NetComm™

IAC4000

Internet Access Controller

- Integrated Solution for rapid deployment
- Deliver instant PnP connectivity service
- Complete user authentication and accounting
- Sophisticated Remote Management
- Comprehensive security
- Enhance Local and Personalized Service
- Hotel PMS System Support
- Built-in AAA/Billing System

USER GUIDE

Contents

1. Introduction 4
   - 1-1 Package Contents 5
   - 1-2 Features 6
   - 1-3 Specification 7
   - 1-4 Precautions 9
   - 1-5 Overview 10
     - 1-5-1 Front Panel 10
     - 1-5-2 Rear Panel 11
2. Installation 12
   - 2-1 Installation Requirements 13
     - System Requirements 13
     - ISP Requirements 13
     - Dynamic IP 13
     - Fixed IP 13
     - PPPoE 13
     - PPTP 13
     - Your PC Requirements 14
     - The Dynamic IP settings for the PC 14
   - 2-2 Getting Start 14
3. Configuring the IAC4000 15
   - 3-1 Console Configuration 16
     - 3-1-1 Login 16
     - 3-1-2 Main Menu 17
     - 3-1-2-1 System Configuration 18
     - 3-1-2-2 WAN Configuration 19
     - 3-1-2-3 LAN Configuration 20
     - 3-1-2-4 System Status 22
     - 3-1-2-5 Utilities Menu 23
     - 3-1-2-6 Restart System 25
     - 3-1-2-7 Logout 26
     - 3-1-2-8 Factory Defaults 26
   - 3-2 Web Configuration 26
     - 3-2-1 Configuration Menu 27
     - 3-2-2 System Setting 28
     - 3-2-2-1 System 29
     - 3-2-2-2 WAN/LAN 33
     - 3-2-2-3 Server 40
     - 3-2-2-4 Authentication 43
     - 3-2-2-5 Billing 55
     - 3-2-2-6 Accounting 61
     - 3-2-2-7 Port-Location Mapping 74
     - 3-2-3 Advanced Setting 80
     - 3-2-3-1 Customization 82
     - 3-2-3-2 Bandwidth 90

3-2-3-3 Portal Page 92
3-2-3-4 Advertisement 93
3-2-3-5 Walled Garden 94
3-2-3-6 Passthrough 95
3-2-3-7 LAN Devices 99
3-2-3-8 Static Route 100
3-2-3-9 Logs 101
3-2-3-10 SNMP 106
3-2-4 System Status 108
3-2-4-1 System Status 109
3-2-4-2 Current User List 109
3-2-4-3 DHCP Clients 111
3-2-4-4 Session List 112
3-2-4-5 LAN Devices Status 112
3-2-4-6 Billing Log 113
3-2-4-7 PMS Transaction Log 114
3-2-4-8 Static Route Table 115
3-2-5 System Tools 115
3-2-5-1 Configuration 118
3-2-5-2 Firmware Upgrade 119
3-2-5-3 System Account 121
3-2-5-4 SSL Certificate 125
3-2-5-5 Restart 125
3-2-5-6 Logout 126
Appendix A. DHCP Private/Public IP Pool Setup 126
Use Public IP (Billing Profile'Service Type=Public Service) 128
Use Private IP (Billing Profile'Service Type=Private Service) 130
Appendix B. Use RADIUS server to setup your Internet Service 130
Accumulate 131
Case 1: RADIUS Server will reply "Session time-out" attribute 131
Case 2: RADIUS Server do not reply "Session timeout" attribute 132
Time to Finish 133
Appendix C. Ethernet Cable Connections 134
RJ-45 Ethernet Network Ports 134
Appendix D. Registering your NetComm Product 136
Contact Information 136
Legal & Regulatory Information 137
Customer Information 137
Product Warranty 138
Limitations of Warranty 138

1. Introduction

The IAC4000 - Internet Access Controller is a freestanding or rack-mounted intelligent gateway integrated with a four-port port-based V-LAN switch and two serial ports for system management and PMS. It provides plug and play instant Internet access with advanced security & network management. The IAC4000 - Internet Access Controller is designed for service providers and system integrators to enhance their service performance.

The IAC4000 - Internet Access Controller is an ideal solution for hotels, coffee shops, airports, conference facilities and other sites that commonly host business travelers, and offers instant high-speed Internet connections without requiring user configuration to connect to the facility's network and No Extra MIS resource needed.

The IAC4000 - Internet Access Controller helps solve connectivity problems by offering instant Internet access with no settings to change; Users simply plug into the network and they are immediately connected.

With its PMS interface, the IAC4000 - Internet Access Controller can be easily integrated with a service provider's billing system to help them to provide an Internet access service. And the built-in AAA (Authentication / Accounting / Authorization) and Billing mechanism provides the hotspot operator a complete AAA solution.

Figure 1-1 IAC4000 - Internet Access Controller

1-1 Package Contents

Please inspect your package. The following items should be included:

- IAC4000 - Internet Access Controller

- 240 Volt IEC Power Cord

- CD including this user guide

- 9 pin to 9 pin serial cable.

- 19" Rack mount kit.

- 9 pin to 25 pin serial adaptor. Black moulded type.

- 4 x Self adhesive rubber foots.

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

1-2 Features

Integrated Solution for rapid deployment

The IAC4000 - Internet Access Controller is a complete access controller for medium to large hotspots. It can serve up to 1024 simultaneous users and it is an ideal hotspot solution to be deployed in the hotels, coffee shops, airports and other sites that commonly host business travelers and offer instant high-speed Internet connections.

Deliver instant PnP connectivity service

With its IP Plug and Play technology, the IAC4000 - Internet Access Controller helps solve connectivity problems by offering instant Internet access without the need for configuration changes to the client computer or any resident client-side software and allows guests to send E-mail as usual without changing E-mail SMTP server settings even if their configured mail server is unavailable or behind a corporate firewall.

Complete user authentication and accounting

The IAC4000 - Internet Access Controller works with industry-standard RADIUS server that is allowed administer to control user's login name and password to fully support AAA (Authentication, Accounting and Authorization).

Sophisticated Remote Management

The IAC4000 - Internet Access Controller enables you to manage all your underlying network devices with Syslog messaging, SNMP and LAN devices Management to reduce maintenance overhead.

Comprehensive security

The IAC4000 - Internet Access Controller provides a fully-secure operating environment with VPN pass through, SSL certificate, 802.1x and Layer 2 Isolation V-LAN Security.

Enhance Local and Personalized Service

The login and logout pages are fully customizable. The IAC4000 - Internet Access Controller has the ability to let you redirect end users to your advertising web pages, increase your potential for revenue and customize locations where end-users can visit free (walled garden).

Hotel PMS System Support

The IAC4000 - Internet Access Controller works with hotel Micros Fidelio, Marriott, Spectrum MK II PMS billing system that is allowed hotel to fully support PMS billing system of Internet Access.

Built-in AAA/Billing System

The IAC4000 - Internet Access Controller has built-in AAA and billing system that is allowed manager to control user for Internet access and billing mechanism individually without any external AAA server and billing server.

1-3 Specification

Networking

- IEEE802.3 10BaseT Ethernet
- IEEE802.3u 100BaseTX Fast Ethernet
- Supports 1024 Simultaneous Users
- Supports all operation systems with TCP/IP support
- IP Plug and Play (iPnP) without any IP setting change
- Various WAN connections (Static IP/DHCP Client/PPPoE/PPTP)
- HTTP Proxy Support without any proxy-port setting change
- SMTP Server Redirection
- DHCP Server / Relay
- IP Multicast support
- DNS Redirection
- NAT (RFC 1631)
- NTP Server Support

AAA

- RADIUS AAA Authentication/ Accounting
- Secondary RADIUS Server
- Built-in Authentication/Accounting
- Static/ Dynamic Accounting
- Bandwidth Management (Equal bandwidth/ Class of Service)

Billing

- Flexible Billing Plan
- Time-based Billing (by minute, hour, day, week, etc.)
- Subscriber Selective Service
- Port-Location Mapping

Security

- Port-based V-LAN
- Layer 2 Isolation
- SSL Secure User Login Process
- SSL Secure Web-based administration
- VPN Pass through (IPSec/PPTP)
- Authorized Remote Management

Management

- Web-based Management
- HTTP/TFTP Firmware Upgrade

- Backup/Restore Configuration
- Scheduled Firmware Upgrade
- Real-time Status List
- LAN Device Management
- Syslog
- SNMP v1/v2 (MIB II with traps)

Local Service

- Advertisement URL link
- Walled Garden (Free web sites)
- Login Page Redirection
- Customize Login Page
- Passthrough IP/MAC/URL

PMS Billing System

- Support Micros Fidelio
- PMS Transaction Logs
- Support 802.1Q Tag-based VLAN infrastructure
- Support Low-cost infrastructure

Interface

- One WAN Port (IEEE 802.3/802.3u 10BaseT/100BaseTX) support Auto crossover
- Four LAN Ports (IEEE 802.3/802.3u 10BaseT/100BaseTX) support Auto crossover
- DB9 Serial Port: Console setting or exclusive Account Generator Printer
- PMS DB9 Serial Port: PMS application
- One Reset Button: for factory setting

LED Indicators

- LINK/ACT, 10/100, Full Duplex, Power, Alarm

Compliance

- FCC part 15 Class A
- CE
- VCCI Class A
- UL

Power Requirement

- Internal universal switching power supply
- 100-240 VAC, 50/60 Hz
- Power Consumption: 10W

Dimension

- Size: 1U Rack-mount-sized 440 (W) x 116(L) x 44 (H) mm
- Weight: About 1.7 kg (Net)

Environment Conditions

- Operating Temperature: 0 to 50°C
- Storage Temperature: -10 to 65°C
- Humidity: 10% to 95% non-condensing

1-4 Precautions

- Never remove or open the cover. You may suffer serious injury if you touch these parts.
- Never install the system in the wet locations.
- Use only the original fitting power cord otherwise there is a danger of severe electrical shock.
- Avoid exposing the IAC4000 to direct sunlight or another heat source.

  Choose a well-ventilated area to position your IAC4000.

1-5 Overview

1-5-1 Front Panel

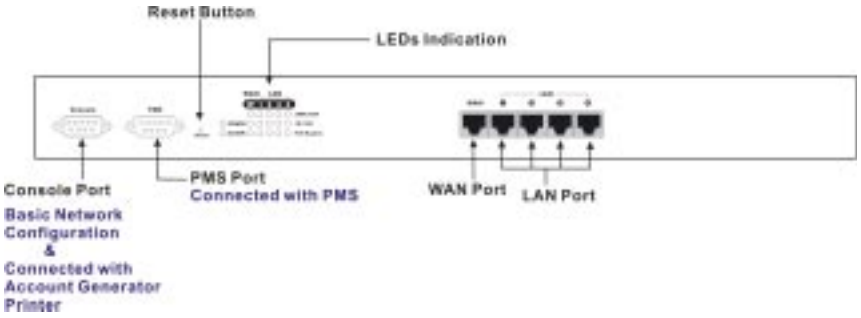


Figure 1-2 IAC4000 Front Panel

Console Port:	To configure the system, connect an RS232 serial cable to a COM port on a PC and to the Console Port of the device.
PMS Port:	Standard RS232 DB 9 female Connector. It's a data transmission cable of PMS system.
Reset Button:	The IAC4000 has a reset button at the front panel. For some circumstances you might need to reset the IAC4000.
WAN Port:	One Ethernet port used for linking xDSL or Cable Modem.
LAN Port:	The front panel supports four auto-sensing RJ-45 ports and all ports can be auto-switched to MDI-II connections. The LAN ports used for linking hosts or other network devices. The individual port can be either connected to 100BaseTX networks or 10BaseT networks. When connecting to a 100BaseTX network, the ports operate at 100Mbps in half-duplex mode or 200Mbps in full-duplex mode. When connecting to a 10BaseT network, the ports operate at 10Mbps in half-duplex mode or 20Mbps in full-duplex mode.

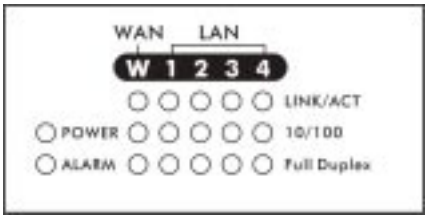


Figure 1-3 LEDs

LED	State	Description
Power	Off	The IAC4000 is not receiving electrical power.
	Green	The IAC4000 is receiving electrical power.
ALARM	Off	The IAC4000 is operating normally.
	Red	The IAC4000 has just been started up.
WAN		
LINK/ACT	Green	The WAN port is connecting with a device.
	Green (Blinking)	The WAN port is receiving or transmitting data.
	Off	No device is attached.
10/100M	Off	The WAN port is operating at 10Mbps or no device is attached.
	Green	The WAN port is operating at 100Mbps.
Full Duplex	Green	The WAN port is operating in full-duplex mode.
	Off	The WAN port is operating in half-duplex mode.
LAN (1-4)		
LINK/ACT	Green	The LAN port is connecting with a device.
	Green (Blinking)	The LAN port is receiving or transmitting data.
	Off	No device is attached.
10/100M	Off	The LAN port is operating at 10Mbps or no device is attached.
	Green	The LAN port is operating at 100Mbps.
Full Duplex	Green	The LAN port is operating in full-duplex mode.
	Off	The LAN port is operating in half-duplex mode.

1-5-2 Rear Panel

The rear panel of the IAC4000 is shown below.

Figure 1-4 IAC4000 Rear Panel

AC Power Connector: This is a three-prong connector that mates with the device end of the power cord. Plug the female end of the supplied power cord into this connector and the male end into an AC power outlet. Supported input voltages range from 100 to 240 VAC at 50 or 60 Hz.

2. Installation

The following are instructions for setting up the IAC4000. Refer to the illustration and follow the simple steps below to quickly install your IAC4000.

2-1 Installation Requirements

Before installing the IAC4000, make sure your network meets the following requirements.

System Requirements

The IAC4000 requires one of the following types of software:

- Windows 98 Second Edition/NT/2000/XP
- Red Hat Linux 7.3 or later version
- MAC OS X 10.2.4 or later version
- Any TCP/IP-enabled systems like Mac OS and UNIX (TCP/IP protocol installed)
- Standard phone line for xDSL modem

  Or

- Coaxial cable for Cable modem
- Web Browser Software (Microsoft I.E 5.0 or later version or Netscape Navigator 5.0 or later version)
- One computer with an installed 10Mbps, 100Mbps or 10/100Mbps Ethernet card
- UTP network Cable with a RJ-45 connection (Package contents)

Note: Prepare twisted-pair cables with RJ-45 plugs. Use Cat.5 cable for all connections. Make sure each cable not exceed 328 feet (Approximately 100 meters).

ISP Requirements

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

Dynamic IP

- Dynamic IP Setting

Fixed IP

- Your fixed IP address for the IAC4000
- Your subnet mask for the IAC4000
- Your default gateway IP address
- Your DNS IP address

PPPoE

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

PPTP

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

Your PC Requirements

The Static IP settings for the PC

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

Note:

1. The IAC4000's default IP address setting is "10.59.1.1".
2. The IAC4000's default subnet mask setting is "255.0.0.0".

The Dynamic IP settings for the PC

We recommend that you leave your IP settings as automatically assigned. By default, the IAC4000 is a DHCP server, and it will give your PC the necessary IP settings.

2-2 Getting Start

1. Place the IAC4000 on a flat work surface.
2. Connect the power cord to the IAC4000 and wait for the alarm LED to stop flashing.
3. Ensure that your modem and computer are both switched on.
4. Use the supplied cable to connect the IAC4000's WAN port to the modem. Check that the Cable/xDSL Status LED lights.
5. Connect your computer to one of the 10/100 LAN ports on the IAC4000. Check that the LAN Port Status LED lights.
6. Configure the further parameters via a web browser.

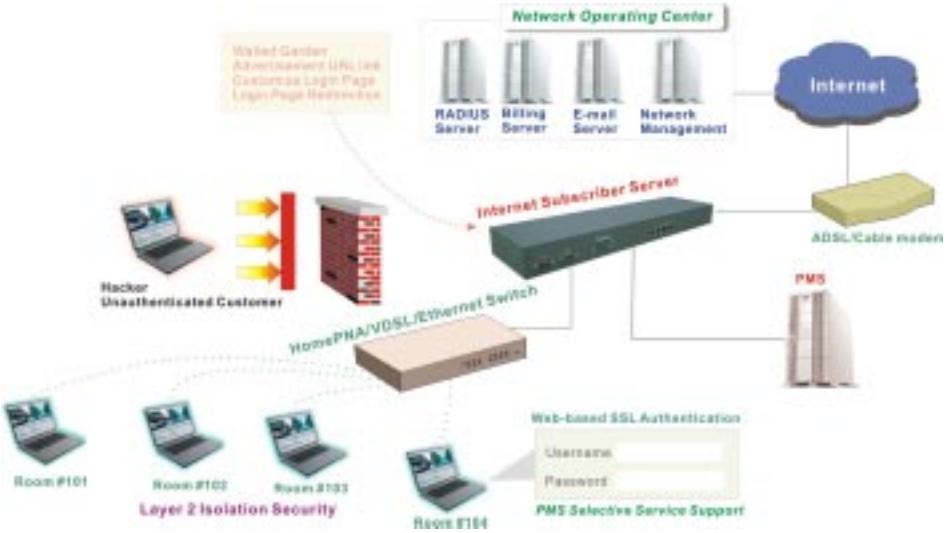


Figure 2-1 Connecting the IAC4000

3. Configuring the IAC4000

The IAC4000 offer friendly user interface, one is console user interface and other is Web user interface. However, the Console UI provides only basic system configuration and Status. For advanced function, please use the Web Configuration.

3-1 Console Configuration

To access the IAC4000 User Interface, the administrator needs to connect a VT100 terminal and a PC running a VT100 compatible terminal emulation program to the IAC4000 Console port by using the provided DB9 RS-232 cable.

Follow these steps to set up your first local serial console port session using the Window98/2K Terminal emulation program HyperTerminal.

1. From the Windows screen, click on the Start button.
2. From the Start menu, choose "Programs" (or Open file Hypertrm.exe).
3. From the Programs menu, choose "Accessories"
4. From the Accessories menu, select the HyperTerminal folder. Click on the HyperTerminal icon.
5. From the connection Description windows, enter a name (i.e., IAC4000) and choose an icon for the connection. Click "OK".
6. When the Phone Number window opens, click on the "Cancel" button.
7. From the File menu, choose "Properties".
8. From the Properties windows, click on the "Configure" button.
9. From the COM1 Properties windows, set the following parameters:

Baud Rate:	9600
Date bits:	8
Parity Checking:	None
Stop bits:	1
Flow control:	None

10. If you intend to use this PC and serial connection in the future save this configuration by selecting "Files/Save As" and entering the name of the file for this configuration.
11. Once you have completed configuring your serial terminal, use the following steps to logon to your IAC4000. If you have not already done so, use a male-female DB-9 serial communication cable to connect the COM port on your PC to the Console port on the front of the IAC4000.
12. Go to the Call menu and select Connect.
13. If you have not completed initial power up, power up the IAC4000 now.
14. To verify that you have a correctly configured your Console port press <Enter> and the login screen will display.
15. If your serial terminal remains bland, make sure that you entered the correct settings in Step7. Also, verify that you are using the correct cable, that the cable is not damaged, and that you have good cable connections.

