



NCT240 IP DSLAM with IAC3000 VLAN Tagging Implementation

The NetComm NCT240 24 Port IP DSLAMs support 802.1Q VLAN Tagging. This white paper is written to assist IP DSLAM system integrator to set up and configure NetComm's NCT240 IP DSLAMs running firmware version V3.0.9 to work with an IAC3000 Internet Access Controller for Internet access and billing application using the VLAN Tagging and Port Location Mapping. It is recommended that the readers of this document has read and understood the Installation Guide and User Manual of the NCT240 IP DSLAM.

The NCT240 IP DSLAM combined with an IAC3000 offers two methods of connection. User can either be issued with a unique user name and password which is required on log in, or using VLAN tagging and the *Port Location Mapping* Feature in the IAC3000. Rooms can then be recognized via its room number.

Both options in the IAC3000 offer zero configurations for subscribers/hotel room guests. Guests simply plug the Ethernet cable into their laptop, enter a username and password or simply accepts the terms and conditions and they are connected without changing any settings at all.

Figure 1 illustrates the logical network diagram for NCT240 IP DSLAM working with an IAC3000.

Logical Network Diagram

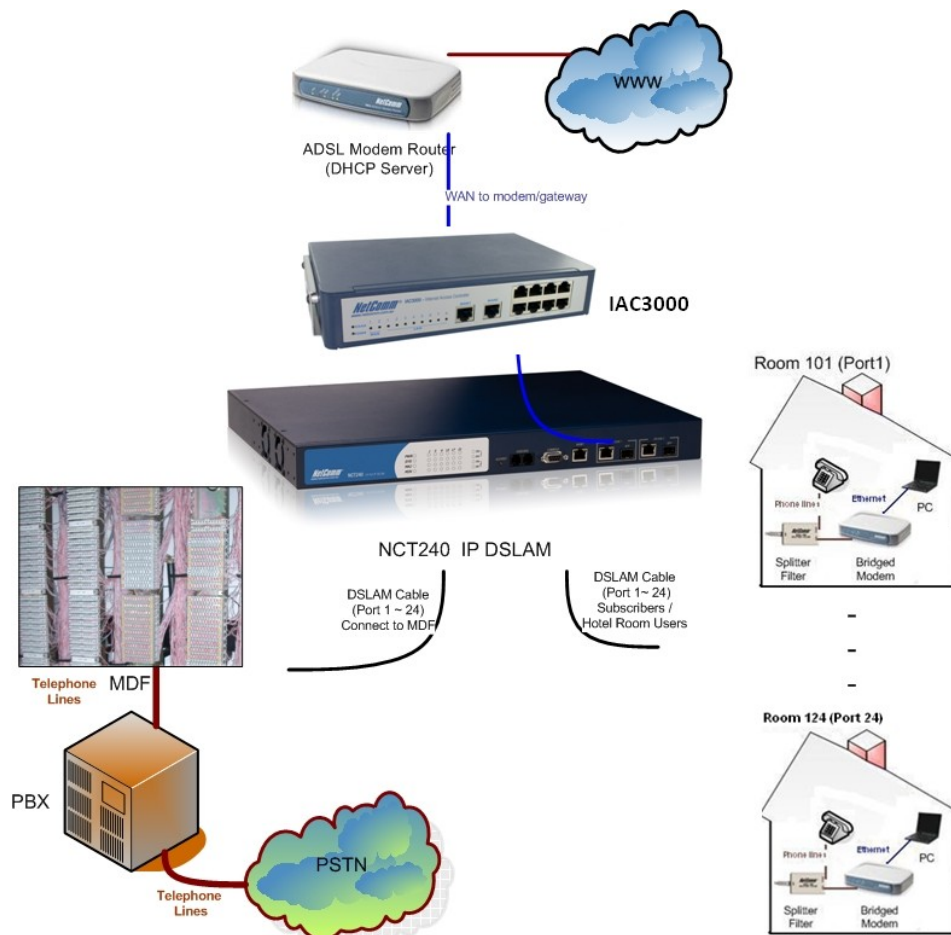


Figure 1: NCT240 with IAC3000 Internet Access Controller

Terms & Concepts

PMS

It stands for Property Management System. Property management systems may be used in real estate, logistics, intellectual property, or hospitality accommodation management. They are computerised systems that facilitate the management of properties, including maintenance, legalities and personnel all through a single piece of software. In this white paper it is referred to the software used by hotel/motel/service apartment to keep guest check-in check –out records and to produce billing invoices and receipts.

AAA

It stands for Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

IAC

It stands for Internet Access Controller; it is referring to the NetComm IAC3000 in this white paper which is responsible for guest Internet AAA management control.

Net Retriever

It is a middleware that acts as an interpreter to between the data that is outputted from the IAC system to the PMS server for billing purposes.

PLM

It stands for Port Location Mapping. It is an IEEE802.1Q VLAN tagging feature implemented in IAC3000.

R2T8

Postfix 'R2T8' of the modem router NB6plus4_R2T8 is referring to a modem router that is running bridge mode hotel firmware. It acts as a plug and play device to convert ADSL signals to Ethernet signals.

GE

It stands for Gigabit Ethernet. It is the standard for a high-speed Ethernet. It has a maximum data transmission rate of 1000Mb/s or 1 Gigabit/s.

xDSL

It is refer ADSL in this document. It covers ADSL, ADSL2, and ADSL2+, unless otherwise indicated.

IAC3000 VLAN Management

The IAC3000 offers two methods of connection. Users can either be issued a unique user name and password, or using VLAN tagging, the *Port Location Mapping* Feature in the IAC. Rooms can then be recognized via its room number. Both options offer zero configurations for subscribers/hotel room guests. Guests simply plug the Ethernet cable into their laptop, enter a username and password or simply accepts the terms and conditions and they are connected without changing any settings at all. This

white paper will focus on the configuration for setting up VLAN tagging, the port location mapping function of the IAC3000.

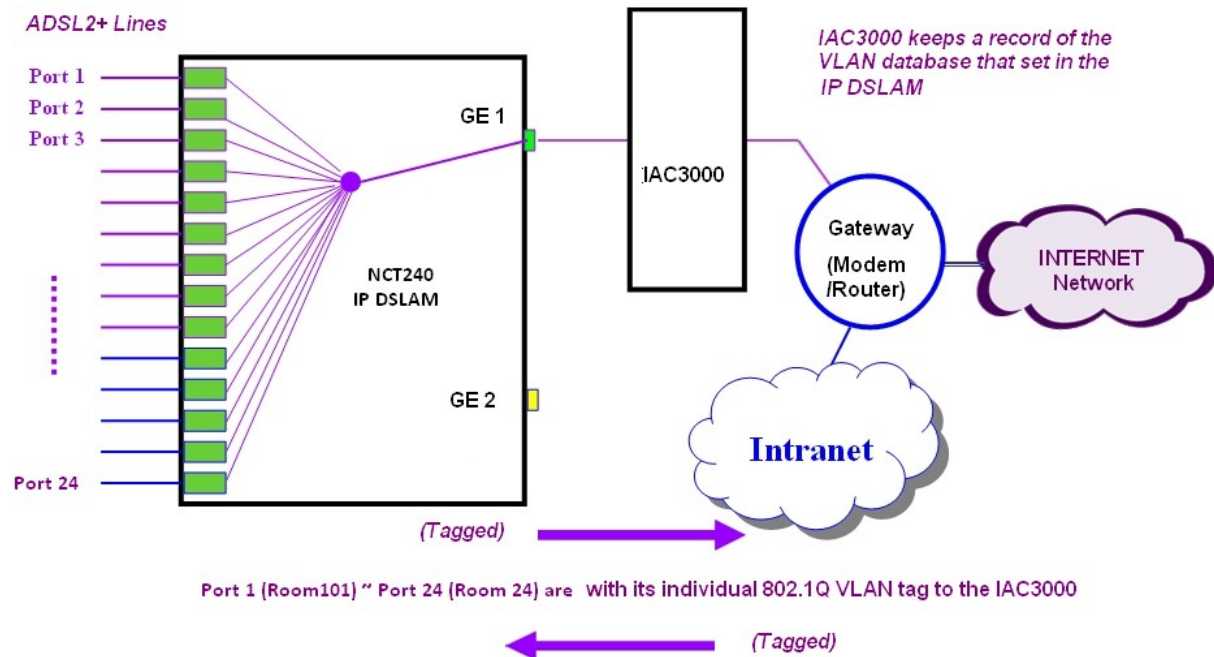


Figure 2: 802.1Q VLAN Tagging relationship between NCT240 and IAC3000

Service Zones

The IAC3000 support 9 different service zones (the default service zone, service zone 1 to 8). The two system modes for service zones are 'Port Based Mode' and 'Tagged Based Mode'. The default service zone is always enabled in both modes; SZ1 to SZ8 are disabled by default and require the administrator to enable it and make necessary configurations when needed.

Each SZ configuration page is a summarized page that consists of hyperlinks to its sub configuration pages. The settings that you can make in a SZ configuration are:

- Service Zone Status
- Service Zone Name
- Service Zone VLAN Tagged Number (required in tagged based mode)
- Service Zone Mgmt IP address
- Service Zone DHCP Server/Relay
- Service Zone Authentication Setting/Options (Which Authentication server to be used in this SZ)
- Service Zone Authentication Setting/Options > Configure Authentication Server/s
- Service Zone Custom Pages (this means every SZ in the IAC3000 can have its own custom login/logout pages; the custom pages include PLM user charge / free login pages)
- Service Zone Group Configuration (Bandwidth, QoS)

- Service Zone Policy Configuration (FW Rule, Route Rule, Session Limit)
- Service Zone APs (central management)

By default under 'Tagged based' Mode, each SZ has its pre-assigned VLAN tagged number 1 to 8. See screen shot below.

Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default	--	NetCom m_IAC3 000	None	Policy 1	Server 1	Enable	Configure
SZ1	1	NetCom m_IAC3 000-1	None	Policy 1	Server 1	Disable	Configure
SZ2	2	NetCom m_IAC3 000-2	None	Policy 1	Server 1	Disable	Configure
SZ3	3	NetCom m_IAC3 000-3	None	Policy 1	Server 1	Disable	Configure
SZ4	4	NetCom m_IAC3 000-4	None	Policy 1	Server 1	Disable	Configure
SZ5	5	NetCom m_IAC3 000-5	None	Policy 1	Server 1	Disable	Configure
SZ6	6	NetCom m_IAC3 000-6	None	Policy 1	Server 1	Disable	Configure

Note:

The Service Zone VLAN tagged number is used to identify the Service Zone. Please do not use the same VLAN tagged number in the PLM configuration.

VLAN

VLAN stands for Virtual Local Area Network. It is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain. A VLAN allows a physical network to be divided into several logical networks. An end device can be assigned to more than one VLAN group. Devices from different VLANs cannot communicate with each other. VLAN tags can be added to the MAC header to identify the VLAN membership of a frame across bridges. A tagged frame is four bytes longer than an untagged frame.

Part 1: NCT240 VLAN Tagging Configuration

There are 3 types of management interfaces available for NCT240 IP DSLAM system management. The web management interface, the CLI interface and the Telnet interface.

It is recommended to use the built-in web management interface for NCT240 system configuration. This white paper is written in the basis of using the web management interface of the NCT240 IP DSLAM.

