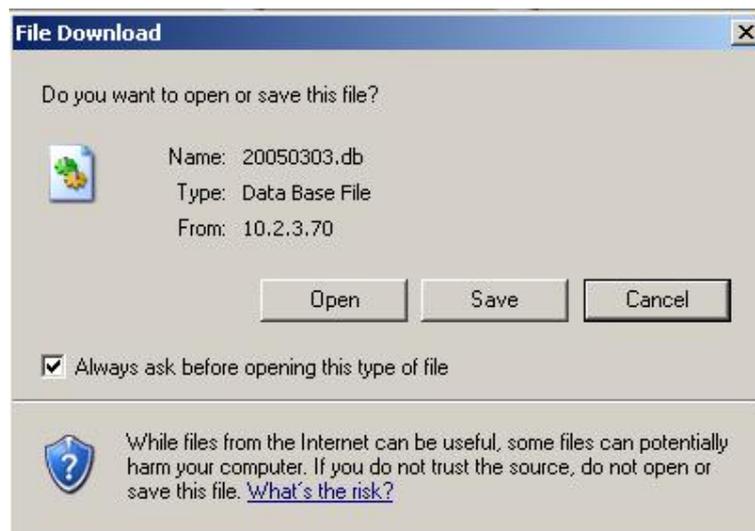
Caution: If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial port, console/printer port.

4.5.2.Backup/Restore Settings

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



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



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

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

| Firmware Upgrade | |
|------------------|---|
| Current Version | 1.00.B1 |
| File Name | <input type="text"/> <input type="button" value="Browse..."/> |

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

4.5.4. Restart

This function allows the administrator to safely restart 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.

Do you want to **Restart** AMG-2000?

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

4.6. Status

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

4.6.1. System Status

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

| System Status | | |
|-----------------------------------|---|-----------------|
| Current Firmware Version | 1.01.01 | |
| System Name | AP Management Gateway | |
| 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 | |
| Friendly Logout | Enabled | |
| Warning of Internet Disconnection | Disabled | |
| WAN Failover | Disabled | |
| Management | Remote Management IP | 0.0.0.0/0.0.0.0 |
| | SNMP | Disabled |

| | | |
|---------|----------------------|---------------------------|
| History | Retained Days | 3 days |
| | Email To | N/A |
| | | N/A |
| N/A | | |
| Time | NTP Server | (tock.usno.navy.mil) |
| | Date Time | 2006/10/05 14:05:35 +0800 |
| User | Idle Timer | 10 Min(s) |
| | Multiple Login | Disabled |
| DNS | Preferred DNS Server | 10.2.3.203 |
| | Alternate DNS Server | 168.95.1.1 |

The description of the table is as follows:

| <u>Item</u> | <u>Description</u> | |
|--|---|---|
| Current Firmware Version | The present firmware version of AMG-2000 | |
| System Name | The system name. The default is AP Management Gateway | |
| 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. | |
| Friendly Logout | 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. | |
| WAN Failover | Show WAN Failover status of WAN1 and WAN2 | |
| Management | Remote Management IP | The IP or IPs that is allowed for accessing the management interface. |
| | SNMP | Enabled/disabled stands for the current status of the SNMP management function. |
| History | Retained Days | The maximum number of days for the system to retain the users' information. |

| | | |
|-------------|-----------------------------|--|
| | Email To | The up to three email addresses that the traffic history, monitor IP report, on-demand user log, or AP status 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 | 00:90:08:07:60:93 |
| | IP Address | 10.2.3.90 |
| | Subnet Mask | 255.255.255.0 |
| LAN1~4 | Mode | NAT |
| | MAC Address | 00:90:08:07:60:91 |
| | IP Address | 192.168.1.254 |
| | Subnet Mask | 255.255.255.0 |
| LAN1~4 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) |
| Private LAN | Mode | NAT |
| | MAC Address | 00:90:0B:07:60:92 |
| | IP Address | 192.168.2.254 |
| | Subnet Mask | 255.255.255.0 |
| Private LAN DHCP Server | Status | Enabled |
| | WINS IP Address | N/A |
| | Start IP Address | 192.168.2.1 |
| | End IP Address | 192.168.2.100 |
| | Lease Time | 1440 Min(s) |

| <u>Item</u> | | <u>Description</u> |
|-------------------------------|-------------------------|--|
| WAN1 | MAC Address | The MAC address of the WAN1 port. |
| | IP Address | The IP address of the WAN1 port. |
| | Subnet Mask | The Subnet Mask of the WAN1 port. |
| WAN2 | MAC Address | The MAC address of the WAN2 port. |
| | IP Address | The IP address of the WAN2 port. |
| | Subnet Mask | The Subnet Mask of the WAN2 port. |
| LAN1~4 | 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. |
| LAN1~4 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. |
| Private LAN | Mode | The mode of the private port. |
| | MAC Address | The MAC address of the private port. |
| | IP Address | The IP address of the private port. |

| | | |
|------------------------------------|-------------------------|--|
| | Subnet Mask | The Subnet Mask of the private port. |
| Private LAN DHCP Server | Status | Enable/disable stands for status of the DHCP server on the private 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** page.

| Current Users List | | | | | | |
|--------------------|--------------|-------------------|----------|-----------|------|--------------------------|
| Item | Username | | Pkts In | Bytes In | Idle | Source AP |
| | 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 |



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 3 days.

| Traffic History | |
|----------------------------|-------------|
| Date | Size (Byte) |
| 2007-01-05 | 65 |

| On-demand User Log | |
|----------------------------|-------------|
| Date | Size (Byte) |
| 2007-01-05 | 239 |

| Roaming Out Traffic History | |
|-----------------------------|-------------|
| Date | Size (Byte) |
| 2007-01-05 | 106 |

| Roaming In Traffic History | |
|----------------------------|-------------|
| Date | Size (Byte) |
| 2007-01-05 | 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**, **Validtime** and **Remark**, of user activities.

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

- **Roaming Out Traffic History**

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

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

- **Roaming In Traffic History**

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

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

4.6.5. 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 addresses. Enter the related information and select the desired items and then apply the settings.

| E-mail Notification Configuration | | | | |
|-----------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Send To | Monitor IP Report | Traffic History | On-demand User Log | AP Status |
| casper.wu@yahoo.com.tw | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| felix@gmail.com | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Interval | 1 Hour | 1 Hour | 1 Hour | N/A |
| Send Test Email | Send | Send | Send | Send |
| Send From | casper.wu@yahoo.com.tw | | | |
| SMTP | smtp.mail.yahoo.com.tw | | | |
| Auth Method | None | | | |

| Syslog Configuration | | | |
|---------------------------|----|------------|----------|
| Traffic History | IP | 10.2.3.219 | Port 514 |
| On-demand User Log | IP | 10.2.3.203 | Port 514 |

- **Send To:** You can set up to 3 e-mail addresses to receive the notification. These are the receivers' 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.

| E-mail Notification Configuration | | | | |
|-----------------------------------|--|-------------------------------------|-------------------------------------|-------------------------------------|
| Send To | Monitor IP Report | Traffic History | On-demand User Log | AP Status |
| casper.wu@yahoo.com.tw | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| felix@gmail.com | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Interval | 1 Hour | 1 Hour | 1 Hour | N/A |
| Send Test Email | <input type="button" value="Send"/> | <input type="button" value="Send"/> | <input type="button" value="Send"/> | <input type="button" value="Send"/> |
| Send From | casper.wu@yahoo.com.tw | | | |
| SMTP | smtp.mail.yahoo.com.tw | | | |
| Auth Method | <div style="border: 1px solid black; padding: 2px;"> None Plain Login CRAM-MD5 NTLMv1 </div> | | | |
| Syslog Configuration | | | | |
| Traffic History | IP | 10.2.3.219 | Port | 514 |
| On-demand User Log | IP | 10.2.3.203 | Port | 514 |

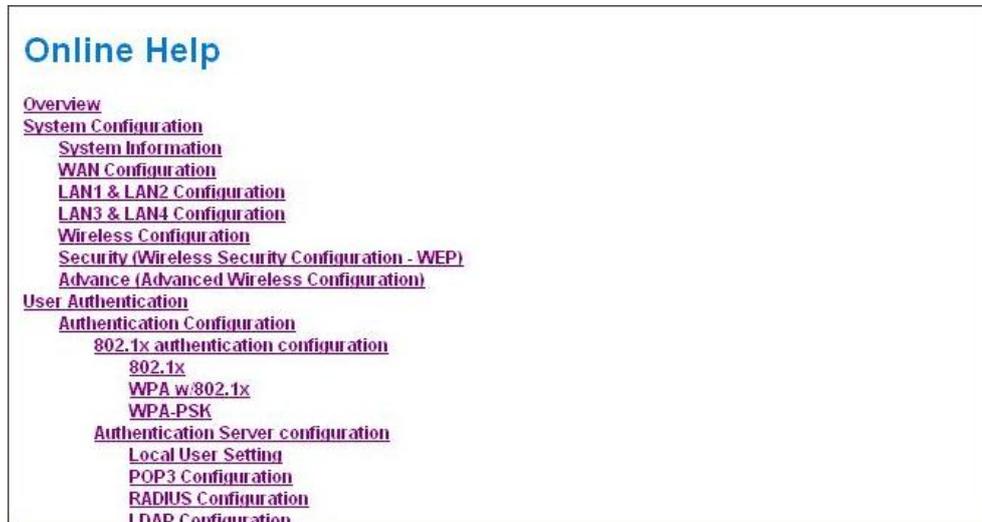
- **Syslog Configuration:** Enter the IPs and Ports of the Syslog server to receive system events including Traffic History and On-demand User Log.