3-1-1 Login

Figure 3-1 Login Screen

The default Username is "admin". The default Password is "admin".

User can change password setting after accessing the IAC4000 system.

Note: The administrator can change the password via utilities item.

3-1-2 Main Menu

Figure 3-2 Main Menu Screen

1) System Configuration: Including IAC4000 system basic parameter setting.
2) WAN Configuration: Including IAC4000 system WAN parameter setting.
3) LAN Configuration: Including IAC4000 system LAN parameter setting.
4) System Status: Display IAC4000 system basic status.
5) Utilities: Including firmware upgrade and change password capability.
6) Restart: Restart the IAC4000 system.
7) Logout: Logout the IAC4000 serial session
8) Factory Defaults: Erase all setting and back to the original factory setting

Enter a numeric that you need between 1~8 and press 'Enter' to the subdirectory.

3-1-2-1 System Configuration

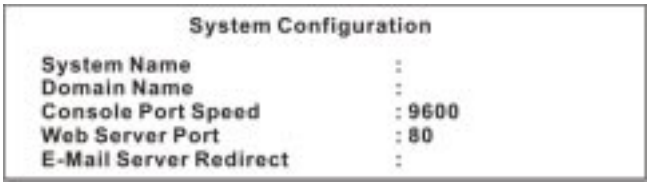


Figure 3-3 System Configuration Screen

1) System Name: You can assign a name to this unit. Up to 40 characters are allowed.
2) Domain Name: You can assign a name to this unit. Up to 80 characters are allowed.
3) Console Port Speed: The Console port speed is only relative to connection of console. There are nine different rates: 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600 or 115200.
4) Web Server Port: The Web server port default is 80, however some user may set up the IAC4000 under the NAT network. The administrator has to set the special Web server port so that IAC4000 can be remote access under NAT network.

Note: The web server port allowed range is from 8000 to 8099 if administrator wants to remote access under NAT Network. For access the IAC4000 system under NAT, please tab the "http://WAN Port IP Address: Port Number"."210.66.37.200:8001"

5) E-mail Server Redirect: To prevent some subscriber's original Email server may protect by firewall or NAT network. The IAC4000 redirects the subscribers' E-mail via specified SMTP server. The recipient of your E-mail sees the message as if you sent it from your local Internet Service Provide, not form the hotel or other place.

3-1-2-2 WAN Configuration

- DHCP Client: This allows the device to obtain the IP address and other TCP/IP settings.

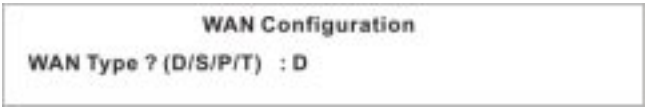


Figure 3-4 WAN Configuration Screen- DHCP (Default)

- Static IP: Enter IP address, Subnet Mask and Gateway.

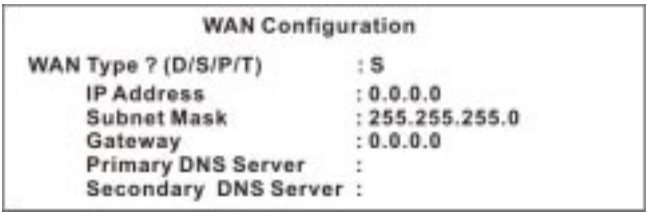


Figure 3-5 WAN Configuration Screen - Static IP

- PPPoE Client: Enter the username and password (provided by your ISP).

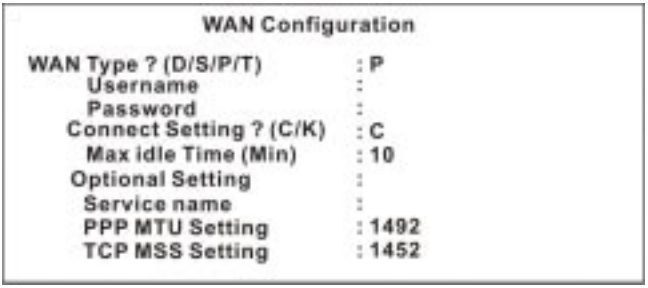


Figure 3-6 WAN Configuration Screen - PPPoE

- PPTP Client: Enter the Local IP Address, Local Subnet Mask, Gateway IP Address, Server IP Address, username and password (provided by your ISP).

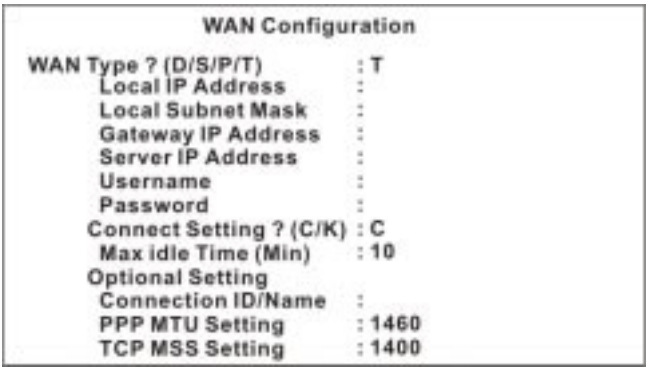


Figure 3-7 WAN Configuration Screen - PPTP

3-1-2-3 LAN Configuration

There are three types of DHCP Services. Enter 'D' to disable the DHCP server function, 'R' to enable DHCP Relay function, or 'S' to enable DHCP Server function.

- DHCP Server: IAC4000 include a DHCP sever inside. To enable this function please choose the DHCP service as 'S', and set the DHCP server information.

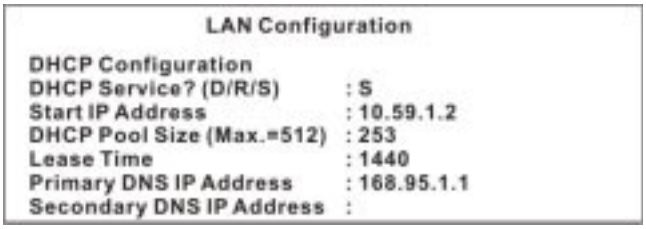


Figure 3-8 LAN Configuration Screen-DHCP Server

Start IP Address: Enter the DHCP pool start IP address.

DHCP Pool Size (Max.=512): Enter the DHCP pool size.

Lease Time: Enter the lease time for DHCP clients. The maximum of DHCP lease time is 71582788 minutes.

Primary DNS IP Address: Enter Primary DNS IP address.

Secondary DNS IP Address: Enter Secondary DNS IP address.

Note:

1. DHCP IP Pool only support up to 512 IP address

2: Subnet mask support 255.0.0.0, 255.255.0.0, 255.255.255.0

- DHCP Disable

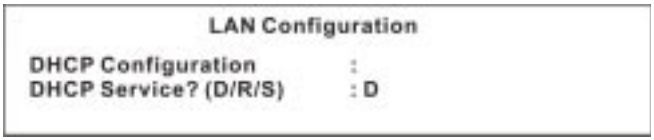


Figure 3-9 LAN Configuration Screen - DHCP Disable

- DHCP Relay: To route DHCP through an external server, the administrator needs to enable the DHCP Relay and assign a valid DHCP server IP address.

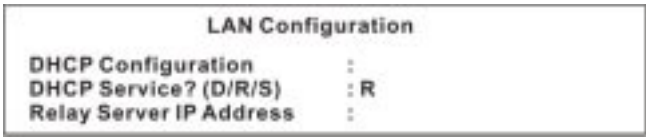


Figure 3-10 LAN Configuration Screen - DHCP Relay

Relay Server IP Address: Enter DHCP Server IP Address for DHCP clients.

3-1-2-4 System Status

System Status is only displaying system information from screen no authority to change any setting.

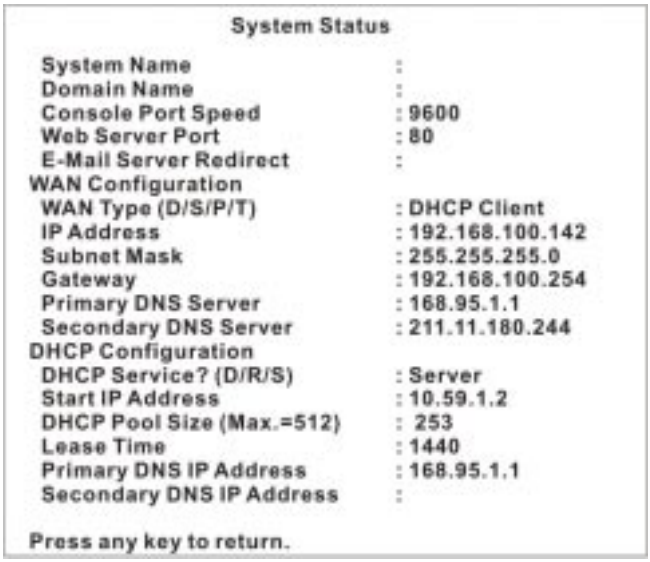


Figure 3-11 System Status Screen

3-1-2-5 Utilities Menu

Figure 3-12 Utilities Menu Screen

1) Firmware Upgrade: IAC4000 allow user to upgrade last firmware.

2) Change Password: IAC4000 allow user to change password.

3) Return to Main Menu: Leave this page and return to Main Menu screen.

- Firmware Upgrade:

The IAC4000 uses TFTP Download to upgrade firmware. User needs to specify TFTP server IP address and the filename that you wish to download.

Figure 3-13 Firmware Upgrade Setting Screen

How to make a TFTP download

Step 1. Get the TFTP server software firstly. You can get TFTP server from all our distributors or our web site or any other TFTP server software.

Step 2. Connect the TFTP server directly into the console port of the IAC4000.

Step 3. Copy the TFTP server program to a specified folder.

Step 4. Execute the TFTP server program and specify the location of firmware file.

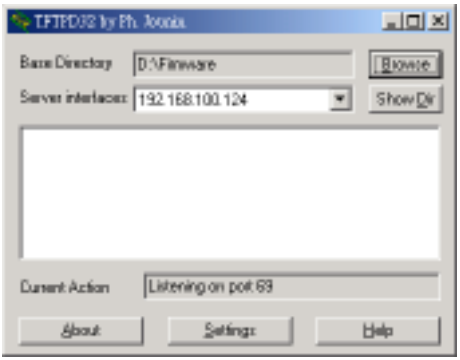


Figure 3-14 Example-TFTP Server

Step 5. Access to Figure 3-13 screen and specify the TFTP server IP address and the filename that you wish to upgrade.

Step 6. Executive and you will finish the upgrade procedures.

Note:

1. You can also download firmware using the Web agent or by a direct console connection.
2. Do not turn the power off during the upgrade process. This will damage the unit.

■ Change Password: The Password Change screen allows you to change an existing password.

Figure 3-15 Change Administrator Password Setting Screen

Note: A permitted password string is from 8 to 20. The characters are limited by alphabets and numerals.

3-1-2-6 Restart System

IAC4000 can be restart by software; the administrator doesn't need to turn off the power. This function can help you when making multiple changes to different menu function and you want to reboot just one time after completing all your changes. Type 'Y' then press 'Enter' key to restart the system. Type 'N' and then press 'Enter' to return to the Main Menu screen.

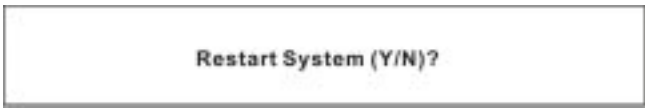


Figure 3-16 Restart System Screen

3-1-2-7 Logout

If you would like to leave the configuration page, please Type 'Y' and then press 'Enter' key to restart the system or type 'N' and then press 'Enter' to return to the Main Menu screen.

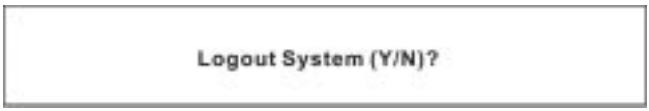


Figure 3-17 Logout System Screen

3-1-2-8 Factory Defaults

If you enter "Y" the IAC4000 will erase all setting, and back to the original factory setting. There are two different choices after you decided to change to the factory setting. One is to change all the parameters into factory setting but only reserve the user profiles (subscribers' table). The other is to clear all the parameters into factory setting including the user profiles.

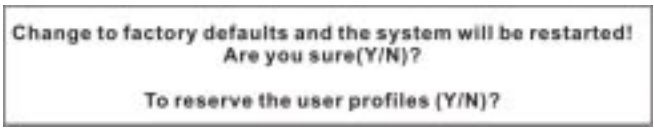


Figure 3-18 Factory Setting Screen

3-2 Web Configuration

Follow the steps below to access the Web configuration.

Step 1: Make sure your IAC4000 is properly connected.

Step 2: Start your Web browser and enter the factory default IP address 10.59.1.1 in your browser's location box. Press Enter.

Figure 3-19 Web Browser Location Field (Factory Default)

Step 3: The IAC4000 configuration main menu will appear. Enter "admin" (default) as the Username and "admin" (default) as the password and click "Get Started".

Figure 3-20 IAC4000 Login Page

Step 4: After a valid user name and password have been provided, the IAC4000 configuration homepage will appear.

Note: This Web agent is best viewed with IE 5.5 or Netscape 6.0 and above browsers.

If you would like to change the password please see system session of advanced setup.

Username and Password can consist of up to 20 alphanumeric characters and are case sensitive.

If for some reason your password is lost or you cannot gain access to the IAC4000 Configuration Program, please press the reset button to load the device to manufacturer defaults.

If the IAC4000 doesn't send packet in 5 minutes (system default), the IAC4000 wills logout automatically. You can change the idle timeout parameter, please refer to the 3-2-2-3 Server section.

3-2-1 Configuration Menu

The Configuration Menu on the left of all Web pages provides a consistent way to access all system functions.

Click System Setting for initial configuration.

Click Advance Setting for future configuration and setting up advanced features.

Click System Status to view information about your IAC4000.

Click System Tools to backup/restore configuration or upgrade system firmware.

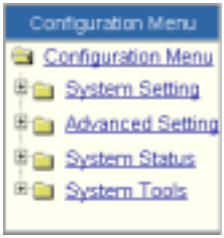


Figure 3-21 Configuration Menu

3-2-2 System Setting

The System Setting enables you to configure basic settings related to accessing the Internet, including,

1. System
2. WAN/LAN
3. Server
4. Authentication
5. Billing
6. Accounting
7. Port-Location Mapping

Figure 3-22 System Setting Menu

3-2-2-1 System

Define the IAC4000 System parameter.

Figure 3-23 System Setting Screen

Item	Default	Description
System/Host Name	Empty	The system name can consist of up to 40 alphanumeric characters.
Domain Name	Empty	The Domain name can consist of up to 80 alphanumeric characters.
Location Information		Sometime it required for compatibility of IPASS GIS.
Date/Time		
Date	System Date	(Year/Month/Day) The system date of the IAC4000. The valid setting of year is from 2002 to 2035.
Time	System Time	(Hour:Minute:Second) The system time of the IAC4000.
Use NTP Time Server	Disable	(Network Time Protocol) Enables or disables NTP Time Server. Network Time Protocol can be utilized to synchronize the time on devices across a network. A NTP Time Server is utilized to obtain the correct time from a time source and adjust the local time.
Server IP/Domain Name	Empty	Enter the IP address/domain name of NTP server.
Time Zone	GMT-12:00	Select the appropriate time zone for your location.
Update Time	0 hours	Enter the number of hours for update time.
Daylight Saving Time	Disable	Enables or disables Daylight Saving Time (DST).
Start Date/End Date	Month/Day	Set the Daylight Saving Time (DST) on the IAC4000. Adjust the begin time and end time.
NAT	Enable	(Network Address Translation) Enables or disables NAT Address Translation function.
IP Plug and Play	Enable	(iPnP Technology) Enables or disables plug & play function. When enabled, the user needn't change their network configuration to access the Internet.

Item	Default	Description
DNS Fake IP Reply	Enable	While Internet servers on your LAN such as proxy server and SMTP server require IP addresses, it is often not necessary to assign real IP addresses to each end-user workstation on a LAN. NAT is the process of assigning fake IP addresses to network devices, then translating them into a real IP address for Internet communication.
Item	Default	Description
User Session Limit	Unlimited	Enables or disables user session limit function. This feature provides you an ability to control a number of sessions allowed for particulars user(s) at the one time.
Layer 2 Isolation Security	Enable	If enable plug and play is selected, you can enable Layer 2 Isolation Security function. When the "Layer 2 Isolation Security" enabled, everyone cannot communicate with each other.
Console Type	Console Setting	There are two type, console setting and Account Generator Device.
Account Generator		
Printer Model Number	AG-100	Select one account generator printer's model number to print out user accounts.
Console Port		Attach a VT100 compatible terminal or a PC running a terminal emulation program to the Console Port on the IAC4000's front panel by using the cable provided with this package.
Bits per second	9600	
Data bits	8	
Parity	None	
Stop bits	1	

Figure 3-24 Connecting Account Generator Printer

Note: Before you use account generator printer, you must setup your device to "Authentication" mode (System Setting-⋯›Authentication-⋯›Built-in Authentication).

Administrator Authorized Access IP Address		Any Options: Any and Specify. User can specify 5 IP addresses or a range to allow remote control access from network.
Multicast Passthrough	Disable	This function allows for multiple transmissions to specific recipients at same time.
Allow remote user to ping the device		Enable This function allows remote user to ping the IAC4000 through Internet. Ping is normally used to test the physical connection between two devices, to ensure that everything is working correctly.
SSL Certificate	Default	Options: default or customize certificate, These are two ways to create a certificate, one is purchase a certificate from a certificate authority (Ex. Verisign or Thawte), and another is creating a self-certificate (For example: Uses OpenSSL tool).

After change the settings, please click Apply button to update the new settings, then the success dialog box appears, click on back to return to system setting screen.

Figure 3-25 Success Dialog Box

3-2-2-2 WAN/LAN

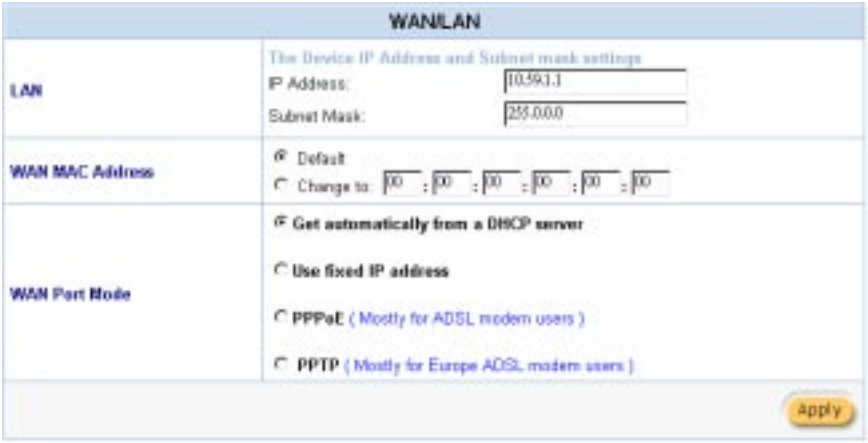


Figure 3-26 WAN/LAN Setting Screen

Figure 3-27 Restart Dialog Box

Note: After change the settings, please click Apply button to update the new settings, then the agent will restart it.