Step 1

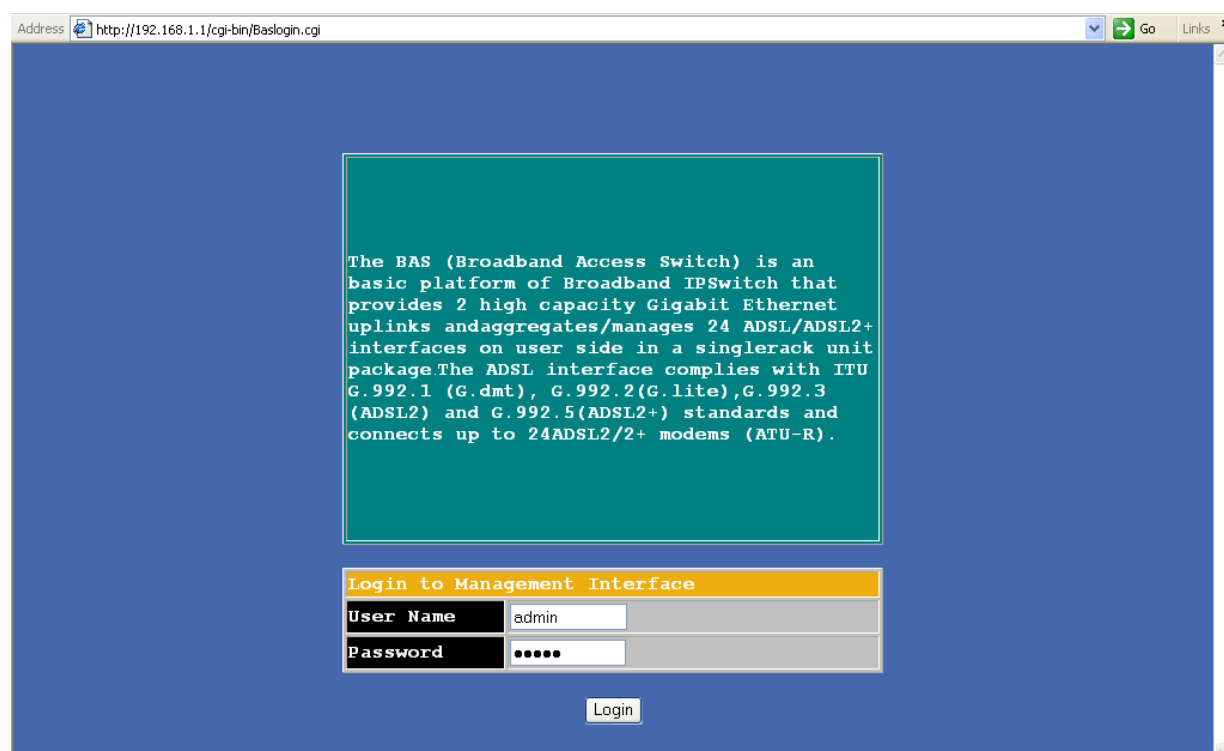
Connect the PC to the management port. Manually configure your PC to 192.168.1.x address (eg: 192.168.1.2/24)

Login to NCT240 web management interface.

Default IP address for ixp0 (system management port): **192.168.1.1/24**

Default User Name: admin

Default Password: admin



Navigate to:

Home > Switch > VLAN

- Basic VLAN Settings > (Refer to settings as shown) then click Apply then OK.
- VLAN Switch Mode > (Refer to settings as shown) then click Apply then OK.
- VLAN Frame Type > (Refer to settings as shown) then click Apply then OK.

Address <http://192.168.1.1/main.html> Go Links »

Broadband Access Switch

[Home](#) [Logout](#)

- Home
- + System
- + ADSL
- Switch
 - VLAN
 - EthPortSetting
 - MAC
 - IGMP Snooping
 - IGMP Group List
 - 802.1x
 - QueueMap
 - DHCP Relay Option82
 - LoopTest
 - RSTP
- + Status
- + IP
- + Performance
- + Statistics
- + Configuration

VLAN Basic Setting

DeviceID:0 TargetID:0 [VlanAdvSetting](#) [DisplayVlanSetting](#)

Basic VLAN Setting

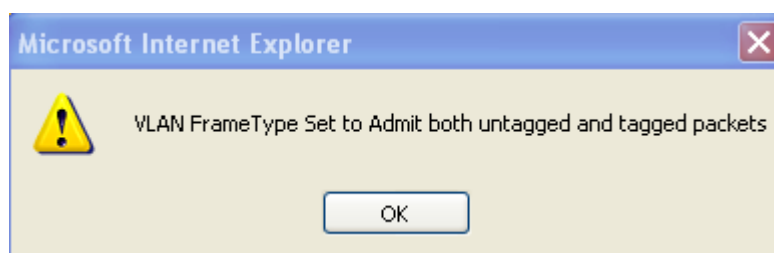
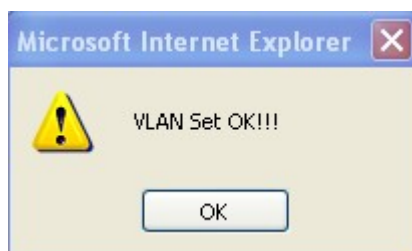
Default VLAN	Priority	MinPortID	PVC ID	MaxPortID	PVC ID
101 (0~4095)	0 (0~7)	1	1	1	1

VLAN SwitchMode

Mode
Forwarding by MAC only

VLAN FrameType

FrameType	MinPortID	PVC ID	MaxPortID	PVC ID
Admit both untagged and tagged packets	1	1	1	1



By following the above settings, it means that ADSL port 1 (PVC1: 8/35) packets are to be assigned with a VLAN 101 number and will be tagged as they leave the uplink of the NCT240 IP DSLAM. NCT240 will both admit untagged and tagged packets.

Repeat the above VLAN configuration to create VLAN 101 ~ VLAN 124 for all the 24 ADSL Ports in the NCT240. Example: refer to screen shot for VLAN 102 configuration shown as follows

Address <http://192.168.1.1/main.html> Go Links »

Broadband Access Switch

[Home](#) [Logout](#)

- Home
- System
- ADSL
- Switch
 - VLAN
 - EthPortSetting
 - MAC
 - IGMP Snooping
 - IGMP Group List
 - 802.1x
 - QueueMap
 - DHCP Relay Option82
 - LoopTest
 - RSTP
- Status
- IP
- Performance
- Statistics
- Configuration

VLAN Basic Setting

DeviceID:0 TargetID:0 [VlanAdvSetting](#) [DisplayVlanSetting](#)

Basic VLAN Setting

Default VLAN	Priority	MinPortID	PVC ID	MaxPortID	PVC ID
102 (0~4095)	0 (0~7)	2	1	2	1

VLAN SwitchMode

Mode
Forwarding by MAC only

VLAN FrameType

FrameType	MinPortID	PVC ID	MaxPortID	PVC ID
Admit both untagged and tagged packets	2	1	2	1

To view the current VLAN setting, click on **DisplayVLANSettings** to view the current VLAN information for all the 24 ADSL ports.

Address <http://192.168.1.1/main.html> Go Links »

Broadband Access Switch

[Home](#) [Logout](#)

- Home
- System
- ADSL
- Switch
 - VLAN
 - EthPortSetting
 - MAC
 - IGMP Snooping
 - IGMP Group List
 - 802.1x
 - QueueMap
 - DHCP Relay Option82
 - LoopTest
 - RSTP
- Status
- IP
- Performance
- Statistics
- Configuration

Display VLAN Setting

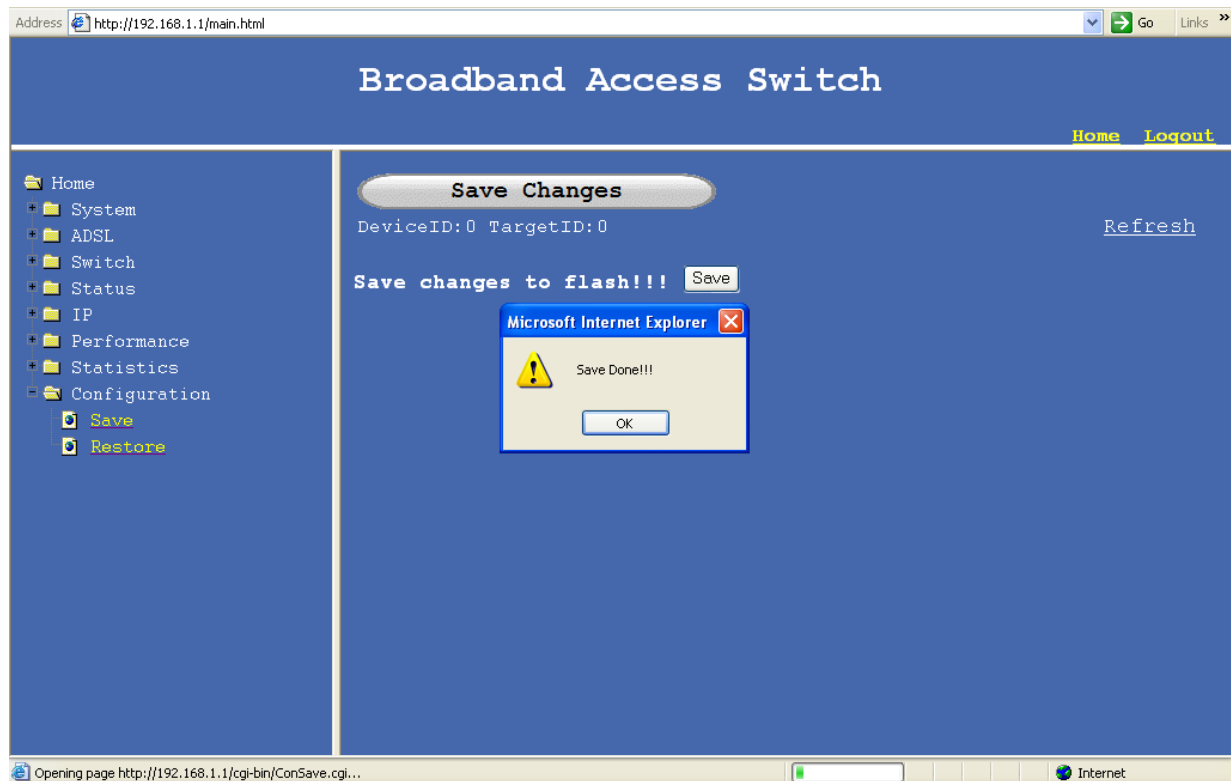
DeviceID:0 TargetID:0 [VlanAdvSetting](#) [VlanBasicSetting](#) [Refresh](#)

Port	PVC	Default VLAN	Priority	Stack VLAN	Stack Priority	RX Strip	RX Tag	TX Strip	TX Tag
1	1	101	0	101	0	0	1	1	0
1	2	0	0	0	0	0	0	0	0
1	3	0	0	0	0	0	0	0	0
1	4	0	0	0	0	0	0	0	0
1	5	0	0	0	0	0	0	0	0
1	6	0	0	0	0	0	0	0	0
1	7	0	0	0	0	0	0	0	0
1	8	0	0	0	0	0	0	0	0
2	1	102	0	102	0	0	1	1	0
2	2	0	0	0	0	0	0	0	0
2	3	0	0	0	0	0	0	0	0
2	4	0	0	0	0	0	0	0	0
2	5	0	0	0	0	0	0	0	0
2	6	0	0	0	0	0	0	0	0
2	7	0	0	0	0	0	0	0	0

Step 2

Navigate to:

Home > Configuration > Save > click on Save then Ok.



Part 2: IAC3000 Port Location Mapping Configuration

Overview

Part 2 describes how to configure the IAC3000 for Port Location Mapping application with PMS billing integration.

The logical order of configuration described in this section is as follows.

- Configure IAC3000 system information
- Configure administration accounts
- Configure WAN 1, WAN 2, and WAN traffic load balancing settings
- Configure system to tag-based mode
- Configure service zone (SZ) settings
- Configure 'on-demand billing plans' under on-demand user server
- Configure 'custom login pages'
- Configure 'group' and 'policy' setting for user bandwidth control
- Configure port location mapping VLAN entries and map to the appropriate service zone
- Configure NetRetriever parameters for PMS billing integration

IAC3000 described in this white paper will have two service zone enabled. The two service zones are the default SZ: 192.168.30.1/24 and SZ 1:192.168.31.1/24. Default service zone provides user login page for untagged traffic and for VLAN account roaming purposes. SZ1 is set up for Port Location Mapping VLAN users. The default service zone is enabled by default but SZ1 and its configuration will require administrator configuration; details are discussed in the next section.

Steps & Procedures

Step 1:

Connect an Ethernet cable to one of the LAN port of the IAC3000. Open the IAC3000 web management interface by using the following login details

Default LAN Mgt IP address: <http://192.168.30.1>

Default admin user name: admin

Default admin Password: admin

This document is being created at a time when the following version of firmware was in production:

- IAC3000: Firmware V2.00.01_01000

Please make sure the IAC3000 is running the firmware V2.00.01_01000 or later to use port location mapping feature. For more details please visit the NetComm website <http://www.netcomm.com.au/support> for more details.

