





NCT192

Software Operation Guide

Table of Contents

Chapter 1	Preface.....	4
	Purpose.....	4
	Organization	4
	Conventions	4
Chapter 2	NCT192 Management System Overview.....	6
	NCT192 Overview	6
	NCT192 Features	6
	System Hardware and Software Requirement	6
Chapter 3	Getting Started NCT192	8
	Installing the NCT192	8
	Starting a NCT192 Session	10
	Navigating of NCT192	11
	Keyboard Commands	11
	Right Mouse Button	11
	NCT192 Window Overview	11
	Managing the Trap Log View	11
	Icons and LED Sign Overview	13
	Error Handling Dialog	15
	Data Exporting and Graphic Displaying.....	16
Chapter 4	Initiating the NE	18
	Constructing the NE Objects	18
	NE SNMP Management	24
	Configuring the SNMP Trap Manager	24
	Configuring the SNMP Community.....	26
	User Account Management	27
	Secured Host Management	29
	NE Date and Time Management	30
	DNS Server Setting	31
	Time Server Setting	32
	Managing the NE Configuration	34
	Saving NE configuration to Flash	34
	Erasing NE configuration from Flash.....	34
Chapter 5	Profile Management.....	36
	Configuring the xDSL Profile	38
	ADSL Profile	38
	SHDSL Profile.....	50
	Configuring the VLAN Profile.....	55
	IP Traffic Profile.....	55
	TV Channel Profile.....	57
	Multicast Service Profile	59
	Configuring the Alarm Definition Profile.....	60
Chapter 6	Interface Port Management.....	63
	xDSL Line Interface Management	63
	GE Network Interface Management	66
	Link Aggregation (Static / Dynamic).....	68
	RSTP Configuration.....	70
	CoS Configuration	75
	Manual VLAN Setting	77
	Cascaded NE Management.....	78
	Configuring the NE Role	80

Adding Remote NE	81
Chapter 7 Connection Port Management.....	84
VC-to-VLAN Connection Management.....	84
ISP Information for IP over ATM	92
Access Control List	94
NetBIOS/NetBEUI Packet Filtering.....	94
Source MAC Access Control List.....	95
Static MAC configuration on xDSL Port.....	98
Multicast Service Management	101
Multicast Channel Configuration.....	101
IGMP snooping/IGMP proxy Configuration	103
System Services Configuration	106
MAC Aging for Bridged Services	106
VLAN MAC Limit.....	106
DHCP Service Configuration	108
PPPoE Sub-option Configuration	111
xDSL Port Agent ID Management.....	111
Chapter 8 Fast Provision Management.....	113
Interface and VC-VLAN Fast Provisioning	113
Multicast Service Fast Provisioning.....	121
Chapter 9 Performance Management.....	125
xDSL Line Current Performance Information	125
xDSL Line Historical Performance Information.....	128
GE Interface Performance Statistics.....	131
Chapter 10 Fault Management	133
NE Alarm Information.....	133
System Alarm Management.....	135
Alarm Synchronization.....	136
Relay-Input Alarm Management	136
Relay-Output Alarm Management	138
Hardware Status Monitoring	139
Chapter 11 Diagnosis Management.....	142
xDSL Line Status Diagnosis	142
Port Rate Status.....	142
Bits Allocation Monitoring.....	144
Loop Monitoring	146
Loop Diagnosis (DELT <Dual-Ended Line Test>)	149
Loop SELT Test (Single End Loop Test)	152
xDSL Service Status Diagnosis	153
ATM OAM F5 VC Diagnosis	153
Bridge Filtering Database	154
VLAN Membership.....	159
xDSL MAC Spoofing Status	161
Multicast Channel Status	162
Multicast Group Membership.....	163
xDSL Downstream Broadcast Forwarding VLANs	165
DHCP Session Information.....	165
PPPOE Session Information	166
Trunk Current Status Diagnosis	168
LACP Diagnosis.....	168
RSTP Diagnosis	169
UGE VLAN List.....	172
SFP Information List	173
Network Diagnosis	175

Ping NE	175
Traceroute	177
Telnet	178
Telnet Timeout	179
Check SNMP Connection	179
Chapter 12 General System Management.....	181
NCT192 Options	181
Configuring the Alarm Warning Options	181
Chapter 13 Administrating and Maintenance	183
NE Inventory Information	183
NE Configuration Backup and Restore.....	184
NE Firmware Upgrade	185
SHDSL LC Firmware Upgrade	187
NE Boot Partition	188
NE File System List	189
Reset the Unit	190
Appendix A Abbreviations and Acronyms	191
Appendix B Alarm Definition	193
Appendix C: Legal & Regulatory Information.....	195

Chapter 1 Preface

This preface describes the “*NCT192 Software Operation Guide*” about how it is organized, and its document conventions. It contains the following topics.

- Purpose
- Organization
- Conventions
- Revision History

Purpose

The purpose of this guide is to provide detailed information and description of NCT192 (Local Craft Terminal) software, despite the variation in experience of the technicians. This document is intended to help them to operate the software and connect the NCT192 IP-DSLAM to the network as quickly as possible.

Organization

This guide contains the following chapters:

- Preface
- NCT192 Management System Overview
- Getting Started
- Initiating the NE
- Profile Management
- Interface Port Management
- Connection Port Management
- Fast Provision Management
- Performance Management
- Fault Management
- Diagnosis Management
- General System Management
- Administrating and Maintenance
- Abbreviations and Acronyms
- Alarm Definition

Conventions

This section describes the conventions used in this guide.

NE/NEs mentioned in this document means NCT192 IP-DSLAM unless specifically indicated..

ADSL mentioned in this document covers ADSL, ADSL2, and ADSL2+, unless specifically indicated. The **ADSL** specified in this document complies with ITU-T Rec. G.992.1, G.992.2, G.992.3 and G.992.5.

SHDSL mentioned in this document complies with ITU-T Rec. G.991.2,

xDSL hereinafter is referred as both the ADSL and SHDSL, unless specifically indicated.

CLI Ex – The command line management with a local console or Telnet through in-band or out-of-band IP interface for CIT (Craft Interface Terminal) connection.



This sign indicates the **NOTICE**. A note contains helpful suggestions or reference relay on the topical subjects.



This sign indicates the **TIP**. Performing the information described in the paragraph will help you solve a problem. The tip information might not be troubleshooting or even an action, but could be useful information.



This sign indicates the **CAUTION**. In this situation, you might do something that could result in equipment damage or loss of data.



This sign indicates the **DANGER**. You are in situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Chapter 2 NCT192 Management System Overview

This chapter describes the NCT192 user interface. This chapter contains the following sections:

- NCT192 Overview
- NCT192 Feature
- System Hardware and Software Requirement

NCT192 Overview

NCT192 is designed according to the following principles:

- Monitor and configure the network in real-time such as diagnostics, status gathering, service provision and NE reset
- Easy to maintain. The NCT192 is designed on the PC platform and is compatible to Microsoft Windows 98SE/ME/2000/XP
- Easy to operate. The NCT192 provides user-friendly configuration interface
- Various alarm severity levels are provided for all possible events/conditions

NCT192 Features

The NCT192 system supports various functions for the effective operation and maintenance of the NE. The system supports, fault management (FM), performance management (PM), configuration management (CM), and security management (SM) of NCT192 IP-DSLAM.

Real-time System Status Monitoring

The NCT192 collects the SNMP traps for the discrete alarm, faceplate LEDs, and system failures in real time for monitoring and displays of the xDSL and network interfaces, and Fan, Power, and Alarm relay status.

The NE indicated with colors for different status by GUI interface. Any addition and deletion of element or plug-in unit of NE will automatically detect and reflected in NCT192.

Administration

Administrative function allows operator to plan or manage their NEs on the network.

Error Handling

When execution is not successful, error message will be displayed, and the operator has to configure problem entries and the process before proceeding further.

NCT192 support function to depict the failure status of the NE in registered manage network.

System Hardware and Software Requirement

NCT192 is designed on a high stability and reliability platform, for performing fluent in management. The NCT192 recommends the hardware/software in list below to achieve the performance.

The recommend hardware & OS for NCT192:

- Pentium 4 1.6 GHz or higher

- 256 MB RAM
- 40 GB Hard disk
- 10/100 Base-T Ethernet network card

The Software require for NCT192 System:

- Operating System – Microsoft Windows 98SE/ME/2000/XP (2000 is recommend)
- NCT192 Installation Package

Chapter 3 Getting Started NCT192

This chapter describes on how to install the NCT192, and provides the general navigating concept of NCT192 to help you to quickly handle it.

This chapter contains the following sections:

- Installing the NCT192
- Starting NCT192 Session
- Navigating in NCT192 Client
- Managing the Trap Log View
- Icon and LED Sign Overview
- Error Handling Dialog
- Data Exporting and Graphic Displaying

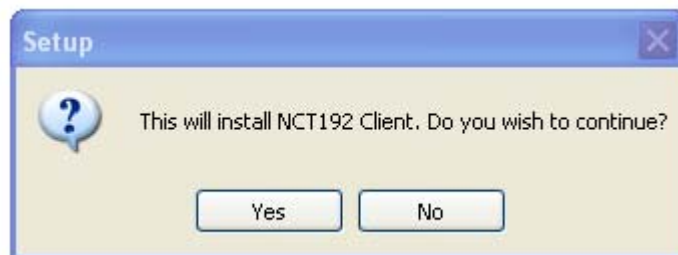
Installing the NCT192

Before installing the NCT192 software, please make sure both of your requirement of hardware and software are completed with recommend specification list in “Chapter 2 System Hardware and Software Requirement”.

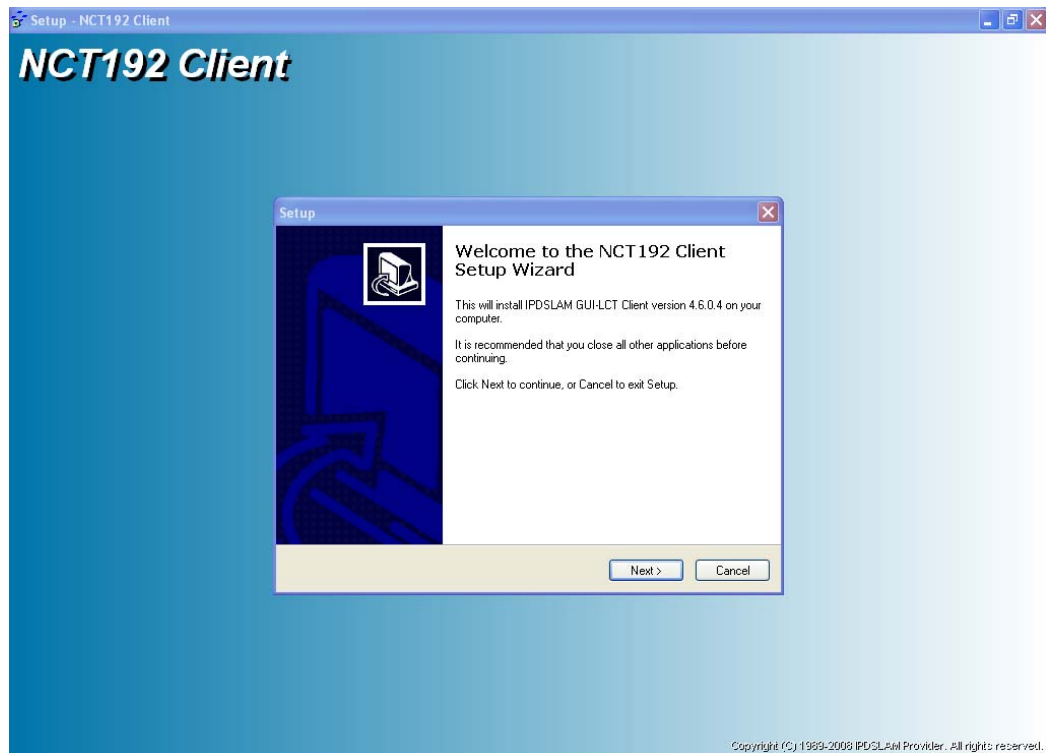
- Step 1** Insert the ‘NCT192 Installation Package’ CD to your CD/DVD driver, from the directory of ‘NCT192_LCT’ double click on the ‘NCT192_GUI_LCT_setup.exe’ executable file.



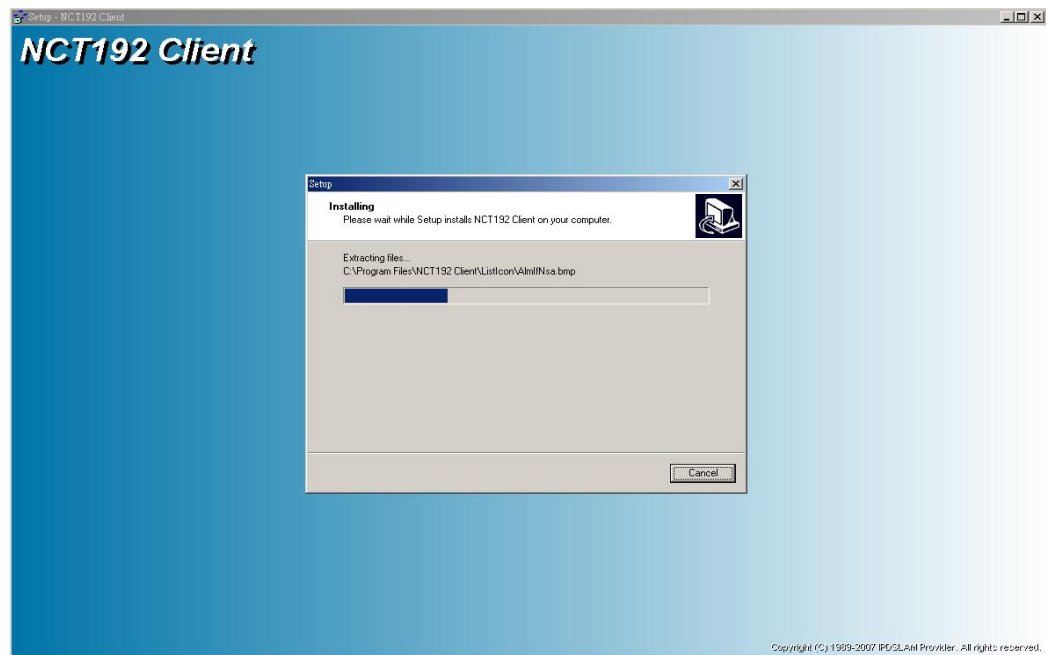
- Step 2** Select ‘Yes’ from the launched window to continuous the installation.



Step 3 Click the 'Next' button to start the setup wizard.

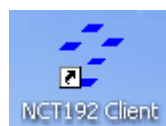


Step 4 Identify the program directory and additional task before processing installation.



Step 5 Once the installation is completed, you will have an 'NCT192 Client' icon on your desktop; double click this icon to run the NCT192 Client software.

Step 6 Double click this icon on desktop to run the NCT192 Client software.



Starting a NCT192 Session

Double click the 'NCT192 Client' icon on your desktop to launch the NCT192 login dialog.

Use default user and community to access with read-write privilege.

User: **admin**
Community: **netman**

For default read-only privilege using:

User: **guest**
Community: **public**

You can change the login account and privilege from CLI Ex mode or later from NCT192.

To start an NCT192 session, follow these steps.

- Step 1** Open NCT192 session by double clicking the 'NCT192 Client' icon on the MS-Windows.
The Login window appears.

Figure 3-1 NCT192 Login Dialog

- Step 2** Specify NE IP address and enter the associated user name and SNMP community.

- Step 3** Click **Login** to proceed.
If you enter an unknown user name or invalid community, the system will display an error message. To continue, click **OK**, and then enter a valid user name and SNMP community.
When you enter a valid user name and SNMP community, the session starts and the NCT192 application appears.



Both the user name and SNMP community are case-sensitive.



If you don't have any account creates initially or you have trouble to login, please refer to NCT192 System Configuration Guide "*Chapter 2 Managing the Session Login Account*" to managing the user account, also refer to "*Chapter 3 Configuring the SNMP Manager*" to managing the SNMP community.

Navigating of NCT192

NCT192 software uses familiar functionality and menus found in most MS-Windows-based graphical user interface. This section describes the functions available in NCT192.

Keyboard Commands

Certain Keyboard commands are available in NCT192. These commands serve as an alternative to mouse functionality.

Keyboard Command	Description
Operation	
Tab	Move among the fields in a window/dialog.
Arrow Keys	Scroll through the text in a data entry field or through the values of a list box.
Alt Key	Access a menu by typing the appropriate keyboard command.

Right Mouse Button

NCT192 software provides right-click mouse functionality. By positioning the mouse cursor over an “NE object”, you can click the right mouse button to view the launched **Function Menu**. The **Function Menu** options available depend on selected “NE object”. You can then use the left or right mouse button to open the associated function dialog window.

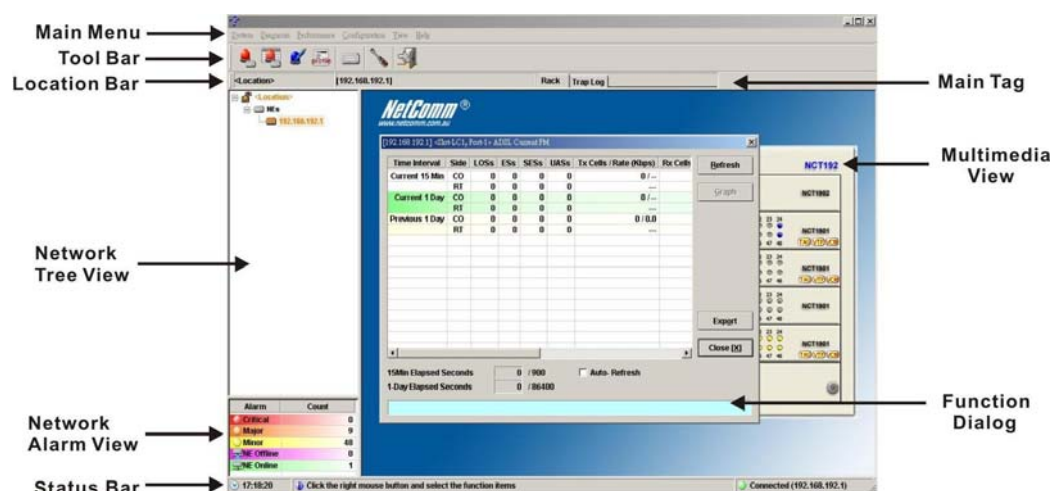


The “NE object” denotes the NE entity, Shelf, Slot/Box, and Port displaying on the Rack tab of Multimedia View area or Network Tree View area.

NCT192 Window Overview

The NCT192 Operation window contains several parts; each part varies depending on the window in which you are viewing or configuring.

Figure 3-2 NCT192 Operation Window



Managing the Trap Log View

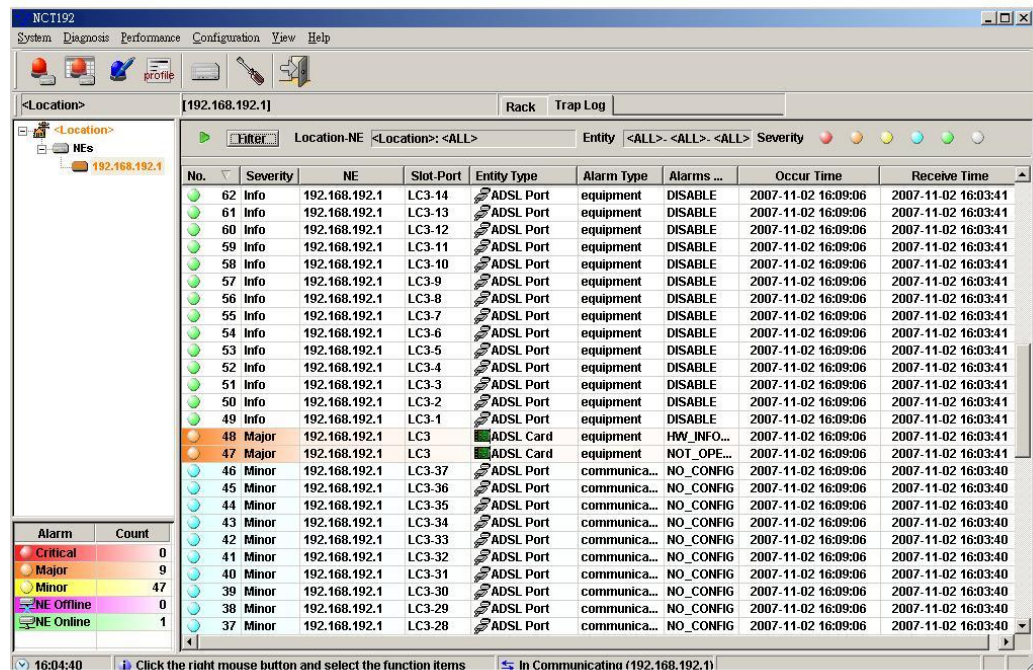
Click the “Trap Log” tab view to display the system trap (alarm) information.

