



# Air Live<sup>®</sup>

[www.ovislink.com.tw](http://www.ovislink.com.tw)

IAS 2000

Internet Access Gateway

## User's Manual



Made by OvisLink Corp.

# Table of Contents

<b>Table of Contents</b> .....	<b><i>i</i></b>
<b>Chapter 1. Before You Start</b> .....	<b><i>1</i></b>
1.1 Audience.....	1
1.2 Document Signal .....	1
1.3 Glossary .....	1
<b>Chapter 2. Overview</b> .....	<b><i>15</i></b>
2.1 Introduction of IAS-2000 .....	15
2.2 System Concept .....	15
<b>Chapter 3. Hardware Installation</b> .....	<b><i>18</i></b>
3.1 Panel Function Descriptions .....	18
3.2 Package Contents.....	19
3.3 System Requirement.....	20
3.4 Installation Steps.....	20
<b>Chapter 4. Network Configuration on PC</b> .....	<b><i>22</i></b>
4.1 Internet Connection Setup .....	22
4.1.1 Windows 9x/2000 .....	22
4.1.2. Windows XP .....	24
4.2 TCP/IP Network Setup .....	27
4.2.1. Check the TCP/IP Setup of Window 9x/ME .....	27
4.2.2. Check the TCP/IP Setup of Window 2000 .....	30
4.2.3. Check the TCP/IP Setup of Window XP .....	33
<b>Chapter 5. Web Interface Configuration</b> .....	<b><i>36</i></b>
5.1 System Configuration .....	38
5.1.1 Configuration Wizard.....	38
5.1.2 System Information.....	47
5.1.3 WAN1 Configuration .....	48
5.1.4 WAN2 Configuration .....	50
5.1.5 LAN1 / LAN2 Configuration .....	51
5.2 Network Configuration .....	56
5.2.1 Network Address Translation .....	56
5.2.2 Privilege List .....	59
5.2.3 Monitor IP List.....	62

5.2.4	Walled Garden List.....	64
5.2.5	Proxy Server Properties.....	64
5.2.6	Dynamic DNS .....	65
5.2.7	IP Mobility .....	66
5.3	User Authentication .....	66
5.3.1	Authentication Configuration.....	67
5.3.2	Policy Configuration .....	86
5.3.3	Black List Configuration.....	91
5.3.4	Guest User Configuration.....	94
5.3.5	Additional Configuration .....	95
5.4	Utilities .....	101
5.4.1	Change Password .....	101
5.4.2	Backup/Restore Setting .....	102
5.4.3	Firmware Upgrade .....	103
5.4.4	Restart .....	104
5.5	Status .....	105
5.5.1	System Status .....	106
5.5.2	Interface Status.....	108
5.5.3	Current Users .....	110
5.5.4	Traffic History .....	111
5.5.5	Notification Configuration .....	115
5.5.6	Online Report.....	116
5.6	Help .....	118
<b>Appendix A</b>	<b>External Network Access.....</b>	<b>119</b>
<b>Appendix B</b>	<b>Console Interface Configuration .....</b>	<b>121</b>
<b>Appendix C</b>	<b>Specifications .....</b>	<b>124</b>
1.	Hardware Specification.....	124
2.	Technical Specification.....	124

# Chapter 1. Before You Start


## 1.1 Audience

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


## 1.2 Document Signal


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

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

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

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

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

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

## 1.3 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](http://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 network's 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 LAN. 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.

## Chapter 2. Overview

### 2.1 Introduction of IAS-2000

IAS-2000 is a Network Access Control System specially designed for simple small and middle-scaled wireless network environments while retaining network efficiency. IAS-2000 delivers “**manageability**”, “**efficiency**” and “**friendly interface**” and suits perfectly for campuses (or libraries, gymnasiums, etc.), small and middle enterprises, factories, Hotspots and community hospitals.

#### **Quick Installation • Get Online Immediately**

The installation and setup of IAS-2000 can be easily done without changing the existing network architecture. The system can be installed and logged within a short amount of time to establish the security mechanism. With the protection by IAS-2000, users must be authenticated before logging in to the network, and the administrator can assign a fine-grained priority to each user stratifying the scope and right of using network resources.

#### **Friendly Management and Application Interfaces**

IAS-2000 is not only easy to install, but also has multilingual management interface with operation logic that is easy to use. All of the functions of the system can be performed with a simple few clicks. The full web-based management interface allows users to operate and manage the system online via a browser. Users can easily log on to the authenticated LAN ports via the browser without any additional software installation.

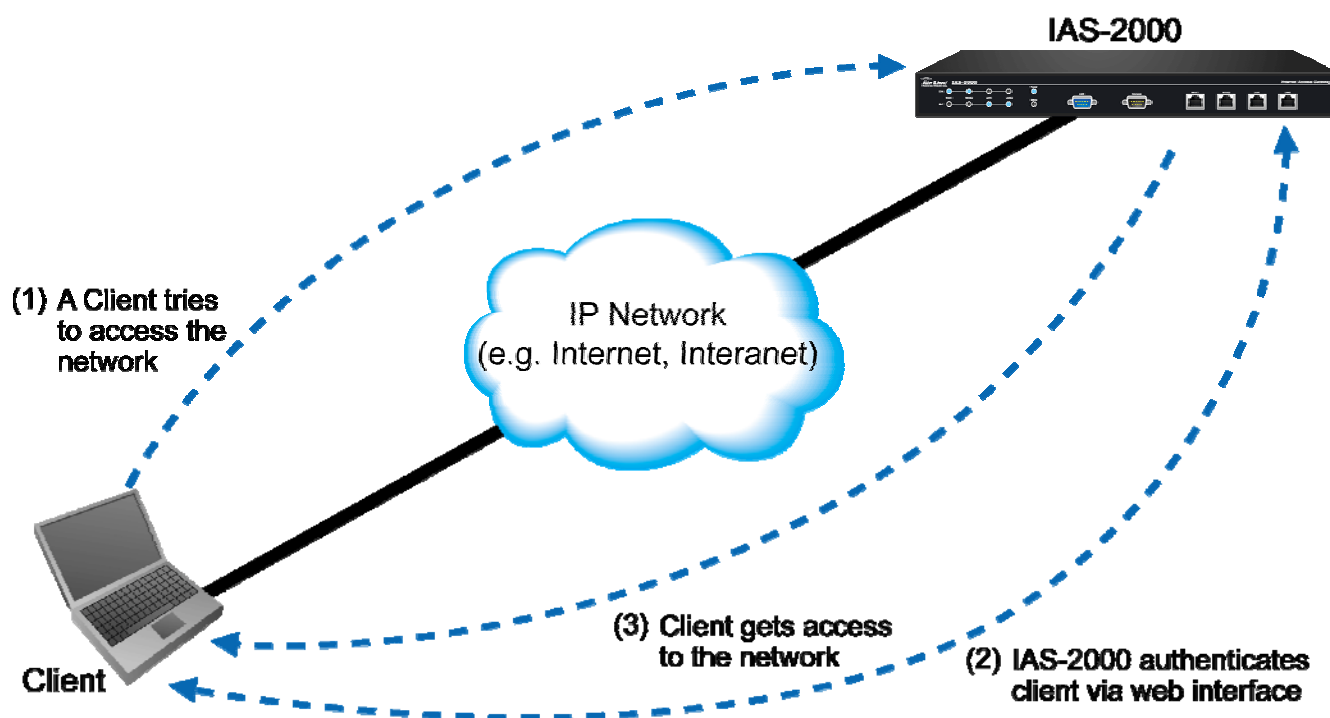
#### **Integrating the Existing User Password Database**

In general, most organizations use specific database system to centralize and manage user passwords before introducing the wireless network into the organization. IAS-2000 supports Local, POP3 (+SSL), RADIUS and LDAP external Public LAN mechanisms, and allows integration of the current user password database. This system also provides a built-in user database, so that the administrator can create or upload the Public LAN data by a batch process.

### 2.2 System Concept

IAS-2000 is responsible for controlling all network data passing through the system. The users under the managed network must be authenticated in order to obtain the right to access the network beyond the managed area. The authentication mechanism at the user’s end is provided by the IAS-2000 server, and the SSL encryption is used to protect the webpage. In the system, IAS-2000 is responsible for authentication, authorization, and management

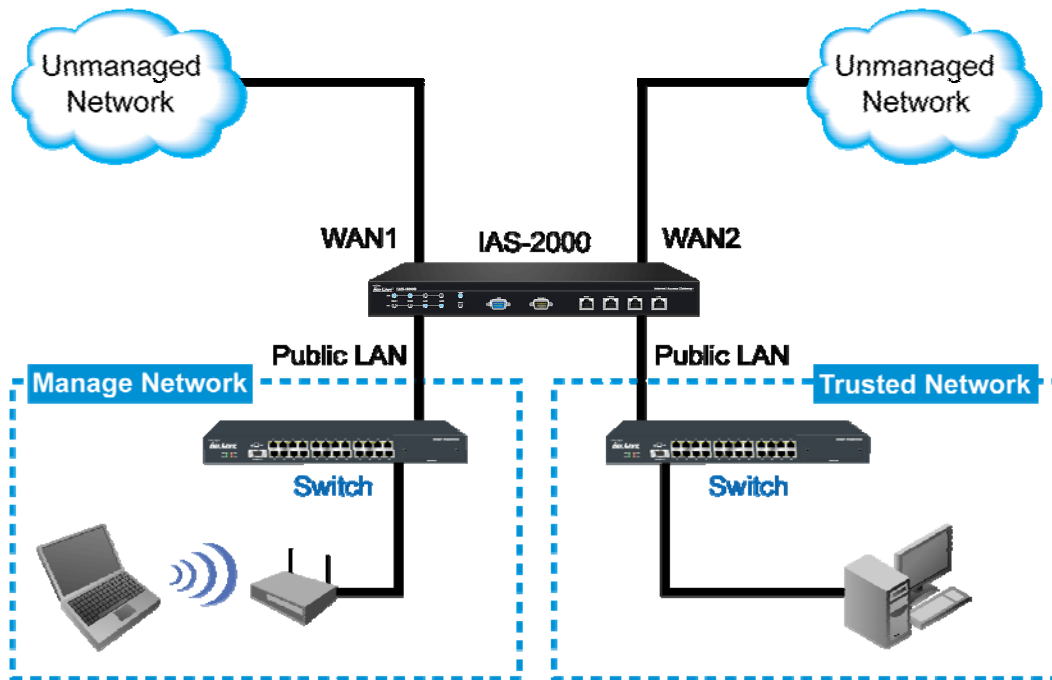
functions. The user account information is stored in the IAS-2000 database, or other specified external authentication databases.



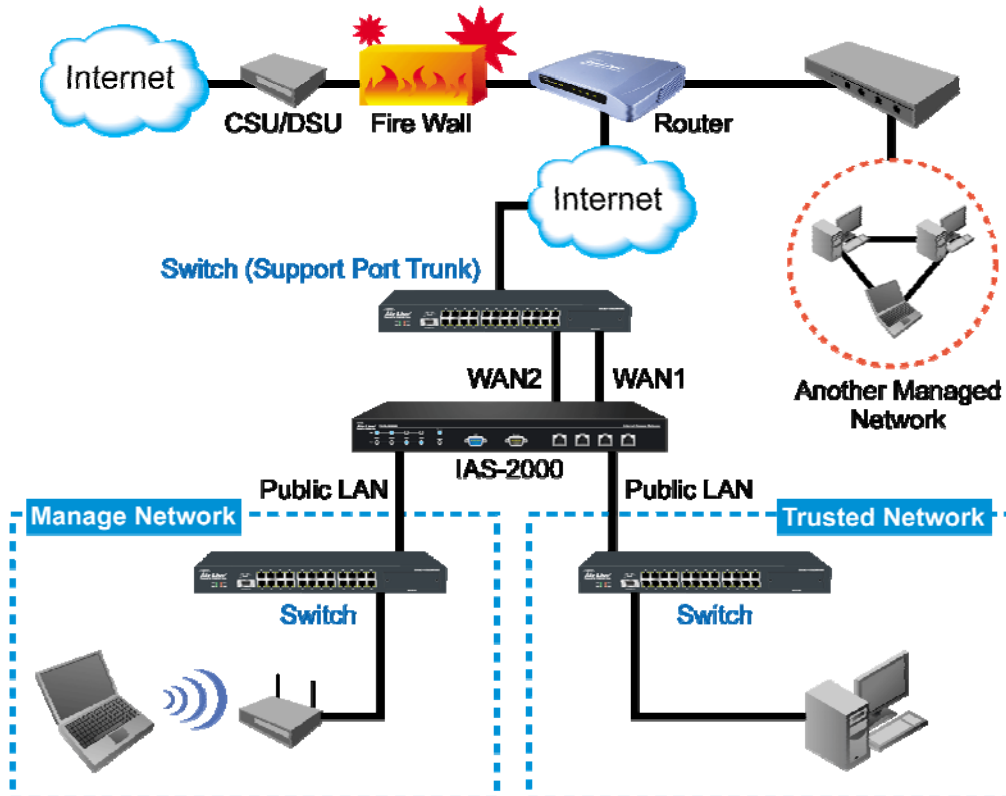
The process of authenticating the user's identity is executed via the SSL encrypted webpage. Using the web interface, it can be ensured that the system is compatible to most desktop systems and palm computers. When a user authentication is requested, the IAS-2000 server software will check the authentication database at the rear end to confirm the user's access right. The authentication database can be the local database of IAS-2000 or any external database that IAS-2000 supports. If the user is not an authorized user, IAS-2000 will refuse the user's request for the access. In the meantime, IAS-2000 will also continue blocking the user from accessing the network. If the user is an authorized user, then IAS-2000 will authorize the user with an appropriate access right, so that the user can use the network. If the online user remains idle without using the network for a time exceeding a predetermined idle time on IAS-2000 or the online user logs out of the system, IAS-2000 will exit the working stage of such user and terminate the user's access right of the network.

The following figure provides a simple example of setting up a small enterprise network. IAS-2000 is set to control a part of the company's intranet. The whole managed network includes cable network users and wireless network users. In the beginning, any user located at the managed network is unable to access the network resource without permission. If the access right to the network beyond the managed area is required, an Internet browser such as the Internet Explorer must be opened and a connection to any website must be performed. When the browser attempts to connect to a website, IAS-2000 will force the browser to redirect to the user login webpage. The user must enter the username and password for authentication. After the identity is authenticated successfully, the user will gain proper access right defined on IAS-2000.

**Attention: Public LAN** is referred to as the LAN port with the authentication function enabled from where the Authentication is required for the users to get access of the network; And, **Private LAN** is referred to as the LAN port with the authentication function disabled.



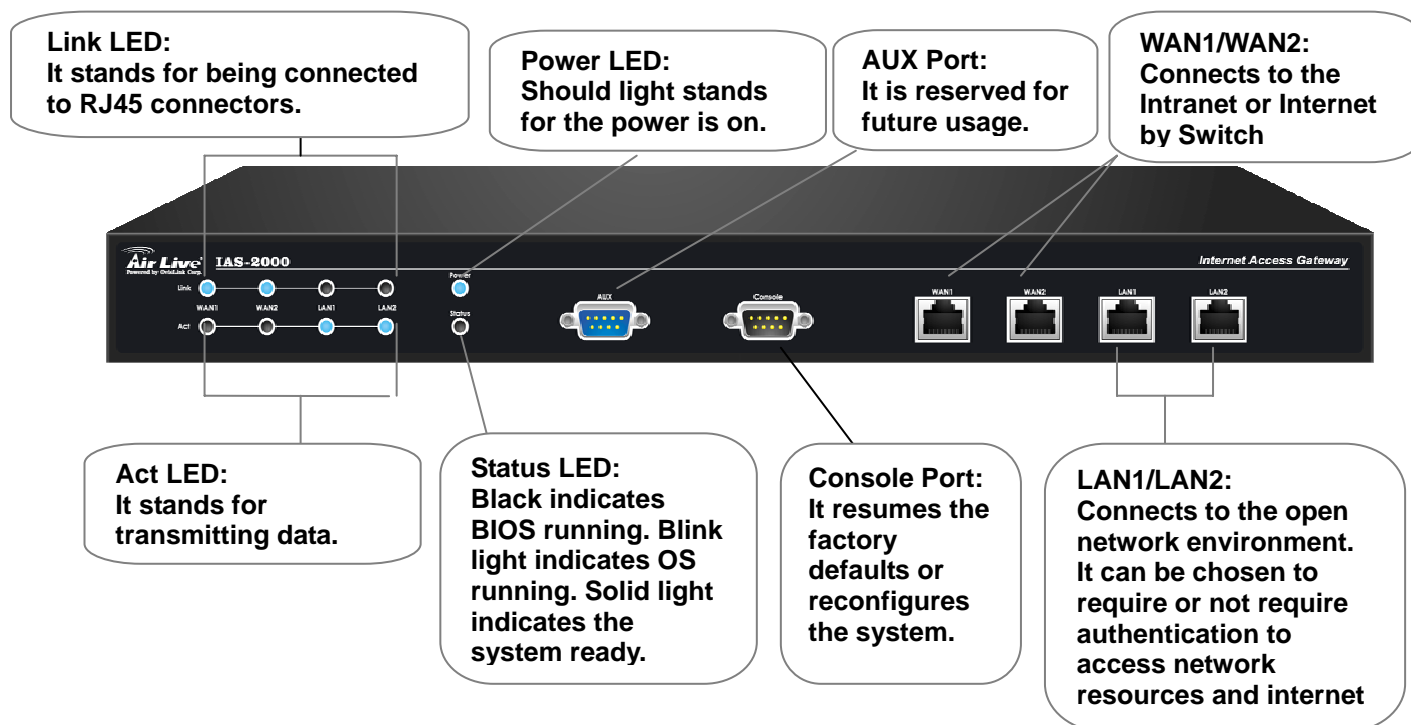
Another setup example is shown in the following figure. The WAN1 and WAN2 of IAS-2000 simultaneously supports the Switch of 802.3ad (Support Port Trunk), and the bandwidth of the Switch will be the sum of the WAN1 and WAN2 bandwidths, which aims at eliminating the bottleneck caused by the narrow bandwidth between IAS-2000 and the 802.3ad Switch.



## Chapter 3. Hardware Installation

### 3.1 Panel Function Descriptions

#### Front Panel



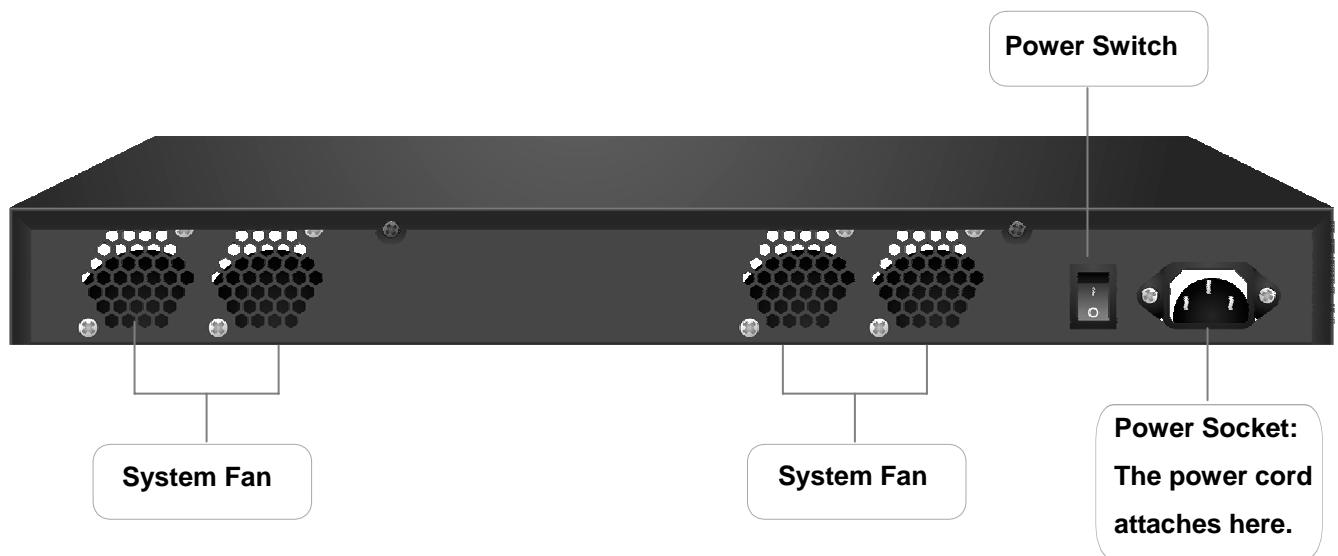
**LCD:** There are four kinds of LCD, power, status, port speed and link/act LCD, to indicate different status of the system.

**AUX Port:** It is reserved for future usage.

**Console Port:** The system can be configured via HyperTerminal. For example, if you need to set the Administrator's Password, you can connect a PC to this port as a Console Serial Port via a terminal connection program (such as the super terminal with the parameters of 9600, 8, N, 1, None flow control) to change the Administrator's Password.

**LAN1/LAN2:** The two LAN ports can be independently configured such that users cannot access Internet before authentication. Thus, administrators can choose to force the authentication for users connected to these ports.

**WAN1/WAN2:** The two WAN ports are connected to a network which is not managed by the IAS-2000 system, and this port can be used to connect the ATU-Router of ADSL, the port of Cable Modem, or the Switch or Hub on the LAN of a company.

**Rear Panel**

**System Fan:** Keeps the machine cool.

**Power Socket:** The power cord attaches here.

**Power Switch:** Turns on and off the machine.

## 3.2 Package Contents

The standard package of IAS-2000 includes:

- IAS-2000 x 1
- CD-ROM x 1
- Quick Installation Guide x 1
- Power Cord x 1
- Ethernet Cable (Crossover) x 1
- Ethernet Cable (Straight) x3
- Console Cable x 1
- Accessory Packing x 1

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

### 3.3 System Requirement

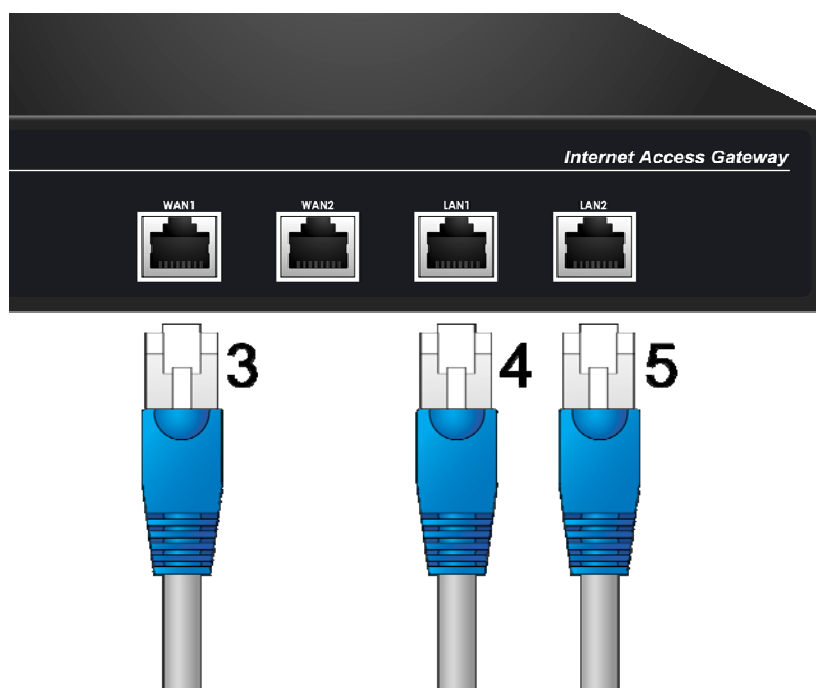
- Standard 10/100BaseT including five network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

### 3.4 Installation Steps

Please follow the following steps to install IAS-2000:



1. Connect the power cord to the power socket on the rear panel.
2. Turn on the power switch on the rear panel. The Power LED will light up.