| Syslog Configuration | | | | |
|---------------------------|----|------------|------|-----|
| Traffic History | IP | 10.2.3.219 | Port | 514 |
| On-demand User Log | IP | 10.2.3.203 | Port | 514 |

4.7. Help

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

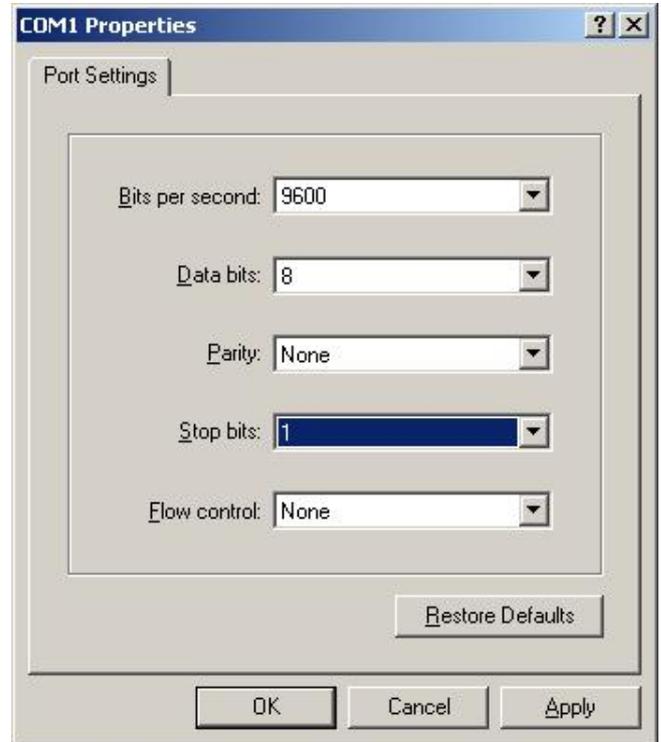
Click **Help** to the **Online Help** window and then click the hyperlink of the items to get the information.



5. Appendix A -- Console Interface

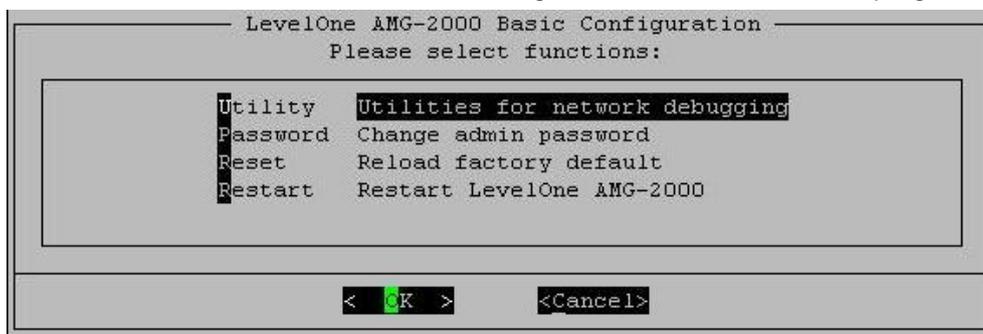
Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. To connect the console port of 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**.



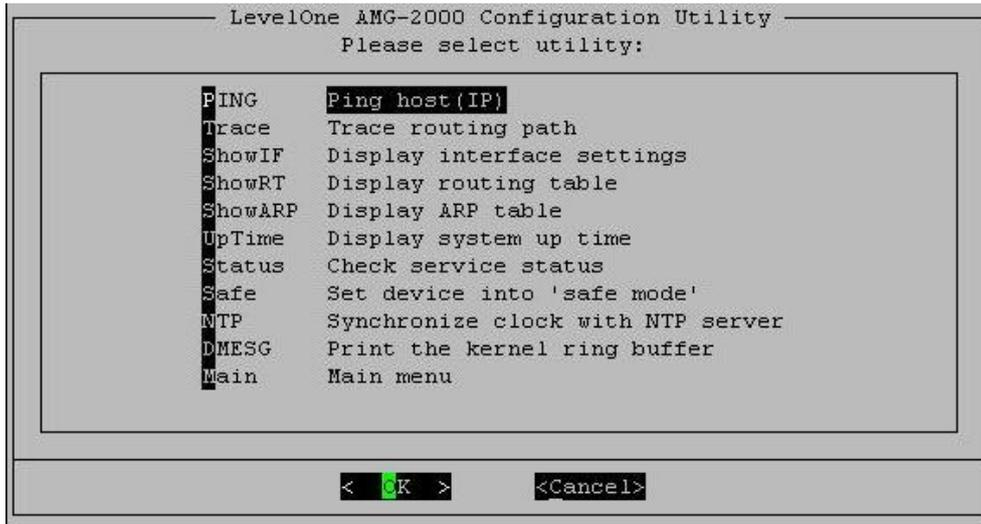
Caution: the main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the **Enter** key to make selection or confirm what you enter.

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 LevelOne AMG-2000**
Choosing this option will restart AMG-2000.

6. Appendix B -- Network Configuration on PC

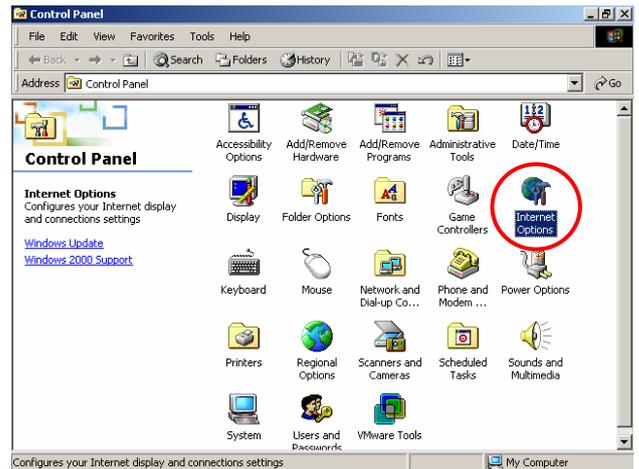
After AMG-2000 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**

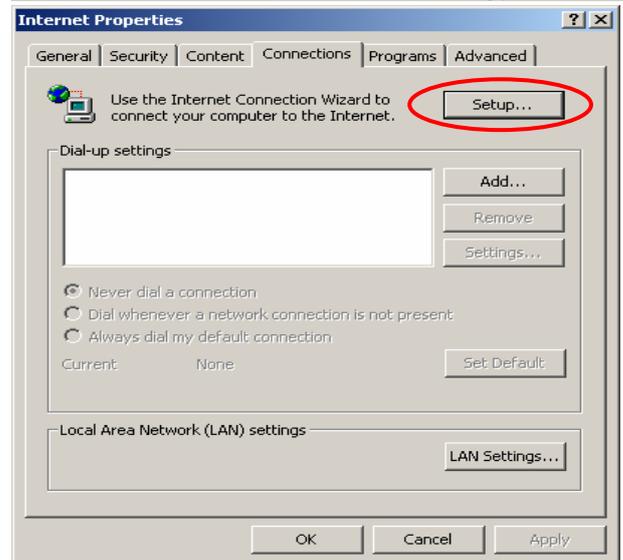
If the Internet Connection of this client PC has been configured as use local area network already, you can skip this setup.

- ◆ **Windows 9x/2000**

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



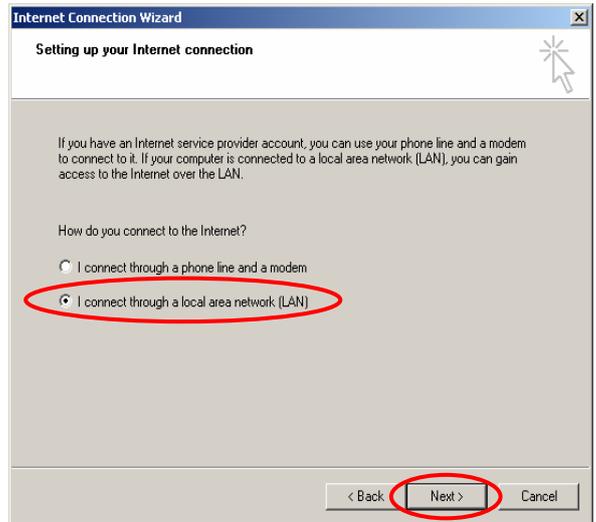
2. Choose the “**Connections**” label, and then click **Setup**.