The NE would send SNMP traps to a designated host IP address when there is one or more status are changed. The “Trap Log” records and saves the SNMP traps on the host which is specified a trap station since the host logged in LCT.

Operator will not see the trap logs on LCT if the host IP address is not one of the trap stations.

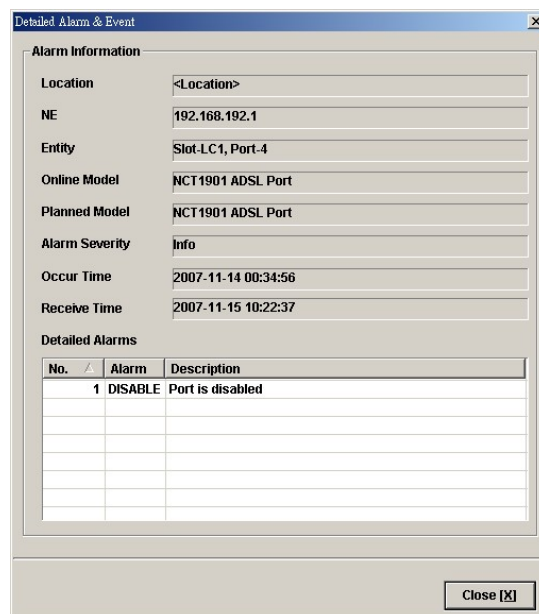
Chapter 4 “Configuring the SNMP Trap Manager” shows you how to configure the SNMP trap station.

Figure 3-3 NCT192 Trap Log View



Select a specific trap from **List Table** and using right mouse button to launch the **Function Menu**, select ‘**Detail**’ to view the detailed alarm & event dialog.

Figure 3-4 Detailed Alarm & Event Dialog

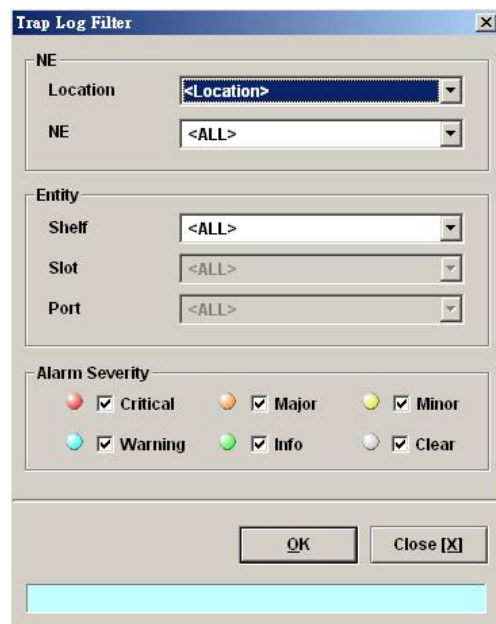


You can also select the ‘**Pause**’ or ‘**Reset**’ from launched **Function Menu** to stop refreshing traps

or clearing all traps cached in the NCT192.

Click the **Filter** button at top-left corner of **Trap Log** tab view to open the Trap Log Filter dialog. Here you can define the rule of showing filtering new coming traps. This is a useful tool to filter out unnecessary traps.

Figure 3-5 Trap Log Filter Dialog



Icons and LED Sign Overview

Table 3-1 lists the icons and LED signs used inside the NCT192.

Table 3-1 Icon and LED Sign Description








Symbol	Description
Tool Combo-box	
	System active alarm (current alarm).
	System history alarm (history alarm).
	System alarm profile (alarm definition).
	System profile configuration.
	NE management.
	NCT192 Options.
	Exit NCT192.

Table 3-1 Icon and LED Sign Description (Continued)






















































Symbol	Description
Status Combo-box	
	Hint information.
	PC data and time.
 /  / 	Connection status. (idle, disconnected, in communication)
Network List View	
 / 	NE contains critical alarm
 / 	NE contains major alarm
 / 	NE contains minor alarm
 / 	NE contains events
 / 	NE is in normal status
Network Alarm View	
	Critical Alarm
	Major Alarm
	Minor Alarm
	NE offline
	NE online
Rack View	
	Port disable or no such profile
	Port contains critical alarm
	Port contains major alarm
	Port contains minor alarm
	Port contains warning alarm
	Port contains no alarm / Port linked
	NC card in working mode (Not applicable to NCT192)
	NC card in standby mode (Not applicable to NCT192)
	NC / LC card type is mismatch
	NC / LC card not exist
	NC / LC card in the Tagged VLAN mode.
	NC / LC card in the Un-tagged VLAN mode.
	LC card in the VLAN tag Pass-through mode
	LC card in the RFC2684 VC-MUX mode.
Trap Log View	
	Current Critical alarm
	Current Major alarm
	Current Minor alarm
	Current Event alarm
	Alarm clear / No alarm
	Identify as card alarm
	Identify as port alarm

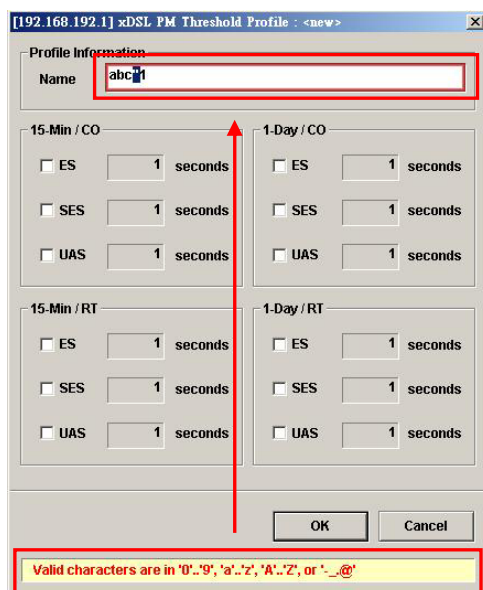
Table 3-1 Icon and LED Sign Description (Continued)

Symbol	Description
Function Dialog	
	Indicates data in list table is active and valid.
	Indicates data in list table is inactive or invalid.
	Indicates the status of specific port in list table is link up.
	Indicates the status of specific port in list table is link down.
	Indicates the status of task is finished.
	Indicates the status of task is successful.
	Indicates the status of task is failed.
	Indicates the item is checked.
	Indicates the item is unchecked.
	Indicates the field is sorted by ascendant order in list table.
	Indicates the field is sorted by descendant order in list table.
	Indicates the field is sorted by another field in list table.

Error Handling Dialog

NCT192 provides the error handling dialog. Each dialog has a text block at button edge, this text block will shown error message and highlight the red rectangle at specifics box where contains invalid or illogical parameter. You must fix the error to proceed with the task.

The following figure depicts the example on how dialog performs the error handling.

Figure 3-6 Error Handling Message

Data Exporting and Graphic Displaying

NCT192 provides the data exporting of dialog List Table information.

Figure 3-7 **Export Dialog**

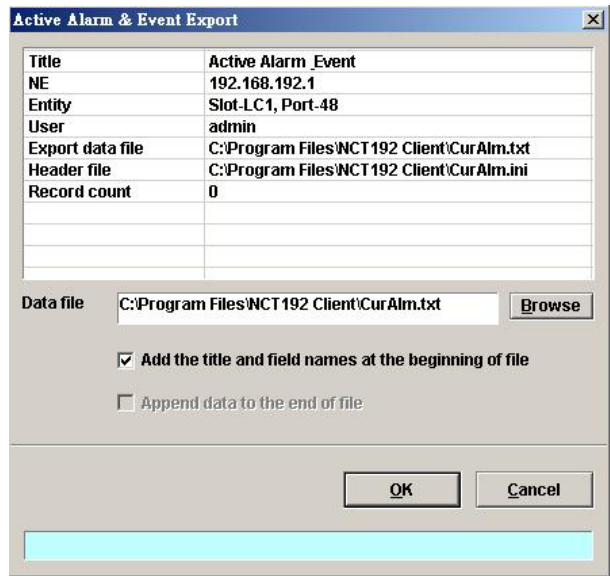


Table 3-2 **Export Dialog Description**

Field	Description
Data file	Data file location
Add the title and field names at the beginning of file	Check to add the title and field names in the front of output file.
Append data to the end of file	Check to append data to the end of output file.
Browse	Click to select the output file by way of file manager.

Figure 3-8 2D/3D Data Graph Displaying Dialog

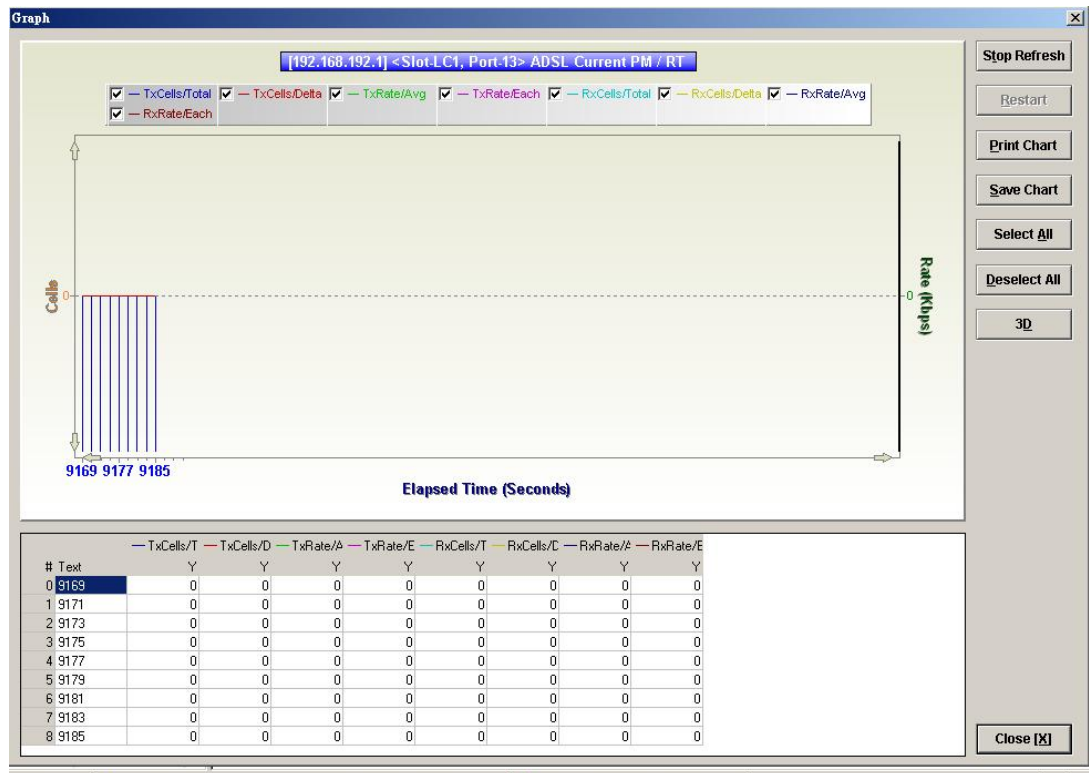


Table 3-3 2D/3D Data Graph Displaying Dialog Description

Field	Description
Print Chart	Click to print the chart diagram
Save Chart	Click to save the chart diagram in file.
Select All	Click to check all linear elements.
Deselect All	Click to uncheck all linear elements.
3D/2D	Click to toggle the style of chart diagram.
Close	Exit the data graph displaying Dialog.

Chapter 4 Initiating the NE

This chapter describes how to initially configure the NCT192 IP-DSLAMs before the advanced configuration depicted in the rest of this document.

This chapter contains the following sections:

- Constructing the NE Objects
- NE SNMP Management
- User Account Management
- Secured Host Management
- NE Date and Time Management
- DNS Server Setting
- Time Server Setting
- Managing the NE Configuration

Constructing the NE Objects

As the NCT192 IP-DSLAM provides the flexibility to be equipped with various card modules such as ADSL-LC (Line Card) and SHDSL-LC, constructing the NE board type of card module is the first task you need to perform.

Once the card modules to be equipped to the NCT192 IP-DSLAM are determined, you need to set the planned type according to their correspondent slot to secure the system operation. For any reason (removed or type error), if the planned type is not the same as the online type detected from the system, the board mismatch alarm message will be reported to NCT192 and the configured NCT192 Server..

The NE supports the following functions on a per LC/NC basis.

- Planning the card type of a LC slot
To ease the operator to plan the usage of each LC slot in advance, the NE support to configure the planned type of a LC slot. There will be an alarm arise if the planned card type and the actual plug-in card type are different.
- RFC 2684 encapsulation method for ADSL line card, either LLC or VCMUX.
- “Service Type Control” for ADSL line card.
Operator can define the service which allow user to pass, they are “DHCP”, “PPPoE” and “Static IP”.
- VLAN tag pass-through function for ADSL line card
Whenever the VLAN tag pass-through (VTP) is configured as enabled, the LC provides transparent transportation of the VLAN traffic from subscriber interface to network interface without any VLAN tag attachment. The LC will not attach any VLAN tag to the upstream subscriber traffic. In the mean time, the LC will also not replace the existing VLAN tag of the upstream subscriber traffic.
On the other hand, in the case that the VTP function is configured as disabled, the LC will attach a VLAN tag to all the traffic from subscriber interface to network interface.
- IEEE 802.1Q VLAN forwarding function for ADSL line card and GE ports
The operator can set the xDSL subscriber ports as well as the GE ports to only forward either tagged traffic or untagged traffic.

- Step 1** From the **‘Rack’** tab view, point the mouse cursor on the NE object (Shelf, NC slot, or LC slot), and then right click the mouse button to launch the function menu and then click **‘Board Setting on Function Menu’** to open the **Board Setting List** Dialog, or click Diagnosis → Board Setting on **Main Menu** to open the **Board Setting List** Dialog as shown in Figure 4-1 and Table 4-1 depicts the related parameters.

Figure 4-1 Board Setting List Dialog

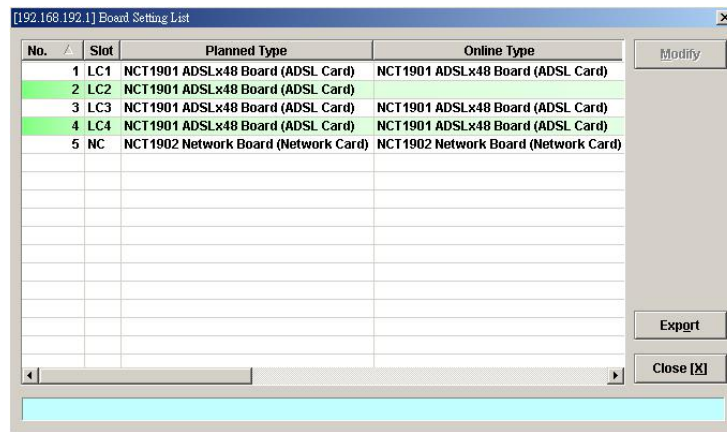


Table 4-1 Board Setting List Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
Slot	This indicates the location of board.
Planned Type	This indicates the board type planned to be equipped to the slot of NCT192 IP-DSLAM. If the planned type is mismatched (removed or type error) with online type detected from the system, the board mismatch alarm message will be reported.
Online Type	This indicates the observed board type of the card module in the slot (current type)
AAL5 Encapsulation	This indicates the AAL5 encapsulation mode, either “LLC” or “VC-MUX”(VC Based Multiplexing) per RFC-2684. RFC 2684 defines the encapsulation methods for transporting the routed and bridged Protocol Data Units (PDUs) across a native ATM network.
Service Type Control	This indicates the “Service Type Control” function is enables or not. The service type control can be enabled to provide control of PPPoE, DHCP or static IP on a per line card basis.
Configured Tagged mode	This indicates the tagged mode is configured as either tagged or untagged mode.
Run-Time Tagged mode	This indicates the operational status of tagged mode. Tagged-only: LC (or NC) only forwards the tagged Ethernet frame and drops the untagged Ethernet frame. Untagged-only: LC (or NC) only forwards the untagged Ethernet frame and drops the untagged Ethernet frame. It is noted that the value of configured Tagged mode and its Run-Time Status may be different. Please refer to Table 4-3 for the NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.

Table 4-1 Board Setting List Description (Continued)

Field	Description
List Table	
Configured VLAN Tag Pass Through (VTP)	This indicates the VLAN tag pass-through (VTP) is configured as enables or not. (per LC setting) The VTP function provides transparent transportation of the VLAN traffic from subscriber interface to network interface without VLAN tag attachment, this allows subscriber deployed their own VLAN ID to associate in the network without double tag or replace the existing VLAN ID by system.
Run-Time VLAN Tag Pass Through (VTP)	This indicates the operational status of VTP. It is noted that the value of configured VTP and its Run-Time Status may be different. Please refer to Table 4-3 for the NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.
Function Button	
Modify	Selected the row and click ' Modify ' button to perform the modification of specific item on the selected board.
Export	Click this button to save the contents of Board Setting List to the Personal Computer.
Close	Exit the Board Setting List Dialog.

Step 2 To modify the slot setting, click and highlight a slot from **Board Setting List** and click '**Modify**' button to launch the **Board Setting** Dialog as shown in Figure 4-2 and Figure 4-3 for LC and NC setting, respectively. Table 3-1 depicts the related parameters.

Figure 4-2 xDSL Board Setting Dialog

The screenshot shows the 'xDSL Board Setting Dialog' for Slot-LC1. The 'Board Type' section shows 'Online Type' as 'NCT1901 ADSLx48 Board (ADSL Card)' and 'Planned Type (NE)' as a dropdown menu with the same value. The 'Board Settings' section contains four rows of settings: 'AAL5 Encapsulation' with 'LLC' selected; 'Service Type Control' with 'Disable' selected; 'Tagged Mode' with 'Untagged-Only' selected and a text field showing 'Untagged-Only'; and 'VLAN Tag Pass Through' with 'Disable' selected and a text field showing 'Disable'. The dialog has 'OK' and 'Close [X]' buttons at the bottom right.

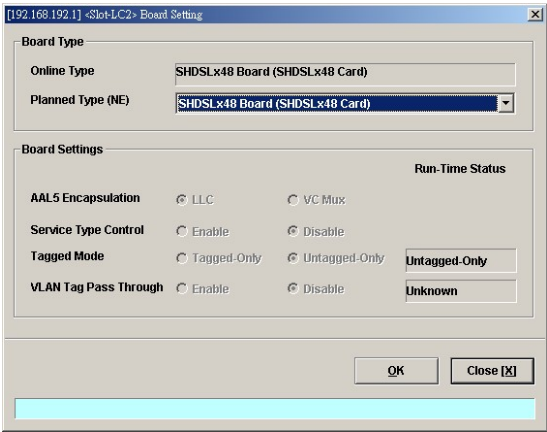


Figure 4-3 NC Boarding Setting Dialog

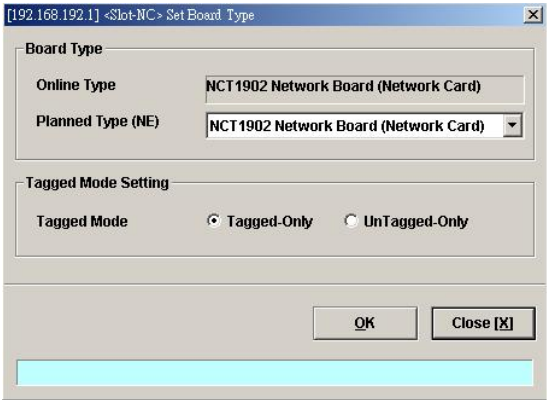


Table 4-2 Board Setting Dialog Description

Field	Description
Board Type	
Planned Type [Modify]	This specifies the board type planned to be equipped to the slot of NCT192 IP-DSLAM. If the planned type is mismatched (removed or type error) with online type detected from the system, the board mismatch alarm message will be reported.
Online Type	This specifies the observed board type of the card module in the slot (current type)
Board Settings	
AAL5 Encapsulation [Modify]	This specifies the AAL5 encapsulation mode, either “LLC” or “VC-MUX”(VC Based Multiplexing) per RFC-2684. RFC 2684 defines the encapsulation methods for transporting the routed and bridged Protocol Data Units (PDUs) across an native ATM network.
Service Type Control [Modify]	This specifies the “Service Type Control” function is enables or not. The service type control can be enabled to provide control of PPPoE, DHCP or static IP on a per line card basis.
Tagged mode [Modify]	This specifies the tagged mode is configured as either tagged or untagged mode.
Run-Time Status of Tagged mode	This specifies the operational status of tagged mode. Tagged-only: LC (or NC) only forwards the tagged Ethernet frame and drops the untagged Ethernet frame. Untagged-only: LC (or NC) only forwards the untagged Ethernet frame and drops the untagged Ethernet frame. It is noted that the value of configured Tagged mode and its Run-Time Status may be different. Please refer to Table 4-3 for the NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.
VLAN Tag Pass Through (VTP) [Modify]	This specifies the VLAN tag pass-through (VTP) is configured as enables or not. (per LC setting) The VTP function provides transparent transportation of the VLAN traffic from subscriber interface to network interface without VLAN tag attachment, this allows subscriber deployed their own VLAN ID to associate in the network without double tag or replace the existing VLAN ID by system.
Run-Time Status of VTP	This specifies the operational status of VTP. It is noted that the value of configured VTP and its Run-Time Status may be different. Please refer to Table 4-3 for the NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.
Function Button	
OK	Press this button to commit setting.
Cancel	Press this button to cancel setting.