3. Connect an Ethernet cable to one LAN Port with the user authentication function enabled on the front panel. The default ports are LAN1 and LAN2 ports. (Note: Authentication is required for the users to access the network via these LAN Ports. The LAN port with authentication function is referred to as **Public LAN**.) Connect the other end of the Ethernet cable to an AP or switch. The LED of this LAN should be on to indicate a proper connection.
4. Connect an Ethernet cable to one LAN Port with the user authentication function disabled on the front panel. The default ports are LAN3 and LAN4 ports. (Note: No authentication is required for the users to access the network via these LAN Ports. The LAN port without authentication function is referred to as **Private LAN** and the administrator can enter the administrative user interface to perform configurations via Private LAN.) Connect the other end of the Ethernet cable to a client's PC. The LED of this LAN should be on to indicate a proper connection.
5. Connect an Ethernet cable to the WAN Port on the front panel. Connect the other end of the Ethernet cable to ADSL modem, cable modem or a switch/hub of the internal network. The LED of this WAN should be on to indicate a proper connection.

**Attention:** Usually a straight RJ-45 could be applied if IAS-2000 is connected to a hub/computer which supports automatic crossover, such as the Access Point. However, after the Access Point hardware reset, IAS-2000 should not be able to connect to Access Point while connecting with a straight cable unless the cable was pulled out and plug-in again. This scenario does NOT occur while using a crossover cable.

After the hardware of IAS-2000 is installed completely, the system is ready to be configured in the following sections. The manual will guide you step by step to set up the system using a single IAS-2000 to manage the network.



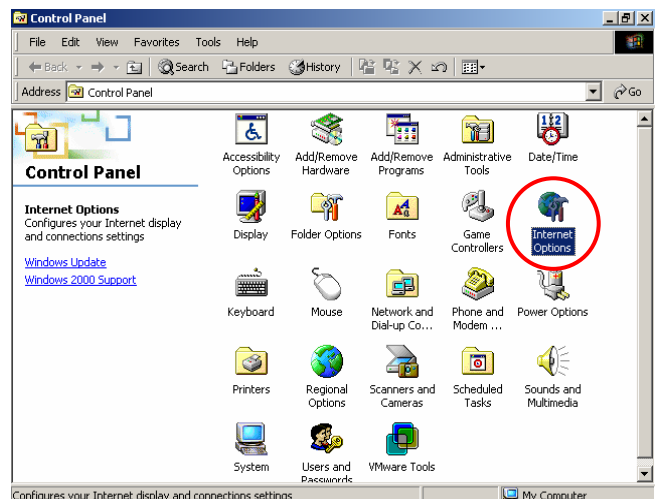
## Chapter 4. Network Configuration on PC

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

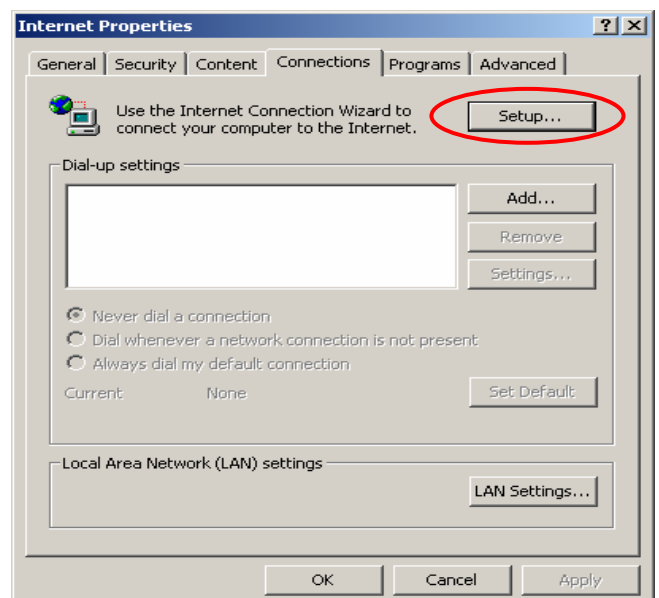
### 4.1 Internet Connection Setup

#### 4.1.1 Windows 9x/2000

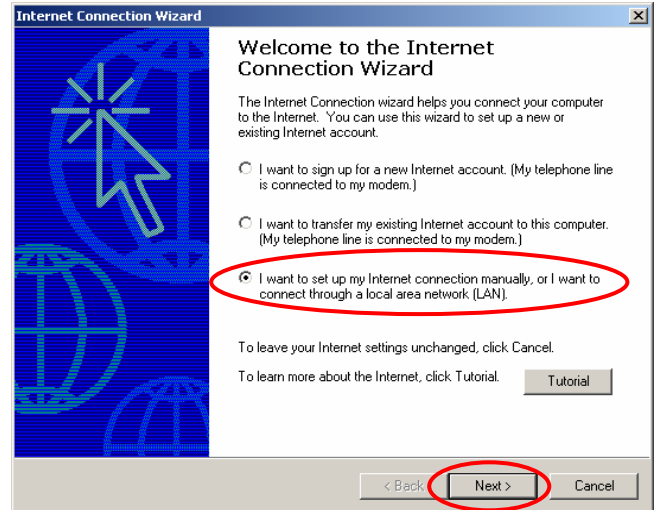
1. Choose **Start > Control Panel > Internet Options**.



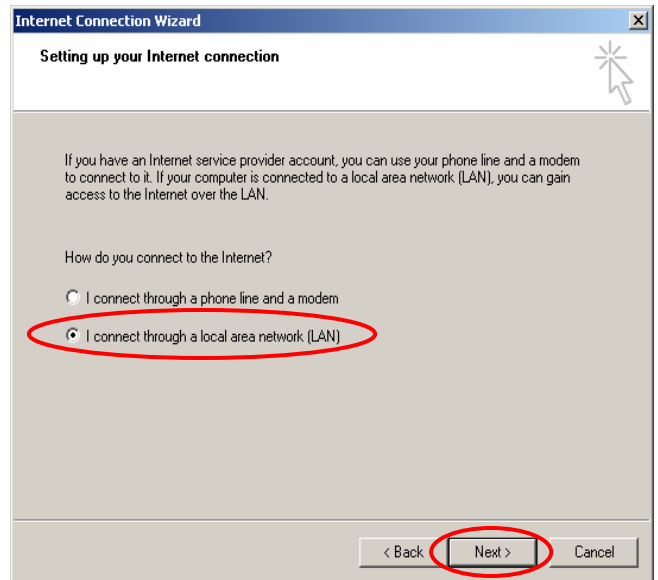
2. Choose the “**Connections**” label, and then click **Setup**.



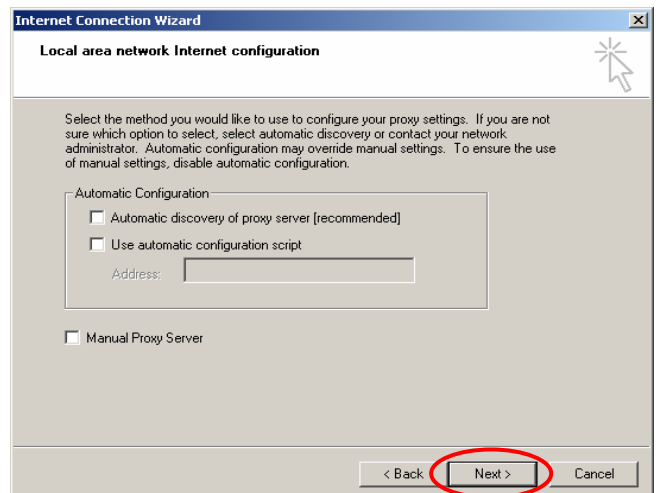
3. Choose “I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)”, and then click **Next**.



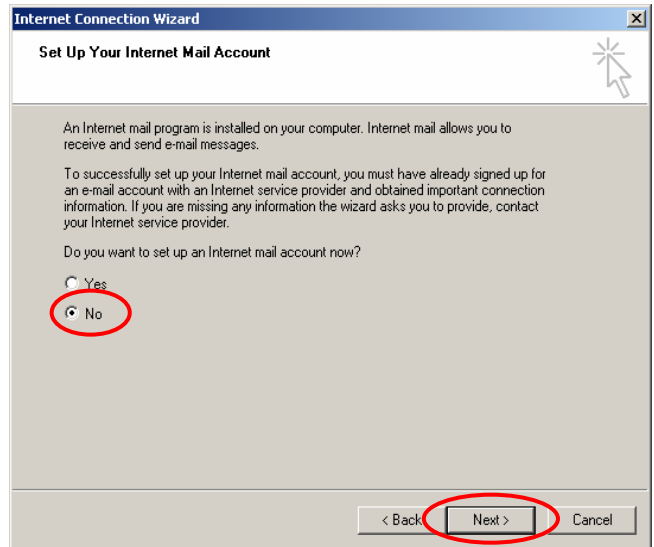
4. Choose “I connect through a local area network (LAN)” and click **Next**.



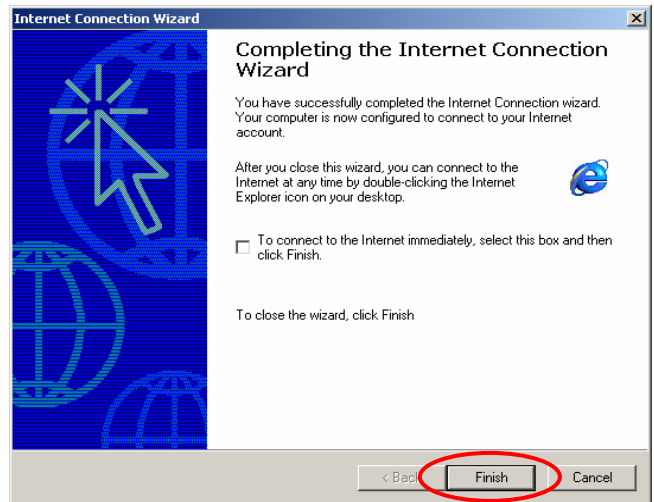
5. Do **NOT** check any option in the following LAN window for Internet configuration, and just click **Next**.



6. Choose **“No”**, and click **Next**.

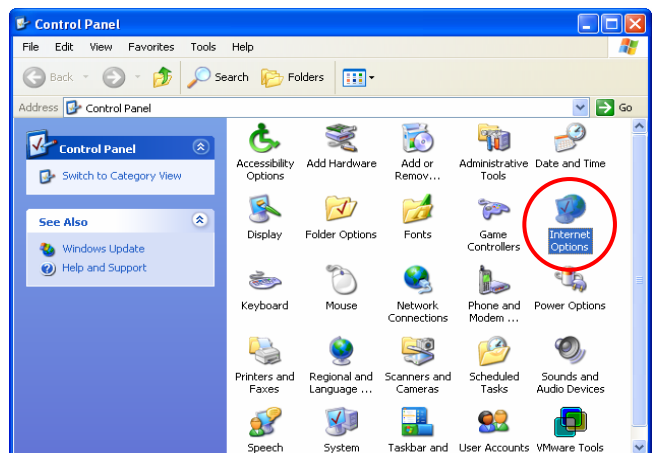


7. Finally, click **Finish** to exit the **Internet Connection Wizard**. Now, the setup has been completed.

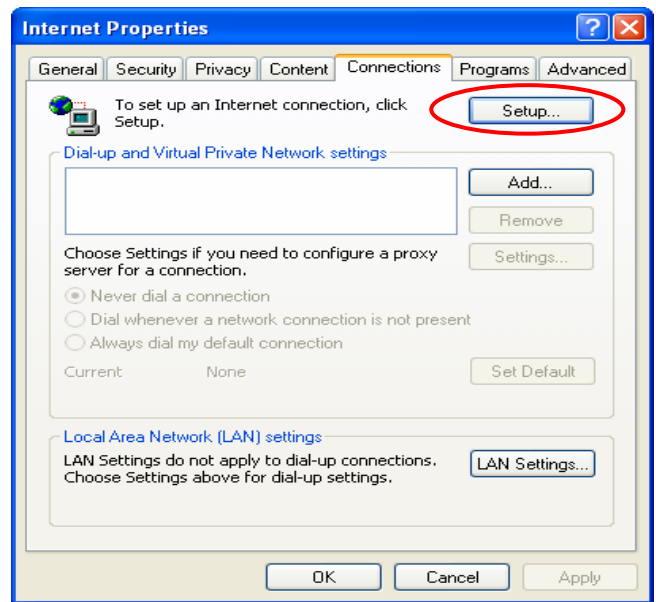


## 4.1.2.Windows XP

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



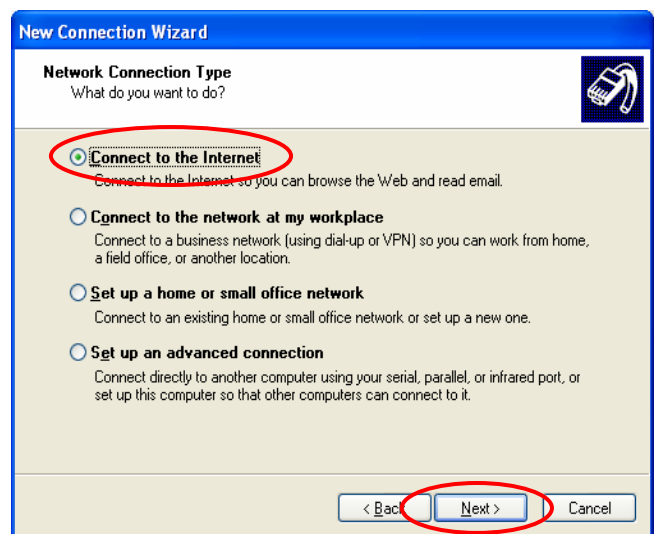
- Choose the “**Connections**” label, and then click **Setup**.



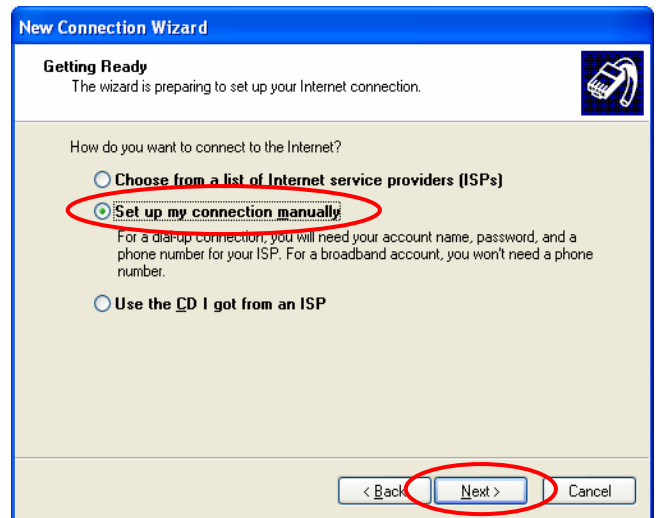
- Click **Next** when **Welcome to the New Connection Wizard** screen appears.



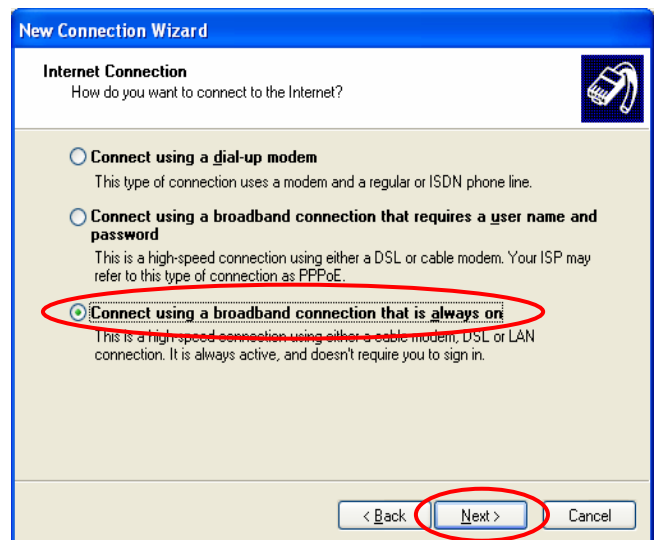
- Choose “**Connect to the Internet**” and then click **Next**.



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



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



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



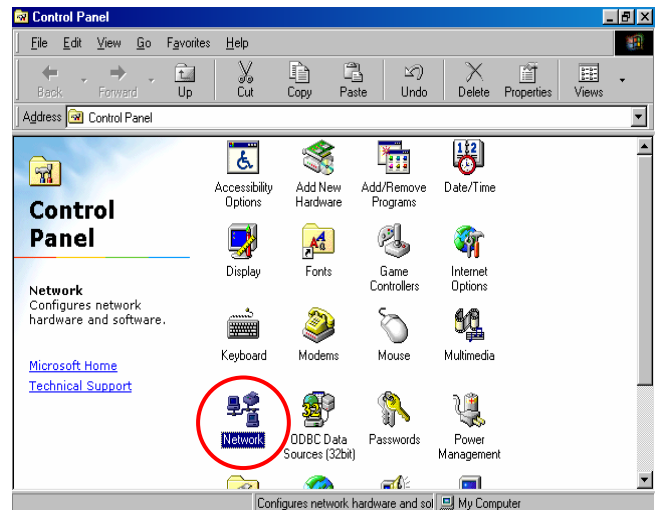
## 4.2 TCP/IP Network Setup

If the operating system of your PC is Windows 95/98/ME/2000/XP, then just keep the default settings without any change to directly start/restart the system. With the factory default settings, during the process of starting the system, IAS-2000 with DHCP function will automatically assign an appropriate IP address and related information for each PC. If the Windows operating system is not a server version, the default settings of the TCP/IP will regard the PC as a DHCP client, and this function is called “**Obtain an IP address automatically**”.

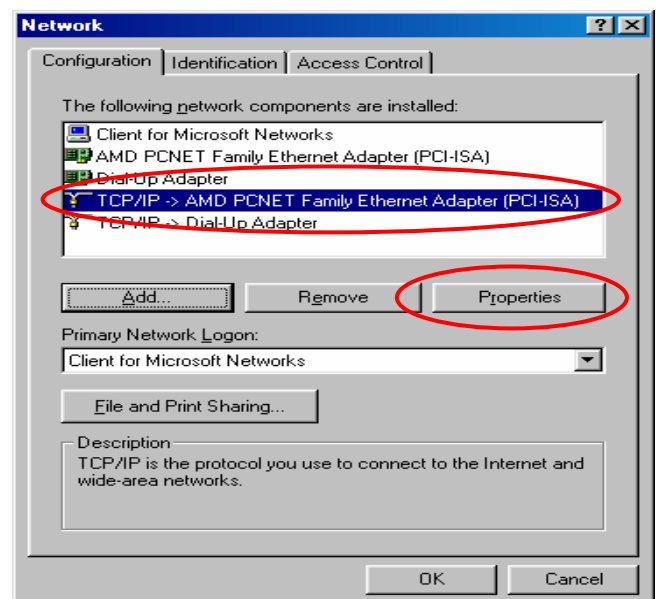
If you want to check the TCP/IP setup or use the static IP in the LAN1/LAN2 or LAN3/LAN4 section, please follow the steps below

### 4.2.1. Check the TCP/IP Setup of Window 9x/ME

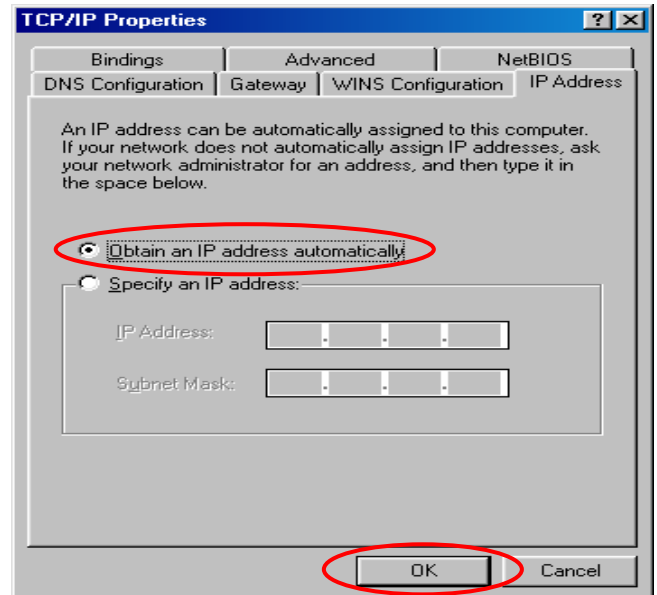
1. Choose **Start > Control Panel > Network**.



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.



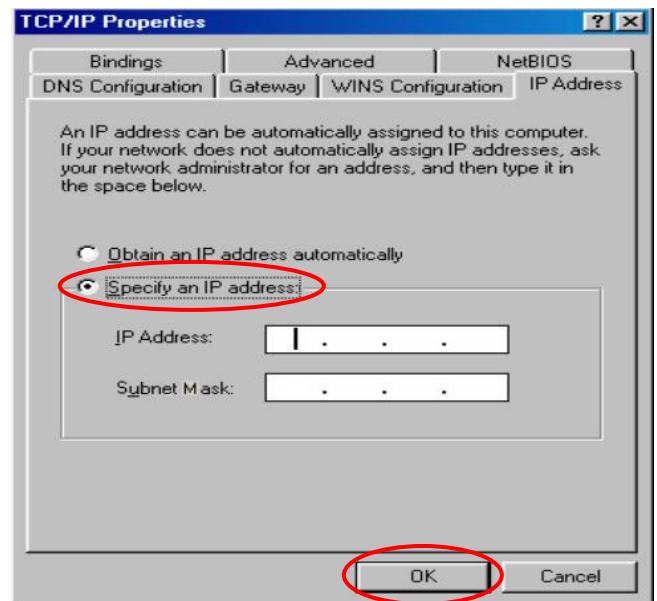
3-1. **Using DHCP:** If you want to use DHCP, please choose “**Obtain an IP address automatically**” under the “**IP Address**” label and click **OK**. This is also the default setting. Then, reboot the PC to make sure an IP address is obtained from IAS-2000.