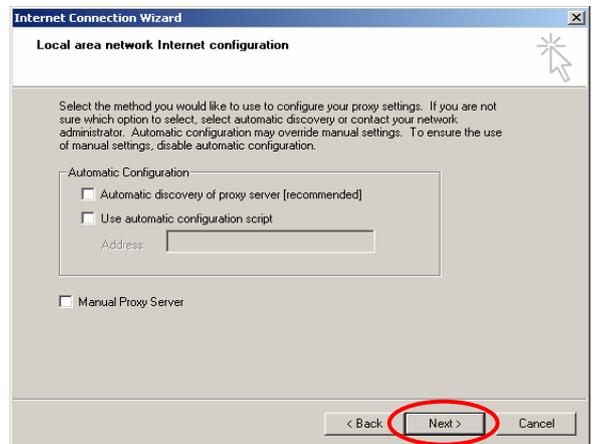
3. Choose “**I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)**”, and then click **Next**.



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.



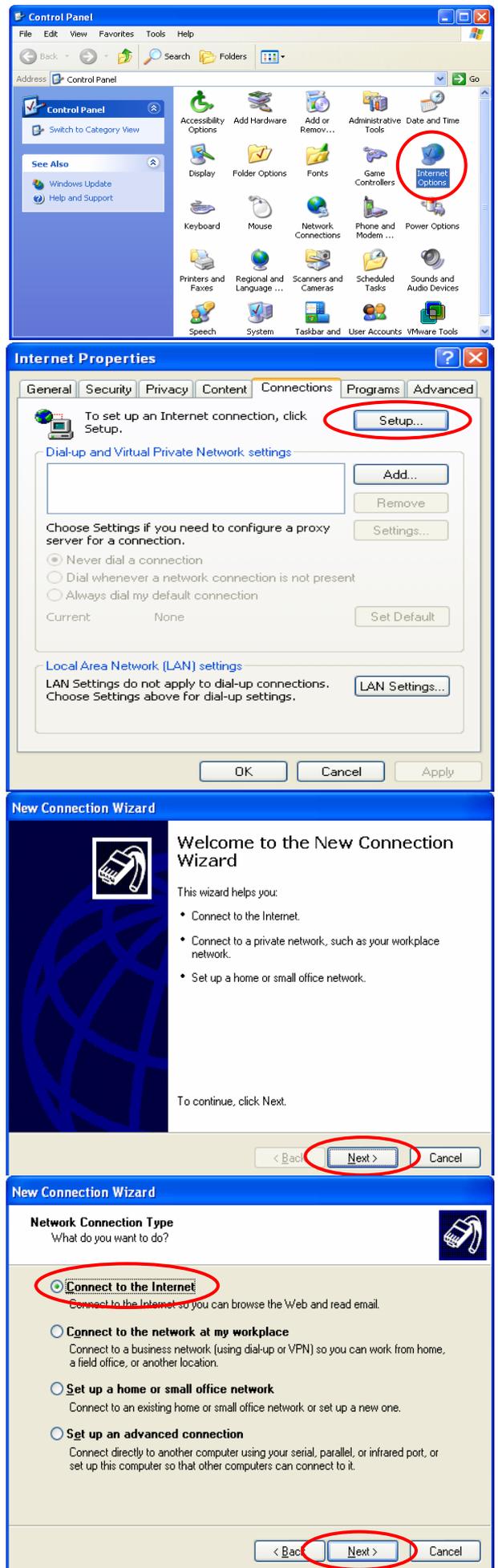
◆ **Windows XP**

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

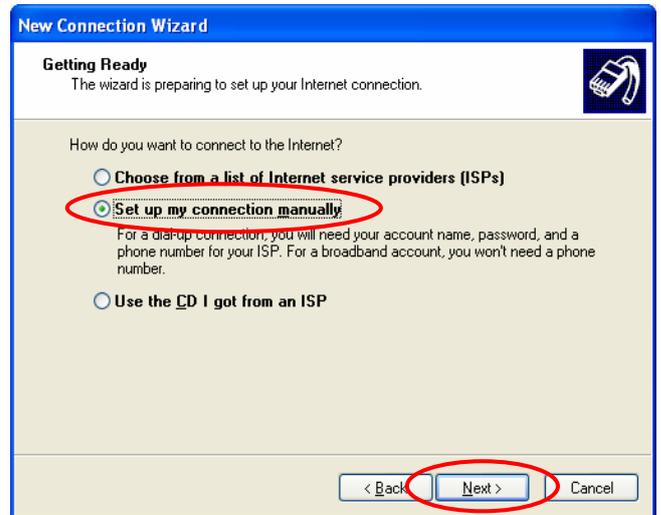
3. Choose the “**Connections**” label, and then click **Setup.**

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

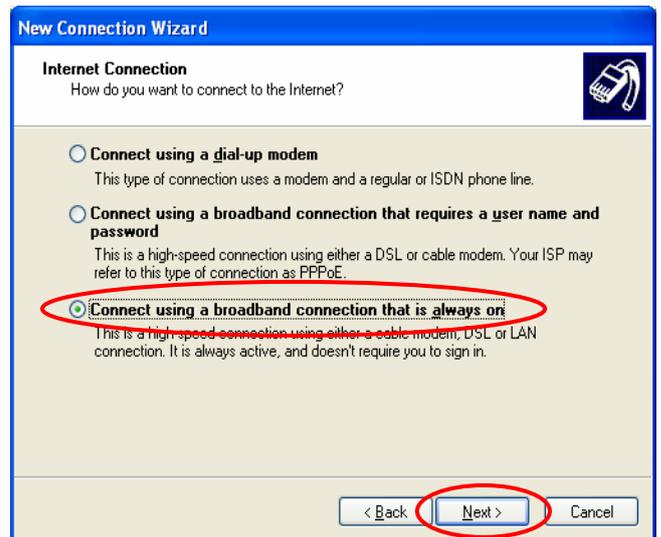
5. Choose “**Connect to the Internet**” and then click **Next.**



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



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



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



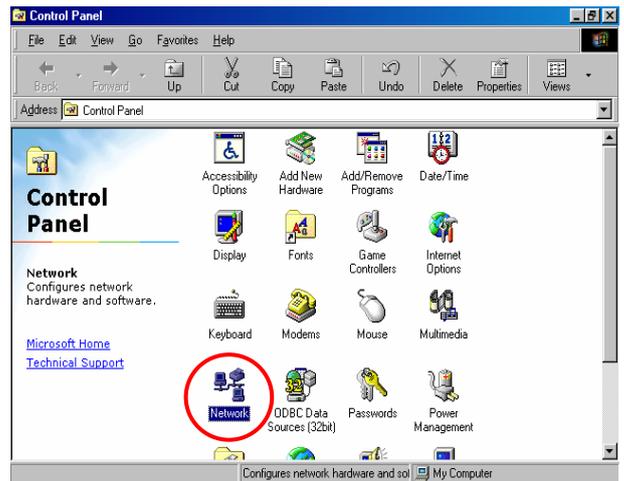
- **TCP/IP Network Setup**

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.

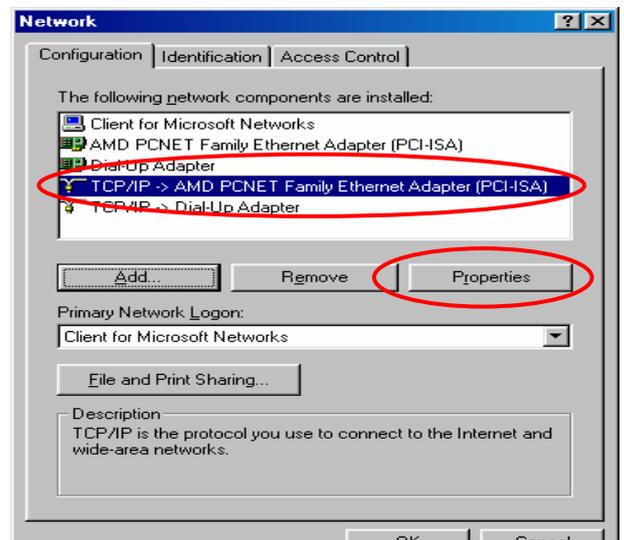
If you want to check the TCP/IP setup or use a static IP to connect to AMG-2000 LAN port, please follow the following steps:

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

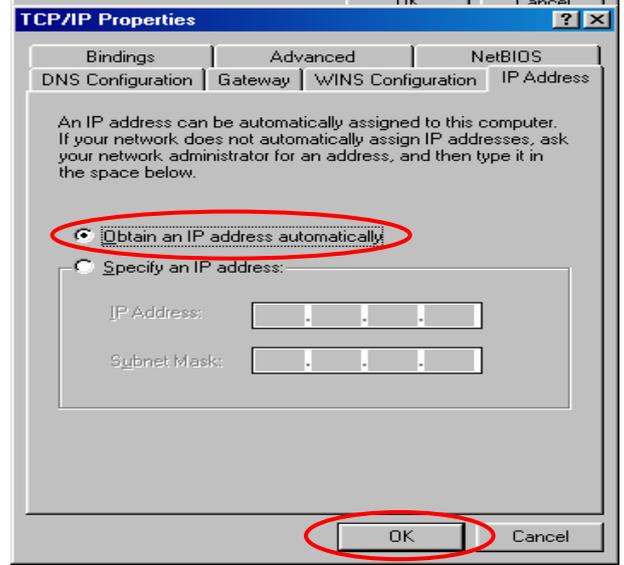
1. Choose **Start > Control Panel > Network**.