Configure IAC3000 system information:

System
Configuration

User
Authentication

AP
Management

Network
Configuration

Utilities

Status

Configuration Wizard

System Information

WAN1 Configuration

WAN2 Configuration

WAN Traffic Settings

LAN Port Mapping

Service Zones

Port Mapping

System Information

System Information

System Name	<input type="text" value="NetComm IAC3000"/>
Administrator Contact Information	<input type="text" value="Network Administrator Phone Number"/>
Device Name	<input type="text"/> <input type="checkbox"/> Use the name on the security certificate (FQDN for this device)
Portal URL	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="text" value="http://www.netcomm.com.au"/> (e.g. http://www.google.com/)
Access History IP	<input type="text"/> (e.g. 192.168.2.1)
Management IP Address List	Setup Management IP Address List
SNMP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
User Logon SSL	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Time	<p>Device Time : 2009/09/03 12:07:31</p> <p>Time Zone : <input type="text" value="(GMT+10:00)Canberra,Melbourne,Sydney"/> </p> <p><input checked="" type="radio"/> NTP Enable</p> <p>NTP Server 1: <input type="text" value="ntp1.cs.mu.OZ.AU"/> *(e.g. tock.usno.navy.mil)</p> <p>NTP Server 2: <input type="text" value="tock.usno.navy.mil"/></p> <p>NTP Server 3: <input type="text" value="ntp1.fau.de"/></p> <p>NTP Server 4: <input type="text" value="clock.cuhk.edu.hk"/></p> <p>NTP Server 5: <input type="text" value="ntps1.pads.ufrj.br"/></p> <p><input type="radio"/> Set Device Date and Time</p>

Note:

'Management IP Address List' by default is set to allow IP address 0.0.0.0/0.0.0.0 to see the IAC3000 web management interface, this settings will be site specific. It is recommended to only allow a specific IP address or a specific IP address range to access the IAC3000 device management interface. For example, if you only allow the device management via the WAN interface, you need to remove the 0.0.0.0/0.0.0.0 in the first entry and replace it with your desired IP address range, eg: 172.16.1.0/24. Please refer to the IAC3000 user manual for more details.

Step 2:

Change IAC3000 administration password.

Navigate to **Utilities > Change Password > change administrator, manager and operator password.**

Default Admin user name: admin

Default Admin password: admin

Default Manager User name: manager

Default Manager Password: manager

Default Operator User name: operator

Default Operator Password: operator

The screenshot displays the 'Change Password' utility in the IAC3000 web interface. The top navigation bar includes 'System Configuration', 'User Authentication', 'AP Management', 'Network Configuration', 'Utilities' (highlighted), and 'Status'. The left sidebar contains 'Change Password' (highlighted), 'Backup/Restore Settings', 'Firmware Upgrade', 'Restart', and 'Network Utilities'. The main area is titled 'Change Password' and contains three sections:

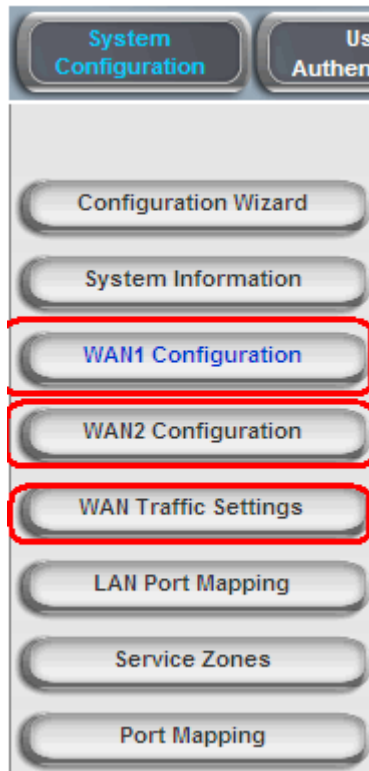
- Change Admin Password:** Includes fields for 'Old Password', 'New Password', and 'Verify Password', with 'Apply' and 'Clear' buttons below.
- Change Manager Password:** Includes fields for 'New Password' and 'Verify Password', with 'Apply' and 'Clear' buttons below.
- Change Operator Password:** Includes fields for 'New Password' and 'Verify Password', with 'Apply' and 'Clear' buttons below.

Step 3:

Configure WAN 1, WAN 2, and WAN traffic load balancing settings.

- Navigate to **System Configuration > WAN 1 Configuration**
- Navigate to **System Configuration > WAN 2 Configuration**
- Navigate to **System Configuration > WAN Traffic Settings**

It is recommended to assign static IP addresses to the WAN interfaces of the IAC3000 for device management purposes. If there is only one WAN internet connection available, steps 'b' and 'c' are not required. Since the IP address details for WAN 1 and WAN 2 are site specific, they are not discussed in this whitepaper.



Step 4:

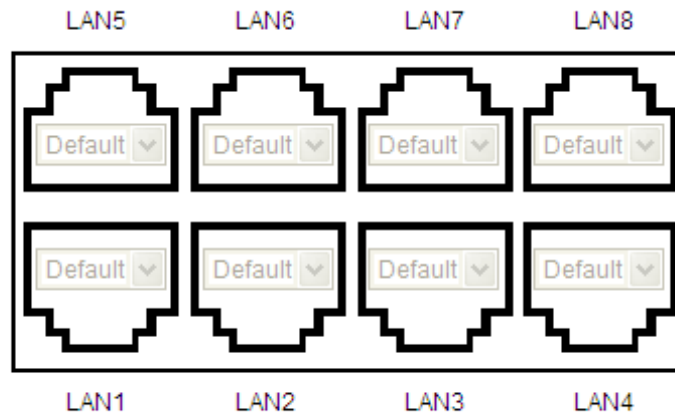
Configure and confirm that the IAC3000 is set to tag-based mode. By default the IAC3000 LAN Port Mapping is set to Tagged Mode. To begin with, it is assumed that you have performed a factory load default to the IAC3000 via the management interface. Please verify IAC3000 is configured in VLAN Tagged Mode.

Navigate to **System Configuration > LAN Port Mapping > Service Zone Mode > Tagged based.**

Service Zone Port Role Setting

Select Service Zone Mode ☐ Port Based
☒ Tag Based

In tag based mode, every port maps to every Service Zone.



Step 5:

Configure Service Zone settings

Step 5.1

Click on 'Configure' button to configure SZ1.

Perform the following configurations to SZ1.

- Change the VLAN tagged number from 1 to 10 for SZ1
- Configure IP Address, DHCP server, DHCP server pool, and DNS details for SZ1
- Configure 'on-demand billing plans' under on-demand user server
- Configure 'custom login pages'
- Configure PLM charge login page
- Configure PLM free login page
- Configure User Group for SZ1 (bandwidth control)
- Configure User Policy for SZ1 (user session limit)

Warning:

Please make sure the VLAN tagged number of the service zone and the port location VLAN room number are unique in the IAC3000 system for the Port Location Mapping to work properly. They should not share the same VLAN tagged number.

Navigate to **System Configuration > Service Zones > SZ1** to configure **SZ1 basic settings**.

The area that requires attention is highlighted by red boxes in the screen shot below. Please make sure the valid DNS server addresses are used for 'Prefer DNS server' and 'the alternate DNS server'. The detail setting for 'authentication servers', 'custom pages', group and policy settings will be described later in this section.

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

Service Zone Settings

Basic Settings

Service Zone Status: ☒ Enable ☐ Disable

Service Zone Name:

Network Settings

VLAN Tag: (range: 1 ~ 4094)

Operation Mode: ☒ NAT ☐ Router

IP Address:

Subnet Mask:

DHCP Server Settings

☐ Disable DHCP Server ☒ Enable DHCP Server

Start IP Address:

End IP Address:

Preferred DNS Server:

Alternate DNS Server:

Domain Name:

WINS Server IP:

Lease Time:

[Reserved IP Address List](#)

☐ Enable DHCP Relay

SIP Interface Configuration					
Enabled <input type="checkbox"/>	WAN Interface		WAN1		

Authentication Settings					
Authentication Status <input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	Server 2	POP3	pop3	<input type="radio"/>	<input type="checkbox"/>
	Server 3	RADIUS	radius	<input type="radio"/>	<input type="checkbox"/>
	Server 4	LDAP	ldap	<input type="radio"/>	<input type="checkbox"/>
	On-demand User	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>
Custom Pages	SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>
	Login Page				Configure
	Port Mapping Free Login Page				Configure
	Port Mapping Charge Login Page				Configure
	Logout Page				Configure
	Login Success Page				Configure
	Login Failed Page				Configure
	Login Success Page for On-demand User				Configure
	Logout Success Page				Configure
Logout Failed Page				Configure	

Group Permission for this Service Zone		Configure
Default Policy in this Service Zone		Policy 1 Edit System Policies
Email Message for Login Reminding		<input checked="" type="radio"/> Enable <input type="radio"/> Disable Edit Mail Message

Wireless Settings			
Set SSID	NetComm_IAC3000-1		
Access Point Security	Authentication	Open System <input type="checkbox"/> Enable 802.1X Authentication	
	Encryption	None	

Managed AP in this Service Zone			
AP Type	AP Name	IP Address	Status
		MAC Address	

You should restart the system to activate the changes. [Restart](#)

Click the '**Apply**' button to apply new settings to SZ1. Click on '**Restart**' to restart the system to make new changes to take effect.

Step 5.2

Reboot the system to make SZ1 changes effective. IAC3000 system reboot generally takes 100sec to complete. Once the system has finished rebooting, you should see the SZ1 overview page shown as follows.

Re-login to IAC3000 using the new admin password, navigating to **System Configuration > Service Zone**, it is expected that **SZ1 is now enabled with VLAN tag number 10**.

System Configuration
User Authentication
AP Management
Network Configuration
Utilities
Status

Configuration Wizard

System Information

WAN1 Configuration

WAN2 Configuration

WAN Traffic Settings

LAN Port Mapping

Service Zones

Port Mapping

Service Zone Settings

Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default	--	NetCom m_IAC3 000	None	Policy 1	Server 1	Enable	Configure
SZ1	10	NetCom m_IAC3 000-1	None	Policy 1	Server 1	Enable	Configure
SZ2	2	NetCom m_IAC3 000-2	None	Policy 1	Server 1	Disable	Configure
SZ3	3	NetCom m_IAC3 000-3	None	Policy 1	Server 1	Disable	Configure

Step 5.3

Configure on-demand account billing plans. Navigate to **System Configuration > SZ1** and click on 'On-Demand User' server, and navigate to 'Billing Plans' to create your desired billing plans; or navigate to **User Authentication > Authentication Configuration > On-demand User >**

System Configuration
User Authentication
AP Management
Network Configuration
Utilities
Status

Authentication Configuration

Black List Configuration

Group Configuration

Policy Configuration

Net Retriever

Additional Configuration

Authentication Server Configuration

Authentication Server - On-demand User	
General Settings	Configure
Ticket Customization	Configure
Billing Plans	Configure
External Payment Gateway	Configure
On-demand Account Creation	Create
On-demand Account List	View

Note:

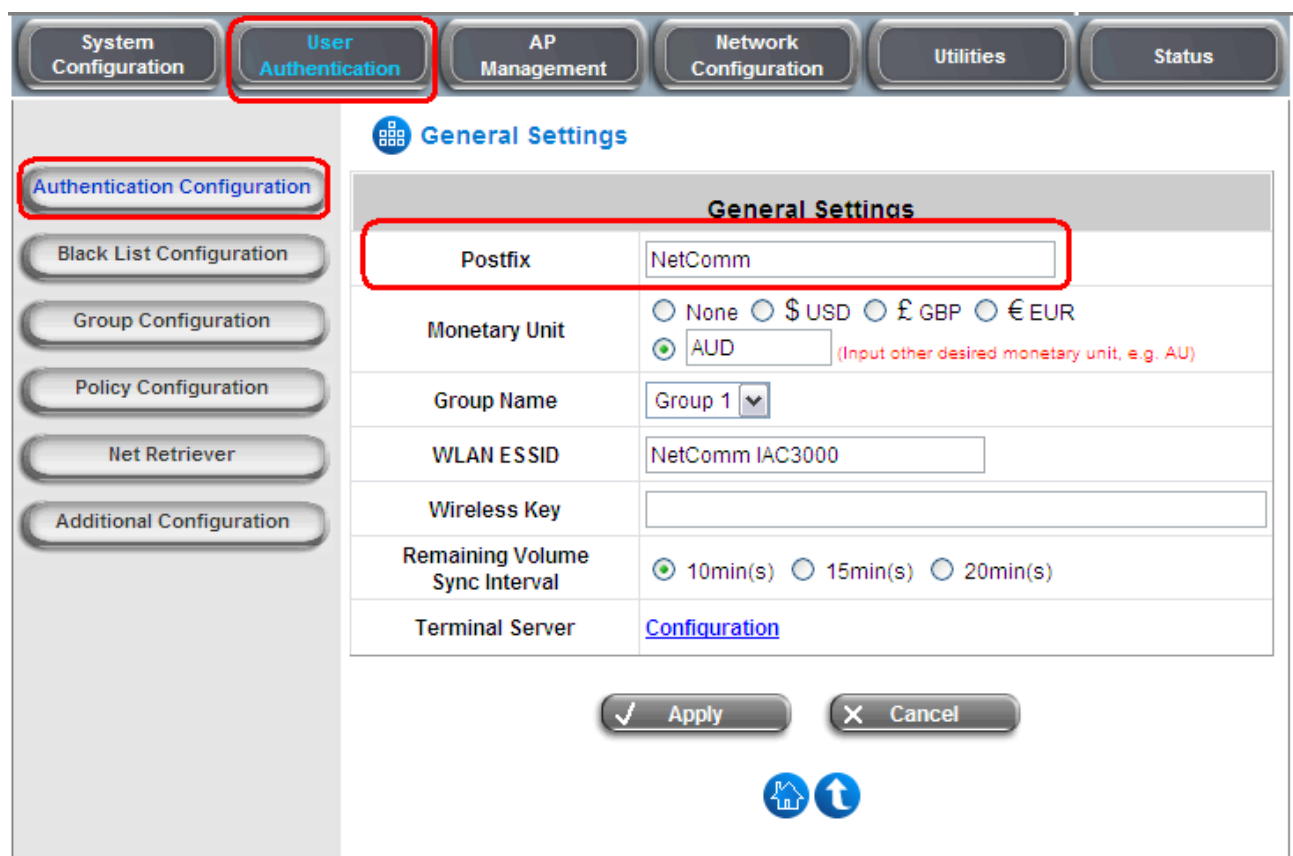
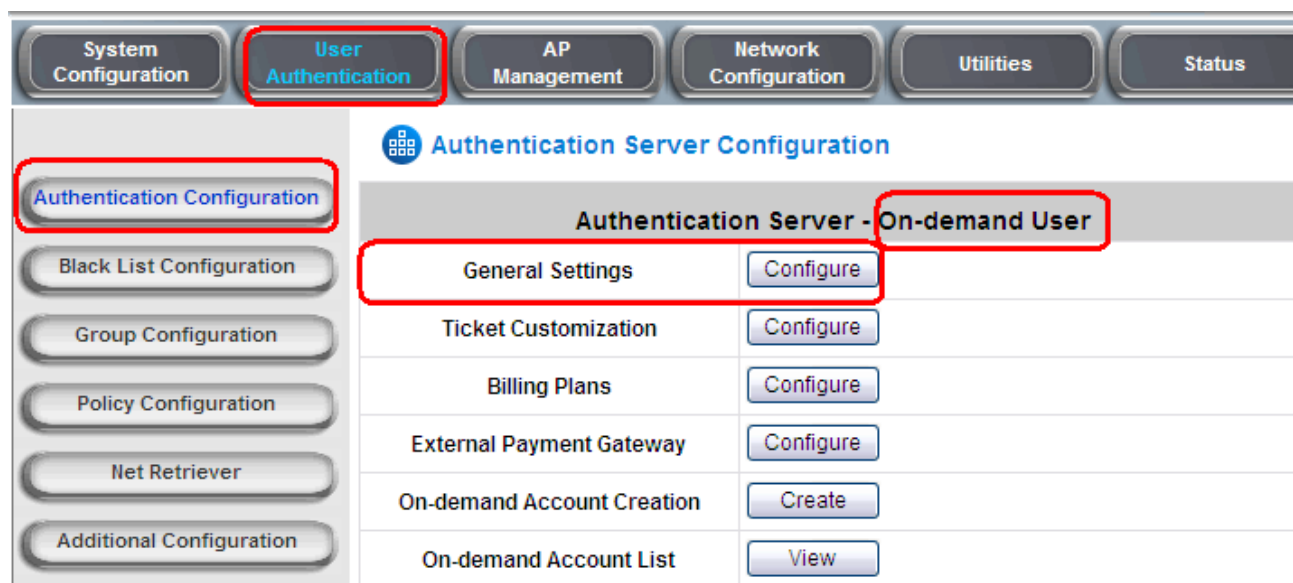
IAC3000 Port Location billing is based on the 'on-demand user server' billing profiles. This is also the billing packages that will appear in PLM user login page. In addition, if the administrator chooses 'PLM user free' implementation method when configuring port location mapping VLANs in the IAC3000, no billing data will be sent to the PMS server; if the administrator chooses 'PLM user charge' implementation method, the respective billing data will be sent to the PMS server.

The following billing profiles are used in this white paper

Plan	Type	Quota	Price (AUD)	Enable <input type="checkbox"/>	Privilege <input type="checkbox"/>	Function
1	Time	1 hr(s)	5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit
2	Time	24 hr(s)	18	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit
3	Time	48 hr(s)	32	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit
4	Time	120 hr(s)	60	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit
5	Time	168 hr(s)	74	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit
6	Volume	1000 Mbyte(s)	65	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit
7	Cut-off	Until 22 : 00	12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit
8	N/A			<input type="checkbox"/>	<input type="checkbox"/>	Edit
9	N/A			<input type="checkbox"/>	<input type="checkbox"/>	Edit
0	N/A			<input type="checkbox"/>	<input type="checkbox"/>	Edit

Step 5.4

Configure Postfix. The postfix for on-demand user server can be modified to reflect the company or business names. To configure 'on-demand user server' postfix, navigate to **User Authentication > Authentication Configuration > On-demand User server > General settings > Postfix = Netcomm**



Click '**Apply**' to apply the new postfix name.

Step 5.5

Configure SZ1 custom login pages.

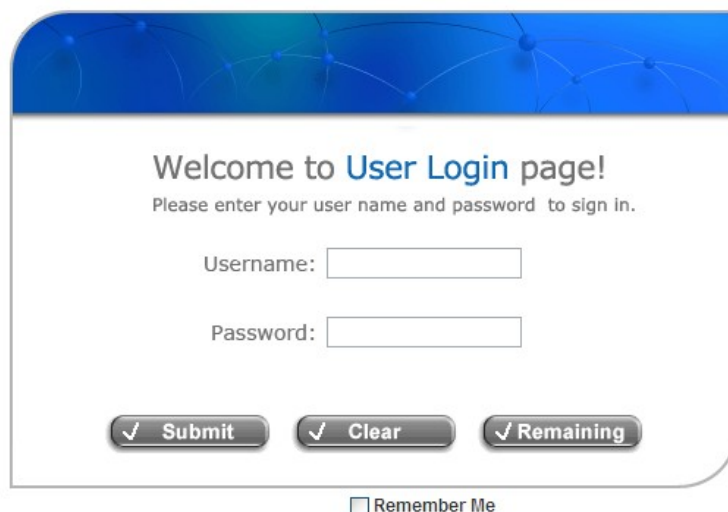
Navigate to **System Configuration > Service Zones > SZ1 > Custom Pages**

The default login pages are used by default.

A preview some the default login pages used are as follows.

Login Page	Configure
Port Mapping Free Login Page	Configure
Port Mapping Charge Login Page	Configure

Login Page



Welcome to **User Login** page!

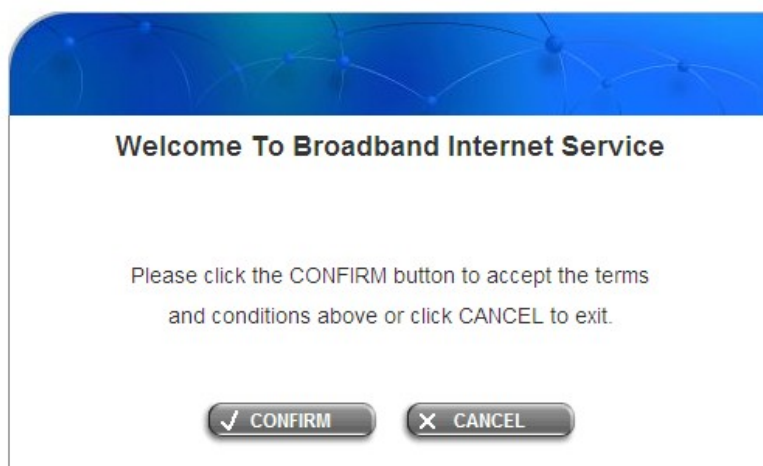
Please enter your user name and password to sign in.

Username:

Password:

☐ Remember Me

Port Mapping Free Login Page Preview



Welcome To Broadband Internet Service

Please click the CONFIRM button to accept the terms and conditions above or click CANCEL to exit.

Port Mapping Charge Login Page Preview

Welcome to Broadband Internet Service

Please choose from the following service selection

Plan	Price
<input checked="" type="radio"/> 1 hr(s)	5
<input type="radio"/> 24 hr(s)	18
<input type="radio"/> 48 hr(s)	32
<input type="radio"/> 120 hr(s)	60
<input type="radio"/> 168 hr(s)	74
<input type="radio"/> 1000 Mbyte(s)	65
<input type="radio"/> Until 22:00	12

Service Agreement

Please kindly note that there will be no refund once connectivity is confirmed.

Please click CONFIRM to accept the usage charge or CANCEL to exit.

The selected service charge will be posted directly into your guest folio.

✓ CONFIRM

✕ CANCEL

If you already have an user account, please click [here](#) to login.

Step 5.6

Configure 'Group 1' to map to SZ1 for user bandwidth management.

Group Permission for this Service Zone	<div style="border: 2px solid red; padding: 2px; display: inline-block;"> <div style="border: 1px solid #ccc; background-color: #eee; padding: 2px 10px; border-radius: 3px; display: flex; align-items: center; gap: 5px;"> Configure </div> </div>
Default Policy in this Service Zone	<div style="display: flex; align-items: center; gap: 10px;"> <div style="border: 1px solid #ccc; background-color: #eee; padding: 2px 10px; border-radius: 3px;">Policy 1</div> <div style="font-size: 0.8em;">▼</div> <div style="border: 1px solid #ccc; background-color: #eee; padding: 2px 10px; border-radius: 3px;">Edit System Policies</div> </div>
Email Message for Login Reminding	<div style="display: flex; align-items: center; gap: 10px;"> <div style="display: flex; flex-direction: column; gap: 5px;"> <div style="display: flex; align-items: center;"> <input checked="" type="radio"/> Enable </div> <div style="display: flex; align-items: center;"> <input type="radio"/> Disable </div> </div> <div style="border: 1px solid #ccc; background-color: #eee; padding: 2px 10px; border-radius: 3px;">Edit Mail Message</div> </div>

Click on **Configure > Group 1 > QoS Profile > and map 'Group 1' bandwidth control to policy 1 and SZ1**. The 'Group 1 – Traffic Configuration' details are shown as follows.

Traffic Configuration

Group 1 - Traffic Configuration	
Traffic Class	Best Effort ▼
Group Total Downlink	54 Mbps ▼
Individual Maximum Downlink	1 Mbps ▼
Individual Request Downlink	512 Kbps ▼
Group Total Uplink	54 Mbps ▼
Individual Maximum Uplink	1 Mbps ▼
Individual Request Uplink	512 Kbps ▼

You will then **map 'Group 1', 'Policy 1' and 'SZ1' together.**

Group Configuration

Group Configuration - Group 1			
Select Group:	Group 1 ▼		
QoS Profile	Setting		
Privilege Profile	Setting		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Name	Enabled	Policy	Edit Group Permission
Service Zone : Default	<input checked="" type="checkbox"/>	Policy 1 ▼	Default
Service Zone : SZ1	<input checked="" type="checkbox"/>	Policy 1 ▼	SZ1

Step 5.7

Configure 'Policy 1' for SZ1 for Session Limit Control:

Group Permission for this Service Zone	Configure
Default Policy in this Service Zone	Policy 1 ▼ Edit System Policies
Email Message for Login Reminding	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Edit Mail Message

Step 5.8

Configure 'Policy 1' settings. Click 'Edit System Policies' under SZ1 to configure settings. Change the user session limit from 500 to 50 and click 'Apply'. The default values are used under 'Firewall Profile', 'Specific Route Profile' and 'Schedule Profile' in this white paper. 'Firewall Profile', 'Route Profile', and 'Schedule Profile' should be site specific. For more details, please refer to the IAC3000 User Manual.