LAN

Figure 3-28 Device IP (LAN IP) Setting Screen

Item	Default	Description
IP Address	10.59.1.1	The internal LAN IP address of your IAC4000.
Subnet Mask	255.0.0.0	The subnet mask of your IAC4000.

WAN MAC Address

Figure 3-29 WAN MAC Address Setting

Item	Description
IP Address	The default MAC address is set to the WAN physical interface on device. If required by your ISP, fill in the MAC address of the network interface card in the change to field.

WAN Port Mode

Figure 3-30 WAN Port Mode Setting

Get automatically from a DHCP Server

The device can work as a DHCP client. This allows the device to obtain the IP address and other TCP/IP settings from your ISP. If your xDSL/Cable comes with this feature, please enable Use DHCP Client.

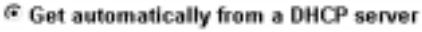


Figure 3-31 DHCP Client Setting Screen

Use fixed IP address

Figure 3-32 Static IP Setting Screen

Item	Description
IP Address	An IP address for the xDSL/Cable connection (provided by your ISP)
Subnet Mask	An IP address (provided by your ISP)
Default IP Gateway	The default IP Gateway address for the xDSL/Cable connection (provided by your ISP).
Primary DNS Server	A primary DNS server IP address for the xDSL/Cable connection (provided by your ISP).
Secondary DNS Server	A secondary DNS server IP address for the xDSL/Cable connection (provided by your ISP). If the primary DNS Server IP were not available, meanwhile, Secondary DNS Server IP would start in the same time.

PPPoE

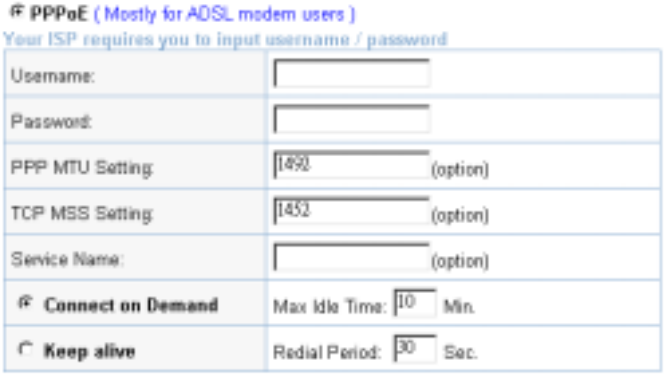


Figure 3-33 PPPoE Setting Screen

Item	Default	Description
User Name	Empty	The user name of your ISP account. The user name can consist of up to 80 alphanumeric characters and is case sensitive.
Password	Empty	The user password of your ISP account. The password can consist of up to 80 alphanumeric characters and is case sensitive.
PPP MTU Setting	1492	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.
TCP MSS Setting	1452	MSS (Maximum Segment Size) specifies maximum segment size.
Service Name (Option)	Empty	Your ISP will provide the service name.
Connect on Demand and Max Idle Time		
Connect on Demand	Enable	You can configure your IAC4000 to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables your IAC4000 to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain, click the radio button of keep alive. The Max Idle Time maximum value is 65535 minutes.

Item	Default	Description
Max Idle Time	10 Minutes	
Keep alive and Redial Period		
Keep alive	Disable	This option keeps your PPPoE enabled Internet access connected indefinitely, even when it sits idle. The Redial Period maximum value is 65535 seconds.
Redial Period	30 Seconds	

PPTP

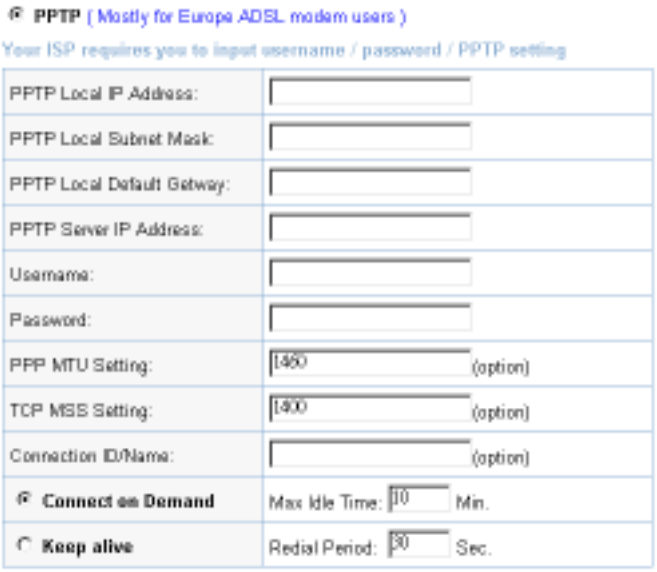


Figure 3-34 PPTP Setting Screen

Item	Default	Description
PPTP Local IP Address	Empty	A PPTP local IP address for the xDSL/Cable connection (provided by your ISP).
PPTP Local Subnet Mask	Empty	A PPTP local IP address for the xDSL/Cable connection (provided by your ISP).
PPTP Local Default Gateway	Empty	A PPTP local default gateway for the xDSL/Cable connection (provided by your ISP).
PPTP Server IP Address	Empty	A PPTP server IP address for the xDSL/Cable connection (provided by your ISP).
Username	Empty	The user name of your ISP account. The user name can consist of up to 80 alphanumeric characters and is case sensitive.
Password	Empty	The user password of your ISP account. The password can consist of up to 80 alphanumeric characters and is case sensitive.
Connection ID/Name	Empty	Connection ID or connection name.
PPP MTU Setting	1460	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.

Item	Default	Description
TCP MSS Setting	1400	MSS (Maximum Segment Size) specifies maximum segment size.
Connect on Demand and Max Idle Time		
Connect on Demand	Enable	You can configure your IAC4000 to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables your IAC4000 to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain, click the radio button of keep alive. The Max Idle Time maximum value is 65535 minutes.
Max Idle Time	10 Minutes	
Keep alive and Redial Period		
Keep alive	Disable	This option keeps your PPTP enabled Internet access connected indefinitely, even when it sits idle. The Redial Period maximum value is 65535 seconds.
Redial Period	30 Seconds	

3-2-2-3 Server

Figure 3-35 Server Configuration Screen (Authentication Type=No Authentication)

Figure 3-36 Server Configuration Screen (Authentication Type=Built-in Authentication)

Item	Default	Description
Web Server	80	The web server port allowed range is 80 or 8010 to 8060 if administrator wants to remote access under NAT Network. For access the IAC4000 system under NAT, please tab the "http://WAN Port IP Address: Port Number". The function of remote access Internet.
SSL Security	Disable	Enables or disables the SSL security.
Item	Default	Description
Administrator Idle -Timeout	5 Minutes	The idle time out valid range is 1-1440. If the idle time out is set as 5 minutes, it means if the administrator doesn't send packet in 5 minutes, the administrator will logout automatically.
DHCP Server	Enable	There are three types of DHCP Services. DHCP Disable-Disable the DHCP server function. DHCP Relay-Enable DHCP Relay function. DHCP Server-Enable DHCP Server (Private) function. DHCP Server-Enable DHCP Server (Public) function.
DHCP Relay		To route DHCP through an external server, the administrator needs to enable the DHCP relay and assign a valid DHCP server IP address.
DHCP Server IP Address	Empty	The IP address of DHCP relay server.
DHCP Server (Private)		
IP Pool Starting Address	10.59.1.2	Enter the DHCP Pool Starting IP address.
DHCP Pool Size	253	The DHCP pool size range is 1 to 512.
Lease Time (Private)	1440 Minutes	The DHCP lease time (Private). The DHCP lease time range is 1 to 71582788 minutes.
Lease Time (Temporal)	5 Minutes	The DHCP lease time (Temporal).
Primary DNS Server	168.95.1.1	The IP address of the network's primary DNS server.
Secondary DNS Server	Empty	The IP address of a second DNS server on the network.

DHCP Server(Public)	Disable	Enables or disables DHCP Server (Public). Regarding the detail please refer to appendix A "DHCP Private/Public IP pool Setup".
IP Pool Starting Address	Empty	Enter the DHCP Pool Starting IP address.
Pool Size	253	The DHCP pool size range is 1 to 512.
Lease Time (Public)	1440 Minutes	Enter the DHCP lease time. The DHCP lease time range is 1 to 71582788 minutes.
Email Server Redirect		To prevent some subscriber's original Email server may protect by firewall or NAT network. IAC4000 provides an extra Email server parameter to forward the subscriber's Email. The IAC4000 not only forwards the subscribers' E-mail via other E-mail server but also changes the SMTP header. The recipient of your E-mail sees the message as if you sent it from your local Internet Service Provide, not form the hotel or other place. Note: Before setting this sever, please make sure the e-mail sever relay function is opened.
IP Address or Domain Name	Empty	Enter the e-mail server IP address or domain name. The field must not exceed 50 characters.
SMTP Port	25	Enter the SMTP port. The SMTP port allowed range is 25 or 2500 to 2599.

3-2-2-4 Authentication

Authentication Type

Figure 3-37 Authentication Configuration Setting Screen

Item	Default	Description
Authentication Type		
No Authentication /Built-in Authentication /RADIUS	No Authentication	Options: No Authentication, Built-in Authentication or RADIUS. No Authentication: Subscriber can direct access the Internet without enter username and password. Built-in Authentication: IAC4000 provides "Built-in Authentication" for service provider to build up an Internet service without any extra authentication software. If "Built-in Authentication" is selected, service provider can generate the subscriber account inside IAC4000, and the system will authenticate the subscriber login according to the generated account. RADIUS: IAC4000 provides "RADIUS Authentication" for service provider to build up an Internet service with RADIUS server. If "RADIUS Authentication" is selected, all subscribers' authentication will send to RADIUS Server by RADIUS protocol (RFC 2865, 2866).
Built-in Authentication		
Current Preset option	Scenario C	This is the best way to setup your authentication of Internet Service. Follow the instructions of Scenario Guide below to quickly install your IAC4000.
Select option		Click this button to select the scenario.

Figure 3-38 Scenario Guide Setting Screen

Item	Default	Description
Items check	Scenario C	Scenario A: This solution is applying for the Hotel Internet solution where already has PMS system. With using the "Port-location Mapping" or "VLAN Tag" infrastructure, subscriber can access to the Internet directly from their room and on-line select the billing profile. For some circumstances (staff, VIP…), you can still create static or dynamic accounts to access Internet. About the create account method, please refer to "Accounting" section.

Login Page

Item	Default	Description
Items check	Scenario C	Scenario B: This solution is applying for the Hotel Internet solution where already has PMS system, but the existing infrastructure that in use do not support "Port-Location Mapping" or "VLAN Tag". Before subscriber access to Internet, Hotel staff must register the room number and generate an account (username & password). Subscriber uses this account and selects billing profile to access Internet.

Login Page

Scenario C: This solution is applying for the Hotel Internet solution where do not have PMS. Before the subscriber access to Internet, subscriber has to ask for an account (username & password) from Hotel staff. Subscriber has to inform the staffs that what billing profile subscriber wants to choose. After the account has been generated, subscriber has to pay the charging amount to Hotel staff. Subscriber can use this account to access Internet.

Login Page

Figure 3-39 Scenario A Application

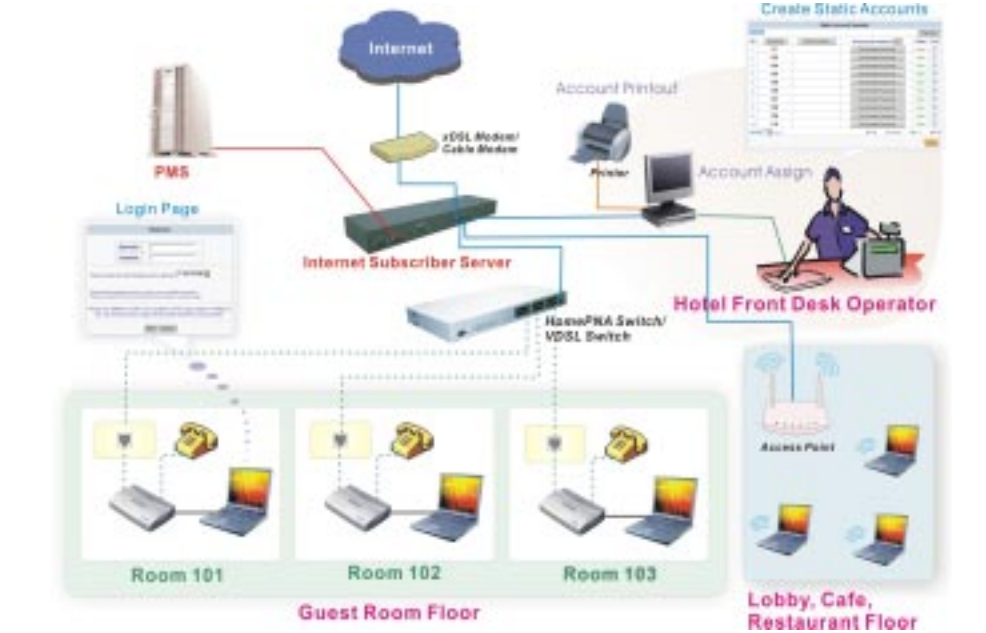


Figure 3-40 Scenario B Application 1

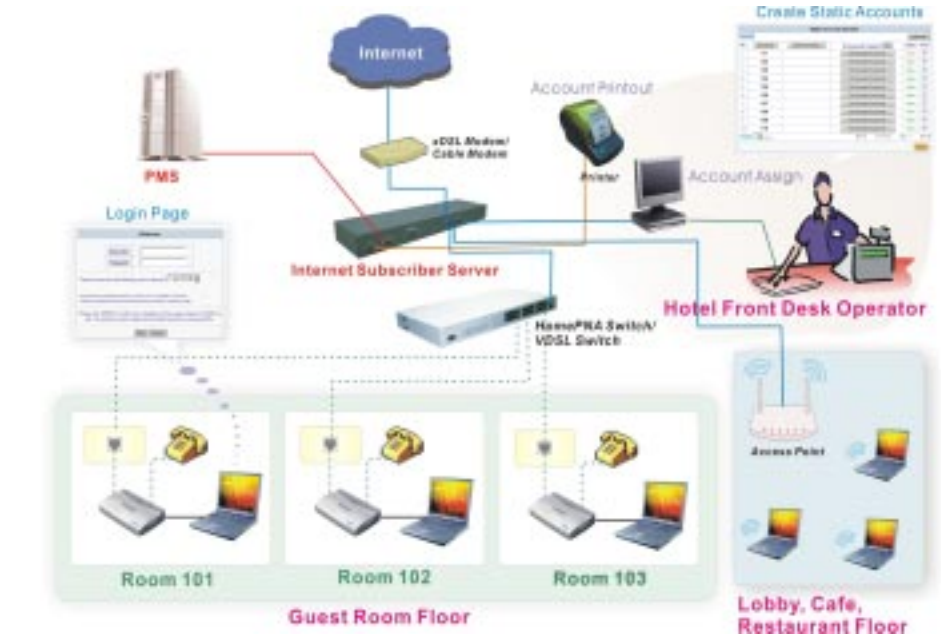


Figure 3-41 Scenario B Application 2

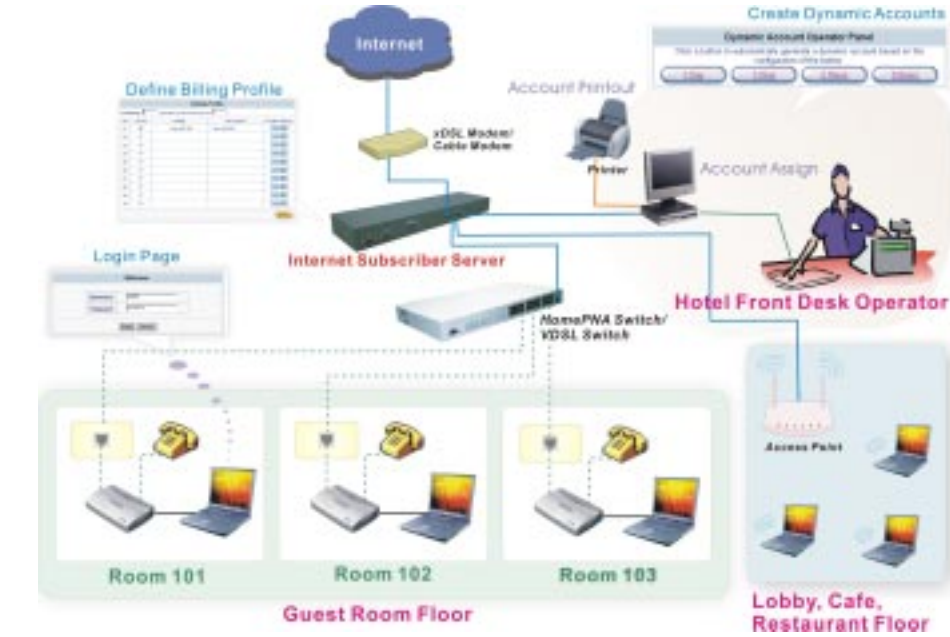


Figure 3-42 Scenario C Application 1

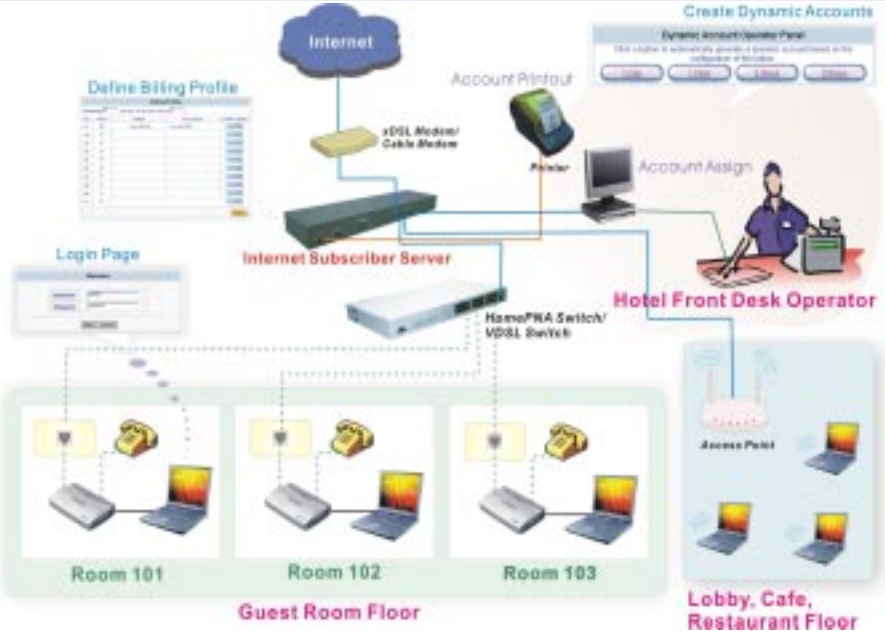


Figure 3-43 Scenario C Application 2

Item	Default	Description
Billing Charge Mode Based on Room / Based on Subscriber	Based on Room	The system provides two different billing charge methods for the Internet service. Based on Room: The charge method is based on the room, the system allows only subscriber using specific account to access Internet from his/her room. Based on Subscriber: The charge method is based on the subscriber, the system allows subscriber to access Internet from anywhere.
Allow concurrent access	Enable	Disable: The system allows only one user to access Internet with one account. Enable: The system allows up to eight concurrent users to access Internet with one account.
Max. concurrent access	2	The field specifies how many times the account be used simultaneously. The field maximum value is 5.

