



IAC4500

Internet Access Controller

Safety and Precaution

Installation

- Use only the type of power source indicated on the marking labels.
- Use only power adapter supplied with the product.
- Do not overload wall outlet or extension cords as this may increase the risk of electric shock or fire. If the power cord is frayed, replace it with a new one.
- Proper ventilation is necessary to prevent the product overheating. Do not block or cover the slots and openings on the device, which are intended for ventilation and proper operation. It is recommended to mount the product with a stack.
- Do not place the product near any source of heat or expose it to direct sunlight.
- Do not expose the product to moisture. Never spill any liquid on the product.
- Do not attempt to connect with any computer accessory or electronic product without instructions from qualified service personnel. This may result in risk of electronic shock or fire.
- Do not place this product on unstable stand or table.

When in Use

- Power off and unplug this product from the wall outlet when it is not in use or before cleaning. Pay attention to the temperature of the power adapter. The temperature might be high.
- After powering off the product, power on the product at least 15 seconds later.
- Do not block the ventilating openings of this product.
- When the product is expected to be not in use for a period of time, unplug the power cord of the product to prevent it from the damage of storm or sudden increases in rating.

Service

Do not attempt to disassemble or open covers of this unit by yourself. Nor should you attempt to service the product yourself, which may void the user's authority to operate it. Contact qualified service personnel under the following conditions:

- If the power cord or plug is damaged or frayed.
- If liquid has been spilled into the product.
- If the product has been exposed to rain or water.
- If the product does not operate normally when the operating instructions are followed.
- If the product has been dropped or the cabinet has been damaged.
- If the product exhibits a distinct change in performance.

Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Copyright Notice

- * 2005 All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of the seller.

Disclaimer

Information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. The seller therefore assumes no responsibility and shall have no liability of any kind arising from the supply or use of this document or the material contained herein.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, the seller reserves the right to make changes to the products described in this document without notice.

The seller does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Trademarks

All other product or service names mentioned in this document may be trademarks of the companies with which they are associated.

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 IAC4500	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 IAC4500 Internet Access Controller is a freestanding or rack-mounted intelligent gateway with two serial ports for system management and PMS. It provides plug and play instant Internet access, advanced security & network management. The IAC4500 Internet Access Controller is designed for service providers and system integrators to enhance service performance and increase business exposure and cooperative business operation.

The IAC4500 - Internet Access Controller is an ideal solution for hotels, coffee shops, airports, conference facilities and other sites that commonly host business travellers, and offers instant high-speed Internet connections without requiring user configuration to connect to the facility's network with no extra MIS resource needed.

The Internet Access Controller helps solve connectivity problems by offering instant Internet access with no settings to change; user's laptop settings are static IP or http proxy with no subnets or gateways to negotiate to properly configure a user's laptop for the facility's network. Users simply plug into the network and they are immediately connected.

With its PMS interface, the IAC4500 - Internet Access Controller can be easily integrated with a service providers billing system, or with a PMS to help to provide an Internet access service. The built-in AAA (Authentication / Accounting / Authorization) and Billing mechanism provides the hotspot operator with a complete AAA solution.



Figure 1-1 IAC4500 Internet Subscriber Server

1-1 Package Contents

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



Figure 1-2 IAC4500 Internet Subscriber Server

- One IAC4500 Internet Access Controller
- One Power Cord
- One CD containing a User's Guide and MIB file
- A rack-mounting kit which includes two rack-mounting brackets and six mounting screws
- Four Rubber Foot Pads
- One RS-232 console cable

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

1-2 Features

Integrated Solution for rapid deployment

The IAC4500 Internet Access Controller is a complete access controller for medium to large hotspots. It can serve up to 1024 simultaneous users and is an ideal hotspot solution to be deployed in hotels, coffee shops, airports and other sites that commonly host business travellers to offer instant high speed Internet connections.

Deliver instant PnP connectivity service

With its IP Plug and Play technology, the IAC4500 Internet Access Controller helps solve connectivity problems by offering instant Internet access without the need for configuration changes to the clients computer or any client-side software, and it allows guests to send E-mail as usual without changing their SMTP server settings, even if their configured SMTP server is behind a corporate firewall.

Complete user authentication and accounting

The IAC4500 Internet Access Controller works with either no authentication, built-in authentication or RADIUS authentication).

Sophisticated Remote Management

The IAC4500 Internet Access Controller enables service operators to manage the device with Web UI, Syslog messaging, E-mail messaging, SNMP and LAN Device Management remotely.

Comprehensive security

The IAC4500 Internet Access Controller provides a fully secured operating environment with VPN pass through, SSL certificate, SSL login page and SSL configuration page.

Enhance Local and Personalized Service

The login and logout pages are fully customisable. The IAC4500 Internet Access Controller has the ability to let the operator redirect end users to an advertising web page, increasing operator potential for revenue through affiliation marketing. The IAC4500 can also allow a list of up to 10 pages that end users can visit free through the walled garden feature.

Hotel PMS System Support

The IAC4500 Internet Access Controller works with Hotel's PMS billing systems to integrate the Internet access charges and the room charge into one bill. This keeps staff training and interaction to provide the internet access to a minimum

Proprietary AAA/Billing System

The IAC4500 Internet Access Controller has proprietary AAA and billing system that allows the operator to control the Internet access and billing mechanism individually without any external authentication server or billing server. The internal AAA engine will allocate user names and passwords and will monitor usage and control users as a stand alone device.

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
- SMTP Server Redirection
- DHCP Server / Relay
- IP Multicast support
- NAT (RFC 1631)
- NTP Server Support

AAA

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

Billing

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

Security

- Layer 2 Isolation
- SSL Secure User Login Process
- SSL Secure Web-based administration
- VPN Pass through (IPSec/PPTP)
- PPTP client for secure remote access and RADIUS communication

Management

- Web-based Management
- HTTP/TFTP Firmware Upgrade
- Authorised remote Management
- Backup/Restore Configuration
- Scheduled Firmware Upgrade
- Real-time Current User List/ DHCP Clients List/ Session List/ Account List
- LAN Device Management
- Syslog
- SNMP

Local Service

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

PMS Billing System

- Supports Micros Fidelio, Marriott and Hilton
- PMS Transaction Logs
- Support 802.1Q Tag-based VLAN infrastructure

Interface

- One WAN Port (IEEE 802.3/802.3u 10BaseT/100BaseTX) supports Auto crossover
- One LAN Ports (IEEE 802.3/802.3u 10BaseT/100BaseTX) supports Auto crossover
- DB9 Serial Port: Console setting or 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 B
- CE Class B
- VCCI Class B
- CSA
- C-Tick
- RoHS Compliance

Power Requirement

- Internal universal switching power supply
- 100-240 VAC, 50/60 Hz
- Power Consumption: <9W

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 wet locations.
- Use only the original power cord otherwise there is a danger of severe shock.
- Avoid exposing the IAC4500 to direct sunlight or another heat source.
- Choose a well-ventilated area to position your IAC4500.

1-5 Overview

1-5-1 Front Panel



Figure 1-3 IAC4500 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. Data transmission cable to a PMS system.
Reset Button	The Internet Access Controller has a reset button at the front panel.
LAN Port	The port can be auto-switched to MDI-II connections. The LAN port is used for linking host or other network devices. The port can be either connected to 100BaseTX network or 10BaseT network. When connecting to a 100BaseTX network, the port operates 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.
WAN Port	One Ethernet port used for linking xDSL or Cable Modem.

LEDs Indication

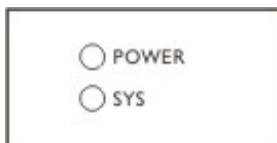


Figure 1-4 LEDs

LED	State	Description
Power	Off	The Internet Access Controller is not receiving electrical power.
	Green	The Internet Access Controller is receiving electrical power.
SYS	Off	The Internet Access Controller is operating normally.
	Green	The Internet Access Controller has just been started up.
	Green (Blinking)	The Internet Access Controller is abnormal.
WAN		
10M	Green	The WAN port is operating at 10Mbps.
	Green (Blinking)	The WAN port is receiving or transmitting data.
	Off	No device is attached.
100M	Yellow	The WAN port is operating at 100Mbps.
	Yellow (Blinking)	The WAN port is receiving or transmitting data
	Off	No device is attached.
LAN		
10M	Green	The LAN port is operating at 10Mbps.
	Green (Blinking)	The LAN port is receiving or transmitting data.
	Off	No device is attached.
100M	Yellow	The LAN port is operating at 100Mbps.
	Yellow (Blinking)	The LAN port is receiving or transmitting data
	Off	No device is attached.

2. INSTALLATION

The following are instructions for setting up the IAC4500. Refer to the illustration and follow the simple steps below to quickly install your IAC4500.

2-1 Installation Requirements

Before installing the IAC4500, make sure your network meets the following requirements.

System Requirements

The IAC4500 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 uses fixed or dynamic IP. If it is a fixed IP, be sure to get the IP from your ISP. For dynamic IP, which is most commonly 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 IAC4500
- Your subnet mask for the IAC4500
- 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 IAC4500's default IP address setting is "10.59.1.1".

2. The IAC4500'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 IAC4500 is a DHCP server, and it will give your PC the necessary IP settings.

2-2 Getting Started

1. Place the IAC4500 on a flat work surface.
2. Connect the power cord to the IAC4500 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 IAC4500'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 IAC4500. Check that the LAN Port Status LED lights.
6. Configure the further parameters via a web browser.

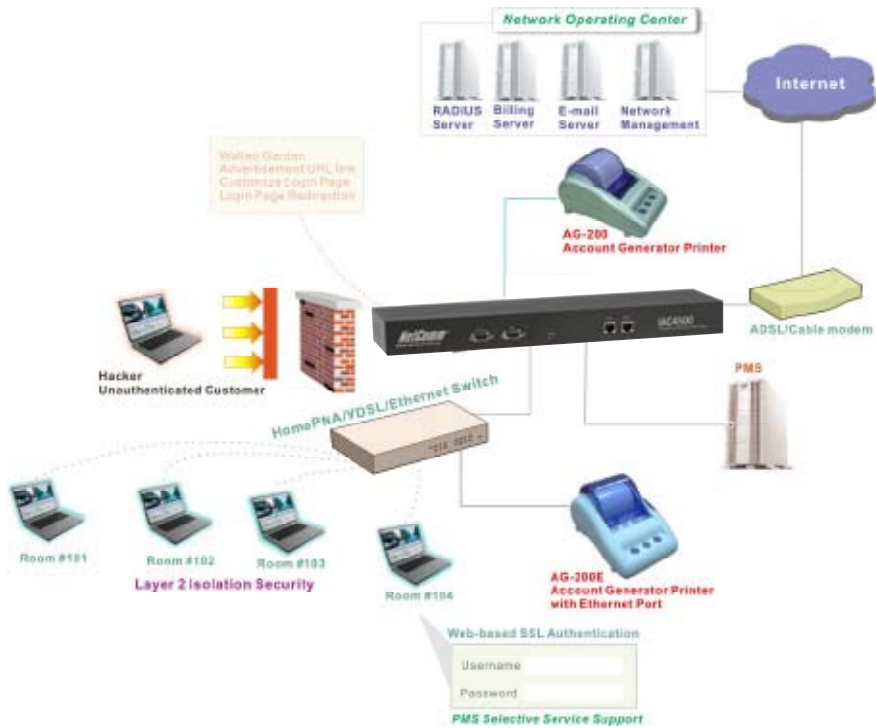


Figure 2-1 Connecting the IAC4500

3. CONFIGURING THE IAC4500

The IAC4500 offers a friendly user interface, accessed through either a console user interface or a Web user interface. The Console UI provides basic system configuration and status. For advanced functions, please use the Web Configuration.



3-1 Console Configuration

To access the IAC4500 User Interface, the administrator needs to connect a VT100 terminal and a PC running a VT100 compatible terminal emulation program to the IAC4500 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., IAC4500) 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
 - Data 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 login to your IAC4500. 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 IAC4500.
- 12 Go to the Call menu and select Connect.
- 13 If you have not completed an initial power up, power up the IAC4500 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 blank, make sure that you have entered the correct settings in Step 7. 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



The login screen is a rectangular box with a black border. Inside, the text is centered. At the top, it says 'Internet Subscriber Server III'. Below that is 'Copyright (c) 2005~2015 All Rights Reserved.' and 'Version 1.00.01'. Then there are labels for 'Username:' and 'Password:'. At the bottom, there is a black horizontal bar with the white text 'Enter username.'.

Internet Subscriber Server III

Copyright (c) 2005~2015 All Rights Reserved.

Version 1.00.01

Username:

Password:

Enter username.

Figure 3-1 Login Screen

The default Username is "**admin**". The default Password is "**admin**". The password can be changed after accessing the IAC4500 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 IAC4500 system basic parameter settings.
 - 2) WAN Configuration:** Including IAC4500 system WAN parameter settings.
 - 3) LAN Configuration:** Including IAC4500 system LAN parameter settings.
 - 4) System Status:** Displays the IAC4500 system basic status.
 - 5) Utilities:** Including firmware upgrades and changes to the password.
 - 6) Restart:** Restart the IAC4500 system.
 - 7) Logout:** Logout the IAC4500 serial session.
 - 8) Factory Defaults:** Erases all settings and reverts back to the original factory settings.
- Enter a numeric that you need between 1~8 and press 'Enter' to the subdirectory.

3-1-2-1 System Configuration

System Configuration	
System Name	:
Domain Name	:
Console Port Speed	: 9600
Web Server Port	: 80
E-Mail Server Redirect	:

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 the 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 users may set up the IAC4500 under a NAT network. The administrator has to set the Web server port so that the IAC4500 can be remotely accessed under a 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 IAC4500 system under NAT, please tab the "http://WAN Port IP Address: Port Number". "210.66.37.200:8001"

- 5) **E-mail Server Redirect:** The IAC4500 redirects the subscribers' E-mail via a specified SMTP server. The recipient of your E-mail sees the message as if it was sent from your local Internet Service Provider, not from the hotel or location of the IAC4500.

3-1-2-2 WAN Configuration

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

WAN Configuration	
WAN Type ? (D/S/P/T) :	D

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

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

WAN Configuration	
WAN Type ? (D/S/P/T) :	S
IP Address :	0.0.0.0
Subnet Mask :	255.255.255.0
Gateway :	0.0.0.0
Primary DNS Server :	
Secondary DNS Server :	

Figure 3-5 WAN Configuration Screen - Static IP

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

WAN Configuration	
WAN Type ? (D/S/P/T) :	P
Username :	
Password :	
Connect Setting ? (C/K) :	C
Max idle Time (Min) :	10
Optional Setting :	
Service name :	
PPP MTU Setting :	1492
TCP MSS Setting :	1452

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).

WAN Configuration	
WAN Type ? (D/S/P/T) :	T
Local IP Address :	
Local Subnet Mask :	
Gateway IP Address :	
Server IP Address :	
Username :	
Password :	
Connect Setting ? (C/K) :	C
Max idle Time (Min) :	10
Optional Setting :	
Connection ID/Name :	
PPP MTU Setting :	1460
TCP MSS Setting :	1400

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:** IAC4500 includes a DHCP server. To enable this function please choose the DHCP service as 'S', and set the DHCP server information.

LAN Configuration	
DHCP Configuration	
DHCP Service? (D/R/S)	: S
Start IP Address	: 10.59.1.2
DHCP Pool Size (Max.=512)	: 253
Lease Time	: 1440
Primary DNS IP Address	: 168.95.1.1
Secondary DNS IP Address	:

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**

LAN Configuration	
DHCP Configuration	
DHCP Service? (D/R/S)	: D

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.

LAN Configuration	
DHCP Configuration	
DHCP Service? (D/R/S)	: R
Relay 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 only displays system information, there is no authority to change settings available in this section.

System Status	
System Name	:
Domain Name	:
Console Port Speed	: 9600
Web Server Port	: 80
E-Mail Server Redirect	:
WAN Configuration	
WAN Type (D/S/P/T)	: DHCP Client
IP Address	: 192.168.100.142
Subnet Mask	: 255.255.255.0
Gateway	: 192.168.100.254
Primary DNS Server	: 168.95.1.1
Secondary DNS Server	: 211.11.180.244
DHCP Configuration	
DHCP Service? (D/R/S)	: Server
Start IP Address	: 10.59.1.2
DHCP Pool Size (Max.=512)	: 253
Lease Time	: 1440
Primary DNS IP Address	: 168.95.1.1
Secondary DNS IP Address	:
Press any key to return.	

Figure 3-11 System Status Screen

3-1-2-5 Utilities Menu

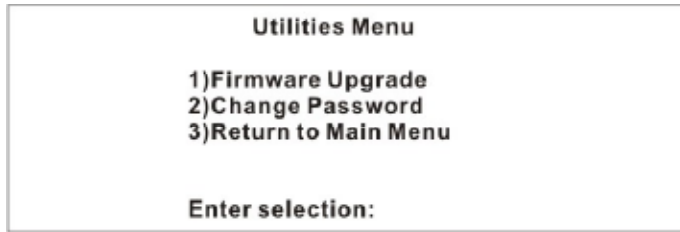


Figure 3-12 Utilities Menu Screen

- 1) **Firmware Upgrade:** IAC4500 allows the administrator to upgrade firmware.
- 2) **Change Password:** IAC4500 allows the administrator to change the password.
- 3) **Return to Main Menu:** Leave this page and return to Main Menu screen.

• Firmware Upgrade:

The IAC4500 uses TFTP Download to upgrade firmware. The Administrator needs to specify the TFTP server IP address and the filename that you wish to download.

Firmware Upgrade

TFTP Server IP Address :

Download Filename :

Figure 3-13 Firmware Upgrade Setting Screen

How to make a TFTP download

1. Get the TFTP server software.
2. Connect the TFTP server directly into the console port of the IAC4500.
3. Copy the TFTP server program to a specified folder.
4. Execute the TFTP server program and specify the location of firmware file.

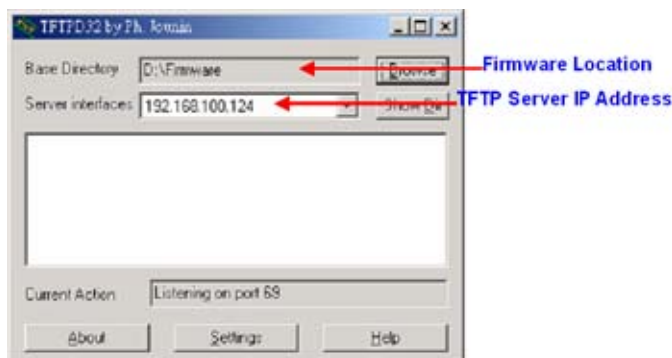


Figure 3-14 Example-TFTP Server

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

Change Administrator Password

Enter the old password :

Enter the new password :

Confirm the new 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

This function can assist when making multiple changes to different menu functions and you want to reboot once 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.