Policy Configuration - Policy 1	
Select Policy:	Policy 1 ▾
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
Maximum Concurrent Sessions	50 ▾ (Sessions per User)

Step 5.9

There is no Managed Access Point required in this PLM test so we won't make changes to 'Wireless Settings' and 'Managed AP in this Service Zone'.

Wireless Settings			
Set SSID	NetComm_IAC3000-1		
Access Point Security	Authentication	Open System ▾ <input type="checkbox"/> Enable 802.1X Authentication	
	Encryption	None ▾	

Managed AP in this Service Zone			
AP Type	AP Name	IP Address	Status
		MAC Address	

✓ Apply	✗ Clear
---------	---------

Click '**Apply**' to apply the new settings to SZ1.

(For instructions on how to configure IAC3000 to centrally control and manage NetComm NP725 and NP726, please refer to the product user manual and NetComm support website for more details.)

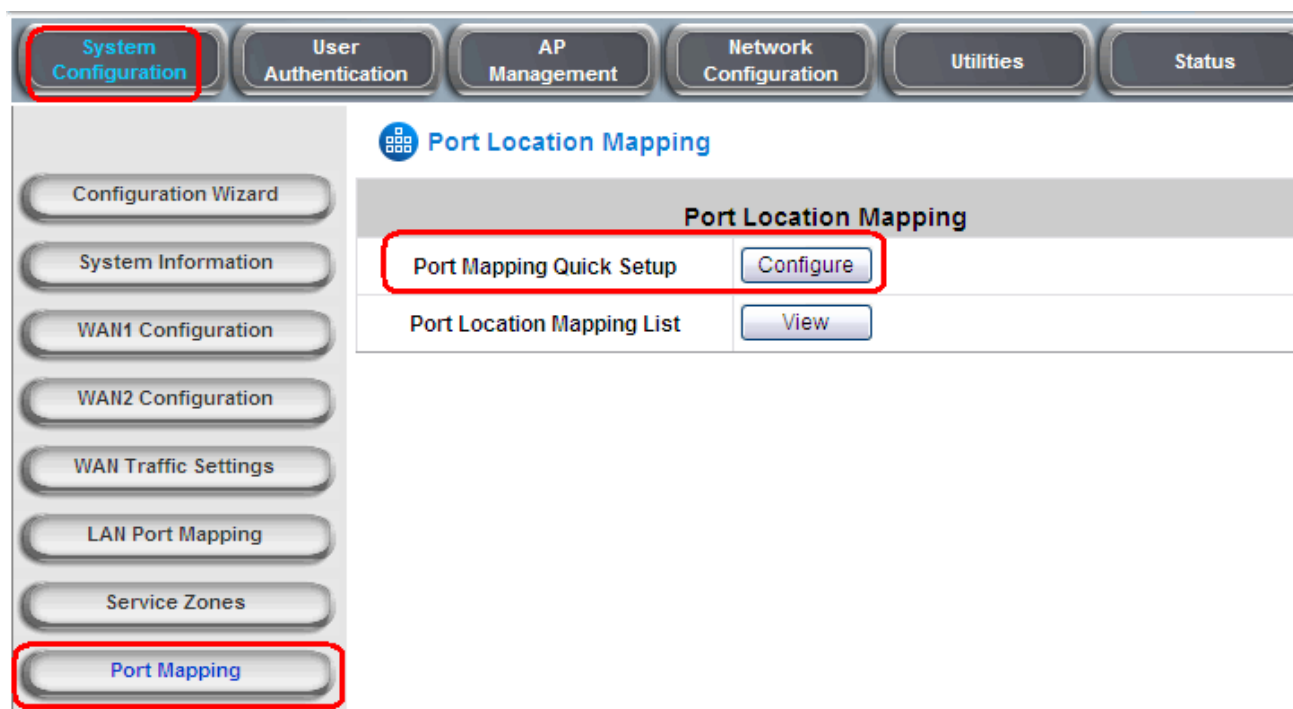
Reboot the system to make the changes to take effect. Once system finished reboot, you should see that SZ1 overview page shown as follows.

Service Zone Settings							
Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default	--	NetComm_IAC3000	None	Policy 1	Server 1	Enable	Configure
SZ1	10	NetComm_IAC3000-1	None	Policy 1	Server 1	Enable	Configure
SZ2	2	NetComm_IAC3000-2	None	Policy 1	Server 1	Disable	Configure
SZ3	3	NetComm_IAC3000-3	None	Policy 1	Server 1	Disable	Configure
SZ4	4	NetComm_IAC3000-4	None	Policy 1	Server 1	Disable	Configure
SZ5	5	NetComm_IAC3000-5	None	Policy 1	Server 1	Disable	Configure
SZ6	6	NetComm_IAC3000-6	None	Policy 1	Server 1	Disable	Configure
SZ7	7	NetComm_IAC3000-7	None	Policy 1	Server 1	Disable	Configure
SZ8	8	NetComm_IAC3000-8	None	Policy 1	Server 1	Disable	Configure

Step 6:

Configure Port Location Mapping VLAN table

Navigate to **System Configuration > Port Mapping > Port Mapping Quick Setup**
(Refer to screen shot below)



Please note you can 'single-create' or 'batch create' PLM VLAN entries. The 'Batch Create' method is used in the white paper.

The following screen shot illustrates how to batch-create VLAN 101 to VLAN 148 entries in the IAC3000.

- Configuration Wizard
- System Information
- WAN1 Configuration
- WAN2 Configuration
- WAN Traffic Settings
- LAN Port Mapping
- Service Zones
- Port Mapping**

Port Mapping Quick Setup

Create Batch

VLAN ID Start: 101
How many VLAN: 48
Room Number Start: 101
Room Prefix: Room
Room Postfix:
Room Default State: ☒ Charge ☐ Free ☐ Block
Service Zone: SZ1
Create

Change All Room State

Room State: ☒ Charge ☐ Free ☐ Block
Service Zone: SZ1
Change

Add One











VLAN ID:
Room Number:
Room Default State: ☒ Charge ☐ Free ☐ Block
Room Description:
Service Zone: SZ1
Add

To view the PLM table, please click on '**View**' under Port Location Mapping List.

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

Port Location Mapping

Port Mapping Quick Setup	Configure
Port Location Mapping List	View


Port Location Mapping List						
	VLAN ID	Room Num	State	Description	Service Zone	Delete All
	101	Room101	Charge		SZ1	Delete
	102	Room102	Charge		SZ1	Delete
	103	Room103	Charge		SZ1	Delete
	104	Room104	Charge		SZ1	Delete
	105	Room105	Charge		SZ1	Delete
	106	Room106	Charge		SZ1	Delete
	107	Room107	Charge		SZ1	Delete
	108	Room108	Charge		SZ1	Delete
	109	Room109	Charge		SZ1	Delete
	110	Room110	Charge		SZ1	Delete
(Total:48) First Prev Next Last						



Note:

Room description cannot be added via 'Batch Create' batch configuration.









If there are VIP rooms that will not be charge for their Internet access, 'charge' mode can be changed to 'Free' mode.

To change VLAN 101 (Room 101) to User-Free mode, **click on '101' hyperlink, and change the 'Room state' to Free, add in Room Description** such as 'VIP Room-Free of Charge', then click '**Apply**' to apply new settings for Room 101.

Port Mapping Profile	
VLAN ID	101
Room Number	Room101
Room State	<input checked="" type="radio"/> Free <input type="radio"/> Charge <input type="radio"/> Block
Room Description	VIP Room - Free of Charge
Service Zone	SZ1
Room Available	
User Name / Password	xz32 / x4v6a48g
Plan Type	CUTOFF
Plan Quota	N/A
Remaining Quota	Until 2009/09/09-12:30
User Account Status	Normal
Reference	roomN-Room101

 Apply
 Clear

To view PLM table, please click on '**View**' under Port Location Mapping List.

Port Location Mapping List						
	VLAN ID	Room Num	State	Description	Service Zone	Delete All
	101	Room101	Free	VIP Room - Free of Charge	SZ1	Delete
	102	Room102	Charge		SZ1	Delete
	103	Room103	Charge		SZ1	Delete
	104	Room104	Charge		SZ1	Delete
	105	Room105	Charge		SZ1	Delete
	106	Room106	Charge		SZ1	Delete
	107	Room107	Charge		SZ1	Delete
	108	Room108	Charge		SZ1	Delete
	109	Room109	Charge		SZ1	Delete
	110	Room110	Charge		SZ1	Delete

(Total:48) [First](#) [Prev](#) [Next](#) [Last](#)

Please reboot system to make PLM entries to take effect.

Step 7:

Configure NetRetriever settings for PMS billing integration. This step is only applicable to scenarios where you need to integrate the billing data from the IAC3000 to PMS system.

Note:

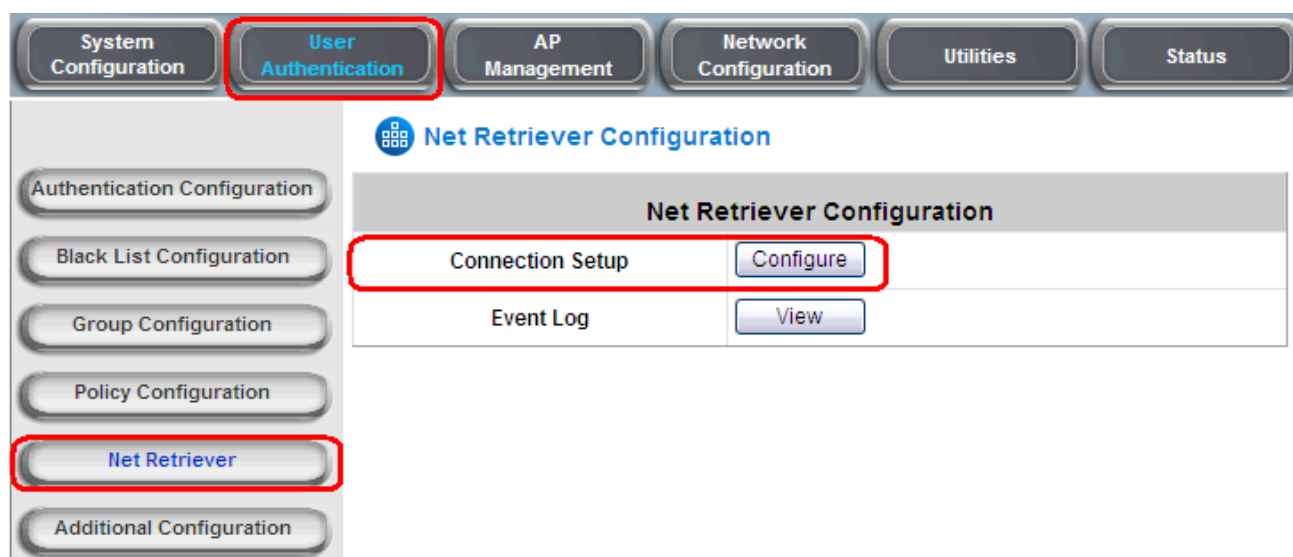
IAC3000 supports PMS billing integration via middleware called NetRetriever via IP connection. Please make sure the NetRetriever parameter settings in the IAC3000 matches the settings in the NetRetriever software. You may need to work with a NetRetriever engineer to complete the IAC3000 PMS billing integration set up.

Note:

*IAC3000 keeps a record of the billing data locally. If no PMS integration is required, you may make use of the local billing data and produce internet usage billing report in your own format. To see the billing data, please navigate to **User Authentication > Net Retriever > Event Log** or navigate to **Status > Traffic History > On-demand User Log**.*

To configure NetRetriever parameter settings, navigate to **User Authentication > Net Retriever > Connection Setup** and fill in the parameter values required.

The parameter values shown below are only an example. Please make sure the settings in the NetRetriever software.