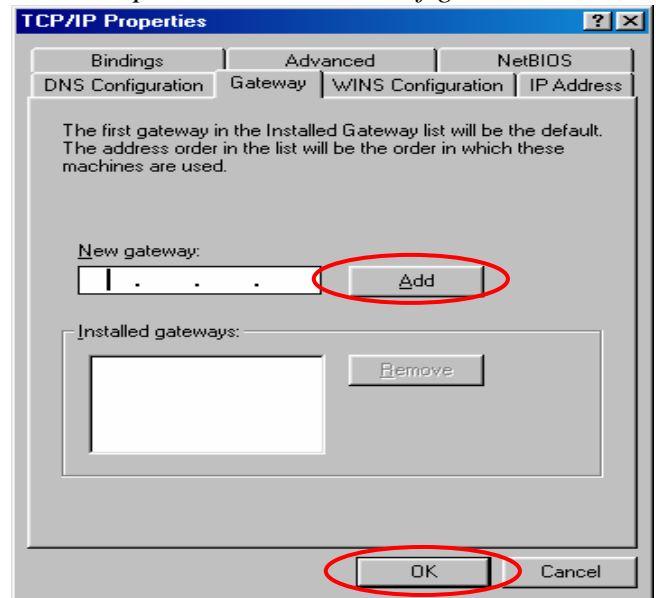
3-2. **Using Specific IP Address:** If you want to use specific IP address, you have to ask the network administrator for the information of IAS-2000: **IP address**, **Subnet Mask**, **Gateway** and **DNS server address**.

**Caution:** If your PC has been set up completed, please inform the network administrator before modifying the following setup.

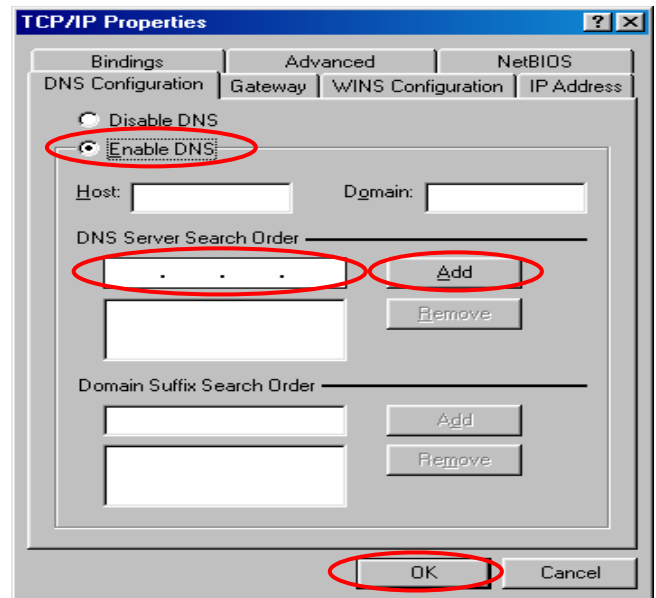
- Please choose “**Specify an IP address:**” and enter the information given to you from the network administrator in “**IP Address:**” and “**Subnet Mask:**” under the “**IP Address**” label and then click **OK**.



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



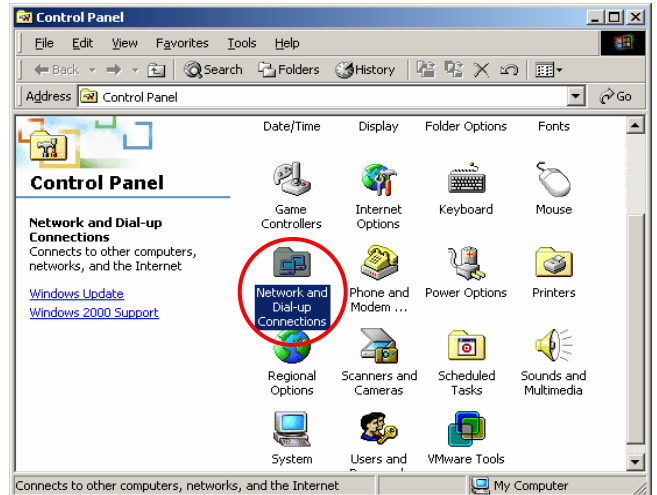
- Choose “**DNS Configuration**” label. If no DNS Server is defined in the DNS Server column, please click **Enable DNS** and then enter a known DNS address or the DNS address provided by ISP. Then, click **Add** and click **OK**.



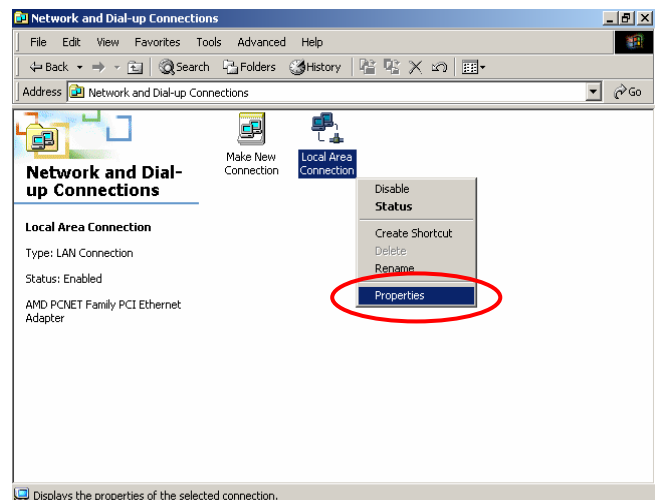


### 4.2.2. Check the TCP/IP Setup of Window 2000

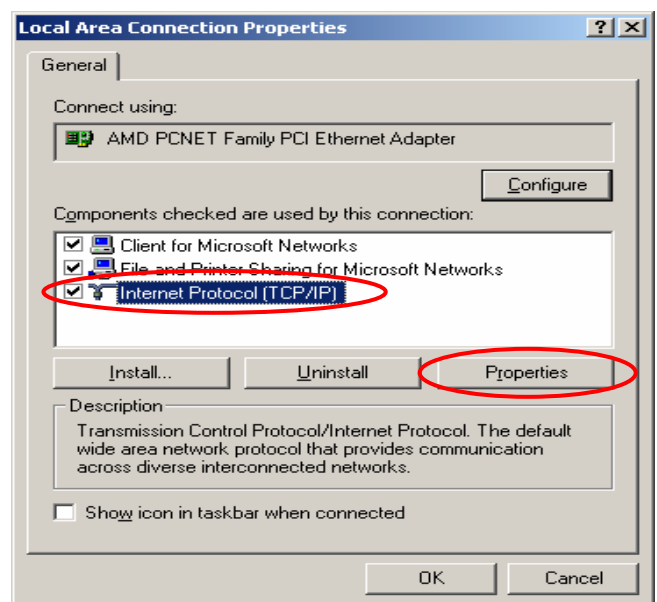
1. Select **Start > Control Panel > Network and Dial-up Connections**.



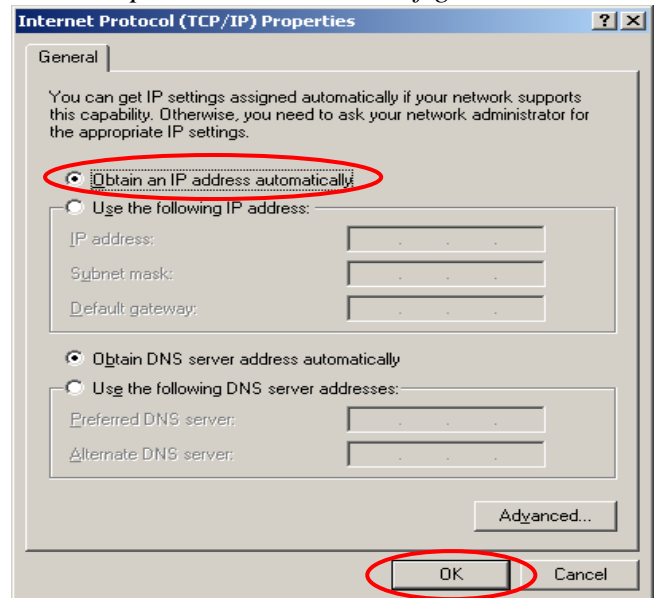
2. Click the right button of the mouse on “**Local Area Connection**” icon and then select “**Properties**”.



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



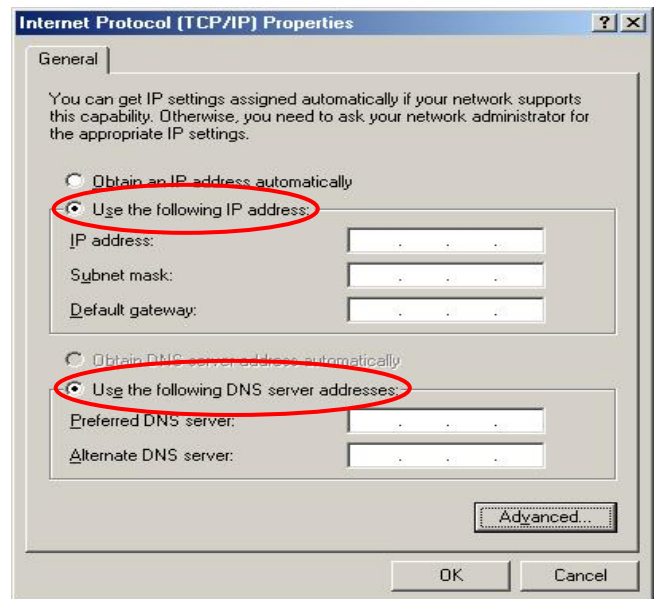
4-1. **Using DHCP:** If you want to use DHCP, please choose **“Obtain an IP address automatically”** and click **OK**. This is also the default setting. Then, reboot the PC to make sure an IP address is obtained from IAS-2000.



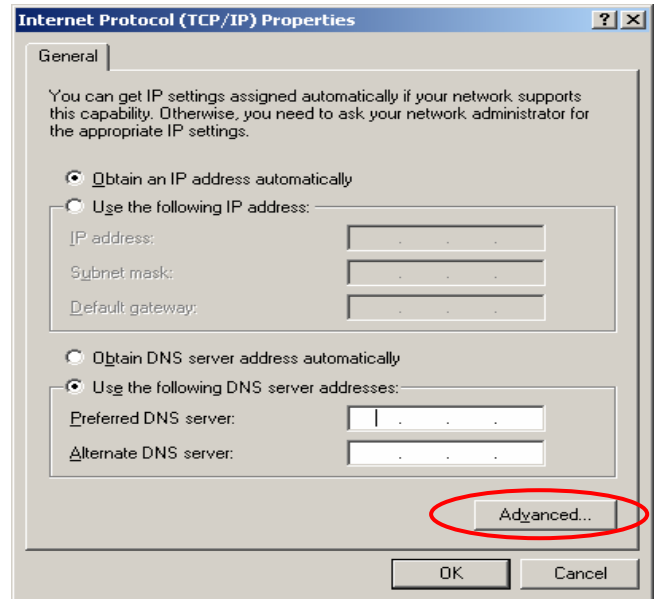
4-2. **Using Specific IP Address:** If you want to use specific IP address, you have to ask the network administrator for the information of IAS-2000: **IP address**, **Subnet Mask**, **Gateway** and **DNS server address**.

**Caution:** If your PC has been set up completed, please inform the network administrator before modifying the following setup.

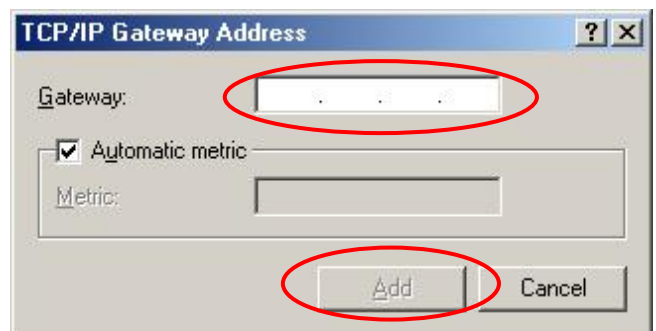
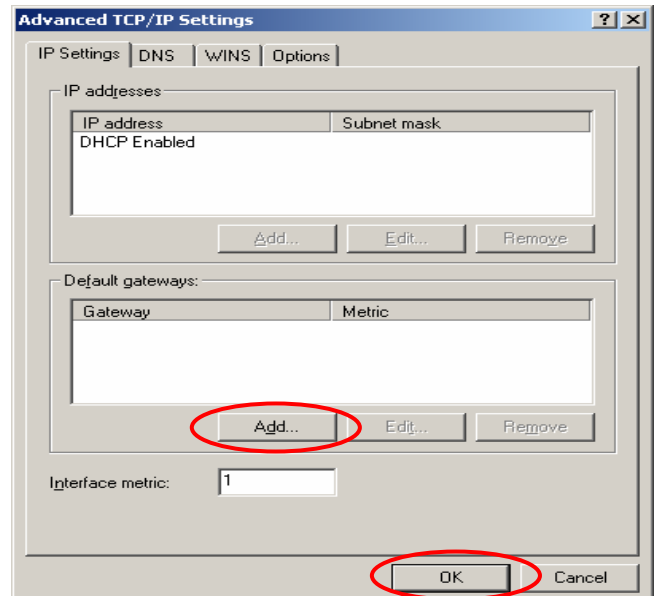
- Please choose **“Use the following IP address:”** and enter the information given from the network administrator in **“IP address:”** and **“Subnet mask:”** as well as **“Default gateway:”** If the DNS Server column is blank, please choose **“Use the following DNS server addresses:”** and then enter a known DNS address or the DNS address provided by ISP and then click **OK**.



- Then, click **Advanced** in the window of **“Internet Protocol (TCP/IP) Properties”**.

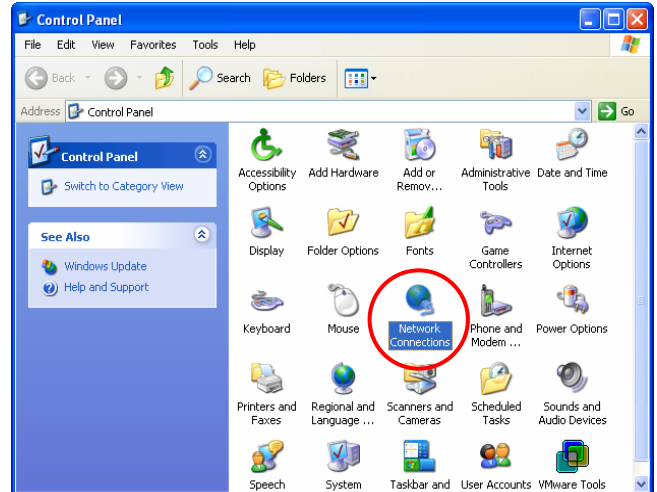


- Choose the **“IP Settings”** label and click **Add** below the **“Default gateways”** column and the **“TCP/IP Gateway Address”** window will appear. Enter the gateway address of IAS-2000 in the **“Gateway:”** of **“TCP/IP Gateway Address”** window, and then click **Add**. After returning to the **“IP Settings”** section, click **OK** to finish.

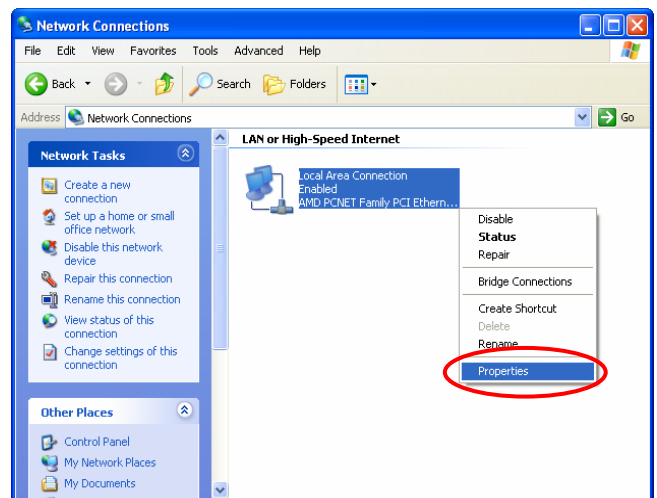


### 4.2.3. Check the TCP/IP Setup of Window XP

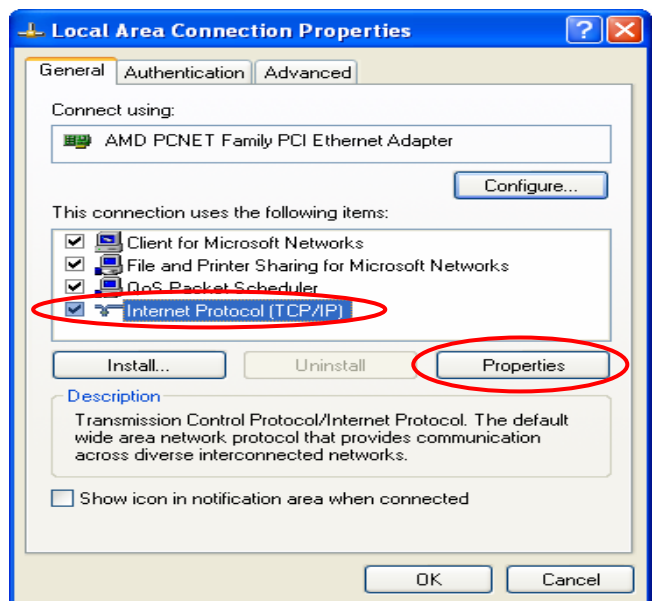
1. Select **Start > Control Panel > Network Connections**.



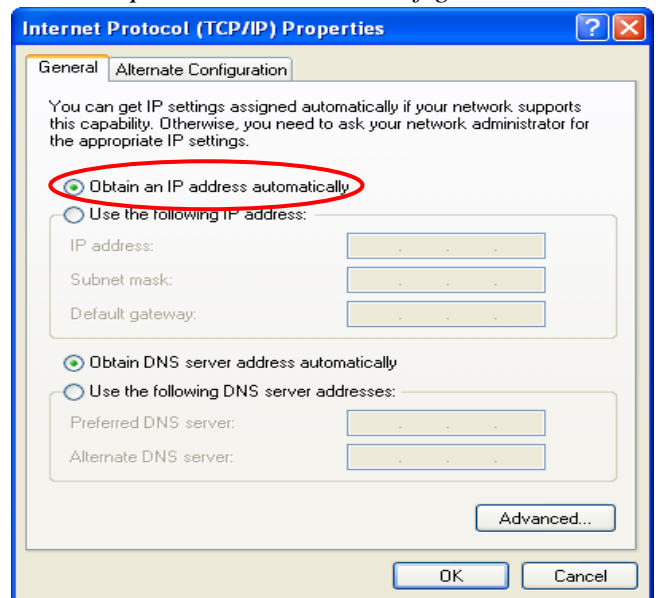
2. Click the right button of the mouse on the **“Local Area Connection”** icon and select **“Properties”**



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**.



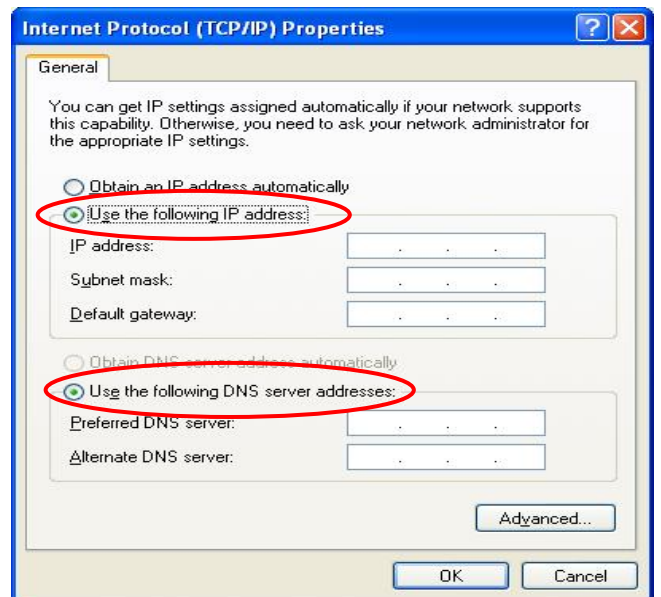
4-1. **Using DHCP:** If you want to use DHCP, please choose “**Obtain an IP address automatically**” and click **OK**. This is also the default setting. Then, reboot the PC to make sure an IP address is obtained from IAS-2000.



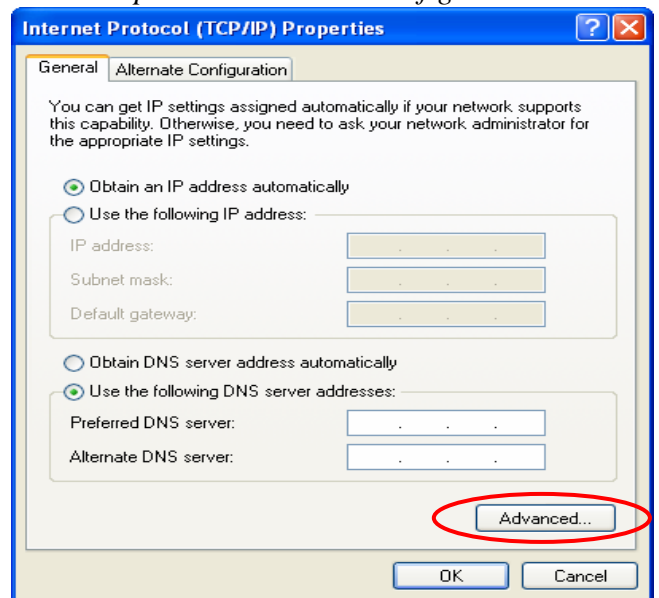
4-2. **Using Specific IP Address:** If you want to use specific IP address, you have to ask the network administrator for the information of IAS-2000: **IP address**, **Subnet Mask**, **Gateway** and **DNS server address**.

**Caution:** If your PC has been set up completed, please inform the network administrator before modifying the following setup.

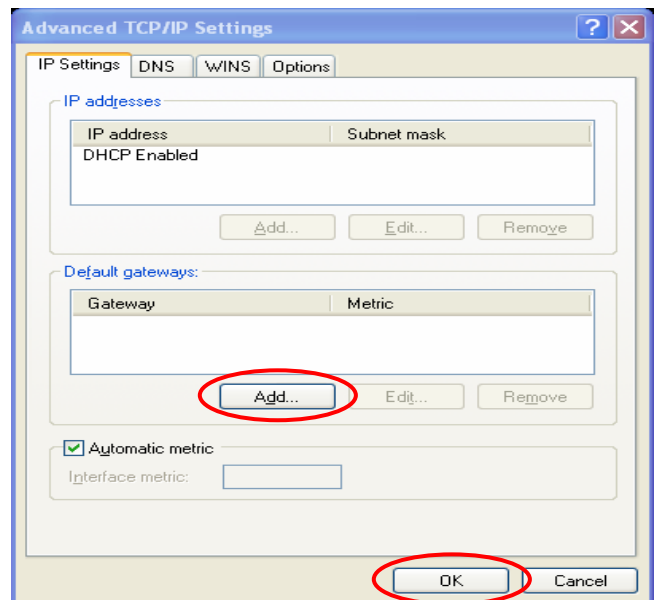
- Please choose “**Use the following IP address:**” and enter the information given from the network administrator in “**IP address:**” and “**Subnet mask:**” as well as “**Default gateway**” If the DNS Server column is blank, please choose “**Use the following DNS server addresses:**” and then enter a known DNS address or the DNS address provided by ISP and then click **OK**.