Figure 3-44 RADIUS Setting Screen

Item	Default	Description
RADIUS	Disable	The IAC4000 supports Remote Authentication Dial-In User Service (RADIUS). RADIUS is an authentication and accounting system used by many Internet Service Providers (ISPs). RADIUS enables ISPs to maintain a very large central database of subscribers. By using RADIUS, Service Providers can implement policy-based management of their subscriber database. The RADIUS also helps ISP to collect accounting data such like login time and logout time.
Check Local Account first	Disable	Click the check box to check local account. If the checks succeed, the request is processed and answered.
Accumulation/Time to finish (No idle timeout)		Accumulation Service provider provides two different accounting calculate for the internet service. Regarding the detail please refer to appendix B "Use RADIUS Server to setup your Internet Service".

Figure 3-45 Usage Time

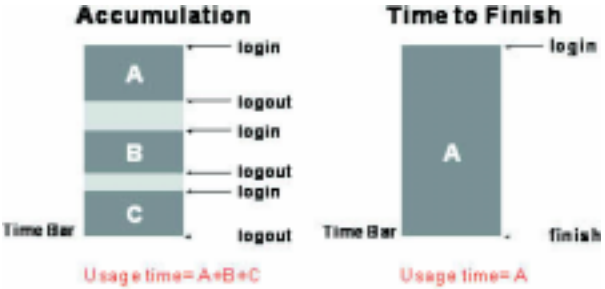


Figure 3-46 Accumulation and Time to Finish

Item	Default	Description
RADIUS	Disable	The IAC4000 supports Remote Authentication Dial-In User Service (RADIUS). RADIUS is an authentication and accounting system used by many Internet Service Providers (ISPs). RADIUS enables ISPs to maintain a very large central database of subscribers. By using RADIUS, Service Providers can implement policy-based management of their subscriber database. The RADIUS also helps ISP to collect accounting data such like login time and logout time.
Primary RADIUS Server IP	Empty	The primary IP address of RADIUS server.
Authentication Port	0	The authentication port number, the number must match with the RADIUS server setting. The allowed numbers are from 0 to 65535.
Accounting Port	0	The accounting port number, the number must match with the RADIUS server setting. The allowed numbers are from 0 to 34463.
RADIUS Secret Key	Empty	The RADIUS secret key, the key number also has to match with the Server setting. Up to 64 characters are allowed.

Item	Default	Description
Secondary Radius Server IP		Empty The secondary IP address of RADIUS server.
Authentication Port	0	The authentication port number, the number must match with the RADIUS server setting. The allowed numbers are from 0 to 65535.
Accounting Port	0	The accounting port number, the number must match with the RADIUS server setting. The allowed numbers are from 0 to 34463.
RADIUS Secret Key	Empty	The RADIUS secret key, the key number also has to match with the Server setting. Up to 64 characters are allowed.
Retry times when Primary failed		5 Specify the retry times when primary fail.
Accounting Service	Disable	Enables or disables the accounting service.
Update Time	0 Minutes	Specify the update time.
Authentication Method	CHAP	The authentication method of RADIUS server.

Note:

1. The RADIUS Server follows the RFC 2865 and RFC 2866 stand. And the authentication port number is 1645 and 1812. The administrator can configure the port number according to his own RADIUS server. For more detail information of RADIUS please check the manual of your RADIUS server.
2. After change the settings, please click Apply button to update the new settings, then the agent will restart it.

Figure 3-47 Restart Dialog Box

Idle Time Out

Figure 3-48 Idle Time Out Setting Screen

Item	Default	Description
Idle Time Out	5	The idle time out valid range is 1-1440. If the idle time out is set as 5 minutes, it means if the subscriber doesn't send packet in 5 minutes, the subscriber will logout automatically. If the subscriber is off-line over the logout time, he must re-login again for Internet service.

Current User Information Backup

The system provides automatically backup account information and unused dynamic account to flash ROM.

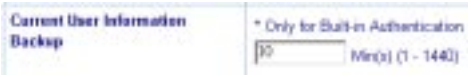


Figure 3-49 Current User Information Backup

Item	Default	Description
Current User Information Backup	10 Minutes	This function allow administrator to adjust the backup time. The default value is 10 minute. The Current User Information valid range is 1 to 1440.

SSL Login Security

Figure 3-50 SSL Login Security Setting Screen

Item	Default	Description
SSL Login Security	Disable	Enables or disables SSL security.

Figure 3-51 Smart Client Support Setting Screen

Item	Default	Description
IPASS GIS	Disable	Enables or disables IPASS GIS roaming function.
Login Mode	Directly Reply	Options: Directly Reply, Proxy Reply with "Redirect Login Page" URL and Proxy Reply with Specific URL. The login mode information for the IPASS GIS connection. (Provided by your ISP).
Proxy Reply with Specific URL	Empty	Enter the URL page. The input format can be "http://www.yahoo.com". The maximum character of the URL Link is 200.

3-2-2-5 Billing

The function is used to setup a billing profile. A billing profile is a description of how you want to charge your customer.

Billing Profile

Figure 3-52 Billing Plan Setting Screen

Item	Default	Description
Currency	$	Enter the appropriate currency unit or currency symbol.
Number of decimals places	2	The field maximum value is 3.
No	1~10	The index number of billing profile.
Active	Disable	Click on check box, active or inactive the billing profile.
Name	Empty	It is the name of billing profile. The maximum allowed characters length is 10.
Description	Empty	It is the description of the Billing Profile. The maximum allowed characters length is 60.
Profile Setting		
To Change a billing profile	-	Click it from the grid, change any of the data as needed, and then click Apply.
Click Apply button to save the new settings.		

Edit Billing Profile

Billing calculation is according to the Billing Profile.

Figure 3-53 Billing Profile Setting Screen

Item	Default	Description
NO	1~10	The index number of the billing profile.
NAME	Empty	The name of the billing profile.
Description	Empty	The description of the billing profile.
Price		
Duration	1 day	The duration of the billing period. When this period expires, user account will be discontinued.

Charge	10.00	Enter the unit rate amount (i.e. 35.00) that most of your accounts are charged for one day of service.
Check Time	Period Time finish	The check time options let you specify an expiry time for Internet Service.
Selective Unit	1 to 10	Enter a range of purchase unit. The field valid range is 1 to 99.

Click Reset button to restore system configuration.

Click Apply button to save the new settings.

Figure 3-54 Example-Login Page

Figure 3-55 Bandwidth Limit Setting Screen

Item	Default	Description
Maximum Upstream Bandwidth	64Kbps	Specify the amount of upstream bandwidth for a billing profile that has already been configured on this device.
Maximum Downstream Bandwidth	256Kbps	Specify the amount of downstream bandwidth for a billing profile that has already been configured on this device.

Note: You must activate Bandwidth Management feature and select a class of service.

The Bandwidth Management Setting Screen is shown below,

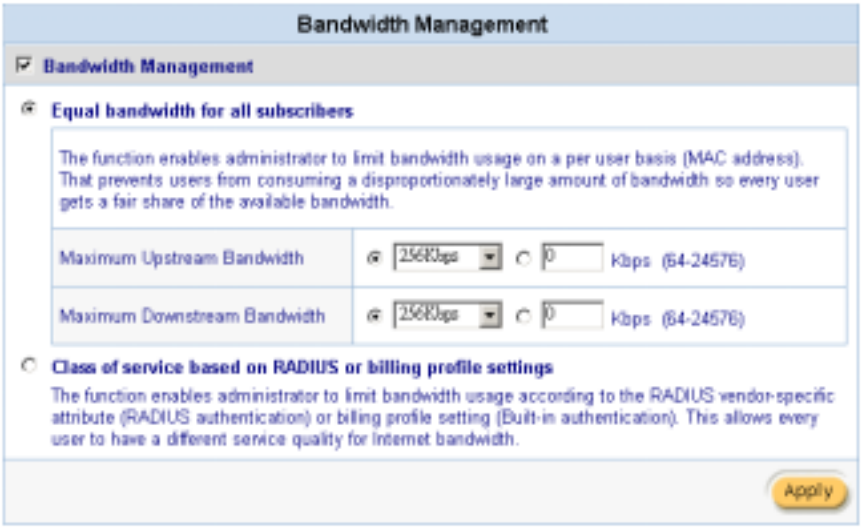


Figure 3-56 Bandwidth Management Setting Screen

Service Type

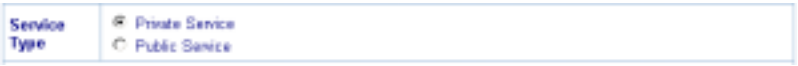


Figure 3-57 Service Type Setting Screen

Item	Default	Description
Service Type	Private Service	Specify the service type, private service or public service.

PMS Configuration

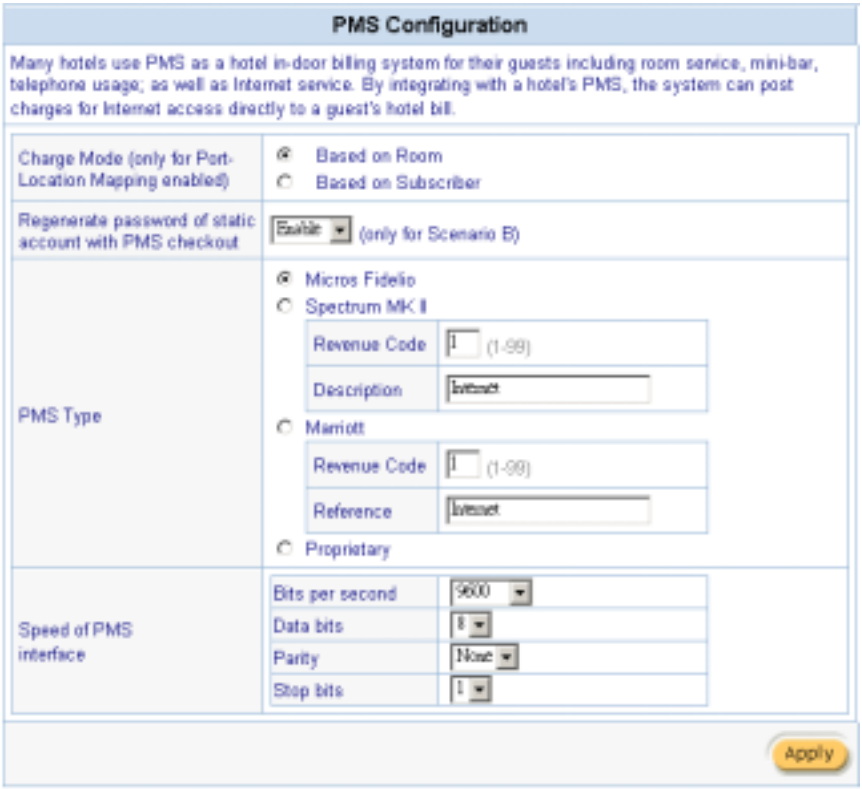


Figure 3-58 PMS Configuration Setting Screen

Item	Default	Description
Charge Mode (only for Port-Location Mapping enabled)	Base on Room	Options: Base on Room, Base on Subscriber.

Item	Default	Description
Regenerate password of static account when PMS checkout (only for Scenario B)	Enable	Enables or disables regenerate password function. When enable, the system will regenerate the password of static account automatically.
PMS Type	Micros Fidelio	The IAC4000 offer support Micros Fidelio PMS, Spectrum MK II PMS, Marriott PMS and proprietary PMS perform in-room billing.
Spectrum MK II		
Revenue Code	1	Enter the revenue code of Spectrum MK II PMS system; the value must match with the PMS System setting. The revenue code valid range is 1 to 99.
Description	Internet	It is the description of the PMS system.
PMS interface	Attach your PMS system to the PMS port on the IAC4000's front panel by using the cable provided with this package.	
Marriott		
Revenue Code	1	Enter the revenue code of Marriott PMS system; the value must match with the PMS System setting. The revenue code valid range is 1 to 99.
Description	Internet	It is the description of the PMS system.
PMS interface	Attach your PMS system to the PMS port on the IAC4000's front panel by using the cable provided with this package.	
Proprietary	The Internet Server Gateway provides proprietary PMS type, which is allowed service provider follow the specification to build up a PMS system.	
Speed of PMS interface		
Bits per second	9600	
Data bits	8	
Parity	None	
Stop bits	1	

3-2-2-6 Accounting

This allow service provider to generate the subscriber accounts (static accounts and dynamic accounts).

Static Account Setting

Figure 3-59 Static Account Setting Screen

Item	Default	Description
Concurrent Access Allow concurrent access with one account	Enable	Disable: The system allows only one user to access Internet with one account. Enable: The system allows up to eight concurrent users to access Internet with one account.
Max. concurrent access	2	The field specifies how many times the account be used simultaneously. The field maximum value is 8
Customize Printout	-	This function allows you to produce custom bill based on your requirements. Click on Customize printout text to display the Account Printout Customization setting screen.
Print to …	Account Generator Printer	Select a printer to print account information.

Figure 3-60 Account Printout Customization Setting Screen

Click Apply button to save the new settings.

Figure 3-61 Scenario A/C-Static Account Printout-PC-connected printer

Figure 3-62 Scenario B-Static Account Printout-PC-connected Printer

Figure 3-63 Scenario A/C-Static Account Printout-Account Generator Printer

Figure 3-64 Scenario B-Static Account Printout-Account Generator Printer

Figure 3-65 Dynamic Account Printout-PC-connected Printer

Figure 3-66 Dynamic Account Printout-Account Generator Printer

Create Static Account

This allow service provider to generate the static subscriber accounts.

Figure 3-67 Create Static Account Setting Screen

Item	Default	Description
Prefix	Empty	Enter the prefix. The field can consist of up to 30 alphanumeric characters and is case sensitive.
Postfix	Empty	Enter the postfix. The field can consist of up to 30 alphanumeric characters and is case sensitive.
From	0	The field must contain only numbers and it maximum allow digits length is 5.
To	0	The field must contain only numbers and it maximum allow digits length is 5.
Billing Profile	-	Select billing profile by clicking in the list box.
Random Password Length	8	The field maximum value is 8.

Static Accounts backup and restore

Figure 3-68 Static Accounts Backup and Restore Setting Screen

Item	Default	Description
Backup	sta_acc.txt	Click it to save the static account information to your computer.
Restore	Click it to restore your static account information.	
File Path	Empty	Enter the file pathname of static account information in the File Path field.

Click Apply button to execute the file restore process.

Manually Add Subscriber Account

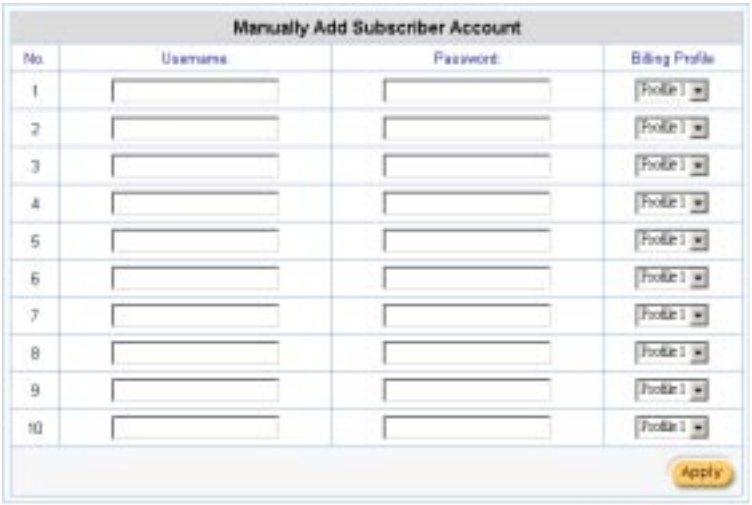


Figure 3-69 Manually Add Subscriber Account Setting Screen

Item	Default	Description
Username	Empty	The username can consist of up to 30 alphanumeric characters and is case sensitive.
Password	Empty	The password can consist of up to 30 alphanumeric characters and is case sensitive.
Billing Profile	-	Select billing profile by clicking in the list box.

Static Account Operator

This allows front desk clerk to manage the Internet Service and print out the billing.

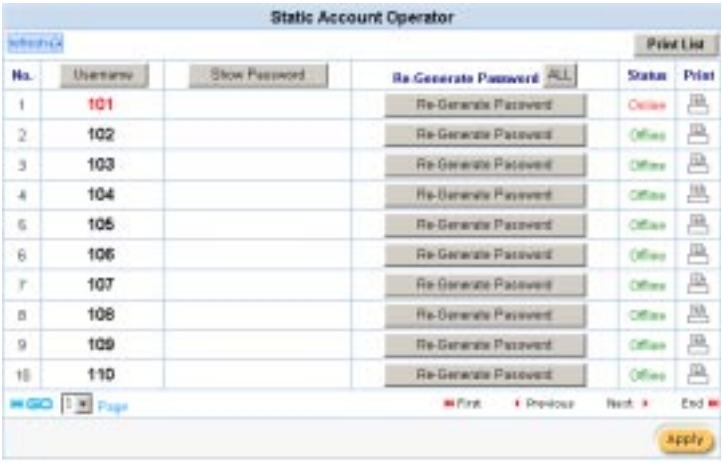


Figure 3-70 Static Account Operator Screen

Item	Description
Status	This field displays the current state of a subscriber's connection. (Online/Offline)

Click on refresh button to update the static account operator page.

This button allows you to print the static account list.

Click the column button to sort the column in ascending/descending order.

To show or hide the password information.

Click the all button to re-generate all passwords of static account operator table.

If you feel concern about security, please click Re-Generate Password button to change password.

This button allows you to print bill for you and your customer.

Static Account List

You can display a list of all the static account information on this device. This table includes the username, password, billing profile, concurrent access, login time, expiration time and status.

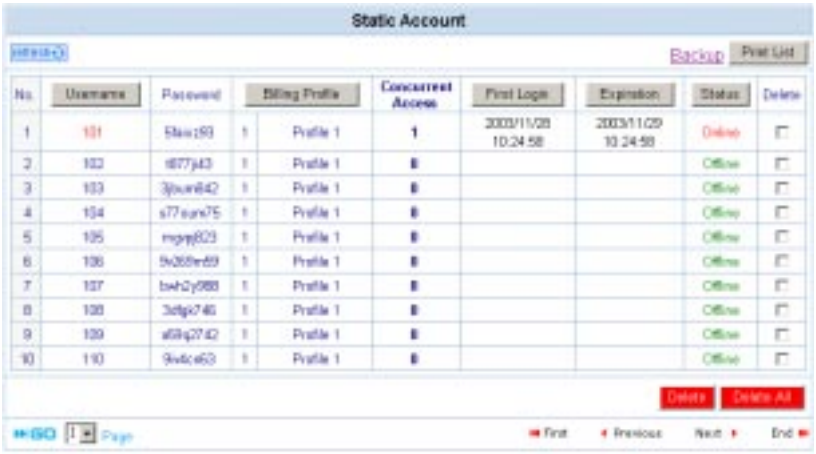


Figure 3-71 Static Account List

Click on refresh button to update the static account list page.