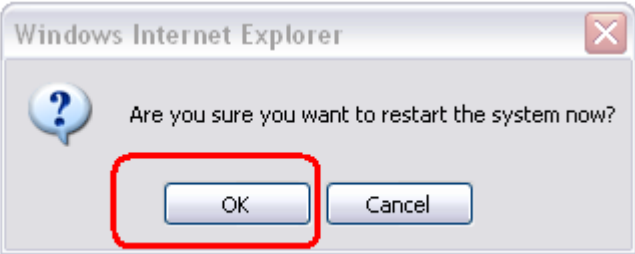
Net Retriever Connection Setup	
Secret	NetIAC123#
Net Retriever Server Port	8324 -
NR ID	1 <small>*(1 ~ 9999)</small>
GSD ID	1 <small>*(1 ~ 9999)</small>
Link Test Interval	60 <small>*(60~600 seconds)</small>

You should restart to activate this. Click to [restart](#).

Click 'Apply' to apply the new settings. Click 'Restart' to reboot system.

Do you want to **RESTART** the system?

YES
NO



Step 8:

Configure IAC3000 'Walled Garden List' and 'Walled Garden Ad List'

Navigate to **Network Configuration > Walled Garden List >**, add **'www.netcomm.com.au' as a free access website and click 'Apply'**.

Walled Garden List

Item	Address	Item	Address
1	www.netcomm.com.au	2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

Apply Clear

Navigate to **Network Configuration > Walled Garden Ad List > add** 'www.netcomm.com.au' as a free website to display at the user login page and **click 'Display' and 'Apply'**. See screen shot below for details.

Walled Garden Ad List

Item	URL	Topic	Edit	Display
1	http://www.netcomm.com.au	NetComm Limited	Edit	<input checked="" type="checkbox"/>
2			Edit	<input type="checkbox"/>

Walled Garden Ad List Item 1

URL	http://www.netcomm.com.au
Topic	NetComm Limited
Description	Broadband Solutions

Apply Clear Delete

You have now completed setting up the IAC3000 for user-free and user-charge application using Port Location Mapping VLAN tagging. Default SZ and SZ1 are now both set up and enabled in the IAC3000 system ready for PLM user.

Part 3: Test and verify the port location mapping function of the IAC3000 and NCT240 system

Connect the Bridged NB6plus4_R2T8 to the line tails of the NCT240 line port 1; connect the GE1 of the NCT240 to the IAC3000 LAN port.

Steps and Procedures

Step 1:

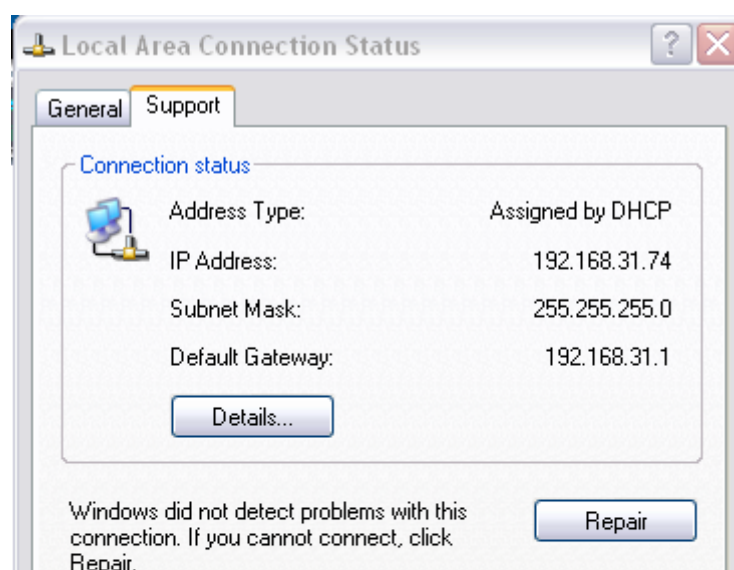
Connect the test modems NB6plus4_R2T8 to an ADSL Port of the NCT240 DSLAM system (The ADSL data point socket in the guest room) and wait for ADSL light on the test modem turn solid green.

Step 2:

Connect the test PC to the LAN Port of the test modem. (Note: TCP/IP setting of the PC is to be set to *obtain IP Address/ DNS address from DHCP server automatically*).

Step 3:

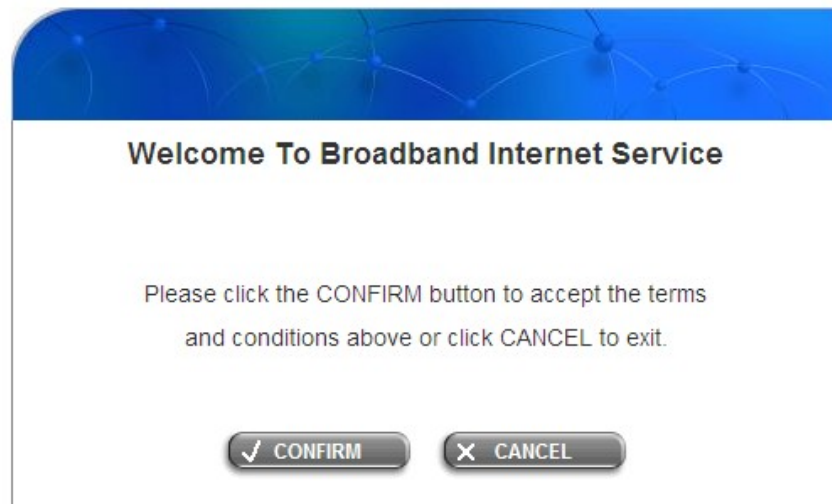
Wait for a valid IP address assigned by the IAC3000 to your subscriber PC/Guest room PC.



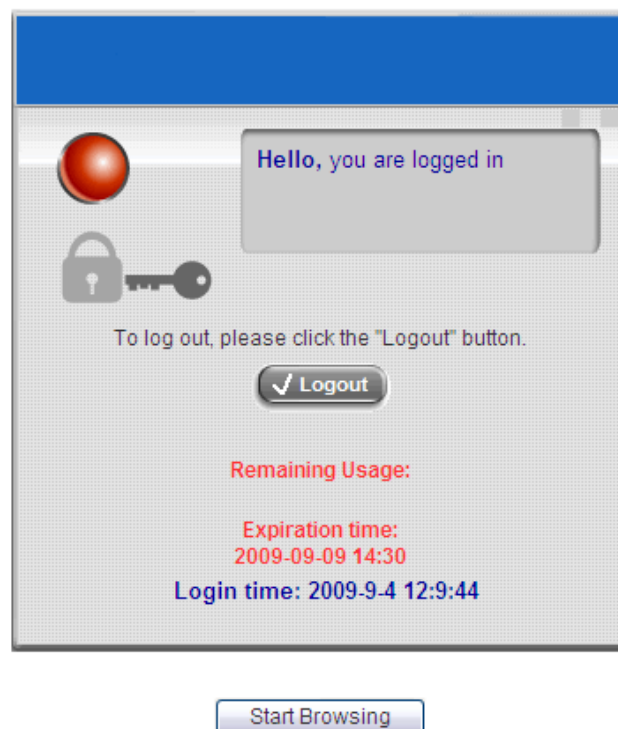
Once a valid IP address is received by the subscriber/guest room PC, you then open Internet Explorer. Attempt to access the Internet by browsing a website. If PLM has been setup correctly, the following page will be presented. You will then need to select and accept the Internet access conditions and hit '**Enter**' then '**OK**' to proceed.

Step 3.1

If you are testing from a free of charge VIP room (for example Room 101), you will expect to see the following login page

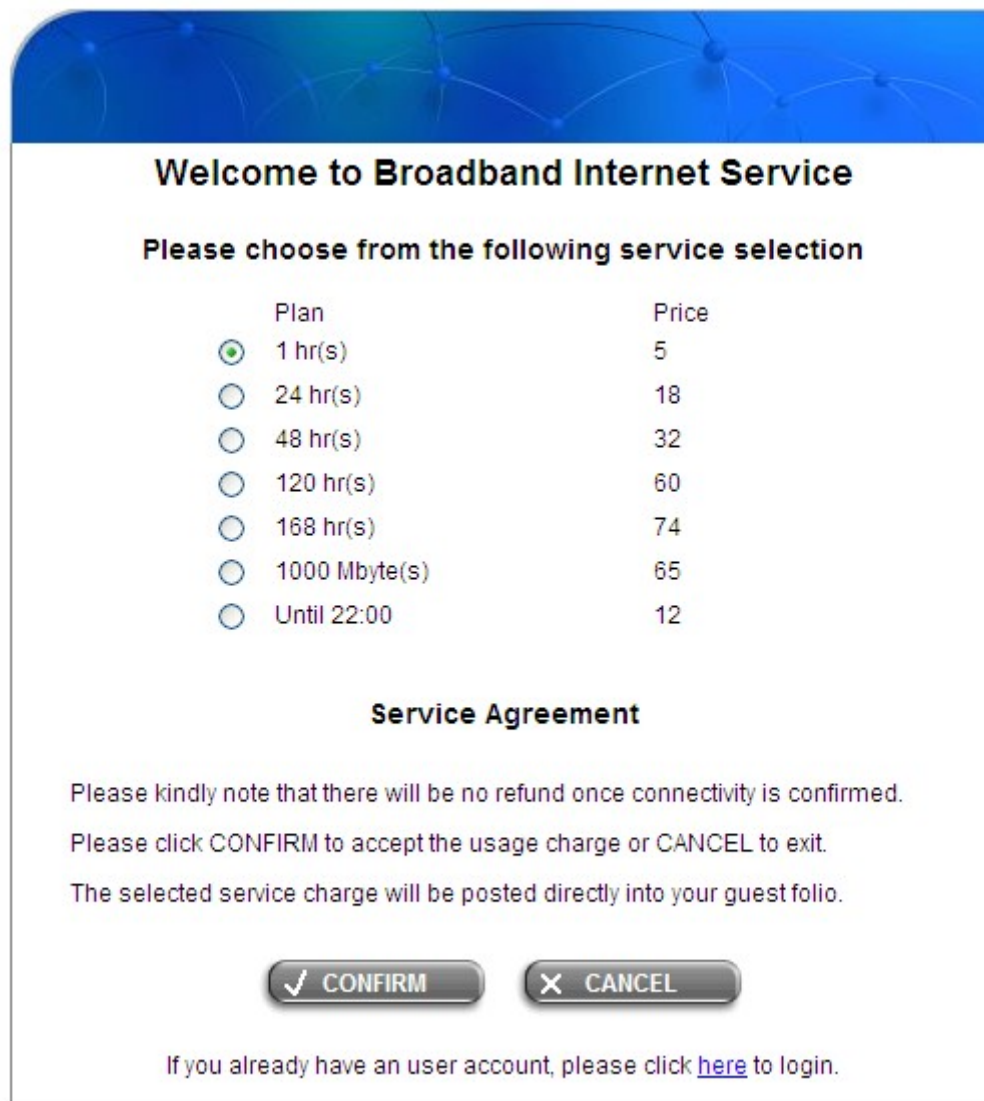


Click on '**CONFIRM**' to surf the Internet.