Board Setting Dialog allows you to define the line card (LC) AAL5 encapsulation mode, “VLAN Tag pass-through (VTP)” mode, Tagged mode and “Service Type Control” mode. Those functions indicate as per board, configuration affects the setting of all ports of selected LC.



The ADSL LC needs to be reset to perform the expected system behavior as depicted in Table 4-3 whenever its run-time status changes.



The NC needs to be reset to perform the expected system behavior as depicted in Table 4-3 whenever its configured tagged mode changes.



Whenever the GE2 is set as subtended port and the NC is set as “tagged-only” mode, in order to make the NE forward the VLAN-specific traffic between GE1 and GE2, the operator needs to manually set GE1 and GE2 as the member ports of VLANs in interest. Please refer Section “Manual VLAN Setting” for the VLAN-member port setting of GE1 and GE2 whenever GE2 works as a subtended port.

It is noted that the run-time status of LC may be different to its corresponding configuration. In this case, the behavior of the NE is per the run-time status of NE instead of their configuration. To describe the NE behavior, the following notations are adopted in Table 4-3

- Q_S represents the service VLAN-tag and its VLAN-ID value is provided by the NE.
- $Q_{S(CPE)}$ represents the service VLAN-tag and the notation $_{(CPE)}$ indicates that its VLAN-ID value is provided by the CPE (or the subscriber's PC behind the CPE).
- $Q_{(CPE)}$ represents the 802.1Q VLAN-tag.
- $Q_{C(CPE)}$ represents the customer VLAN-tag and the notation $_{(CPE)}$ indicates that its VLAN-ID value is provided by the CPE (or the subscriber's PC behind the CPE).

Table 4-3 The NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.

NC Setting	ADSL LC setting		ADSL LC Run-Time Status		Expected NE behavior			
	Tagged mode	VTP	Tagged mode	VTP	VLAN-tagging Status of Egress Traffic		Acceptable Ingress Traffic	
Tagged mode					On NC	On the ADSL line	On NC	On the ADSL line
Tagged	Tagged	Enabled	Tagged	Enabled	$Q_{S(CPE)}$	$Q_{(CPE)}$	Tagged	Tagged
		Disabled	Tagged	Disabled	$Q_S + Q_{C(CPE)}$	$Q_{(CPE)}$	Tagged	Tagged
	Untagged	Enabled	Untagged	Disabled	Q_S	Untagged	Tagged	Untagged
		Disabled	Untagged	Disabled	Q_S	Untagged	Tagged	Untagged
Untagged	Tagged	Enabled	Untagged	Disabled	Untagged	Untagged	Untagged	Untagged
		Disabled	Untagged	Disabled	Untagged	Untagged	Untagged	Untagged
	Untagged	Enabled	Untagged	Disabled	Untagged	Untagged	Untagged	Untagged
		Disabled	Untagged	Disabled	Untagged	Untagged	Untagged	Untagged



It is noted that the NE will drop the tagged Ethernet frames of VLAN-ID not configured by the VC-to-VLAN setting (see Figure 7-5) in the following case.

NC tagged mode = Tagged
 LC tagged mode Run-Time Status = Tagged
 LC VTP Run-Time Status = Enabled



The tagged mode (run-time) indicates the operational status of tagged mode.

Tagged-only: LC (or NC) only forwards the tagged Ethernet frame and drops the untagged Ethernet frame.

Untagged-only: LC (or NC) only forwards the untagged Ethernet frame and drops the tagged Ethernet frame.

It is noted that the value of configured Tagged mode and its Run-Time Status may be different. Please refer to Table 4-3 for the NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.

NE SNMP Management

SNMP (Simple Network Management Protocol) is an application-layer protocol that facilitates the exchange of management information between a NE and LCT. SNMP enables the administrators to manage the NE by the LCT. In the term of SNMP, the NE plays the role of SNMP agent and the LCT serves as the SNMP server. This section describes how to configure the SNMP on the NE.



Beware of the SNMP community setting, this will affects the communication between the NCT192 and NE, re-login the NCT192 if the SNMP community has been modified.

Configuring the SNMP Trap Manager

SNMP Trap Manager records the hosts (any SNMP server, like LCT, NCT192 Server, and so on) to be notified whenever the NE encounters abnormalities. When a trap condition happens to the NE, the NE sends the corresponding SNMP trap message to the hosts (SNMP server) specified in the SNMP Manager IP Address List.

Follow the subsequent procedures to configure the NE's SNMP Manager.

Step 1 Click Configuration → NE Management → SNMP Managers on **Main Menu** to open the **NE SNMP Manager IP Address List** Dialog as shown in Figure 4-4 and Table 4-4 depicts the related parameters.

Figure 4-4 NE SNMP Manager IP Address List Dialog

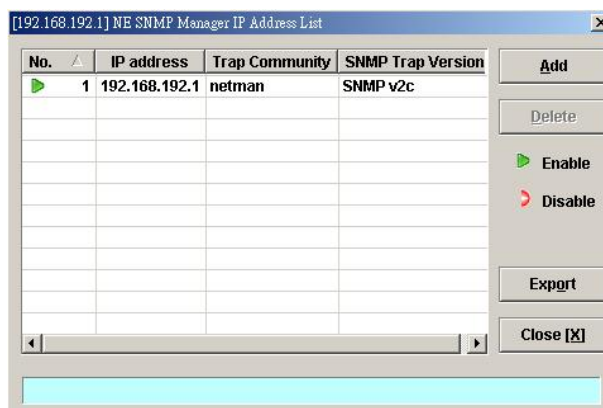


Table 4-4 NE SNMP Manager IP Address List Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
IP address	This indicates the IP address (Server / Host IP) of SNMP Manager.
Trap Community	This specifies the SNMP trap community of NE (Send Trap).
SNMP Trap Version	This specifies the Trap version.
Function Button	
Add	Click this button to create a new SNMP Manager (Trap) IP Address.
Delete	Select a trap community from the list table to remove.
Export	Click this button to save the contents of NE SNMP Manager IP Address List to the Personal Computer.
Close	Exit the NE SNMP Manager IP Address List Dialog.

Step 2 Click 'Add' button to create a new trap receiver host with community, while to remove the trap receiver, click and highlight a host in the list and click 'Delete' button, as shown in Figure 4-5 and Table 4-5 depicts the related parameters.

Figure 4-5 Add NE SNMP Manager IP Address Dialog

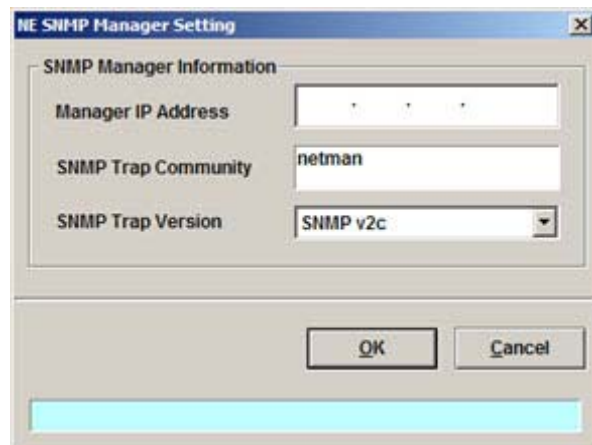


Table 4-5 Add NE SNMP Manager IP Address Dialog Description

Field	Description
IP address	This specifies the IP address (Server / Host IP) of SNMP Manager. Valid values: Any valid class A/B/C address
Trap Community	This specifies the SNMP trap community of NE (Send Trap). Valid values: String of up to 20 characters and any combination of printable characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_', '@').
SNMP Trap Version	This specifies the Trap version. Valid values: SNMP v2c

Configuring the SNMP Community

The SNMP community is a string representing the password to access the MIB of NE with the associated privilege. The NE supports two levels of privilege (Permission) as follows.

- Read / Write / Create – Allow the SNMP server to read and write all objects in the MIB, as well as the community strings.
- Read-only – Only allow the SNMP server to read all objects in the MIB except the community strings.



The community string definitions on your NCT192 must match at least one of those community string definitions on the NE. Otherwise, the LCT is not allowed to access the NE.

Follow the subsequent procedures to configure the NE's SNMP Community.

- Step 1** Click Configuration → NE Management → SNMP Community on **Main Menu** to open the **NE SNMP Community List** Dialog as shown in Figure 4-6 and Table 4-6 depicts the related parameters.

Figure 4-6 NE SNMP Community List Dialog

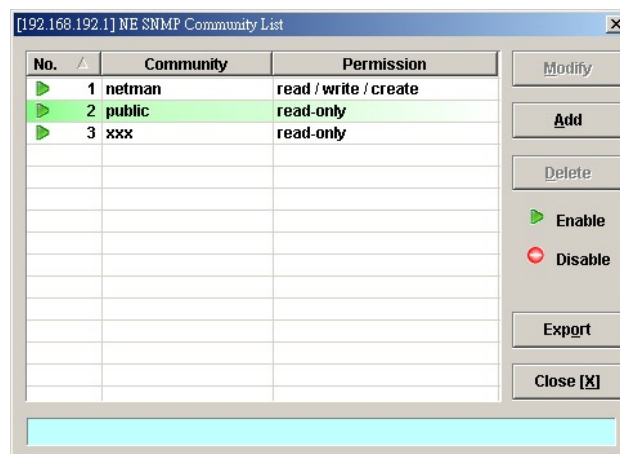


Table 4-6 NE SNMP Community List Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
Community	This indicates the case-sensitive SNMP community name.
Permission	This indicates the permission level, either “read only” or “read & write”
Function Button	
Modify	Select a SNMP community to modify.
Add	Click this button to create a new SNMP community of NE.
Delete	Select a SNMP community to remove.
Export	Click this button to save the contents of NE SNMP Community List to the Personal Computer.
Close	Exit the NE SNMP Community List Dialog.

- Step 2** Click ‘Add’ button to create a new SNMP community strings, while to remove the

SNMP community strings, click and highlight a community in the list and click **'Delete'** button, as shown in Figure 4-7 and Table 4-7 depicts the related parameters.

Figure 4-7 Add NE SNMP Community Dialog

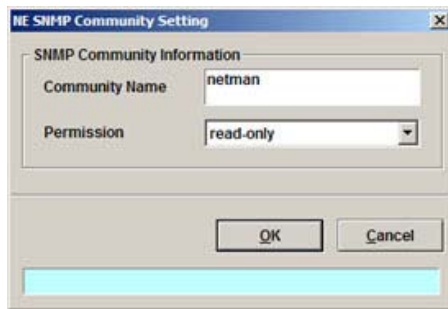


Table 4-7 Add NE SNMP Community Dialog Description

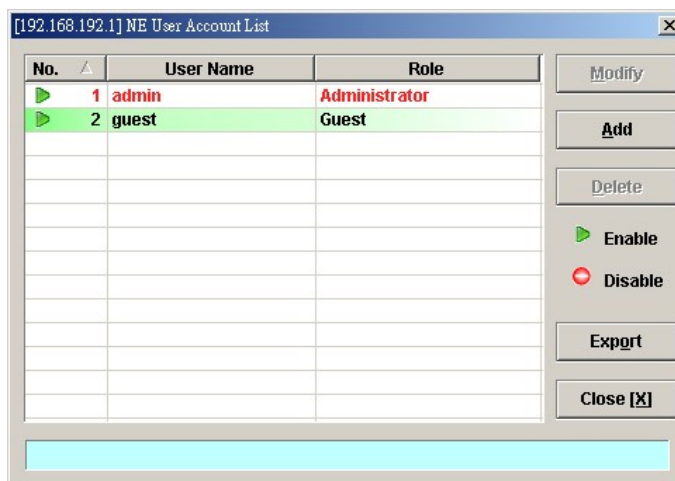
Field	Description
Community Name	This indicates the case-sensitive SNMP community name. Valid values: String of up to 20 characters and any combination of printable characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_', '@').
Permission	This indicates the permission level. Valid values: read-only, read/write/create

User Account Management

Follow the subsequent procedures to configure the user account of the NE.

- Step 1** Click Configuration → NE Management → NE connection → NE User Account on **Main Menu** to open the **NE User Account List** Dialog as shown in Figure 4-8 and Table 4-8 depicts the related parameters.

Figure 4-8 NE User Account List Dialog



- Step 2** Click **'Add'** button to create a new user account, while to remove the user account, click and highlight a user name in the list and click **'Delete'** button, as shown in Figure 4-9 and Table 4-9 depicts the related parameters.

Table 4-8 NE User Account List Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
User Name	This indicates the user account name.
Role	This indicates the permission right of user group.
Function Button	
Modify	Select a user name from the list table to modify.
Add	Click this button to create a new user of NE.
Delete	Select a user from the list table to remove.
Export	Click this button to save the contents of NE User Account List to the Personal Computer.
Close	Exit the NE User Account List Dialog.

Figure 4-9 NE User Account Setting Dialog
Table 4-9 NE User Account Setting Dialog Description

Field	Description
User Name	This indicates the user account name. Valid values: String of up to 20 characters and any combination of printable characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_', '@').
Password	This specifies the password.
Verification	This verifies the password again.
Role	This indicates the permission right of user group. Administrator – Owns privilege of Read/Write Guest – Owns only Read privilege



The single NE supports up to 12 concurrent telnet sessions. Only one concurrent telnet session is allowed to enter by admin account user at a time (Console access included).

Secured Host Management

The security host mechanism protects the NCT192 IP-DSLAM against unauthorized access from untrustful host. This feature allows you to specify up to 10 sections of IPs of trusted hosts and authorized services (e.g. SNMP, TELNET, and FTP)

Follow the subsequent procedures to configure the secured (trusted) hosts allowed to access the NE.

- Step 1** Click Configuration → NE Management → Secured Hosts on **Main Menu** to open the **NE Secured Host List** Dialog as shown in Figure 4-10 and Table 4-10 depicts the related parameters.

Figure 4-10 NE Secured Host List Dialog

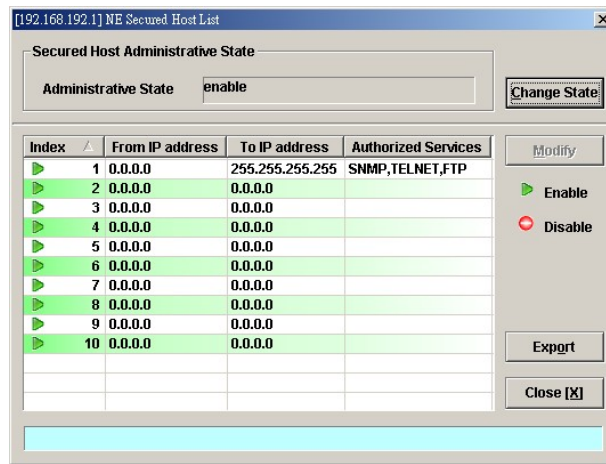
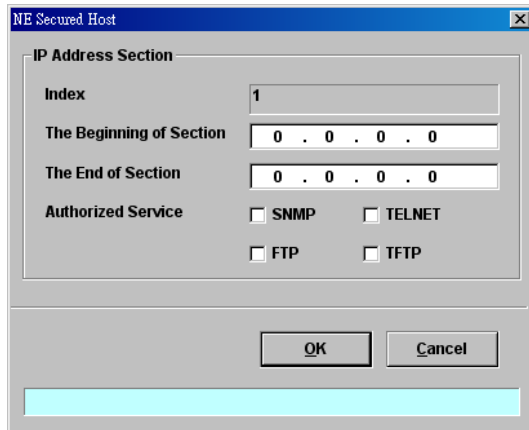


Table 4-10 NE Secured Host List Dialog Description

Field	Description
Secured Host Administrative State	
Administrative State	This indicates the state of NE secured host function. In case of enabled state, only the hosts of configured IP addresses are allowed to access the NE via the configured 'Authorized Services'.
List Table	
Index	This indicates the number of List Table.
From IP Address	This indicates the beginning of the IP address range of the secured hosts.
To IP Address	This indicates the end of the IP address range of the secured hosts.
Authorized Services	This indicates the services (any combination of SNMP, TELNET, FTP and TFTP) the specified secured hosts are allowed.
Function Button	
Change State	Click this button to enable or disable the secured host function.
Modify	Click this button to modify the specified secured host list.
Export	Click this button to save the contents of NE Secured Host List to the Personal Computer.
Close	Exit the NE Secured Host List Dialog.

- Step 2** Click and highlight a row and click '**Modify**' button to modify the secured hosts, as shown in Figure 4-11 and Table 4-11 depicts the related parameters.

Figure 4-11 NE Secured Host Setting Dialog


The dialog box is titled "NE Secured Host". It contains an "IP Address Section" with the following fields:

- Index:** A text box containing the value "1".
- The Beginning of Section:** A text box containing "0 . 0 . 0 . 0".
- The End of Section:** A text box containing "0 . 0 . 0 . 0".
- Authorized Service:** Four checkboxes are displayed:
 - ☐ SNMP
 - ☐ TELNET
 - ☐ FTP
 - ☐ TFTP

At the bottom of the dialog are two buttons: "OK" and "Cancel".

Assign the IP range and check the authorized services (any combination of SNMP, TELNET, FTP and TFTP) of trusted hosts to be allowed.

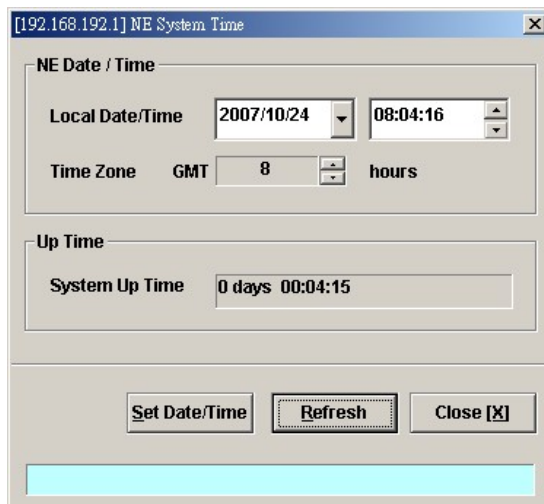
Table 4-11 NE Secured Host Setting Dialog Description

Field	Description
IP Address Section	
Index	This indicates the index of IP address section under modifying.
The Beginning of Section	This specifies the beginning of the IP address section of the secured hosts.
The End of Section	This specifies the end of the IP address section of the secured hosts.
Authorized Service	Check the checkbox to select the authorized services.

NE Date and Time Management

Follow the subsequent procedures to configure the NE system time.

Click Configuration → NE Management → System Time on **Main Menu** to open the **NE System Time** Dialog as shown in Figure 4-12 and Table 4-12 depicts the related parameters.

Figure 4-12 NE System Time Dialog


The dialog box is titled "[192.168.192.1] NE System Time". It contains the following sections:

- NE Date / Time:**
 - Local Date/Time:** A date field showing "2007/10/24" and a time field showing "08:04:16".
 - Time Zone:** A dropdown menu showing "GMT", a text box containing "8", and the word "hours".
- Up Time:**
 - System Up Time:** A text box showing "0 days 00:04:15".

At the bottom of the dialog are three buttons: "Set Date/Time", "Refresh", and "Close [X]".

Table 4-12 NE System Time Dialog Description

Field	Description
Date / Time	
Local Date / Time	This indicates the current NE date and time.
Time Zone	
GMT	This indicates the time differences between the Greenwich Mean Time and the local time. Unit: hour
Up Time	
System Up Time	This indicates the period since the NE is rebooted last.
Function Button	
Set Date/Time	Click this button to apply the configured Local Date/Time.
Refresh	Click this button to refresh the Date/Time and Up Time information.
Close	Exit the NE System Time Dialog.



The date and time will be reset due to reboot system. However, the NE will synchronize its date and time with the configured time server's.

(Please refer to Section “Time Server Setting” of Chapter 4 for the setting of time server.