- Then, click **Advanced** in the window of **“Internet Protocol (TCP/IP) Properties”**.

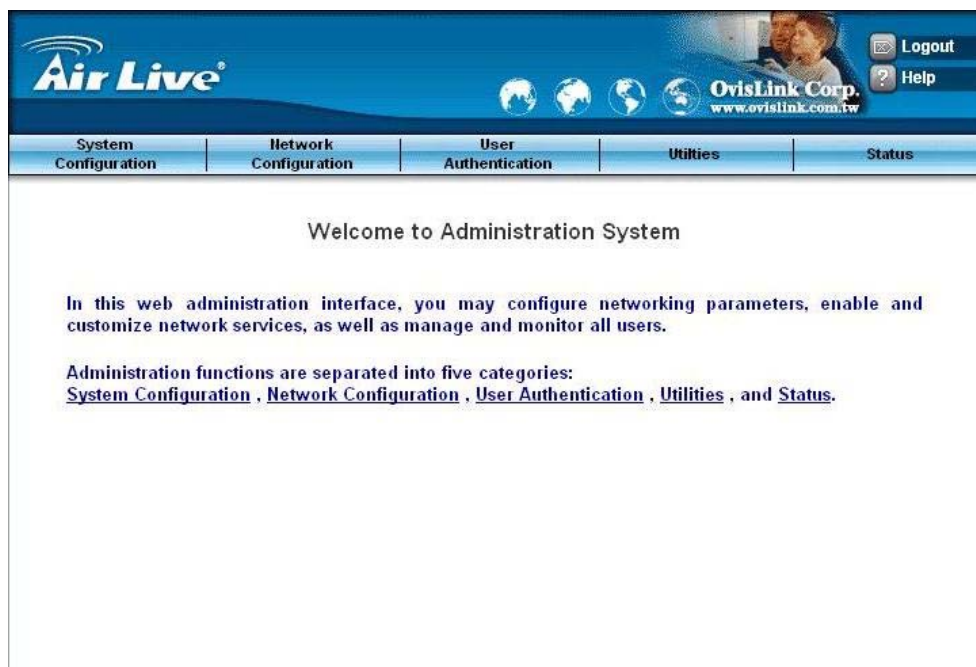


- Choose the **“IP Settings”** label and click **“Add”** below the **“Default gateways”** column and the **“TCP/IP Gateway Address”** window will appear. Enter the gateway address of IAS-2000 in the **“Gateway:”** of **“TCP/IP Gateway Address”** window, and then click **Add**. After returning to the **“IP Settings”** label, click **OK** to finish.



## Chapter 5. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table shows all the functions of IAS-2000.

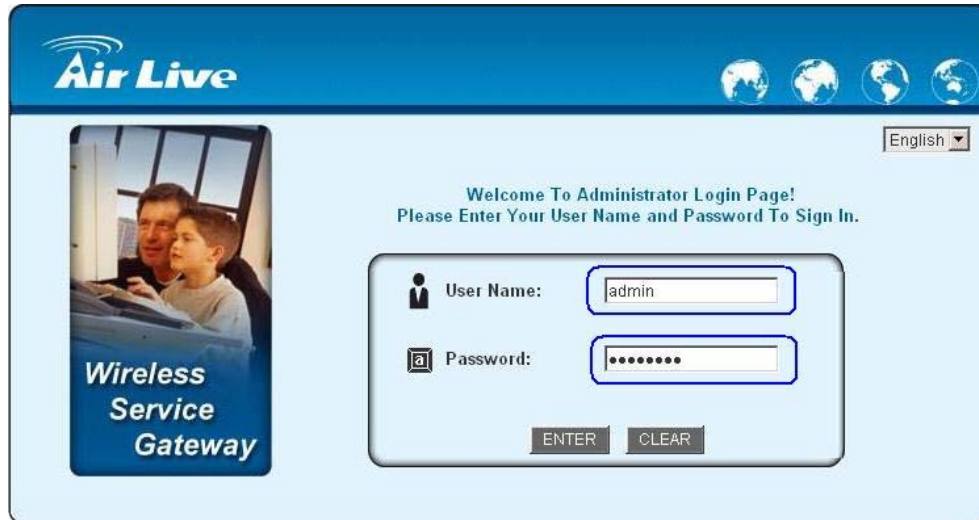


OPTION	System Configuration	Network Configuration	User Authentication	Utilities	Status
FUNCTION	Configuration Wizard	Network Address Translation	Authentication Configuration	Change Password	System Status
	System Information	Privilege List	Policy Configuration	Backup Restore Strategy	Interface Status
	WAN1 Configuration	Monitor IP List	Black List Configuration	Firmware Upgrade	Current Users
	WAN2 Configuration	Walled Garden List	Guest User Configuration	Restart	Traffic History
	LAN1 Configuration	Proxy Server Properties	Additional Configuration		Notification Configuration
	LAN2 Configuration	Dynamic DNS			Online Report
		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.

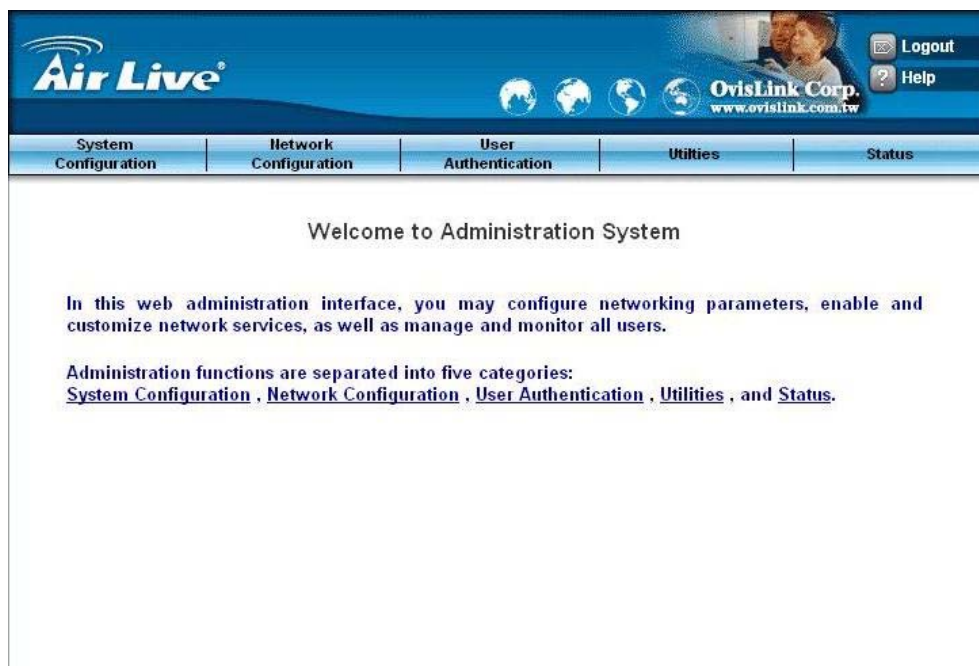
After the previous installation is completed, IAS-2000 can be further configured with the following steps

1. Use the network cable of the 10/100BaseT to connect a PC to the authenticated port, and then start a browser (such as Microsoft IE). Next, enter the gateway address for that port, the default is <https://192.168.2.254>. In the opened webpage, you will see the login screen. Enter the default username, “**admin**”, and the default password, “**sohoware**”, in the User Name and Password column. Click **Enter** to log in.



**Caution:** If you can't get the login screen, you may have incorrectly set your PC to obtain an IP address automatically from authentication LAN port or the IP address used does not have the same subnet as the URL. Please use default IP address such as 192.168.2.xx in your network and then try it again.

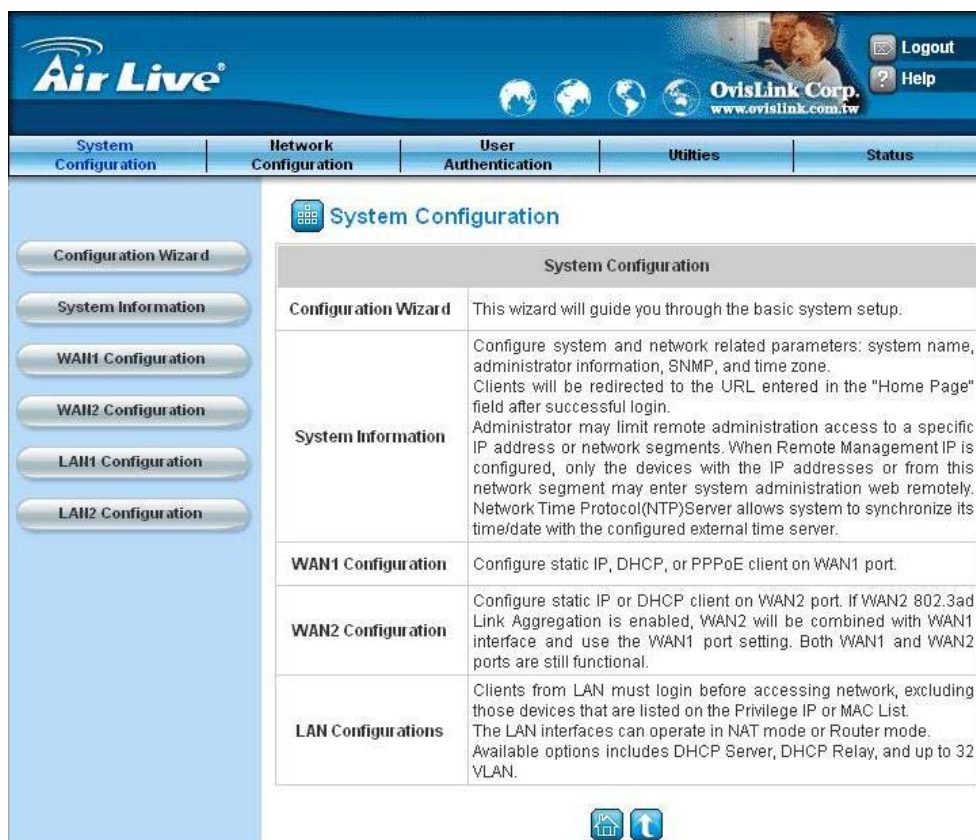
2. After successfully logging into IAS-2000, you can enter the web management interface and see the welcome screen. There is a **Logout** button on the upper right corner to log out the system when finished.





## 5.1 System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN1 Configuration**, **WAN2 Configuration**, **LAN1 Configuration** and **LAN2 Configuration**.

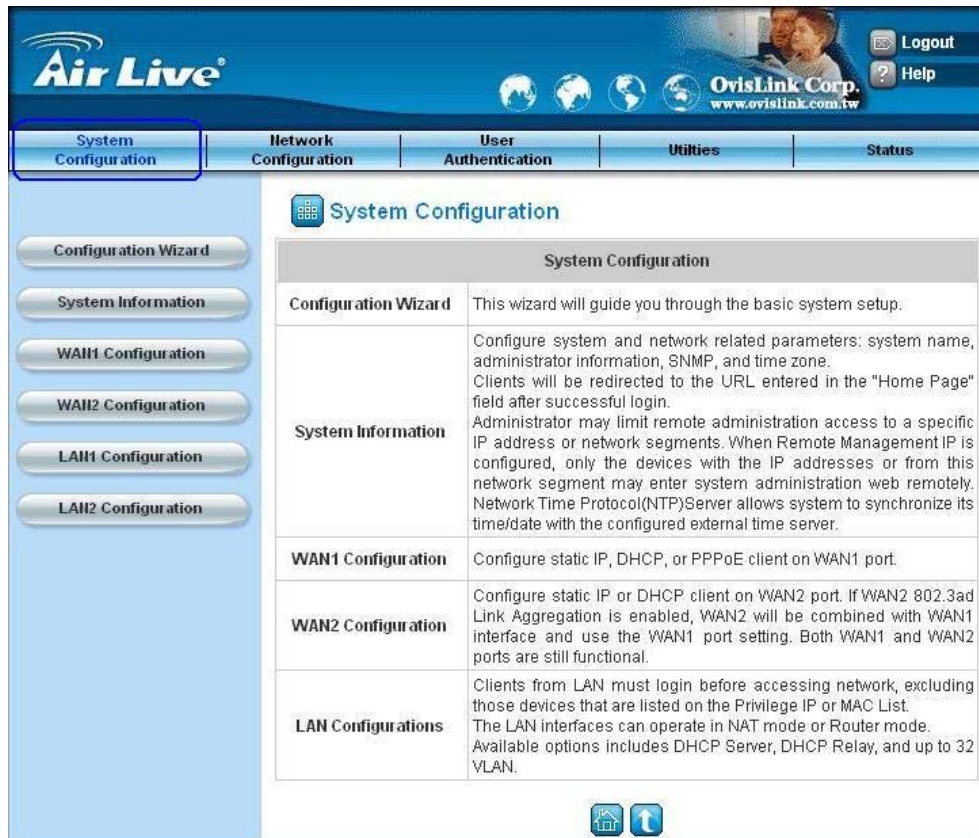


### 5.1.1 Configuration Wizard

There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard has 7 steps providing a simple and easy way to guide you through the setup of IAS-2000. 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 IAS-2000, it is ready to use. There will be 7 steps as listed below:

1. Change Admin's Password
2. Choose System's Time Zone
3. Set System Information
4. Select the Connection Type for WAN1 Port
5. Configure LAN1
6. Select Authentication Method
7. Restart

Now, click **System Configuration** to go to the **System Configuration** page.

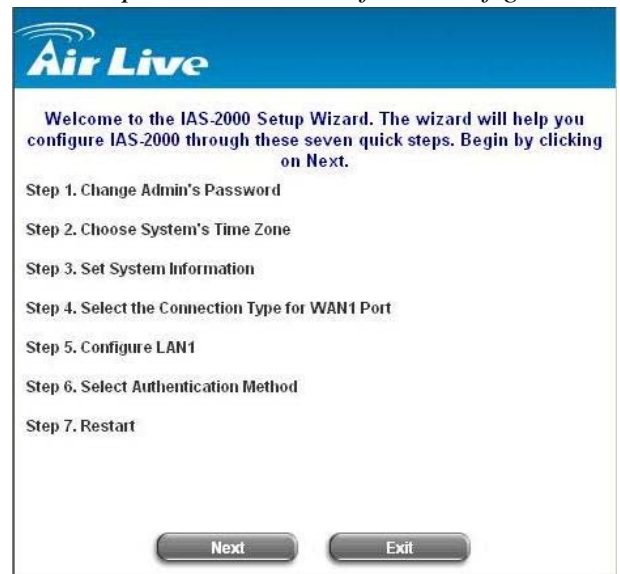


Click the **System Configuration** from the top menu and the **System Configuration** page will appear. Then, click on **Configuration Wizard** and click the **Run Wizard** button to start the wizard.



- **Running the Wizard**

First of all, you will see a welcome screen to briefly introduce the 7 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).

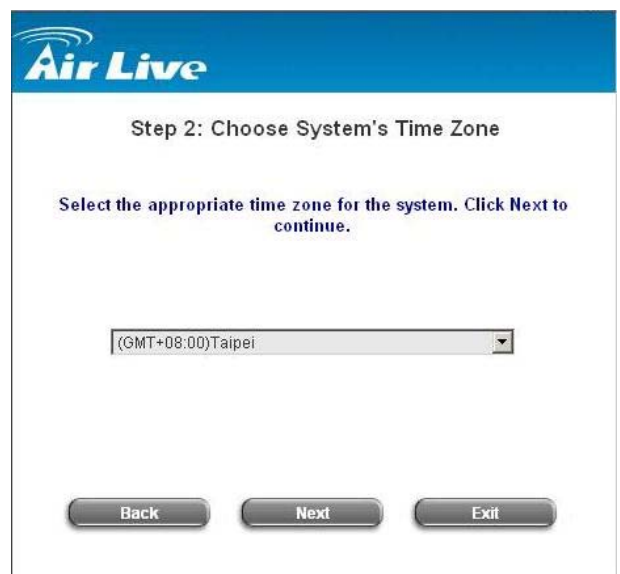
Click **Next** to continue.



- **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 URL of external time server for IAS-2000 time synchronization or use the default.

**DNS Server:** Enter a DNS Server provided by your ISP (Internet Service Provider). Contact your ISP if you are not sure of the DNS IP Address.

Click **Next** to continue.

- **Step 4: Select the Connection Type for WAN1 Port**

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

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

- **Dynamic IP Address**

If this option is selected, an appropriate IP address and related information will automatically be assigned.

Click **Next** to continue.

- **Static IP Address: Set WAN1 Port's Static IP Address**

Enter the “**IP Address**”, “**Subnet Mask**” and “**Default Gateway**” provided by your ISP.

Click **Next** to continue.

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

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

Click **Next** to continue.

• **Step 5: Configure LAN1's Information**

**IP Address:** Enter the Public LAN port IP Address or use the default.

**Subnet Mask:** Enter the Public port Subnet Mask or use the default.

**Disable DHCP Server:** If the DHCP server is disabled, the Public LAN clients must be configured with an IP address manually.

**Enable DHCP Server:** When the option is selected, IAS-2000 will automatically provide the necessary IP address to all Public LAN clients.

Click **Next** to continue.

• **Step 5: Set LAN1 DHCP Server**

If the Enable DHCP Server option is selected, fields marked with red asterisk must be filled in.

**DHCP Scope:** These fields define the IP address range that will be assigned to the Public LAN clients. **(Note: Be sure that IP address assigned in this range is NOT used in other settings by IAS-2000.)**

**Domain Name:** Enter a domain name provided by your ISP (e.g. yahoo.com.tw).

**WINS Server:** Enter the IP address of the WINS Server (Windows Internet Naming Service Server). This field is optional.

**Preferred DNS Server:** The DNS Server settings are provided by your ISP. Only the Preferred DNS Server field is mandatory. Contact your ISP if you are unsure of the DNS Server settings.

**Alternate DNS Server:** The DNS Server settings are provided by your ISP. This field is optional.

Click **Next** to continue.

- **Step 6: Select Default Authentication Server**

Set the user's information in advance. Enter an easily identified name as the postfix name in the **Postfix Name** field (e.g. Local), select a policy to assign to (you can use the default), and choose an authentication method.

Click **Next** to continue.

- **Local User- Add User**

A new user can be added to the local user data base. To want to add a user here, enter the **Username** (e.g. test), **Password** (e.g. test), **MAC** (optional) and assign it a policy (or use the default). Upon completing a user adding, more users can be added to this authentication method by clicking the **ADD** bottom.

Click **Next** to continue.

➤ **POP3 User- Authentication Method-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.

➤ **RADIUS User- Authentication-RADIUS**

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

Click **Next** to continue.

➤ **LDAP User- Authentication Method-LDAP**

You can add a new user to the LDAP user data base. Enter the “**LDAP Server**”, “**Server Port**” and “**Base DN**”. And then, you have to select one kind of **Binding Type** and **Account Attribute** to access the LDAP server.

If you select **User Account** binding type, the system will use the **Base DN** to be the user account to access the LDAP server.

If you select **Anonymous** binding type, the system will access the LDAP servers without requiring authentication.

The screenshot shows the 'Step 6: Authentication Method-LDAP' configuration screen. The 'Binding Type' dropdown is set to 'Anonymous'. The 'Account Attribute' section has radio buttons for 'UID' (selected), 'CN', and 'sAMAccountName'. The 'LDAP Server', 'Server Port', and 'Base DN' fields are empty. The 'Next' button is highlighted.

If you select **Specific DN** binding type, you have to enter the **username** and **password** in the “**Bind RDN**” and “**Bind Password**” fields to access the LDAP server.

The screenshot shows the 'Step 6: Authentication Method-LDAP' configuration screen. The 'Binding Type' dropdown is set to 'Specified DN'. The 'Bind RDN' and 'Bind Password' fields are present and empty. The 'Account Attribute' section has radio buttons for 'UID' (selected), 'CN', and 'sAMAccountName'. The 'LDAP Server', 'Server Port', and 'Base DN' fields are empty. The 'Next' button is highlighted.

If you select **Windows AD** binding type, please enter the domain name of Windows AD to access the LDAP server.  
Click **Next** to continue.

The screenshot shows the 'Step 6: Authentication Method-LDAP' configuration screen. The 'Binding Type' dropdown is set to 'Windows AD'. A 'Domain' text field is present and empty. The 'Account Attribute' section has radio buttons for 'UID' (selected), 'CN', and 'sAMAccountName'. The 'LDAP Server', 'Server Port', and 'Base DN' fields are empty. The 'Next' button is highlighted.



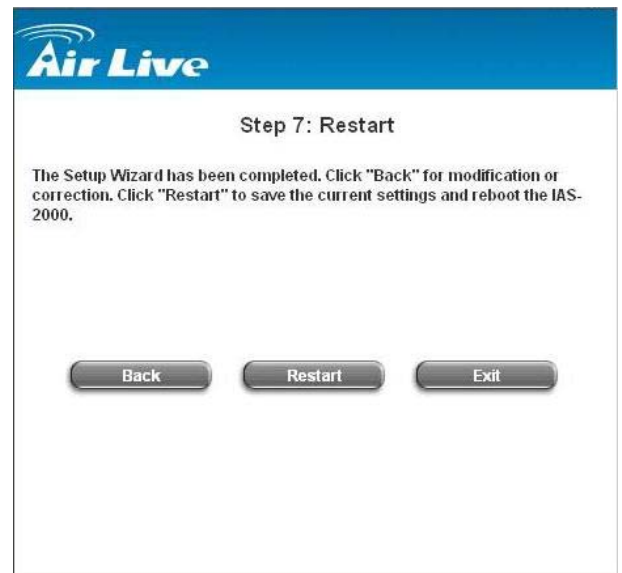
➤ **LDAP User- Authentication Method-NT Domain**

When NT Domain User is selected, enter the information for “**Server IP Address**”, and enable/disable “**Transparent Login**”. After this setup is completed, click **Next** to continue.