Click it to save the static account information to your computer. (sta_list.txt)

This button allows you to print the static account list.

Click the column button to sort the column in ascending/descending order.

Select the check boxes and click 'Delete' to delete the accounts.

Delete all accounts in static account list.

Dynamic Account

Dynamic Accounts can be created randomly when you click the 4 pre-defined buttons from the Web-based dynamic account operator and print out from general connected printer.

Dynamic Account Setting

Figure 3-72 Dynamic Account Setting Screen

Item	Default	Description
Web-based Account Generator Panel Settings		
Button Name (1~4)	Button 1~4	The button name can be specified text. The maximum character of the button name is 12.
Billing Profile	Default Billing Profile	Define each button's usage time.
General Settings		
Unused Accounts	12 hours	Enter the number of hours.
Printout copy		
No of copies to print	1	Select the number of copies. The field maximum value is 3.
		Click on Customize printout text to display Account Printout Customization setting screen.
Print to …	Account Generator Printer	Select a printer to print account information.
		Click the button to preview the dynamic account printout.

Click Apply button to save the new settings.

Figure 3-73 Dynamic Account Operator Panel

Click on button, to add a new account.

Figure 3-74 Dynamic Account Printout

Close window.

Click Print button to print this account information.

Before you create static account, you must enable Built-in Authentication option (System Setting->Authentication->Built-in Authentication). For details, see section 3-2-2-4 Authentication.

Figure 3-75 Error Dialog Box

Dynamic Account List

This list will allow you to view or print all account status.

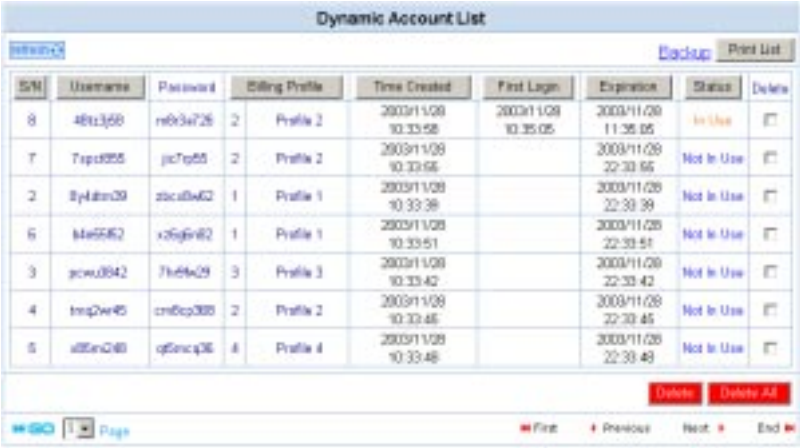


Figure 3-76 Dynamic Account List

Item	Description
Status	This field displays the current state of a subscriber's connection. (In Use/Not In Use)

Click on refresh button to update the dynamic account list page.

Click it to save the dynamic account information to your computer. (dyn_list.txt)

Click the Print List button to print the dynamic accounts list.

The field name button in this list show that this list can be sorted in ascending/descending order according to the corresponding field name.

Select the check boxes and click 'Delete' to delete the accounts.

Delete all accounts in dynamic account list.

3-2-2-7 Port-Location Mapping

Figure 3-77 Port-Location Mapping Setting Screen

Item	Default	Description
Single Create		
Location Identifier (ID)	Empty	The field can consist of up to 20 numeric characters and it must match with the VLAN Tag/Port-Location mapping device setting. Note: When you using VLAN-Tag infrastructure, the Location Identifier (ID) is VLAN ID.
Port Identifier (ID)	Empty	The Port Identifier (ID) is a number you set in the PMS system. The field valid range is 1 to 999999.
Description	Empty	The field can consist of up to 32 characters.
Status	Charge for use	Select the status of a location-mapping. Options: No Charge, Charge for use and Blocked.

Item	Default	Description
Batch Create		
Location ID From	Empty	Enter the Location ID. The field can consist of up to 20 numeric characters and it must match with the VLAN Tag/Port-Location mapping device setting. Note: When you using VLAN-Tag infrastructure, the Location Identifier (ID) is VLAN ID.
Port ID From	Empty	Enter the Port ID. The Port Identifier (ID) is a number you set in the PMS system. The field valid range is 1 to 999999.
Batch Numbers	Empty	Enter the batch number. The field valid range is 1 to 512.
Status	Charge for use	Select the status of a location-mapping. Options: No Charge, Charge for use and Blocked.
Backup/Restore		
Backup		
Empty	Click it to backup the port-location mapping records to your computer. (port_conf.txt)	
	Remote TFTP Server IP Address	Empty Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.
	Restore	Click it to restore your port-location mapping records.
Local PC File Path	Empty	Enter the file pathname of the port-location mapping backup file in the Local PC File Path field.
Remote TFTP Server IP Address		Empty Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.
The field name button in this list show that this list can be sorted in ascending/descending order according to the corresponding field name.		
Select the check boxes and click 'Delete' to delete the accounts.		
Delete all accounts in Port-Location Mapping list.		

Please refer to the following instructions for Port-Location Mapping Operation.

Step 1: In the Authentication Configuration screen, select Built-in Authentication and Scenario A.

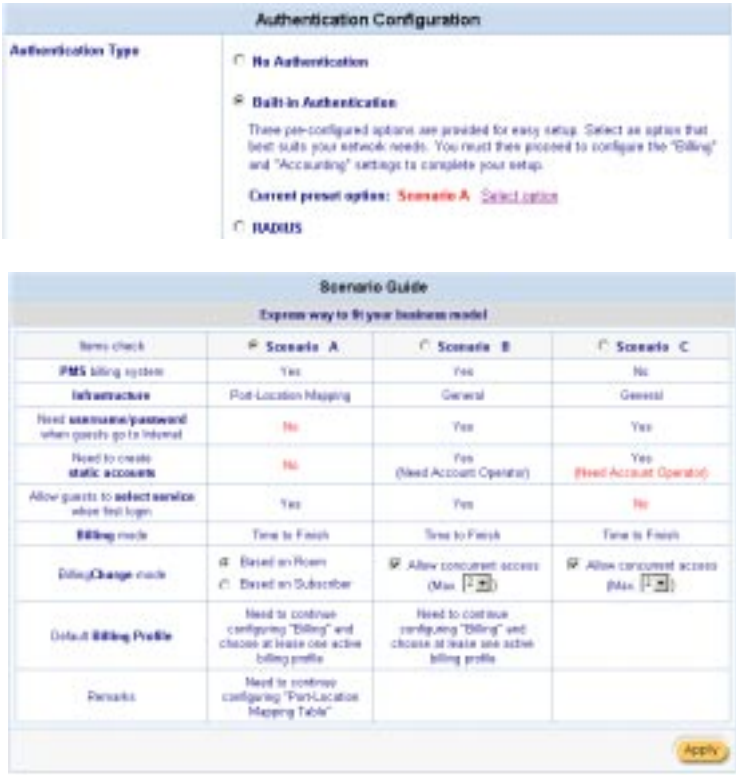


Figure 3-78 Authentication Setting Screen

Step 2: Define Billing Profile.

Figure 3-79 Billing Profile Setting Screen

Step 3: In the PMS Configuration screen, configure the PMS parameters for PMS connection.

Figure 3-80 PMS Configuration Setting Screen

Step 4: To set up your switch.

In Port-Location Mapping Configuration screen of switch, enable Port-Location Mapping and type Access Controller IP Address. (The IP address of IAC4000)

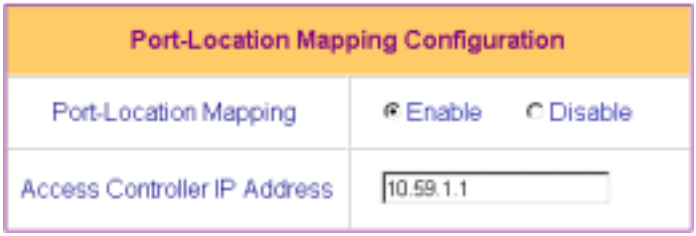


Figure 3-81 Port-Location Mapping Configuration Setting Screen (Switch)

To define port name for port-location mapping

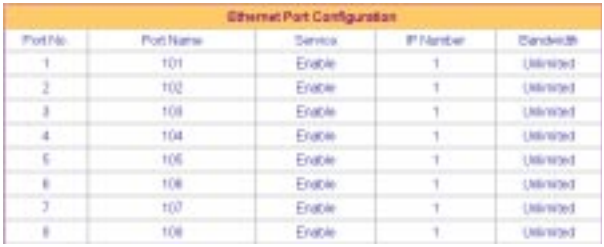


Figure 3-82 Ethernet Port Configuration Setting Screen (Switch)

Step 5: In Port-location Mapping screen, set up port-location mapping.

Figure 3-83 Port-Location Mapping Setting Screen

Step 6: Subscriber wants to access Internet, subscriber start his/her Web Browser; a subscriber login page will appear. Subscriber select billing profile and purchase unit and click "Enter", subscriber can use Internet now.

Figure 3-84 Subscriber Login Page

3-2-3 Advanced Setting

The Advanced Setting enables you to configure advanced settings related to accessing the Internet, including,

1. Customization
2. Bandwidth
3. Portal Page
4. Advertisement
5. Walled Garden
6. Passthrough
7. LAN Devices
8. Static Route
9. Logs
10. SNMP

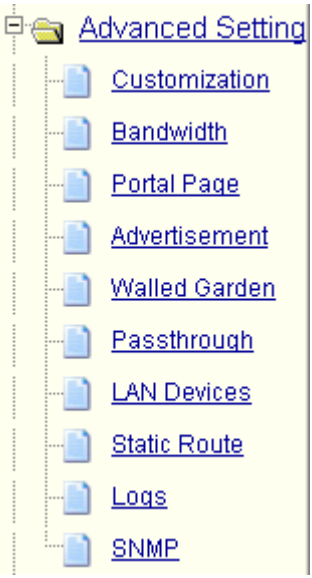


Figure 3-85 Advanced Setting Item Screen

3-2-3-1 Customization

Login Page

For some Hotels or ISPs, they may hope to have a customize subscriber's login page to the users. This function helps them to realize the ideal. The page elements are including welcome image, background color, article etc. Certainly the administrator can decide to use only standard form. The IAC4000 provides three different login page formats, including standard, redirect, advanced and frame format.

Standard

This is IAC4000 default login page, can't be changed.

Figure 3-86 Login Page Customization Setting Screen

Item	Default	Description
Title	Welcome	Enter the title name of subscriber login page. The maximum allowed characters length is 80.
Footnote	Disable	Allow the administrator to input the footnote such like "Pleas Contact to our Customer Service Center, EXT 142". The maximum character of the footnote is 240.
Copyright	Enable	The copyright is allowed the administrator to input a paragraph in the subscriber login page for copyright information. The maximum character of the copyright is 80.
Background Color	FFFFFF	The background text color can be specified color. For the specified text color format please views the color grid. The allowed format is Hexadecimal.

Figure 3-87 Login Page Screen

Figure 3-88 Login Page Screen
Scenario A

Figure 3-89 Login Page Screen
Scenario B

Figure 3-90 Login Page Screen
Scenario C

Redirect

This allow service provider to redirect the subscriber's browser to a specified home page.

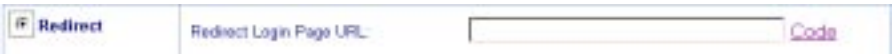


Figure 3-91 Redirect Login Page Setting Screen

Copy and paste the following HTML Code into your home page to produce redirect subscriber login page.

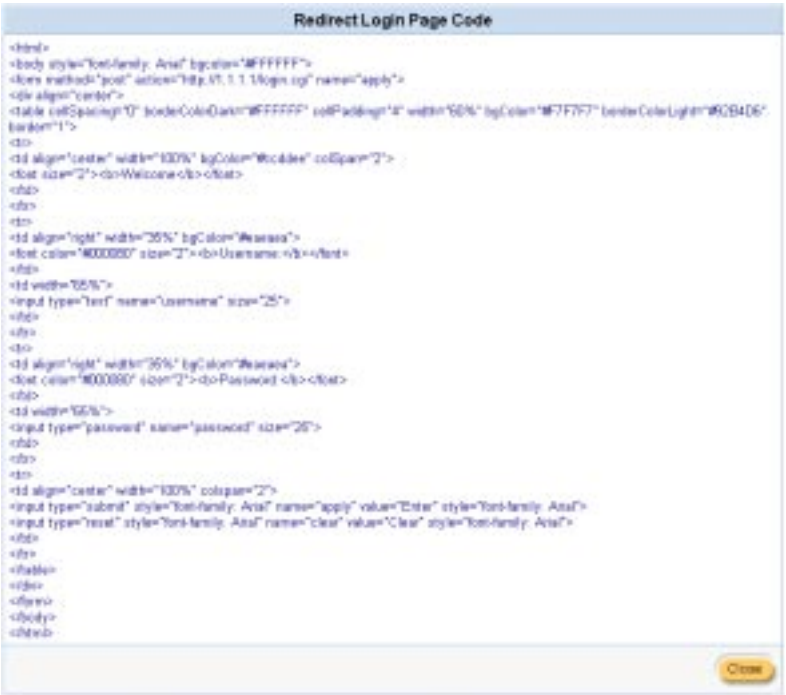


Figure 3-92 Redirect Login Page Code Screen

Advanced

This function allow user to design login page of IAC4000.

Figure 3-93 Advanced Login Page Setting Screen

Item	Default	Description
Welcome Slogan	Welcome	The maximum allowed characters length is 80.
Page Background	None	The page background can be none or specified color. For the background color format please views the color grid. The allowed format is Hexadecimal (RGB values, 000000 is black and FFFFFF is white.)
Article	Empty	The article is allowed the administrator to input a paragraph in the subscriber login page for advisement or announcement. The maximum character of the article is 1024.
Article Text Color	000000	The article text color can be specified color. For the specified text color format please views the color grid. The allowed format is Hexadecimal.
Article Background Color		None The article background can be specified color. For the background color format please views the color grid. The allowed format is Hexadecimal (RGB values of Red, Green, and Blue, where each component has a hexadecimal value of from 00 to FF. 000000 is black and FFFFFF is white.)

Information	Empty	Allow the administrator to input the text information such like address, telephone number and fax information. The maximum character of the information is 80.
Comments	Empty	Allow the administrator to input the text comments such like "Pleas Contact to our Customer Service Center, EXT 142". The maximum character of the comment is 80.

Figure 3-94 Example-Advanced Login Page Screen

Frame

If "Frame" is selected the subscriber login page will be separate into Top Frame and Bottom Frame. Bottom Frame is a default format for username and password input, Top Frame is allowed to be specified a URL to link.

Figure 3-95 Frame Login Page Setting Screen

Item	Default	Description
Top Frame URL Link	Empty	The input format can be http:// www.yahoo.com. The maximum character of the URL Link is 200.
Bottom Frame	-	This frame will show the standard login page.

Figure 3-96 Example-Login Page Screen

Service Selection Customization

This function allow service provider to specified text of login page.

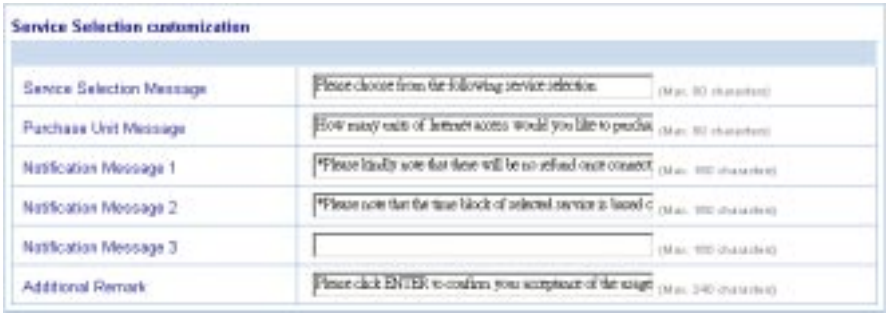


Figure 3-97 Service Selection Customizations

Figure 3-98 Login Page

Information Window

This function allow service provider can decide whether they want an "Information Window" pop-up on subscriber PC when authenticate successful or not and specified text of information window.

Figure 3-99 Information Window Customization Setting Screen

Click Apply button to save the new settings.

Figure 3-100 Information Window

An "Information Window" will pop up on subscriber PC when subscriber login successful. The purpose for "Information Window" is to remind subscribers the remaining usage time.

Figure 3-101 Information Window

Account Printout

This function allow service provider to specified text of account printout.

Figure 3-102 Account Printout Customization Setting Screen

3-2-3-2 Bandwidth

This function allows you to control the bandwidth on the LAN.

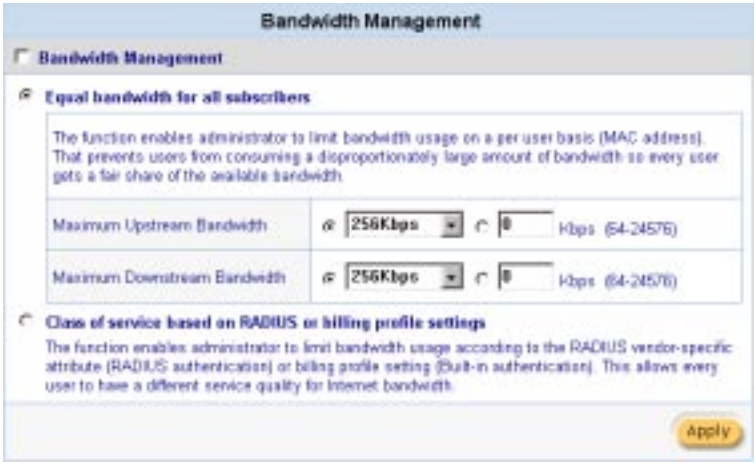


Figure 3-103 Account Printout Customization Setting Screen

Item	Default	Description
Bandwidth Management	Disable	Enables or disables Bandwidth Management.
Equal bandwidth for all subscribers	Enable	The function enables administrator to limit bandwidth usage on a per user basis (MAC address). That prevents users from consuming a disproportionately large amount of bandwidth so every user gets a fair share of the available bandwidth.
Maximum Upstream Bandwidth	256Kbps	Specify the amount of upstream bandwidth for IAC4000 that has already been configured on this device.
Maximum Downstream Bandwidth	256Kbps	Specify the amount of downstream bandwidth for IAC4000 that has already been configured on this device.
Class of service based on RADIUS or billing profile settings	Disable	The function enables administrator to limit bandwidth usage according to the RADIUS vendor-specific attribute (RADIUS authentication) or billing profile setting (Built-in authentication). This allows every user to have a different service quality for Internet bandwidth.