DNS Server Setting

The DNS (Domain Name System) server is used for the resolution of domain name. For example, a query for www.netcomm.com.au will receive a reply with the IP address of the web server of NetComm. Therefore the DNS Server is designed for the resolution of domain name. In other words, the DNS replies the corresponding IP address to the URL like the given example.

Follow the subsequent procedures to configure the DNS Server.

Click Configuration → NE Management → DNS Servers on **Main Menu** to open the **NE DNS Server Setting** Dialog as shown in Figure 4-13 and Table 4-13 depicts the related parameters.

Figure 4-13 DNS Server Setting Dialog

The screenshot shows a Windows-style dialog box titled "[192.168.192.1] NE DNS Server Setting". Inside, there's a group box labeled "DNS Server Information". It contains three labels: "The First Server", "The Second Server", and "The Third Server". Each label is followed by a text input field. The first field contains "168 . 95 . 1 . 1", the second contains "0 . 0 . 0 . 0", and the third contains "0 . 0 . 0 . 0". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Table 4-13 DNS Server Setting Dialog Description

Field	Description
DNS Server Information	
The First Server	This specifies the first DNS server IP address.
The Second Server	This specifies the second DNS server IP address.
The Third Server	This specifies the third DNS server IP address.

Time Server Setting

A time server is a server that reads the actual time from a reference clock and distributes this information to its clients using a computer network. The NE supports to synchronize its date and time with the configured time server's via the Simple Network Time Protocol (SNTP). Follow the subsequent procedures to configure the time servers.

- Step 1** Click Configuration → NE Management → Time Servers on **Main Menu** to open the **Time Server Status** Dialog as shown in Figure 4-14 and Table 4-14 depicts the related parameters.

Figure 4-14 NE Time Server Status Dialog

The screenshot shows the 'NE Time Server Status' dialog box. The title bar indicates the IP address [192.168.192.1]. The main area is titled 'Time Server Information'. It contains the following fields and controls:

- NE System Time:** A text field showing '2011-10-27 00:07:01' with an 'Adjust Time' button to its right.
- Network Timing Protocol:** A dropdown menu currently set to '<none>'.
- Update Period:** Two spinners for 'hour' (set to 12) and 'minute' (set to 0).
- Server List:** Three rows for 'The First Server', 'The Second Server', and 'The Third Server'. Each row has a text input field and a status field, all of which currently show 'not set'.
- Buttons:** At the bottom right are 'Refresh', 'Modify', and 'Close [X]' buttons.

Table 4-14 NE Time Server Status Dialog Description

Field	Description
Time Server Information	
NE System Time	This indicates the current NE system time.
Network Timing Protocol	This indicates the current network time protocol, SNTP or None.
Update Period	This indicates the time period between two consecutive synchronizations of the NE's local time with the time server.
The First Server	This indicates the first time server the NE tries to synchronize with.
The Second Server	This indicates the second time server the NE tries to synchronize with.
The Third Server	This indicates the third time server the NE tries to synchronize with.
Status	This indicates connection status between the NE and the time server.
Function Button	
Adjust Time	Click this button to enforce the NE to synchronize its local time with the time server immediately.
Refresh	Click this button to refresh this launched window.
Modify	Click this button to set the NE time servers.
Close	Exit the NE Time Server Status Dialog.

Step 2 Click '**Modify**' button to modify the Time Server information, as show in Figure 4-15 and Table 4-15 depicts the related parameters.

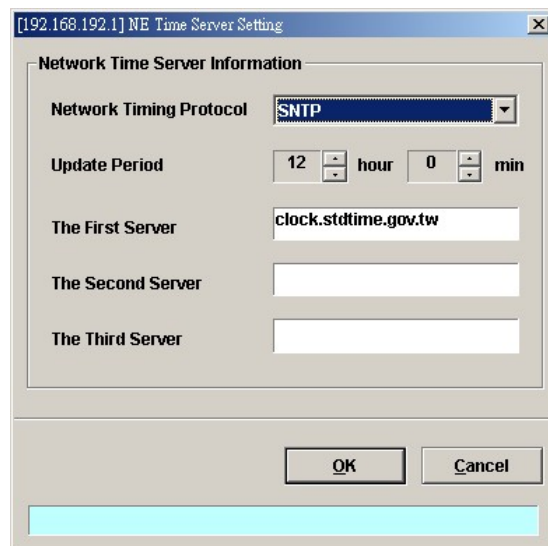
Figure 4-15 NE Time Server Setting Dialog

Table 4-15 NE Time Server Setting Dialog Description

Field	Description
Network Time Server Information	
Network Timing Protocol	This specifies the network timing protocol, either SNTP or None.
Update Period	This specifies the time period between two consecutive synchronizations of the NE's local time with the time server.
The First Server	This specifies the first time server the NE tries to synchronize with.
The Second Server	This specifies the second time server the NE tries to synchronize with.
The Third Server	This specifies the third time server the NE tries to synchronize with.



The NE will synchronize its local time with the first time server's time as a top priority. If the first time server fails to respond, the NE tries to synchronize its local time with the second and third time server's time in sequence.

Managing the NE Configuration

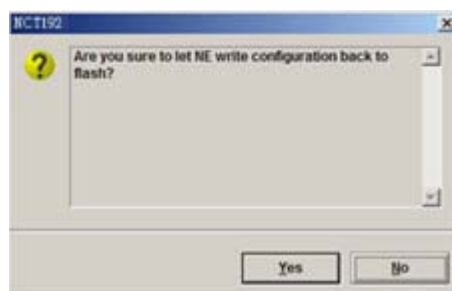
The modified configuration will be lost due to the rebooting of hardware without saving (storing).

Saving NE configuration to Flash

Follow the subsequent procedures to save your NE configuration to Flash.

Click Configuration → NE Management → Configuration Data → **Save** on **Main Menu** to open the **NE Write Flash Confirm** Dialog, or alternative select from the '**Rack**' tab view, point the mouse cursor on the NE object (NC slot), and then right click the mouse button to launch 'NE Management → Configuration Data' and select '**Save**' from this menu, as shown in Figure 4-16.

Figure 4-16 NE Write Flash Confirm Dialog



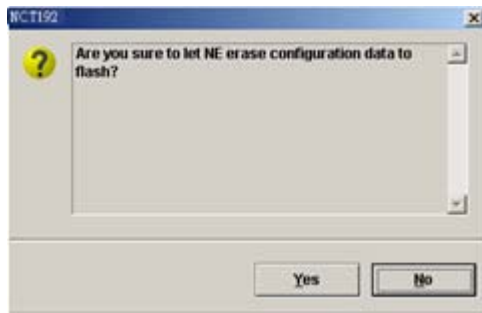
Erasing NE configuration from Flash

Follow the subsequent procedures to erase your NE configuration from Flash.

Click Configuration → NE Management → Configuration Data → **Erase** on **Main Menu** to open the **NE Erase Flash Confirm** Dialog, or alternative select from the '**Rack**' tab view, point the mouse cursor on the NE object (LC slot), and then right click the mouse button to launch 'NE

Management → Configuration Data' and select '**Erase**' from this menu, as shown in Figure 4-17.

Figure 4-17 NE Erase Flash Confirm Dialog



Chapter 5 Profile Management

A profile is a named list of configuration parameters with a value assigned to each parameter. By using a profile, the operator can configure the NE without to key in a lot of configuration parameters. However, whenever the operator modifies a profile, the modification will affect all ports using that profile.

This chapter describes the management of two kinds of profiles, data transport related profiles and alarm definition profile. The alarm definition profile defines the attributes of the report (alarm) of abnormality launched by the NE.

As to the data transport related profiles, they are

- xDSL Profile
- VLAN Profile

The xDSL Profile indicates the ADSL Profile and SHDSL Profile. It defines the attributes of the connection established via the xDSL subscriber loop. As to the VLAN Profile, it defines the attributes of services/applications applied to the xDSL subscriber.

Figure 5-1 and Table 5-1 help you to understand each profile and their interrelationship.

As shown in Figure 5-1, NE forwards traffic on 2 kinds of connections, unicast connection and multicast connection, on the Data Level. For the unicast connection, it carries all traffic (unicast and broadcast) except multicast traffic. The attributes of unicast connection are specified by the IP Traffic Profile. As for the multicast connection, its attributes are specified by the Multicast Channel Profile. Moreover, the NE also supports to restrict the subscriber to receive a set of specific Multicast Channels. Multicast Service Profile records the set of specific Multicast Channels.

Figure 5-1 Interrelationship of Data Transport Related Profiles

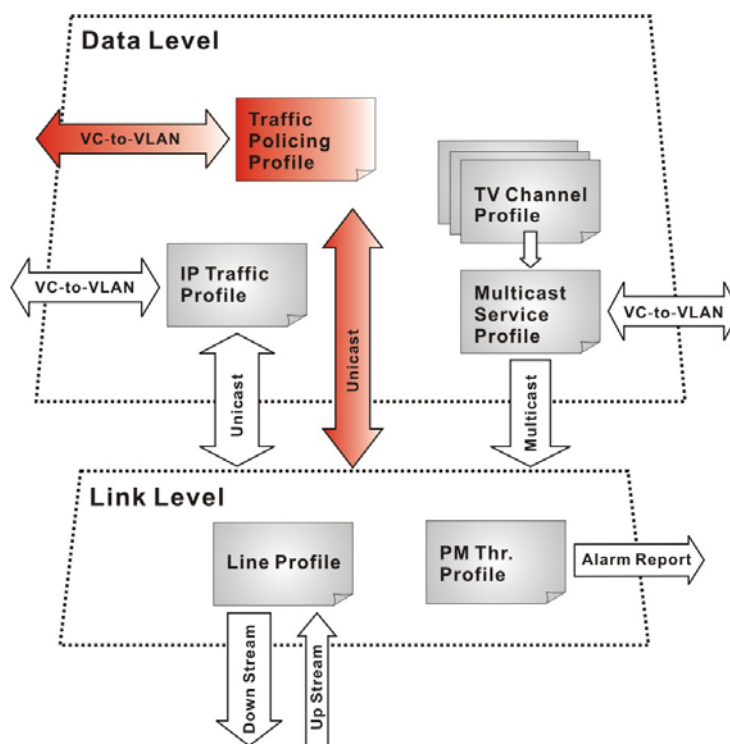


Table 5-1 Data Transport Related Profiles

Profile		Capacity	Level	Category	Description
XDSL Profile	Line Profile	60 sets	Link	Loop	Define the attributes of xDSL loop connection.
	PM Threshold Profile	60 sets	Link	Loop	Report the message if loop connection error across the threshold.
	Traffic Policing Profile (ADSL LC only)	60 sets	Data	User Data	Define the rule of traffic policing for user data.
VLAN Profile	IP Traffic Profile	60 sets	Data	Unicast	Define the traffic bandwidth of Unicast connection.
	Multicast Service Profile	60 sets	Data	Multicast	A set of service selected from menu list.
	TV Channel Profile	800 sets	Data	Multicast	A menu list of multicast channel, it also defines the traffic bandwidth of Multicast connection.



To make Traffic Policing Profile take effect, it needs to set IP Traffic Profile properly. Please refer to the NOTE under Table 5-9.



To make an xDSL line works normally, the IP Traffic Profile is essential. As to the Traffic Policing Profile, it is optional and is only applicable to ADSL LC.



A profile is a named list of configuration parameters with a value assigned to each parameter. When you delete a profile you will affect the change on all port or connection using that profile. If you want to change a single port or a subset of ports, you can create another profile with desired parameters, and then assign the new profile to the desired port.

This chapter contains the following sections:

- Configuring the xDSL Profile
- Configuring the VLAN Profile
- Configuring the Alarm Definition Profile

At first, the usage of **Function Button** in the **ADSL Profile List Dialog** is described as follows. Click Configuration → Profile → ADSL Profile on **Main Menu** to open the **ADSL Profile List Dialog**. Figure 5-2 indicates the position of the **Function Button** by red rectangle.

Figure 5-2 xDSL Profile List Dialog Function Button

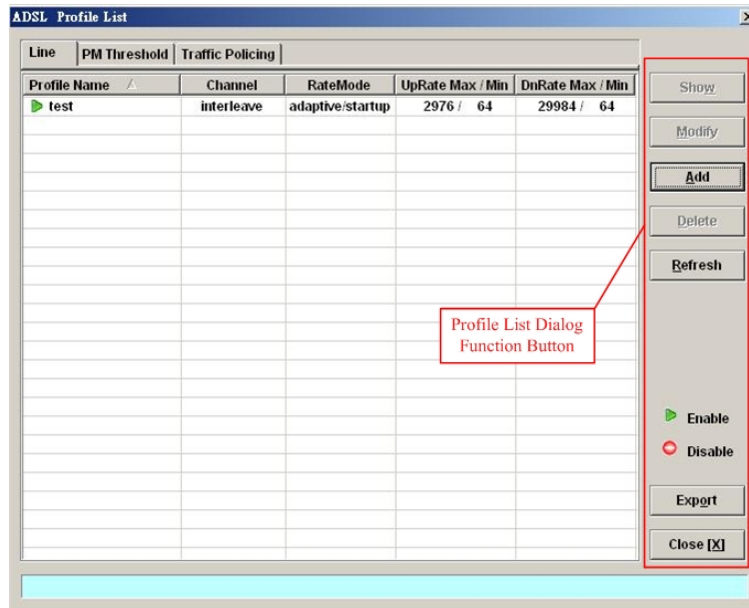


Table 5-2 xDSL Line Profile List Dialog Function Button

Field	Description
Show	Click this button to view the details of selected profile.
Modify	Click this button to modify the parameters of selected profile
Add	Click to add a new profile.
Delete	Click this button to delete the selected profile.
Refresh	Click to refresh the xDSL Profile List
Export	Click this button to save the contents of xDSL Profile List to the Personal Computer.
Close	Exit the xDSL Profile List Dialog.

Configuring the xDSL Profile

The xDSL profiles enable you to simplify the process to configure the different xDSL loops with the same loop/data connection attributes. For example, you may classify the subscribers to several categories like category of residential customers, category of small office customers, category of enterprise customers and so on. Each category of subscribers is with the same loop/data connection attributes. Different categories are with their specific attributes like the line speed and performance monitoring to secure their particular service quality. Once the profiles are created, you can easily assign the xDSL subscriber with the request xDSL loop attributes.

This section depicts the supported xDSL profiles

- ADSL Profile
- SHDSL Profile

ADSL Profile

Three types of profiles are relative to the ADSL loop, which are Line Profile, Traffic Policing Profile and PM Threshold Profile.



Once the ADSL connection profile is created, the operator can apply it to distinct ADSL line port by the “ADSL Port Modification Dialog” shown in Figure 6-2 for the related command.

Click Configuration → Profile → ADSL Profile on **Main Menu** to open the **ADSL Profile List** Dialog.

Line Profile

Click the **Line** tab in ADSL Profile List dialog to launch the **ADSL Profile List – Line Dialog** to configure the ADSL Line profile as shown in Figure 5-3.

Figure 5-3 ADSL Profile List – Line Dialog

Profile Name	Channel	RateMode	UpRate Max / Min	DnRate Max / Min
ADSL	fast	adaptive/startup	256 / 64	512 / 128
Adsl_test	interleave	adaptive/startup	512 / 64	1024 / 64
bank_pm	fast	adaptive/startup	2976 / 64	29984 / 64

Click ‘Add’ button to generate a line profile. Or select an existent profile and click ‘Modify’ to modify it. It is noted that each profile must have its unique profile name.

The line profile consists of the following groups of ADSL loop related parameters.

- Transmission Rate
- SNR margin
- PSD
- Power management
- INP

Transmission Rate

Click the **Transmission Rate** tab in **ADSL Line Profile Dialog** to launch the **ADSL Line Profile– Transmission Rate Dialog** as shown in Figure 5-4. Table 5-3 depicts the related parameters.

Figure 5-4 Add ADSL Line Profile– Transmission Rate Dialog
Table 5-3 Add Line Profile– Transmission Rate Dialog Description

Field	Description
Profile Information	
Profile Name	Enter to give a profile name
Channel Mode	
Interleave	Click to let the ADSL loop to be in the interleave mode. Interleave mode enhances the immunity to the impulse noise like lighting. However, its side effect is to introduce the transmission latency. Hence it is suitable for the time-insensitive data transmission, like file transfer. Its associated parameters are the 'Upstream/Downstream Max Delay'
Fast	Click to let the ADSL loop to be in the fast mode. Fast mode is suitable for the transmission of time-sensitive information such as audio.
Rate Mode	
Fixed	Click to let the ADSL loop to be of a fixed rate as specified by the 'Upstream/Downstream Min Rate'. In this mode, the NE will fail to establish the connection with ATU-R whenever it is not allowed in the physical loop environment. The failure may be due to the loop length, line quality, and so on.
Adaptive at Startup	Click to let the ADSL loop to be of the rate adapted in the range specified by the 'Upstream/Downstream Min/Max Rate'. In comparison with 'Adaptive at Run-time', the NE will re-try to establish a new lower-rate connection with the ATU-R whenever the NE or ATU-R detects 10 consecutive SESs (Severely Error Seconds) in this mode.
Adaptive at Run-time	Click to let the ADSL loop to be of the rate adapted in the range specified by the 'Upstream/Downstream Min/Max Rate'. In comparison with 'Adaptive at Startup', the NE will trigger the SRA (Seamless Rate Adaptation) process to change the line rates without losing the connection with ATU-R whenever the physical loop environment varies in this mode.

Table 5-3 Add Line Profile– Transmission Rate Dialog Description (Continued)

Field	Description
Upstream	
Min Rate	Choose the minimum rate for the ATU-R to transmits traffic
Max Rate	Choose the maximum rate for the ATU-R to transmits traffic
Max Delay	Choose the maximum interleaved delay in milliseconds. (interleave mode only) Interleaved delay applies only to the interleave channel and defines the mapping between subsequent input bytes at the inter-leaver input and their placement in the bit stream at the interleave output. Larger numbers provide greater separation between consecutive input bytes in the output bit stream, allowing for improved impulse noise immunity at the expense of payload latency.
Downstream	
Min Rate	Choose the minimum rate for the ATU-C to transmits traffic
Max Rate	Choose the maximum rate for the ATU-C to transmits traffic
Max Delay	Choose the maximum interleaved delay in milliseconds. (applied to the interleave mode only)



The associated parameters of the Rate Mode ‘Adaptive at Run-Time’ are as follows.
‘Upshift Noise Margin’, ‘Downshift Noise Margin’, ‘Upshift Time’ and ‘Downshift Time’



In the Rate Mode ‘Adaptive at Run-Time’, the NE will lose the connection with ATU-R if it fails to complete the SRA process to change the line rates

SNR Margin

Click the **SNR Margin tab** in **ADSL Line Profile Dialog** to launch the **ADSL Line Profile– SNR Margin Dialog** as shown in Figure 5-5. Table 5-4 depicts the related parameters.

Figure 5-5 Add ADSL Line Profile– SNR Margin Dialog

Table 5-4 Add Line Profile– SNR Margin Dialog Description

Field	Description
Upstream	
Downstream	
Max Margin	It specifies the maximum margin in 0.1 dB steps. Default value is 310.
Upshift	It specifies the up-shift margin in 0.1dB steps. Default value is 200
Target	It specifies the target margin in 0.1dB steps. Default value is 60.
Downshift	It specifies the downshift margin in 0.1 dB steps. Default value is 30
Min	It specifies the minimum margin in 0.1 dB steps. Default value is 0.
Upshift Time	It specifies the upshift time in sec. It defines the minimum time interval during which the upstream noise margin should stay above the Upshift SNR before the ATU-C triggers the SRA process to increase the line rate. Default value is 1000.Default value is 1000.
Downshift Time	It specifies the downshift time in sec. It defines the minimum time interval during which the upstream noise margin should stay above the Downshift SNR before the ATU-C triggers the SRA process to decrease the line rate. Default value is 1000.



‘Upshift Noise Margin’, ‘Downshift Noise Margin’, ‘Upshift Time’ and ‘Downshift Time’ are only applied to the Rate Mode ‘Adaptive at Run-Time’.



The following relationship holds when setting their value

Minimum Noise Margin ≤ Downshift Noise Margin ≤ Target Noise Margin ≤ Upshift Noise Margin ≤ Maximum Noise Margin.

PSD

Click the **PSD tab** in **ADSL Line Profile Dialog** to launch the **ADSL Line Profile– PSD Dialog** as shown in Figure 5-6. Table 5-5 depicts the related parameters.

Figure 5-6 Add ADSL Line Profile– PSD Dialog

Table 5-5 Add Line Profile – PSD Dialog Description

Field	Description
Upstream	
Downstream	
Nominal PSD	It specifies the discrepancy with respect to the ITU-T G.992.3-defined MAXNOMPSD value. Its unit is 0.1 dBm/Hz. And its allowed range is from 40 to -400.