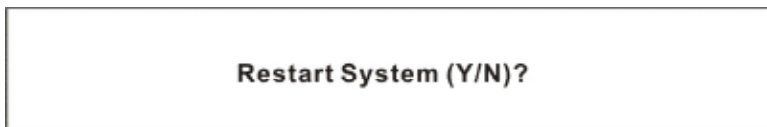


Figure 3-16 Restart System Screen

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.

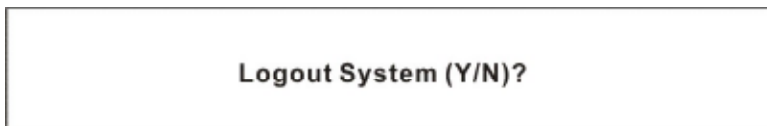


Figure 3-17 Logout System Screen

3-1-2-8 Factory Defaults

If you enter "Y" the IAC4500 will erase all setting, and go back to the original factory settings. There are two different choices after you decided to return to the factory setting. The first is to change all the parameters to factory settings but only reserve the user profiles (subscribers' table). The other is to clear all the parameters into factory settings including the user profiles.

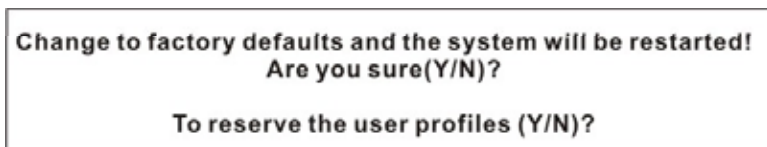


Figure 3-18 Factory Setting Screen

3-2 Web Configuration

Follow the steps below to access the Web configuration.

1. Make sure your IAC4500 is properly connected.
2. Start your Web browser and enter the factory default IP address 10.59.1.1 in your browser's location box. Press Enter.

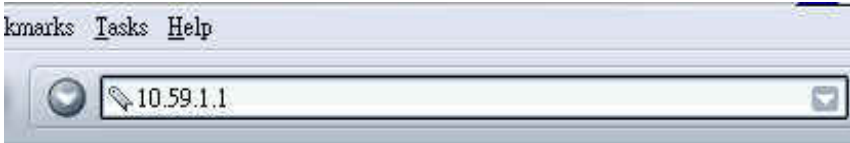


Figure 3-19 Web Browser Location Field (Factory Default)

3. The IAC4500 configuration main menu will appear. Enter “**admin**” (default) as the Username and “**admin**” (default) as the password and click “Get Started”.



Figure 3-20 IAC4500 Login Page

4. After a valid user name and password have been provided, the IAC4500 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.

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

If for any reason your password is lost or you cannot gain access to the IAC4500 Configuration Program, please press the reset button to load the device to manufacturer defaults.

If the IAC4500 doesn't send a packet in 5 minutes (system default), the IAC4500 will logout automatically.

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 IAC4500.

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

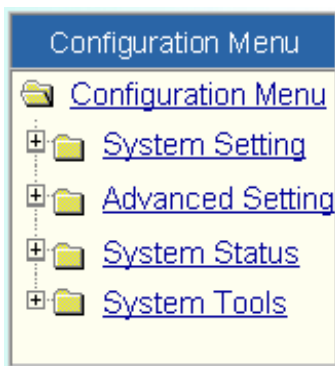


Figure 3-21 Configuration Menu

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 IAC4500 System parameter.

System		
System/Host Name	<input type="text"/>	
Domain Name	<input type="text"/>	
Locator Information	<div>Location Name: <input type="text"/> Max=50</div> <div>Address: <input type="text"/> Max=200</div> <div>City: <input type="text"/> Max=50</div> <div>State / Province: <input type="text"/> Max=50</div> <div>Zip / Postal Code: <input type="text"/> Max=10</div> <div>Country: <input type="text"/> Max=50</div> <div>Contact Name: <input type="text"/> Max=50</div> <div>Contact Telephone: <input type="text"/> Max=50</div> <div>Contact FAX: <input type="text"/> Max=50</div> <div>Contact Email: <input type="text"/> Max=50</div>	
	<div>Date: <input type="text"/> / <input type="text"/> / <input type="text"/> (Month/Day/Year)</div> <div>Time: <input type="text"/> : <input type="text"/> : <input type="text"/> Hour Minute Second</div> <div> <input type="button" value="Get from my Computer"/> <input type="button" value="Get from NTP server"/> </div> <div> <input type="checkbox"/> Use NTP (Network Time Protocol) Time Server </div> <div> <div>Server IP/Domain Name: <input type="text"/></div> <div>Time Zone: <input type="text"/> GMT-12:00</div> <div>Update Time: <input type="text"/> hours</div> <div> <input type="checkbox"/> Daylight Saving Time </div> <div> <div>Start Date: <input type="text"/> Month / <input type="text"/> Day</div> <div>End Date: <input type="text"/> Month / <input type="text"/> Day</div> </div> </div>	
	<div> <input checked="" type="checkbox"/> Enable </div> <div> <input checked="" type="checkbox"/> IP Plug and Play (IPvP Technology) </div> <div> <div>User Session Limit: <input type="text"/> Unlimited</div> <div><input type="text"/> 64 (1=1024)</div> </div> <div> <input type="checkbox"/> Disable </div>	
	Layer 2 Isolation Security	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Console Type	<input checked="" type="radio"/> Console Setting
		<input type="radio"/> Account Generator Profile: <input type="text"/> AC5-100
	Console Port	<div>Bits per second: <input type="text"/> 9600</div> <div>Data bits: <input type="text"/> 8</div> <div>Parity: <input type="text"/> None</div> <div>Stop bits: <input type="text"/> 1</div>
	Administrator Authorized Access IP Address	<div><input checked="" type="radio"/> Any</div> <div><input type="radio"/> Specify</div> <div> <div>1: <input type="text"/> - <input type="text"/></div> <div>2: <input type="text"/> - <input type="text"/></div> <div>3: <input type="text"/> - <input type="text"/></div> <div>4: <input type="text"/> - <input type="text"/></div> <div>5: <input type="text"/> - <input type="text"/></div> </div>
	Multicast Passthrough	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Allow remote user to ping the device	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
SSL Certificate	<input checked="" type="radio"/> Default <input type="radio"/> Custom Certificate	
<input type="button" value="Apply"/>		

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		
Date/Time		
Date	System Date	(Year/Month/Day) The system date of the IAC4500. The valid setting of year is from 2002 to 2035.
Time	System Time	(Hour:Minute:Second) The system time of the IAC4500.
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 IAC4500. 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.
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.
User	Session	Choosing Limit or Unlimited Enables or disables user session limit function. This feature provides you with 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, users 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 IAC4500's front panel by using the cable provided with this package.

Item	Default	Description
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).

Item	Default	Description
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 users to ping the IAC4500 through the 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: Using an OpenSSL tool).

After changing the settings, please click Apply button to update the new settings. The success dialog box will appear, click on back to return to the system setting screen.



Figure 3-25 Success Dialog Box

3-2-2-2 WAN/LAN

WAN/LAN	
LAN	<p>The Device IP Address and Subnet mask settings</p> <p>IP Address: <input type="text" value="10.59.1.1"/></p> <p>Subnet Mask: <input type="text" value="255.0.0.0"/></p>
WAN MAC Address	<p><input checked="" type="radio"/> Default</p> <p><input type="radio"/> Change to: <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/></p>
WAN Port Mode	<p><input checked="" type="radio"/> Get automatically from a DHCP server</p> <p><input type="radio"/> Use fixed IP address:</p> <p><input type="radio"/> PPPoE (Mostly for ADSL modem users)</p> <p><input type="radio"/> PPTP (Mostly for Europe ADSL modem users)</p>
<input type="button" value="Apply"/>	

Figure 3-26 WAN/LAN Setting Screen

Restart
To Restart the system, click Apply
<input type="button" value="Apply"/>

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

LAN	The Device IP Address and Subnet mask settings	
	IP Address:	10.59.1.1
	Subnet Mask:	255.0.0.0

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 IAC4500.
Subnet Mask	255.0.0.0	The subnet mask of your IAC4500.

WAN MAC Address

WAN MAC Address	<input checked="" type="radio"/> Default
	<input type="radio"/> Change to: 00 : 00 : 00 : 00 : 00 : 00

Figure 3-29 WAN MAC Address Setting

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

WAN Port Mode

WAN Port Mode	<input checked="" type="radio"/> Get automatically from a DHCP server
	<input type="radio"/> Use fixed IP address
	<input type="radio"/> PPPoE (Mostly for ADSL modem users)
	<input type="radio"/> PPTP (Mostly for Europe ADSL modem users)

Figure 3-30 WAN Port Mode Setting

Item	Description
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.

☒ Get automatically from a DHCP server

Figure 3-31 DHCP Client Setting Screen

Use fixed IP address

☒ Use fixed IP address

You have static IP information from your ISP

IP Address:	<input type="text" value="0.0.0.0"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default IP Gateway:	<input type="text" value="0.0.0.0"/>
Primary DNS Server:	<input type="text"/>
Secondary DNS Server:	<input type="text"/>

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 (Mostly for ADSL modem users)

Your ISP requires you to input username / password

Username:	<input type="text"/>
Password:	<input type="password"/>
PPP MTU Setting:	<input type="text" value="1492"/> (option)
TCP MSS Setting:	<input type="text" value="1452"/> (option)
Service Name:	<input type="text"/> (option)
<input checked="" type="radio"/> Connect on Demand	Max Idle Time: <input type="text" value="10"/> Min.
<input type="radio"/> Keep alive	Redial Period: <input type="text" value="30"/> Sec.

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 IAC4500 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 IAC4500 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 PPPoE enabled Internet access connected indefinitely, even when it sits idle. The Redial Period maximum value is 65535 seconds.
Redial Period	30 Seconds	

PPTP

☒ PPTP (Mostly for Europe ADSL modem users)

Your ISP requires you to input username / password / PPTP setting

PPTP Local IP Address:	<input type="text"/>
PPTP Local Subnet Mask:	<input type="text"/>
PPTP Local Default Gateway:	<input type="text"/>
PPTP Server IP Address:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
PPP MTU Setting:	<input type="text" value="1460"/> (option)
TCP MSS Setting:	<input type="text" value="1400"/> (option)
Connection ID/Name:	<input type="text"/> (option)
<input checked="" type="radio"/> Connect on Demand	Max Idle Time: <input type="text" value="10"/> Min.
<input type="radio"/> Keep alive	Redial Period: <input type="text" value="30"/> Sec.

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.
TCP MSS Setting	1400	MSS (Maximum Segment Size) specifies maximum segment size.

Item	Default	Description
Connect on Demand and Max Idle Time		
Connect on Demand	Enable	You can configure your IAC4500 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 IAC4500 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

Server	
Web Server	Server Port: <input type="text" value="80"/> <input type="checkbox"/> SSL Security Administrator Idle-Timeout: <input type="text" value="5"/> Min(s) (1 - 1440)
DHCP Server	<input type="radio"/> Disable <input type="radio"/> DHCP Relay DHCP Server IP Address: <input type="text"/>
	<input checked="" type="radio"/> DHCP Server(Private) IP Pool Starting Address: <input type="text" value="10.59.1.2"/>
	Pool Size: <input type="text" value="253"/> (Max.=512)
	Lease Time (Private): <input type="text" value="1440"/> (Minutes)
	Primary DNS Server: <input type="text" value="168.95.1.1"/>
	Secondary DNS Server: <input type="text"/>
Email Server Redirect	IP Address or Domain Name: <input type="text"/> SMTP Port: <input type="text" value="25"/> (25, 2500 - 2599)
<input type="button" value="Apply"/>	

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

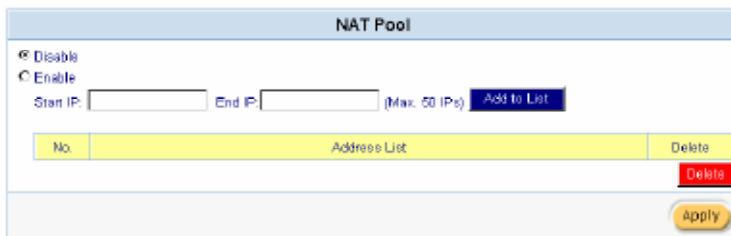
Server	
Web Server	Server Port: <input type="text" value="80"/> <input type="checkbox"/> SSL Security Administrator Idle-Timeout: <input type="text" value="5"/> Min(s) (1 - 1440)
DHCP Server	<input type="radio"/> Disable <input type="radio"/> DHCP Relay DHCP Server IP Address: <input type="text"/>
	<input checked="" type="radio"/> DHCP Server(Private) IP Pool Starting Address: <input type="text" value="10.59.1.2"/>
	Pool Size: <input type="text" value="253"/> (Max.=512)
	Lease Time (Private): <input type="text" value="1440"/> (Minutes)
	Lease Time (Temporal): <input type="text" value="5"/> (Minutes)
	Primary DNS Server: <input type="text" value="168.95.1.1"/>
	Secondary DNS Server: <input type="text"/>
	<input type="checkbox"/> DHCP Server(Public) If the network ID is different from WAN, this function will be disabled automatically.
	IP Pool Starting Address: <input type="text"/>
	Pool Size: <input type="text" value="253"/> (Max.=512) Lease Time (Public): <input type="text" value="1440"/> (Minutes)
Email Server Redirect	IP Address or Domain Name: <input type="text"/> SMTP Port: <input type="text" value="25"/> (25, 2500 - 2599)
<input type="button" value="Apply"/>	

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 the administrator wants to remote access under NAT Network. For access to the IAC4500 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.
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 a 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	<p>The IAC4500 provides an extra Email server parameter to forward the subscriber's Email. The IAC4500 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 Provider.</p> <p><i>Note: Before setting this sever, please make sure the e-mail sever relay function is opened.</i></p>	
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 NAT Pool

Some VPN servers have limitations on clients, where it may only accept one client with the same source IP address. In the IAC4500 scenario, if there are 2 client PCs behind a normal NAT router both accessing a VPN connection to the same VPN server at the same time, one of the clients may not gain a successful connection. The “NAT Pool for VPN packet” function is implemented to overcome this problem. When “NAT Pool for VPN packet” is enabled, the source IP of the PPTP and IPSec packets from the clients PCs will be translated to more than one global IP and forwarded to the VPN server.



The NAT Pool setting screen features a title bar labeled 'NAT Pool'. Below the title bar, there are two radio buttons: 'Disable' (selected) and 'Enable'. Under the 'Enable' option, there are two input fields for 'Start IP' and 'End IP', followed by a note '(Max. 50 IPs)' and an 'Add to List' button. Below these fields is a table with three columns: 'No.', 'Address List', and 'Delete'. The 'Address List' column is highlighted in yellow. At the bottom right of the screen, there is a red 'Delete' button and a yellow 'Apply' button.

Figure 3-37 NAT Pool Setting Screen

Item	Default	Description
Disable/Enable	Disable	Enables or disables the NAT Pool function.
Start IP	Empty	Enter the Starting IP address.
End IP	Empty	Enter the Ending IP address.
Add to List		Click Add to List button to add a new entry.
No.	The index number of NAT pool.	
Address List	Display the address range of the pool.	
Delete	Disable	Select the check boxes and click Delete button to delete the entries.
Delete	Click Delete & Apply button to delete all entries.	
Apply	Click Apply button to save the new settings.	

Different client PCs establish VPN connect to same VPN server at the same time

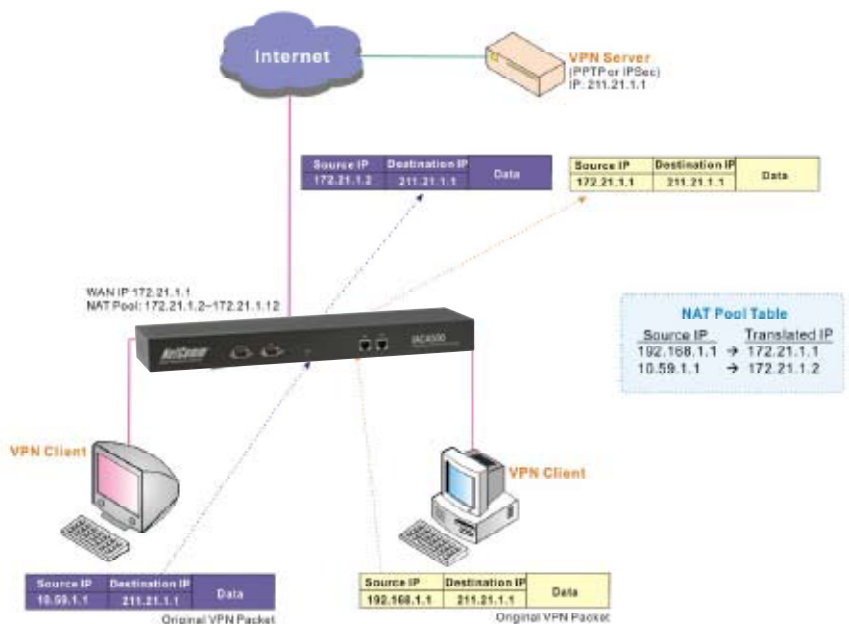


Figure 3-38 Application 1

Different client PCs establish VPN connect to different VPN servers at the same time

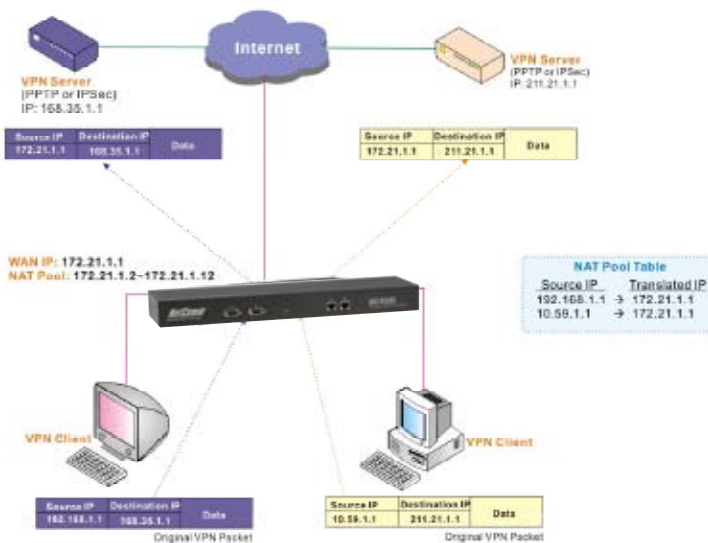


Figure 3-39 Application 2

Three different client PCs establish VPN connection. Two client PCs access same VPN server and one client PC access to another VPN server at the same time