3-2-3-3 Portal Page

Figure 3-104 Account Printout Customization Setting Screen

Item	Default	Description
URL Link	Empty	This function allows redirecting subscriber's browser to a specified portal page after successful login. The input format can be "http://www.yahoo.com". The maximum character of the URL Link is 200.

3-2-3-4 Advertisement

The system allow service provider to input 10 URL links for advertisement link purpose.

Figure 3-105 Advertisement Setup

Item	Default	Description
Frequency	One Time Only	One Time Only-One Time Only means to send the advertisement link once after the subscriber Login. Every~Min(s)-The field means to send the advertisement link every interval minutes. The value range is 1 to 60 (minutes).
Sequence	Randomly	Randomly-Display the advertisement page in the random order. Orderly (From 1 to 10) -Display the advertisement page in the order as setting.
Link 1~10	Empty	This function allows the administrator to input ten different websites in the table for advertisement. And these 10 websites will display to the subscribers at random when the subscribers login in the IAC4000 system. The input format can be "http://www.yahoo.com". The maximum character of the URL Link # is 200.

3-2-3-5 Walled Garden

We prepare ten URL links that allows subscriber to access the specific Web pages even they didn't have a username or password. It's free trying and can use for advertisement.

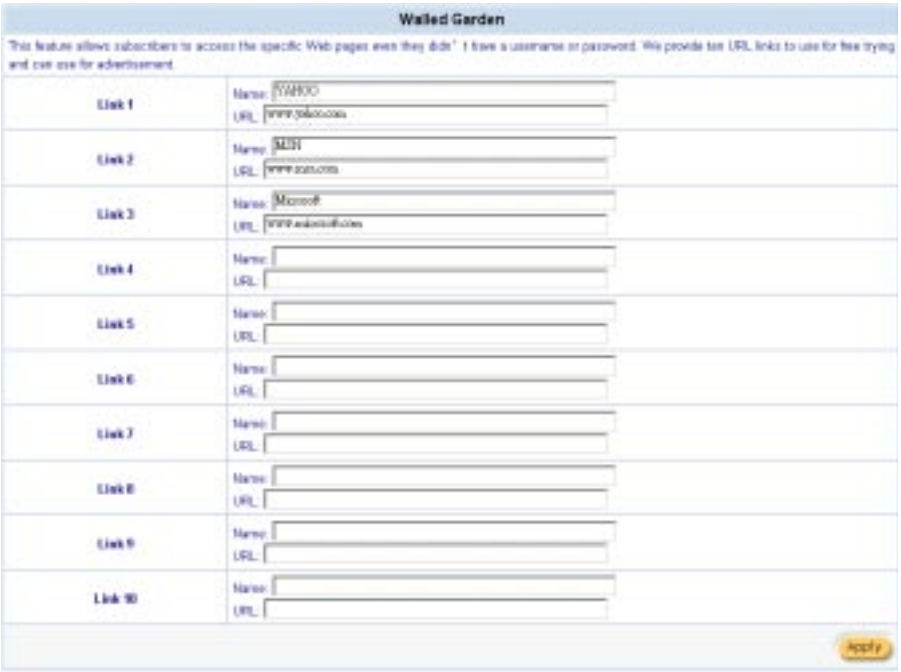


Figure 3-106 Walled Garden

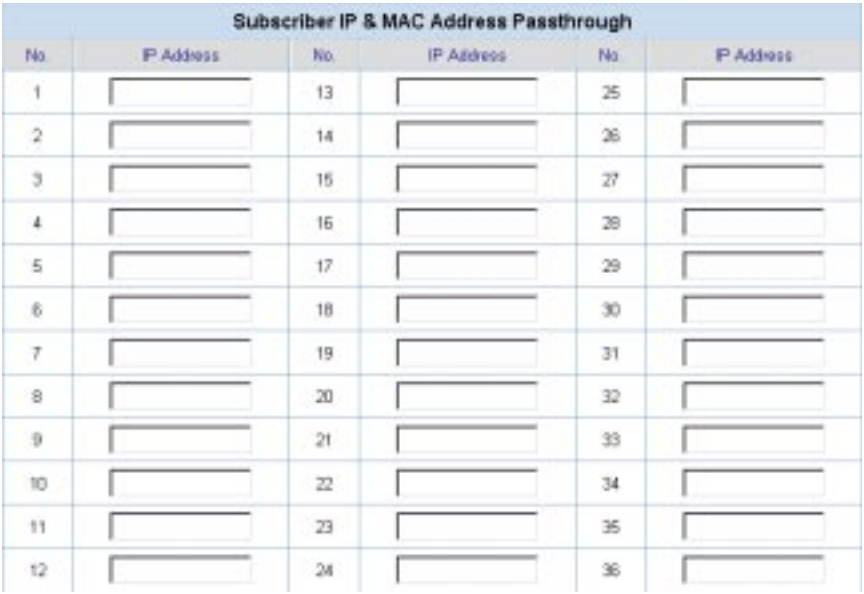
Figure 3-107 Login Page

Item	Description
Name	The name is allowed user to set the prompt string in user customize login page. The maximum allowed characters length is 80.
URL 1~10	The input format can be "http://www.yahoo.com". The maximum character of the Link# is 200.

3-2-3-6 Passthrough

This function allow administrator to set some special devices pass through the IAC4000 system. Because some network devices might be constructed under the IAC4000. However these devices needn't be checked and authorized. The IAC4000 provides a pass through table and the administrator can control which devices can be pass through with authentication.

Subscriber IP Address Pass through



Subscriber IP & MAC Address Passthrough

No.	IP Address	No.	IP Address	No.	IP Address
1		13		25	
2		14		26	
3		15		27	
4		16		28	
5		17		29	
6		18		30	
7		19		31	
8		20		32	
9		21		33	
10		22		34	
11		23		35	
12		24		36	

Figure 3-108 Subscriber IP Address Pass through Setting Screen

Item	Description
IP Address	There are 36 entries can input the pass through source IP Address. For input the IP address, please use this format such like "210.208.122.1".

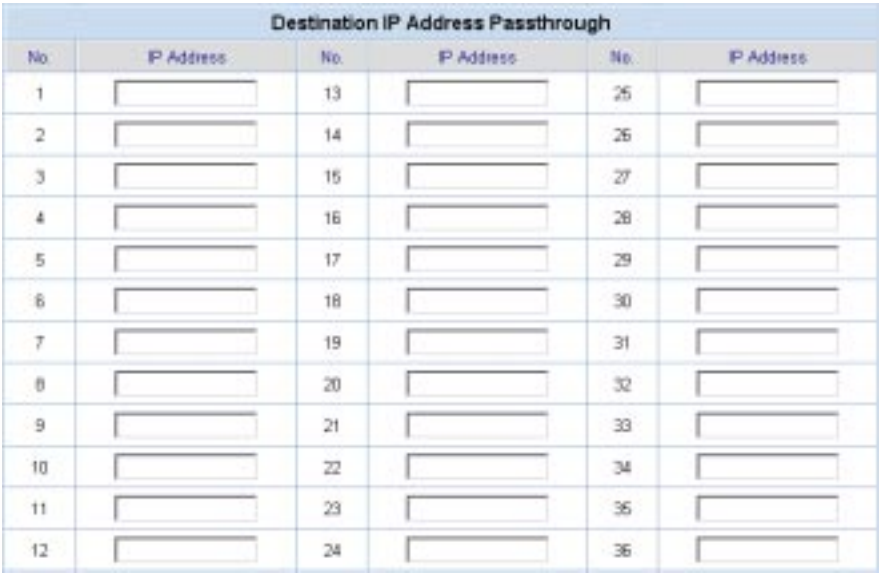
Subscriber MAC Address Pass through

No.	MAC Address	No.	MAC Address	No.	MAC Address
1		11		21	
2		12		22	
3		13		23	
4		14		24	
5		15		25	
6		16		26	
7		17		27	
8		18		28	
9		19		29	
10		20		30	

Figure 3-109 Subscriber MAC Address Pass through Setting Screen

Item	Description
MAC Address	There are 30 entries can input the pass through source MAC Address. For input the source MAC address, please use this format such like" 0050BA8D2296".

Destination IP Address Pass through



Destination IP Address Passthrough					
No.	IP Address	No.	IP Address	No.	IP Address
1		13		25	
2		14		26	
3		15		27	
4		16		28	
5		17		29	
6		18		30	
7		19		31	
8		20		32	
9		21		33	
10		22		34	
11		23		35	
12		24		36	

Figure 3-110 Destination IP Address Pass through

Item	Description
IP Address	There are 36 entries can input the pass through destination IP Address.

Destination URL Pass through

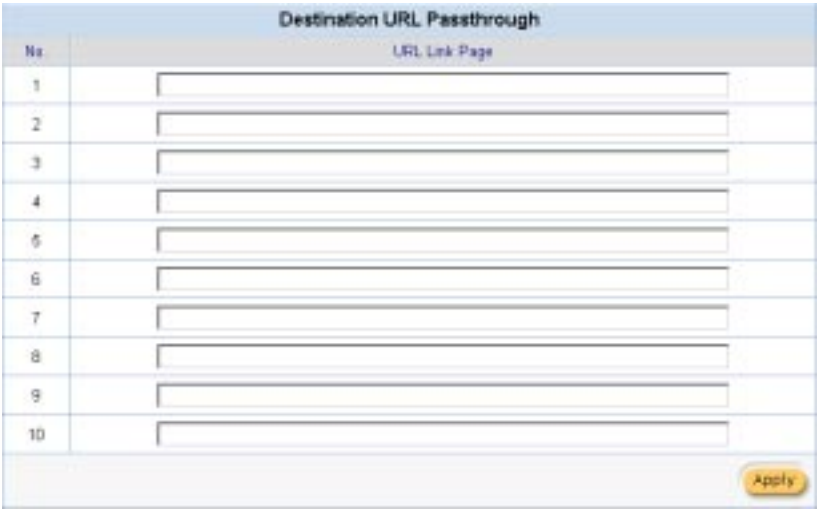


Figure 3-111 Destination URL Pass through Setting Screen

Item	Description
URL Link Page	There are ten entries can input the pass through URL Link Page. For input the URL Link Page, please use this format such like "http://www.yahoo.com". The maximum character of the URL Link Page is 200.

Click Apply button to save the new settings.

3-2-3-7 LAN Devices

Administrator can direct remote control to LAN Devices via the IAC4000 implemented the feature.

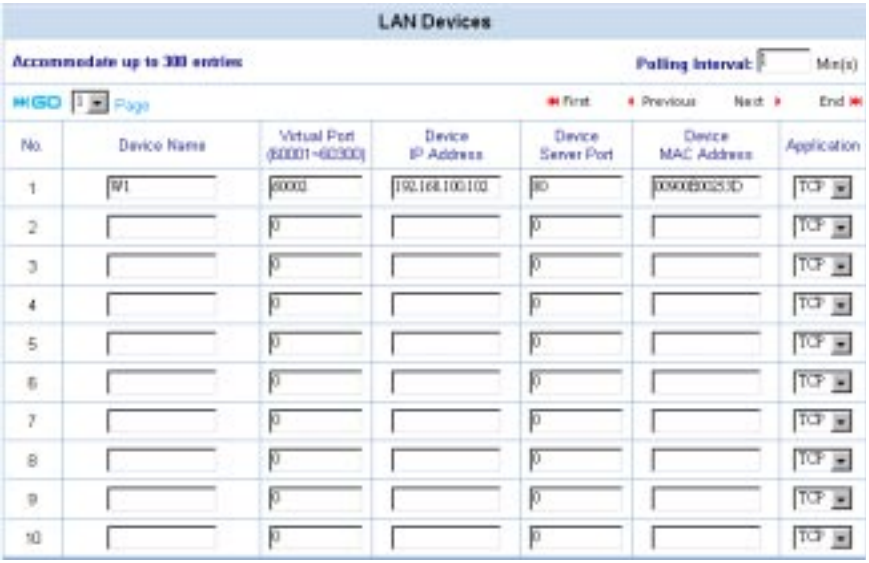


Figure 3-112 LAN Devices Management Screen

Item	Default	Description
Polling Interval	1 Min.	The default value is 1 minute. The Polling Interval valid range is 1 to 1440.
Device Name	Empty	The LAN device name. The maximum character of the device name is 20.
Virtual Port (60001~60300)	0	The virtual port number valid range is 60001 to 60300.
Device IP Address	Empty	The IP address of LAN device.
Device Server Port	0	The server port of LAN device.
Device MAC Address	Empty	The MAC address of LAN device. For input the device MAC address, please use this format such like" 0050BA8D2296".
Application	TCP	The protocol type of LAN device.

Click Apply button to save the new settings.

Click Delete All button to delete all entries.

Note: The system does not support FTP.

3-2-3-8 Static Route

This function allow computers that are connected to the IAC4000 directly or through a switch to communicate with other computers in the respective LAN segment which are connected to the IAC4000 through another router.

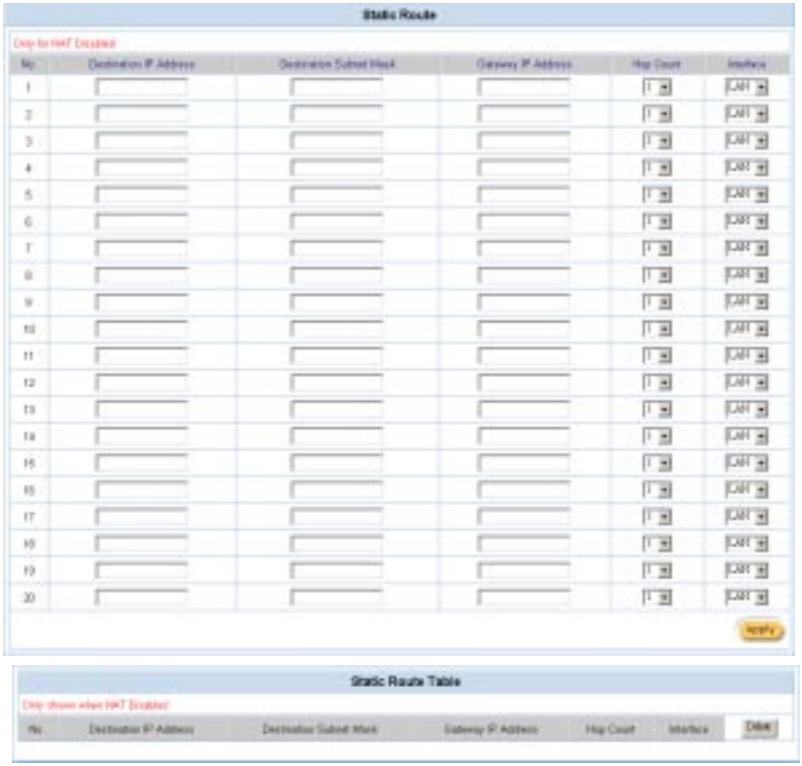


Figure 3-113 Static Route Setting Screen

Item	Default	Description
Destination IP Address	Empty	Enter the target network IP address or host IP address.
Destination Subnet Mask	Empty	Enter the target network subnet mask.
Gateway IP Address	Empty	Enter the IP address of the next hop router.
Hop Count	1	Select the number of the hops.
Interface	LAN	Select the network interface.

Click Apply button to save the new settings.

Click Delete button to delete the entry.

3-2-3-9 Logs

The function allows the device to transmit event messages to a syslog server for monitoring and troubleshooting.

Syslog

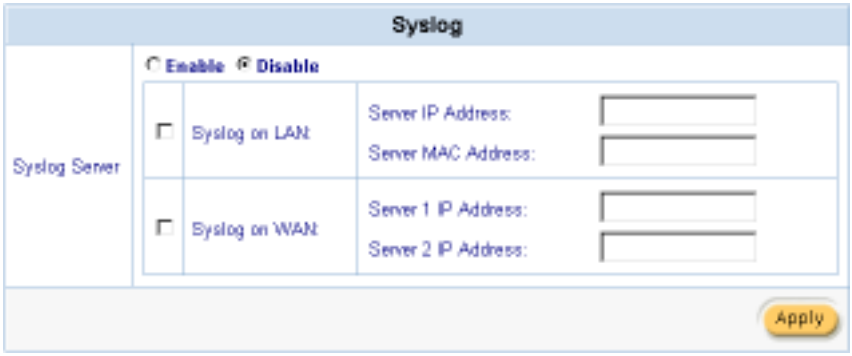


Figure 3-114 Syslog Setting Screen

Item	Default	Description
Syslog	Disable	Enables or disables the syslog server function.
Syslog on LAN		
Server IP Address	Empty	Enter syslog server's IP address. The IAC4000 will send all of its logs to the specified syslog server.
Server MAC Address	Empty	Enter the syslog server's MAC address. The IAC4000 will send all of its logs to the specified syslog server.
Syslog on WAN		
Server 1 IP Address	Empty	Enter IP address of first syslog server.
Server 2 IP Address	Empty	Enter IP address of second syslog server.

Figure 3-115 Logs Setting Screen

Item	Interval Time	Description
System		
System Information	60 minutes 1~10080 Min.	The log included system information would be sent according to specified interval time. Format: (Id, MAC Address) (System Uptime, 0 days 00h:04m:00s) (WAN, FrameTxOK, FrameRxOK, FrameTxError, FrameRxError) (LAN, FrameTxOK, FrameRxOK, FrameTxError, FrameRxError)

Item	Interval Time	Description
System Boot Notice	When system reboot	If device have been rebooted, the log would be send. Format: (Id, MAC Address) (System Up)
System Account Activity Information	When system account login or logout	A log would be sent if System Manager login to or logout from the device. Format: (Id, MAC Address) (System Account Activity Information, Username, User IP, Status) Username: Administrator | Supervisor | Accounting Operator Status: Login | Logout | Idle Time Out
Accounting		
Account Created	When an account is created	A log will be sent once after an account is created. (Id, Mac Address) (Account Create, username, Account usage time, Billing profile information) username: Single account : username Batch account : [prefix, from, to, postfix] Billing profile information: [index, name]
Subscriber Trace	When subscriber logout	A log including subscriber login/logout time will be sent once after subscriber logout. Format: (Id, MAC Address) (Subscriber Trace, username, user IP, user MAC, interface, login time, logout time, RxData count, TxData count) Subscriber Trace: Location | Static | Dynamic
Logged-in Users	60 Minutes	Login user's information will be sent according to specified interval time. Format: (Id, MAC Address) (Logged-in Users, Number of Logged-in users, Start Number, End Number) (Username, user IP, user MAC, interface, login time, RxData count, TxData count) (….)(….)