It is noted that the MAXNOMPSD settings are different for the following three protocol groups.

- G.992.1 Annex A and B; G.992.2 Annex A and G; G.992.3 Annex A, B and J;
- G.992.5 Annex A, B and M
- G.992.3 Annex L

To ease the configuration, the Nominal PSD is defined to be the discrepancy with respect to the MAXNOMPSD..



The default upstream/downstream PSD spectrums in G.992.1 ADSL, G.992.3 ADSL2 and G.992.5 ADSL2+ are different. To simply the configuration effort, the upstream/downstream MAXNOMPSD here indicate the deviation from the default upstream and downstream PSD spectrums in G.992.x, respectively. Hence, it is recommended to set upstream/downstream MAXNOMPSD here as zero in normal case.



The relationship among “upstream MAXNOMPSD”, observed upstream SNR margin, observed ADSL line upstream rate and ADSL line reach.

- Higher “upstream MAXNOMPSD” results in either higher observed SNR margin or higher observed ADSL line rate or longer ADSL line reach.
- Higher “upstream MAXNOMPSD” also results in more severe Cross Talk.

Hence, for fixed ADSL reach, you will observe either high SNR margin or high ADSL line rate. When you do not need high SNR margin or high ADSL line rate, you can lower the “upstream MAXNOMPSD” to save power (save money).

The above description applies to the relationship among “downstream MAXNOMPSD”, observed downstream SNR margin, observed ADSL line downstream rate and ADSL line reach.

Power Management

In order to save power, G.992.3 and G.992.5 define the power management function. The operator can either configure the ADSL line Transmission (Tx) power be either manually or automatically managed.

The automatic power management function enables the ADSL line to automatically transfer from the L0 (full-on) state to the L2 (low power) state whenever the downstream net data rate is lower than expected. And it also enables the ADSL line to automatically transfer from the L2 state to the L0 state once the NE begins to drop the downstream data.



Concepts about the setting of automatic L0/L2 power management

- The default values are to let the ADSL line be always in the L0 state. If you want to save power, you can alter these values.
- Whenever the ADSL chip detects that the subscriber's data traffic is low on this ADSL line, and it meets the criterion constructed by the setting of "L2 State Min & Low Rate", "L2 state Max Rate", "L2 Low Rate Min Contiguous Time" and "L0 State Min Time to Start Monitoring". The ADSL chip will let the ADSL line enter L2 state to save power. (The ADSL chip will lower the PSD Spectrum to achieve this purpose)

Click the **Power Management** tab in **ADSL Line Profile Dialog** to launch the **ADSL Line Profile– Power Management Dialog** as shown in Figure 5-7. Table 5-6 depicts the related parameters.

Figure 5-7 Add ADSL Line Profile– Power Management Dialog

[192.168.192.1] ADSL Line Profile : Adsl_test

Profile Information

Profile Name: Adsl_test

Transmission Rate | **SNR Margin** | **PSD** | **Power Management** | **INP**

Management Mode

☐ Automatic

☒ Manual

Trigger Criteria of State Transition

L2 State Min & Low Rate: 32 Kbps

L2 State Max Rate: 29984 Kbps

L0 State Min Time to Start Monitoring: 900 sec

L2 State Low Rate Min Contiguous Time: 300 sec

CPE L3 State Request: ☒ Accept ☐ Reject

OK Cancel

Table 5-6 Add Line Profile – Power Management Dialog Description

Field	Description
Management Mode	
Automatic – This mode enables the ADSL line to automatically transfer from the L0 (full-on) state to the L2 (low power) state whenever the downstream net data rate is lower than expected. And it also enables the ADSL line to automatically transfer from the L2 state to the L0 state once the NE begins to drop the downstream data.	
Manual –This mode allows the operator to manually force the specific ADSL line to transfer from the L2 state to the L0 state, and vice versa.	
Trigger Criteria Of State Transition	
L2 State Min & Low Rate	It specifies the minimum rate (manual mode) or Lowest criteria (auto mode) of L2 state. (See the Note below) Default value is 32.
L2 State Max Rate	It specifies the maximum rate of L2 state. (See the Note below) Default value is 29984.
L0 State Min Time to Start Monitoring	It specifies the minimum time (seconds) the ADSL line must stay at the L0 state. During this time interval, the ADSL line is not allowed to transfer to the L2 state. It is the so-called L0-TIME as defined in ITU-T G.997.1. (See the Note below) Default value is 900.
L2 State Low Rate Min Contiguous Time	It specifies the contiguous time interval for which the downstream mean net data rate is below the 'L2 State Min & Low Rate' on a ADSL line. (See the Note below) Default value is 300.
CPE L3 State Request	It specifies whether the ADSL port accepts L3 command from CPE or not. Default value is "Accept".



In order to let the ADSL line avoid going into and out of L2 too often, the following L0↔L2 state transition criteria are adopted.

L0→L2:

- The ADSL line must stay at the L0 state for a period specified by 'L0 State Min Time to Start Monitoring' (i.e., the L0-TIME as defined in ITU-T G.997.1)
- After the L0-TIME, the NE begins to compute the mean net-data rate for a period of 'L2 State Low Rate Min Contiguous Time' on a ADSL line.
- The ADSL line transfers to the L2 state once the computed mean net-data rate is below the 'L2 State Min & Low Rate'.
- Once an ADSL line is at the L2 state, its downstream ADSL line rate is in the range from 'L2 State Min & Low Rate' to 'L2 State Max Rate'.

L2→L0:

- The ADSL line immediately transfers to the L0 state once the NE detects packet loss on the ADSL line in the down stream direction.

INP

The INP (Impulse Noise Protection) defines the minimum protection symbol time both for upstream and downstream on this ADSL subscriber.

Click the **INP** tab in **ADSL Line Profile Dialog** to launch the **ADSL Line Profile– INP Dialog** as shown in Figure 5-8. Table 5-7 depicts the related parameters.

Figure 5-8 Add ADSL Line Profile– INP Dialog

The screenshot shows a window titled "[192.168.192.1] ADSL Line Profile : Adsl_test". Inside, there's a "Profile Information" section with "Profile Name" set to "Adsl_test". Below this is a tabbed interface with tabs for "Transmission Rate", "SNR Margin", "PSD", "Power Management", and "INP". The "INP" tab is active, displaying two sections: "Upstream" and "Downstream". Each section has a "Minimum INP" label and a dropdown menu currently showing "0", with "(symbol time)" written below each dropdown. At the bottom right are "OK" and "Cancel" buttons.

Table 5-7 Add Line Profile – INP Dialog Description

Field	Description
Upstream	
Downstream	
Minimum INP	It specifies the impulse noise protection symbol time in {0, 1/2, 1, 2, 4, 8, 16}.

PM Threshold Profile

The PM threshold profile sets the threshold values for the performance parameters associated with the ADSL line. The NE will report the threshold-over trap (i.e. TCA, Threshold-Crossing Alarm) to the NCT192 when the specified performance threshold is over.

During the accumulation cycle, if the current value of a performance parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the system and sent to trap station. TCAs provide early detection of performance degradation. When a threshold is crossed, the ADSL line port continues to count the errors during a given accumulation period. If 0 is entered as the threshold value, the NE never sends the corresponding TCA.

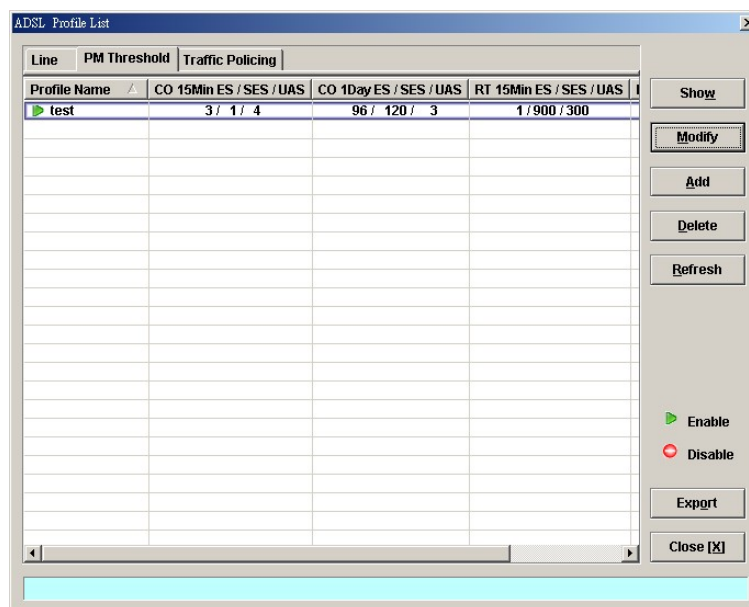
The NE supports to define the Near-End and Far-End thresholds of ES (Errored Seconds), SES (Severely Errored Seconds), and UAS (Unavailable Seconds) conditions in 15 minutes and 1 day interval. The definition of ES, SES and UAS are as follows.

- ES (Error Second)
ES corresponds to “ES-L” defined in ITU-T G.997.1 (2003 Edition)
ITU-T G.997.1 defines ES as a count of 1-second intervals with one or more CRC-8 anomalies summed over all received bearer channels, or one or more LOS defects, or one or more SEF defects, or one or more LPR defects.
- SES (Several Error Second)
SES corresponds to the “SES-L” defined in ITU-T G.997.1 (2003 Edition).
ITU-T G.997.1 defines ES as a count of 1-second intervals with 18 or more CRC-8 anomalies summed over all received bearer channels, or one or more LOS defects, or one or more SEF defects, or one or more LPR defects
- UAS (UnAvailable Second)
UAS corresponds to the “UAS-L” defined in ITU-T G.997.1 (2003 Edition).
ITU-T G.997.1 defines ES as a count of 1-second intervals for which the ADSL line is unavailable. The ADSL line becomes unavailable at the onset of 10 contiguous SES-Ls. The 10 SES-Ls are included in unavailable time. Once unavailable, the ADSL line becomes available at the onset of 10 contiguous seconds with no SES-Ls. The 10 seconds with no SES-Ls are excluded from unavailable time. Some parameter counts are inhibited during unavailability

Figure 5-9 shows ADSL PM threshold profiles accommodated in the system and allows adding a new profile or deleting the existing profile, by system (NE) unit.

Click the **PM Threshold** tab in **ADSL Profile List Dialog** to launch the **ADSL Line Profile – PM Threshold Dialog** as shown in Figure 5-9.

Figure 5-9 xDSL Profile List– PM Threshold Dialog



Click ‘Add’ button to generate a PM threshold profile, each profile must have its unique profile name. Or select an existent profile and click ‘Modify’ to modify it. Figure 5-10 shows **Add ADSL PM Threshold Profile Dialog**. Table 5-8 depicts the related parameters.

Figure 5-10 Add ADSL PM Threshold Profile Dialog
Table 5-8 Add PM Threshold Profile Field Description

Field	Description
15-Min / CO	
This field indicates the CO side errors. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes.	
1-Day / CO	
This field indicates the CO side errors. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 1 day.	
15-Min / RT	
This field indicates the RT side (CPE) errors. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes.	
1-Day / RT	
This field indicates the RT side (CPE) errors. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 1 day.	
ES	It specifies the Error second (0 ~ 900 sec)
SES	It specifies the Several Error Second (0 ~ 900 sec)
UAS	It specifies the unavailable Second (0 ~ 900 sec)

Traffic Policing Profile

The NE supports to prevent the subscriber to receive un-booked TV channel (multicast channel) by checking the received “IGMP join” packet with a preconfigured Multicast Service Profile. (A Multicast Service Profile consists of a number of Multicast Channel Profiles.) The subscriber is restricted to receive the TV channels (recorded in the Multicast Channel Profile).

Traffic policing is to monitor network traffic for conformity with the Service Level Agreement (SLA) between subscribers and ISP (or NSP).

According to the SLA, the edge network equipment (NE) either drops or marks subscriber’s out-of-profile traffic with designated DSCP values to enforce compliance with that SLA. The traffic policing profile serves to keep the rules per the SLA.

Once the traffic policing profile is created, the operator can apply it to distinct ADSL line

port by the by the “ADSL Port Modification Dialog” shown in Figure 6-2 for the related command.

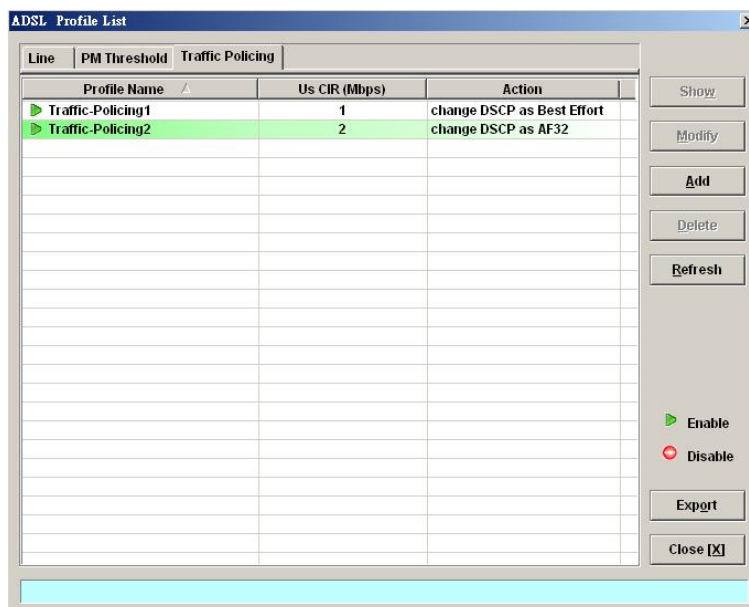
One example of application of traffic policing is as follows.

Suppose that the SLA defines that the subscriber can send upstream traffic at the rate up to 1.5Mbps. However, the NSP has the right to remark the DSCP value of traffic higher than 1Mbps when the network is in congestion. To accomplish this SLA, the operator can set the CIR to be 1Mbps, and set the out-of-profile action to remark the DSCP value to BE.

To verify the aforementioned setting, you can send 1.5Mega bit in one second in the upstream direction, then set the SmartBit (which connects to GE port to receive the upstream traffic) to capture the upstream traffic. And you will see that the DSCP of IP packet about 0.5Mbit is the value what you set “out-of-profile action”.

To set the traffic policing profile, click **Configuration → Profile → ADSL Profile → Traffic Policing Dialog**.

Figure 5-11 xDSL Profile List– Traffic Policing Dialog



Click ‘Add’ button to generate a Traffic Policing profile, each profile must have its unique profile name. Or select an existent profile and click ‘Modify’ to modify it. Figure 5-12 shows the **Add Traffic Policing Profile Dialog**. Table 5-9 depicts the related parameters.

Figure 5-12 Add Traffic Policing Profile Dialog

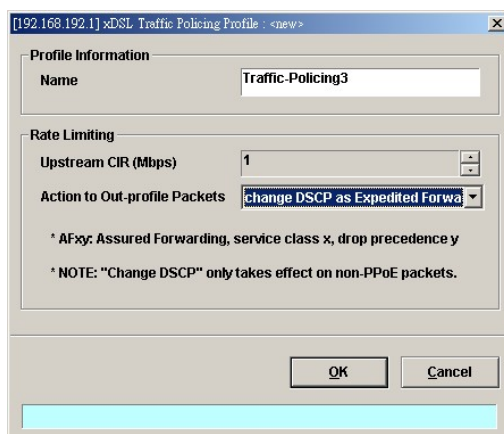


Table 5-9 Add Traffic Policing Profile Field Description

Field	Description
Profile Information	
Name	It specifies the name of traffic policing profile.
Rate Limiting	
Upstream CIR (Mbps)	It specifies the CIR (Commit Information Rate). Valid value is 0~2 Mbps.
Action to Out-profile Packets	It specifies the DSCP value to be set, drop packets or do nothing whenever the user's upstream traffic exceeds CIR.



The Service Type Control shall be enabled when Traffic Policing Profile is assign to xDSL subscribers (refer to Figure 6-2).



Please refer to Figure 6-13 for more details of Differentiated Service Code Point.

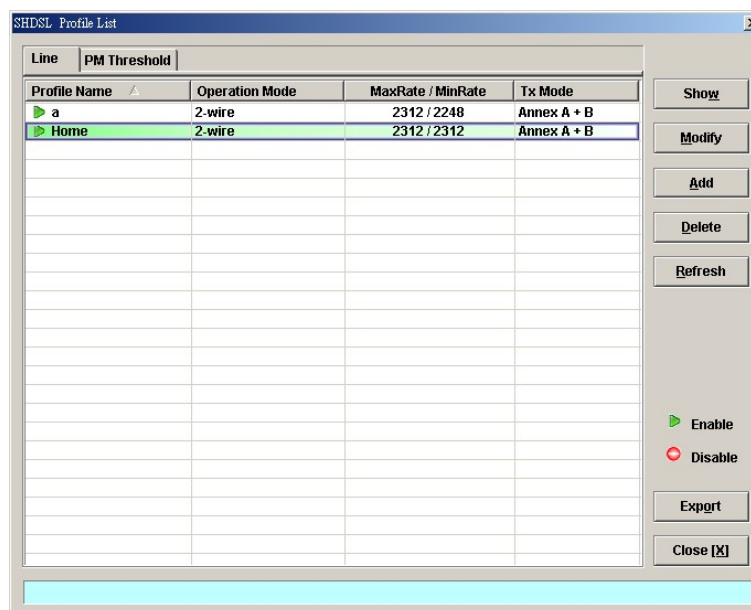
SHDSL Profile

Two types of profiles are related with the SHDSL loop, which are Line Profile and PM Threshold Profile.

Line Profile

The line profile contains parameter relate to the loop connection of SHDSL. Click the **Line** tab in **SHDSL Profile List Dialog** to launch the **SHDSL Profile List – Line Dialog** to configure the ADSL Line profile as shown in Figure 5-13.

Figure 5-13 SHDSL Profile List– Line Dialog



Click 'Add' button to generate a line profile. Or select an existent profile and click 'Modify' to modify it. It is noted that each profile must have its unique profile name.

The line profile consists of the following groups of SHDSL loop related parameters.

- Transmission Rate
- SNR margin
- Miscellaneous

Transmission Rate

Click the **Transmission Rate** tab in **SHDSL Line Profile Dialog** to launch the **SHDSL Line Profile– Transmission Rate Dialog** as shown in Figure 5-14. Table 5-10 depicts the related parameters.

Figure 5-14 Add SHDSL Line Profile– Transmission Rate Dialog

Table 5-10 Add SHDSL Line Profile– Transmission Rate Dialog Description

Field	Description
Profile Information	
Profile Name	Enter to give a profile name
Rate Mode	
Fixed	Click to let the SHDSL loop to be of a fixed rate as specified by the 'Min Rate'. In this mode, the NE will fail to establish the connection with STU-R whenever it is not allowed in the physical loop environment. The failure may be due to the loop length, line quality, and so on.
Adaptive at Startup	Click to let the SHDSL loop to be of the rate adapted in the range specified by the 'Min/Max Rate'.
Rate Limit	
Min Rate	Choose your minimum rate.
Max Rate	Choose your maximum rate.

SNR Margin

Click the **SNR Margin** tab in **SHDSL Line Profile Dialog** to launch the **SHDSL Line Profile–SNR Margin Dialog** as shown in Figure 5-15. Table 5-11 depicts the related parameters.

Figure 5-15 Add SHDSL Line Profile– SNR Margin Dialog

[192.168.192.1] SHDSL Line Profile : Home

Profile Information

Profile Name: Home

Transmission Rate | SNR Margin | Miscellaneous

Upstream

☒ Current Target Margin: 6 dB

☐ Worst Target Margin: 6 dB

Downstream

☒ Current Target Margin: 6 dB

☐ Worst Target Margin: 6 dB

OK Cancel

Table 5-11 Add SHDSL Line Profile - SNR Margin Dialog Description

Field	Description
Upstream / Downstream	
Current Target Margin	It specifies the current target margin. Default value is 6.
Worst Target Margin	It specifies the worst target margin. Default value is 6.

Miscellaneous

Click the **Miscellaneous** tab in **SHDSL Line Profile Dialog** to launch the **SHDSL Line Profile–Miscellaneous Dialog** as shown in Figure 5-16. Table 5-12 depicts the related parameters.