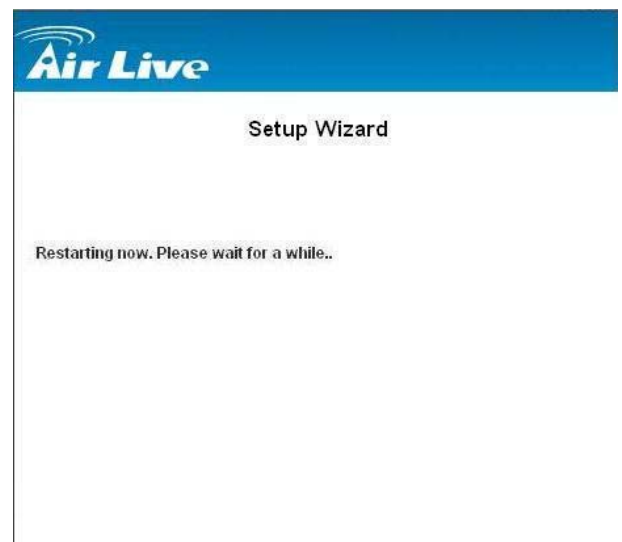


• **Step 7: Restart**

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



- During IAS-2000 restart, a “**Restarting now. Wait for a minute.**” message will appear on the screen. Please do not interrupt IAS-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.

### 5.1.2 System Information

These are some main information about IAS-2000. Please refer to the following description for these blanks:

System Information	
<b>System Name</b>	<input type="text" value="OvisLink IAS-2000"/>
<b>WAN Failure Message</b>	<input type="text" value="Sorry! The service is unavailable."/> *(It'll appear on the login page when WAN fails.)
<b>Device Name</b>	<input type="text"/> (FQDN for this device)
<b>Home Page</b>	<input type="text" value="http://www.ovislink.com"/> *(e.g. http://www.ovislink.com/)
<b>Remote Management IP</b>	<input type="text" value="0.0.0.0/0.0.0.0"/> *(e.g. 192.168.3.1 or 192.168.3.0/24)
<b>SNMP</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Manager IP: <input type="text" value="10.2.3.203"/> * Community: <input type="text" value="read"/> * SNMP v3 Account: <input type="text"/> SNMP v3 Password: <input type="text"/>
<b>System Time</b>	Device Time: 2005/12/01 15:08:04 <input checked="" type="radio"/> Enable NTP NTP Server: <input type="text" value="tock.usno.navy.mil"/> *(e.g. tock.usno.navy.mil) Time Zone: <input type="text" value="(GMT+08:00)Taipei"/> ▼ <input type="radio"/> Set Device Date and Time (UTC)
<b>History Report Interval</b>	<input checked="" type="radio"/> 5 <input type="radio"/> 10 <input type="radio"/> 15 <input type="radio"/> 60 minutes

- **System Name:** Set the system's name or use the default.
- **WAN Failure Message:** Enter the Administrator's information here, such as administrator's name, telephone number, e-mail address, etc. If users encountered problems in the connection of the WAN port to the system, this information will appear on the user's login screen.
- **Device Name:** FQDN (Fully-Qualified Domain Name). This is used as the domain name used in login page. For example, if Device Name=IAS-2000.com, the URL of login page will be <https://IAS-2000.ovislink.com/loginpages/login.shtml>
- **Home Page:** Enter the website of a Web Server to be the homepage. When users log in successfully, they will be directed to the homepage set. Usually, the homepage is the company's website, such as <http://www.default.homepage.com>. Regardless of the original webpage set in the users' computer, they will be redirect to this page after login.
- **Remote Manage IP:** Set the IP block with a system which is able to connect to the web management interface via the authenticated port. For example, 10.2.3.0/24 means that as long as you are within the IP address range of 10.2.3.0/24, you can reach the administration page of IAS-2000. Another example is 10.0.0.3, if you are using the IP address 10.0.0.3, you can reach the administration page of IAS-2000.
- **SNMP:** IAS-2000 supports SNMPv2 and SNMPv3. If the function is enabled, you can assign the Manager IP and the community of SNMPv2 and SNMPv3 to access the management information base (MIB) of the system.
- **System Time:** IAS-2000 supports NTP communication protocol to synchronize the network time. Please specify the IP address of a server and select the desired time zone 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**". Please enter the date and time for these fields.

<b>System Time</b>	Device Time: 2005/09/29 14:27:06																	
	<input type="radio"/> Enable NTP																	
	<input checked="" type="radio"/> Set Device Date and Time (UTC)																	
	<table border="0"> <tr> <td>--</td><td>▼</td><td>Year</td> <td>--</td><td>▼</td><td>Month</td> <td>--</td><td>▼</td><td>Day</td> </tr> <tr> <td>--</td><td>▼</td><td>Hour</td> <td>--</td><td>▼</td><td>Minute</td> <td>--</td><td>▼</td><td>Second</td> </tr> </table>	--	▼	Year	--	▼	Month	--	▼	Day	--	▼	Hour	--	▼	Minute	--	▼
--	▼	Year	--	▼	Month	--	▼	Day										
--	▼	Hour	--	▼	Minute	--	▼	Second										

- **History Report Interval:** Time interval for sending the history notice.

### 5.1.3 WAN1 Configuration

There are 3 methods of obtaining IP address for the WAN1 Port: **Static IP Address**, **Dynamic IP Address**, and **PPPoE**.

WAN1 Configuration	
WAN1 Port	<input checked="" type="radio"/> Static IP Address IP Address: <input type="text" value="10.10.10.208"/> * Subnet Mask: <input type="text" value="255.255.255.0"/> * Default Gateway: <input type="text" value="10.10.10.254"/> * Preferred DNS Server: <input type="text" value="168.95.1.1"/> * Alternate DNS Server: <input type="text"/> <input type="checkbox"/> Enable Bridge Mode <input type="radio"/> Dynamic IP Address <input type="radio"/> PPPoE Client

- Static IP Address:** Manually specifying the IP address of the WAN1 Port is applicable for the network environment where the DHCP service is unavailable. The option of 802.3ad for WAN2 is only available when WAN1 is using a static IP address. The fields with red mark are required. Please fill in these fields.

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

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

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

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

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

**Enable Bridge Mode:** When you set WAN1 with a static IP address and check “**Enable Bridge Mode**”, WAN2 and all LAN ports will share the WAN1 IP address and go into bridge mode as well. See the following figures.

WAN2 Configuration	
WAN2	Bridge Mode

Lan 1 Configuration	
LAN 1	Bridge Mode

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

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

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

“**Password**”. 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"/> *
	Maximum Idle Time: <input type="text" value="0"/> minutes
	Dial on Demand <input checked="" type="radio"/> Enable <input type="radio"/> Disable

### 5.1.4 WAN2 Configuration

There are 4 methods of obtaining IP address for the WAN2 Port: **None**, **Static IP Address**, **Dynamic IP Address**, and **802.3ad**.

- **None**: The WAN2 Port is not functional.

WAN2 Configuration	
WAN2 Port	<input checked="" type="radio"/> None <input type="radio"/> Static IP Address <input type="radio"/> Dynamic IP Address <input type="radio"/> 802.3ad

- **Static IP Address**: Specify the IP address of WAN2 Port, which is applicable for the network environment that IP address cannot be obtained automatically. See the following figure.

WAN2 Configuration	
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"/> *
	<input type="radio"/> Dynamic IP Address <input type="radio"/> 802.3ad

- **Dynamic IP Address**: It is applicable for the network environment that the WAN2 Port can obtain IP address automatically. For example, a DHCP Server is constructed on the network of the WAN2 Port. See the following figure.

WAN2 Configuration	
WAN2 Port	<input type="radio"/> None <input type="radio"/> Static IP Address <input checked="" type="radio"/> Dynamic IP Address <input type="button" value="Renew"/> <input type="radio"/> 802.3ad

- **802.3ad:** This mode will be available if WAN1 is set to Static IP Address. When 802.3ad is enabled, the bandwidth of WAN1 and WAN2 are combined provided that WAN1 and WAN2 are connected to the same set of Switch supporting 802.3ad. See the following figure.

WAN2 Configuration	
WAN2 Port	<input type="radio"/> None <input type="radio"/> Static IP Address <input type="radio"/> Dynamic IP Address <input checked="" type="radio"/> 802.3ad

### 5.1.5 LAN1 / LAN2 Configuration

All of the following four LAN ports can enable or disable user authentication function. In this part, you can set the related configurations about LAN1 port and DHCP server. The configurations of other three LANs are the same with that of LAN1.

Lan 1 Configuration	
LAN 1	Enable VLAN <input type="checkbox"/> Enable User Authentication <input checked="" type="checkbox"/> Operation Mode <input type="text" value="NAT"/> IP Address <input type="text" value="192.168.1.254"/> * Subnet Mask <input type="text" value="255.255.255.0"/> *
DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay

- **LAN1**  
**Enable VLAN:** If you want to split LAN1 into several interfaces, please select the **Enable VLAN** option on the LAN interface. After **Enable VLAN** is selected, the following screen will appear. Choose the desired Item and click **Edit** for further configuration. See the following figure.

Lan 1 Configuration			
<b>LAN 1</b>	Enable VLAN <input checked="" type="checkbox"/>		
VLAN			
Item	Tag	Status	
1		Disable;	<a href="#">edit</a>
2		Disable;	<a href="#">edit</a>
3		Disable;	<a href="#">edit</a>
4		Disable;	<a href="#">edit</a>
5		Disable;	<a href="#">edit</a>

The system will need confirmation for enabling individual VLAN segment. Click **Enable** to continue. See the following figure.

VLAN Interface Configuration		
<b>VLAN</b>	Enabled	<input type="checkbox"/>

After enabling this VLAN segment, the following screen will appear. See the following description and figure for details.

**Enable User Authentication (on VLAN)**

VLAN Interface Configuration		
<b>VLAN</b>	Enabled	<input checked="" type="checkbox"/>
	Enable User Authentication	<input type="checkbox"/>
	VLAN Tag	<input type="text"/> *
	Mode	NAT
	IP Address	192.168.12.254*
	Subnet Mask	255.255.255.0*
<b>VLAN DHCP Configuration</b>	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> DHCP Relay	

- **Enable:** Enable this VLAN segment.
- **Enable User Authentication:** Control the User Authentication according to individual VLAN segment.

- **VLAN Tag:** Enter any integer number within the range of 2~4094 as the Tag for this VLAN segment.
- **Mode:** Two modes are provided: NAT mode and ROUTER mode.
  - 1. NAT:** All IP addresses externally connected through the VLAN port (these IP addresses must belong to the same network for the VLAN port) will be converted into the IP addresses of the WAN1 port by IAS-2000 and onward to outside the network.
  - 2. Router:** All IP addresses externally connected through the VLAN port use its original IP address for external connections. Thus, IAS-2000 acts like a Router.
- **IP Address:** Enter the desired IP address for setup.
- **Subnet Mask:** Enter the desired Subnet Mask for setup.

### VLAN DHCP Configuration

- **Disable DHCP Server:** Disable the function of the DHCP Server.

The screenshot shows a web interface titled "VLAN DHCP Configuration". On the left is a sidebar with the title. The main content area contains three radio button options: "Disable DHCP Server" (which is selected), "Enable DHCP Server", and "DHCP Relay".

- **Enable DHCP Server:** If you want to use the DHCP Server function, you must set it up properly. Related information needed on setting up the DHCP Server is described as follows: DHCP Pool Start IP Address, DHCP Pools End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Server, Lease Time, and Reserved IP Address List. See the following figure.

The screenshot shows the "VLAN DHCP Configuration" web interface with "Enable DHCP Server" selected. Below the radio buttons, there are several configuration fields:
 

- DHCP Scope:** A sub-section header.
- Start IP Address:** A text input field with a red asterisk.
- End IP Address:** A text input field with a red asterisk.
- Preferred DNS Server:** A text input field with a red asterisk.
- Alternate DNS Server:** A text input field.
- Domain Name:** A text input field with a red asterisk.
- WINS Server:** A text input field.
- Lease Time:** A dropdown menu currently set to "1 Hour".
- Reserved IP Address List:** A blue hyperlink.

 At the bottom of the main content area, the "DHCP Relay" radio button is visible and unselected.



If you want to use the reserved IP address 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 -- VLAN Tag:			
Item	Reserved IP Address	MAC	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>
(Total:40) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a>			

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

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

- **DHCP Server Configuration**

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

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

**2. Enable DHCP Server:** If you want to use the DHCP Server function, you must set it up properly. Related information needed on setting up the DHCP Server is described as follows: DHCP Pool Start IP Address, DHCP Pools End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Server, Lease Time, and Reserved IP Address List. See the following figure.

DHCP Server Configuration

Disable DHCP Server  
 Enable DHCP Server

DHCP Scope:

Start IP Address:  \*

End IP Address:  \*

Preferred DNS Server:  \*

Alternate DNS Server:

Domain Name:  \*

WINS Server:

Lease Time:  ▼

[Reserved IP Address List](#)

Enable DHCP Relay

If you want to use the reserved IP address 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 -- lan 1			
Item	Reserved IP Address	MAC	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>
(Total:40) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a>			

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

See the following figure.

<b>DHCP Server Configuration</b>	<input type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input checked="" type="radio"/> Enable DHCP Relay DHCP Server IP <input style="width: 100px;" type="text"/> *
----------------------------------	--

## 5.2 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	
<b>Network Address Translate</b>	System provides three types of Network Address Translation: DMZ, Virtual Server and Port/IP Redirection.
<b>Privilege List</b>	System provides Privilege IP Address List and Privilege MAC Address List. Authentication is NOT required for those listed devices. Policies defined in "User Authentication" can be applied to devices in MAC Address List as well.
<b>Monitor IP List</b>	System can monitor up to 40 network devices using IP packets periodically.
<b>Walled Garden List</b>	Up to 20 URLs or IP addresses could be defined in Walled Garden List. Clients may access these sites without authentication.
<b>Proxy Server Properties</b>	System has one built-in Proxy Server and supports up to 20 external Proxy Servers.
<b>Dynamic DNS</b>	System supports dynamic DNS (DDNS) to translate WAN IP to a domain name automatically.
<b>IP Mobility</b>	System supports IP PNP and Mobile IP Configuration

### 5.2.1 Network Address Translation

There are three parts, **DMZ, Virtual Servers and Port and IP Redirect**, need to be set.

<b>Network Address Translate</b>
<a href="#">DMZ</a>
<a href="#">Virtual Servers</a>
<a href="#">Port and IP Redirection</a>

- DMZ**

**De-Militarized Zone.** A computer within a DMZ is unprotected by firewall and typically all port accesses are routed through to that computer. A router will forward all traffic to the computer specified in the DMZ if it does not otherwise have a rule for how to forward traffic on a given port. There are 40 sets of static **Internal IP Address** and **External IP Address** available. These settings will become effective immediately after clicking the **Apply** button.

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

- Virtual Servers**

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

Virtual Servers					
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"/>

- **Port and IP Redirect**

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

Port and IP Redirection					
Item	Original Destination		Redirect to		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

### 5.2.2 Privilege List

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

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

- Privilege IP Address List**

If there are some workstations belonging to the managed server that need to access the network without authentication, and enter the IP addresses of these workstations in this list. The “**Remark**” blank is not necessary but is useful to keep track. IAS-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"/>
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"/>

**Warning:** Permitting specific IP addresses to have network access rights without going through standard authentication process at the authenticated LAN 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. IAS-2000 allows 100 privilege MAC addresses at most. The list can be created by entering data in the table or by import from a file. The list can be exported as well.

If you want to manually create the list, be sure to enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (not necessary), and select a policy for the individual entry. These settings will become effective immediately after clicking **Apply**.

**Attention:** No matter how you choose to create the list, you must select an **Access Gateway** first.

Privilege MAC Address List			
<input type="text"/>		MAC Search	<a href="#">Import List</a> <a href="#">Export List</a>
Item	MAC Address	Policy	Remark
1	<input type="text"/>	Policy1 ▾	<input type="text"/>
2	<input type="text"/>	Policy1 ▾	<input type="text"/>
3	<input type="text"/>	Policy1 ▾	<input type="text"/>
4	<input type="text"/>	Policy1 ▾	<input type="text"/>
5	<input type="text"/>	Policy1 ▾	<input type="text"/>
6	<input type="text"/>	Policy1 ▾	<input type="text"/>
7	<input type="text"/>	Policy1 ▾	<input type="text"/>
8	<input type="text"/>	Policy1 ▾	<input type="text"/>
9	<input type="text"/>	Policy1 ▾	<input type="text"/>
10	<input type="text"/>	Policy1 ▾	<input type="text"/>

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

**Import List:** Select an Access Gateway and then click **Import List** to enter the **Upload Privilege MAC Address List** interface. Click the **Browse** button to select the text file for the user account upload. Then click **Submit** to complete the upload.

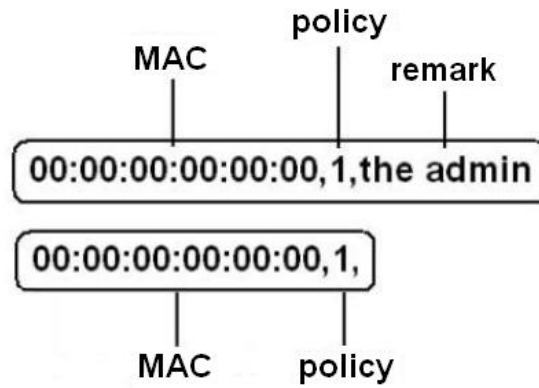
**Note:** The format of each line is "MAC, Policy, Remark" without the quotes. There must be no space between the fields and commas. The Remark field could be omitted but the leading comma must be retained. While uploading the list, existing MAC address in the Privilege MAC Address List will not be replaced.

Upload MAC Address

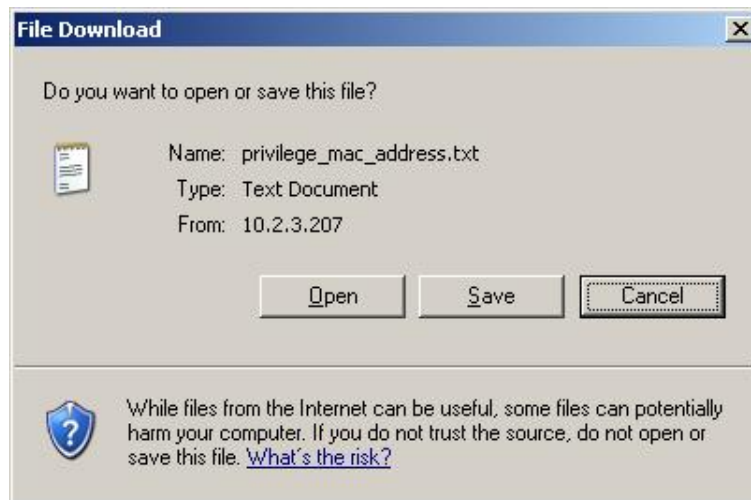
File Name

The uploading file should be a text file and the format of each line is "**MAC, Group, Remark**" without the quotes. There must be no spaces between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by new ones.





**Export List:** Click this to export the Mac List to create a .txt file and then save it on disk.



### 5.2.3 Monitor IP List



The system will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the related information, click **Apply** and these settings will become effective immediately. You can click **Monitor** to check the current status of all the monitored IP. The system provides 40 IP addresses a most on the "**Monitor IP List**".

Monitor IP List			
Monitor Email			
Send From		<input type="text"/>	
Send To		<input type="text"/>	
Interval		6 Hours ▾	
SMTP Server		<input type="text"/>	
Auth Method		NONE ▾	
Item	IP Address	Item	IP Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

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

**Monitor**

- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Send To:** The e-mail address of the person whom the monitoring result is for. This will be the receiver's e-mail.
- **Interval:** The time interval to send the e-mail report.
- **SMTP Server:** The IP address of the SMTP server.
- **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method you select, you have to enter the **Account Name**, **Password** and **Domain**.
- **IP Address:** The IP addresses under monitoring.

Monitor IP result		
No	IP Address	Result
1	192.168.1.200	
2	192.168.1.100	

## 5.2.4 Walled Garden List

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

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

## 5.2.5 Proxy Server Properties

IAS-2000 supports Internal Proxy Server and External Proxy Server functions. Please perform the necessary configurations.

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

Please click **Apply** and these settings will become effective immediately.

## 5.2.6 Dynamic DNS

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

<b>DDNS</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Provider</b>	3322.org(Dynamic) ▼
<b>Host name</b>	1111111
<b>Username/E-mail</b>	2222222
<b>Password/Key</b>	333333

- **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.

Please click **Apply** and these settings will become effective immediately.

## 5.2.7 IP Mobility

<b>Enable Mobile IP</b>	<input type="checkbox"/> Enable
<b>Enable IP PNP</b>	<input type="checkbox"/> Enable

- **Enable IP PNP**  
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 IAS-2000 and access the network.
- **Enable Mobile IP**  
If you construct a network environment using several sets of IAS-2000, a user can use the same group of IP configurations. When you roam into different locations, the connection will be kept alive; therefore no disconnection will occur for example when downloading data.

## 5.3 User Authentication

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

**Air Live**  
OvisLink Corp.  
www.ovislink.com.tw

Logout  
Help

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

**User Authentication**

User Authentication	
<b>Authentication Configuration</b>	System provides four external server configurations (POP3, RADIUS, LDAP and NT Domain), one internal user DB (Local User) and two pre-defined mechanisms for paying users (On-Demand User and PMS) to authenticate user access. Each authentication method can apply one Black List profile and one Policy for traffic control. Regarding paying users, On-Demand Server Configuration supports print-out of user account information from an optional ticket printer. As for PMS, PMS Server Configuration supports unified Micros Fidelio Property Management System Billing.
<b>Policy Configuration</b>	System supports one Global and five policies for traffic control. Administrator can define a policy with the firewall profile, specific route profile, login schedule profile, and bandwidth.
<b>Black List Configuration</b>	System supports five Black Lists for authentication. On-Demand and PMS Server DOES NOT support Black List configuration.
<b>Guest User Configuration</b>	System provides up to 10 guest accounts. Guest accounts have permission different from general user accounts. Guest accounts are stored on embedded-database under Global policy.
<b>Additional Configuration</b>	System supports other authentication settings, such as: Idle/Session timeout, Multiple login enable/disable, Friendly logout, and Permit MAC address list. It also supports uploading customized login/logout pages and certificate file.

Authentication Configuration  
Policy Configuration  
Black List Configuration  
Guest User Configuration  
Additional Configuration

Home Back

### 5.3.1 Authentication Configuration

This function is to configure the settings for different authentication servers. The system provides 5 servers (Local, POP3, RADIUS, LDAP and NT Domain), one On-demand User and one PMS User 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 screen to choose a server to be the default server and enable or disable any server on the list.

Authentication Server Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enabled
<a href="#">Local Server</a>	LOCAL	local	Policy1	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
<a href="#">POP3 Server</a>	POP3	Postfix2	Policy1	<input type="radio"/>	<input checked="" type="checkbox"/>
<a href="#">RADIUS Server</a>	RADIUS	Postfix3	Policy1	<input type="radio"/>	<input checked="" type="checkbox"/>
<a href="#">LDAP Server</a>	LDAP	Postfix4	Policy1	<input type="radio"/>	<input checked="" type="checkbox"/>
<a href="#">NT Domain</a>	NTDOMAIN	Postfix5	Policy1	<input type="radio"/>	<input checked="" type="checkbox"/>
<a href="#">On Demand User</a>	ONDEMAND	bonalinx	Policy1	<input type="radio"/>	<input checked="" type="checkbox"/>
<a href="#">PMS User</a>	PMS	MyHotel	Policy1	<input type="radio"/>	<input checked="" type="checkbox"/>

### 5.3.1.1 Local Server

This server is only for “**Local User**”, you can’t change the authentication method for the server.