Item	Interval Time	Description
Billing		
Billing Log	When log created	A log would be sent according to specified interval time. Format: (Id, Mac Address) (Billing Log, Username, Billing profile information, Log time, Usage time, Bill, Charge From) Billing Log: PMS| Dynamic| Static Charge From: PMS | Dynamic Billing profile name: [Name] Log time: 09/06/2002 08:22:25 (example) Usage time: "30 minutes" or "Expire when 00:00" (example) Billing profile information: [index, name]
LAN Devices Management		
LAN Devices Information		60 Minutes 1~10080 Min. A log included current LAN devices status would be sent according to specified interval time. Format: (Id, MAC Address) (LAN Devices Information, Number of devices, Start Number, End number) (Device name, status)(…)(…)
LAN Devices Alarm	When device fail	A log would be sent if one of the LAN devices detected results were "Fail". Format: (Id, MAC Address) (LAN Device Alarm, Device name, FAIL)
Alert		
Administrator access Fail	When someone failed to access the system Web server	A log would be sent when someone failed to access the administration Web server. Format: (Id, MAC Address) (Administration Access Fail, Fail message, User IP, Username)

Item	Interval Time	Description
		Fail message: Bad Username/Password | Unauthorized IP | Exceeded Maximum Login o Unauthorized IP We can't get the username in this situation, so "None" will be displayed. o Exceeded Maximum Login In this situation, we just show the username as below. Administrator | Supervisor | Accounting Operator

3-2-3-10 SNMP

The SNMP Agent Configuration screen enables you to access to your device via Simple Network Management Protocol. If you are not familiar with SNMP, please consult your Network Administrator or consult SNMP reference material. You must first enable SNMP on the SNMP Agent Configuration screen. The IAC4000 allows 5 entries to be set.

Figure 3-116 SNMP Agent Configuration

Item	Default	Description
SNMP	Disable	Disables or enables the SNMP management.
SNMP Port	161	If the SNMP enables, also allowed to specific the SNMP port number via NAT. The allowed SNMP port numbers are 161 (default), 16100-16199 and Trap port numbers are 162 (default), 16200-16299. This Port setting is useful for remote control via NAT network.
Trap Port	162	
Configuration		
Community Name	public/private	Every unit with SNMP enable must be configured to recognize one or more community names up to 20 characters. The default setting for the community of entry 1 is "public" and for the entry 2 is "private" and others are empty.
NMS Address	ANY	The address of the NMS. The default settings for the NMS Networking are "ANY".

Item	Default	Description
Privileges	Read/Write	Choose "Read", "Write", "Trap Recipients" and "All" for different privileges. The default setting of the entry 2 is "write" and others are "read".
Status	Valid/Invalid	Chosen "Valid" or "Invalid". The default setting of entry 1, 2 are valid and others are invalid.

3-2-4 System Status

Display IAC4000 system basic status, including,

1. System
2. Current User List
3. DHCP Clients
4. Session List
5. LAN Devices
6. Billing Log
7. PMS Transaction
8. Static Routing Table

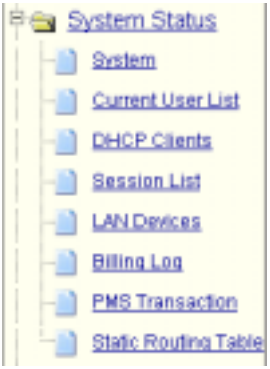


Figure 3-117 System Status Item Screen

Note: After change the settings, please click Apply button to update the new settings.

3-2-4-1 System Status

The System Information Menu displays current system basic information including the host name, LAN, WAN, DHCP Configuration, DNS, E-mail Server, SSL Certificate Information and the system hardware/firmware version number.

System		
System Status	Host Name:	
	Domain Name:	
	Bootrom Version:	1.01
	Firmware Version:	1.01.07
	Concurrent Users Limitation:	1024
	WAN MAC Address:	00:90:0E:00:77:DA
	LAN MAC Address:	00:90:0E:00:77:D9
WAN IP Settings	WAN Port Mode:	Get automatically from a DHCP server
	IP Address:	None
	Subnet Mask:	None
	Default IP Gateway:	None
DNS	Primary DNS Server:	
	Secondary DNS Server:	
DHCP	DHCP Status:	Server
	Start IP Address (Private):	10.59.1.2
	End IP Address (Private):	10.59.1.254
	Lease Time (Private):	1440
E-Mail	Server IP Address:	
SSL Certificate	Country:	00
	State:	Local State
	Local City:	Local City
	Organization:	Local Group
	Organization Unit:	Local Host
	Common Name:	1.1.1.1
	Email Address:	mail@1.1.1.1

Figure 3-118 System Information Screen

3-2-4-2 Current User List

Display the current logged-in subscribers' status. It allow service provider to disconnect any subscribers.

Figure 3-119 Current User Screen-No Authentication

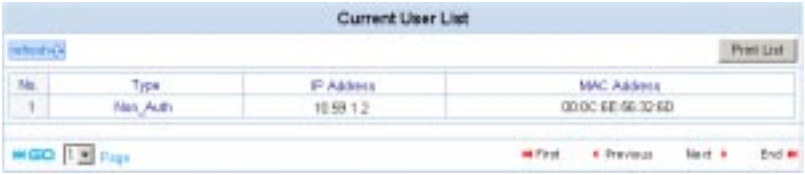


Figure 3-120 Current User Screen-Port Location Mapping

Figure 3-121 Current User Screen-Dynamic Account

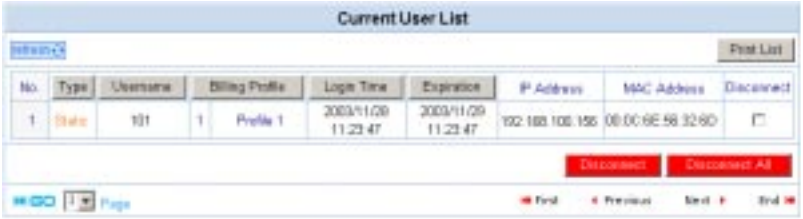


Figure 3-122 Current User Screen-Static Account

Click on refresh button to update the current user list page.

Print the current user list.

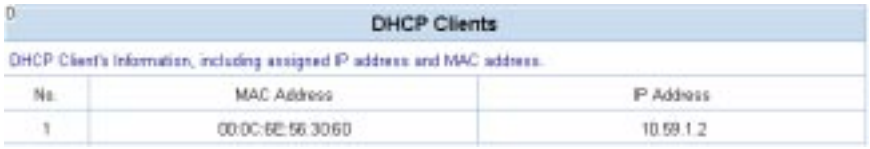
Click the column button to sort the column in ascending/descending order.

Select the check boxes and click 'Disconnect' to disconnect the accounts.

Disconnect all accounts in current user list.

3-2-4-3 DHCP Clients

The DHCP Clients table shows the current DHCP users on the LAN.



DHCP Clients

DHCP Client's Information, including assigned IP address and MAC address.

No.	MAC Address	IP Address
1	00:0C:6E:56:30:60	10.59.1.2

Figure 3-123 Current User Screen

3-2-4-4 Session List

This feature is display the sessions of network events and records or the newest 2048 incoming and outgoing packet information.

Session List

List of sessions of Network events, and records or the newest 2048 incoming and outgoing packet information, including source IP address, destination IP address, and port number.

GO 1 Page First Previous Next End

No.	TCP/UDP	IP Client	Port Client	Port Fake	IP Remote	Port Remote	Idle
1	TCP	192.168.100.184	1191	50012	203.136.232.66	80	51
2	TCP	192.168.100.184	1192	50013	203.136.232.66	80	51
3	TCP	192.168.100.184	1199	50018	207.46.80.139	80	51
4	TCP	192.168.100.184	1201	50020	211.72.253.73	80	51
5	TCP	192.168.100.184	1213	50028	211.72.253.75	80	51
6	TCP	192.168.100.184	1217	50032	203.69.44.140	80	51
7	TCP	192.168.100.184	1219	50034	211.72.253.51	80	51
8	TCP	192.168.100.184	1232	50043	207.68.178.119	80	25
9	TCP	192.168.100.184	1247	50058	61.120.150.15	80	25
10	TCP	192.168.100.184	1250	50059	63.240.15.5	80	25

GO 1 Page First Previous Next End

Figure 3-124 Session List Screen

3-2-4-5 LAN Devices Status

You can manage all devices by clicking on device name to access device's Web-based interface.

LAN Devices Status

We detect below listed devices to check if alive every **1 min**.
You can manage below listed devices by clicking device name to access its Web-based UI.

NO.	Device Name	Status	Virtual Port (60001~60300)	Device IP Address	Device Server Port	Device MAC Address	Application
1	W1	OK	60002	192.168.100.102	80	00:90:0E:00:25:3D	TCP

Figure 3-125 LAN Devices Status Screen

Figure 3-126 Example- W1 LAN Device Management Screen

3-2-4-6 Billing Log

This allows you to manage guest connection status.

Billing Log

refresh | Export to Txt File | Clear Log

No.	Username/Location	Billing Profile	Log Time	Usage Time	Bill	Charge from
1	101	Profile 1	2003/11/28 10:09:18	1 day(s)	10.00	PMS
2	101	Profile 1	2003/11/28 10:24:58	1 day(s)	10.00	Static
3	b3rg3557	Profile 1	2003/11/28 10:28:57	1 day(s)	10.00	Dynamic
4	8y4dm39	Profile 1	2003/11/28 10:33:39	1 day(s)	10.00	Dynamic
5	gcwu3842	Profile 3	2003/11/28 10:33:42	6 hour(s)	4.00	Dynamic
6	tmg2wn45	Profile 2	2003/11/28 10:33:45	1 hour(s)	0.80	Dynamic
7	x85m248	Profile 4	2003/11/28 10:33:48	1 minute(s)	0.00	Dynamic
8	b4e5552	Profile 1	2003/11/28 10:33:51	1 day(s)	10.00	Dynamic
9	7spct855	Profile 2	2003/11/28 10:33:55	1 hour(s)	0.80	Dynamic
10	48tz3j68	Profile 2	2003/11/28 10:33:58	1 hour(s)	0.80	Dynamic
11	102	Profile 1	2003/11/28 10:48:48	1 day(s)	10.00	PMS
12	101	Profile 1	2003/11/28 11:23:47	1 day(s)	10.00	Static

GO 1 Page | First | Previous | Next | End

Figure 3-127 Billing Logs Screen

Click on refresh button to update the Billing Log page.

This allow you to export the billing logs to a text file format. (bill_log.txt)

Click on Clear Log to remove all billing log entries.

Click the column button to sort the column in ascending/descending order.

3-2-4-7 PMS Transaction Log

This function allow administrator to monitor the usage status of PMS system.

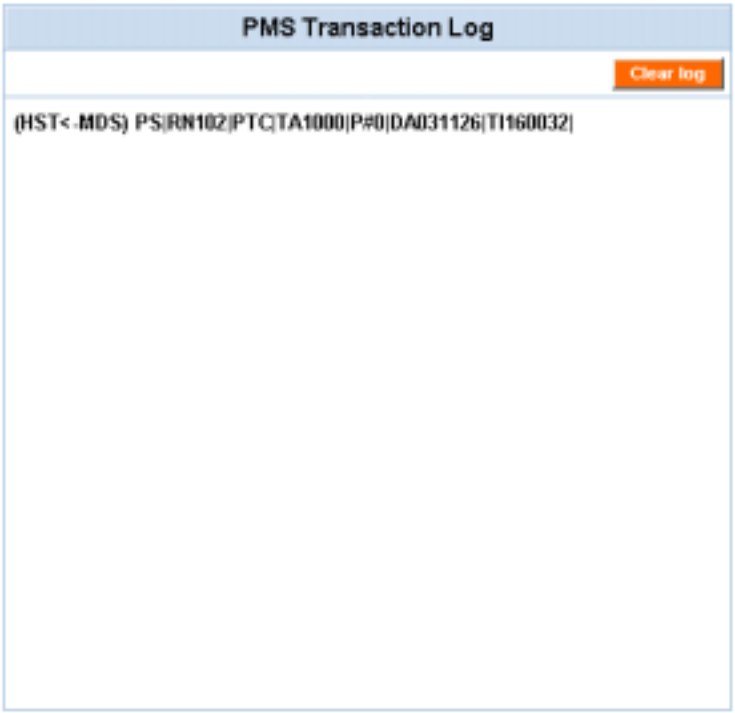


Figure 3-128 PMS Transaction Logs Screen

Click on Clear log to remove all PMS Transaction log entries.

3-2-4-8 Static Route Table

The Static Routing Table lists the routes through which all recognized Ethernet networks.

Static Route Table

Only shown when NAT Disabled

No.	Destination IP Address	Destination Subnet Mask	Gateway IP Address	Hop Count	Interface
1	192.168.100.1	255.255.255.0	192.168.100.254	1	WAN

Figure 3-129 Static Route Table

3-2-5 System Tools

This allows service provider or administrator to process Firmware upgrade, change password and backup or restore configuration.

1. Configuration
2. Firmware
3. System Account
4. SSL Certificate
5. Restart
6. Logout

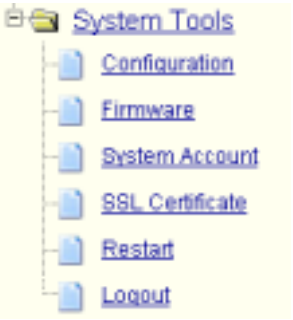


Figure 3-130 System Tools Item Screen

3-2-5-1 Configuration

Use the Configuration item to save, restore or reset configuration parameters of the IAC4000.

Figure 3-131 Configuration Setting Screen

Item	Default	Description
Backup		Click it to save the system configuration to your computer. (sys_conf.txt)
TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
Text File Name	Empty	Enter the file name in the Text File Name field.
Restore		Click it to restore your system configuration.
File Path	Empty	Enter the file pathname of the system configuration file in the file path field.
TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
Text File Name	Empty	Enter the file name in the Text File Name field.
Reset the system back to	factory defaults	Erase all setting and back to factory setting.
Keep subscriber profile	Disable	Click the keep subscriber profile to change all the parameters into factory setting but still reserve the subscriber profiles.
Keep port-location mapping profile	Disable	Click the keep port-location mapping profile to change all the parameters into factory setting but still reserve the port-location mapping profiles.

3-2-5-2 Firmware Upgrade

The Firmware Upgrade menu loads updated firmware to be permanent in flash ROM. The download file should be a binary file from factory; otherwise the agent will not accept it. After downloading the new firmware, the agent will automatically restart it.

Manual Firmware Upgrade

Figure 3-132 Manual Firmware Upgrade Setting Screen

Item	Default	Description
This allows the administrator to upgrade the firmware via HTTP.		
Local PC File Path	Empty	Enter the file name and location in the Local PC File Path field.
This allows administrator use TFTP server to upgrade firmware.		
TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
Binary File Name	Empty	Enter the file name in the Binary File Name field.

Note: Before downloading the new firmware, users must save the configuration file for restore configuration parameters of the device.

Scheduled Firmware Upgrade

Scheduled Firmware Upgrade is a program that enables an automatic upgrade to the latest firmware version through the TFTP server.

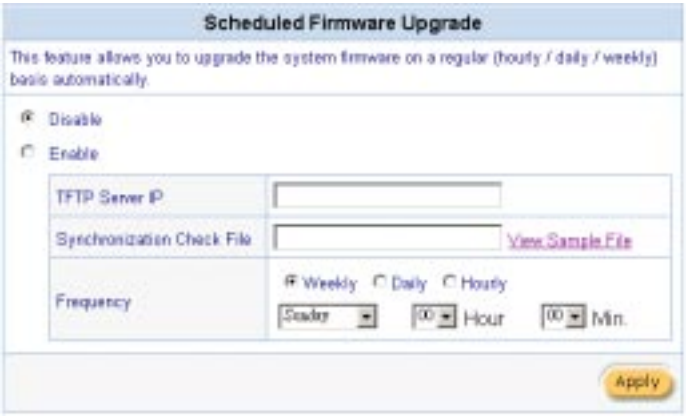


Figure 3-133 Scheduled Firmware Upgrade Setting Screen

Item	Default	Description
Disable/Enable		Disables or enables the scheduled firmware upgrade function.
TFTP Server IP	Empty	The IP address of TFTP Server.
Synchronization Check File	Empty	The new firmware file.
Frequency	Weekly	The default value is "Weekly".

3-2-5-3 System Account

Use the System Account screen to change the system accounts.

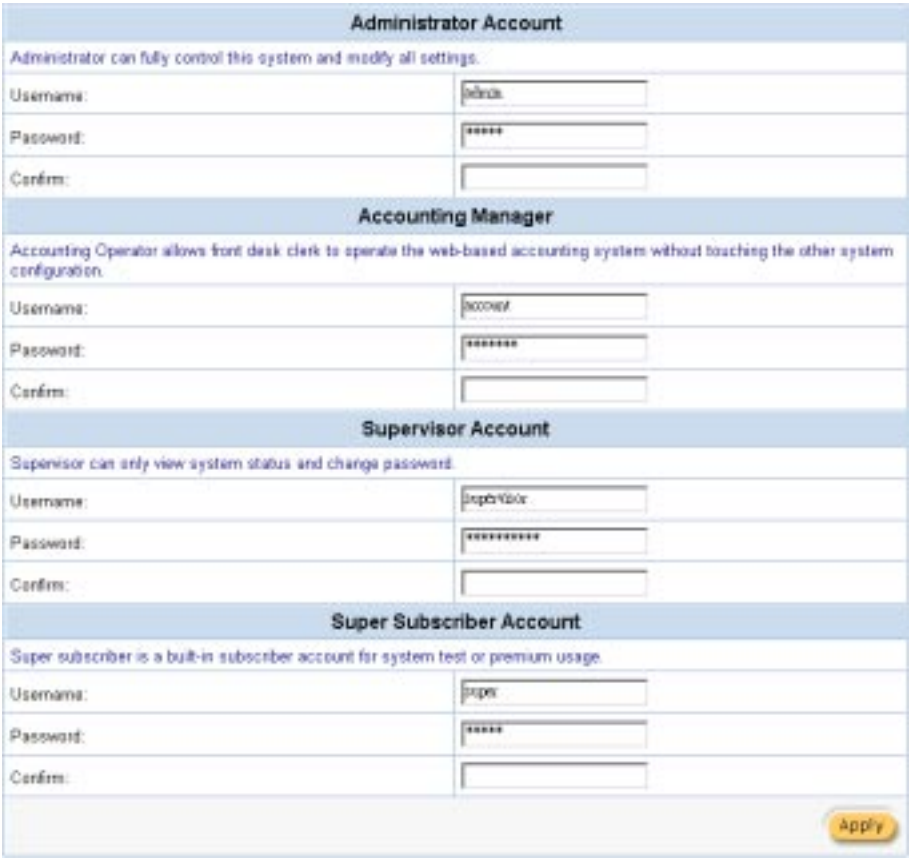


Figure 3-134 System Account Setting Screen

Item	Description
Username	The username can consist of up to 20 alphanumeric characters and is sensitive.
Password	The password can consist of up to 20 alphanumeric characters and is sensitive.
Confirm	The password for confirmation.

Administrator Account

Step 1: Start your Web browser and enter the factory default IP address 10.59.1.1 in your browser's location box. Press Enter.

Figure 3-135 Web Browser Location Field (Factory Default)

Step 2: The IAC4000 configuration main menu will appear. Enter "admin" (default) as the Username and "admin" (default) as the password and click "Get Started"

Figure 3-136 Administrator Account Login Screen

Step 3: After a valid user name and password have been provided, the IAC4000 configuration homepage will appear.