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**.

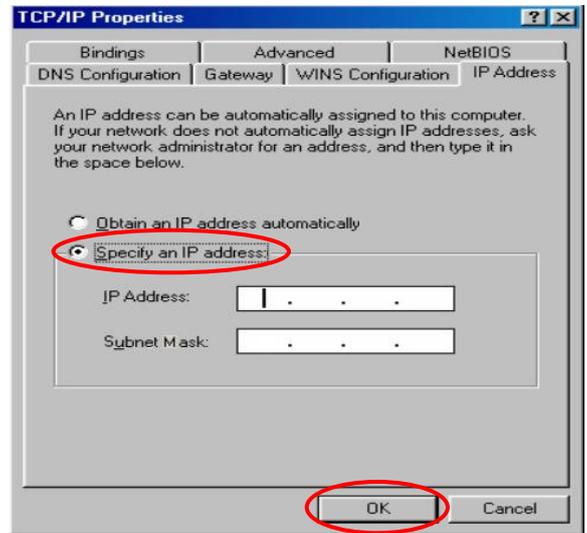


3-1. **Using DHCP:** If you want to use DHCP, please choose “**Obtain an IP address automatically**” on the “**IP Address**” label and click **OK**. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AMG-2000.

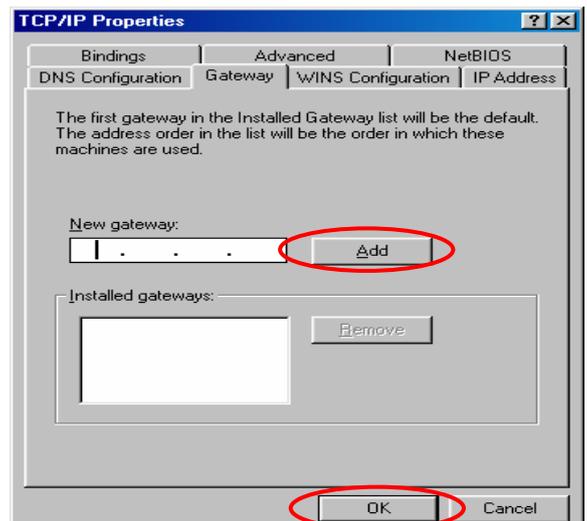


3-2. **Using Specific IP Address:** If you want to use specific IP address, you have to ask the network administrator for the information of AMG-2000: **IP address, Subnet Mask, New gateway** and **DNS server address**.

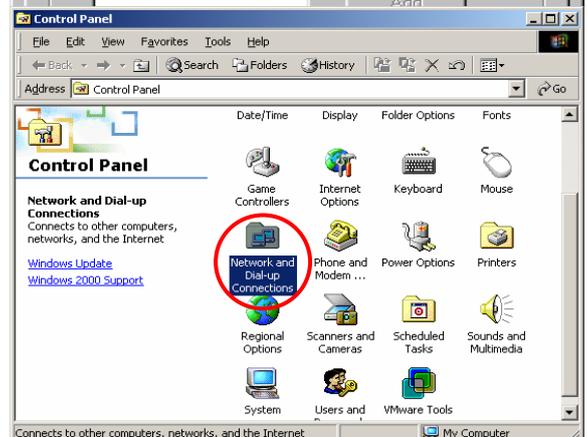
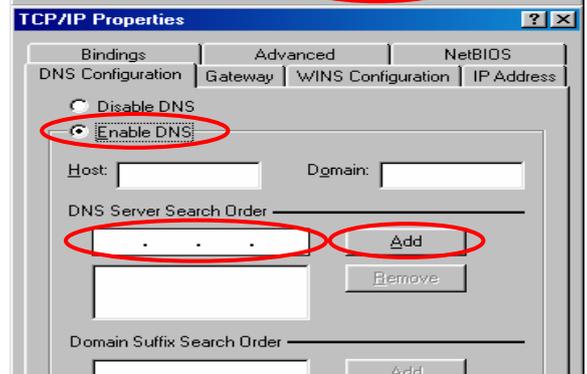
- Please choose “**Specify an IP address**” and enter the information given by the network administrator in “**IP Address**” and “**Subnet Mask**” on the “**IP Address**” label and then click **OK**.



- 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**

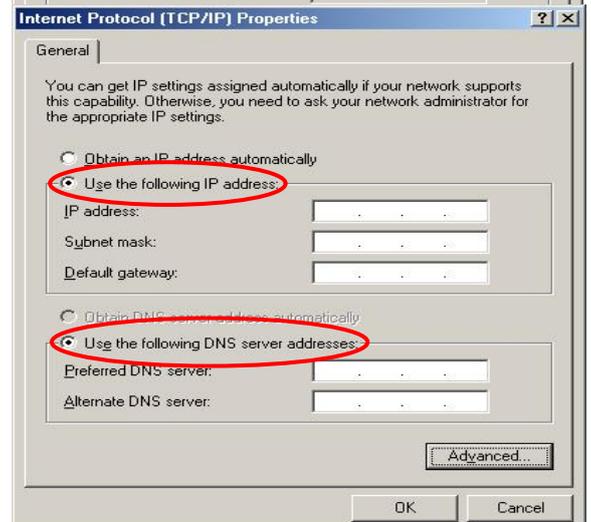
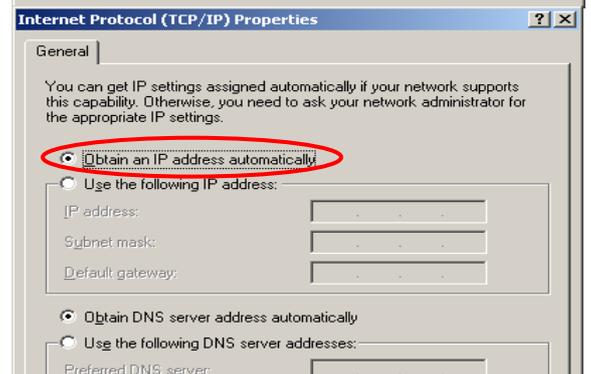
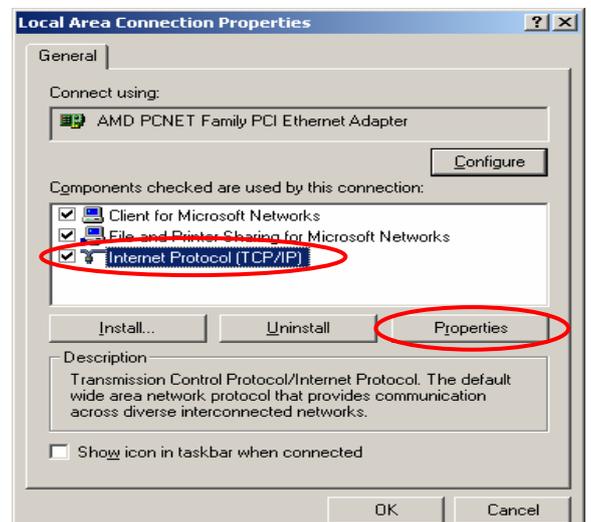
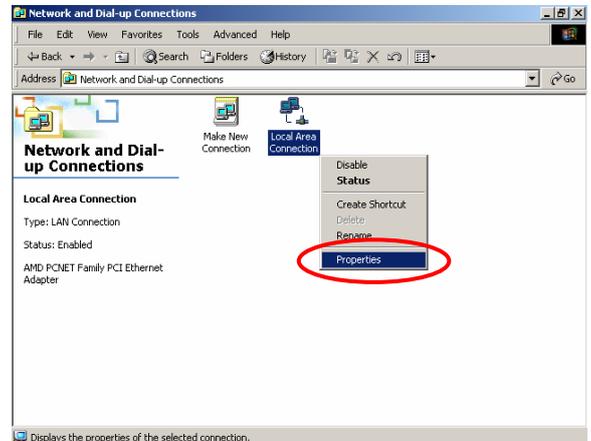
1. Select **Start > Control Panel > Network and Dial-up Connections**.

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 address**.

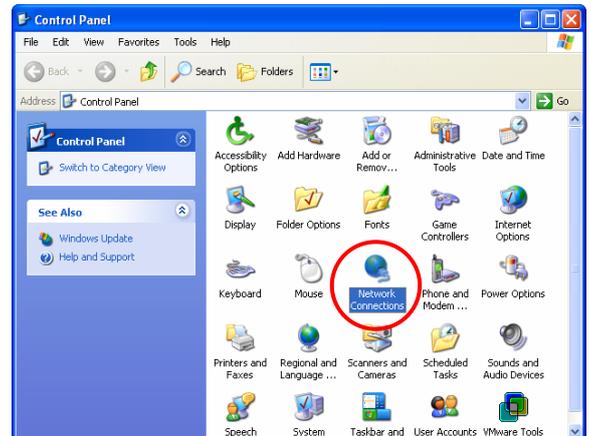


server address.