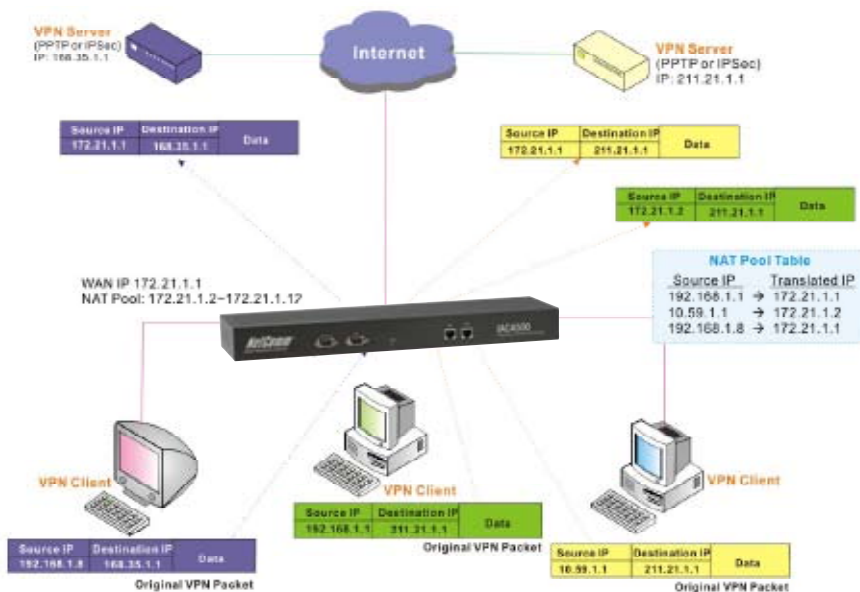


Figure 3-40 Application 3

3-2-2-5 Authentication

Authentication Type

Authentication										
Authentication Type	<input checked="" type="radio"/> No Authentication <input type="radio"/> User Agreement <input type="checkbox"/> Redirect URL Link <input type="text"/> Code <input checked="" type="radio"/> Standard User Agreement page <input type="radio"/> Built-in Authentication <p>Three pre-configured options are provided for easy setup. Select an option that suits your network needs. You must then proceed to configure the "Billing" and "Accounting" settings to complete your setup.</p> <p>Current preset option: Scenario B Select Option</p> <input type="radio"/> RADIUS									
	<input type="checkbox"/> Check Local Account first									
	<input checked="" type="radio"/> Accumulation <input type="radio"/> Time to Finish (No idle timeout)									
	<table border="1"> <tr> <td rowspan="4">Primary RADIUS Server</td> <td>Server IP address</td> <td><input type="text"/></td> </tr> <tr> <td>Authentication Port</td> <td><input type="text" value="0"/></td> </tr> <tr> <td>Accounting Port</td> <td><input type="text" value="0"/></td> </tr> <tr> <td>Shared Secret</td> <td><input type="text"/></td> </tr> </table>	Primary RADIUS Server	Server IP address	<input type="text"/>	Authentication Port	<input type="text" value="0"/>	Accounting Port	<input type="text" value="0"/>	Shared Secret	<input type="text"/>
	Primary RADIUS Server		Server IP address	<input type="text"/>						
			Authentication Port	<input type="text" value="0"/>						
			Accounting Port	<input type="text" value="0"/>						
		Shared Secret	<input type="text"/>							
	<table border="1"> <tr> <td rowspan="4">Secondary RADIUS Server</td> <td>Server IP address</td> <td><input type="text"/></td> </tr> <tr> <td>Authentication Port</td> <td><input type="text" value="0"/></td> </tr> <tr> <td>Accounting Port</td> <td><input type="text" value="0"/></td> </tr> <tr> <td>Shared Secret</td> <td><input type="text"/></td> </tr> </table>	Secondary RADIUS Server	Server IP address	<input type="text"/>	Authentication Port	<input type="text" value="0"/>	Accounting Port	<input type="text" value="0"/>	Shared Secret	<input type="text"/>
	Secondary RADIUS Server		Server IP address	<input type="text"/>						
Authentication Port			<input type="text" value="0"/>							
Accounting Port			<input type="text" value="0"/>							
Shared Secret		<input type="text"/>								
Retry Attempts when Primary failed: <input type="text" value="1"/>										
Retry Frequency: <input type="text" value="3"/> seconds (3-75)										
<table border="1"> <tr> <td rowspan="2">Accounting Service</td> <td> <input checked="" type="radio"/> Disable <input type="radio"/> Enable Update every <input type="text" value="0"/> minute(s) </td> </tr> </table>	Accounting Service	<input checked="" type="radio"/> Disable <input type="radio"/> Enable Update every <input type="text" value="0"/> minute(s)								
Accounting Service		<input checked="" type="radio"/> Disable <input type="radio"/> Enable Update every <input type="text" value="0"/> minute(s)								
	<table border="1"> <tr> <td>Authentication Method</td> <td><input type="text" value="CHAP"/></td> </tr> </table>	Authentication Method	<input type="text" value="CHAP"/>							
Authentication Method	<input type="text" value="CHAP"/>									
<table border="1"> <tr> <td>Vendor Specific Attribute</td> <td> Vendor Code <input type="text" value="0"/> <input type="checkbox"/> Send VSA together with Authentication Request </td> </tr> </table>	Vendor Specific Attribute	Vendor Code <input type="text" value="0"/> <input type="checkbox"/> Send VSA together with Authentication Request								
Vendor Specific Attribute	Vendor Code <input type="text" value="0"/> <input type="checkbox"/> Send VSA together with Authentication Request									
Idle Time Out: <input type="text" value="5"/> Min(s) (1 - 1440)										
SSL Login Security: <input checked="" type="radio"/> Disable <input type="radio"/> Enable										
Smart Client Support: <input type="checkbox"/> WISPr Smart Client										
<table border="1"> <tr> <td rowspan="3">Login Mode</td> <td> <input checked="" type="radio"/> Directly Reply <input type="radio"/> Proxy Reply with "Redirect Login Page" URL <input type="radio"/> Proxy Reply with Specific URL <input type="text"/> </td> </tr> </table>	Login Mode	<input checked="" type="radio"/> Directly Reply <input type="radio"/> Proxy Reply with "Redirect Login Page" URL <input type="radio"/> Proxy Reply with Specific URL <input type="text"/>								
Login Mode		<input checked="" type="radio"/> Directly Reply <input type="radio"/> Proxy Reply with "Redirect Login Page" URL <input type="radio"/> Proxy Reply with Specific URL <input type="text"/>								
		<input type="button" value="Apply"/>								

Figure 3-41 Authentication Configuration Setting Screen

Item	Default	Description
Authentication Type		
No Authentication/Built-in Authentication/RADIUS	No Authentication	<p>Options: No Authentication, Built-in Authentication or RADIUS.</p> <p>No Authentication: Subscriber can direct access the Internet without entering username and password.</p> <p>Built-in Authentication: If "Built-in Authentication" is selected, the service provider can generate the subscriber account via the IAC4500, and the system will authenticate the subscriber login according to the generated account.</p> <p>RADIUS: If "RADIUS Authentication" is selected, all subscribers' authentication requests will be send to the RADIUS Server via RADIUS protocol (RFC 2865, 2866).</p> <p><i>Note: When Authentication mode or Scenario is changed, the accounts, logs, user on the account List, billing Logs and current user list page will be erased.</i></p>
User Agreement	Standard User Agreement Page	Option: Redirect URL Link or Standard User Agreement Page.
Redirect URL Link	Empty	Enter the URL Page; please use this format "http://www.yahoo.com". The maximum character of the URL Page is 200.
Built-in Authentication		
Current Preset option	Scenario C	This is the best way to setup your Internet Service authentication. Follow the instructions of the Scenario Guide below to quickly install your IAC4500.
Select option	Click this button to select the scenario.	

Scenario Guide			
Express way to fit your business model			
Items check	<input type="radio"/> Scenario A	<input type="radio"/> Scenario B	<input checked="" type="radio"/> Scenario C
PMS billing system	Yes <input type="checkbox"/> Output bill to AB Number of copies: <input type="text" value="1"/>	Yes	No
Infrastructure	Port-Location Mapping	General	General
Need username/password when guests go to Internet	No	Yes	Yes
Need to create static accounts	Option	Yes	Option
Allow guests to select service when first login	Yes	Yes	No
Billing mode	Time to Finish	Time to Finish	<input checked="" type="radio"/> Time to Finish <input type="radio"/> Accumulation Idle Timeout: <input type="text" value="5"/> Min (5, 15, 30, 60) Accumulation account will be deleted after logged in <input type="text" value="7"/> days
BillingCharge mode	<input checked="" type="radio"/> Based on Room <input type="radio"/> Based on Subscriber	-	-
Default Billing Profile	Need to continue configuring "Billing" and choose at least one active billing profile	Need to continue configuring "Billing" and choose at least one active billing profile	<input type="checkbox"/> Allow Credit Card Payment
Remarks	Need to continue configuring "Port-Location Mapping Table"		

Figure 3-42 Scenario Guide Setting Screen

Item	Description
Items check	Scenario A: This solution applies where the Hotel has a PMS system. Using the "Port-location Mapping" or "VLAN Tag" infrastructure, subscribers 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 the Internet.

Welcome

Please choose from the following service selection:

How many units of Internet access would you like to purchase?

*Please kindly note that there will be no refund made accordingly is confirmed.
*Please note that the time block of wireless service is based on world-wide usage.

Please click ENTER to confirm your acceptance of the usage charge or CANCEL to exit. The selected service charge will be posted directly into your guest file.

Figure 3-43 Login Page

Item	Description
Items check	Scenario B: This solution applies where the Hotel has a PMS system, and does not wish to use "Port-Location Mapping" or "VLAN Tags". Before subscribers can access the Internet, Hotel staff must register the room number and generate an account (username & password). The Subscriber uses this account and selects a billing profile to access the Internet.

Welcome	
Please choose from the following service selection	1 day \$10.00
How many units of Internet access would you like to purchase?	1
Username:	<input type="text"/>
Password:	<input type="password"/>
<p>*Please kindly note that there will be no refund once connectivity is confirmed. *Please note that the time block of selected service is based on continuous usage.</p>	
<p>Please click ENTER to confirm your acceptance of the usage charge or CANCEL to exit. The selected service charge will be posted directly into your guest folio.</p>	
<div>Enter</div> <div>Cancel</div>	

Figure 3-44 Login Page

Item	Description
Items check	Scenario C: This solution applies where the Hotel does not have a PMS. Before the subscriber can access the Internet, a subscriber has to ask for an account (username & password) from Hotel staff. The Subscriber has to inform the staff which billing profile they want to choose. After the account has been generated, the subscriber has to pay the charges to Hotel staff. The Subscriber can then use this account to access the Internet.

The figure consists of two screenshots of a web application interface. Both screenshots show a page titled "Welcome".

The top screenshot shows a login form with two input fields: "Username:" and "Password:". The "Username:" field contains the text "jdoe". The "Password:" field contains the text "jdoe". Below the input fields are two buttons: "Enter" and "Cancel".

The bottom screenshot shows the same login form. The "Username:" field is now empty. The "Password:" field still contains the text "jdoe". The "Enter" and "Cancel" buttons are still present.

Figure 3-45 Login Page

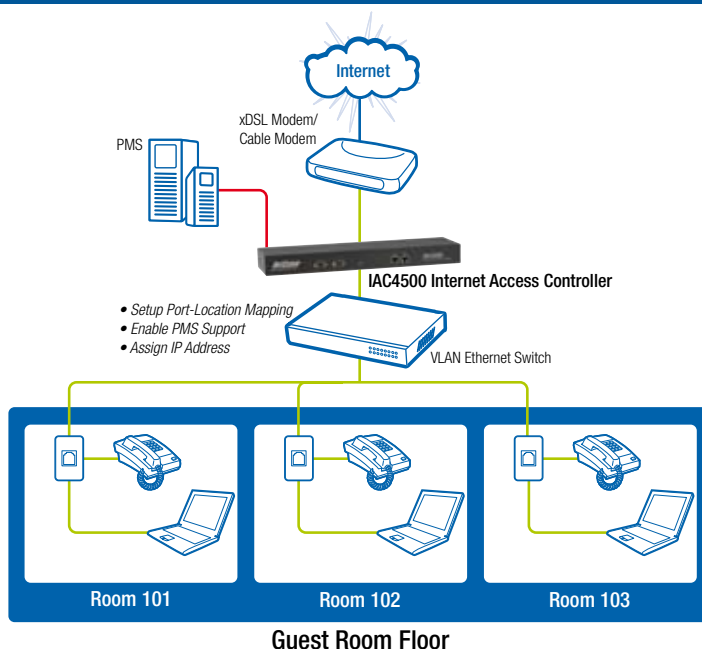


Figure 3-46 Scenario A – VLAN tagging with Port Based Mapping and PMS Integration

