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

**************************************************************************************************

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.
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
To view the current VLAN setting, click on *Display VLAN Settings* to view the current VLAN information for all the 24 ADSL ports.
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:
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
Step 3:

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

a. Navigate to **System Configuration > WAN 1 Configuration**
b. Navigate to **System Configuration > WAN 2 Configuration**
c. 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.**
Step 5:
Configure Service Zone settings

Step 5.1
Click on 'Configure' button to configure SZ1.

Perform the following configurations to SZ1.

a. Change the VLAN tagged number from 1 to 10 for SZ1
b. Configure IP Address, DHCP server, DHCP server pool, and DNS details for SZ1
c. Configure ‘on-demand billing plans’ under on-demand user server
d. Configure ‘custom login pages’
e. Configure PLM charge login page
f. Configure PLM free login page
g. Configure User Group for SZ1 (bandwidth control)
h. 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.
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**.
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 >
**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

<table>
<thead>
<tr>
<th>Billing Plans</th>
<th>Billing Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan</td>
<td>Type</td>
</tr>
<tr>
<td>1</td>
<td>Time</td>
</tr>
<tr>
<td>2</td>
<td>Time</td>
</tr>
<tr>
<td>3</td>
<td>Time</td>
</tr>
<tr>
<td>4</td>
<td>Time</td>
</tr>
<tr>
<td>5</td>
<td>Time</td>
</tr>
<tr>
<td>6</td>
<td>Volume</td>
</tr>
<tr>
<td>7</td>
<td>Cut-off</td>
</tr>
<tr>
<td>8</td>
<td>N/A</td>
</tr>
<tr>
<td>9</td>
<td>N/A</td>
</tr>
<tr>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**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](image)

**Welcome to User Login page!**

Please enter your user name and password to sign in.

Username: 

Password: 

[Submit] [Clear] [Remaining]

[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.

[CONFIRM] [CANCEL]

---

**Port Mapping Charge Login Page Preview**
Step 5.6

Configure ‘Group 1’ to map to SZ1 for user bandwidth management.

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

### Step 5.7

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

<table>
<thead>
<tr>
<th>Group Permission for this Service Zone</th>
<th>Default Policy in this Service Zone</th>
<th>Email Message for Login Reminding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure</td>
<td>Policy 1</td>
<td>Enable</td>
</tr>
</tbody>
</table>

[Diagram of 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
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.

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’.

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

<table>
<thead>
<tr>
<th>Service Zone Name</th>
<th>VLAN Tag</th>
<th>SSID</th>
<th>WLAN Encryption</th>
<th>Applied Policy</th>
<th>Default Authentication</th>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>--</td>
<td>NetComm m_IAC3 000</td>
<td>None</td>
<td>Policy 1</td>
<td>Server 1</td>
<td>Enable [Configure]</td>
<td></td>
</tr>
<tr>
<td>SZ1</td>
<td>10</td>
<td>NetComm m_IAC3 000-1</td>
<td>None</td>
<td>Policy 1</td>
<td>Server 1</td>
<td>Enable [Configure]</td>
<td></td>
</tr>
<tr>
<td>SZ2</td>
<td>2</td>
<td>NetComm m_IAC3 000-2</td>
<td>None</td>
<td>Policy 1</td>
<td>Server 1</td>
<td>Disable [Configure]</td>
<td></td>
</tr>
<tr>
<td>SZ3</td>
<td>3</td>
<td>NetComm m_IAC3 000-3</td>
<td>None</td>
<td>Policy 1</td>
<td>Server 1</td>
<td>Disable [Configure]</td>
<td></td>
</tr>
<tr>
<td>SZ4</td>
<td>4</td>
<td>NetComm m_IAC3 000-4</td>
<td>None</td>
<td>Policy 1</td>
<td>Server 1</td>
<td>Disable [Configure]</td>
<td></td>
</tr>
<tr>
<td>SZ5</td>
<td>5</td>
<td>NetComm m_IAC3 000-5</td>
<td>None</td>
<td>Policy 1</td>
<td>Server 1</td>
<td>Disable [Configure]</td>
<td></td>
</tr>
<tr>
<td>SZ6</td>
<td>6</td>
<td>NetComm m_IAC3 000-6</td>
<td>None</td>
<td>Policy 1</td>
<td>Server 1</td>
<td>Disable [Configure]</td>
<td></td>
</tr>
<tr>
<td>SZ7</td>
<td>7</td>
<td>NetComm m_IAC3 000-7</td>
<td>None</td>
<td>Policy 1</td>
<td>Server 1</td>
<td>Disable [Configure]</td>
<td></td>
</tr>
<tr>
<td>SZ8</td>
<td>8</td>
<td>NetComm m_IAC3 000-8</td>
<td>None</td>
<td>Policy 1</td>
<td>Server 1</td>
<td>Disable [Configure]</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Room Num</th>
<th>State</th>
<th>Description</th>
<th>Service Zone</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>Room 101</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>102</td>
<td>Room 102</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>103</td>
<td>Room 103</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>104</td>
<td>Room 104</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>105</td>
<td>Room 105</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>106</td>
<td>Room 106</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>107</td>
<td>Room 107</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>108</td>
<td>Room 108</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>109</td>
<td>Room 109</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>110</td>
<td>Room 110</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
</tbody>
</table>