Figure 5-16 Add SHDSL Line Profile– Miscellaneous Dialog

[192.168.192.1] SHDSL Line Profile : Home

Profile Information

Profile Name: Home

Transmission Rate | SNR Margin | Miscellaneous

Miscellaneous Parameters

PSD Mask: ☒ Symmetric ☐ Asymmetric

Tx Mode: Annex ☐ A ☐ B ☒ A + B

Line Probe: ☒ Enable ☐ Disable

OK Cancel

Table 5-12 Add SHDSL Line Profile– Miscellaneous Dialog Description

Field	Description
Miscellaneous Parameters	
PSD Mask	It specifies the setting of PSD Mask to be symmetric or asymmetric
Tx Mode	It specifies the setting of Tx mode. A: Indicates the ITU-T G.991.2 Annex A B: Indicates the ITU-T G.991.2 Annex B A+B: Compatible with ITU-T G.991.2 Annex A and Annex B.
Line Probe	Enable or disable the line probe state before training with STU-R. Enable: To make the 'line rate limit' up to 2312Kbps. Disable: To make the 'line rate limit' up to 1.5Mbps.

PM Threshold Profile

The PM threshold profile sets the threshold values for the performance parameters associated with the SHDSL line. The NE will report the threshold-over trap (i.e. TCA, Threshold-Crossing Alarm) to the NCT192 when the specified performance threshold is over.

During the accumulation cycle, if the current value of a performance parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the system and sent to trap station. TCAs provide early detection of performance degradation. When a threshold is crossed, the SHDSL line port continues to count the errors during a given accumulation period. If 0 is entered as the threshold value, the NE never sends the corresponding TCA.

The NE supports to define the Near-End and Far-End thresholds of ES (Errored Seconds), SES (Severely Errored Seconds), and UAS (Unavailable Seconds) conditions in 15 minutes and 1 day interval. The definition of ES, SES and UAS are as follows.

- ES (Error Second)
ES corresponds to “ES-L” defined in ITU-T G.997.1 (2003 Edition)
ITU-T G.997.1 defines ES as a count of 1-second intervals with one or more CRC-8 anomalies summed over all received bearer channels, or one or more LOS defects, or one or more SEF defects, or one or more LPR defects.
- SES (Several Error Second)
SES corresponds to the “SES-L” defined in ITU-T G.997.1 (2003 Edition).
ITU-T G.997.1 defines ES as a count of 1-second intervals with 18 or more CRC-8 anomalies summed over all received bearer channels, or one or more LOS defects, or one or more SEF defects, or one or more LPR defects
- UAS (UnAvailable Second)
UAS corresponds to the “UAS-L” defined in ITU-T G.997.1 (2003 Edition). ITU-T G.997.1 defines ES as a count of 1-second intervals for which the SHDSL line is unavailable. The SHDSL line becomes unavailable at the onset of 10 contiguous SES-Ls. The 10 SES-Ls are included in unavailable time. Once unavailable, the SHDSL line becomes available at the onset of 10 contiguous seconds with no SES-Ls. The 10 seconds with no SES-Ls are excluded from unavailable time. Some parameter counts are inhibited during unavailability.

Figure 5-17 lists SHDSL PM threshold profiles accommodated in the system and allows adding a new profile or deleting the existing profile, by system (NE) unit.

Click the **PM Threshold tab** to launch the **PM Threshold Dialog** as shown in Figure 5-17.

Table 5-13 Add SHDSL PM Threshold Profile Dialog Description

Field	Description
CO SNR Margin and Loop Attenuation Threshold	
This field indicates the minimum SNR margin and maximum loop attenuation. When the minimum SNR margin is set to 10, if the current SNR margin is below 10 dB, a trap (alarm) occurs. When the maximum loop attenuation is set to 100, if the current loop attenuation exceeds 100 dB, a trap (alarm) occurs.	
CO 15-Min PM High-Threshold	
This field indicates the CO side errors. When the threshold is set to 10, if the count of specific errors exceeds 10 seconds for the last error accumulated, a trap (alarm) occurs.	
ES	It specifies the Error second (0 ~ 900 sec)
SES	It specifies the Several Error Second (0 ~ 900 sec)
UAS	It specifies the unavailable Second (0 ~ 900 sec)
LOSWs	It specifies the Loss of Synchronization Word Second (0 ~ 900 sec)
CRC Anomalies	It specifies the count of anomaly of Cyclic Redundancy Check (1 ~ 44100)

Configuring the VLAN Profile

VLAN Profile contains three categories of profiles.

- IP Traffic Profile
- TV Channel Profile
- Multicast Service Profile

As shown in Figure 5-1, NE forwards traffic on 2 kinds of connections, unicast connection and multicast connection, on the Data Level. For the unicast connection, it carries all traffic (unicast and broadcast) except multicast traffic. The attributes of unicast connection are specified by the IP Traffic Profile. As for the multicast connection, the NE supports to prevent the subscriber to receive un-booked TV channel (multicast channel) by checking the received “IGMP join” packet with a preconfigured Multicast Service Profile. Here, a Multicast Service Profile represents a set of Multicast (TV) Channel Profiles. Each Multicast (TV) Channel Profile describes the attributes of a multicast stream (TV channel). In other words, the subscriber is restricted to receive the TV channels described recorded in the Multicast Service Profile.

Click Configuration → Profile → VLAN Profile on **Main Menu** to open the **VLAN Profile List Dialog**.

IP Traffic Profile

The IP traffic profile is design to specify the traffic attributes of the PVC on the ADSL line. The operator can create the IP Traffic Profile according to the Service Level Agreement (SLA) and apply it to the corresponding VC-to-VLAN on demand. (see Chapter 7 VC-to-VLAN Connection).

Similar to the traffic policing profile, the IP traffic profile serves to keep the rules to enforce compliance with that SLA. (Please refer to Section “ADSL Profile” of Chapter 5 for the description of traffic policing)

However, it is noted that the scope of traffic policing profile is to police the traffic on a whole ADSL line. As to the IP traffic profile, its scope of is to police the traffic on a PVC in an ADSL line.

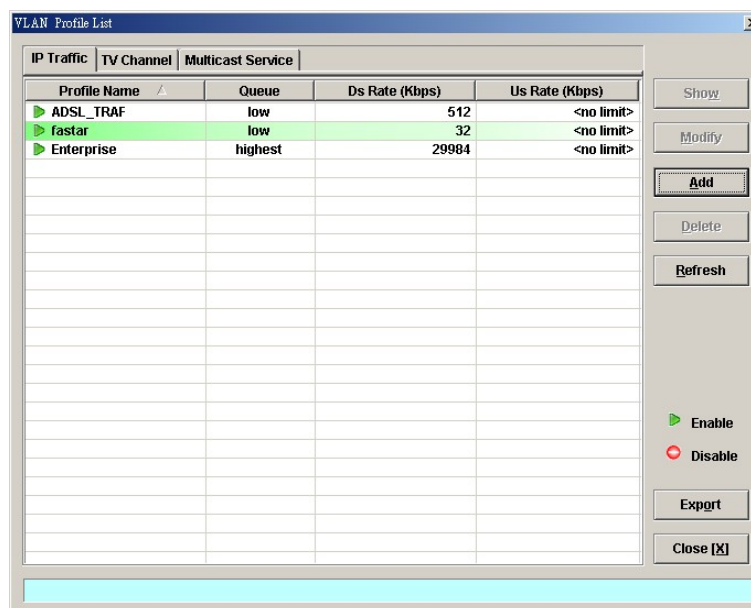
The operator can create the IP Traffic Profile according to the SLA and apply it to the corresponding VC-to-VLAN on demand.

By configures IP Traffic Profile, the following traffic attributions of a PVC is specified.

- The maximum upstream/downstream net-data rate is allowed.
The system drops upstream/downstream packets whenever it exceeds the corresponding specified rate
- The downstream priority of the PVC
The system forwards the downstream packets in a differentiated manner. That is, the system only forwards the traffic on PVC of lower priority whenever either one of the following conditions happened:
 - There is no traffic on PVC of higher priority to be forwarded.
 - The volume of traffic on PVC of higher priority exceeds the specified downstream net-data rate in a unit time.
- The filtering of the downstream broadcasts traffic

Click the **IP Traffic** tab in **VLAN Profile List Dialog** to launch the **VLAN Profile List-IP Traffic Dialog** as shown in Figure 5-19.

Figure 5-19 VLAN Profile List- IP Traffic Dialog



Click 'Add' button to generate an IP traffic profile, each profile must have its unique profile name. Or select an existent profile and click 'Modify' to modify it. Figure 5-20 shows **Add xDSL IP Traffic Profile Dialog**. Table 5-14 depicts the related parameters.

Figure 5-20 Add xDSL IP Traffic Profile Dialog
Table 5-14 Add xDSL IP Traffic Profile Dialog Description

Field	Description
Profile Information	
Name	Enter the name of traffic profile.
Line Board IP CoS Setting	
Downstream Priority Queue (Kbps)	It specifies the downstream priority queue. Valid values are “Low”, “Medium”, “High” and “Highest”.
Downstream Rate (Kbps)	It specifies the maximum allowed downstream net-data rate. The drops drop packets whenever the downstream traffic exceeds the specified rate.
Upstream Rate (Kbps)	It specifies the maximum allowed upstream net-data rate. The drops drop packets whenever the user’s upstream traffic exceeds the specified rate. Valid values are “no limit”, “32”, “64”, “128”, “256”, “384”, “512”, “768”
Broadcast Control	
Downstream Broadcast	This indicates the rule (forward or drop) for downstream broadcast traffic.

TV Channel Profile

The TV channel profile sets value of multicast group IP and the associated downstream bandwidth resource, it is a menu list of the TV channel (multicast group) provided by the Content Service Provider (CSP) or Application Service Provider (ASP).

Click the **TV Channel** tab in **VLAN Profile List Dialog** to launch the **VLAN Profile List–TV Channel Dialog** as shown in Figure 5-21.

Figure 5-21 VLAN Profile List– TV Channel Dialog

ID	Profile Name	TV Channel IP Address	Queue	Ds Rate(Kbps)
1	HBO	224.0.1.1	highest	29984
2	ESPN	224.0.1.2	high	29984
3	CNN	224.0.1.3	medium	29984

Click 'Add' button to generate a TV channel profile, each profile must have its unique profile name. Or select an existent profile and click 'Modify' to modify it. Figure 5-22 shows **Add xDSL TV Channel Profile Dialog**. Table 5-15 depicts the related parameters.

Figure 5-22 Add xDSL TV Channel Profile Dialog

Profile Information

Profile ID: 1

Name: BBC

TV Channel IP Address: 224.0.1.0

IP CoS Settings

Priority Queue: low

Downstream Rate (Kbps): 29984

OK Cancel

Table 5-15 Add xDSL TV Channel Profile Dialog Description

Field	Description
Profile Information	
Profile ID	It specifies the TV channel ID
Name	Enter the TV channel name
TV Channel IP Address	It specifies the IP address of TV channel (multicast group IP)
IP CoS Settings	
Priority Queue	This specifies the priority queue of TV Channel address. Valid values are “Low”, “Medium”, “High” and “Highest”.
Downstream Rate (Kbps)	It specifies the maximum allowed downstream net-data rate. The drops drop packets whenever the downstream traffic exceeds the specified rate.

Figure 5-24 Add xDSL Multicast Service Profile Dialog

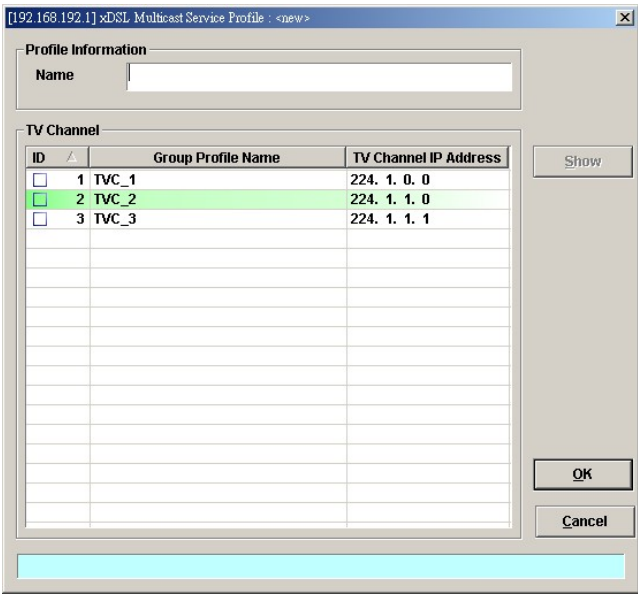


Table 5-16 Add Multicast Service Profile Dialog Description

Field	Description
Profile Information	
Name	Enter the multicast service profile name.
TV Channel	
ID	The serial number for group profile.
Group Profile Name	It specifies the group profile name
TV Channel IP Address	It specifies the multicast IP address
Show	Click this button to view the detail information from List Table.

Configuring the Alarm Definition Profile

The alarm definition profile allows you to define the rule of alarm element in system. Through this profile, you are able to change the severity of individual alarm element and decide to report it or not. Alarm element is specified in the class of module or port. Different types of module may present different alarm element. Different types of port may also present different alarm element. Please refer to Appendix B for the detailed description of the defined alarms and their default severity.

- Step 1

Click Configuration → Profile → Alarm Definition on **Main Menu** to open the **Alarm Definition List** Dialog as shown in Figure 5-25. Table 5-17 depicts the related parameters.

Figure 5-25 Alarm Definition List Dialog

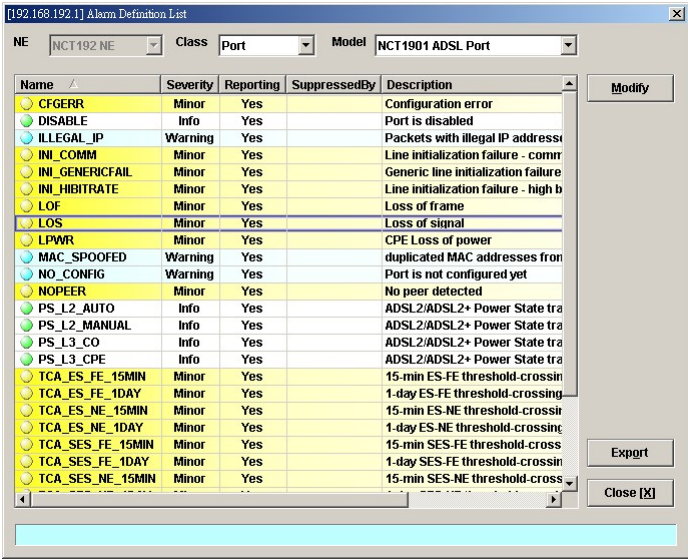


Table 5-17 Alarm Definition List Dialog Description

Field	Description
List Table	
Name	It specifies the alarm name.
Severity	It specifies the alarm severity.
Reporting	It specifies the reporting status.
Suppressed By	It specifies the rule of alarm suppression.
Description	It specifies the alarm description.
Top Combo-box	
NE	This indicates the current NE model.
Class	Use this combo-box to select the alarm class, shelf, module or port.
Model	Use this combo-box to select the card module or port module.
Function Button	
Modify	Select the item from List Table to modify.
Export	Click this button to save the contents of Alarm Definition List to the Personal Computer.
Close	Exit the Alarm Definition List Dialog.

Step 2 Click ‘Modify’ button to modify the Alarm Definition. Figure 5-26 shows **Modify Alarm Definition Dialog**, and Table 5-18 depicts the related parameters.

Figure 5-26 Modify Alarm Definition Dialog

Table 5-18 Modify Alarm Definition Dialog Description

Field	Description
Alarm Information	
Model	It specifies current module name under modifying.
Alarm Name	It specifies the alarm name.
Description	This describes the current selected alarm.
Alarm Severity	Check the radio button to set the alarm severity of the specified alarm.
Alarm Reporting	Enable or disable reporting of the specified alarm.
Alarm Suppression (Suppressed by)	
Name	Check the check box to choose which the specified alarm to be suppressed by.
Description	This describes the alarm's meaning.



The alarm suppression (suppressed by) allows you to mask specific alarms when there are sequences occurred at the same time. For example, let the LOF (Loss of Frame) be configured to be suppressed by the LOS (Loss of Signal), the LOF will not be display on the screen but only LOS whenever the corresponding ADSL loop is cut.

Chapter 6 Interface Port Management

This chapter depicts the management of subscriber interfaces and GE network interfaces. This chapter contains the following sections.

- xDSL Line Interface Management
- GE Network Interface Management
- Cascaded NE Management

xDSL Line Interface Management

This section helps you to attach the profile to the xDSL line interfaces. The function buttons of xDSL Port List dialog provides shortcut of relative port setting. As the ADSL and SHDSL configuration are similar and hence illustrated together in this section.

- Step 1** Click Configuration → xDSL → ADSL Port Setting on **Main Menu** to open the **ADSL Port List** Dialog as shown in Figure 6-1. Table 6-1 depicts the related parameters.
- Or
- Click Configuration → xDSL → SHDSL Port Setting on **Main Menu** to open the **SHDSL Port List** Dialog. Table 6-1 depicts the related parameters.

Figure 6-1 ADSL Port List Dialog

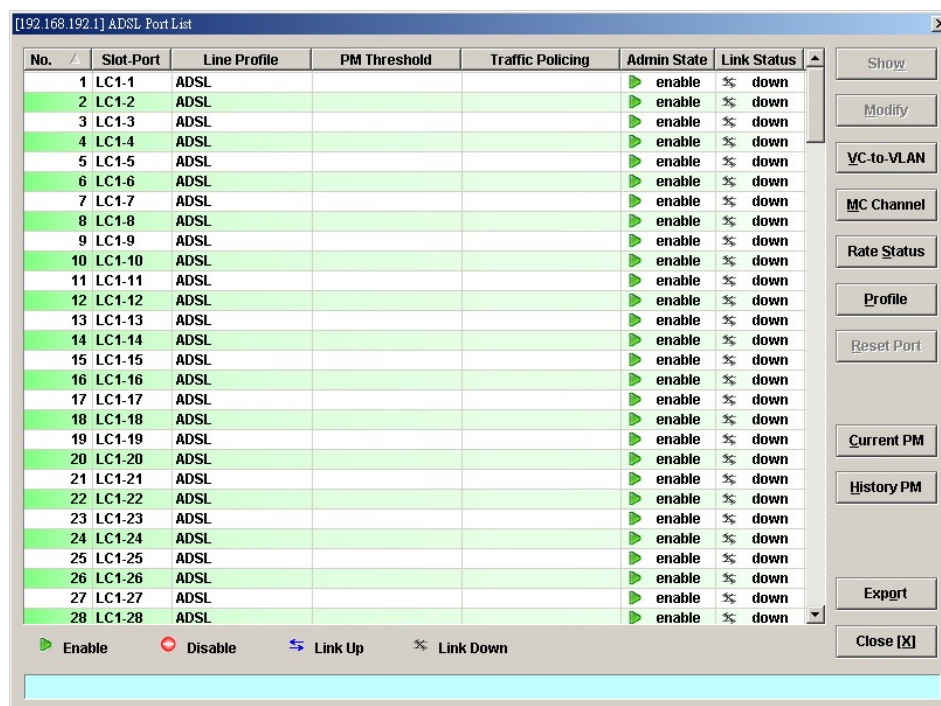


Table 6-1 xDSL Port List Dialog Description

Field	Description
List Table	
No.	This specifies the serial number of entry of List Table.
Slot-Port	This specifies the location of ADSL port
Line Profile	This specifies the line profile.
PM Threshold	This specifies the PM threshold profile.
Traffic Policing	This specifies the Traffic Policing profile. [Only for the ADSL Port List Dialog]
Admin State	This specifies the administrative status (enable or disable)
Link Status	It specifies the link connection status.
Function Button	
Show	Click this button to show.
Modify	Click this button to modify.
VC-to-VLAN	Click this button to configure the VC-to-VLAN parameters
MC Channel	Click this button to configure the multicast channel related parameters. [Only for the ADSL Port List Dialog]
Rate Status	Click this button to monitor the connection rate status.
Profile	Click this button to arrange the profile setting.
Reset Port	Click this button to reset port
Current PM	Click this button to view the current performance
History PM	Click this button to view the historical performance
Export	Click this button to save the contents of ADSL Port List to the Personal Computer.
Close	Exit the ADSL Port List Dialog .

Step 2 Select an ADSL port and click 'Modify' button to modify the ADSL port. Figure 6-2 shows **ADSL Port Modification Dialog**. Table 6-2 depicts the related parameters.

Figure 6-2 ADSL Port Modification Dialog

The screenshot shows the 'ADSL Port Modification Dialog' window. The title bar indicates the IP address '[192.168.192.1]' and the port type 'ADSL Port'. The main content area is divided into sections. The 'ADSL Port' section has a text field containing 'LC1-11'. The 'Administrative State' section has two radio buttons: 'Enable' (which is selected) and 'Disable'. The 'ADSL Profiles' section contains three dropdown menus: 'Line Profile' (set to 'ADSL'), 'PM Threshold' (set to '<none>'), and 'Traffic Policing' (set to '<none>'). Each dropdown menu has a 'Show' button next to it. Below these is a 'Service Type Control' field set to 'disabled'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Table 6-2 ADSL Port Modification Dialog Description

Field	Description
ADSL Port	This indicates the current ADSL Port under modification.
Administrative State	Enable or disable the specified ADSL port.
ADSL Profiles	
Line Profile	Use this combo-box to select an existent ADSL line profile.
PM Threshold	Use this combo-box to select an existent PM Threshold profile.
Traffic Policing	Use this combo-box to select an existent Traffic Policing profile.
Service Type Control	This indicates the state of Service Type Control (STC) of the selected ADSL line card.
Function Button	
OK	Press this button to commit setting.
Cancel	Press this button to cancel setting.