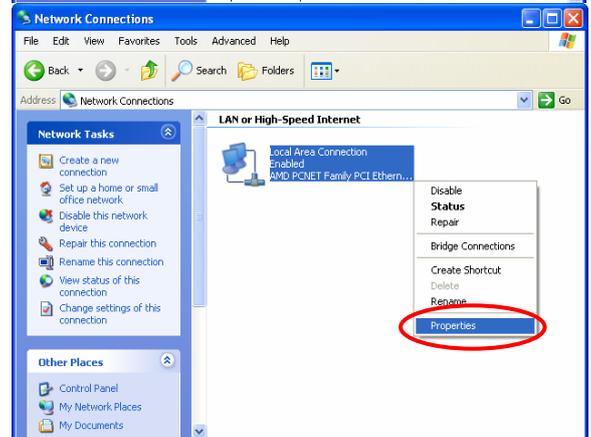
- Please choose **“Use the following IP address”** and enter the information given from the network administrator in **“IP address”**, **“Subnet mask”** and DNS address(es) and then click **OK**.

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

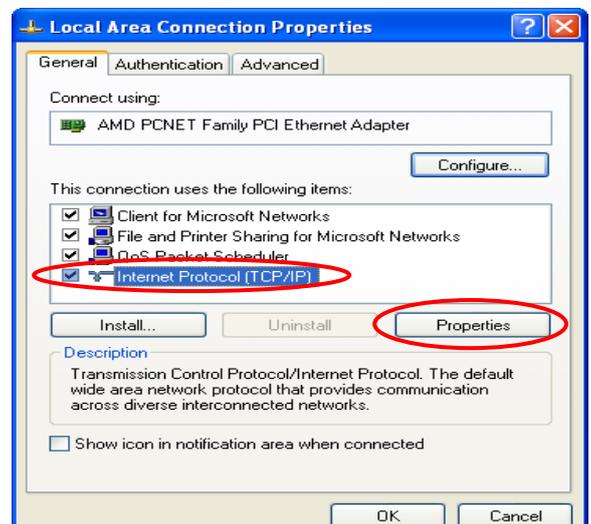
1. Select **Start > Control Panel > Network Connection**.



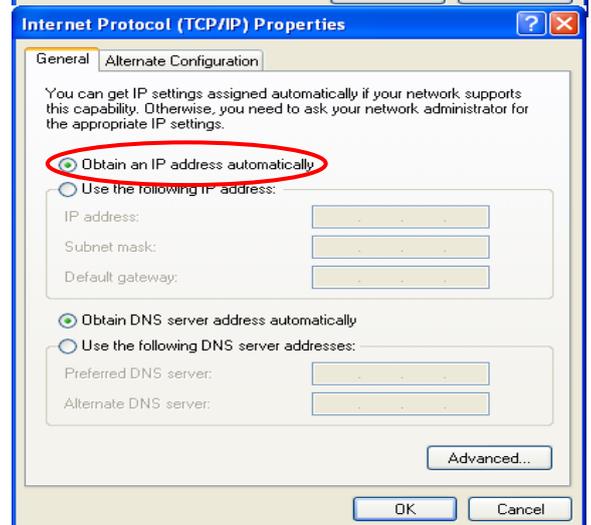
2. Click the right button of the mouse on the **“Local Area Connection”** icon and select **“Properties”**



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.

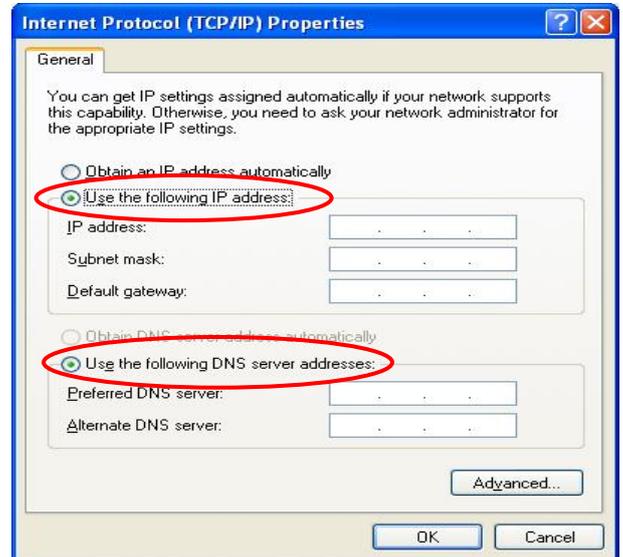


3-1. **Using DHCP:** If want to use DHCP, please choose **“Obtain an IP address automatically”** and click **OK**. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AMG-2000.



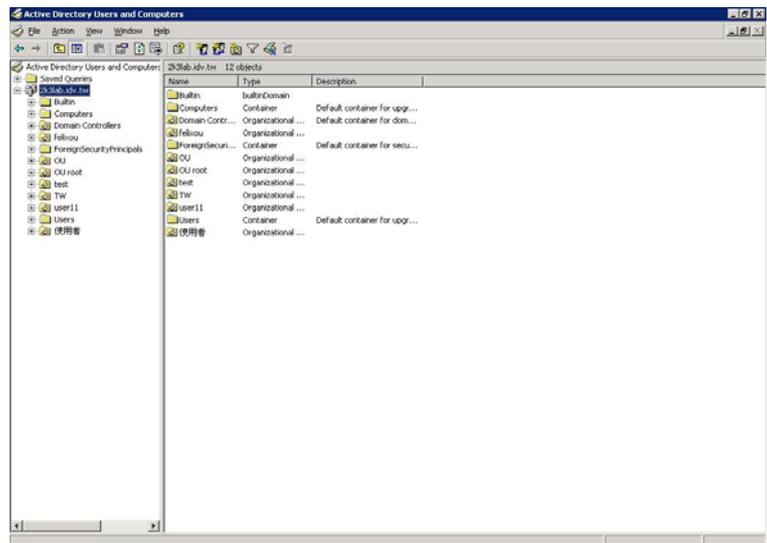
3-2. **Using Specific IP Address:** If want to use specific IP address, you have to ask the network administrator for the information of the AMG-2000: **IP address, Subnet Mask, New gateway** and **DNS server address.**

- 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**.



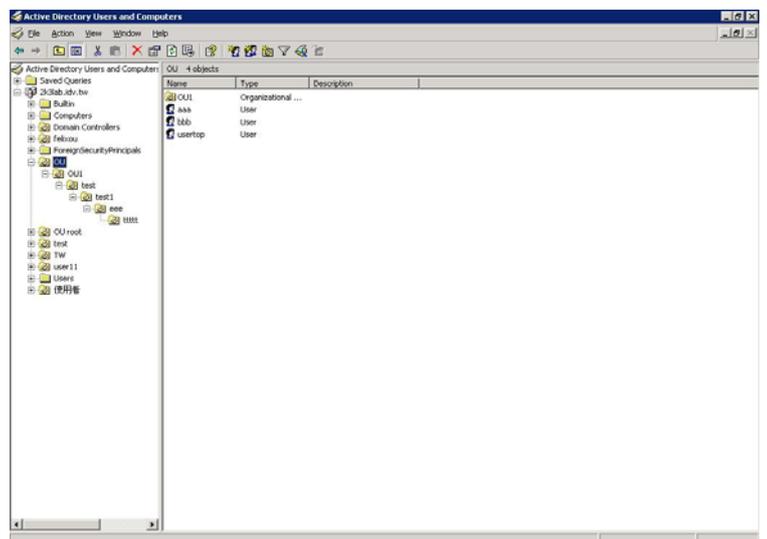
7. Appendix C - Windows Server 2000/2003 AD

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

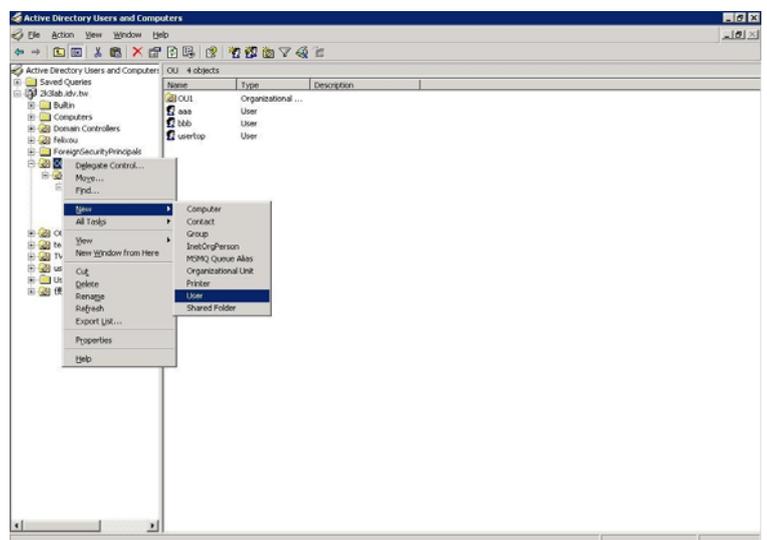


When the AMG-2000 is set up, Windows Server should be also ready by the MIS in your company. Then, you can add new user and group under the OU.