Step 3.2:

If you are testing from a user-charge room, you will expect to see the following login page

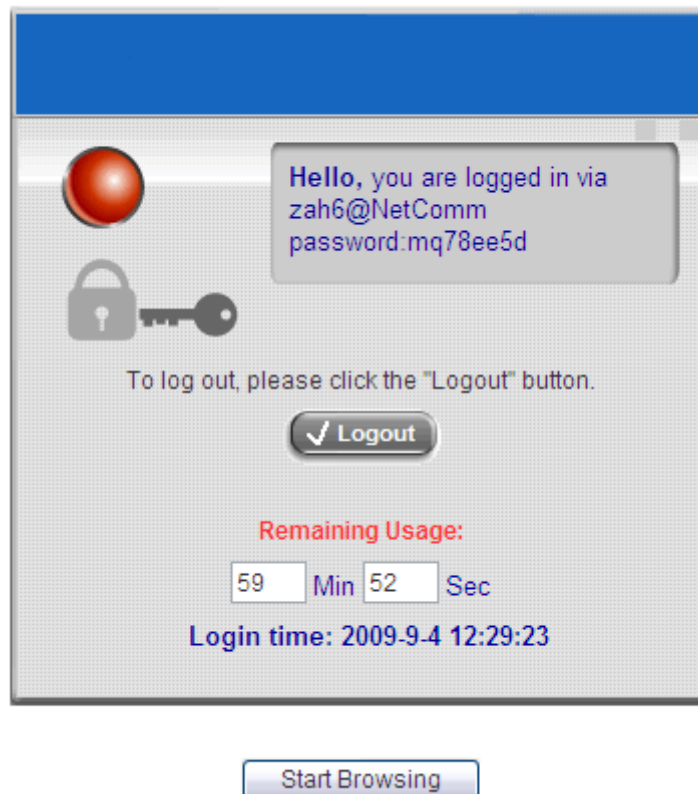


Plan	Price
<input checked="" type="radio"/> 1 hr(s)	5
<input type="radio"/> 24 hr(s)	18
<input type="radio"/> 48 hr(s)	32
<input type="radio"/> 120 hr(s)	60
<input type="radio"/> 168 hr(s)	74
<input type="radio"/> 1000 Mbyte(s)	65
<input type="radio"/> Until 22:00	12

Service Agreement

Please kindly note that there will be no refund once connectivity is confirmed.
Please click CONFIRM to accept the usage charge or CANCEL to exit.
The selected service charge will be posted directly into your guest folio.

If you already have an user account, please click [here](#) to login.



Note:

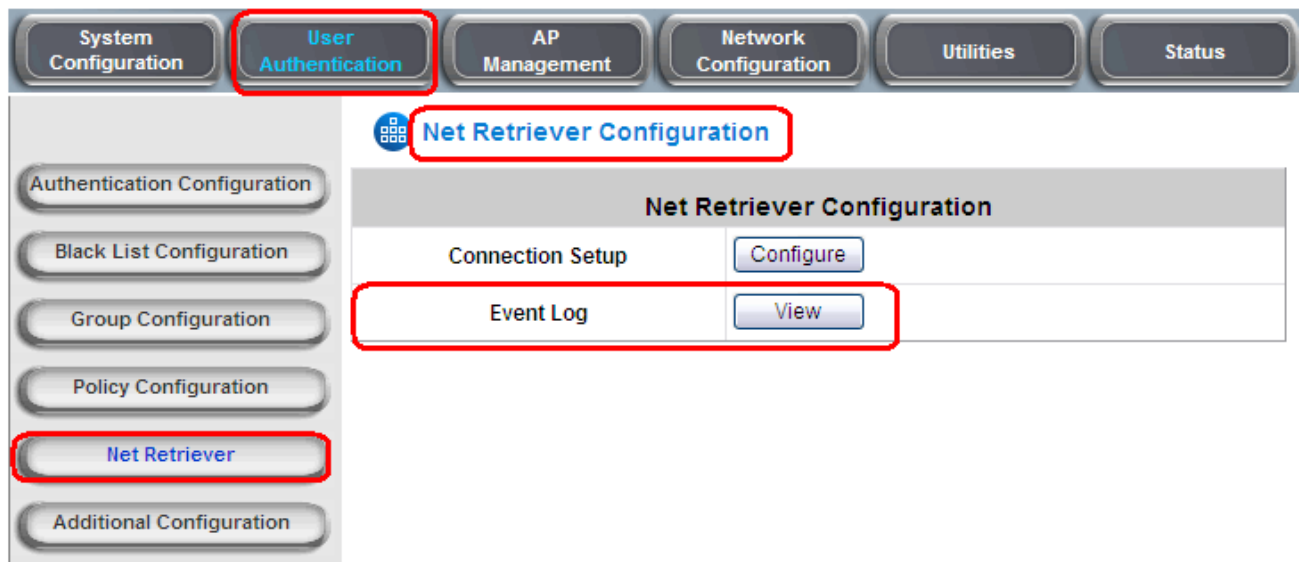
The user name and password presented in the user login success page (for example zah6@NetComm/mq78ee5d) can be used by the user for account roaming. This means this user name/ password is mapped to the same Room (VLAN ID) under the same internet usage account. If the guest user uses this user name and password to access the Internet through wired or wireless area of the IAC300 system, they will be billed under the same guest account.

Once Internet access is confirmed, the billing data will be sent to the PMS system via the PMS Middleware. It is important to verify the middleware NetRetriever parameter settings in the IAC3000 matched the settings in the NetRetriever server.

A billing log will then automatically generate and save locally in the IAC3000 system for system logging and tracking purposes.

Step 4:

To view the PMS log, login to the IAC3000 management interface and navigate to **User Authentication > NetRetriever > Event Log > and click 'view'**



NetRetriever Configuration

Net Retriever Event Log	
Date	Size (Byte)
2009-09-04	127

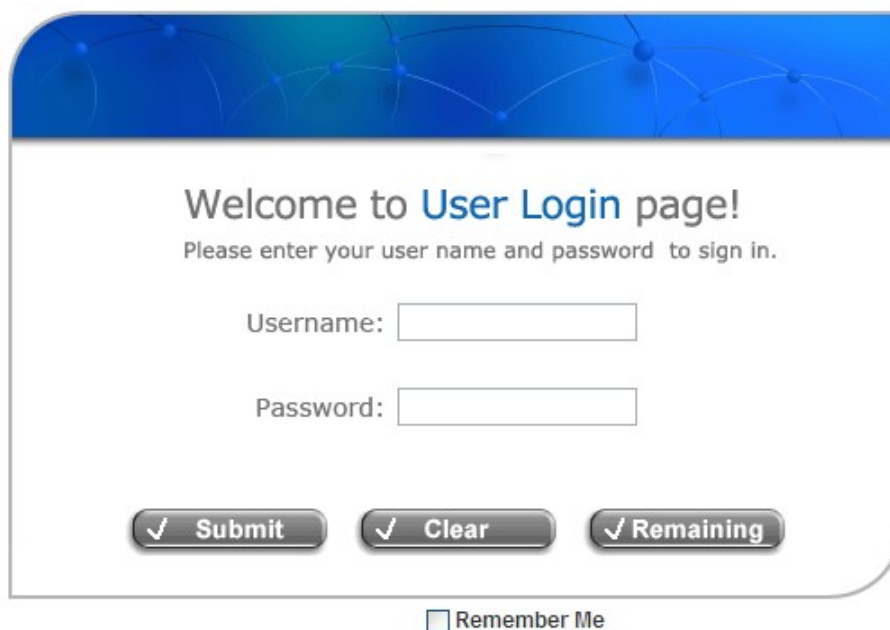
Double click on the date and open the event log file. You will notice the event log will keep a record of the VLAN room number, date, time of access, user name, password, and price. Please note that the Price shown in the log file is in a unit of 'cents'. That is 500 means \$5 dollars or 500cents.

Net Retriever Billing Log 2009-09-04							
Room	Cost	Date	Time	Duration	Description	Name	Bytes Us
Room102	500	20090904	122922	000000	Room number: Room102, plan: 1, username: zah6@NetComm, password: mq78ee5d, price: 500	N/A	0

Note:

If the following page is presented in the guest room instead of the login pages above, then the setup for Port Location Mapping Billing is incorrect in the IAC3000. The VLAN settings in the device/s might be incorrect.

Please review the configuration in the IAC3000 and the NCT240 VLAN settings.



Welcome to **User Login** page!

Please enter your user name and password to sign in.

Username:

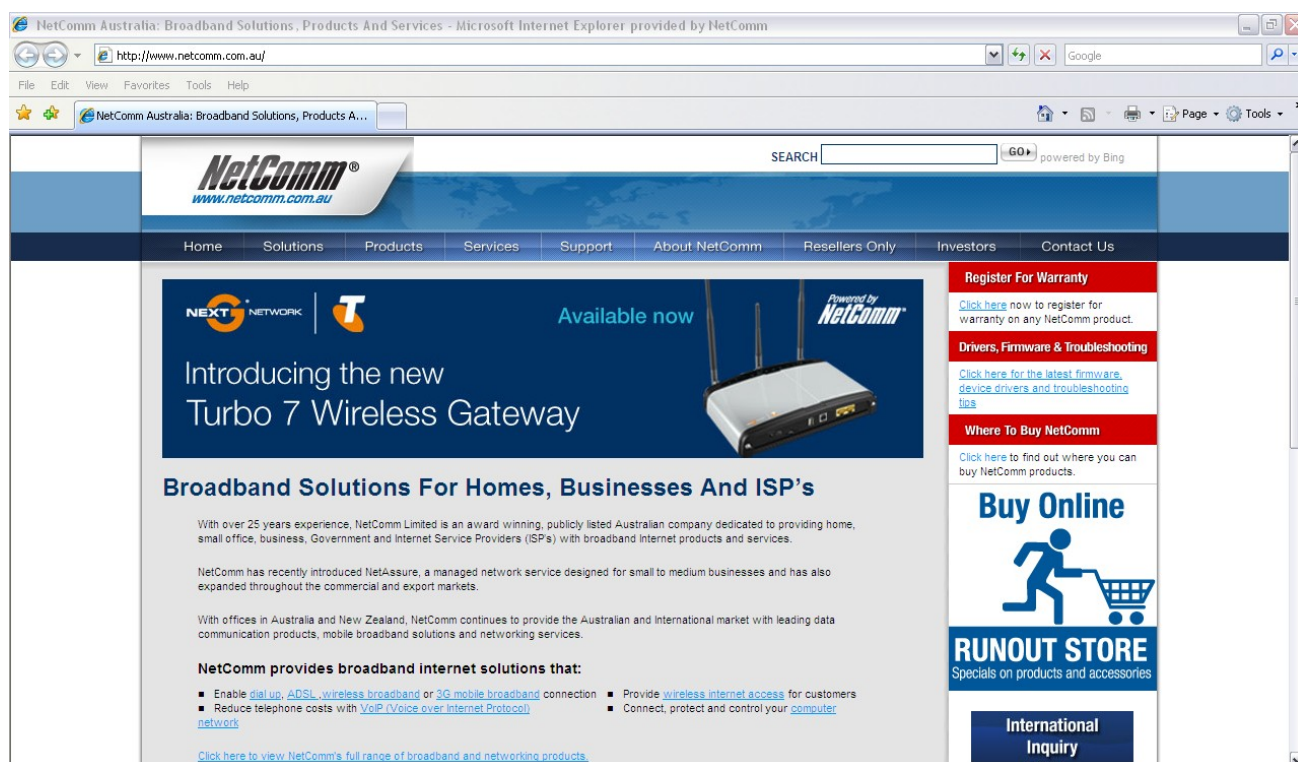
Password:

☐ Remember Me

 **NetComm Limited** Broadband Solutions

Step 5:

Surf the Internet. Test complete!



NetComm Australia: Broadband Solutions, Products And Services - Microsoft Internet Explorer provided by NetComm

http://www.netcomm.com.au/

File Edit View Favorites Tools Help

NetComm Australia: Broadband Solutions, Products A...

SEARCH GO powered by Bing

Home Solutions Products Services Support About NetComm Resellers Only Investors Contact Us

NetComm
www.netcomm.com.au

Available now

Introducing the new
Turbo 7 Wireless Gateway

Broadband Solutions For Homes, Businesses And ISP's

With over 25 years experience, NetComm Limited is an award winning, publicly listed Australian company dedicated to providing home, small office, business, Government and Internet Service Providers (ISPs) with broadband Internet products and services.

NetComm has recently introduced NetAssure, a managed network service designed for small to medium businesses and has also expanded throughout the commercial and export markets.

With offices in Australia and New Zealand, NetComm continues to provide the Australian and International market with leading data communication products, mobile broadband solutions and networking services.

NetComm provides broadband internet solutions that:

- Enable [dial up](#), [ADSL](#), [wireless broadband](#) or [3G mobile broadband](#) connection
- Reduce telephone costs with [VoIP \(Voice over Internet Protocol\)](#)
- Provide [wireless internet access](#) for customers
- Connect, protect and control your [computer network](#)

[Click here to view NetComm's full range of broadband and networking products.](#)

Register For Warranty
[Click here](#) now to register for warranty on any NetComm product.

Drivers, Firmware & Troubleshooting
[Click here for the latest firmware, device drivers and troubleshooting tips](#)

Where To Buy NetComm
[Click here](#) to find out where you can buy NetComm products.