Authentication Server - Local Server	
Server Name	<input type="text" value="Local Server"/> <small>** (its server name.)</small>
Server Status	Enable
Postfix	<input type="text" value="Postfix1"/> <small>** (its postfix name.)</small>
Blacklist	<input type="text" value="None"/>
Local User Account	<a href="#">Local User Setting</a>
Policy Name	<input type="text" value="Policy1"/>
<input checked="" type="button" value="Apply"/> <input type="button" value="Clear"/>	

- **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.

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

- **Black List:** There are five sets of the black lists. You can select one of them or choose “**None**”. Please refer to **5.3.3 Black List Configuration**
- **Local User Account:** Click the Local User Setting hyperlink to set the further configuration.
- **Policy Name:** There are four policies to choose from to apply to this particular server.

Click the **Local User Setting** hyperlink for further configuration.

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

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

Add User Import List Export List Refresh

Search

User List				
Username	Password	MAC	Policy	Del All
			Remark	
<a href="#">user1</a>	user1		Policy1	<a href="#">Delete</a>
			remark1	
<a href="#">user2</a>	user2		Policy1	<a href="#">Delete</a>
			remark2	
<a href="#">user3</a>	user3		Policy1	<a href="#">Delete</a>
			remark3	

**Add User:** Click this button to enter the **Add User** interface. Fill in the necessary information such as “**Username**”, “**Password**”, “**MAC**” and “**Remark**” (optional). Then, select a desired **Maximum Bandwidth**, **Request Bandwidth** and **Group**, and then click **Apply** to complete adding the user or users.



Add User				
Item	Username	MAC (XX:XX:XX:XX:XX:XX)	Maximum Bandwidth	Policy
	Password		Request Bandwidth	Remark
1	<input type="text"/>	<input type="text"/>	Unlimited ▾	None ▾
	<input type="text"/>		None ▾	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	Unlimited ▾	None ▾
	<input type="text"/>		None ▾	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	Unlimited ▾	None ▾
	<input type="text"/>		None ▾	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	Unlimited ▾	None ▾
	<input type="text"/>		None ▾	<input type="text"/>

Users(s) been added successfully:  
aaaa bbbb cccc dddd

Add User				
Item	Username	MAC (XX:XX:XX:XX:XX:XX)	Maximum Bandwidth	Policy
	Password		Request Bandwidth	Remark
1	<input type="text"/>	<input type="text"/>	Unlimited ▾	None ▾
	<input type="text"/>		None ▾	<input type="text"/>

- Import 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.

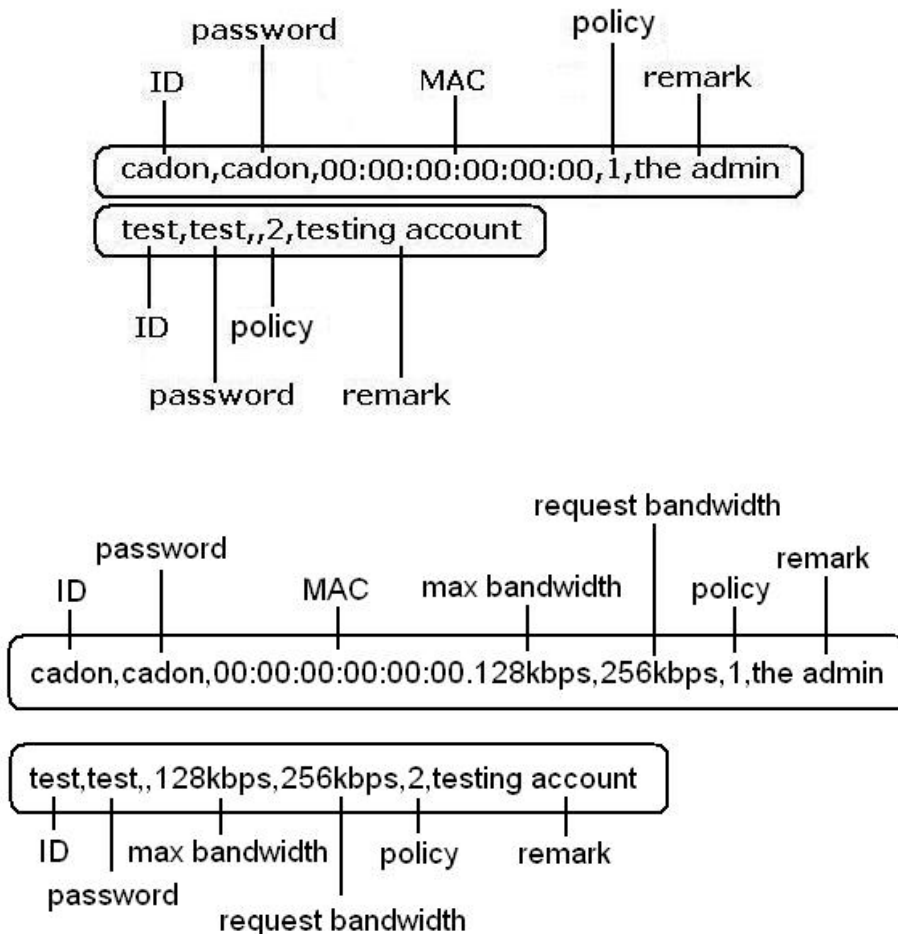
**Note:** The format of each line is "ID, Password, MAC, Policy, Remark" or "ID, Password, MAC, Max bandwidth, Request bandwidth, Policy, Remark" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding 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, Group, Remark" or "ID, Password, MAC, Max bandwidth, Request bandwidth, Policy, Remark" without the quotes. There must be no spaces between the fields and commas. The MAC field could be omitted but the trailing comma

must be retained. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by new ones.



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



- **Refresh:** Click this to renew the list. Refresh button

User List				
Username	Password	MAC	Policy	Del All
			Remark	
<a href="#">user1</a>	user1		Policy1	<a href="#">Delete</a>
			remark1	
<a href="#">user2</a>	user2		Policy1	<a href="#">Delete</a>
			remark2	
<a href="#">user3</a>	user3		Policy1	<a href="#">Delete</a>
			remark3	

- **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	Group	Del All
			Remark	
<a href="#">test</a>	test		None	<a href="#">Delete</a>
<a href="#">test1</a>	test1		None	<a href="#">Delete</a>
<a href="#">test2</a>	test2		Policy1	<a href="#">Delete</a>
<a href="#">TEST</a>	TEST		Policy1	<a href="#">Delete</a>

(Total:4) [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 User** Interface for that particular user, and then modify or add any desired information such as “**Username**”, “**Password**”, “**MAC**”, “**Maximum Bandwidth**”, “**Request Bandwidth**”, “**Policy**” and “**Remark**” (optional) . Then, click **Apply** to complete the modification.

Edit User	
Username	<input type="text" value="usr4001"/> *
Password	<input type="text" value="usr4001"/> *
MAC	<input type="text"/>
Maximum Bandwidth	<input type="text" value="Unlimited"/>
Request Bandwidth	<input type="text" value="None"/>
Policy	<input type="text" value="None"/>
Remark	<input type="text"/>

- **Radius Roaming Out / 802.1x Authentication:** These two functions can be enabled or disabled separately.

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

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

Radius Client Configuration				
No.	Type	IP Address	Segment	Secret
1	<input type="text" value="Disable"/>	<input type="text" value="10.2.3.140"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text" value="cipherium"/>
2	<input type="text" value="Disable"/>	<input type="text" value="10.2.3.245"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text" value="cipherium"/>
3	<input type="text" value="Disable"/>	<input type="text" value="10.10.10.203"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>
4	<input type="text" value="Disable"/>	<input type="text" value="10.0.0.0"/>	<input type="text" value="255.0.0.0 (/8)"/>	<input type="text" value="12345678"/>
5	<input type="text" value="Disable"/>	<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0 (/24)"/>	<input type="text" value="12345678"/>

**Roaming Out:** When you have selected “**Roaming Out**”, the local users can login from other sites using their original accounts.

**802.1x:** This system support **PEAP (Protracted Extensible Authentication Protocol)** function. The 802.1x function must be used in LAN ports.

### 5.3.1.2 POP3 Server

POP3, RADIUS, LDAP and NT Domain Server can change the authentication method. Choose “**POP3**” in the **Authentication Method** field, the hyperlink beside the pull-down menu will become “**POP3 Setting**”.

Authentication Server - POP3 1Server	
Server Name	<input type="text" value="POP3 Server"/> <small>** (Its server name.)</small>
Server Status	Disable
Postfix	<input type="text" value="Postfix2"/> <small>** (Its postfix name.)</small>
Blacklist	None
Authentication Method	POP3 <a href="#">POP3 Setting</a>
Policy Name	<div style="border: 1px solid black; padding: 2px;">           POP3            Radius            LDAP            NTDomain         </div>
<input type="button" value="✓ Apply"/> <input type="button" value="✗ Clear"/>	

- **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.

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

- **Black List:** There are five sets of the black lists. You can select one of them or choose “**None**”. Please refer to **5.3.3 Black List Configuration**
- **Authentication Method:** There are four authentication methods, **POP3**, **RADUUS**, **LDAP** and **NT Domain** to configure from. Select the desired method and then click the link besides the pull-down menu for more advanced configuration.
- **Policy Name:** There are four policies to choose from to apply to this particular server.

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

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

- **Server IP:** Enter the IP address/domain name given by your ISP.
- **Port:** Enter the Port given by your ISP. The default value is 100.
- **SSL Setting:** If this option is enabled, the POP3 protocol will perform the authentication.

### 5.3.1.3 Radius Server

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

Authentication Server - POP2 Server	
Server Name	<input type="text" value="RADIUS Server"/> *(Its server name.)
Server Status	Disable
Postfix	<input type="text" value="Postfix3"/> *(Its postfix name.)
Blacklist	<input type="text" value="None"/>
Authentication Method	<input type="text" value="Radius"/> <a href="#">RADIUS Setting</a>
Policy Name	<input type="text" value="POP3"/> <input type="text" value="Radius"/> <input type="text" value="LDAP"/> <input type="text" value="NTDomain"/>
<input type="button" value="✓ Apply"/> <input type="button" value="✗ Clear"/>	

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

RADIUS Setting	
802.1x Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Radius Client List</a>
Trans Full Name	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Primary RADIUS Server	
Server IP	<input type="text"/> *
Authentication Port	<input type="text"/> *(Default: 1812)
Accounting Port	<input type="text"/> *(Default: 1813)
Secret Key	<input type="text"/> *
Accounting Service	<input type="radio"/> Enable <input type="radio"/> Disable
Authentication Protocol	CHAP ▼
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 type="radio"/> Enable <input type="radio"/> Disable
Authentication Protocol	CHAP ▼

- **802.1X Authentication:** Enable this function and the hyperlink of **Radius Client List** will appear. Click the hyperlink to get into the Radius Client Configuration list for further configuration. Please refer to **Radius Roaming Out/802.1x Authentication in 5.3.1.1 Authentication Method – Local User**.
- **Trans Full Name:** When enabled, the ID and postfix will be transferred to the RADIUS server for authentication. When disabled, only the ID will be transferred to RADIUS server for authentication.
- **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.

**Notice:** If Radius Server does not assign idle-timeout value, IAS-2000 will use the local idle-timeout instead.

### 5.3.1.4 LDAP Server

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

Authentication Server - LDAP Server	
Server Name	<input type="text" value="LDAP Server"/> <small>***(Its server name.)</small>
Server Status	Disable
Postfix	<input type="text" value="Postfix4"/> <small>***(Its postfix name.)</small>
Blacklist	None
Authentication Method	LDAP <a href="#">LDAP Setting</a>
Policy Name	<div style="border: 1px solid black; padding: 2px;">                     POP3                      Radius                      LDAP                      NTDomain                 </div>
<input type="button" value="Apply"/> <input type="button" value="Clear"/>	

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

Primary LDAP Server	
Server IP	<input type="text"/> <small>*(Domain Name/IP Address)</small>
Port	<input type="text"/> <small>*(Default: 389)</small>
Base DN	<input type="text"/> <small>*(CN=,dc=,dc=)</small>
Binding Type	User Account
Account Attribute	<div style="border: 1px solid black; padding: 2px;">                     User Account                      Anonymous                      Specified DN                      Windows AD                 </div> sAMAccountName
Secondary LDAP Server	
Server IP	<input type="text"/>
Port	<input type="text"/>
Base DN	<input type="text"/>
Binding Type	User Account
Account Attribute	<input checked="" type="radio"/> UID <input type="radio"/> CN <input type="radio"/> sAMAccountName

- **Server IP:** Enter the IP address/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.
- **Binding Type:** There are four binding types, User Account, Anonymous, Specific DN and Windows AD to select.
  - **User Account:** Use the user account’s login username and password of the system, and then select one **Account Attribute** (UID, CN or sAMAccountName) to access the LDAP server.



Primary LDAP Server	
Server IP	<input type="text"/> *(Domain Name/IP Address)
Port	<input type="text"/> *(Default: 389)
Base DN	<input type="text"/> *(CN=,dc=,dc=)
Binding Type	User Account ▾
Account Attribute	<input checked="" type="radio"/> UID <input type="radio"/> CN <input type="radio"/> sAMAccountName

- **Anonymous:** Access the LDAP servers without requiring authentication but only select one **Account Attribute** (UID, CN or sAMAccountName).

Primary LDAP Server	
Server IP	<input type="text"/> *(Domain Name/IP Address)
Port	<input type="text"/> *(Default: 389)
Base DN	<input type="text"/> *(CN=,dc=,dc=)
Binding Type	Anonymous ▾
Account Attribute	<input checked="" type="radio"/> UID <input type="radio"/> CN <input type="radio"/> sAMAccountName

- **Specified DN:** Entering the specific DN username and password in the “**Bind RDN**” and “**Bind Password**” fields, and then select one **Account Attribute** (UID, CN or sAMAccountName) to access the LDAP server.

Primary LDAP Server	
Server IP	<input type="text"/> *(Domain Name/IP Address)
Port	<input type="text"/> *(Default: 389)
Base DN	<input type="text"/> *(CN=,dc=,dc=)
Binding Type	Specified DN ▾
Bind RDN:	<input type="text"/>
Bind Password:	<input type="text"/>
Account Attribute	<input checked="" type="radio"/> UID <input type="radio"/> CN <input type="radio"/> sAMAccountName

- **Windows AD:** Enter the domain name of Windows AD to access the LDAP server.

Primary LDAP Server	
Server IP	<input type="text"/> *(Domain Name/IP Address)
Port	<input type="text"/> *(Default: 389)
Base DN	<input type="text"/> *(CN=,dc=,dc=)
Binding Type	Windows AD ▾
Domain	<input type="text"/>

### 5.3.1.5 NT Domain Server

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

Authentication Server - NT Domain	
Server Name	<input type="text" value="NT Domain"/> ***(Its server name.)
Server Status	Disable
Postfix	<input type="text" value="Postfix5"/> ***(Its postfix name.)
Blacklist	None ▾
Authentication Method	NTDomain ▾ <a href="#">NT Domain Setting</a>
Policy Name	POP3 Radius LDAP
<input checked="" type="checkbox"/> Apply <input type="checkbox"/> 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 type="radio"/> Enable <input checked="" type="radio"/> Disable

- **Server IP address:** Enter the server IP address of the domain controller.
- **Transparent Login:** If this function is enabled, when users log into the Windows domain, they will log into IAS-2000 automatically.

### 5.3.1.6 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	Disable
Postfix	<input type="text" value="ovislink"/> *(e.g. ovislink. Max: 40 char)
Receipt Header 1	<input type="text" value="Welcome!"/> (e.g. Welcome!)
Receipt Header 2	<input type="text" value="Header2"/>
Receipt Footer	<input type="text" value="Thank You!"/> (e.g. Thank You!)
Monetary Unit	<input checked="" type="radio"/> None <input type="radio"/> £ GBP <input type="radio"/> € EUR <input type="radio"/> \$ USD
Policy Name	<input type="text" value="Policy1"/> ▼
WLAN ESSID	<input type="text" value="ovislink"/> (e.g. ovislink)
WEP Key	<input type="text"/>
Remark	<input type="text"/> (for customer)
Billing Notice Interval	<input checked="" type="radio"/> 10mins <input type="radio"/> 15mins <input type="radio"/> 20mins
<a href="#">Users List</a> <a href="#">Billing Configuration</a> <a href="#">Create On-Demand User</a>	

**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 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.

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

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

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

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

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	<a href="#">Delete</a>
97UU	V7B23947	2 hour	2 hour	2005/06/05-11:45:26	<a href="#">Delete</a>

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

- **Search:** Enter a keyword of a username 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.
- **Del All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.
- **Billing Configuration:** Click this to enter the **Billing Configuration** screen. In the **Billing Configuration** screen, Administrator may configure up to 10 billing rules.

Billing Configuration						
Button	Status	Type	Expired Info	Valid Duration	Price	
1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> Data <input type="text" value="999"/> Mbyte <input type="radio"/> Time <input type="text" value="999"/> Hrs <input type="text" value="59"/> Mins	<input type="text" value="999"/> Days <input type="text" value="999"/> Hrs	<input type="text" value="999"/> Days	<input type="text" value="0"/>	
2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> Data <input type="text" value="0"/> Mbyte <input type="radio"/> Time <input type="text" value="0"/> Hrs <input type="text" value="0"/> Mins	<input type="text" value="0"/> Days <input type="text" value="0"/> Hrs	<input type="text" value="0"/> Days	<input type="text" value="0"/>	
3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> Data <input type="text" value="0"/> Mbyte <input type="radio"/> Time <input type="text" value="0"/> Hrs <input type="text" value="0"/> Mins	<input type="text" value="0"/> Days <input type="text" value="0"/> Hrs	<input type="text" value="0"/> Days	<input type="text" value="0"/>	
4	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> Data <input type="text" value="0"/> Mbyte <input type="radio"/> Time <input type="text" value="0"/> Hrs <input type="text" value="0"/> Mins	<input type="text" value="0"/> Days <input type="text" value="0"/> Hrs	<input type="text" value="0"/> Days	<input type="text" value="0"/>	

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

**Type:** Set the billing rule by **“Data”** (the maximum volume allowed is 999 Mbyte) or **“Time”** (the






maximum time allowed is 999 hours and 59 minutes).

**Expired Info:** 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 (the maximum days allowed is 999 days and the maximum time allowed is 999 hours).

**Valid Duration:** 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.

**Price:** The price charged for this billing rule.

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

On-Demand User Generate			
Button	Type	Status	Function
1	2 hrs 0 mins	Enabled	
2	12 Mbyte	Enabled	
3	N/A	Disabled	
4	N/A	Disabled	
5	N/A	Disabled	

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

Welcome!  
Header2

Username	2CSO@ovislink
Password	7N799687
Price	2
Usage	1 hrs 0 mins
ESSID : ondemand	
Share WEP Keys:	
Valid to use until: 2005/10/01 15:24:48	

Thank You!




### 5.3.1.7 PMS User

The system integrates a hotel in-door billing system, PMS, developed by Micros Fidelio, and it usually used in a hotel environment. When the customers need to use wireless Internet in the hotel, they have to get a printed receipt with username and password form the hotel to log in the system for wireless access.

PMS User Configuration	
Server Status	Disable
PMS Server IP	<input type="text"/> (e.g. 10.0.0.1)
PMS Server Port	<input type="text" value="9877"/>
Postfix	<input type="text" value="pms"/> *(e.g. pms. Max: 40 char)
Policy Name	<input type="text" value="Policy1"/> ▼
Receipt Header 1	<input type="text" value="Welcome!"/> (e.g. Welcome!)
Receipt Header 2	<input type="text" value="Enjoy your stay"/>
Receipt Footer	<input type="text" value="Thank You !"/> (e.g. Thank You!)
WLAN ESSID	<input type="text" value="pms"/> (e.g. pms)
WEP Key	<input type="text"/>
Remark	<input type="text" value="Have a nice day!"/> (for customer)
<a href="#">Users List</a> <a href="#">Billing Configuration</a> <a href="#">Create PMS User</a>	

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

**PMS Server IP:** Enter the IP address of the PMS server.

**PMS Server Port:** Enter the Port of the PMS server.

**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.

**Policy Name:** There are five policies to select from.

**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.

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

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

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

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

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

**Room No.:** The room number of the PMS user.

**Username:** The login name of the PMS user.

**Password:** The login password of the PMS user.

**Remain Time:** 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/Valid Time:** The **Valid Time** indicates 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-expires. The **Expire Time** indicates the duration of time that the user can use the account after the activation of the account. After this duration, the account will self-expires.

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

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

**Redeem:** This is used to increase the remaining time of the account. When the remaining time or data quota is insufficient, the user has to pay for adding credit at the counter and the user will get a new username and password.

- **Billing Configuration:** Click this to enter the **Billing Configuration** screen. In the **Billing Configuration** screen, Administrator may configure up to 5 billing rules.

PMS User Billing Configuration					
Plan	Status	Hr. Purchased (Hours)	Valid Period (Hours)	Assign to Policy	Price (e.g.: 10.00)
1	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="text" value="1"/>	<input type="text" value="1"/>	0: NONE ▼	<input type="text" value="1.00"/>
2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="text" value="0"/>	<input type="text" value="0"/>	0: NONE ▼	<input type="text" value="0"/>
3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="text" value="0"/>	<input type="text" value="0"/>	0: NONE ▼	<input type="text" value="0"/>
4	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="text" value="0"/>	<input type="text" value="0"/>	0: NONE ▼	<input type="text" value="0"/>
5	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="text" value="0"/>	<input type="text" value="0"/>	0: NONE ▼	<input type="text" value="0"/>

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

**Hr. Purchased:** This is the duration of time that the user can use the account after the activation of the account. After this duration, the account will self-expires. You can enter 1-999 hours.

**Valid Period:** 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-expires. You can enter 1-999 hours.

**Assign to Policy:** Assign a policy for this billing rule.

**Price:** The price charged for this billing rule.

**Note:** There is an **Auto Expired** mechanism is for preventing that an account is created but never logged in. If the account is created but never been logged in, the account will be invalid after a period. **The auto expired time = the exact created time of the account + Valid Period.**

- **Created PMS User:** Click this to enter the **PMS User Generate** screen. There are 5000 PMS user accounts available.