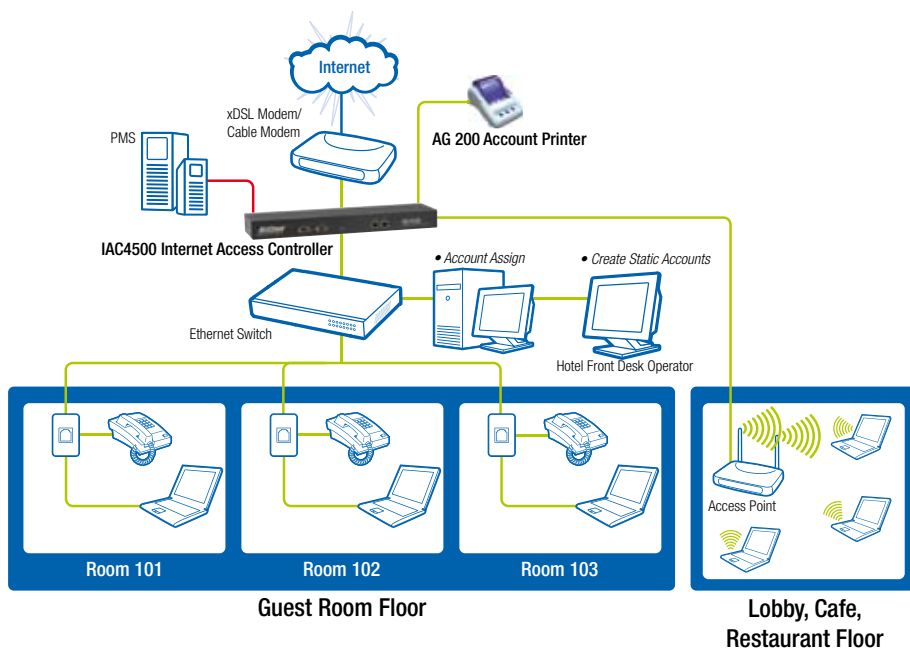


Figure 3-47 Scenario B – Issue Username and Password with PMS Integration

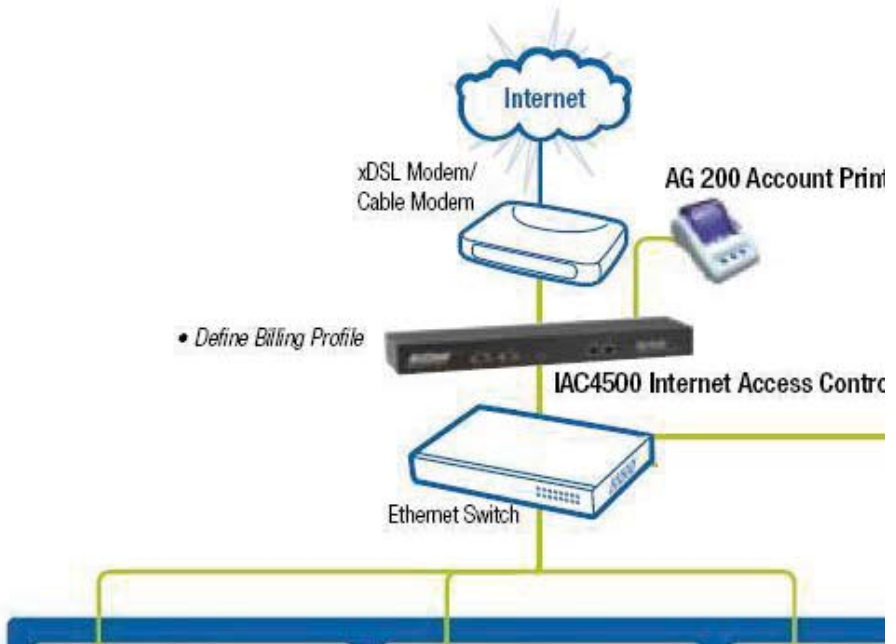


Figure 3-48 Scenario B – Username and Password

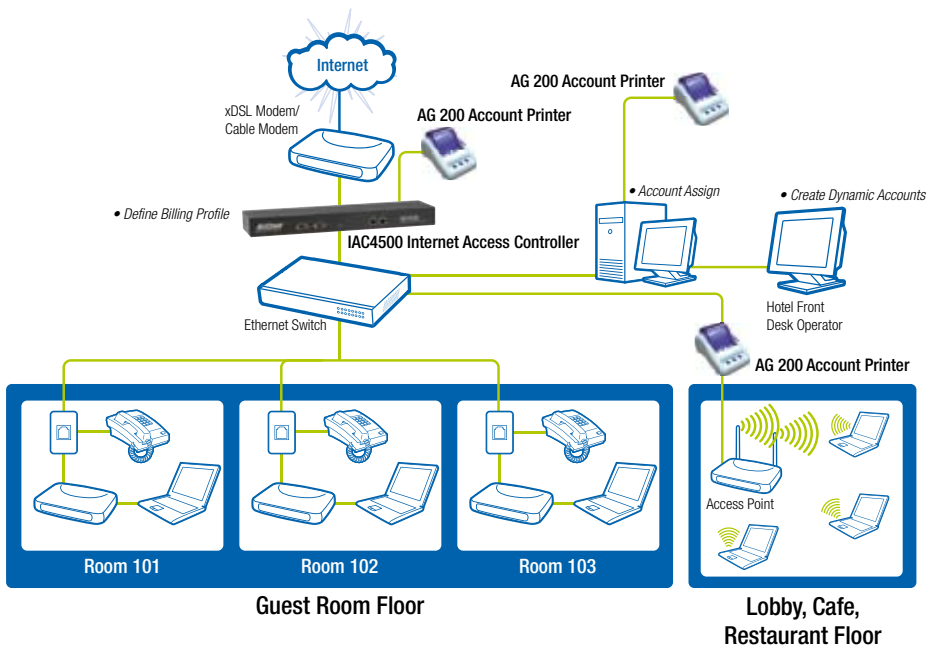


Figure 3-49 Scenario C – Username and Password

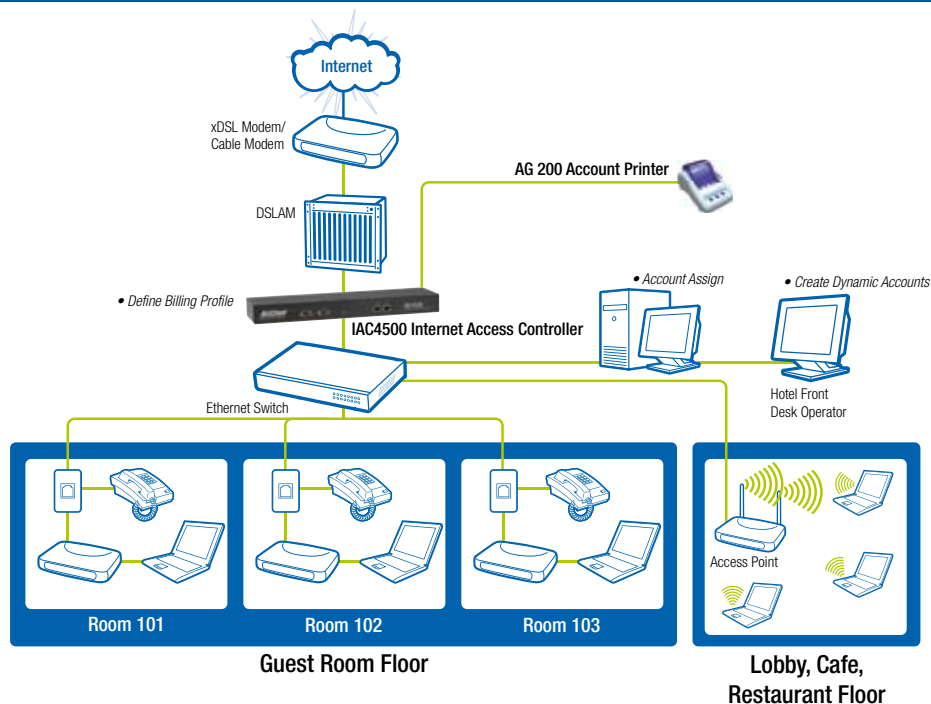


Figure 3-50 DSLAM required

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

RADIUS

☐ Check Local Account first

☒ **Accumulation**

☐ Time to Finish (No idle timeout)

Primary RADIUS Server	Server IP address	<input type="text"/>
	Authentication Port	<input type="text"/>
	Accounting Port	<input type="text"/>
	Shared Secret	<input type="text"/>
Secondary RADIUS Server	Server IP address	<input type="text"/>
	Authentication Port	<input type="text"/>
	Accounting Port	<input type="text"/>
	Shared Secret	<input type="text"/>
Retry Attempts when Primary failed		<input type="text" value="5"/>
Retry Frequency		<input type="text" value="3"/> seconds (3 ~ 75)
Accounting Genie		<input checked="" type="radio"/> Disable <input type="radio"/> Enable Update every: <input type="text" value="3"/> Min(s)
Authentication Method		<input type="text" value="CHAP"/>
Vendor Specific Attribute		Vendor Code <input type="text" value="0"/> <input type="checkbox"/> Send VSA together with Authentication Request

Figure 3-51 RADIUS Setting Screen

Item	Default	Description
RADIUS	Disable	The IAC4500 supports Remote Authentication Dial-In User Service (RADIUS). RADIUS is an authentication and accounting system used by many Internet Service Providers (ISPs). By using RADIUS, Service Providers can implement policy-based management of their subscriber database. The RADIUS also helps ISP to collect accounting data such as 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".

RADIUS

☐ Check Local Account first

☒ **Accumulation**

☐ Time to Finish (No idle timeout)

Figure 3-52 Usage Time

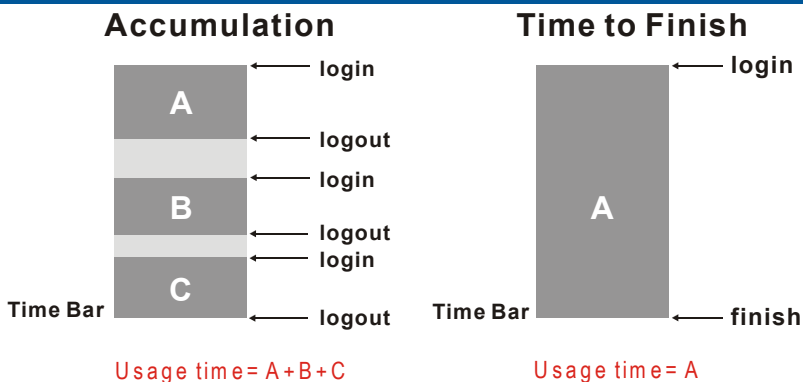


Figure 3-53 Accumulation and Time to Finish

Item	Default	Description
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.
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.

Item	Default	Description
Vendor Specific Attribute		
Vendor Code	0	1: Traffic-Limit 2: SMTP Redirect 3: BW-Up 4: BW-Down 5: Portable Page URL Traffic-Limit: Control user's access based on the data volume (Unit=Mbyte), include upload and download data. SMTP Redirect: 0 = Do not support SMTP Redirect 1 = Support SMTP Redirect BW-Up: Control user's upload bandwidth (Kbps). BW-Down: Control user's download bandwidth. (Kbps) Portable Page URL: Specific advertisement URL for each client.
Send VSA together with Authentication Request	Disable	Click the check box to send VSA together with authentication-request.

Note:

1. The RADIUS Server follows the RFC 2865 and RFC 2866 standards. And the authentication port number is 1645 and 1812. The administrator can configure the port number according to their own RADIUS server details. For more detailed information on RADIUS please check the manual of your RADIUS server.

2. After changing the settings, please click the Apply button to update the new settings, then the IAC4500 will restart.

When Traffic-Limit attributes are included in Authentication Replies from the RADIUS Server, the information Window will appear "Mbyte".



Figure 3-54 Information Window-Traffic Limit

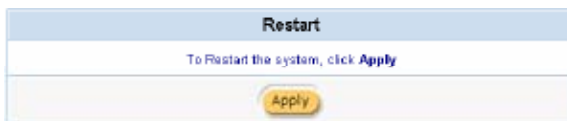


Figure 3-55 Restart Dialog Box

Idle Time Out

Idle Time Out	<input type="text" value="5"/> Min(s) (1 - 1440)
----------------------	--

Figure 3-56 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 a packet in 5 minutes, the subscriber will logout automatically. If the subscriber is off-line over the logout time, they 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 3-57 Current User Information Backup

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

SSL Login Security

SSL Login Security	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
---------------------------	---

Figure 3-58 SSL Login Security Setting Screen

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

Smart Client Support

Smart Client Support	<input checked="" type="checkbox"/> WISP Smart Client
<div> <div>Login Mode</div> <div> <input checked="" type="radio"/> Directly Reply <input type="radio"/> Proxy Reply with "Redirect Login Page" URL <input type="radio"/> Proxy Reply with Specific URL <input type="text"/> </div> </div>	

Figure 3-59 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.

3-2-2-6 Billing

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

Billing Profile

No	Active	Name	Description	Profile Setting
01	<input checked="" type="checkbox"/>	Profile 1	1 day \$10.00	Edit
02	<input type="checkbox"/>			Edit
03	<input type="checkbox"/>			Edit
04	<input type="checkbox"/>			Edit
05	<input type="checkbox"/>			Edit
06	<input type="checkbox"/>			Edit
07	<input type="checkbox"/>			Edit
08	<input type="checkbox"/>			Edit
09	<input type="checkbox"/>			Edit
10	<input type="checkbox"/>			Edit

Apply

Figure 3-60 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.

Billing Profile Setting			
No	1		
Name	Profile 1		
Description	1 day \$10.00		
Price	Duration	Charge	Check Time
	<input type="radio"/> 1 minute	<input type="text" value="0"/>	Period Time finish
	<input type="radio"/> 1 hour	<input type="text" value="0"/>	Period Time finish
	<input checked="" type="radio"/> 1 day	<input type="text" value="10.00"/>	<input checked="" type="radio"/> Period Time finish <input type="radio"/> Expire when 00:00
	<input type="radio"/> 1 week	<input type="text" value="0"/>	<input checked="" type="radio"/> Period Time finish <input type="radio"/> Expire when Sat 00:00
	<input type="radio"/> 1 month	<input type="text" value="0"/>	<input checked="" type="radio"/> Period Time finish <input type="radio"/> Expire when 01 00:00
	<input type="radio"/> Unlimited	<input type="text" value="0"/>	
Bandwidth Limit	<p>Note: You must activate the bandwidth management feature and select a class of service</p> <p>Maximum Upstream Bandwidth <input checked="" type="radio"/> 64 Kbps <input type="radio"/> Kbps (64-24576)</p> <p>Maximum Downstream Bandwidth <input checked="" type="radio"/> 256 Kbps <input type="radio"/> Kbps (64-24576)</p>		
Service Type	<input checked="" type="radio"/> Private Service <input type="radio"/> Public Service		
Reset		Apply	

Figure 3-61 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, the 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 the number of units purchased. The field valid range is 1 to 99.

Click the Reset button to restore system configuration.

Click the Apply button to save the new settings.

Welcome	
Username:	<input type="text"/>
Password:	<input type="password"/>
Description of Billing Profile Please choose from the following service selection: 1 day \$10.00 Selective Unit How many units of Internet access would you like to purchase? 1 <small>*Please kindly note that there will be an refund some connectivity is confirmed. *Please note that the time block of selected service is based on continuous usage.</small>	
Please click ENTER to confirm your acceptance of the usage charge or CANCEL to exit. The selected service charge will be posted directly into your guest folio.	
<input type="button" value="Enter"/> <input type="button" value="Cancel"/>	

Figure 3-62 Example-Login Page

Bandwidth Limit

Bandwidth Limit	Note: You must activate the bandwidth management feature and select a class of service	
	Maximum Upstream Bandwidth	<input checked="" type="radio"/> 64 Kbps <input type="radio"/> 0 Kbps (64-24576)
	Maximum Downstream Bandwidth	<input checked="" type="radio"/> 256 Kbps <input type="radio"/> 0 Kbps (64-24576)

Figure 3-63 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,

Bandwidth Management

☒ **Bandwidth Management**

☒ **Equal bandwidth for all subscribers**

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 ☐ 0 Kbps (64-24576)

Maximum Downstream Bandwidth: ☒ 256Kbps ☐ 0 Kbps (64-24576)

☐ **Class of service based on RADIUS or billing profile settings**

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.

Figure 3-64 Bandwidth Management Setting Screen

Service Type

Service Type	<input checked="" type="radio"/> Private Service
	<input type="radio"/> Public Service

Figure 3-65 Service Type Setting Screen

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

PMS Configuration

PMS Configuration

Many hotels use PMS as a hotel in-door billing system for their guests including room service, mini-bar, telephone usage, as well as Internet service. By integrating with a hotel's PMS, the system can post charges for Internet access directly to a guest's hotel bill.

Charge Mode (only for Port-Location Mapping enabled)	<input checked="" type="radio"/> Based on Room <input type="radio"/> Based on Subscriber
Regenerate password of static account with PMS checkout	<input type="button" value="Enable"/> (only for Scenario B)
PMS Type	<input checked="" type="radio"/> Micros Fidelio <input type="radio"/> Spectrum MK II
	Revenue Code: <input type="text" value="1"/> (1-99)
	Description: <input type="text" value="Internet"/>
	<input type="radio"/> Marriott
	Revenue Code: <input type="text" value="1"/> (1-99)
	Reference: <input type="text" value="Internet"/>
	<input type="radio"/> Proprietary
Speed of PMS interface	Bits per second: <input type="text" value="9600"/>
	Data bits: <input type="text" value="8"/>
	Parity: <input type="text" value="None"/>
	Stop bits: <input type="text" value="1"/>

Figure 3-66 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.
Regenerate password of static account when PMS checkout (only for Scenario B)	Enable	Enables or disables regenerate password function. When enabled, the system will regenerate the password of static account automatically.
PMS Type	Micros Fidelio	The IAC4500 offers support Micros Fidelio PMS, Marriott PMS and proprietary PMS to perform in-room billing.
Spectrum MK II		
Revenue Code	1	Enter the revenue code of the PMS system; the value must match with the PMS System setting. The revenue code valid range is 1 to 99.
Description	Internet	This is the description of the PMS system.
PMS interface	Attach your PMS system to the PMS port on the IAC4500's front panel by using the cable provided with this package.	

3-2-2-7 Accounting

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

Static Account Setting

Figure 3-67 Static Account Setting Screen

Item	Default	Description
Concurrent Access		
Allow concurrent access with one account	Enable	<p>Disable: The system allows only one user to access the Internet with one account.</p> <p>Enable: The system allows up to eight concurrent users to access Internet with one account.</p>
Max. concurrent access	2	The field specifies how many times the account can be used simultaneously. The field maximum value is 8
Customize Printout	-	This function allows you to produce custom bills 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.

Account Printout Customization	
Title:	Welcome! (Max=23)
Subtitle:	This is your account information, please keep this for your Internet Service. (Max=80)
Username:	Username:
Password:	Password:
Usage Time:	Usage Time:
Billing Method:	Billing:
Billing Profile:	Profile:
Purchase Unit:	Purchase Unit:
<input type="checkbox"/> Additional Label 1:	ESSID: Value: (Max=23)
<input type="checkbox"/> Additional Label 2:	WEP: Value: (Max=23)
<input checked="" type="checkbox"/> Price:	Total:
<input checked="" type="checkbox"/> Account Create Time:	yyyy/mm/dd HH:mm:ss (HH:24h Min:12h U:AM/PM)
<input checked="" type="checkbox"/> Ending:	Thank you very much! (Max=23)
<input checked="" type="checkbox"/> Serial Number	

[Preview of PC-connected printer for static account printout](#)
[Preview of account generator printer with static account printout](#)
[Preview of PC-connected printer for dynamic account printout](#)
[Preview of account generator printer with dynamic account printout](#)

Apply

Figure 3-68 Account Printout Customization Setting Screen

Click Apply button to save the new settings.

Welcome! ← Title	
This is your account information, please keep this for your Internet Service. ← Subtitle	
Username:	101
Password:	mpty8qc63
Usage Time:	1 day
Billing:	Time to Finish ← Billing Method
Profile:	1 day \$10.00 ← Billing Profile Description
Purchase Unit:	1
ESSID:	
WEP:	
Total: \$ 10.00 ← Price	
Thank you very much! ← Ending	

----- cut ----- cut ----- cut -----

Username:	101
Billing:	Time to Finish
Profile:	1 day \$10.00
Purchase Unit:	1
Total: \$ 10.00	
Signature:	
Account Create Time → 2005/11/8 09:51:52	

Figure 3-69 Scenario A/C-Static Account Printout-PC-connected printer

Welcomel ← Title	
This is your account information, please keep this for your Internet Service. ← Subtitle	
Username:	101
Password:	mpy8qc63
ESSID:	
WEP:	

Thank you very much ! ← Ending

Figure 3-70 Scenario B-Static Account Printout-PC-connected Printer

Welcomel ← Title	
This is your account information, please keep this for your Internet Service. ← Subtitle	

Username:	101
Password:	b3qmkw34
Usage Time:	1 day
Billing:	Time to Finish ← Billing Method
Profile:	1 day \$10.00 ← Billing Profile Description
Purchase Unit:	1
Total:	\$ 10.00 ← Price

ESSID:	
WEP:	

Thank you very much ! ← Ending	
-----CUT-----CUT-----CUT-----	

Username:	101
Password:	b3qmkw34
Billing:	Time to Finish
Profile:	1 day \$10.00
Purchase Unit:	1
Total:	\$ 10.00

Signature:	

2005/11/7 17:34:19 ← Account Create Time	

Figure 3-71 Scenario A/C-Static Account Printout-Account Generator Printer

Welcome! ← **Title**

This is your account information, please keep this for your Internet Service. ← **Subtitle**

Username: 101

Password: mpy8qc63

ESSID:

WEP:

Thank you very much ! ← **Ending**

Figure 3-72 Scenario B-Static Account Printout-Account Generator Printer

Welcome! ← Title	
This is your account information, please keep this for your Internet Service. ← Subtitle	
Username:	f9mdq822
Password:	5vhvdk27
Usage Time:	1 day
Billing:	Time to Finish ← Billing Method
Profile:	1 day \$10.00 ← Billing Profile Description
Purchase Unit:	1
ESSID:	
WEP:	
Total: \$ 10.00 ← Price	

Serial Number → S/N:000003

Expire Description → Please active your account before 2005/11/8 23:35:11

Expire Date/Time → 2005/11/8 11:35:11

Account Create Time →

Ending → **Thank you very much !**

Figure 3-73 Dynamic Account Printout-PC-connected Printer

Welcome! ← **Title**

This is your account information, please keep this for your Internet Service. ← **Subtitle**

Username → Username:xxxxxxxx

Password → Password:xxxxxxxx

Usage Time → Usage Time:

Billing Method → Billing: Time to Finish

Billing Profile → Profile: 1 day \$35.00

Purchase Unit → Purchase Unit: 1

Price → Total: \$ 1.00

Additional Label 1 → ESSID:

Additional Label 2 → WEP:

Account Create Time → 2003/7/28 11:42:03

S/N:000001 ← **Serial Number**

Ending → Thank you very much !

Close Print

Figure 3-74 Dynamic Account Printout-Account Generator Printer

Create Static Account

This allows the service provider to generate static subscriber accounts.

Create Static Account

Static Accounts can be created and managed by a series of specific number like hotel rooms.
Static accounts reside in the flash memory all the time.

Generate a batch of static accounts

This feature can automatically generate a series of specific numbers of accounts like hotel rooms.