Buy Online

RUNOUT STORE
Specials on products and accessories

International Inquiry

Appendix A: How to check current user list in the IAC3000

There are two ways to check the current VLAN user list in the IAC3000 system.



Method 1:

Navigate to System> Configuration > Port Mapping > Port Location Mapping List > Click 'View', then click on '102' to view current status.

Port Location Mapping List

	VLAN ID	Room Num	State	Description	Service Zone	
●	101	Room101	Free	VIP Room - Free of Charge	SZ1	Delete
●	102	Room102	Charge		SZ1	Delete
●	103	Room103	Charge		SZ1	Delete
●	104	Room104	Charge		SZ1	Delete
●	105	Room105	Charge		SZ1	Delete
●	106	Room106	Charge		SZ1	Delete

Port Mapping Profile

Port Mapping Profile	
VLAN ID	102
Room Number	Room102
Room State	<input type="radio"/> Free <input checked="" type="radio"/> Charge <input type="radio"/> Block
Room Description	<input type="text"/>
Service Zone	SZ1 
Room Available	
User Name / Password	zah6 / mq78ee5d
Plan Type	TIME
Plan Quota	1 hr(s)
Remaining Quota	1 hr(s)
User Account Status	Online
Reference	roomN-Room102

✓ Apply
✗ Clear

You will notice that Room 102 is currently 'Online'

Note:

The 'Remaining Quota' shown under VLAN rooms will only updated after guest user has logout or click 'logout' button on the 'success user login page' window.

Method 2:

Another way to view the current user list in the IAC3000 is by navigating to **Status > Current Users > Current Users List**

System Configuration

User Authentication

AP Management

Network Configuration

Utilities

Status

System Status

Interface Status

Routing Table

Current Users

Traffic History

Notification Configuration

Current Users

Current Users List

Item	Username		Pkts In	Bytes In	Idle	Location
	IP	MAC	Pkts Out	Bytes Out		Kick Out
1	zah6@NetComm		0	0	10	N/A
	192.168.31.74	00:1E:68:AC:0E:94	0	0		Logout

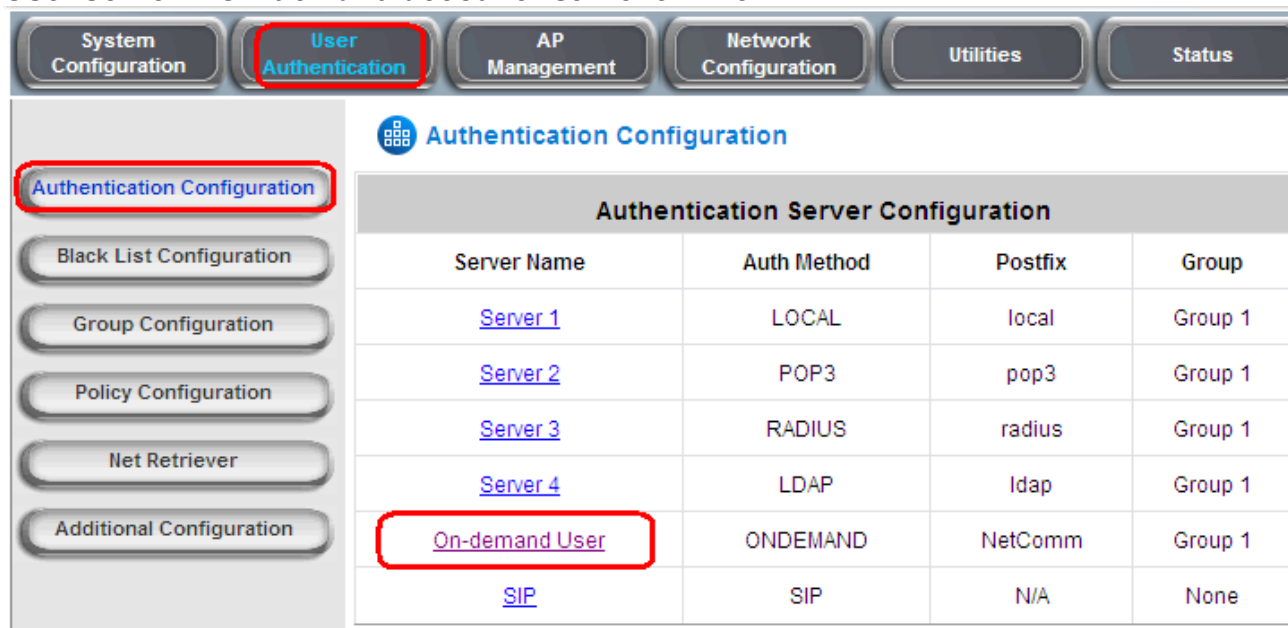
Refresh

Appendix B: How to delete a VLAN roaming account

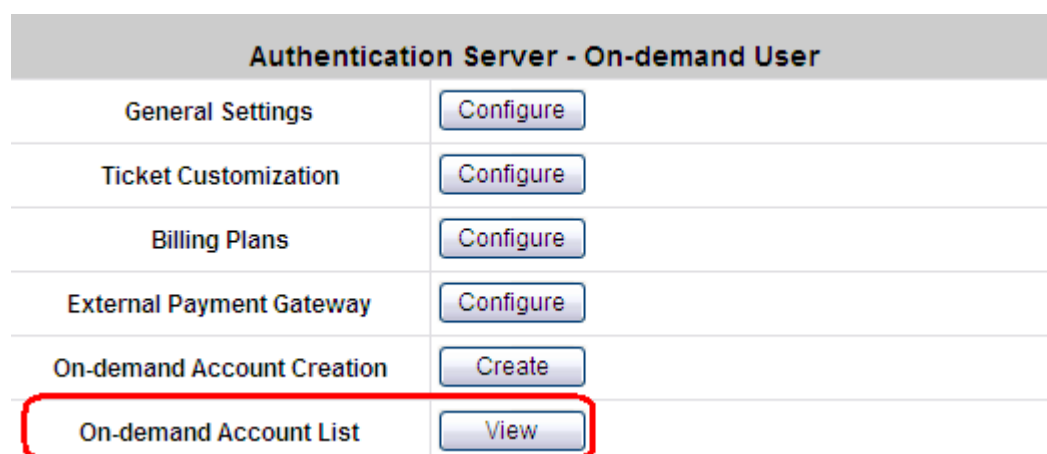
When a VLAN ID room is activated, at the same time the mapping On-demand account is creates in the IAC3000 on-demand user server. In situations where the administrator needs to delete the user name and password that mapped to the VLAN ID room 102, here are the steps to follow.

Step 1:

Navigate to **User Authentication > Authentication Configuration > On-demand User server > On-demand account list > click 'view'**

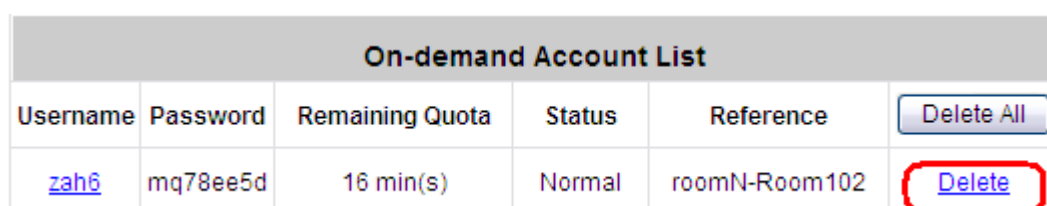


Authentication Server Configuration			
Server Name	Auth Method	Postfix	Group
Server 1	LOCAL	local	Group 1
Server 2	POP3	pop3	Group 1
Server 3	RADIUS	radius	Group 1
Server 4	LDAP	ldap	Group 1
On-demand User	ONDEMAND	NetComm	Group 1
SIP	SIP	N/A	None



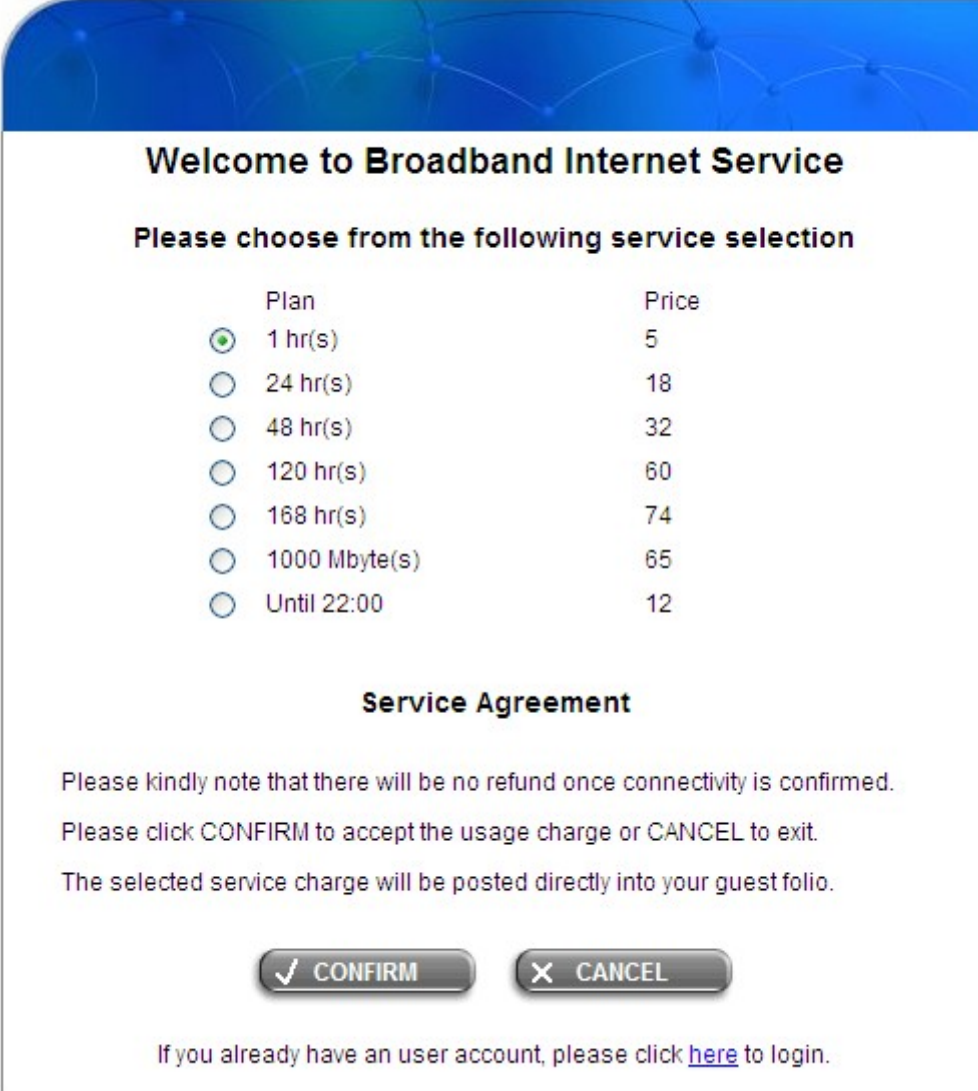
Authentication Server - On-demand User	
General Settings	Configure
Ticket Customization	Configure
Billing Plans	Configure
External Payment Gateway	Configure
On-demand Account Creation	Create
On-demand Account List	View

Click '**Delete**' to delete the user name and password that mapped with Room 102.



On-demand Account List					
Username	Password	Remaining Quota	Status	Reference	Delete All
zah6	mq78ee5d	16 min(s)	Normal	roomN-Room102	Delete

When you try to access the internet from room 102 now, you will be re-presented with the user login page again and if you click 'confirm' the Room 102 PMS billing data will be re-sent with a different set of user name and password



Plan	Price
<input checked="" type="radio"/> 1 hr(s)	5
<input type="radio"/> 24 hr(s)	18
<input type="radio"/> 48 hr(s)	32
<input type="radio"/> 120 hr(s)	60
<input type="radio"/> 168 hr(s)	74
<input type="radio"/> 1000 Mbyte(s)	65
<input type="radio"/> Until 22:00	12

Service Agreement

Please kindly note that there will be no refund once connectivity is confirmed.

Please click CONFIRM to accept the usage charge or CANCEL to exit.

The selected service charge will be posted directly into your guest folio.

If you already have an user account, please click [here](#) to login.