Service Type Control (STC) only takes effect after the applied line card is reset.



To make the applied Traffic Policing Profile take effect, Service Type Control (STC) must be enabled.

For the SHDSL ports, follow the subsequent procedures.

Step 3 Select an SHDSL port and click 'Modify' button to modify the SHDSL port. Figure 6-3 shows **SHDSL Port Modification Dialog**. Table 6-3 depicts the related parameters.

Figure 6-3 SHDSL Port Modification Dialog

Table 6-3 SHDSL Port Modification Dialog Description

Field	Description
SHDSL Port	This indicates the current SHDSL Port which is under modifying.
Administrative State	Enable or disable the specified SHDSL port.
SHDSL Profiles	
Line Profile	Use this combo-box to select an existent SHDSL line profile.
PM Threshold	Use this combo-box to select an existent PM Threshold profile.
Function Button	
OK	Press this button to commit setting.
Cancel	Press this button to cancel setting.



In comparison with the **ADSL Port List** Dialog, the **SHDSL Port List** Dialog does not support the following function

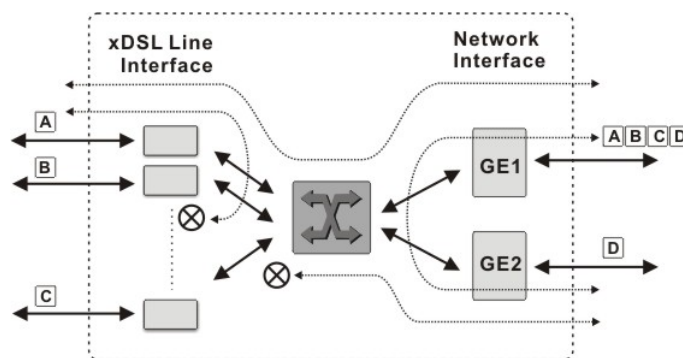
- Traffic Policing
- Service Type Control

GE Network Interface Management

There are two GE network interfaces, GE1 and GE2, for NCT192 IP-DSLAM. By default, GE1 is stated as the uplink GE port. GE2 is stated as the subtended GE port, and it connects to other equipment and forward traffics to GE1 if none of LACP or RSTP is enabled.

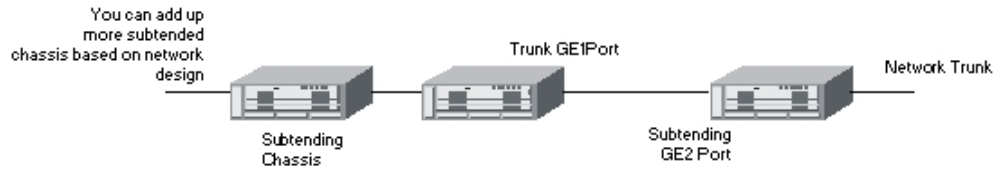
Figure 6-4 shows the packet forwarding diagram. As can be seen, the so-called “Port Isolation” indicates that all xDSL users can not communicate with each other. That is, all traffic from the xDSL line interface is forwarded to the GE1 interface. In the mean time, once the GE2 is configured as a subtended port, all the ingress traffic of GE2 is restricted to be forwarded to GE1.

Figure 6-4 GE Network Interface Packet Forward Illustrate



In some network deployment environment, it is desired to connect several IP-DSLAMs to share a single uplink to the access network as shown in Figure 6-5. As can be seen in Figure 6-5, three NCT192 IP-DSLAMs are connected via their GE ports to each other in a Daisy-Chain topology. The left-most NE connects to the access network (where the Internet is behind) via its GE1 port (uplink GE port). It also connects to the middle NE via its GE2 port (subtending GE port).

Figure 6-5 Illustration of 3 NCT192 IP-DSLAMs are connected in a Daisy-Chain topology



Follow the subsequent procedures to configure the trunk port related parameters.

- Step 1** Point mouse pointer at GE port object, click mouse right button Trunk → Port Setting on launched **Menu** to open the **Trunk Port List** Dialog as shown in Figure 6-6 and Table 6-4 depicts the related parameters.

Figure 6-6 Trunk Port Dialog

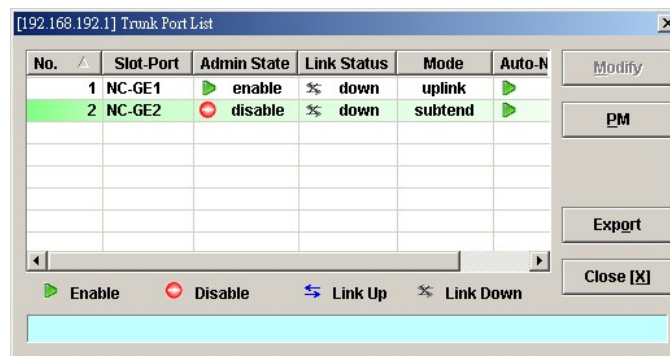


Table 6-4 Trunk Port Dialog Description

Field	Description
Trunk Port List Table	
No.	This indicates the serial number of entry of the List Table.
Slot-Port	This indicates the location of trunk GE port.
Admin State	This indicates the administrative state of GE port.
Link Status	This indicates the operational state of GE port.
Mode	This indicates the mode of GE port, be either an uplink port or a subtended port.
Auto Negotiation	This indicates the auto negotiation status of GE port.
Function Button	
Modify	Click this button to modify.
PM	Click this button to show GE port's performance statistics.
Export	Click this button to save the contents of Trunk Port List to the Personal Computer.
Close	Exit the Trunk Port List Dialog.

- Step 2** Click 'Modify' button to modify the trunk port. Figure 6-7 shows the **Trunk Port Configuration Dialog**, and Table 6-5 depicts the related parameters.

Figure 6-7 Trunk Port Configuration Dialog


The dialog box is titled "[192.168.192.1] Trunk Port". It contains four sections: "Trunk Port" with a text field containing "NC-GE1"; "Administrative State" with radio buttons for "Enable" (selected) and "Disable"; "Port Mode" with radio buttons for "Uplink" (selected) and "Subtend"; and "Auto-Negotiation" with radio buttons for "Enable" (selected) and "Disable". At the bottom are "OK" and "Cancel" buttons, and a light blue status bar.

Table 6-5 Trunk Port Configuration Dialog Description

Field	Description
Trunk Port	This indicates the GE port under configuring.
Administrative State	Enable or disable the specified GE port.
Port Mode	Setting the GE port to uplink mode or subtended mode. Subtended mode is only available on GE2, GE1 is always the uplink port.
Auto-Negotiation	Enable or disable the auto-negotiation mode of the specified GE port.

Link Aggregation (Static / Dynamic)

Link aggregation (LA) is to aggregate the 2 GE ports to form a single logical GE-channel to provide higher uplink bandwidth. This NE supports both static link aggregation and LACP (IEEE802.3ad, Link Aggregation Control Protocol). Figure 6-8 shows a typical GE-channel configuration.

Static link aggregation

In this mode, the NE forces to bundle GE1 and GE2 ports to form a single logical GE-channel without negotiating with its peer L2/L3 switch/router. For the traffic to be forwarded via the GE-channel as depicted in Figure 6-8, the NE will distribute the traffic on the GE1 and GE2 ports.



When the NE is configured to operate in the static LA mode, its peer L2/L3 switch/router needs to be configured in the same mode. Otherwise, the network may malfunction.

Dynamic link aggregation (LACP)

In this mode, the GE1 and GE2 ports are to form a single logical GE-channel by the LACP negotiating with its peer L2/L3 switch/router. By using the LACP, the NE learns the capability of its LACP peer. It then groups similarly configured ports into a single logical link (GE-channel). Once the GE-channel is built at the end of LACP negotiation, the NE will forward traffic via the GE-channel by distributing the traffic on the “member port(s)” of GE-channel as depicted in Figure 6-8. Here, the “member port(s)” indicate GE1, GE2 or both GE ports of the NE.

In the LACP, two modes, active and passive modes, are defined for the LACP engine to decide to actively or passively negotiate with its LACP peer for the physical port in interest.

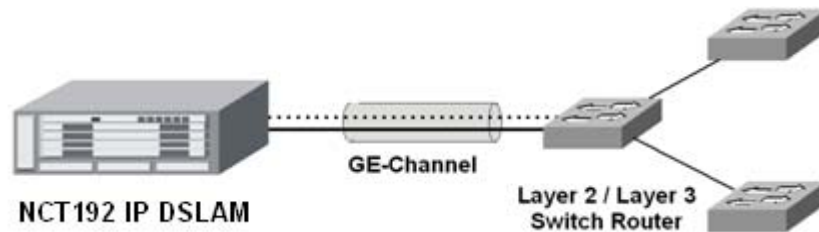
- **Active mode**

In this mode, The NE is willing to initiate the LACP negotiation procedure on the specified group and sends out an LACP packet voluntarily. The aggregation link will be formed if the other end is running in LACP active or passive mode.

- **Passive mode**

In this mode, The NE does not initiate LACP negotiation procedure on the specified group voluntarily, but waits for its LACP peer (in active state) initiates negotiation. The NE will form the aggregation link with its peer at the end of the negotiation procedure.

Figure 6-8 Typical GE-Channel Configuration



A LACP enabled switch/router needs to assign its “System ID”. The “System ID” is of 8 bytes which consists of 2 parts:

SystemPriority: SystemMacAddress

During the LACP negotiation process, the LACP enabled device of lowest System ID has the privilege to determine the configuration of aggregated ports. Its peer will follow it.

Follow the subsequent procedures to configure the related parameters.

Click Configuration → Trunk → Link Aggregation on **Main Menu** to open the **Link Aggregation Setting Dialog** as shown in Figure 6-9. Table 6-6 depicts the related parameters.

Figure 6-9 Link Aggregation Setting Dialog

The screenshot shows the 'Link Aggregation Setting' dialog box for the IP address 192.168.192.1. It contains the following sections:

- Link Aggregation Type:** Radio buttons for LACP, Static, and Disable. 'Disable' is selected.
- LACP Settings:**
 - System Priority:** A numeric field set to 32768.
 - Group 1, Group 2, Port GE1, Port GE2:** A table with four columns for selecting aggregation groups and ports.
 - Activity:** Radio buttons for Active and Passive. 'Passive' is selected.
 - Timeout:** Radio buttons for Long and Short. 'Long' is selected.
- Buttons:** OK and Cancel buttons at the bottom right.

Table 6-6 Link Aggregation Setting Dialog Description

Field	Description
Link Aggregation Type	
LACP	Set link aggregation type to “LACP” for GE ports.
Static	Set link aggregation type to “Static” for GE ports.
Disable	Check this radial button to forbid the GE ports to run any link aggregation function.
LACP Settings	
System Priority	It specifies the system priority required for the LACP.
Group1/Group2 (Tab)	
Activity	<p>It specifies the activity of the GE ports of the specified group, active or passive, for the LACP.</p> <ul style="list-style-type: none"> • Passive: The NE does not initiate LACP negotiation procedure on the specified group voluntarily, but waits for its LACP peer (in active state) initiates negotiation. The NE will form the aggregation link with its peer at the end of the negotiation procedure. • Active: The NE is willing to initiate the LACP negotiation procedure on the specified group and sends out an LACP packet voluntarily. The aggregation link will be formed if the other end is running in LACP active or passive mode.
Timeout	<p>It specifies the interval of periodical transmitting LACP BPDU by the peer NE. If the NE does not receive the LACP BPDU after 3 consecutive specified intervals, the NE will remove the port from the aggregation link. For a busy aggregation link, it is recommended to set a short timeout to ensure that a disabled port is removed as soon as possible.</p> <p>Its value is either long (30 seconds) or short (1 second).</p>
Port GE1/Port GE2 (Tab)	
LACP Group	It specifies which the LACP group of GE1/GE2 is.
Port Priority	It specifies the port priority of GE1/GE2.

RSTP Configuration

The 802.1D Spanning Tree Protocol (STP) standard was designed at a time when the recovery of connectivity after an outage within a minute or so was considered adequate performance. Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) can be seen as an evolution of the 802.1D standard more than a revolution. The 802.1D terminology remains primarily the same.

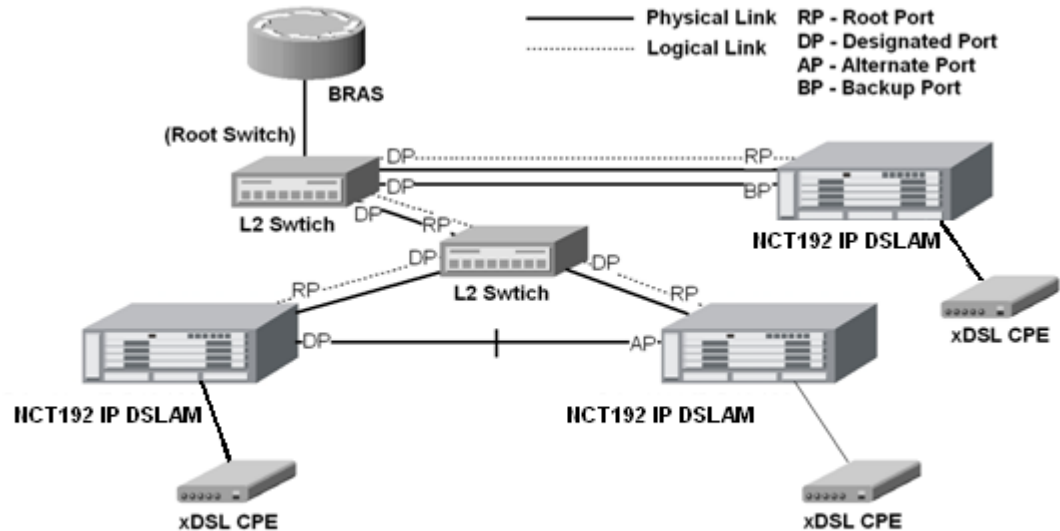
Port Roles and the RSTP Topology

The RSTP selects the bridge with the highest switch priority (lowest numerical priority value) as the root bridge. When the RSTP function of NCT192 IP-DSLAM is enabled, it assigns their network interface to play one of following port-roles. Figure 6-10 shows an example of Rapid Spanning Tree Topology when the RSTP converges.

- Root port – Provides the best path (lowest cost) when the switch forwards packets to the root switch.
- Designated port – Connects to the designated switch, which incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port.

- Alternate port – An alternate port is a port blocked by receiving more BPDUs from another bridge.
- Backup port – A backup port is a port blocked by receiving more useful BPDUs from the same bridge which is on.

Figure 6-10 Rapid Spanning Tree Active Topology



The RSTP protocol smartly prevents the loop connection in your uplink networks. It improves the Spanning Tree Protocol (STP) by reducing the fail-over time whenever there is network topology change. The configuration of RSTP is divided to 2 parts. One is the system-wise configuration, which is described in the subsection “Bridge”. The other one is the port-specific configuration, which is described in the subsection “Port GE1/Port GE2”.

Follow the subsequent procedures to configure the related parameters.

Click Configuration → Trunk → RSTP Setting on **Main Menu** to open the **Rapid Spanning Tree Protocol for Trunk Ports Dialog**

Bridge

Click the **Bridge** tab in **Rapid Spanning Tree Protocol for Trunk Ports Dialog** to launch the **Rapid Spanning Tree Protocol for Trunk Ports – Bridge Dialog** as shown in Figure 6-11. Table 6-7 depicts the related parameters.

Figure 6-11 Trunk RSTP Setting– Bridge Dialog

Table 6-7 Rapid Spanning Tree Protocol for Trunk Ports– Bridge Dialog Description

Field	Description
RSTP Administrative State	
Administrative State	Enable or disable the RSTP function for GE ports.
Version	This specifies the RSTP version the NE runs.
Bridge (Tab)	
Current Bridge ID	It indicates an unique 8-octet bridge ID which consists of a 2-octet Bridge Priority and a 6-octet MAC address.
Bridge Priority	It specifies the 2-octet bridge priority. If the given value is lower than all the other L2 devices', the NE is selected as the root bridge as defined in IEEE 802.1d/ 802.1w. Its valid range is through 0 to 61440 in steps of 4096
Max Age	It specifies the maximum age of STP/RSTP information learned from the network on any port before it is discarded.
Hello Time	It specifies the amount of time between the transmission of configuration bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so.
Forward Delay	This specifies the time value that controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in the Learning states, which precede the Forwarding state. This value is also used, when topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database.
Tx Hold Count	This specifies the value used by the port Transmit state machine to limit the maximum transmission rate.



It is noted that the following relationships have to be maintained.

$$2 \times (\text{Forward Delay} - 1 \text{ second}) \geq \text{Max Age}$$

$$\text{Max Age} \geq 2 \times (\text{Hello Time} + 1 \text{ second})$$

Port GE1/Port GE2

Click the **Port GE1/Port GE2** tab in **Rapid Spanning Tree Protocol Dialog** to launch the **Rapid Spanning Tree Protocol –Port GE1/Port GE2 Dialog** as shown in Figure 6-12. Table 6-8 depicts the related parameters.

Figure 6-12 Trunk RSTP Setting– Port GE1/Port GE2 Dialog

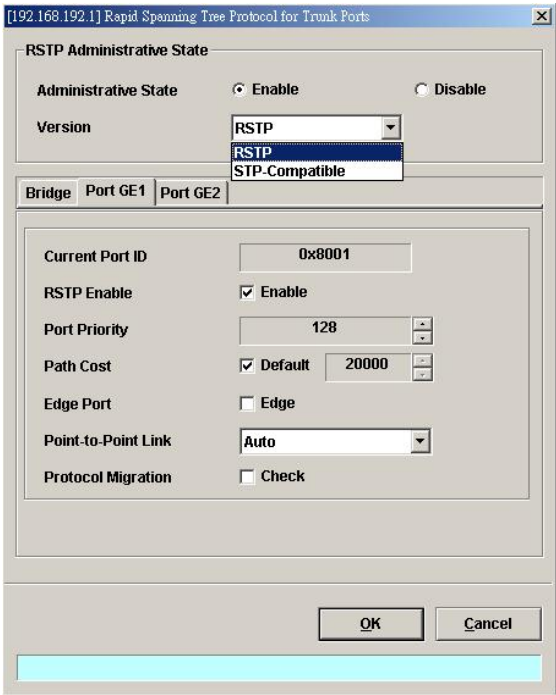


Table 6-8 RSTP for Trunk Ports– Port GE1/Port GE2 Dialog Description

Field	Description
RSTP Administrative State	
Administrative State	Enable or disable the RSTP function for GE ports.
Version	This specifies the RSTP version the NE runs.
Port GE 1 / Port GE 2 (Tab)	
Current Port ID	It specifies the GE1/GE2 port's port ID so far.
Port Enable	The current RSTP enabled/disabled status of the port
Port Priority	It specifies the port priority of a port. In the case that more than one ports form a loop in the NE, the RSTP/STP will block the ports of lower Port Priority (higher numerical value). Only the port of higher Port Priority (lower numerical value) is to be at the Forwarding state. Its valid range is through 0 to 240 in steps of 16
Path Cost	It specifies the contribution of this port to the path cost of paths towards the spanning tree root bridge. A port of higher speed should be configured with lower numerical value. When set it to be "default", its value follows the definition of IEEE 802.1d Table 17-3.
Edge Port	Check to let the port become edge port in spanning tree topology. An edge port on an RSTP switch will immediately transition to the forwarding state. However, the port will be a non-edge port if the NE receives RSTP BPDU on that port. And the port state and port role of the non-edge port will be determined by the RSTP hereafter.
Point-to-Point Link	Select YES to force this port always be treated as if it is connected to a point-to-point link. Select NO to let this port be treated as having a shared media connection. AUTO indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregately, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
Protocol Migration	Check to force this port to transmit RSTP BPDUs.



When set Path Cost to be "default", its value follows the definition of IEEE 802.1d Table 17-3 as follows.