Prefix: <input style="width: 80%;" type="text"/>	From: <input style="width: 80%;" type="text"/> (Maximum 5 numbers)
Postfix: <input style="width: 80%;" type="text"/>	To: <input style="width: 80%;" type="text"/> (Maximum 5 numbers)

Billing Profile: Profile 1 Random Password Length: 8

Note: For PMS billing type, use only numbers for subscriber accounts.

Figure 3-75 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

Static Accounts backup and restore

This feature can backup the account information to your computer or restore a previously saved account information file to your system.

Backup	Click to save the account information to your computer.
Restore	<p>To restore a previously saved account information file to your system, select this option, locate the account information file and click Apply.</p> <p>File Path: <input type="text"/> <input type="button" value="Browse"/></p>

Apply

Figure 3-76 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

Manually Add Subscriber Account			
No.	Username:	Password:	Billing Profile
1	<input type="text"/>	<input type="text"/>	Profile 1 ▾
2	<input type="text"/>	<input type="text"/>	Profile 1 ▾
3	<input type="text"/>	<input type="text"/>	Profile 1 ▾
4	<input type="text"/>	<input type="text"/>	Profile 1 ▾
5	<input type="text"/>	<input type="text"/>	Profile 1 ▾
6	<input type="text"/>	<input type="text"/>	Profile 1 ▾
7	<input type="text"/>	<input type="text"/>	Profile 1 ▾
8	<input type="text"/>	<input type="text"/>	Profile 1 ▾
9	<input type="text"/>	<input type="text"/>	Profile 1 ▾
10	<input type="text"/>	<input type="text"/>	Profile 1 ▾

Figure 3-77 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 the front desk to manage the Internet Service and print out the billing.

Static Account Operator						
						Print List
No.	Username	Show Password	Re-Generate Password ALL	Status	Concurrent Access	Print
1	101		Re-Generate Password	Online	1	
2	102		Re-Generate Password	Offline	0	
3	103		Re-Generate Password	Offline	0	
4	104		Re-Generate Password	Offline	0	
5	105		Re-Generate Password	Offline	0	
6	106		Re-Generate Password	Offline	0	
7	107		Re-Generate Password	Offline	0	
8	108		Re-Generate Password	Offline	0	
9	109		Re-Generate Password	Offline	0	
10	110		Re-Generate Password	Offline	0	

ISO [1] Page First Previous Next End Apply

Figure 3-78 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.
Print List	This button allows you to print the static account list.
Username	Click the column button to sort the column in ascending/descending order.
Show Password Hide Password	To show or hide the password information.
ALL	Click the all button to re-generate all passwords of static account operator table.
Re-Generate Password	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.

Static Account									
refresh		Backup Print List							
No.	Username	Password		Billing Profile	Concurrent Access	First Login	Expiration	Status	Delete
1	101	5faxz93	1	Profile 1	1	2003/11/29 10:24:58	2003/11/29 10:24:58	Online	<input type="checkbox"/>
2	102	1877j43	1	Profile 1	0			Offline	<input type="checkbox"/>
3	103	3jbum842	1	Profile 1	0			Offline	<input type="checkbox"/>
4	104	s77aun75	1	Profile 1	0			Offline	<input type="checkbox"/>
5	105	mngpg823	1	Profile 1	0			Offline	<input type="checkbox"/>
6	106	9v289m58	1	Profile 1	0			Offline	<input type="checkbox"/>
7	107	bwh2y988	1	Profile 1	0			Offline	<input type="checkbox"/>
8	108	3dfgh746	1	Profile 1	0			Offline	<input type="checkbox"/>
9	109	z58q2742	1	Profile 1	0			Offline	<input type="checkbox"/>
10	110	9n4cn63	1	Profile 1	0			Offline	<input type="checkbox"/>
								Delete Delete All	
GO <input type="text"/> Page		First Previous Next End							

Figure 3-79 Static Account List

Item	Description
refresh	Click on refresh button to update the static account list page.
Backup	Click it to save the static account information to your computer. (sta_list.txt)
Print List	This button allows you to print the static account list.
Username Billing Profile First Login Expiration Status	Click the column button to sort the column in ascending/descending order.
Delete	Select the check boxes and click 'Delete' to delete the accounts.
Delete All	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

Dynamic Account Setting			
Dynamic Accounts can be created automatically when you click the button from the Web-based Account Operator.			
Web-based Account Generator Panel Settings			
No.	AG Button	Button name (Max. 12 characters)	Billing Profile
Button 1	AG100 /200 Button A.	<input type="text" value="Button 1"/>	<input type="text" value="Profile 1"/>
Button 2	AG200 Button B	<input type="text" value="Button 2"/>	<input type="text" value="Profile 1"/>
Button 3	AG200 Button C	<input type="text" value="Button 3"/>	<input type="text" value="Profile 1"/>
Button 4	-	<input type="text" value="Button 4"/>	<input type="text" value="Profile 1"/>
General Settings			
Unused Accounts	Automatically delete after <input type="text" value="12"/> hours		
Concurrent Access	<input checked="" type="checkbox"/> Allow concurrent access with one account Max. concurrent access: <input type="text" value="2"/>		
Printout copy	Number of copies to print: <input type="text" value="1"/> Customize printout text		
Print to...	<input checked="" type="radio"/> Account Generator Printer <input type="radio"/> PC-Connected Printer		
<input type="button" value="Apply"/>			

Figure 3-80 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.

Dynamic Account Operator

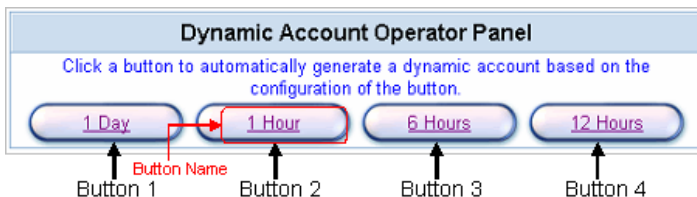


Figure 3-81 Dynamic Account Operator Panel

Click on button, to add a new account.

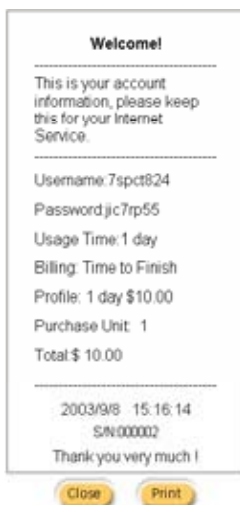


Figure 3-82 Dynamic Account Printout

Item	Description
	Close window.
	Click Print button to print this account information.

Before you create a 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 3-83 Error Dialog Box

Dynamic Account List

This list will allow you to view or print the status of all accounts.

Dynamic Account List								
refresh		Backup Print List						
S/N	Username	Password	Billing Profile	Time Created	First Login	Expiration	Status	Delete
8	48t2358	m8G3a725	2 Profile 2	2003/11/28 10:33:58	2003/11/28 10:35:05	2003/11/28 11:35:05	In Use	<input type="checkbox"/>
7	7spet855	jic7ip55	2 Profile 2	2003/11/28 10:33:55		2003/11/28 22:33:55	Not In Use	<input type="checkbox"/>
2	8y4dm39	zbcx9w62	1 Profile 1	2003/11/28 10:33:39		2003/11/28 22:33:39	Not In Use	<input type="checkbox"/>
6	b4e5552	xz6g6n60	1 Profile 1	2003/11/28 10:33:51		2003/11/28 22:33:51	Not In Use	<input type="checkbox"/>
3	powu3842	7hr9fw29	3 Profile 3	2003/11/28 10:33:42		2003/11/28 22:33:42	Not In Use	<input type="checkbox"/>
4	bmj2w45	cm8cp368	2 Profile 2	2003/11/28 10:33:45		2003/11/28 22:33:45	Not In Use	<input type="checkbox"/>
5	x85mi248	qt5mcq35	4 Profile 4	2003/11/28 10:33:48		2003/11/28 22:33:48	Not In Use	<input type="checkbox"/>
							Delete Delete All	
GO <input type="text"/> Page First Previous Next End								

Figure 3-84 Dynamic Account List

Item	Description
Status	This field displays the current state of a
refresh	subscriber's connection. (In Use/Not In Use)
Backup	Click on refresh button to update the dynamic account list page.
Print List	Click it to save the dynamic account information to your computer. (dyn_list.txt)
S/N Username Billing Profile Time Created First Login Expiration Status	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.
Delete	Select the check boxes and click 'Delete' to delete the accounts.
Delete All	Delete all accounts in dynamic account list.

Status Report	
Items	Keypad Hot Key
Daily Account Report Printout 	Press ABCAA
Monthly Account Report Printout 	Press ABCBB
System Status Report Printout 	Press ABCCC
Network Report Printout 	Press ABCAB

Figure 3-85 Account Generator Printer's Hot Key List

Daily Account Report Printout

Daily Account	
2005/12/1	Press ABCAA
S/N	Username B UN Price
000002 7x3dt669	1 1 1.00
TOTAL ACCOUNTS: 1	
TOTAL PRICE: \$1.00	
2005/12/1 15:04:01	
--End--	

Figure 3-86 Daily Account

Monthly Account Report Printout

Monthly Account	
2005/12	Press ABCBB
S/N	Username B UN Price
000001 44khn6	1 1 1.00
000002 7x3dt669	1 1 1.00
000003 8nj9jnvh	1 1 1.00
TOTAL ACCOUNTS: 3	
TOTAL PRICE: \$3.00	
2005/12/1 15:04:01	
--End--	

Figure 3-87 Monthly Account

System Status Report Printout

System Status	WAST	WAN Port Status
ITEM DESCRIPTION	WSTA	Wireless Status
-----	SYST	System
WAST	HOST	Host Name
WSTA	FRMW	Firmware Version
SYST	WFRM	Wireless Firmware Version
HOST	BTRM	Boot Code Version
FRMW	LOCA	Location
WFRM	WAMA	WAN MAC Address
BTRM	LAMA	LAN MAC Address
LOCA	WATP	WAN Port Type
WAMA	WAIP	WAN Port IP
LAMA	WASM	WAN Subnet Mask
WATP	WAGW	WAN Gateway
WAIP	PDNS	Primary DNS
WASM	SDNS	Secondary DNS
WAGW	DHCP	DHCP Type
PDNS	DHSP	DHCP Start IP
SDNS	DHEP	DHCP End IP
DHCP	DHLT	DHCP Lease Time
DHSP	EMAIL	EMAIL Redirect
DHEP	SSID	SSID
DHLT	WCHA	Wireless Channel
EMAIL	WSEC	Wireless Security
SSID		
WCHA		
WSEC		
2005/12/1 15:04:31		
--End--		

Figure 3-88 System Status Report Printout

Network Report Printout

Network	WAST	WAN Port Status
ITEM DESCRIPTION	WSTA	Wireless Status
-----	SYST	System Up Time
WAST	WATD	WAN Tx Data
WSTA	WARD	WAN Rx Data
SYST	WATE	WAN Tx Error
WATD	WARE	WAN Rx Error
WARD	LATD	LAN Tx Data
WATE	LARD	LAN Rx Data
WARE	LATE	LAN Tx Error
LATD	LARE	LAN Rx Data
LARD	WLTD	Wireless Tx Data
LATE	WLRD	Wireless Rx Data
LARE	WITE	Wireless Tx Error
WLTD	WLRE	Wireless Rx Error
WLRD		
WITE		
WLRE		

Figure 3-89 Network Report Printout

3-2-2-8 Port-Location Mapping

Port-Location Mapping

Single Create

Location Identifier (ID): Port Identifier (ID):

Description:

Status: ☐ No Charge ☒ Charge for use ☐ Blocked Add to List

Batch Create

Location ID From: Port ID From: Batch Numbers:

Status: ☐ No Charge ☒ Charge for use ☐ Blocked Add to List

Backup/Restore

Backup to Local PC

Remote TFTP Server IP Address: File Name: Apply

Local PC File Path: Browse Apply

Restore

Remote TFTP Server IP Address: File Name: Apply

Port-Location Mapping List

Location ID	Port ID	Description	Status	Delete
				Delete Delete All

Page FIRST Previous Next END

Figure 3-90 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. <i>Note: When you using VLAN-Tag infrastructure, the Location Identifier (ID) is VLAN ID.</i>
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.
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. <i>Note: When you using VLAN-Tag infrastructure, the Location Identifier (ID) is VLAN ID.</i>
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.

Item	Default	Description
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 Backup to Local PC	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.
<div>Location ID</div> <div>Port ID</div> <div>Description</div> <div>Status</div>	The field name button in this list show that this list can be sorted in ascending/descending order according to the corresponding field name.	
Delete	Select the check boxes and click 'Delete' to delete the accounts.	
Delete All	Delete all accounts in Port-Location Mapping list.	

3-2-3 Advanced Setting

The Advanced Setting section 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 3-91 Advanced Setting Item Screen

3-2-3-1 Customization

Login Page

You can customise the subscriber's login page. The page elements include welcome image, background color and article. The IAC4500 provides three different login page formats, including standard, redirect, advanced and frame format.

Standard

This is the IAC4500 default login page and cannot be changed.

Figure 3-92 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	Allows the administrator to input footnotes such as "Please Contact our Customer Service Center, EXT 142". The maximum character of the footnote is 240.
Copyright	Enable	The copyright section allows 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 a specified color. For the specified text color format please view the color grid. The allowed format is Hexadecimal.

Figure 3-93 Login Page Screen

Welcome	
Please choose from the following service selection	1 day \$10.00 ▾
How many units of Internet access would you like to purchase?	1 ▾
<p>*Please kindly note that there will be no refund once connectivity is confirmed.</p> <p>*Please note that the time block of selected service is based on continuous usage.</p>	
<p>Please click ENTER to confirm your acceptance of the usage charge or CANCEL to exit. The selected service charge will be posted directly into your guest folio.</p>	
<div>Enter</div> <div>Cancel</div>	

Figure 3-94 Login Page Screen Scenario A

Welcome	
Please choose from the following service selection	1 day \$10.00 ▾
How many units of Internet access would you like to purchase?	1 ▾
<p>*Please kindly note that there will be no refund once connectivity is confirmed.</p> <p>*Please note that the time block of selected service is based on continuous usage.</p>	
<p>Please click ENTER to confirm your acceptance of the usage charge or CANCEL to exit. The selected service charge will be posted directly into your guest folio.</p>	
<div>Enter</div> <div>Cancel</div>	

Figure 3-95 Login Page Screen Scenario B

Welcome	
Username:	<input type="text"/>
Password:	<input type="password"/>
<div>Enter</div> <div>Cancel</div>	

Figure 3-96 Login Page Screen Scenario C

Redirect

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


 Redirect	Redirect Login Page URL: <input type="text"/>	Code
---	---	----------------------

Figure 3-97 Redirect Login Page Setting Screen

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

Redirect Login Page Code
<pre> <html> <body style="font-family: Arial" bgcolor="#FFFFFF"> <form method="post" action="http://1.1.1.1/login.cgi" name="apply"> <div align="center"> <table border="1" bordercolordark="#FFFFFF" cellpadding="4" width="90%" bgcolor="#F7F7F7" bordercolorlight="#92B4D6" border="1"> <tr> <td align="center" width="100%" bgcolor="#cccccc" colspan="2"> Welcome </td> </tr> <tr> <td align="right" width="35%" bgcolor="#e6e6e6"> Username: </td> <td width="65%"> <input type="text" name="username" size="25"> </td> </tr> <tr> <td align="right" width="35%" bgcolor="#e6e6e6"> Password: </td> <td width="65%"> <input type="password" name="password" size="25"> </td> </tr> <tr> <td align="center" width="100%" colspan="2"> <input type="submit" style="font-family: Arial" name="apply" value="Enter" style="font-family: Arial"> <input type="reset" style="font-family: Arial" name="clear" value="Clear" style="font-family: Arial"> </td> </tr> </table> </div> </form> </body> </html> </pre>
<input type="button" value="Close"/>

Figure 3-98 Redirect Login Page Code Screen

Advanced

This function allow user to design login page of IAC4500.

Figure 3-99 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 allows the administrator to input a paragraph in the subscriber login page for advertisements or announcements. The maximum character allowance of the article is 1024.
Article Text Color	000000	The article text color can be specified color. For the specified text color format please view 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 view 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	Allows the administrator to input the information such as address, telephone number and fax information. The maximum character allowance 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 allowance of the comment is 80.

Figure 3-100 Example-Advanced Login Page Screen

Frame

If "Frame" is selected the subscriber login page will be separated into a Top Frame and a Bottom Frame. The Bottom Frame is a default format for username and password input, the Top Frame can be a specified URL or customised with text and logos.

Frame	Top Frame	URL: <input type="text" value="http://www.netcomm.com.au"/>
	Bottom Frame	This frame will show the standard login page

Figure 3-101 Frame Login Page Setting Screen

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



Figure 3-102 Example-Login Page Screen

Service Selection Customization

This function allows a service provider to specify text on the login page.

Service Selection customization	
Service Selection Message	Please choose from the following service selection (Max: 80 characters)
Purchase Unit Message	How many units of Internet access would you like to purchase? (Max: 80 characters)
Notification Message 1	*Please kindly note that there will be no refund once connect (Max: 100 characters)
Notification Message 2	*Please note that the time block of selected service is based on (Max: 100 characters)
Notification Message 3	(Max: 100 characters)
Additional Remark	Please click ENTER to confirm your acceptance of the usage (Max: 240 characters)

Figure 3-103 Service Selection Customizations

Welcome

Username:

Password:

Service Selection Message → Please choose from the following service selection 1 day \$10.00

Purchase Unit Message → How many units of Internet access would you like to purchase?

Notification Message 1 → *Please kindly note that there will be no refund once connect

Notification Message 2 → *Please note that the time block of selected service is based on

Notification Message 3 → *Please contact us if you have any question

Additional Remark → Please click ENTER to confirm your acceptance of the usage charge or CANCEL to exit. The selected service charge will be posted directly into your guest folio.

Enter Cancel

Figure 3-104 Login Page

Information Window

This function allows the service provider to decide whether they want an “Information Window” pop-up on the subscribers PC when authentication is successful.

Information Window

Information window is a pop-up window that is presented to subscribers with their browser once after subscriber login successfully. The subscriber can type `http://1.1.1.1/info` to open this window again.