PMS User Generation				
Plan	Type	Price	Status	Configuration
1	1 hrs	1.00	Enabled	Room Number: <input type="text"/> Maximum User: <input type="text" value="1"/>
2	0 hrs	0	Disabled	Room Number: <input type="text"/> Maximum User: <input type="text" value="1"/>
3	0 hrs	0	Disabled	Room Number: <input type="text"/> Maximum User: <input type="text" value="1"/>
4	0 hrs	0	Disabled	Room Number: <input type="text"/> Maximum User: <input type="text" value="1"/>
5	0 hrs	0	Disabled	Room Number: <input type="text"/> Maximum User: <input type="text" value="1"/>

**Welcome!**  
Enjoy your stay

Room Number	12345
Username	822S@Hotel
Password	6892BN7Q
Price	1.02
Usage	10 hrs
ESSID : PMS	
Shared WEP keys:	
Concurrent user access: 1	
Must login before: 2005/01/26 22:21:58	

Creating Time: 2005/01/26 11:21:58

**Thank You !**

----- cut here ----- cut here -----

Room Number	12345
Username	822S@Hotel
Price	1.02
Usage	10 hrs
Concurrent user access: 1	
Must login before: 2005/01/26 22:21:58	
<i>Signature:</i>	

Creating Time: 2005/01/26 11:21:58

By default, the PMS user database is empty. While you key in the **“Room Number”** and the **“Maximum User”** and press the **Create** button by the desired rule, a PMS user will be created, then click **Printout** to print a receipt which will contain this PMS user’s information. See the following figure.



### 5.3.2 Policy Configuration

There are a Global policy and the other five policies. Every Policy has three profiles, **Firewall Profile**, **Specific Route Profile**, and **Schedule Profile** as well as one **Bandwidth** setting for that policy. But **Global** policy only has **Firewall Profile** and **Specific Route Profile** settings.

- **Global Policy**

Policy Configuration	
Select Policy:	Global ▼
Firewall Profile	<a href="#">Setting</a>
Specific Route Profile	<a href="#">Setting</a>

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

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

Profile Name:

Firewall Profile							
Filter Rule Item	Active	Action	Name	Source IP	Destination IP	Protocol	MAC
1	<input type="checkbox"/>	Block		Any	Any	All	
2	<input type="checkbox"/>	Block		Any	Any	All	
3	<input type="checkbox"/>	Block		Any	Any	All	
4	<input type="checkbox"/>	Block		Any	Any	All	
5	<input type="checkbox"/>	Block		Any	Any	All	

Edit Filter Rule						
Rule Item:						
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, **WAN**, **Wireless**, **Public LAN (LAN1/LAN2)** and **Private LAN (LAN3/LAN4)**.
- **Source/Destination IP:** Enter the source and destination IP addresses.
- **Source/Destination Subnet Mask:** Enter the source and destination subnet masks.
- **Source/Destination Start/End Port:** Enter the range of source and destination ports.

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

[View System Route Table](#)

**Profile Name:**

Global Route Table			
Route Item	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1	<input type="text" value="111.111.111.111"/>	<input type="text" value="255.255.255.255 (/32)"/> ▼	<input type="text" value="111.111.111.111"/>
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"/>

- **View System Route Table:** Click the hyperlink to see the information of the hosts or the networks.

System Route Table				
Network Address	Netmask	Gateway	Interface	Metric
10.118.11.0	255.255.255.0	0.0.0.0	WAN	0
192.168.2.0	255.255.255.0	0.0.0.0	eth3	0
10.2.3.0	255.255.255.0	0.0.0.0	SLAN	0
127.0.0.0	255.0.0.0	0.0.0.0	lo	0
0.0.0.0	0.0.0.0	10.2.3.254	SLAN	0

- **Profile Name:** The profile name can be changed here.
  - **IP Address (Destination):** The destination IP address of the host or the network.
  - **Subnet Netmask:** Select a destination subnet netmask of the host or the network.
  - **IP Address (Gateway):** The IP address of the next router to the destination.
- **Policy 1~Policy 5**

Policy Configuration	
Select Policy:	2: Policy2
Policy Name 2:	Policy2
Firewall Profile	<a href="#">Setting</a>
Specific Route Profile	<a href="#">Setting</a>
Schedule Profile	<a href="#">Setting</a>
Bandwidth	Unlimited

**Select Policy / Policy Name:** Select a desired policy and you can rename it in the Policy Name field.

**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.

Firewall Profile							
Filter Rule Item	Active	Action	Name	Source IP	Destination IP	Protocol	MAC
<u>1</u>	<input type="checkbox"/>	Block		Any	Any	All	
<u>2</u>	<input type="checkbox"/>	Block		Any	Any	All	
<u>3</u>	<input type="checkbox"/>	Block		Any	Any	All	
<u>4</u>	<input type="checkbox"/>	Block		Any	Any	All	
<u>5</u>	<input type="checkbox"/>	Block		Any	Any	All	
<u>6</u>	<input type="checkbox"/>	Block		Any	Any	All	
<u>7</u>	<input type="checkbox"/>	Block		Any	Any	All	

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

- **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, **WAN**, **Wireless**, **Public LAN (LAN1/LAN2)** and **Private LAN (LAN3/LAN4)**.
- **Source/Destination IP:** Enter the source and destination IP addresses.
- **Source/Destination Subnet Mask:** Enter the source and destination subnet masks.

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

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

- **Profile Name:** The profile name can be changed here.
- **IP Address (Destination):** The destination IP address of the host or the network.
- **Subnet Netmask:** Select a destination subnet netmask of the host or the network.
- **IP Address (Gateway):** The IP address of the next router to the destination.
- **Default:** Check this option to apply the default values.

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

Profile Name:   Enable  Disable

Login Schedule Profile							
HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Bandwidth:** Choose one bandwidth limit for that particular policy.

**Policy Configuration**

Select Policy:

Policy Name 1:

Firewall Profile	<a href="#">Setting</a>
Specific Route Profile	<a href="#">Setting</a>
Schedule Profile	<a href="#">Setting</a>
Bandwidth	<div style="display: flex; align-items: center;"> <div style="border: 1px solid gray; padding: 2px;">             Unlimited           </div> <div style="margin-left: 5px;"> <input checked="" type="checkbox"/> </div> <div style="margin-left: 5px;">             Clear           </div> </div> <ul style="list-style-type: none"> <li>Unlimited</li> <li>16 Kbps</li> <li>32 Kbps</li> <li>64 Kbps</li> <li>128 Kbps</li> <li>256 Kbps</li> <li>512 Kbps</li> <li>1 Mbps</li> <li>2 Mbps</li> <li>3 Mbps</li> <li>5 Mbps</li> </ul>

### 5.3.3 Black List Configuration

The administrator can add, delete, or edit the black list for user access control. Each black list can include 500 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
bbb	ccc	<input type="checkbox"/>
ccc	bbb	<input type="checkbox"/>
ggg	ggg	<input type="checkbox"/>
kkk	kkk	<input type="checkbox"/>

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

[Add User to List](#) [Import Black List](#) [Export Black List](#)

- **Select Black List:** There are 5 lists to select from for the desired black list.
- **Name:** Set the black list name and it will show on the pull-down menu above.
- **Add 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"/>

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

Added User(s) : eeee

Add Users to Blacklist Blacklist5		
No	Username	Remark
1	<input type="text"/>	<input type="text"/>

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

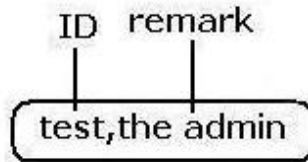
Black List Configuration		
Select Black List:	1:Blacklist1	
Name	Blacklist1	
User	Remark	Delete
bbb	ccc	<input checked="" type="checkbox"/>
ccc	bbb	<input type="checkbox"/>
ggg	ggg	<input checked="" type="checkbox"/>
kkk	kkk	<input type="checkbox"/>

**Import Black List:** Click this to enter the **Upload black List Account – (Blacklist1)** interface. Click the **Browse** button to select the text file for the user account upload to the black list. Then click **Submit** to complete the upload process.

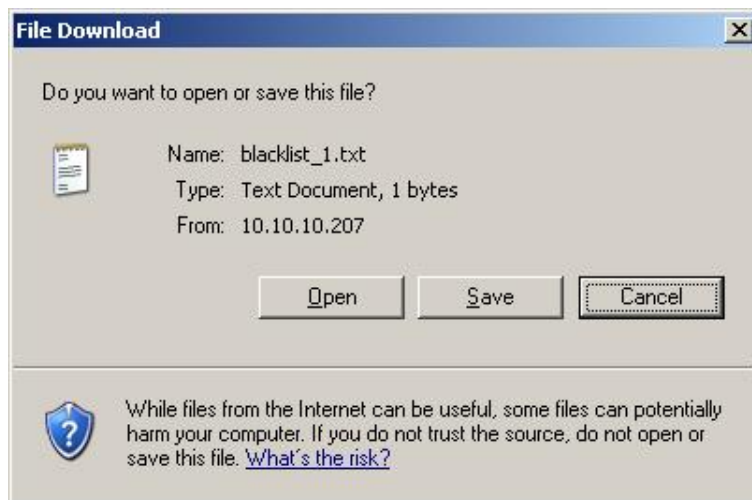
**Note 1:**The format of each line is "ID, Remark" without the quotes. There must be no space between the fields and commas. When adding user accounts by uploading a file, any existing account in the embedded database that has the same user name as the one defined in the uploaded file will not be replaced by the new one.

Upload Black List Account	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

The uploading file should be a text file and the format of each line should be "**ID, Remark**" without the quotes. There must be no spaces between the fields and commas. 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.



- **Export Black List:** Click **Export List** to create a .txt file and then save it on disk.





### 5.3.4 Guest User Configuration

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

Guest User Configuration	
Guest User Configuration	<input checked="" type="radio"/> Enable Guest User <input type="radio"/> Disable Guest User
	<a href="#">Guest User List</a>
	Session Length <input type="text" value="Unlimit"/> hours

- **Guest User List:** IAS-2000 offers ten guest users for log in. To activate a guest user, just enter the password in the corresponding “**Password**” text field for that guest account. Guest accounts with blank password will not be activated.

Guest Users List		
Item	Username	Password
1	guest1	<input type="text"/>
2	guest2	<input type="text"/>
3	guest3	<input type="text"/>
4	guest4	<input type="text"/>
5	guest5	<input type="text"/>
6	guest6	<input type="text"/>
7	guest7	<input type="text"/>
8	guest8	<input type="text"/>
9	guest9	<input type="text"/>
10	guest10	<input type="text"/>

- **Session Length:** This restricts the connection time of the guest users. The default session length is 6 hours and the available session time ranges from 1 to 12 hours or unlimited.

### 5.3.5 Additional Configuration

Additional Configuration	
<b>User Control</b>	Idle Timer: <input type="text" value="10"/> minutes <small>*(Range: 1-1440)</small> Multiple Login <input checked="" type="checkbox"/> <small>(On-Demand User and RADIUS accounting do not support multiple login.)</small> Friendly Logout <input checked="" type="checkbox"/>
<b>Roaming Out Timer</b>	Session Timeout: <input type="text" value="5"/> minutes <small>*(Range: 5-1440)</small> Idle Timeout: <input type="text" value="3"/> minutes <small>*(Range: 1-120)</small> Interim Update: <input type="text" value="1"/> minutes <small>*(Range: 1-120)</small>
<b>Internet Connection Detection</b>	http:// <input type="text"/> Fail Action: <input type="text" value="pass"/>
<b>Upload File</b>	<a href="#">Certificate</a> <a href="#">Login Page</a> <a href="#">Logout Page</a> <a href="#">Login Success Page</a> <a href="#">Logout Success Page</a>
<b>Credit Reminder</b>	Volume <input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="1"/> Mbyte <small>*(Default: 1; Range: 1-10)</small> Time <input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="5"/> minutes <small>*(Default: 5; Range: 1-30)</small>
<b>POP3 Message</b>	<a href="#">Edit Mail Message</a>
<b>Enhanced User Authentication</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

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

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

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

**Friendly Logout:** When a user logs into the network with wireless connection, 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.

- **Internet Connection Detection:** Enter a specific URL or IP address and IAS-2000 will try to detect the network connection by sending packets directly to that specific URL or IP address. If there is a problem in the connection of the WAN port of the system such that the URL or IP address specified cannot be reached, there will be a connection failed message showing on the users' login screen.

**Fail Action:** Set to pass or block all the network connections when the WAN interface fails.

- **Upload File**

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

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

Click **Set To Default** and then click **restart** to use the default certificate and key.

The screenshot shows a message box with the following text: "You just overwrote the KEY & Certificate with default KEY & default Certificate file!" followed by "You should reboot IAS-2000 to activate the modification. Click to [restart](#)."

2. **Login Page:** The administrator can upload new login page. Click the **Browse** button to select the file for the login page upload. Then click **Submit** to complete the upload process.

The screenshot shows a complex form interface. At the top is the 'Upload Login Page' section with a 'File Name' input field, a 'Browse...' button, and two buttons: 'Submit' and 'Use Default Page'. Below this is a section titled 'Existing Image Files :'. Underneath, it displays 'Total Capacity: 512 K' and 'Now Used: 1 K'. The next section is 'Upload Image Files', which includes an 'Upload Images' input field, a 'Browse...' button, and a 'Submit' button. At the very bottom of the form is a 'Preview' link.

Click **Use Default Page** to use the default login page.

You just overwrite login page with default page!

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

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

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

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

```

```

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

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

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

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

3. **Logout Page:** The administrator can upload new logout page. The process is similar to that of Login Page. Click **Use Default Page** to use the default login succeed page.

Upload Logout Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/> <input type="button" value="Use Default Page"/>	
<b>Existing Image Files :</b>	
<b>Total Capacity:</b> 512 K	
<b>Now Used:</b> 1 K	
Upload Image Files	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

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

4. **Login Succeed Page:** The administrator can upload new login succeed page. The process is similar to that of Login Page. Click **Use Default Page** to use the default login succeed page.

Upload Login Succeed Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/> <input type="button" value="Use Default Page"/>	
Existing Image Files :	
<b>Total Capacity:</b> 512 K <b>Now Used:</b> 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

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

5. **Logout Succeed Page:** The administrator can upload new logout succeed page. The process is similar to that of Login Page. Click **Use Default Page** to use the default logout succeed page.

Upload Logout Succeed Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/> <input type="button" value="Use Default Page"/>	
Existing Image Files :	
<b>Total Capacity:</b> 512 K <b>Now Used:</b> 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

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

- **POP3 Message:** Before the users log into the network with their usernames and passwords, the users will receive a welcome mail from IAS-2000. The administrator can edit the content of this welcome mail.



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

MAC Address Control			
Item	MAC Address	Item	MAC Address
1	00:02:6F:20:A3:10	2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

(Total40) [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.

## 5.4 Utilities

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

Utilities	
Change Password	Change the administration password.
Backup/Restore Setting	Backup and restore system settings. Administrator may also reset system settings to factory default.
Firmware Upgrade	Upgrade to the latest system firmware.
Restart	Restart the system.

### 5.4.1 Change Password

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 Password	
Old Password	<input type="password"/>
New Password	<input type="password"/> <small>*(Max length: 10)</small>
Verify Password	<input type="password"/>

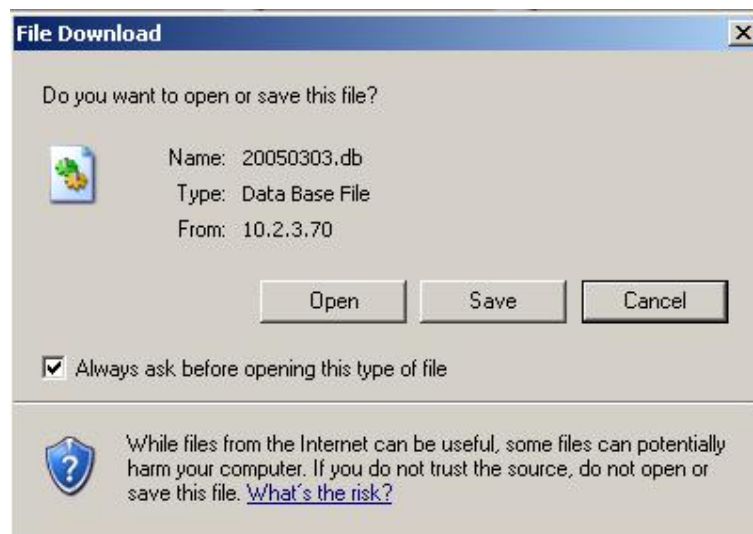
**Caution:** If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial port, console/printer port.



## 5.4.2 Backup/Restore Setting

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

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



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

**Caution:** Resetting to factory default settings will clear/restore all settings such as policies, billing plans, all user databases, and any configuration to the initial states.

### 5.4.3 Firmware Upgrade

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

Firmware Upgrade	
Current Version	2.00.B1
File Name	<input type="text"/> <input type="button" value="Browse..."/>

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

**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.

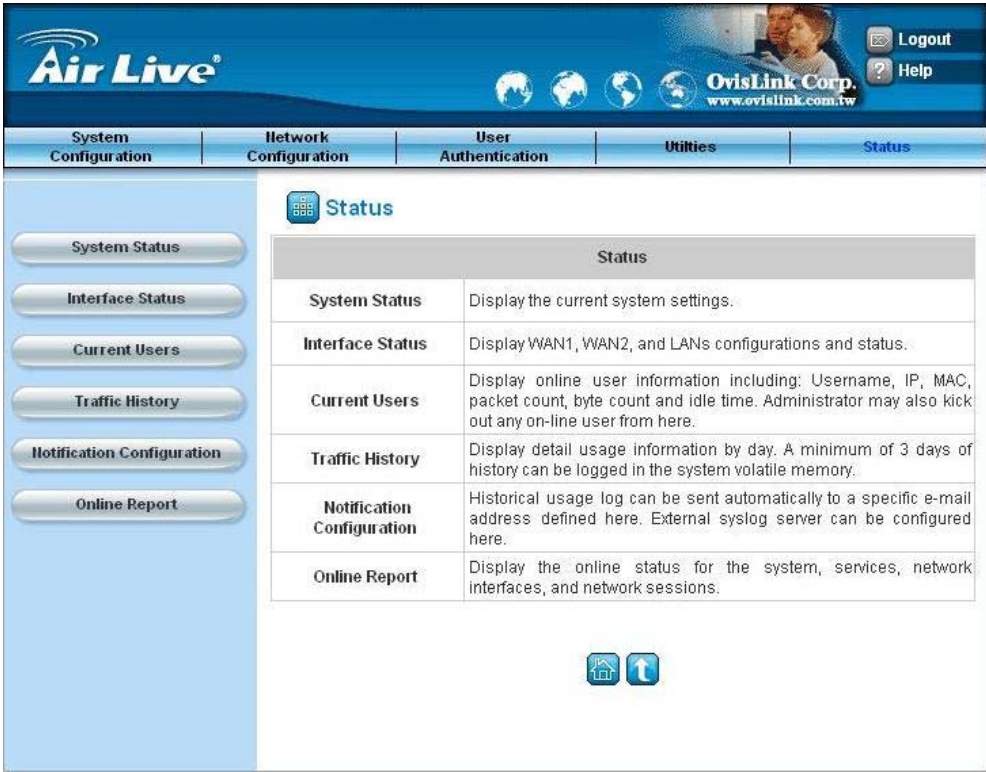
#### 5.4.4 Restart

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

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

## 5.5 Status

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



## 5.5.1 System Status

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

System Status		
<b>Current Firmware Version</b>		1.00.A1
<b>System Name</b>		OvisLink IAS-2000
<b>WAN Failure Message</b>		Sorry! The service is temporarily unavailable.
<b>Home Page</b>		<a href="http://www.ovislink.com">http://www.ovislink.com</a>
<b>Syslog server - Traffic History</b>		N/A:N/A
<b>Proxy Server</b>		Disabled
<b>Friendly Logout</b>		Disabled
<b>Management</b>	<b>Remote Management IP</b>	0.0.0.0/0.0.0.0
	<b>SNMP</b>	Enabled
<b>History</b>	<b>Retainable Days</b>	3 Day(s)
	<b>Traffic log Email To</b>	N/A
<b>Time</b>	<b>NTP Server</b>	tock.usno.navy.mil
	<b>Date Time</b>	2005/12/01 16:02:39 +0800
<b>User</b>	<b>Idle Timer</b>	10 Min(s)
	<b>Multiple Login</b>	Disabled
	<b>Guest Account</b>	Disabled
<b>DNS</b>	<b>Preferred DNS Server</b>	61.64.127.1
	<b>Alternate DNS Server</b>	168.95.1.1
<b>PMS</b>	<b>Server Status</b>	Disable
	<b>IP:Port</b>	N/A:9877

The description of the table is as follows:

<b><u>Item</u></b>		<b><u>Description</u></b>
<b>Current Firmware Version</b>		The present firmware version of IAS-2000
<b>System Name</b>		The system name. The default is IAS-2000
<b>WAN Failure Message</b>		The information to be shown on the login screen when a user has a connection problem.
<b>Home Page</b>		The page the users are directed to after initial login success.
<b>Syslog server- Traffic History</b>		The IP address and port number of the external Syslog Server. <b>N/A</b> means that it is not configured.
<b>Proxy Server</b>		Enabled/disabled stands for the system is currently using the proxy server or not.
<b>Friendly Logout</b>		Enabled/disabled stands for the setting of hiding/displaying an extra confirmation window when users click the logout button.
<b>Management</b>	<b>Remote Management IP</b>	The IP or IPs that is allowed for accessing the management interface.
	<b>SNMP</b>	Enabled/disabled stands for the current status of the SNMP management function.
<b>History</b>	<b>Retainable Days</b>	The maximum number of days for the system to retain the users' information.
	<b>Traffic log Email To</b>	The email address that the traffic history information will be sent to.
<b>Time</b>	<b>NTP Server</b>	The network time server that the system is set to align.
	<b>Date Time</b>	The system time is shown as the local time.
<b>User</b>	<b>Idle Timer</b>	The number of minutes allowed for the users to be inactive.
	<b>Multiple Login</b>	Enabled/disabled stands for the current setting to allow/disallow multiple logins form the same account.
	<b>Guest Account</b>	Enabled/disabled stands for the current status of allowing Guest Accounts to log in.
<b>DNS</b>	<b>Preferred DNS Server</b>	IP address of the preferred DNS Server.
	<b>Alternate DNS Server</b>	IP address of the alternate DNS Server.
<b>PMS</b>	<b>Server Status</b>	The current status of the PMS server.
	<b>IP:Port</b>	The IP and Port information of the PMS server.

## 5.5.2 Interface Status

Provides an overview of the interface for the administrator including **WAN1**, **WAN2**, **LAN1** and **LAN2**.