(Total: 40) 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.
To view PLM table, please click on ‘View’ under Port Location Mapping List.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Room Num</th>
<th>State</th>
<th>Description</th>
<th>Service Zone</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>Room101</td>
<td>Free</td>
<td>VIP Room - Free of Charge</td>
<td>SZ1</td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>Room102</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>103</td>
<td>Room103</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>104</td>
<td>Room104</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>105</td>
<td>Room105</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>106</td>
<td>Room106</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>107</td>
<td>Room107</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>108</td>
<td>Room108</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>109</td>
<td>Room109</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
<tr>
<td>110</td>
<td>Room110</td>
<td>Charge</td>
<td></td>
<td>SZ1</td>
<td>Delete</td>
</tr>
</tbody>
</table>

(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.
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’**.
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.

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

### Welcome to Broadband Internet Service

**Please choose from the following service selection**

<table>
<thead>
<tr>
<th>Plan</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 hr(s)</td>
<td>5</td>
</tr>
<tr>
<td>24 hr(s)</td>
<td>18</td>
</tr>
<tr>
<td>48 hr(s)</td>
<td>32</td>
</tr>
<tr>
<td>120 hr(s)</td>
<td>60</td>
</tr>
<tr>
<td>160 hr(s)</td>
<td>74</td>
</tr>
<tr>
<td>1000 Mbyte(s)</td>
<td>65</td>
</tr>
<tr>
<td>Until 22:00</td>
<td>12</td>
</tr>
</tbody>
</table>

### 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.
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’
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 500 cents.

**************************************************************************************************

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.
Step 5:

Surf the Internet. Test complete!
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._
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**
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 created 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 Configuration](image)

Click ‘Delete’ to delete the user name and password that mapped with Room 102.

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Remaining Quota</th>
<th>Status</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>zah6</td>
<td>mq78ee5d</td>
<td>10 min(s)</td>
<td>Normal</td>
<td>roomN-Room102</td>
</tr>
</tbody>
</table>

**NetComm NCT240 V3.0.9 IP DSLAM VLAN Tagging with IAC3000 Configuration Instruction**

Last updated on: Feb2010
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.

Welcome to Broadband Internet Service

Please choose from the following service selection

<table>
<thead>
<tr>
<th>Plan</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 hr(s)</td>
<td>5</td>
</tr>
<tr>
<td>24 hr(s)</td>
<td>18</td>
</tr>
<tr>
<td>48 hr(s)</td>
<td>32</td>
</tr>
<tr>
<td>120 hr(s)</td>
<td>60</td>
</tr>
<tr>
<td>188 hr(s)</td>
<td>74</td>
</tr>
<tr>
<td>1000 Mbyte(s)</td>
<td>65</td>
</tr>
<tr>
<td>Until 22:00</td>
<td>12</td>
</tr>
</tbody>
</table>

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.