☒ **Display Information Window once after a subscriber logs in successfully**

☐ Redirect

☒ Pop Up
 ☐ Allow to close the pop up window

Information Window Content

Window Name	<input type="text" value="Information Window"/> (Max: 30 characters)
Main message	<input type="text" value="You can use Internet now!"/> (Max: 30 characters)
Message Description	<input type="text" value="This is an information window to show the usage"/> (Max: 150 characters)
Usage count label	<div style="border: 1px solid #add8e6; padding: 2px; margin-bottom: 2px;">Standard usage count time/traffic label or RADIUS with session timeout</div> <div style="display: flex; justify-content: space-between;"> <input type="text" value="Remaining Usage"/> (Max: 30 characters) <input type="text" value="without session timeout"/> </div> <div style="display: flex; justify-content: space-between;"> <input type="text" value="Connecting Usage"/> (Max: 30 characters) <input type="text" value=""/> </div>
<input type="checkbox"/> Warning/Alarm message	<input type="text" value="If you don't want to continue using Internet, please remember to log out. Just click the following button."/> (Max: 150 characters)
<input type="checkbox"/> Notice Message	<div style="border: 1px solid #add8e6; padding: 2px; margin-bottom: 2px;">Notice Text 1</div> <div style="border: 1px solid #add8e6; padding: 2px; margin-bottom: 2px;">Notice Text 2</div> <div style="border: 1px solid #add8e6; padding: 2px; margin-bottom: 2px;">If you are going to use VPN, please close the window before 200.000 VPN connection.</div> <div style="border: 1px solid #add8e6; padding: 2px;">Notice Text 3</div>

Figure 3-105 Information Window Customization Setting Screen

Click Apply button to save the new settings.

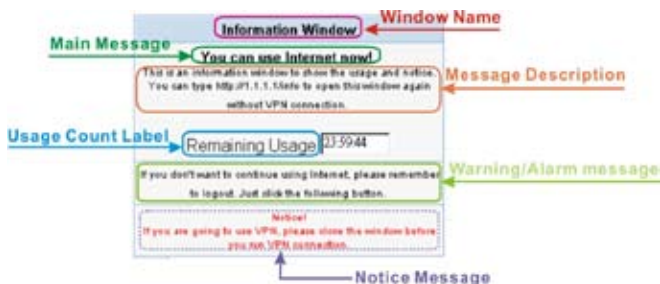


Figure 3-106 Information Window

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

Information Window

You can use Internet now!

This is an information window to show the usage and notice.
You can type `http://1.1.1.1/info` to open this window again
without VPN connection.

Remaining Usage

21:37:5

Figure 3-107 Information Window

Account Printout

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

Account Printout Customization

Title:	<input type="text" value="Welcome!"/> (Max.=23)		
Subtitle:	<input type="text" value="Use to show account information, please login first for your Internet Service."/> (Max.=80)		
Username:	<input type="text" value="Username"/>		
Password:	<input type="text" value="Password"/>		
Usage Time:	<input type="text" value="Usage Time"/>		
Billing Method:	<input type="text" value="Billing"/>		
Billing Profile Description:	<input type="text" value="Profile"/>		
Purchase Unit:	<input type="text" value="Purchase Unit"/>		
<input type="checkbox"/> Additional Label 1:	<input type="text" value="ADD1"/>	Value:	<input type="text"/> (Max.=23)
<input type="checkbox"/> Additional Label 2:	<input type="text" value="ADD2"/>	Value:	<input type="text"/> (Max.=23)
<input checked="" type="checkbox"/> Place:	<input type="text" value="Title"/>		
<input checked="" type="checkbox"/> Account Create Time:	<input type="text" value="profileName"/> <input type="text" value="HH:mm:ss"/> (HH:24h h:12h tt:AM/PM)		
Copy:	<input type="text" value="Please active your account before"/>		
	Description: <input type="text" value="profileName"/> <input type="text" value="HH:mm:ss"/> (HH:24h h:12h tt:AM/PM)		
	Date/Time: <input type="text" value="profileName"/> <input type="text" value="HH:mm:ss"/> (HH:24h h:12h tt:AM/PM)		
	Accumulation: <input type="text" value="After your start login, please finish your login time within."/> (Max.=56)		
<input checked="" type="checkbox"/> Ending:	<input type="text" value="Thank you very much!"/> (Max.=23)		
<input checked="" type="checkbox"/> Serial Number:			

[Preview of PC-connected printer for static account printout](#)

[Preview of account generator printer with static account printout](#)

[Preview of PC-connected printer for dynamic account printout](#)

[Preview of account generator printer with dynamic account printout](#)

Figure 3-108 Account Printout Customization Setting Screen

User Agreement Page

This function allows the user to design a user agreement page for the IAC4500.


User Agreement Page	
Title	<input type="text" value="User Agreement Page"/> (Max. 100 characters)
Title Text Color	<input type="text" value="000000"/> View Color Grid
Article	<div><div></div></div> (Max. 5000 characters)
Article Text Color	<input type="text" value="000000"/> View Color Grid
Article Background Color	<input type="text" value="FFFFFF"/> View Color Grid
Page Background Color	<input type="text" value="FFFFFF"/> View Color Grid
Agree Button	<input type="text" value="Agree"/> (Max. 60 characters)
Disagree Button	<input type="text" value="Do not agree"/> (Max. 60 characters)
 Standard User Agreement Page Preview	
<div>Apply</div>	

Figure 3-109 User Agreement Page Setting Screen

User Agreement Page
<div><div>Agree</div><div>Do not agree</div></div>

Figure 3-110 User Agreement Page Setting Screen

Follow the steps below to setup the user agreement page.

- 1 Select User Agreement, click Apply. (System Setting>Authentication)



Figure 3-111 Authentication Configuration Setting Screen

- 2 Customize the User Agreement Page. (Advanced Setting>Customization>User Agreement Page)

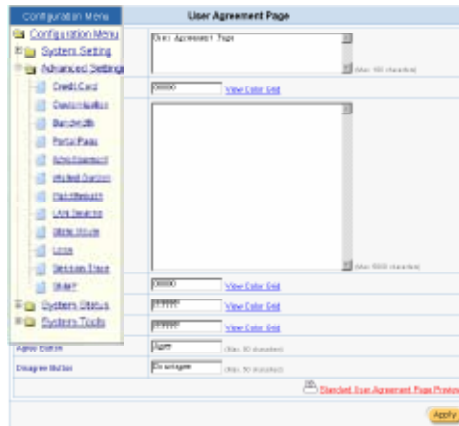


Figure 3-112 User Agreement Page Setting Screen

- 3 Open your browser, the User Agreement Page appears as show below, click Agree.



Figure 3-113 User Agreement Page Dialog Box

- 4 The Login Successfully dialog box appears as show below.



Figure 3-114 Login Successfully Dialog Box

- 5 Enter the IP address/URL of your choice in your browser's location box. Press Enter.

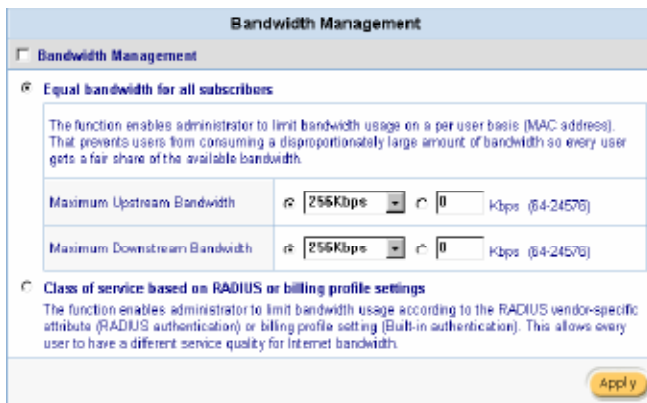


Figure 3-115 Web Browser Location Field

- 6 You can use the Internet now.

3-2-3-2 Bandwidth

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



Bandwidth Management

☒ **Bandwidth Management**

☒ **Equal bandwidth for all subscribers**

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: Kbps (0-24576)

Maximum Downstream Bandwidth: Kbps (0-24576)

☐ **Class of service based on RADIUS or billing profile settings**

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.

Apply

Figure 3-116 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 the administrator to limit bandwidth usage on a per user basis (MAC address). This 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 IAC4500 that has already been configured on this device.
Maximum Downstream Bandwidth	256Kbps	Specify the amount of downstream bandwidth for IAC4500 that has already been configured on this device.
Class of service based on RADIUS or billing profile settings	Disable	This function enables the 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

Portal Page	
This feature allows to redirect subscriber's browser to a specified portal page after successful login.	
URL Link	<input type="text"/>
<div>Apply</div>	

Figure 3-117 Account Printout Customization Setting Screen

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

3-2-3-4 Advertisement

The system allows the service provider to input up to 10 URL links for advertising link purposes.

Advertisement	
This feature allows ISP to specify the advertisement URL link. The advertisement Web page will show on the browser when the subscribers start Network access.	
Frequency	<input checked="" type="radio"/> One Time Only <input type="radio"/> Every <input type="text" value="1"/> Min(s)
Sequence	<input checked="" type="radio"/> Randomly <input type="radio"/> Orderly (From 1 to 10)
Link 1	<input type="text"/>
Link 2	<input type="text"/>
Link 3	<input type="text"/>
Link 4	<input type="text"/>
Link 5	<input type="text"/>
Link 6	<input type="text"/>
Link 7	<input type="text"/>
Link 8	<input type="text"/>
Link 9	<input type="text"/>
Link 10	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 3-118 Advertisement Setup

Item	Default	Description
Frequency	One Time Only	<p>One Time Only – One Time Only means to send the advertisement link once after the subscriber Login.</p> <p>Every-Min(s) – The field means to send the advertisement link every interval minutes. The value range is 1 to 60 (minutes).</p>
Sequence	Randomly	<p>Randomly – Display the advertisement page in the random order.</p> <p>Orderly (From 1 to 10) – Display the advertisement page in the order as setting.</p>
Link 1~10	Empty	<p>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 IAC4500 system. The input format can be "http://www.yahoo.com". The maximum character of the URL Link # is 200.</p>

3-2-3-5 Walled Garden

Allows up to ten URL links that subscribers can access without a username or password. It's free viewing and can be used for advertising local businesses.

Walled Garden

This feature allows subscribers to access the specific Web pages even they didn't have a username or password. We provide ten URL links to use for free trying and can use for advertisement.

Link 1	Name: <input type="text" value="Yahoo"/>
	URL: <input type="text" value="http://www.yahoo.com"/>
Link 2	Name: <input type="text" value="MSN"/>
	URL: <input type="text" value="http://www.msn.com"/>
Link 3	Name: <input type="text" value="Microsoft"/>
	URL: <input type="text" value="http://www.microsoft.com"/>
Link 4	Name: <input type="text"/>
	URL: <input type="text"/>
Link 5	Name: <input type="text"/>
	URL: <input type="text"/>
Link 6	Name: <input type="text"/>
	URL: <input type="text"/>
Link 7	Name: <input type="text"/>
	URL: <input type="text"/>
Link 8	Name: <input type="text"/>
	URL: <input type="text"/>
Link 9	Name: <input type="text"/>
	URL: <input type="text"/>
Link 10	Name: <input type="text"/>
	URL: <input type="text"/>

Apply

Figure 3-119 Walled Garden

Welcome

Username:

Password:

Enter

Cancel

Name

Yahoo

MSN

Microsoft

Copyright(c)2001, 2002 All Rights Reserved.

Figure 3-120 Login Page

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

3-2-3-6 Passthrough

This function allows the administrator to set up some special devices that can pass through the IAC4500 system. These devices do not need to be checked and authorized and may include network devices and local LAN PCs. The IAC4500 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	<input type="text"/>	13	<input type="text"/>	25	<input type="text"/>
2	<input type="text"/>	14	<input type="text"/>	26	<input type="text"/>
3	<input type="text"/>	15	<input type="text"/>	27	<input type="text"/>
4	<input type="text"/>	16	<input type="text"/>	28	<input type="text"/>
5	<input type="text"/>	17	<input type="text"/>	29	<input type="text"/>
6	<input type="text"/>	18	<input type="text"/>	30	<input type="text"/>
7	<input type="text"/>	19	<input type="text"/>	31	<input type="text"/>
8	<input type="text"/>	20	<input type="text"/>	32	<input type="text"/>
9	<input type="text"/>	21	<input type="text"/>	33	<input type="text"/>
10	<input type="text"/>	22	<input type="text"/>	34	<input type="text"/>
11	<input type="text"/>	23	<input type="text"/>	35	<input type="text"/>
12	<input type="text"/>	24	<input type="text"/>	36	<input type="text"/>

Figure 3-121 Subscriber IP Address Pass through Setting Screen

Item	Description
IP Address	There are 36 entries that can be input into the pass through source IP Address. For inputting the IP addresses, please use the format such as "210.208.122.1".

Subscriber MAC Address Pass through

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

Figure 3-122 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	<input type="text"/>	13	<input type="text"/>	25	<input type="text"/>
2	<input type="text"/>	14	<input type="text"/>	26	<input type="text"/>
3	<input type="text"/>	15	<input type="text"/>	27	<input type="text"/>
4	<input type="text"/>	16	<input type="text"/>	28	<input type="text"/>
5	<input type="text"/>	17	<input type="text"/>	29	<input type="text"/>
6	<input type="text"/>	18	<input type="text"/>	30	<input type="text"/>
7	<input type="text"/>	19	<input type="text"/>	31	<input type="text"/>
8	<input type="text"/>	20	<input type="text"/>	32	<input type="text"/>
9	<input type="text"/>	21	<input type="text"/>	33	<input type="text"/>
10	<input type="text"/>	22	<input type="text"/>	34	<input type="text"/>
11	<input type="text"/>	23	<input type="text"/>	35	<input type="text"/>
12	<input type="text"/>	24	<input type="text"/>	36	<input type="text"/>

Figure 3-123 Destination IP Address Pass through

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

Destination URL Pass through

Destination URL Passthrough	
No.	URL Link Page
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>
9	<input type="text"/>
10	<input type="text"/>
<div>Apply</div>	

Figure 3-124 Destination URL Pass through Setting Screen

Item	Description
URL Link Page	There are ten entries that can be input into the pass through URL Link Page. For inputting the URL Link Page, please use the format “http://www.yahoo.com”. The maximum character allowance of the URL Link Page is 200.

Click Apply button to save the new settings.

3-2-3-7 Filtering

This function allows the system administrator to have a list of restricted destinations on the IAC4500.

FILTER

☐ **ENABLE FILTER**

Filtering allows the system administrator to have a list of restricted destinations.

Single IP Address

NO.	IP ADDRESS	NO.	IP ADDRESS
1	<input type="text"/>	4	<input type="text"/>
2	<input type="text"/>	5	<input type="text"/>
3	<input type="text"/>	6	<input type="text"/>

IP Address Range

NO.	IP ADDRESS
1	<input type="text"/> ~ <input type="text"/>
2	<input type="text"/> ~ <input type="text"/>
3	<input type="text"/> ~ <input type="text"/>
4	<input type="text"/> ~ <input type="text"/>
5	<input type="text"/> ~ <input type="text"/>

Apply

Figure 3-125 Filtering Setting Screen

Click Apply button to save the new settings.

3-2-3-8 LAN Devices

Administrator can directly remotely control the LAN Devices via the IAC4500.








LAN Devices						
Accommodate up to 300 entries				Polling Interval: <input type="text"/> Min(s)		
 <input type="button" value="Page"/>  First  Previous  Next  End 						
No.	Device Name	Virtual Port (60001~60300)	Device IP Address	Device Server Port	Device MAC Address	Application
1	<input type="text" value="W1"/>	<input type="text" value="60003"/>	<input type="text" value="192.168.100.102"/>	<input type="text" value="80"/>	<input type="text" value="00900B00253D"/>	<input type="button" value="TCP"/>
2	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="TCP"/>
3	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="TCP"/>
4	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="TCP"/>
5	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="TCP"/>
6	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="TCP"/>
7	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="TCP"/>
8	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="TCP"/>
9	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="TCP"/>
10	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="TCP"/>

Figure 3-126 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.

3-2-3-9 Static Route

This function allows computers that are connected to the IAC4500 directly or through a switch to communicate with other computers in the respective LAN segments which are connected to the IAC4500 through another router.

Static Route					
No.	Destination IP Address	Destination Subnet Mask	Gateway IP Address	Hop Count	Interface
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>
20	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="LAN"/>

Figure 3-127 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.	

3-2-3-10 Private LAN

This function allows the administrator to setup a private LAN under the device's LAN port. Due to the Plug and Play and Layer 2 isolation functions in the IAC4500 devices connected under the LAN port can not communicate with each other. This function is provided to build up a LAN for specified devices to communicate each other.

Figure 3-128 Private LAN Setting Screen

Item	Default	Description
Private LAN	Disable	Enables or disables Private LAN function.
Private LAN Device		
<input checked="" type="radio"/> Start / End IP Address:	<input type="text"/> ~ <input type="text"/>	
Start IP Address	Empty	Enter the start IP address.
End IP Address	Empty	Enter the end IP address
<input checked="" type="radio"/> IP Address:	<input type="text"/>	
IP Address	Empty	
No.	The index number of Private LAN Device.	
Activate	Click on check box, active or inactive the Private LAN device.	
Private LAN Device IP Address List	Display the address(s).	
Delete	Select the check boxes and click 'Delete' to delete the address(s).	
<input type="button" value="Add to List"/>	Click Add to List button to add a new entry.	
<input type="button" value="Apply"/>	Click Apply button to save the new settings.	
<input type="button" value="Delete All"/>	Click Delete All & Apply button to delete all entries.	

Note: The system do not reply ARP to the device which IP address have been registered on Private LAN

3-2-3-11 Logs

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

Syslog

Syslog

Send to Syslog Server

☒ Disable ☐ Enable

☐ Syslog Server on LAN:

Server IP Address:

Server MAC Address:

☐ Syslog Server on WAN:

Server 1 IP Address:

Server 2 IP Address:

Send to Email

☒ Disable ☐ Enable

Email Server:

IP Address or Domain Name:

SMTP Port:

☐ E-mail (SMTP) server needs to check my account

Username:

Password:

Email From:

Name:

Email Address:

Email To:

Email Address 1:

Email Address 2:

Apply

Figure 3-129 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 IAC4500 will send all of its logs to the specified syslog server.
Server MAC Address	Empty	Enter the syslog server's MAC address. The IAC4500 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.