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**.

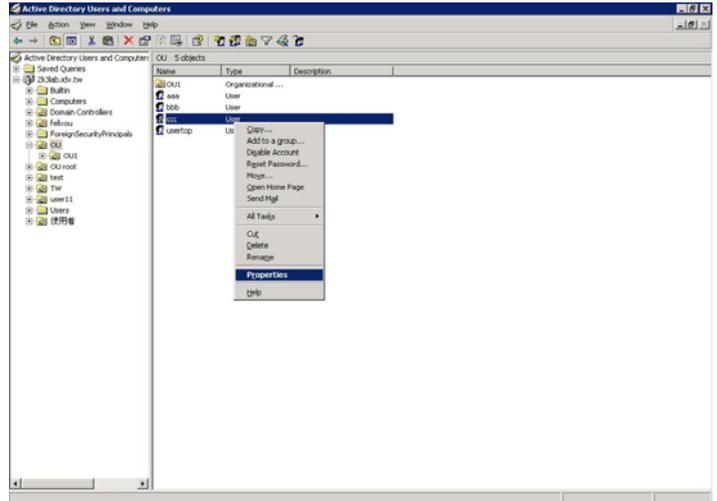
The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: 2k3lab.idv.tw/OU'. Below this are two password input fields: 'Password:' and 'Confirm password:', both containing six dots. There are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (checked), and 'Account is disabled' (unchecked). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

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

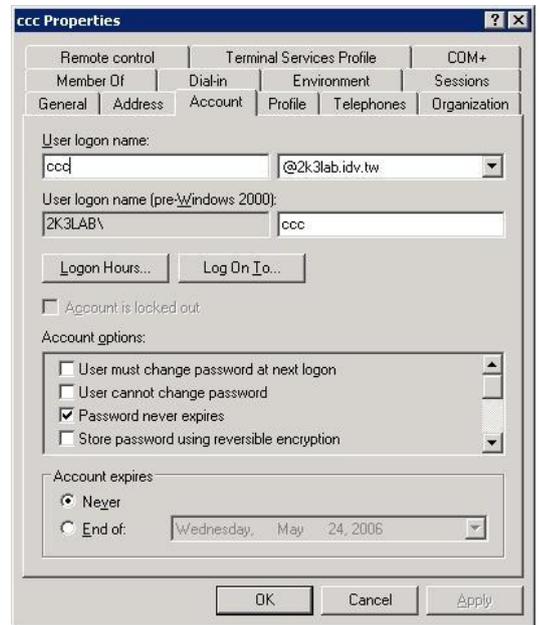
The screenshot shows the 'New Object - User' dialog box. It says 'Create in: 2k3lab.idv.tw/OU'. Below are several input fields: 'First name:' with 'ccc', 'Initials:' (empty), 'Last name:' (empty), 'Full name:' with 'ccc', 'User logon name:' with 'ccc' and a dropdown menu showing '@2k3lab.idv.tw', and 'User logon name (pre-Windows 2000):' with '2K3LAB\' and 'ccc'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

The screenshot shows the 'New Object - User' dialog box. It says 'Create in: 2k3lab.idv.tw/OU'. Below the text 'When you click Finish, the following object will be created:' is a scrollable text box containing: 'Full name: ccc', 'User logon name: ccc@2k3lab.idv.tw', and 'The password never expires.'. At the bottom are three buttons: '< Back', 'Finish', and 'Cancel'.

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

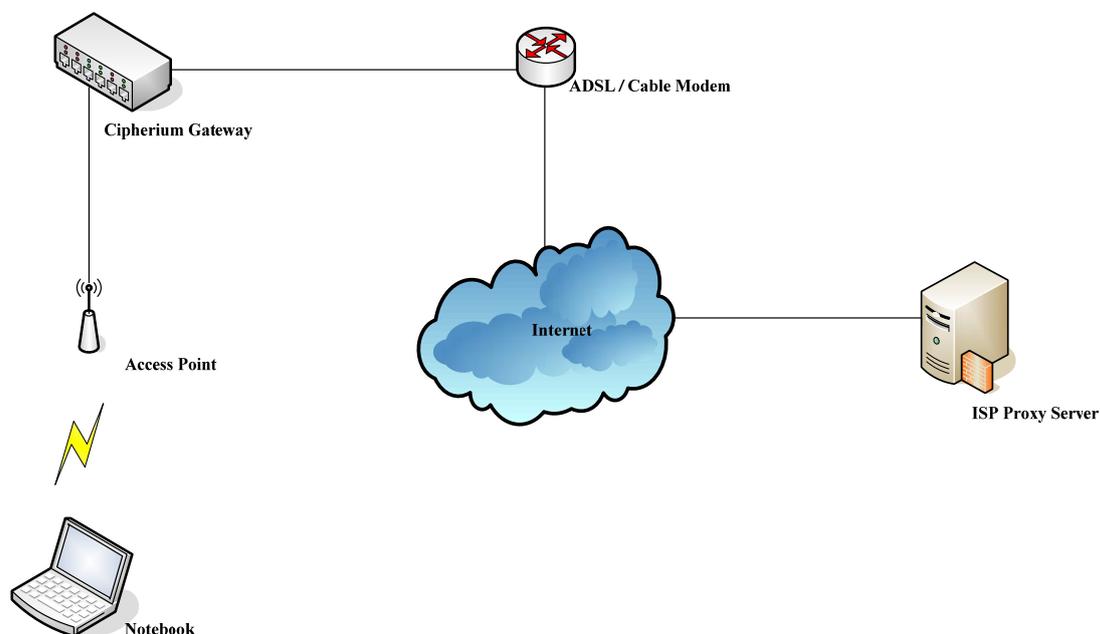
| Primary LDAP Server | |
|-----------------------|--|
| Server IP | <input type="text"/> *(Domain Name/IP) |
| Port | <input type="text"/> *(Default: 389) |
| Base DN | <input type="text"/> *(CN=,dc=,dc=) |
| Account Attribute | <input type="text"/> (Default: uid) |
| Secondary LDAP Server | |
| Server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

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**.

8. 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.

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

Network Configuration

Network Address Translation

Privilege List

Monitor IP List

Walled Garden List

Proxy Server Properties

Dynamic DNS

IP Mobility

| Network Configuration | |
|------------------------------------|--|
| Network Address Translation | AMG-2000 provides 3 types of network address translation: DMZ (Demilitarized Zone), Public Accessible Server and IP/Port Redirect. |
| Privilege List | System provides Privilege IP Address List and Privilege MAC Address List. System will NOT authenticate those listed devices. |
| Monitor IP List | System can monitor up to 40 network devices online status with an option to add them as public access servers via HTTP or HTTPS. Even under NAT mode, after added the devices as public access servers, the devices can be accessed by clicking the hypertext. |
| Walled Garden List | Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication. |
| Proxy Server Properties | AMG-2000 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server. |
| Dynamic DNS | AMG-2000 supports dynamic DNS (DDNS) feature. |
| IP Mobility | System supports IP PNP Configuration. |

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

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

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

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

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

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

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

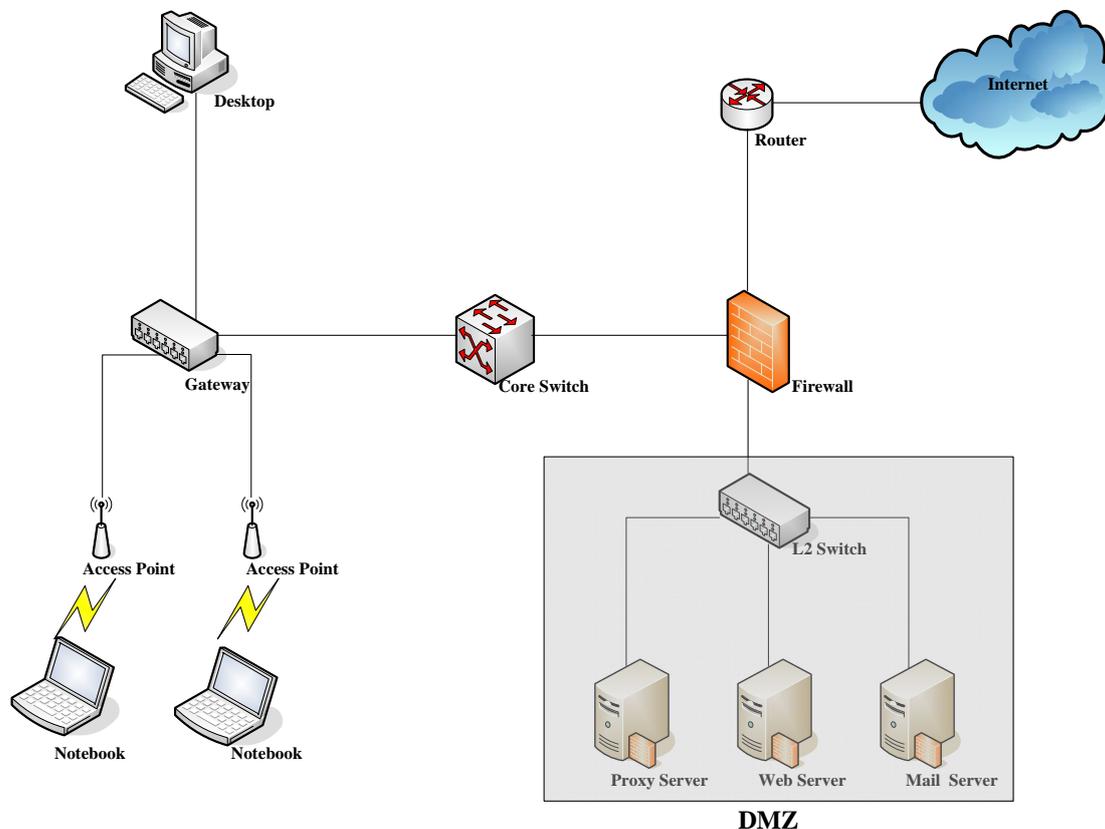
| External Proxy Server | | |
|-----------------------|---|-----------------------------------|
| Item | Server IP | Port |
| 1 | <input type="text" value="10.2.3.203"/> | <input type="text" value="6588"/> |
| 2 | <input type="text"/> | <input type="text"/> |
| 3 | <input type="text"/> | <input type="text"/>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