Interface Status		
<b>WAN 1</b>	<b>MAC Address</b>	00:90:0B:04:1D:07
	<b>IP Address</b>	10.2.3.103
	<b>Subnet Mask</b>	255.255.255.0
<b>LAN 1</b>	<b>Mode</b>	NAT
	<b>MAC Address</b>	00:90:0B:04:1D:05
	<b>IP Address</b>	192.168.1.254
	<b>Subnet Mask</b>	255.255.255.0
	<b>Preferred DNS Server</b>	168.95.1.1
	<b>Alternate DNS Server</b>	N/A
<b>LAN 1 DHCP Server</b>	<b>Status</b>	Enabled
	<b>WINS IP Address</b>	N/A
	<b>Start IP Address</b>	192.168.1.1
	<b>End IP Address</b>	192.168.1.100
	<b>Lease Time</b>	1440 Min(s)
<b>LAN 2</b>	<b>Mode</b>	NAT
	<b>MAC Address</b>	00:90:0B:04:1D:04
	<b>IP Address</b>	192.168.2.254
	<b>Subnet Mask</b>	255.255.255.0
	<b>Preferred DNS Server</b>	168.95.1.1
	<b>Alternate DNS Server</b>	N/A
<b>LAN 2 DHCP Server</b>	<b>Status</b>	Enabled
	<b>WINS IP Address</b>	N/A
	<b>Start IP Address</b>	192.168.2.1
	<b>End IP Address</b>	192.168.2.100
	<b>Lease Time</b>	1440 Min(s)

The description of the table is as follows:


<u>Item</u>		<u>Description</u>
<b>WAN1</b>	<b>MAC Address</b>	The MAC address of the WAN1 port.
	<b>IP Address</b>	The IP address of the WAN1 port.
	<b>Subnet Mask</b>	The Subnet Mask of the WAN1 port.
<b>WAN2</b>	<b>MAC Address</b>	The MAC address of the WAN2 port.
	<b>IP Address</b>	The IP address of the WAN2 port.
	<b>Subnet Mask</b>	The Subnet Mask of the WAN2 port.
<b>LAN1</b>	<b>Mode</b>	The mode of the LAN1 port.
	<b>MAC Address</b>	The MAC address of the LAN1.
	<b>IP Address</b>	The IP address of the LAN1.
	<b>Subnet Mask</b>	The Subnet Mask of the LAN1.
	<b>Preferred DNS Server</b>	The primary DNS server of the LAN1.
	<b>Alternate DNS Server</b>	The secondary DNS server of the LAN1.
<b>LAN1 DHCP Server</b>	<b>Status</b>	Enable/disable stands for status of the DHCP server on the LAN1.
	<b>WINS IP Address</b>	The WINS server IP on DHCP server. <b>N/A</b> means that it is not configured.
	<b>Start IP Address</b>	The start IP address of the DHCP IP range.
	<b>End IP Address</b>	The end IP address of the DHCP IP range.
	<b>Lease Time</b>	Minutes of the lease time of the IP address.
<b>LAN2</b>	<b>Mode</b>	The mode of the LAN2.
	<b>MAC Address</b>	The MAC address of the LAN2.
	<b>IP Address</b>	The IP address of the LAN2.
	<b>Subnet Mask</b>	The Subnet Mask of the LAN2.
	<b>Preferred DNS Server</b>	The primary DNS server of the LAN2.
	<b>Alternate DNS Server</b>	The secondary DNS server of the LAN2.
<b>LAN2 DHCP Server</b>	<b>Status</b>	Enable/disable stands for status of the DHCP server on the LAN2.
	<b>WINS IP Address</b>	The WINS server IP on DHCP server. <b>N/A</b> means that it is not configured.
	<b>Start IP Address</b>	The start IP address of the DHCP IP range.
	<b>End IP Address</b>	The end IP address of the DHCP IP range.
	<b>Lease Time</b>	Minutes of the lease time of the IP address.



### 5.5.3 Current Users

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

Current Users List						
Item	Username		Pkts In	Bytes In	Idle	Logout
	IP	MAC	Pkts Out	Bytes Out		
1		guest4	12	1008	454	<a href="#">Logout</a>
	192.168.1.107	00:D0:C9:60:01:04	12	1008		
2		guest5	15	1260	454	<a href="#">Logout</a>
	192.168.1.100	00:D0:C9:60:01:05	15	1260		
3		guest6	25	2100	64	<a href="#">Logout</a>
	192.168.1.131	00:D0:C9:60:01:06	25	2100		
4		guest7	25	2100	64	<a href="#">Logout</a>
	192.168.1.165	00:D0:C9:60:01:07	25	2100		
5		guest8	20	1680	395	<a href="#">Logout</a>
	192.168.1.200	00:D0:C9:60:01:08	20	1680		
6		guest9	17	1428	395	<a href="#">Logout</a>
	192.168.1.9	00:D0:C9:60:01:09	17	1428		
7		guest10	15	1260	425	<a href="#">Logout</a>
	192.168.1.147	00:D0:C9:60:01:0A	15	1260		
8		guest11	651	124826	0	<a href="#">Logout</a>
	192.168.3.6	00:04:23:62:0A:0C	649	48284		

 Refresh

## 5.5.4 Traffic History

This function is used to check the history of IAS-2000. The history of each day will be saved separately in the DRAM for at least 3 days.

Traffic History			
Date	Items	Download	Delete
<a href="#">2005-08-25</a>	24	<a href="#">Download</a>	<a href="#">Delete</a>

Interface Performance			
Date	Items	Download	Delete
<a href="#">2005-08-26</a>	840	<a href="#">Download</a>	<a href="#">Delete</a>
<a href="#">2005-08-25</a>	564	<a href="#">Download</a>	<a href="#">Delete</a>

Internal Service			
Date	Items	Download	Delete
<a href="#">2005-08-26</a>	1400	<a href="#">Download</a>	<a href="#">Delete</a>
<a href="#">2005-08-25</a>	940	<a href="#">Download</a>	<a href="#">Delete</a>

System Performance			
Date	Items	Download	Delete
<a href="#">2005-08-26</a>	140	<a href="#">Download</a>	<a href="#">Delete</a>
<a href="#">2005-08-25</a>	94	<a href="#">Download</a>	<a href="#">Delete</a>

On-demand User Log			
Date	Items	Download	Delete
<a href="#">2005-08-23</a>	1	<a href="#">Download</a>	<a href="#">Delete</a>

PMS User Log			
Date	Items	Download	Delete
<a href="#">2005-08-23</a>	1	<a href="#">Download</a>	<a href="#">Delete</a>

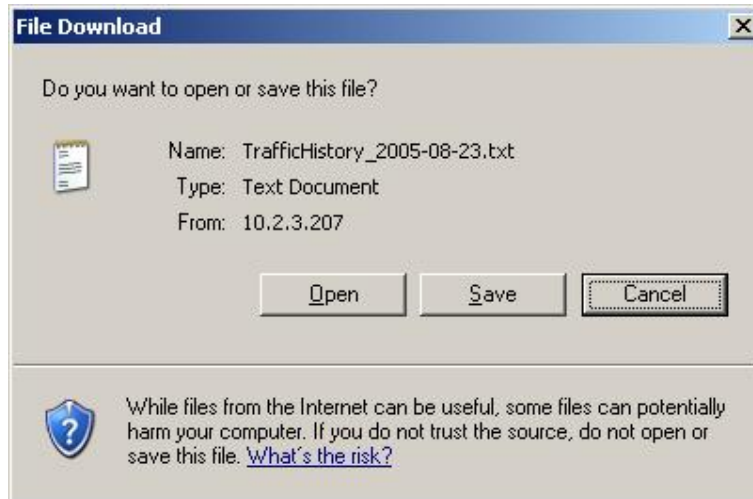
Roaming Out Traffic History			
Date	Items	Download	Delete

Roaming In Traffic History			
Date	Items	Download	Delete

**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.

Click **Download**, you can save every history log in a text file.



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	

- **Interface Performance**

As shown in the following figure, the history record consists of 5 fields, **Interface**, **Speed-IN (bps)**, **Speed-OUT (bps)**, **Packet-IN (pps)** and **Packet-OUT (pps)** for WAN and LAN status.

Interface Performance (2005-09-20)				
Interface	Speed-IN (bps)	Speed-OUT (bps)	Packet-IN (pps)	Packet-OUT (pps)
<b>--14:25--</b>				
WAN2	0.00	0.00	0.00	0.00
WAN1	3.375000 K	1.145830 K	4.67	1.33
LAN2	0.00 K	0.00 K	0.00	0.00
LAN1	0.00 K	0.00 K	0.00	0.00
<b>--14:20--</b>				
WAN2	0.00 K	0.00 K	0.00	0.00
WAN1	0.770830 K	1.145830 K	1.33	1.33
LAN2	0.00 K	0.00 K	0.00	0.00
LAN1	0.00 K	0.00 K	0.00	0.00
<b>--14:15--</b>				
WAN2	0.00 K	0.00 K	0.00	0.00
WAN1	0.927080 K	1.145830 K	1.67	1.33

- **Internal Service**

As shown in the following figure, the history record consists of 6 fields, **DHCP Server**, **Syslog Server**, **SNMP Server**, **HTTP Server**, **Agent**, **SSH Server**, **EMS Server**, **RADIUS Server**, **Proxy Server** and **Redirector Server** for network service status.

Internal Service Status (2005-09-12)	
Service	Status
<b>--16:55--</b>	
DHCP	Running
Syslog	Stop
SNMP	Stop
HTTP	Running
Agent	Running
SSH	Running
RADIUS	Stop
PROXY	Running
Redirector	Running

- **System Performance**

As shown in the following figure, the history record consists of 5 fields, **CPU Usage %**, **Memory Usage %**, **Total Memory (KB)**, **Memory Used (KB)** and **Memory Free (KB)** of IAS-2000 status.

System Performance (2005-08-23)				
CPU Usage %	Memory Usage %	Total Memory (KB)	Memory Used (KB)	Memory Free (KB)
<b>--17:30--</b>				
100	86.16	1034084	891044	143040
<b>--17:25--</b>				
100	87.06	1034084	900372	133712
<b>--17:20--</b>				
100	86.18	1034084	891252	142832
<b>--17:10--</b>				
100	85.23	1034084	881380	152704
<b>--16:40--</b>				
100	84.18	1034084	870580	163504

- **On-demand User Log**

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

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

- **PMS User Log**

As shown in the following figure, each line is a on-demand user log record consisting of 14 fields, **Date**, **Posting Number**, **Type**, **Name**, **Room ID**, **IP**, **MAC**, **Packets In**, **Packets Out**, **Bytes In**, **Bytes Out**, **Expiretime**, **Validation** and **Remark**, of user activities.

PMSUserLogName 2005-08-23													
date	postingNum	type	name	roomID	ip	mac	packetsIn	packetsOut	bytesIn	bytesOut	expiretime	validtime	remark
2005-08-23 10:50:15 +0800	2724	Create_PMS_User	T744	1234	0.0.0.0	00:00:00:00:00:00	0	0	0	0	0	999 hr.	3596400

- **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

## 5.5.5 Notification Configuration

IAS-2000 will save the traffic history into the internal DRAM. If the administrator wants the system to automatically send out the history to a particular email address, please enter the related information in these fields.

Notification Configuration		
History Email	Send From	<input type="text"/>
	Send To	<input type="text"/>
	Interval	1 Hour <input type="button" value="v"/>
	SMTP Server	<input type="text"/>
	Authentication Method	NTLMv1 <input type="button" value="v"/>
	Account Name	<input type="text"/>
	Password	<input type="text"/>
	Domain	<input type="text"/>
Syslog To	IP: <input type="text"/>	Port: <input type="text"/>

- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Send To:** The e-mail address of the person whom the history email is for. This will be the receiver's e-mail.
- **Interval:** The time interval to send the e-mail report.
- **SMTP Server:** The IP address of the SMTP server.
- **Authentication Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or "**None**" to use none of the above. Depending on which authentication method you select, you have to enter the **Account Name**, **Password** and **Domain**.

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

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

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

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

- **Syslog To:** It specifies the IP and Port of the Syslog server.

## 5.5.6 Online Report

This function provides real time on-line report of the IAS-2000 system including **System Status**, **Service Status**, **Network Interface Status** and **Network Session Status**.

Online Report
<a href="#">System Status</a>
<a href="#">Service Status</a>
<a href="#">Network Interface Status</a>
<a href="#">Network Session Status</a>

- **System Status**

As shown in the following figure, the online report consists of 5 fields, **CPU Usage**, **Memory Usage**, **Total Memory**, **Memory Used** and **Memory Free** of IAS-2000 status.

System Performance				
CPU Usage %	Memory Usage %	Total Memory (KB)	Memory Used (KB)	Memory Free (KB)
48	67.88	1034084	701980	332104

- **Service Status**

As shown in the following figure, the online report consists of 6 fields, **DHCP Server**, **Syslog Server**, **SNMP Server**, **HTTP Server**, **Agent**, **SSH Server**, **RADIUS Server**, **Proxy Server** and **Redirector Server** for network service status.

Internal Service Status	
Service	Status
DHCP	Running
Syslog	Stop
SNMP	Stop
HTTP	Running
Agent	Running
SSH	Running
RADIUS	Stop
PROXY	Running
Redirector	Running

- **Network Interface Status**

As shown in the following figure, the online report consists of 5 fields, **Interface**, **Speed-IN (bps)**, **Speed-OUT (bps)**, **Packet-IN (pps)** and **Packet-OUT (pps)** for WAN and LAN status.

Interface Performance					
Interface	Speed-IN (bps)	Speed-OUT (bps)	Packet-IN (pps)	Packet-OUT (pps)	Status
WAN1	1.402344 K	3.470703 K	2.75	1.25	UP
WAN2	0.00	0.00	0.00	0.00	DOWN
LAN1	0.00	0.00	0.00	0.00	UP
LAN2	0.00	0.00	0.00	0.00	UP

- **Network Session Status**

As shown in the following figure, the online report consists of 3 fields, **IP**, **TCP session count** and **UDP session count**. This report tells how many connections each IP address uses now.

Session Information		
IP	TCP session count	UDP session count
10.2.3.7	0	1
10.2.3.84	2	0
10.2.3.207	2	2
10.2.3.203	0	1
10.2.3.123	0	2
10.2.3.1	0	2
10.2.3.169	0	1
10.2.3.45	2	0
10.2.3.135	0	2
10.2.3.111	0	2



## 5.6 Help

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

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



## Appendix A External Network Access

If all the steps are set properly, IAS-2000 can be further connected to the managed network to experience the controlled network access environment. Firstly, connect an end-user device to the network at IAS-2000's LAN1/LAN2 and set to obtain an IP address automatically. After the network address is obtained at the user end, open an Internet browser and link to any website. Then, the default logon webpage will appear in the Internet browser.

1. First, connect a user-end device to LAN3/LAN4 port of IAS-2000, and set the dynamical access network. After the user end obtains the network address, please open an Internet browser and the default login webpage will appear on the Internet browser.

Key in the username and password created in the local user account or the on-demand user account in the interface and then click **Submit** button. Here, we key in the local user account (e.g. **test@Local** for the username and **test** for the password) to connect the network.



2. Login page appearing means IAS-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 that you have clicked the wrong button, the **“Remaining”** button. This button is only for on-demand users and if you are not an on-demand user, please just click the **Submit** button.



- 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.

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

- 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 rest of use time that the on-demand user can surf Internet.
- **Redeem:** When the remaining time or data size is insufficient, the user has to pay for adding credit at the counter, and then, the user will get a new username and password. After clicking the **Redeem** button, you will see the following screen. Please enter the new username and password you got and click **Redeem** button to merge the two accounts and add up the available use time and data size by the system, and then, you will see the total available use time and data size after adding credit.

The screenshot shows a "Login Successfully" screen. It features a red sphere icon and a key icon. A message box says "Hello, 9AC7@ovislink". Below that, it says "Please close this window or click this button to" followed by a "Logout" button. Then it says "Thank you!!" and "Remaining Usage:" in red. Below that, there are input fields for "3" Hour, "36" Min, and "29" Sec. At the bottom, it says "Login time: 2005-8-24 14:18:7" and a "Redeem" button.

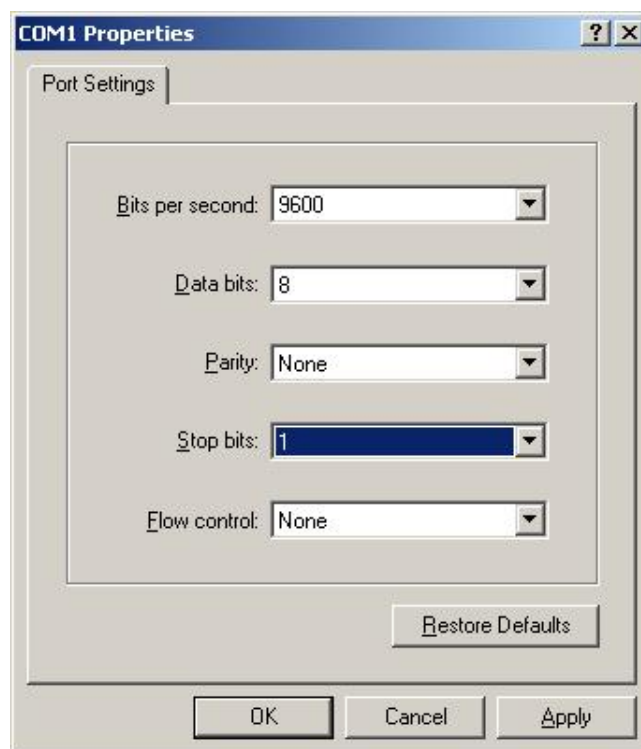
This screenshot is identical to the one above, showing the "Redeem Page" login form with "User Name" and "Password" fields and "ENTER" and "Clear" buttons.

**Caution:** The maximum session time/data transfer is 24305 days/2003 Mbyte. If the redeem amount exceeds this number, the system will automatically reject the redeem process.

## Appendix B Console Interface Configuration

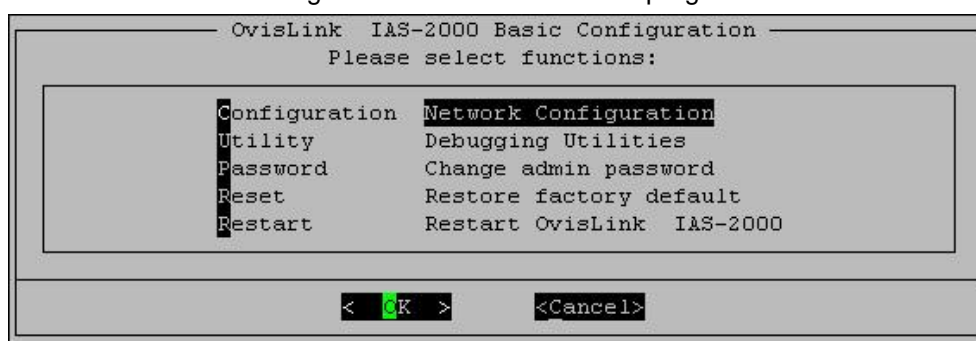
Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. To connect the console port of IAS-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**.



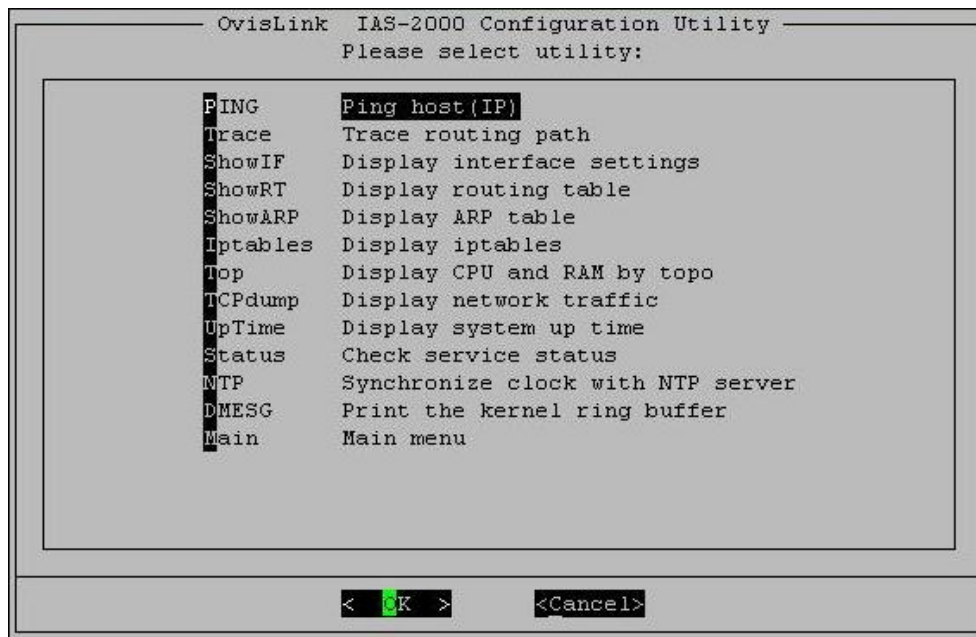
**Caution:** the main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the **Enter** key to make selection or confirm what you enter.

3. Once the console port of IAS-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, and the welcome screen or the main menu will 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 debugging. The utilities are described as following:



- 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 live 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 IAS-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.

- **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 that administrator's password to access the console management interface. But connecting the system by SSH, we have to enter the username and password.

## *Appendix B. Console Interface Configuration*

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 IAS-2000 Admin username and password after logging into the system for the first time.*

- **Reload factory default**  
Choose this option to reset the system configuration to the factory default settings.
- **Restart IAS-2000**  
Choose this option to restart IAS-2000.

# Appendix C Specifications

## 1. Hardware Specification

- Dimensions: 42.5cm(W) x 4.4cm(H) x 24cm(D)
- Weight: 4.2kg
- Power: 110-240 VAC 50/60Hz
- Operating Temperature: 5-45°C
- 19" 1U Rack Mount Design
- 4 Fast Ethernet RJ 45 Connectors
- 2 RS-232 Serial Ports
- Supports 10/100Mbps Full / Half Duplex Transfer Speed

## 2. Technical Specification

- **Standards**  
This system supports IEEE 802.1x, 802.11b and 802.11g
- **Networking**  
WAN interface supports Static IP, DHCP client, and PPPoE client  
Interface supports static IP  
Supports NAT mode and router mode  
Built-in DHCP server  
Built-in NTP client  
Supports Redirect of network data  
Supports IPSec (ESP), PPTP and H.323 pass through (under NAT)  
Customizable static routing table  
Supports Virtual Server  
Supports DMZ Server  
Supports machine operation status monitoring and reporting system  
Supports roaming across networks
- **Firewall**  
Provides Several DoS protection mechanisms  
Customizable packet filtering rules

Customizable walled garden (free surfing area)

- **User Management**

Supports at least 500 on-line users concurrently

Supports Local, POP3 (+SSL), RADIUS, and LDAP LAN1/LAN2 mechanisms

Supports LAN1& LAN2 mechanisms simultaneously

Can choose MAC address locking for built-in user database

Can set the time for the user to log in to the system

Can set the user's idle time

Can specify the MAC addresses to enter the managed network without authentication

Can specify the IP addresses to enter the managed network without authentication

Supports the setting to pass or block all the connections when the WAN interface failed

Supports web-based login

Supports several friendly logout methods

Supports RADIUS accounting protocol to generate the billing record on RADIUS server

- **Administration**

Provides online status monitoring and history traffic

Supports SSL encrypted web administration interface and user login interface

Customizable user login & logout web interface

Customizable redirect after users are successfully authenticated during login & logout

Supports Console management interface

Supports SSH remote administration interface

Supports web-based administration interface

Supports SNMP v2

Supports user's bandwidth restriction

Supports remote firmware upgrade

- **Accounting**

Supports built-in user database and RADIUS accounting

P/N: V10020051202