IAC4500 Internet Access Controller User Guide
100

YML858 Rev1
www.netcomm.com.au

Log Settings

Log Settings

The Syslog supports 4 types of syslog level. (161 Alert / 164 Warning / 165 Notice / 166 Inform)

System

Syslog	E-mail	Syslog Name	Description	Interval Time	Type
<input type="checkbox"/>	<input type="checkbox"/>	System Information	A log included system information would be sent according to specified interval time	60 minutes	166
<input type="checkbox"/>	<input type="checkbox"/>	System Boot Notice	Once system reboots, the log would be send	When system reboot	165
<input type="checkbox"/>	<input type="checkbox"/>	System Account Activity Information	A log would be sent if system account (Administrator, Supervisor or Account Operator) login to or logout from the device	When system account login or logout	166

Accounting

Syslog	E-mail	Syslog Name	Description	Interval Time	Type
<input type="checkbox"/>	<input type="checkbox"/>	Account Created	A log would be sent once after an account is created	When account created	166
<input type="checkbox"/>	<input type="checkbox"/>	Subscriber Trace	A log included subscribers login/logout time would be sent once after subscriber logout	When subscriber logout	165
<input type="checkbox"/>	<input type="checkbox"/>	Logged-in User	A log included logged-in users information would be sent according to specified interval time	60 minutes	166
<input type="checkbox"/>	<input type="checkbox"/>	User Agreement	A log would be sent when "user agreement" enabled	When subscriber login	166

Billing

Syslog	E-mail	Syslog Name	Description	Interval Time	Type
<input type="checkbox"/>	<input type="checkbox"/>	Billing Log	A log would be sent according to speafied interval time	When log created	166

LAN Devices Management

Syslog	E-mail	Syslog Name	Description	Interval Time	Type
<input type="checkbox"/>	<input type="checkbox"/>	LAN Devices Information	A log included current LAN Devices Status would be sent according to specified interval time	60 minutes	166 164
<input type="checkbox"/>	<input type="checkbox"/>	LAN Devices Alarm	A log would be sent if one of the LAN Devices detected result is "Fail"	When device fail	161

Alert

Syslog	E-mail	Syslog Name	Description	Interval Time	Type
<input type="checkbox"/>	<input type="checkbox"/>	Administration access Fail	A log would be sent when someone failed to access the administration web server	When someone failed to access the system web server	161
<input type="checkbox"/>	<input type="checkbox"/>	NAT Pool exhausted (IP / Port)	A log would be sent when IP or Port mapping exhausted	When NAT Pool exhausted	161

Apply

Figure 3-130 Logs Setting Screen

Item	Interval Time	Description
System		
System Information	60 minutes 1~10080 Min.	The log includes system information which 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 the device hasn't rebooted, the log will send. Format: (Id, MAC Address) (System Up)
System Account Activity Information	When system account login or logout	A log would be sent if the System Manager logs in to or logs out 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. Format: (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

Item	Interval Time	Description
Logged-in Users	60 Minutes	<p>Login user's information will be sent according to specified interval time.</p> <p>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) (...)(...)</p>
Billing		
Billing Log	When log created	<p>A log would be sent according to specified interval time.</p> <p>Format: (Id, Mac Address) (Billing Log, Username, Billing profile information, Log time, Usage time, Bill, Charge From)</p> <p>Billing Log: PMSI Dynamic Static</p> <p>Charge From: PMS I Dynamic</p> <p>Billing profile name: [Name]</p> <p>Log time: 09/06/2002 08:22:25 (example)</p> <p>Usage time: "30 minutes" or "Expire when 00:00" (example)</p> <p>Billing profile information: [index, name]</p>
LAN Devices Management		
LAN Devices Information	60 Minutes 1~10080 Min.	<p>A log including current LAN devices status would be sent according to a specified interval time.</p> <p>Format: (Id, MAC Address) (LAN Devices Information, Number of devices, Start Number, End number) (Device name, status)(...)(...)</p>
LAN Devices Alarm	When device fail	<p>A log would be sent if one of the LAN devices detected results were "Fail".</p> <p>Format: (Id, MAC Address) (LAN Device Alarm, Device name, FAIL)</p>
Alert		
Administrator access Fail	When someone failed to access the system Web server	<p>A log would be sent when someone failed to access the administration Web server.</p> <p>Format: (Id, MAC Address) (Administration Access Fail, Fail message, User IP, Username)</p> <p>Fail message: Bad Username/Password Unauthorized IP Exceeded Maximum Login</p> <ul style="list-style-type: none"> • Unauthorized IP <p>We can't get the username in this situation, so "None" will be displayed.</p> <ul style="list-style-type: none"> • Exceeded Maximum Login <p>In this situation, we just show the username as below.</p> <p>Administrator Supervisor Accounting Operator</p>

3-2-3-12 Session Trace

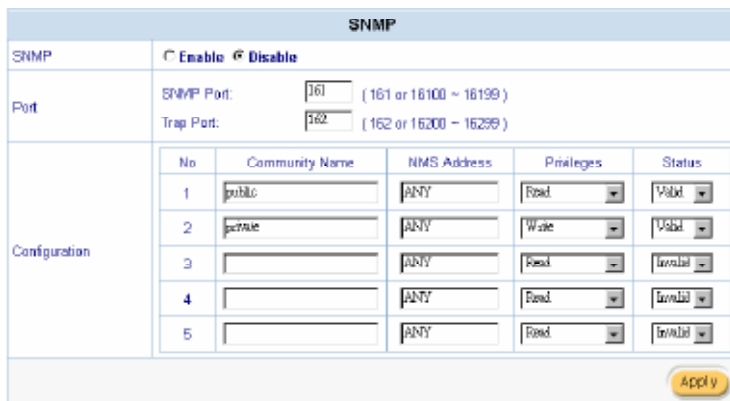
Session Trace	
Session Trace	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
TFTP Server IP Address	Primary TFTP Server IP Address <input type="text"/> Secondary TFTP Server IP Address <input type="text"/>
	Send Session Trace log file every <input type="text" value="10"/> minutes. (5 ~ 1440) <small>(Note: Session Trace log file will be sent also when collected 50 logs)</small>
<input type="button" value="Apply"/>	

Figure 3-131 Session Trace Setting Screen

Item	Default	Description
Session Trace	Disable	Disables or enables session trace function.
TFTP Server IP Address		
Primary TFTP Server IP Address	Empty	Enter the IP address of the primary TFTP server.
Secondary TFTP Server IP Address	Empty	Enter the IP address of the second TFTP server.
Send Session Trace log file every~ minutes.	10 minutes	The field means to send the session trace log file every interval minutes. The value range is 5 to 1440 (minutes).

3-2-3-13 SNMP

The SNMP Agent Configuration screen enables access 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 IAC4500 allows 5 entries to be set.



The screenshot shows the 'SNMP' configuration window. At the top, there's a title bar 'SNMP'. Below it, a tabbed interface with 'Enable' selected. The 'Port' section has 'SNMP Port' set to 161 (range 161-16199) and 'Trap Port' set to 162 (range 162-16299). The 'Configuration' section is a table with 5 rows. Each row has columns for 'No', 'Community Name', 'NMS Address', 'Privileges', and 'Status'. Row 1: 'public', 'ANY', 'Read', 'Valid'. Row 2: 'private', 'ANY', 'Write', 'Valid'. Rows 3-5 are empty, with 'ANY', 'Read', and 'Invalid' as defaults. An 'Apply' button is at the bottom right.

No	Community Name	NMS Address	Privileges	Status
1	public	ANY	Read	Valid
2	private	ANY	Write	Valid
3		ANY	Read	Invalid
4		ANY	Read	Invalid
5		ANY	Read	Invalid

Figure 3-132 SNMP Agent Configuration

Item	Default	Description
SNMP	Disable	Disables or enables the SNMP management.
SNMP Port	161	With SNMP enabled specific port numbers can be selected 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 enabled 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".
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

Displays IAC4500 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 3-134 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 information including the host name, LAN, WAN, DHCP Configuration, DNS, E-mail Server, SSL Certificate Information and the system hardware/firmware version number.

System		
refresh		
System Status	Host Name:	
	Domain Name:	
	Bootrom Version:	1.02
	Firmware Version:	1.00.08
	Concurrent Users Limitation:	1024
	WAN MAC Address:	00:90:0E:01:4A:80
	LAN MAC Address:	00:90:0E:01:4A:7F
WAN IP Settings	WAN Port Mode:	Use fixed IP address
	IP Address:	192.168.100.192
	Subnet Mask:	255.255.255.0
	Default IP Gateway:	192.168.100.254
DNS	Primary DNS Server:	168.95.1.1
	Secondary DNS Server:	
DHCP	DHCP Status:	Server
	Start IP Address (Private):	10.69.1.2
	End IP Address (Private):	10.69.1.254
	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 3-135 System Information Screen

3-2-4-2 Current User List

Displays the current logged-in subscribers' status. It allows the service provider to disconnect subscribers.

No.	Type	IP Address	MAC Address
1		10.99.1.2	001C:8E:56:32:6D

Figure 3-136 Current User Screen-No Authentication

Current User List									
Refresh								Print List	
No.	Type	Username	Billing Profile	Login Time	Expiration	IP Address	MAC Address	Disconnect	
1	Local	102	1	Profile 1	2003/11/08 10:43:48	2003/11/09 10:43:48	192.168.100.156	001C:8E:56:32:6D	<input type="checkbox"/>
								Disconnect Disconnect All	

Figure 3-137 Current User Screen-Port Location Mapping

Current User List

Refresh

Print List

No.	Type	Username	Billing Profile	Login Time	Expiration	IP Address	MAC Address	Disconnect	
1	Dynamic	Top655	2	Profile 2	2003/11/08 11:20:38	2003/11/08 12:20:38	192.168.100.156	00 0C 8E 56:32:6D	<input type="checkbox"/>

WGO

1

Page

First

Previous

Next

Last

Figure 3-138 Current User Screen-Dynamic Account

Current User List

Refresh

Print List

No.	Type	Username	Billing Profile	Login Time	Expiration	IP Address	MAC Address	Disconnect	
1	Static	101	1	Profile 1	2003/11/08 11:23:47	2003/11/09 11:23:47	192.168.100.156	00:0E:56:3C:5D	<input type="checkbox"/>

Disconnect

Disconnect All

1

Page

First

Previous

Next

End

Figure 3-139 Current User Screen-Static Account

Item	Description
	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:5B:3060	10.59.1.2

Figure 3-140 Current User Screen

3-2-4-4 Session List

This feature displays 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 4096 incoming and outgoing packet information, including source IP address, destination IP address, and port number.							
No.	TCP/UDP	IP Client	Port Client	Port Fake	IP Remote	Port Remote	Idle
1	TCP	192.168.100.192	4225	50032	189.254.1.1	445	281
2	TCP	192.168.100.192	4227	50033	189.254.1.1	445	261
3	TCP	192.168.100.192	4239	50040	189.254.1.1	445	163
4	TCP	192.168.100.192	4241	50042	189.254.1.1	445	163
5	TCP	192.168.100.192	4268	50059	207.46.106.105	1863	0
6	TCP	192.168.100.192	4270	50061	189.254.1.1	80	78
7	UDP	192.168.100.192	4274	50064	188.96.1.1	53	51
8	UDP	192.168.100.192	4275	50065	64.4.12.200	7001	51
9	UDP	192.168.100.192	4276	50066	64.4.12.200	7001	51
10	UDP	192.168.100.192	4278	50068	188.96.1.1	53	51
26	TCP	192.168.100.192	4298	50088	211.233.24.82	80	51
27	UDP	192.168.100.192	4299	50089	188.96.1.1	53	51
28	UDP	192.168.100.192	4300	50090	188.96.1.1	53	51
29	UDP	192.168.100.192	4301	50091	188.96.1.1	53	51
30	TCP	192.168.100.192	4302	50092	189.254.1.1	80	26

Figure 3-141 Session List Screen

3-2-4-5 NAT Pool

Displays information about the NAT Pool.

NAT Pool Table				
NAT Pool information. Source IP address, Source MAC address and Translated IP address				
No.	Source IP Address	Source MAC Address	Translated IP Address	VPN Type
1	192.168.100.1	0E-90-80-90-EE-12	211.21.185.240	PPTP
2	192.168.100.2	0E-90-80-90-EE-13	211.21.185.241	PPTP
3	192.168.100.3	0E-90-80-90-EE-14	211.21.185.242	PPTP
4	192.168.100.4	0E-90-80-90-EE-15	211.21.185.243	IPSec
5	192.168.100.5	0E-90-80-90-EE-16	211.21.185.244	IPSec
6	192.168.100.6	0E-90-80-90-EE-17	211.21.185.245	IPSec
7	192.168.100.7	0E-90-80-90-EE-18	211.21.185.246	IPSec
8	192.168.100.8	0E-90-80-90-EE-19	211.21.185.247	IPSec
9	192.168.100.9	0E-90-80-90-EE-20	211.21.185.248	PPTP
10	192.168.100.10	0E-90-80-90-EE-21	211.21.185.249	IPSec

Figure 3-142 Session List Screen

3-2-4-6 LAN Devices Status

You can manage all devices by clicking on the device name to access the 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 (60001~60009)	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

Click

Figure 3-143 LAN Devices Status Screen



Figure 3-126 Example- W1 LAN Device Management Screen

3-2-4-7 Billing Log

This allows you to manage the guest connection status.

Billing Log								
refresh		Export to Text File Clear Log						
No.	Username/Location	Billing Profile	Log Time	Usage Time	Bill	Service Type	Charge from	Status
1	7c182355	Profile 1	2005/10/18 11:19:56	1 day(s)	10.00	Private	Dynamic	Deleted
2	me9ct752	Profile 1	2005/10/18 11:29:52	1 day(s)	10.00	Private	Dynamic	Finished
3	jb9asu23	Profile 1	2005/10/18 11:33:20	1 day(s)	10.00	Private	Dynamic	Finished
4	2p17re42	Profile 1	2005/10/19 10:08:42	1 day(s)	10.00	Private	Dynamic	Finished
5	xipr5t55	Profile 1	2005/10/19 10:08:55	1 day(s)	10.00	Private	Dynamic	Expired
6	111	Profile 1	2005/10/21 10:05:03	1 day(s)	10.00	Private	Static	Deleted
7	222	Profile 1	2005/10/21 10:15:42	3 day(s)	30.00	Private	PMS	Deleted
8	v28hkg30	Profile 1	2005/10/21 10:19:09	1 day(s)	10.00	Private	Dynamic	Expired
9	101	Profile 1	2005/11/02 14:10:18	1 day(s)	10.00	Private	Static	Finished
10	102	Profile 1	2005/11/03 14:32:28	1 day(s)	10.00	Private	Static	Finished
11	103	Profile 1	2005/11/04 14:56:59	1 day(s)	10.00	Private	Static	Finished
12	104	Profile 1	2005/11/07 08:21:25	1 day(s)	10.00	Private	Static	In-Use
GO <input type="text" value="1"/> Page		First Previous Next End						

Figure 3-144 Billing Logs Screen

Item	Description
refresh	Click on refresh button to update the Billing Log page.
Export to Text File	This allow you to export the billing logs to a text file format. (bill_log.txt)
Clear Log	Click on Clear Log to remove all billing log entries.
Username/Location Billing Profile Log Time Usage Time Bill Service Type Charge from	Click the column button to sort the column in ascending/descending order.

3-2-4-8 PMS Transaction Log

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

PMS Transaction Log

Clear log

(HST<-MDS) LS|DA040826|T1151752|

Figure 3-145 PMS Transaction Logs Screen

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

3-2-4-9 Static Route Table

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

Static Route Table					
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 3-146 Static Route Table

3-2-5 System Tools

This allows the service provider or administrator to process Firmware upgrades, change passwords and backup or restore configuration settings.

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

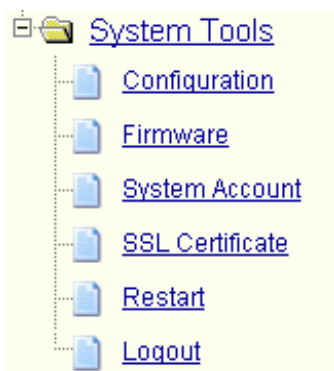


Figure 3-147 System Tools Item Screen

3-2-5-1 Configuration

Use the Configuration item to save, restore or reset configuration parameters of the IAC4500.

Configuration

This feature can import your saved settings to this device or export the stored settings from this device to your PC.

Backup

Click Backup to save the current system configuration to your computer.

TFTP Server IP Address: Text File Name: Apply

Restore

To restore your stored system configuration to this device

File Path: Browse... Apply

TFTP Server IP Address: Text File Name: Apply

Reset the system back to factory defaults

☐ Keep subscriber profile

☐ Keep port-location mapping profile Apply

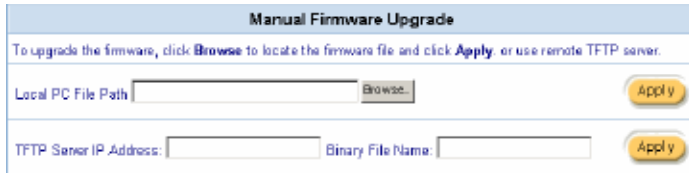
Figure 3-148 Configuration Setting Screen

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; otherwise the agent will not accept it. After downloading the new firmware, the agent will automatically restart.

Manual Firmware Upgrade



The screenshot shows a web-based configuration interface titled "Manual Firmware Upgrade". It contains two sections. The first section, "Local PC File Path", has a text input field, a "Browse..." button, and an "Apply" button. The second section, "TFTP Server IP Address", has a text input field for the IP address, a text input field for the "Binary File Name", and an "Apply" button. A blue instruction bar at the top states: "To upgrade the firmware, click **Browse** to locate the firmware file and click **Apply** or use remote TFTP server."

Figure 3-149 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.

Scheduled Firmware Upgrade

This feature allows you to upgrade the system firmware on a regular (hourly / daily / weekly) basis automatically.

☒ Disable
☐ Enable

TFTP Server IP	<input style="width: 90%;" type="text"/>		
Synchronization Check File	<input style="width: 80%;" type="text"/>		View Sample File
Frequency	<input checked="" type="radio"/> Weekly <input type="radio"/> Daily <input type="radio"/> Hourly <div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">Sunday</div> <div style="margin: 0 10px;">Hour</div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">00</div> <div style="margin: 0 10px;">Min.</div> </div>		

Figure 3-150 Scheduled Firmware Upgrade Setting Screen

Synchronization Check File Sample Code

Version=1.00.01
Filename=iss6000.bin

Figure 3-151 Sample File

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.