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

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

9. Appendix E - Proxy Setting for Enterprises

Enterprises usually isolate their Intranet and Internet by using a complex network architecture. Many enterprises have their own proxy servers which are 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 :

■ Gateway setting

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

System Configuration | User Authentication | AP Management | **Network Configuration** | Utilities | Status

Network Configuration

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

| Network Configuration | |
|------------------------------------|--|
| Network Address Translation | AMG-2000 provides 3 types of network address translation: DMZ (Demilitarized Zone), Public Accessible Server and IP/Port Redirect. |
| Privilege List | System provides Privilege IP Address List and Privilege MAC Address List. System will NOT authenticate those listed devices. |
| Monitor IP List | System can monitor up to 40 network devices online status with an option to add them as public access servers via HTTP or HTTPS. Even under NAT mode, after added the devices as public access servers, the devices can be accessed by clicking the hypertext. |
| Walled Garden List | Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication. |
| Proxy Server Properties | AMG-2000 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server. |
| Dynamic DNS | AMG-2000 supports dynamic DNS (DDNS) feature. |
| IP Mobility | System supports IP PNP Configuration. |

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

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

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

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

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

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

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

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

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

Client setting

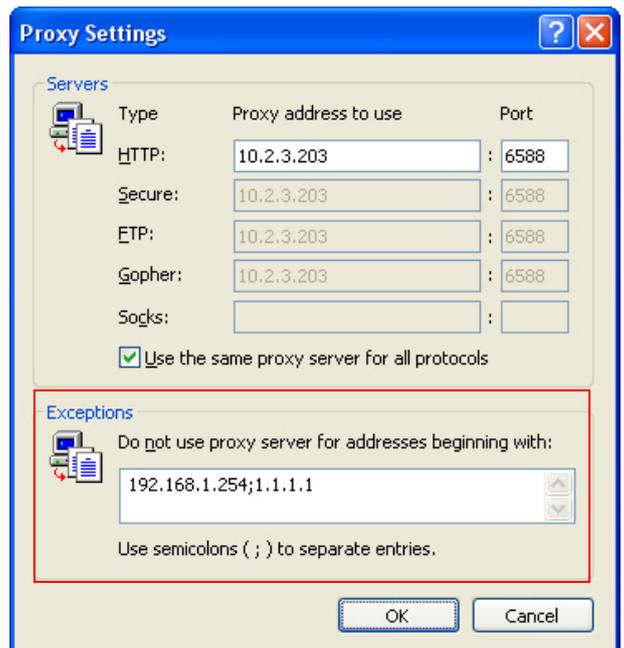
It is necessary for clients to add default gateway IP address into proxy exception information. By the way, user login successful page will appear normally.

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

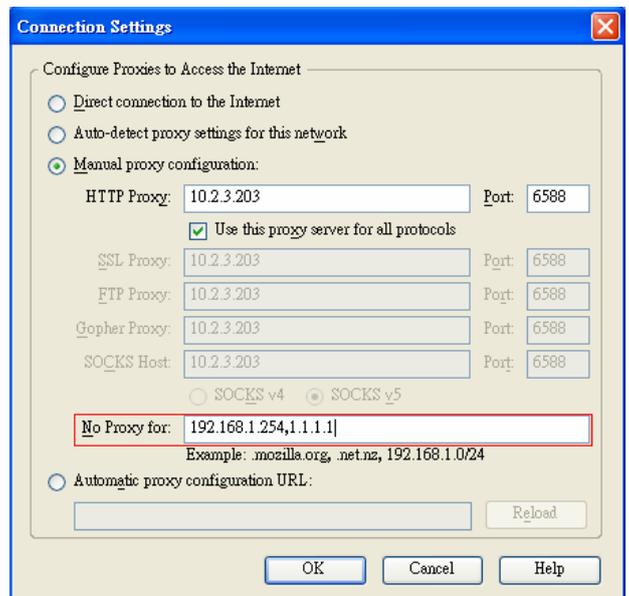


2. Open browser to add **default gateway IP address (e.g. 192.168.1.254)** and **logout page IP address "1.1.1.1"** into proxy exception information.

- For I.E



- For firefox



10. Appendix E - Glossary

802.11 standard

A family of wireless Local Area Network specifications. The 802.11b standard in particular is seeing widespread acceptance and deployment in corporate campuses as well as commercial facilities such as airports and coffee shops that want to offer wireless networking service to their patrons.

802.11a

An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.725 GHz to 5.850 GHz) with a maximum of 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency, because the 802.11a specification offers more radio channels than the 802.11b. These additional channels can help avoid radio and microwave interference.

802.11b

International standard for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput up to 11 Mbps. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz frequency band.

802.11g

Similar to 802.11b, but this standard provides a throughput up to 54 Mbps. It also operates in the 2.4 GHz frequency band but uses a different radio technology in order to boost overall bandwidth.

VLAN

Defines changes to Ethernet frames that will enable them to carry VLAN information. It allows switches to assign end-stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

Four bytes have been added to the Ethernet frame for this purpose, causing the maximum Ethernet frame length to increase from 1518 to 1522 bytes. In these 4 bytes, 3 bits allow for up to eight priority levels and 12 bits identify one of 4,094 different VLANs. 802.3ac will define the specifics of these changes for Ethernet frames.

802.1x

802.1x is a security standard for wired and wireless LANs. It encapsulates EAP processes into Ethernet packets instead of using the protocol's native PPP (Point-to-Point Protocol) environment, thus reducing some network overhead. It also puts the bulk of the processing burden upon the client (called a supplicant in 802.1x parlance) and the authentication server (such as a RADIUS), letting the "authenticator" middleman simply pass the packets back and forth. Because the authenticator does so little, its role can be filled by a device with minimal processing power, such as an access point on a wireless network.

802.3ad

802.3ad is an IEEE standard for bonding or aggregating multiple Ethernet ports into one virtual interface (also known as trunking). The aggregated ports appear as a single IP address to your computer and applications. This means no application changes are required. The advantages of aggregation are that the virtual interface provides increased bandwidth by merging the bandwidth of the individual ports. The TCP connection load is then balanced across the ports. In addition to load balancing, 802.3ad provides automatic fail-over in the event any port or cable fails. All traffic that was being routed over the failed port is automatically re-routed to use one of the remaining ports. This fail-over is completely transparent to the application software using the connection.

Access Point

A device that allows wireless-equipped computers and other devices to communicate with a wired network. It is also used to expand the range of a wireless network.

Bandwidth

The amount of transmission capacity that is available on a network at any point in time. Available bandwidth depends on several variables such as the rate of data transmission speed between networked devices, network overhead, number of users, and the type of device used to connect PCs to a network. It is similar to a pipeline in that capacity is determined by size: the wider the pipe, the more water can flow through it; the more bandwidth a network provides, the more data can flow through it. Standard 802.11b provides a bandwidth of 11 Mbps; 802.11a and 802.11g provide a bandwidth of 54 Mbps.

Baud Rate

A measure of the number of times per second a signal in a communications channel changes state. The state is usually voltage level, frequency, or phase angle.

Beacon Interval

The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.

Bit

A binary digit.

Boot

To start a device and cause it to load executing instructions.

Bridge

A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, wireless, Ethernet or token ring). Wireless bridges are commonly used to link buildings in campuses.

Broadband

A comparatively fast Internet connection. Services such as ISDN, cable modem, DSL and satellite are all considered broadband as compared to dial-up Internet access. There is no official speed definition of broadband but services of

100Kbps and above are commonly thought of as broadband.

Browser

A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web.

Cable Modem

A kind of converter used to connect a computer to a cable TV service that provides Internet access. Most cable modems have an Ethernet out-cable that attaches to the user's Wi-Fi gateway.

Client devices

Clients are the end users. Wi-Fi client devices include PC Cards that slide into laptop computers, mini-PCI modules embedded in laptop computers and mobile computing devices, as well as USB radios and PCI/ISA bus Wi-Fi radios. Client devices usually communicate with hub devices like access points and gateways.