Figure 3-137 System Setting Screen

Step 1: Start your Web browser and enter the factory default IP address 10.59.1.1 in your browser's location box. Press Enter.

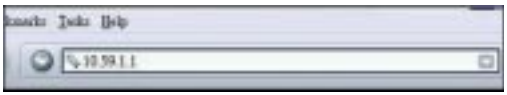


Figure 3-138 Web Browser Location Field (Factory Default)

Step 2: The IAC4000 configuration main menu will appear. Enter "account" as the Username and "account" as the password and click "Get Started".

Figure 3-139 Web-Based Accounting Login Screen

Step 3: After a valid user name and password have been provided, the account operator homepage will appear.

Figure 3-140 Static Account Operator Screen

Or

Figure 3-141 Dynamic Account Operator Screen

Supervisor Account

Step 1: Start your Web browser and enter the factory default IP address 10.59.1.1 in your browser's location box. Press Enter.

Figure 3-142 Web Browser Location Field (Factory Default)

Step 2: The IAC4000 configuration main menu will appear. Enter "supervisor" as the Username and "supervisor" as the password and click "Get Started".

Figure 3-143 Supervisor Account Login Screen

Step 3: After a valid user name and password have been provided, the IAC4000 configuration homepage will appear.

Figure 3-144 System Status & System Tools Setting Screen

Super Subscriber Account

Start your Web Browser; a subscriber login page will appear. Enter "super" as the Username and "super" as the password and click "Enter", you can use Internet now.

Figure 3-145 Super Subscriber Login Page

3-2-5-4 SSL Certificate

The function allows you to download the registered CA certificate into the IAC4000.

Figure 3-146 SSL Certificate Download Setting Screen

Note: The password field must the same as the CA's registered password.

3-2-5-5 Restart

If your IAC4000 is not operating correctly, you can choose this option to display the restart IAC4000 screen. Clicking the apply button restart the IAC4000, with all of your settings remaining intact.

Figure 3-147 Default Settings Screen

3-2-5-6 Logout

If you would like to leave the configuration page, please click apply to exit.

Figure 3-148 Logout Setting Screen

Appendix A. DHCP Private/Public IP Pool Setup

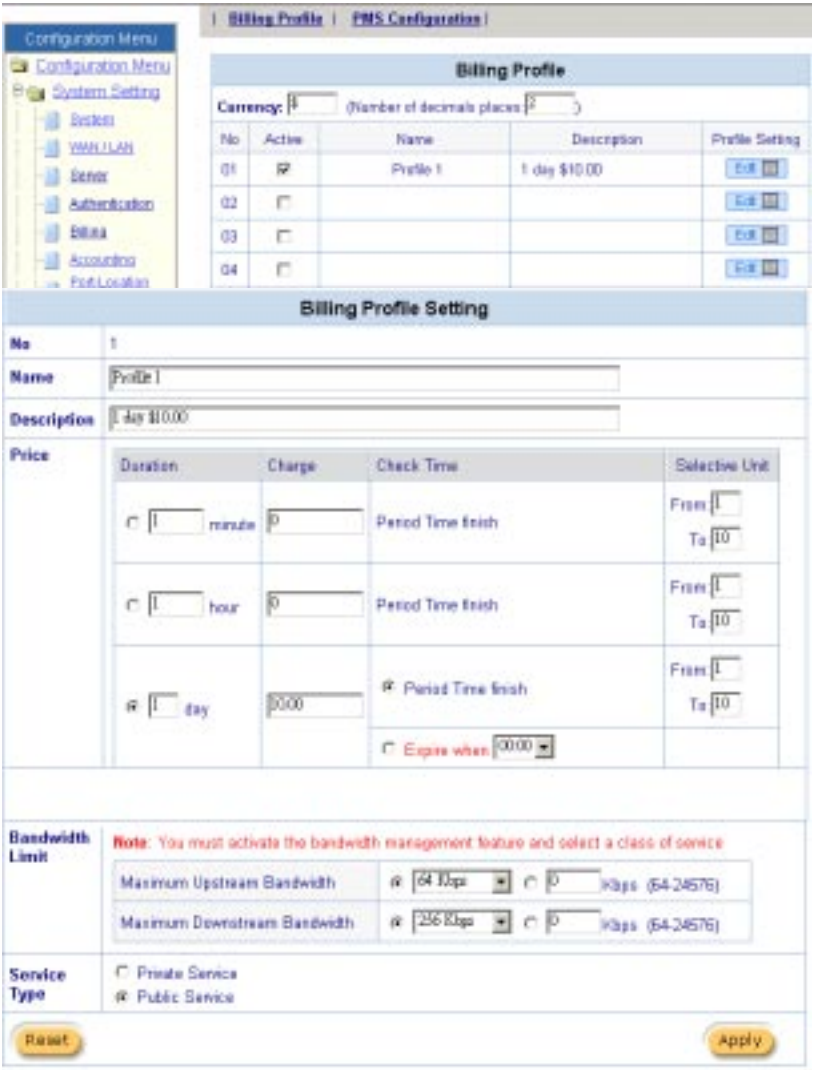
Step 1: Setup the WAN configuration

Step 2: In the Authentication Configuration screen, select Built-in Authentication and Scenario type (A/B/C).

Step 3: In the Server screen, select DHCP server (Private) and enable DHCP Server (Public). Enter IP Pool Starting Address, Pool Size, and lease time (Public).

Note: IP Pool Starting Address (public) must be configured into the same subnet with WAN port.

Step 4: Define Billing Profile. Select one service type, Public or Private Service.



Step 5: Connect client PC (DHCP client) to LAN port.

Use Public IP (Billing Profile'Service Type=Public Service)

1. Power on computer A (DHCP Client), computer A will request an IP address.
2. The device's DHCP Server (Private) will assign a Private IP to computer A with temporal lease time e.g. 5 min. (which is configurable in UI)
3. Open computer A's Web browser. After 2.5 min, computer A will request again an IP (because lease time), at this time IAC4000 will assign "Public IP" e.g. 211.21.1.2 to computer A with lease time ="Lease time (Public)"
4. From this moment computer A will use the assigned Public IP to sent the packet, and IAC4000 will route the packet to internet without doing "NAT"

Use Private IP (Billing Profile'Service Type=Private Service)

1. Power on the computer B (DHCP Client), computer B will request an IP address.
2. The device's DHCP Server (Private) will assign a Private IP to computer B with temporal lease time e.g. 5 min. (which is configurable in UI).
3. Open computer B's Web browser. After 2.5 min, computer B will request again an IP (because lease time), at this time IAC4000 will assign "Private IP" e.g. 10.59.1.2 to computer B with lease time ="Lease time (Private)"
4. From this moment computer B will use the assigned Public IP to send the packet, and IAC4000 will route the packet to internet with "NAT".

Appendix B. Use RADIUS server to setup your Internet Service

IAC4000 supports Remote Authentication Dial-In user Service (RADIUS). RADIUS is an authentication and accounting system used by many Internet Service Providers. By integrating RADIUS with the IAC4000, service provider could store in the RADIUS database the valid usage time each subscriber is allocated. For example, when subscriber logs in, the RADIUS server will send the IAC4000 the usage time parameters (session time-out) and IAC4000 will obey them to control the connection from subscribers.

IAC4000's RADIUS functionality also includes an accounting feature that allows the IAC4000 to post "accounting start" and "accounting stop" records to RADIUS server. Service provider can use these records to accurately track the usage on their network.

IAC4000 provides two accounting types to service providers. "Accumulate" and "Time to finish".

Accumulate

Case 1: RADIUS Server will reply "Session time-out" attribute

Service providers create a subscriber account with a "session timeout" parameter. For example, "Session Timeout"=2 hours account was created and assign to subscriber. When subscriber login, system will send an "Access Request" attribute to Radius Server, if subscriber's account is a valid account, Radius Server will reply "Access Accept" with "session timeout". System will send a "logout Window" include logout button and countdown time start from 2:00:00 to subscriber's browser. Now subscriber could use the service for 2 hours, after 2 hours system will disconnect subscriber's connection automatically. However, if after login 30 minutes subscriber press logout button, system will terminate the connection with subscriber and send "Accounting Stop" include used time=1800 sec. to Radius Server. For next time subscriber login, an "Information Window" include logout button and countdown time start from 1:30:00 will appear again.

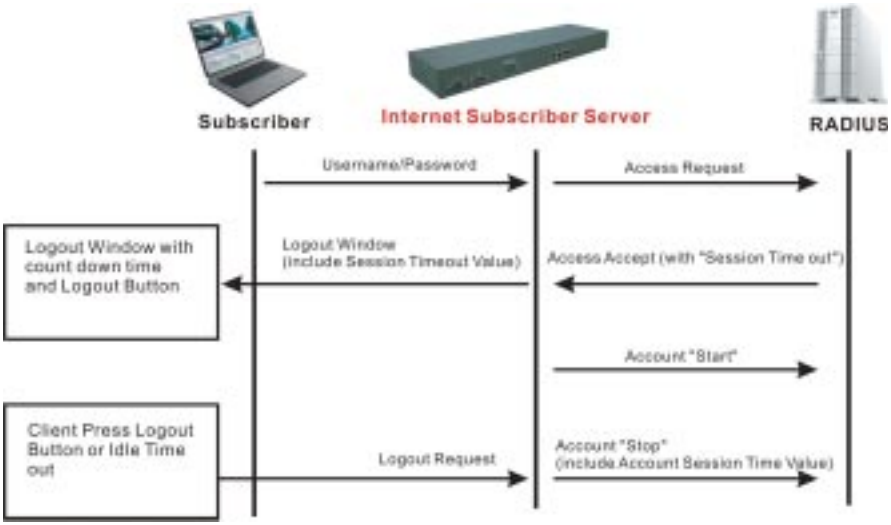


Figure A-1 Accumulate (with Session Time Out)

Figure A-2 Information Window

Case 2: RADIUS Server do not reply "Session timeout" attribute

Service providers create a subscriber account without a "session timeout" parameter. When subscriber logs in, system will send an "Access Request" attribute to Radius Server, if subscriber's account is a valid account, RADIUS Server will reply "Access Accept" but no "session timeout". System will send a "logout Window" include logout button and connect time start from 0:00:00 to subscriber's browser. Now subscriber could use the service until his click logout button. When subscriber press logout button, system will terminate the connection with subscriber and send "Accounting Stop" include used time for example 1800 sec. to RADIUS Server. RADIUS Server will use these records to accurately track the usage on their network.

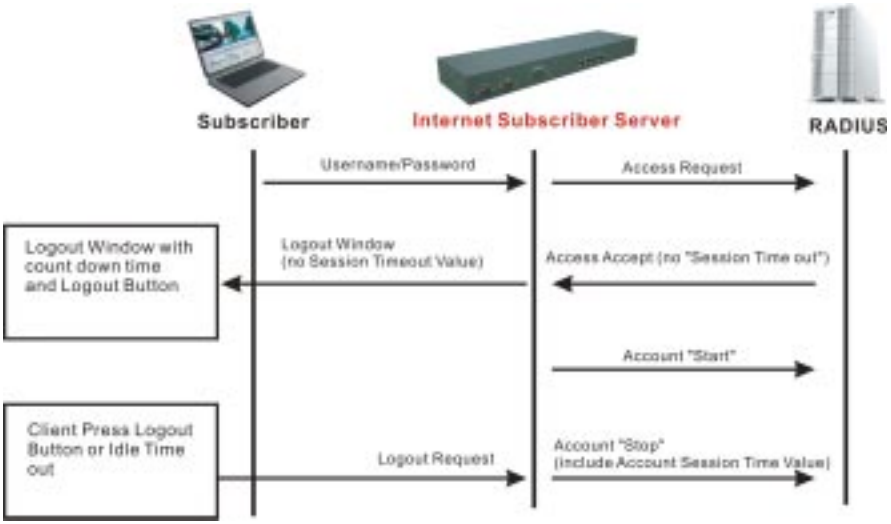


Figure A-3 Accumulate (Without Session Time Out)

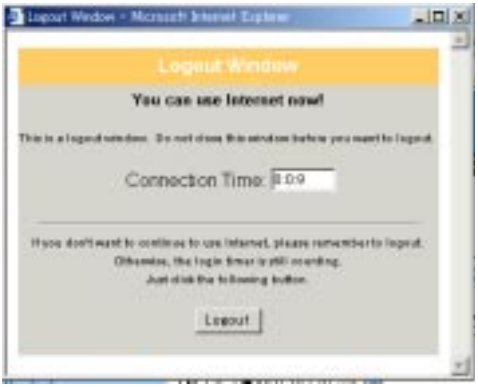


Figure A-4 Information Window

Time to Finish

Service providers create a subscriber account with a "session timeout" parameter. For example, "Session Timeout"=2 hours account was created and assign to subscriber. When subscriber login, system will send an "Access Request" attribute to RADIUS Server, if subscriber's account is a valid account, RADIUS Server will reply "Access Accept" with "session timeout". System will send a "logout Window" only has countdown time start from 2:00:00 but no Logout Button to subscriber's browser. Now subscriber could use the service for 2 hours, after 2 hours system will disconnect subscriber's connection automatically. However, subscriber is not allowed to logout manually. When system terminate the connection with subscriber at the same time it will send "Accounting Stop" include used time=7200 sec. to Radius Server. This is to say that this account only allowed for one time use.

Note: If "Time to finish" is selected, but RADIUS Server do not reply "Session Timeout", an error message "No Session Time out" will pop up on subscriber's browser.

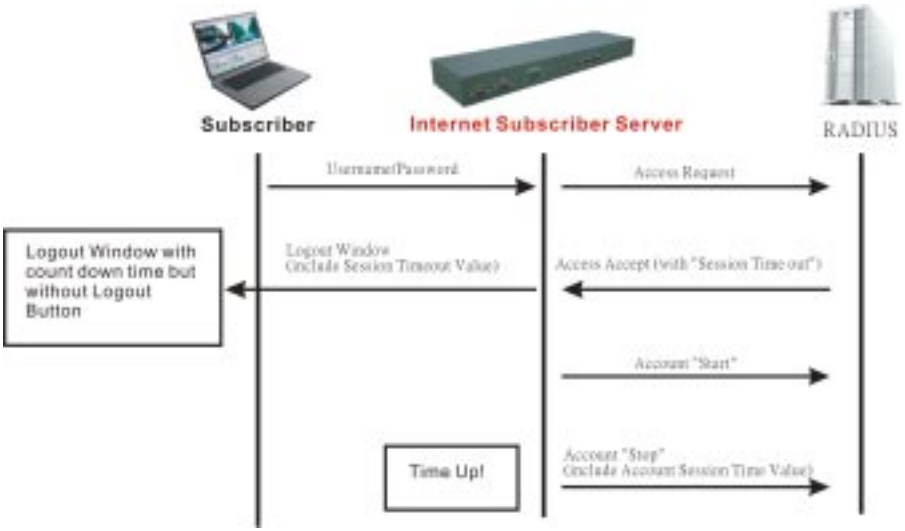


Figure A-5 Time to Finish

Figure A-6 Logout Window

Appendix C. Ethernet Cable Connections

This cable information is provided for your reference only. Please ensure you only connect the appropriate cable into the correct socket on either this product or your computer.

If you are unsure about which cable to use or which socket to connect it to, please refer to the hardware installation section in this manual. If you are still not sure about cable connections, please contact a professional computer technician or NetComm for further advice.

RJ-45 Ethernet Network Ports

RJ-45 Network Ports can connect any networking devices that use a standard LAN interface, such as a Hub/Switch Hub or Router. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable to connect the networking device to the RJ-45 Ethernet port. Depending on the type of connection, 10Mbps or 100Mbps, use the following Ethernet cable, as prescribed.

RJ-45 plug attached to cable

Caution: Please do not use telephone cables. Telephone cables do not support Ethernet or Fast Ethernet

Ethernet Type	Cable Requirements	Maximum Length
10BASE-T	Category 3 or better, UTP or STP	100 metres
100BASE-TX	Category 5 or better, UTP or STP	100 metres

Twisted-pair cabling comes in various grades, or categories. Category 5 is required for Fast Ethernet, and is also the most reliable and most commonly used category. You can buy UTP Category 5 (Unshielded Twisted Pair) Ethernet cabling in precrimped lengths, or you can crimp your own. Crimping your own can result in faulty connections if the RJ-45 tips are not attached properly. Precrimped Category 5 cabling is available at most computer retail stores.

The most reliable and commonly used type of Category 5 cabling used is UTP, or "unshielded twisted pair." STP, or "shielded twisted pair" wiring is only necessary for network environments exposed to excessive amounts of electromagnetic interference, or EMI. These environments include areas with high sources of electrical power, air conditioning, generators, and radio signals.

STP is also used for wiring outdoors.

There are two types of the wiring: Straight-Through Cables and Crossover Cables. Category 5 UTP/STP cable has eight wires inside the sheath. The wires form four pairs. Straight-Through Cables has same pinouts at both ends while Crossover Cables has a different pin arrangement at each end.

In a straight-through cable, wires 1,2,3,4,5,6,7 and 8 at one end of the cable are still wires 1~8 at the other end. In a crossover cable, the wires of 1,2,3,6 are reversed so that wire 1 become 3 at the other end of the cable, 2 becomes 6, and so forth.

To determine which wire is wire 1, hold the RJ-45 cable tip with the spring clip facing towards the ground and the end pointing away from you. The copper wires exposed upwards to your view. The first wire on the far left is wire 1. You can also refer to the illustrations and charts of the internal wiring on the following page.

Straight-Through Cabling

Wire	Becomes
1	1
2	2
3	3
6	6

Cross-Over Cabling

Wire	Becomes
1	3
2	6
3	1
6	2

Note: To prevent loss of signal, make sure that the length of any twisted-pair connection does not exceed 100 metres.

RJ-45 Connector Pin Assignment	Normal Assignment
1	Input Receive Data +
2	Input Receive Data -
3	Output Transmit Data +
6	Output Transmit Data -
4,5,7,8	Power - PoE pins

Appendix D. Registering your NetComm Product

All NetComm Limited ("NetComm") products have a standard 12 month warranty from date of purchase against defects in manufacturing and that the products will operate in accordance with the specifications outlined in the User Guide. However some products have an extended warranty option (please refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at:

www.netcomm.com.au

Contact Information

If you have any technical difficulties with your product, please do not hesitate to contact NetComm's Customer Support Department.

Email: support@netcomm.com.au

Fax: (+612) 9424-2010

Web: www.netcomm.com.au

Legal & Regulatory Information

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

NetComm is a registered trademark of NetComm Limited.

All other trademarks are acknowledged the property of their respective owners.

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

(1) This unit shall be connected to the Telecommunication Network through a line cord which neets the requirements of the ACA TS008 Standard.

(2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:

- Change the direction or relocate the receiving antenna.
- Increase the separation between this equipment and the receiver.
- Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
- Consult an experienced radio/TV technician for help.

(3) The power supply that is provided with this unit is only intented for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at www.netcomm.com.au.

NetComm reserves the right to request proof of purchase upon any warranty claim.