Administrator Account	
Administrator can fully control this system and modify all settings.	
Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="*****"/>
Confirm:	<input type="password"/>
Accounting Operator	
Accounting Operator allows front desk clerk to operate the web-based accounting system without touching the other system configuration.	
Username:	<input type="text" value="account"/>
Password:	<input type="password" value="*****"/>
Confirm:	<input type="password"/>
Supervisor Account	
Supervisor can only view system status and change his password.	
Username:	<input type="text" value="supervisor"/>
Password:	<input type="password" value="*****"/>
Confirm:	<input type="password"/>
Super Subscriber Account	
Super subscriber is a built-in subscriber account for system test or premium usage.	
Super Subscriber	<input type="text" value="Disable"/>
Idle Time Out	<input type="text" value="5"/> Min(s) (1~1440)
Username:	<input type="text" value="super"/>
Password:	<input type="password" value="*****"/>
Confirm:	<input type="password"/>
<input type="button" value="Apply"/>	

Figure 3-152 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

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

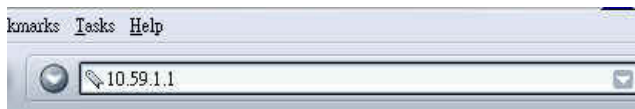


Figure 3-153 Web Browser Location Field (Factory Default)

- 2 The IAC4500 configuration main menu will appear. Enter "admin" (default) as the Username and "admin" (default) as the password and click "Get Started"



Figure 3-154 Administrator Account Login Screen

- 3 After a valid user name and password have been provided, the IAC4500 configuration homepage will appear.



Figure 3-155 System Setting Screen

Web-Based Accounting Manager

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

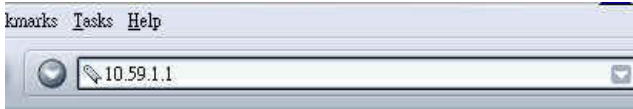


Figure 3-156 Web Browser Location Field (Factory Default)

- 2 The IAC4500 configuration main menu will appear. Enter "account" as the Username and "account" as the password and click "Get Started".



Figure 3-157 Web-Based Accounting Login Screen

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

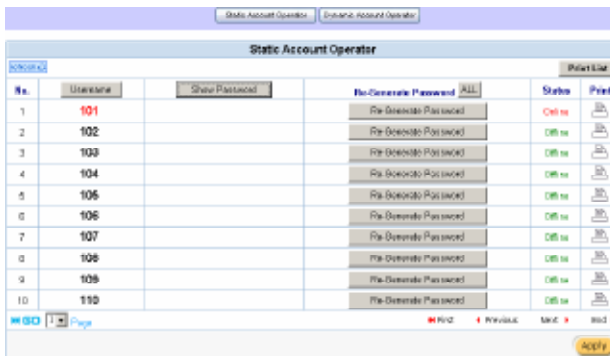


Figure 3-158 Static Account Operator Screen

Or



Figure 3-159 Dynamic Account Operator Screen

Supervisor Account

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

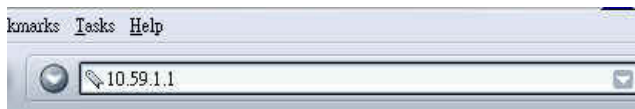


Figure 3-160 Web Browser Location Field (Factory Default)

- 2 The IAC4500 configuration main menu will appear. Enter “supervisor” as the Username and “supervisor” as the password and click “Get Started”.



Figure 3-161 Supervisor Account Login Screen

- 3 After a valid user name and password have been provided, the IAC4500 configuration homepage will appear.

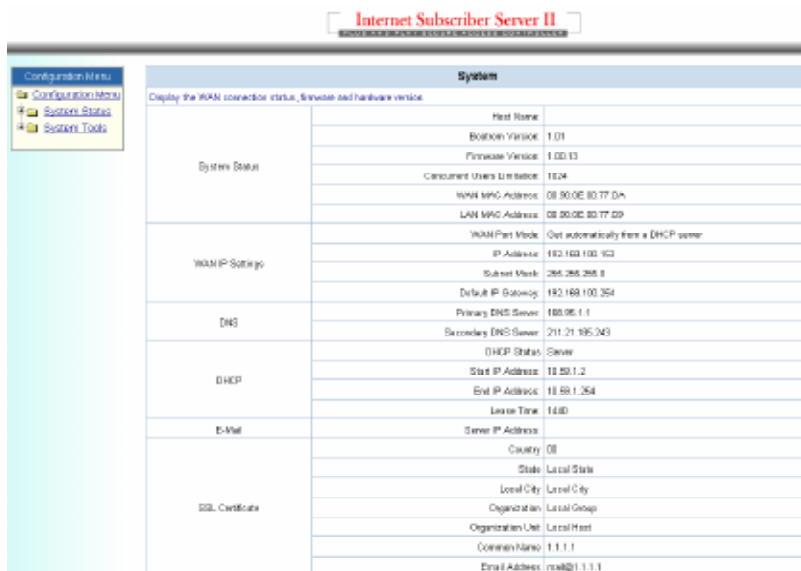


Figure 3-162 System Status & System Tools Setting Screen

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.

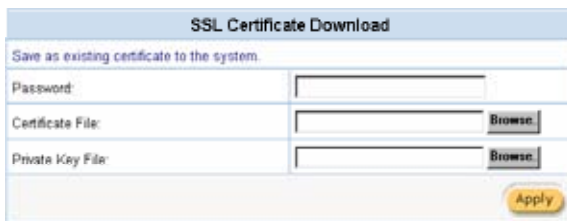


The screenshot shows the NetComm Internet Subscriber Server III login page. It features the NetComm logo on the left and the server name in a red box on the right. Below the header, there are two input fields: 'Username:' and 'Password:'. A 'Get Started' button with a double arrow icon is positioned below the password field. At the bottom, a small line of text reads: 'Web browser: Microsoft Internet Explorer 4.0 and above, Netscape 4.02 or later on'.

Figure 3-163 Super Subscriber Login Page

3-2-5-4 SSL Certificate

The function allows you to download the registered CA certificate into the IAC4500.



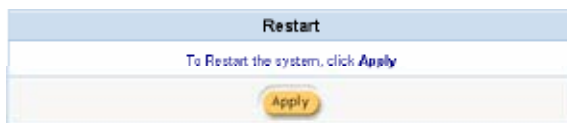
The screenshot shows the 'SSL Certificate Download' screen. It has a title bar and a subtitle 'Save as existing certificate to the system.' Below this, there are three rows of input fields: 'Password:', 'Certificate File:', and 'Private Key File:'. Each row has a 'Browse' button to its right. At the bottom right, there is a yellow 'Apply' button.

Figure 3-164 SSL Certificate Download Setting Screen

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

3-2-5-5 Restart

If your IAC4500 is not operating correctly, you can choose this option to display the restart IAC4500 screen. Clicking the apply button restarts the IAC4500, with all of your settings remaining intact.

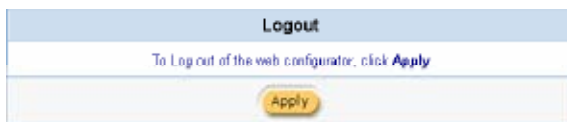


The screenshot shows the 'Restart' screen. It has a title bar and a subtitle 'To Restart the system, click Apply'. Below the subtitle, there is a yellow 'Apply' button.

Figure 3-165 Default Settings Screen

3-2-5-6 Logout

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



The screenshot shows the 'Logout' screen. It has a title bar and a subtitle 'To Log out of the web configurator, click Apply'. Below the subtitle, there is a yellow 'Apply' button.

Figure 3-166 Logout Setting Screen

APPENDIX A. DHCP PRIVATE/PUBLIC IP POOL SETUP

1. Setup the WAN configuration
2. In the Authentication Configuration screen, select Built-in Authentication and Scenario type (A/B/C).



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.

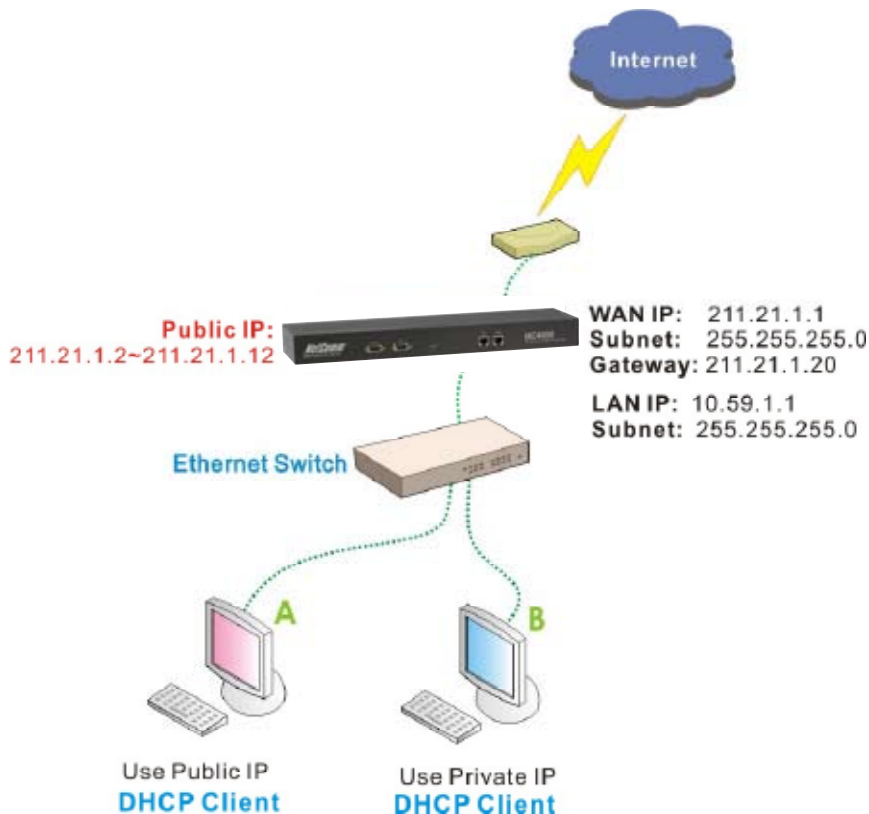
4. Define Billing Profile. Select one service type, Public or Private Service.



Billing Profile Setting				
No.	1			
Name	Profile 1			
Description	As 2008			
Price	Duration	Charge	Check Time	Selective Unit
	0 minutes	0	Period Time Start	From 0 To 23
	0 hour	0	Period Time Start	From 0 To 23
	0 day	10.00	0 Period Time Start	From 0 To 23
	Expire value 10.00			
Bandwidth Limit	<p>Note: You must activate the bandwidth management feature and select a class of service.</p> <p>Maximum Upstream Bandwidth: 0 Kbps 0 Kbps (04-24576)</p> <p>Maximum Downstream Bandwidth: 150 Kbps 0 Kbps (04-24576)</p>			
Service Type	<input type="radio"/> Private Service <input checked="" type="radio"/> Public Service			
Reset		Apply		

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 IAC4500 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 IAC4500 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 IAC4500 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 IAC4500 will route the packet to internet with "NAT".

APPENDIX B: USE RADIUS SERVER TO SETUP YOUR INTERNET SERVICE

IAC4500 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 IAC4500, a 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 IAC4500 the usage time parameters (session time-out) and IAC4500 will obey them to control the connection from subscribers.

IAC4500's RADIUS functionality also includes an accounting feature that allows the IAC4500 to post "accounting start" and "accounting stop" records to RADIUS server. A service provider can use these records to accurately track the usage on their network. IAC4500 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 the subscriber logs in, the system will send an “Access Request” attribute to Radius Server, if subscriber’s account is a valid account, the Radius Server will reply “Access Accept” with “session timeout”. The System will send a “logout Window” including a logout button and countdown timer starting from 2:00:00 to the subscriber’s browser. The subscriber could use the service for 2 hours, and after 2 hours the system will disconnect the subscriber’s connection automatically. However, if 30 minutes after login the subscriber presses the logout button, the system will terminate the connection with the subscriber and send “Accounting Stop” including used time=1800 sec. to the Radius Server. The next time the subscriber logs in, an “Information Window” include a logout button and countdown timer starting from 1:30:00 will appear again.

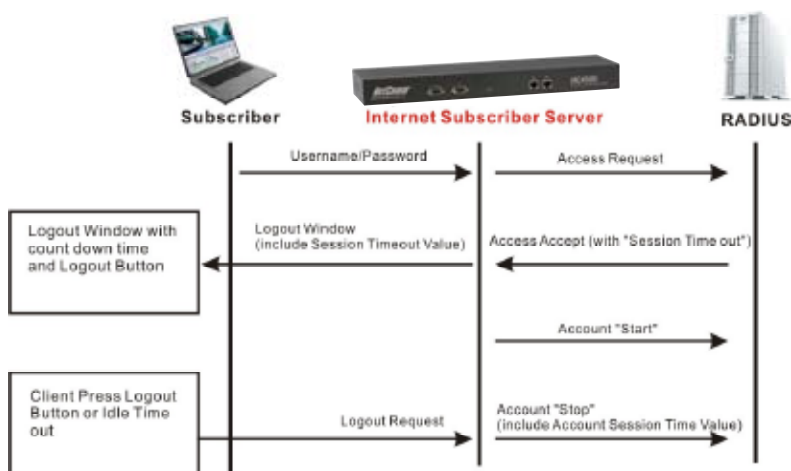


Figure A-1 Accumulate (with Session Time Out)

Information Window
<p>You can use Internet now!</p> <p>This is an information window to show the usage and notice. You can type http://1.1.1.1/info to open this window again without VPN connection.</p>
<p>Remaining Usage: <input type="text" value="01:00:00"/></p>
<p>If you don't want to continue using Internet, please remember to logout. Just click the following button.</p>
<p>Notice! If you are going to use VPN, please close the window before you run VPN connection.</p>
<p>Logout</p>

Figure A-2 Information Window

Case 2: RADIUS Server do not reply “Session timeout” attribute

Service provider creates a subscriber account without a “session timeout” parameter. When the subscriber logs in, the system will send an “Access Request” attribute to the Radius Server, if the subscriber’s account is a valid account, the RADIUS Server will reply “Access Accept” but no “session timeout”. The System will send a “logout Window” including a logout button and connect time starting from 0:00:00 to the subscriber’s browser. Now a subscriber could use the service until they click the logout button. When the subscriber presses the logout button, the system will terminate the connection with the subscriber and send “Accounting Stop” including used time for example 1800 sec. to the RADIUS Server. The RADIUS Server will use these records to accurately track the usage on their network.

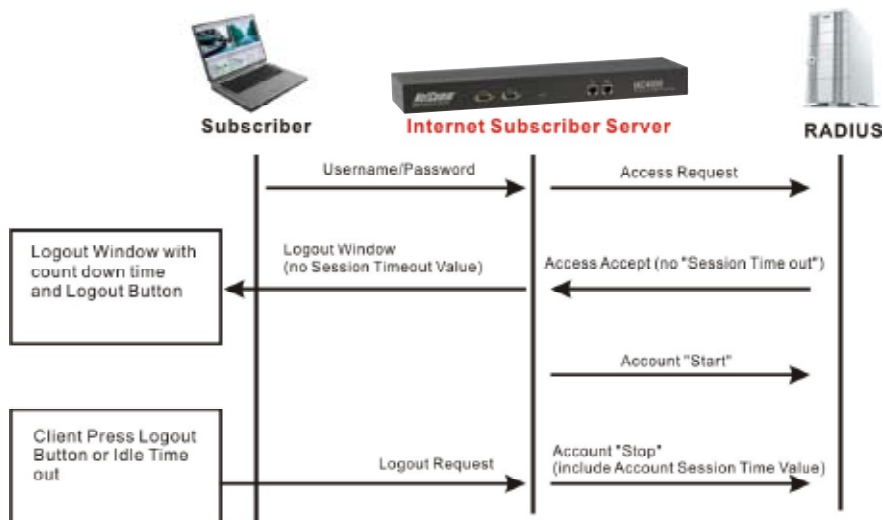


Figure A-3 Accumulate (Without Session Time Out)



Figure A-4 Information Window

Time to Finish

Service providers create a subscriber account with a "session timeout" parameter. For example, "Session Timeout"=2 hour account created and assigned to a subscriber. When the subscriber logs in, the system will send an "Access Request" attribute to the RADIUS Server, the account is a valid account, RADIUS Server will reply "Access Accept" with "session timeout". System will send a "logout window" with a countdown timer starting from 2:00:00 but with no Logout Button to the subscriber's browser. The subscriber could use the service for 2 hours, and after 2 hours the system will automatically disconnect the subscriber's connection. However, the subscriber is not allowed to logout manually. When the system terminates the connection with the subscriber it will send "Accounting Stop" including used time=7200 sec. to the Radius Server. This indicates that the account is only allowed for single 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.

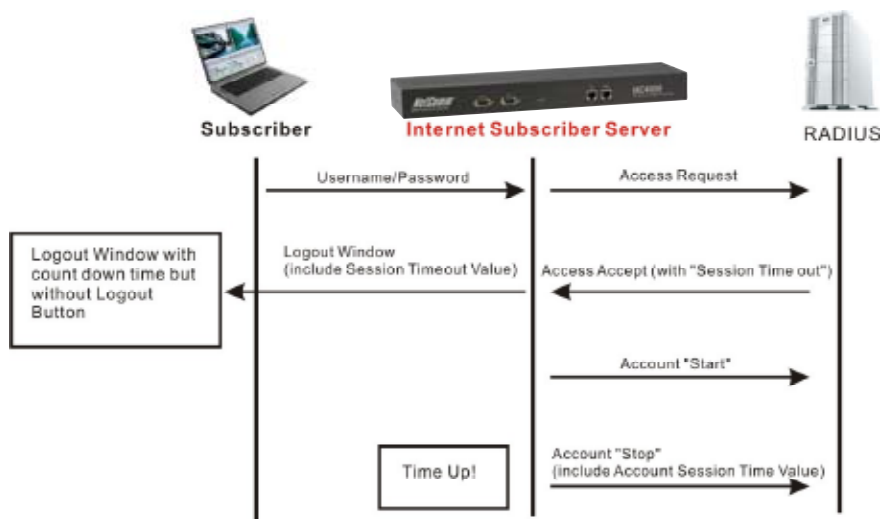


Figure A-5 Time to Finish



Figure A-6 Logout Window

APPENDIX 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

APPENDIX E: 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 meets 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 intended 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



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

www.netcomm.com.au

Note: NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in this User Guide or contact a Network Specialist.

NetComm[®]
www.netcomm.com.au

NetComm Limited ABN 85 002 490 486
PO Box 1200, Lane Cove NSW 2066 Australia
E – sales@netcomm.com.au W – www.netcomm.com.au