CTS

Clear To Send. A signal sent by a device to indicate that it is ready to receive data.

Database

A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS

Dynamic Domain Name System. The capability of having a website, FTP, or e-mail server with a dynamic IP address using a fixed domain name.

Default Gateway

A device that forwards Internet traffic from your local area network.

DHCP

A utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT Manager would have to manually enter in all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it.

DHCP Servers

Dynamic Host Configuration Protocol Servers. PCs and other network devices using dynamic IP addressing are assigned a new IP address by a DHCP server. The PC or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

A DHCP server can either be a designated PC on the network or another network device, such as the Router. By default, the Router's DHCP server function is enabled.

If you already have a DHCP server running on your network, you must disable one of the two DHCP servers. If you

run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses.

Diversity Antenna

A type of antenna system that uses two antennas to maximize reception and transmission quality and reduce interference.

DMZ

Demilitarized Zone. A computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an distrusted external network, such as the public Internet.

Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

The term comes from military use, meaning a buffer area between two enemies.

DNS

A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.

Domain Name

The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general. A given machine may have more than one Domain Name but a given Domain Name points to only one machine.

DoS Attack

A type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers.

Download

To receive a file transmitted over a network.

DTIM

Delivery Traffic Indication Message. A message included in data packets that can increase wireless efficiency.

Dynamic IP Address

A temporary IP address assigned by a DHCP server.

Encryption

Encoding data to prevent it from being read by unauthorized people.

Encryption key

An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. 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.

ESSID

The identifying name of an 802.11 wireless network. When you specify your correct ESSID in your client setup you ensure that you connect to your wireless network rather than another network in range. (See SSID.) The ESSID can be called by different terms, such as Network Name, Preferred Network, SSID or Wireless LAN Service Area.

Ethernet

International standard networking technology for wired implementations. Basic 10BaseT networks offer a bandwidth of about 10 Mbps. Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps) are becoming popular.

Firewall

A system that secures a network and prevents access by unauthorized users. Firewalls can be software, hardware or a combination of both. Firewalls can prevent unrestricted access into a network, as well as restrict data from flowing out of a network.

Firmware

1. In network devices, the program that runs the device.
2. Program loaded into read-only memory (ROM) or programmable read-only memory (PROM) that cannot be altered by end-users.

Fragmentation

Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP

File Transfer Protocol. A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Full Duplex

The ability of a networking device to receive and transmit data simultaneously.

Gateway

In the wireless world, a gateway is an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

Half Duplex

Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware

The physical aspect of computers, telecommunications, and other information technology devices.

Hotspot

A place where you can access Wi-Fi service. This can be for free or for a fee. HotSpots can be inside a coffee shop, airport lounge, train station, convention center, hotel or any other public meeting area. Corporations and campuses are also implementing Hot Spots to provide wireless Internet access to their visitors and guests. In some parts of the world, Hot Spots are known as Cool Spots.

HTTP

HyperText Transport Protocol. The communications protocol used to connect to servers on the World Wide Web.

IEEE

Institute of Electrical and Electronics Engineers, New York, www.ieee.org. A membership organization that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.

Internet appliance

A computer that is intended primarily for Internet access is simple to set up and usually does not support installation of third-party software. These computers generally offer customized web browsing, touch-screen navigation, e-mail services, entertainment and personal information management applications. An Internet appliance can be Wi-Fi enabled or it can be connected via a cable to the local network.

Infrastructure

Currently installed computing and networking equipment.

Infrastructure Mode

Configuration in which a wireless network is bridged to a wired network via an access point.

IP

Internet Protocol. A set of rules used to send and receive messages at the Internet address level.

IP address

A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.

IPsec

IP Security. A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec

has been deployed widely to implement Virtual Private Networks (VPNs).

IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet.

For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

ISDN

Integrated Services Digital Network. A type of broadband Internet connection that provides digital service from the customer's premises to the dial-up telephone network. ISDN uses standard POTS copper wiring to deliver voice, data or video.

ISP

Internet Service Provider. A company that provides access to the Internet.

LAN

Local Area Network. A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.

LDAP

Lightweight Directory Access Protocol. A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called X.500-lite.

Although not yet widely implemented, LDAP should eventually make it possible for almost any application running on virtually any computer platform to obtain directory information, such as email addresses and public keys.

Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

Local User

A user that has signed up for an account from a specific ezboard community, enabling the user to participate only in that ezboard as a registered user. Global user registration from the ezboard home page is recommended for full access to all ezboard communities and the Control Center.

MAC

Media Access Control. Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the

802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.

Mbps

Megabits Per Second. One million bits per second; a unit of measurement for data transmission.

NAT

Network Address Translation. A network capability that enables a houseful of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.

Network

A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

Node

A network junction or connection point, typically a computer or work station.

Packet

A unit of data sent over a network.

Passphrase

Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for the company products.

POP

Post Office Protocol. Short for Post Office Protocol, a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol).

There are two versions of POP. The first, called POP2, became a standard in the mid-80's and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

POP3

Post Office Protocol 3. A standard protocol used to retrieve e-mail stored on a mail server.

Port

1. The connection point on a computer or networking device used for plugging in a cable or an adapter.
2. The virtual connection point through which a computer uses a specific application on a server.

PPPoE

Point-to- Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium,

such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections.

PPTP

Point-to-Point Tunneling Protocol. A new technology for creating Virtual Private Networks (VPNs), developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies, known collectively as the PPTP Forum. A VPN is a private network of computers that uses the public Internet to connect some nodes. Because the Internet is essentially an open network, the Point-to-Point Tunneling Protocol (PPTP) is used to ensure that messages transmitted from one VPN node to another are secure. With PPTP, users can dial in to their corporate network via the Internet.

Plug and Play

A computer system feature that provides automatic configuration of add-ons and peripheral devices such as wireless PC Cards, printers, scanners and multimedia devices.

Proxy server

Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.

RADIUS

Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Range

Most Wi-Fi systems will provide a range of a hundred feet or more. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to mile.

RJ-45

Standard connectors used in Ethernet networks. Even though they look very similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Roaming

Moving seamlessly from one AP coverage area to another with no loss in connectivity.

Router

A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another. Based on routing tables and routing protocols, routers can read the network address in each transmitted frame and make a decision on how to send it via the most efficient route based on traffic load, line costs, speed, bad connections, etc.

RTS

Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

Server

Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP

Simple Mail Transfer Protocol. The standard e-mail protocol on the Internet.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

Software

Instructions for the computer. A series of instructions that performs a particular task is called a "program".

SOHO

Small Office/Home Office. A term generally used to describe an office or business with ten or fewer computers and/or employees.

SSID

Service Set Identifier. A 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. (Also called ESSID.) The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet, it does not supply any security to the network. An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.

SSH

Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides

strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled.

When using ssh's login (instead of rlogin) the entire login session, including transmission of password, is encrypted; therefore it is almost impossible for an outsider to collect passwords.

SSH is available for Windows, Unix, Macintosh, and OS/2, and it also works with RSA authentication.

SSL

Secure Sockets Layer. Commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session.

Static IP Address

A fixed address assigned to a computer or device that is connected to a network.

Subnet Mask

An address code that determines the size of the network.

Subnetwork or Subnet

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

Switch

A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.

TCP

A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as a single file.

TCP/IP

The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.

TFTP

Trivial File Transfer Protocol. A version of the TCP/IP FTP protocol that uses UDP and has no directory or password capability.

UDP

User Datagram Protocol. A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

Upgrade

To replace existing software or firmware with a newer version.

Upload

To transmit a file over a network.

URL

Uniform Resource Locator. The address of a file located on the Internet.

VoIP

Voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (Plain Old Telephone Service).

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 POTS. 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.

Walled Garden

On the Internet, a walled garden refers to a browsing environment that controls the information and Web sites the user is able to access. This is a popular method used by ISPs in order to keep the user navigating only specific areas of the Web, whether for the purpose of shielding users from information -- such as restricting children's access to pornography -- or directing users to paid content that the ISP supports. America Online is a good example of an ISP that places users in a walled garden.

Schools are increasingly using the walled garden approach in creating browsing environments in their networks. Students have access to only limited Web sites, and teachers need a password in order to leave the walled garden and browse the Internet in its entirety.

The term walled garden also commonly refers to the content that wireless devices such as mobile phones have access to if the content provided by the wireless carrier is limited.

WAN

Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks (WLANs).

WEP

Wired Equivalent Privacy. Basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.

Wi-Fi

Wireless Fidelity. An interoperability certification for wireless local area network (LAN) products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards.

WLAN

Wireless Local Area Network. Also referred to as WLAN. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

WPA-Enterprise (Wi-Fi Protected Access)

Stands for Wi-Fi Protected Access – Enterprise. It is Wi-Fi's encryption method that protects unauthorized network access by verifying network users through a server.

WPA-Personal

Stands for Wi-Fi Protected Access – Personal. It is Wi-Fi's encryption method that protects unauthorized network access by utilizing a set-up password.

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.