Link Speed	Recommended value	Recommended range	Range
≤100 Kb/s	200 000 000 ^a	20 000 000–200 000 000	1–200 000 000
1 Mb/s	20 000 000 ^a	2 000 000–200 000 000	1–200 000 000
10 Mb/s	2 000 000 ^a	200 000–20 000 000	1–200 000 000
100 Mb/s	200 000 ^a	20 000–2 000 000	1–200 000 000
1 Gb/s	20 000	2 000–200 000	1–200 000 000
10 Gb/s	2 000	200–20 000	1–200 000 000
100 Gb/s	200	20–2 000	1–200 000 000
1 Tb/s	20	2–200	1–200 000 000
10 Tb/s	2	1–20	1–200 000 000

CoS Configuration

In order for the NE to play the role of edge (boundary) node of a DiffServ domain, the NE supports the the configurable mapping among the following entities.

- IEEE 802.1p User Priority as configured in the VC-to-VLAN configuration.
- Queue (Traffic Class) on each uplink trunk GE port
- DiffServ Code Point (DSCP) of the IP frame to be forwarded via the uplink trunk GE port.

User priority: The IEEE 802.1p user priority is a label carried with the frame that communicates the requested priority to the next hop (bridge, router or end systems). Typically, the user priority is not modified in the intermediate hop. Thus, the user priority has end-to-end significance across bridged LANs.

Queue (traffic class): A bridge can be configured so that multiple queues are used to hold frames waiting to be transmitted on a given outbound port, in which case the traffic class is used to determine the relative priority of the queues. Whenever the bridge's physical port is configured as strict priority (SP), all waiting frames at a higher traffic class are transmitted before any waiting frames of a lower traffic class. As with access priority, traffic class is assigned by the bridge on the basis of incoming user priority.



Currently, the NE supports 8 traffic classes (queues) on its GE ports with the strict priority (SP) scheduling policy only.

Differentiated Service Code Point (DSCP): RFC 2474/2475 defines the DiffServ field, which replaces the Type of Service (ToS) field in the IPv4 header. It facilitates the network devices behind IP-DSLAM to fulfill the end-to-end QoS.

Figure 6-13 shows the DiffServ field.

Figure 6-13 DiffServ Field



The most significant six bits of DiffServ field are called DSCP. The network device classifies packets and marks them with appropriate DSCP value. According to these values, other network devices in the DiffServ domain can make decision for packets behavior and provide the Quality of Service properly.

A network device classify the priorities of traffic with 6 different levels, they are Express Forwarding (EF), Assured Forwarding Class 4 (AF4), Assured Forwarding Class 3 (AF3), Assured Forwarding Class 2 (AF2), Assured Forwarding Class 1 (AF1) and Best Effort (BE). These forwarding classes are represented by the first 3 bits of DSCP as shown in Table 6-9. Moreover, the network device differentiates three drop precedence in AF4~AF1 respectively into last 3 bits of DSCP, they are Low Drop Precedence, Medium Drop Precedence and High Drop Precedence.

Table 6-9 DSCP: DS3~DS5 Bit Representation

Decimal representation of bits DS5, DS4 and DS3	Description
7	For link layer and routing protocol keep alive.
6	For using for IP routing protocols.
5	Express Forwarding (EF)
4	Assured Forwarding Class 4 (AF4)
3	Assured Forwarding Class 3 (AF3)
2	Assured Forwarding Class 2 (AF2)
1	Assured Forwarding Class 1 (AF1)
0	Best Effort (BF)

Expedited Forwarding: The code point of EF is 101110, the packets marked with EF is to be transmitted with highest priority, lowest drop probability.

Assured Forwarding: Assured Forwarding PHB is suggested for applications that require a better reliability than the best-effort service. There are 4 classes of AF. Within Each AF class, there are 3 drop precedences. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. Table 6-10 indicates the relationship of the 4 AF class.

Table 6-10 DSCP Class Relationship

Drop	Class			
	AF1	AF2	AF3	AF4
Low Drop Probability	001010 (AF11)	010010 (AF21)	011010 (AF31)	100010 (AF41)
Medium Drop Probability	001100 (AF12)	010100 (AF22)	011100 (AF32)	100100 (AF42)
High Drop Probability	001110 (AF13)	010110 (AF23)	011110 (AF33)	100110 (AF43)

To rest of this section depicts the setting of so called “per hop behavior (PHB)” defined in DiffServ. The setting of PHB is separated in two parts.

- Mapping the 802.1p user priority value to the queue (Traffic Class) of GE port
- Mapping the 802.1p value to the DSCP value



In the definition of PHB defined in DiffServ, it implicates that the Hop (usually a router) needs to classify the received traffic and remark its DSCP accordingly. The classification here indicates either MFC (Multi-Field classification) or DSCP classification. When the NE is at the edge, it should adopt the MFC. Otherwise, it should adopt the DSCP classification.

Then if the physical link is Ethernet, it has to also reassign the 802.1p value to be consistent with the DSCP assignment.

However, as the NE can only support the PVC-based classification, and can only reassign the 802.1p value. We therefore adopt a way different to the formal DiffServ definition.

Follow the subsequent procedure to configure the Trunk CoS mapping.

Click Configuration → Trunk → CoS Mapping on **Main Menu** to open the **CoS Priority – Queue Mapping Dialog** as shown in Figure 6-14. Table 6-11 depicts the related parameters.

Figure 6-14 Trunk CoS Mapping and DSCP Re-mapping Dialog

User Priority	Queue (Traffic Class)	DiffServ Code Point (DSCP)
0	3	AF11
1	1	AF11
2	2	AF11
3	4	AF21
4	5	AF21
5	6	AF31
6	7	AF31
7	8	Expedited Forwarding

* Queue 8 has the highest priority for packet transmission
 * AFxy: Assured Forwarding, service class x, drop precedence y

DSCP Re-mapping Administrative State
 Administrative State: ☐ Enable ☒ Disable

OK Cancel

Table 6-11 Trunk CoS Mapping and DSCP Re-mapping Dialog Description

Field	Description
802.1p User Priority-CoS Queue Mapping and DSCP Re-mapping	
User Priority	This indicates the 802.1p user priority as configured in the VC-to-VLAN configuration
Queue (Traffic Class)	Use this combo-box to set the mapping relation between each 802.1p and CoS queues on the uplink trunk GE port
DiffServ Code Point (DSCP)	Use this combo-box to set the new DSCP value on the IP frame to be forwarded via the uplink trunk GE port.
DSCP Re-mapping Administrative State	
Administrative State	Enable or disable the DSCP Re-mapping function.

Manual VLAN Setting

This section depicts the manual VLAN-member port setting procedure of GE1 and GE2. The operator needs to choose the VLAN between 1 and 4094 to apply to GE ports when the following cases hold.

- GE1 port and GE2 port on NC is configured as tagged-only mode. (See Section “Constructing the NE Objects”)
- GE2 port is configured as a subtended port. (See “Figure 6-7 Trunk Port Configuration Dialog”)

Follow the subsequent procedures to configure the related parameters.

- Step 1** Click Configuration → Trunk → Manual VLAN Setting on **Main Menu** to open the **Manual VLAN Setting** Dialog as shown in Figure 6-15. Table 6-12 depicts the related parameters.
- Step 2** Click the button to change its color to blue to make both the GE ports join as the member port of the VLAN in interest.
 For example, click the button positioned at the cross of the cloumn”10” and row “91-100” will make both the GE ports join as the member port of the VLAN of

VLAN-ID=100.

Figure 6-15 Manual VLAN Setting Dialog

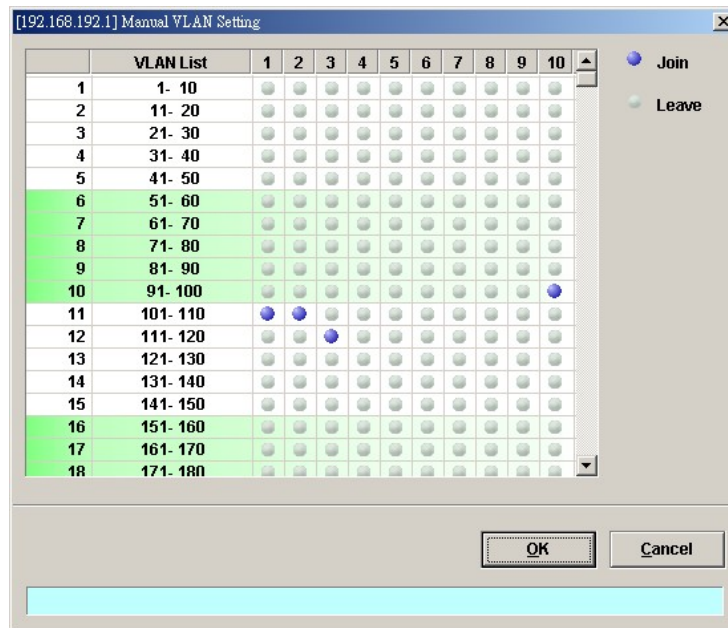
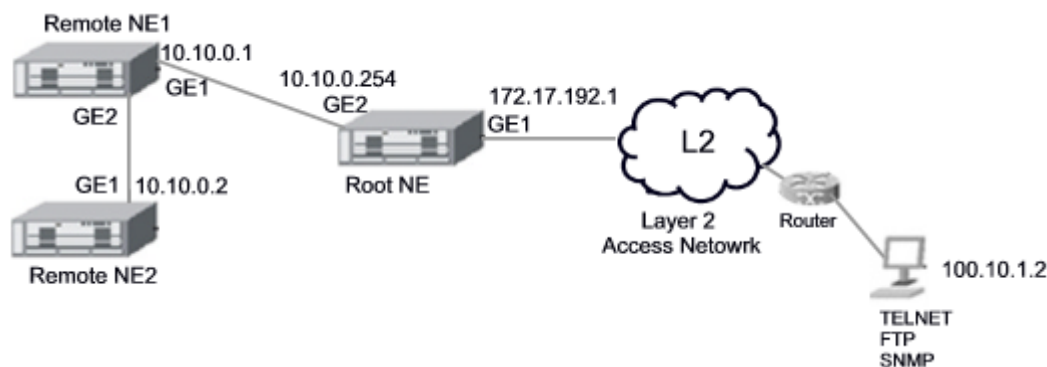


Table 6-12 Manual VLAN Setting Dialog Description

Field	Description
VLAN List	
The combination of VLAN List column and VLAN List row specifies a VLAN. For example, the button positioned at the cross of the cloumn"1" and row "101-110" indicates the VLAN of VLAN-ID=101.	
Fuction Button	
Join	The blue button indicates the both the GE ports are the member ports of VLAN in interest.
Leave	The grey button indicates the both the GE ports are not the member ports of VLAN in interest.

Cascaded NE Management

In some network deployment environment, it is desired to cascade several IP-DSLAMs to share a single uplink as well as the same management IP address to the access network. Hereafter, the NE is said to be connected in a cascading topology when it is deployed in the aforementioned way. And the NE is said to run in the cascade mode. Figure 6-16 depicts a typical cascading topology.

Figure 6-16 Illustration of cascading topology

When the NEs are connected in a cascading topology, the NE plays either one of the following roles.

- **Root-NE**
The Root-NE indicates the NE which is directly connected to the L2 access network as shown in Figure 6-16. The Root-NE possesses 2 IP addresses.
 - UGE IP: “UGE IP” is for the communication with the EMS server, LCT and Telnet hosts.
 - root IP: “root IP” is for the communication with the Remote-NE. It is invisible to the network operator.
- **Remote-NE**
The Remote-NE indicates the NE which is not directly connected to the L2 access network as shown in Figure 6-16. The Remote-NE possesses only one IP address.
 - UGE IP: “UGE IP” is for the communication with the Root-NE.



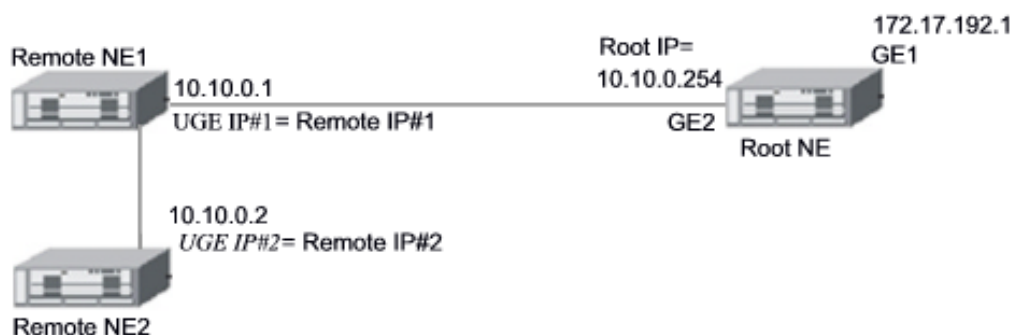
The following 2 IPs should be the same otherwise, the Root-NE can not communicate with Remote-NE.

- “remote-ne-ip” of the Root-NE
- “UGE IP” of the Remote-NE

In order for the operator to manage the NEs in a cascading topology, the operator needs to set them to run in the cascade mode. The configuration covers the following settings.

- Configuring the NE Role
- Adding Remote NE

After appropriate IP configuration on the Root-NE and Remote-NEs as shown in Figure 6-17, these NEs will work as a single NE which possesses several shelves via the EMS.

Figure 6-17 Illustration the IP configuration of NEs in a cascading topology

The following settings of the Root-NE and Remote-NEs are different.

- “Secured Host” of Remote-NE: must be set to be Root-NE.
“Secured Host” of Root-NE: must be set to be LCT, EMS server and so on.
- “SNMP Trap Community” of Remote-NE: must be set to be Root-NE.
“SNMP Trap Community” of Root-NE: must be set to be LCT, EMS server and so on.



The following setting of the Root-NE and Remote-NEs must be the same.

- “SNMP Community” of the read-write privilege.
- “tagged mode” of the UGE ports: Either “Tagged-only” or “Untagged-only”.
- Management VLAN setting (via the CLI command “config mgt set vlan”): when the the UGE ports of Root-NE and Remote-NEs are set to be “Tagged-only”.
- The software version of NC.



The mini-GBIC and fiber have to be of the same type, either SM or MM.



The LCT does not support to manage the Remote-NE.

Configuring the NE Role

Follow the subsequent procedures to configure the related parameters.

Click Configuration → NE Management → Cascaded Management on **Main Menu** to open the **Cascaded Management Setting** Dialog as shown in Figure 6-18 and Table 6-13 depicts the related parameters.

Figure 6-18 Cascaded Management Setting Dialog

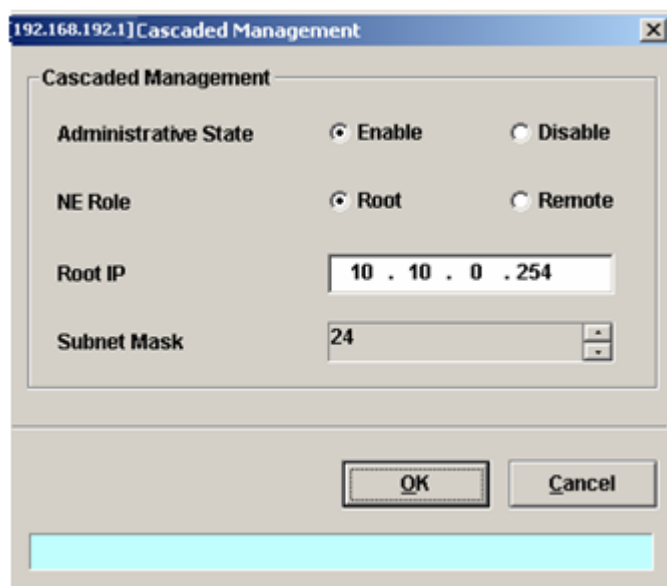


Table 6-13 Cascaded Management Setting Dialog Description

Field	Description
Cascaded Management	
Administrative State	This specifies the administrative state. (enable or disable)
NE Role	This specifies the role of the NE to be either “Root-NE” or “Remote-NE”
Root IP	This specifies the IP address of the Root-NE for the Root-NE to communicate with the Remote-NE. (see Figure 6-17)
Subnet Mask	This specifies the subnet mask associated with “Root IP” to specify a subnet where the Remote-NE to resides in



When deploying NEs to form a cascading topology as shown in Figure 6-17, the IP address of UGE ports of Remote-NE1 and Remote-NE2 have to be setup up frist. As can be seen in Figure 6-17, they are set as UGE IP#1 and UGE IP#2, respectively.

On the Root-NE, suppose the operator sets “IP Address” of Remote-NE corresponding to Remote-NE1 and Remote-NE2 as Remote IP#1 and Remote IP#2, respectively.

In this situation, the operator has to let the following equations hold.

$$\text{Remote IP\#1} = \text{UGE IP\#1}$$

$$\text{Remote IP\#2} = \text{UGE IP\#2}$$

Moreover, the Root IP of Root NE, UGE IP#1 and UGE IP#2, have to be set in the same subnet.

Adding Remote NE

Follow the subsequent procedures to add Remote NE one by one.

- Step 1** Click Configuration → NE Mangement → Cascaded Management on **Main Menu** to open the **Cascaded Remote NE List** Dialog as shown in Figure 6-19 and Table 6-14 depicts the related parameters.

Figure 6-19 Remote NE List Dialog

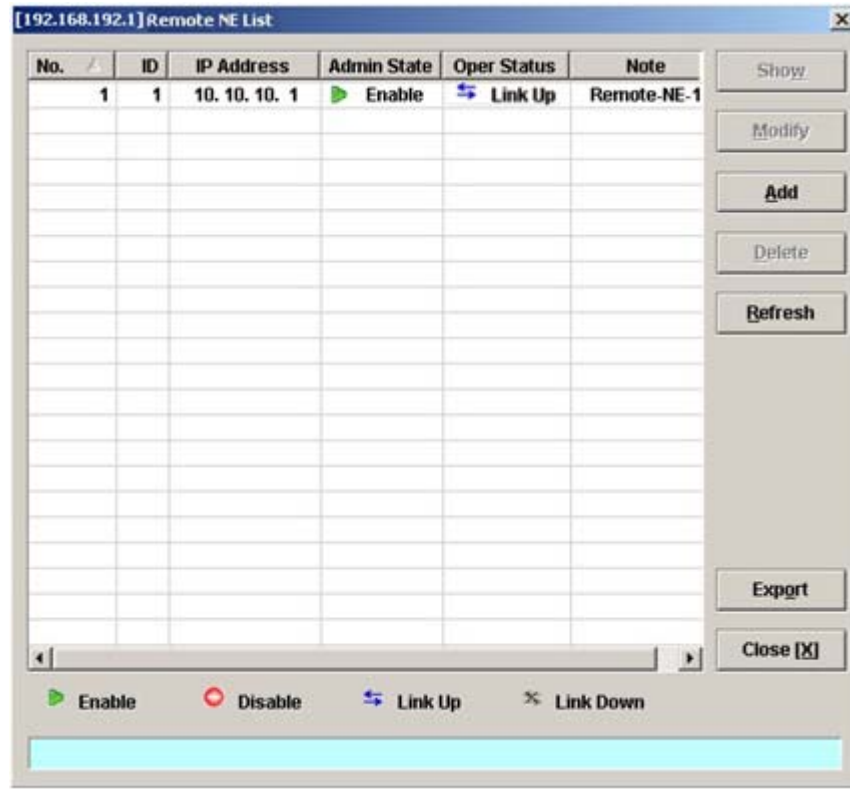


Table 6-14 Remote NE List Dialog Description

Field	Description
List Table	
No.	This specifies the serial number of entry of List Table.
ID	This indicates the serial number of the remote NE.
IP Address	This indicates the IP address of the remote NE.
Admin State	This specifies the administrative state of the cascade mode. (enable or disable)
Oper Status	This specifies the operation status of the cascade mode. (connected or disconnected)
Note	This gives a meaningful name to the specified note of the remote NE. The valid value is string of up to 25 characters.
Function Button	
Show	Click this button to show.
Modify	Click this button to modify.
Add	Click this button to add new remote NE.
Delete	Click this button to delete the remote NE.
Refresh	Click this button to refresh the remote NE list.
Export	Click this button to save the contents of the Remote NE List to the Personal Computer.
Close	Exit the Remote NE List Dialog.

Step 2 Click 'Add' button to launch the **Remote NE Setting** dialog as shown in Figure 6-20 to add the new remote NE setting. Table 6-15 depicts the related parameters.

Figure 6-20 Remote NE Setting Dialog

[192.168.192.1] Remote NE Setting

Remote NE Information

ID

1

Administrative State

Enable

Disable

IP Address

10 . 10 . 10 . 1

SNMP Community

netman

Login User Name

admin

Login Password

Note

Remote-NE-1

OK

Cancel

Table 6-15 Remote NE Setting Dialog Description

Field	Description
Remote NE Information	
ID	This indicates the serial number of the remote NE.
Administrative State	This specifies the administrative state of the cascade mode. (enable or disable)
IP Address	This indicates the IP address of the remote NE.
SNMP Community	This indicates the case-sensitive SNMP community name.
Login User Name	Fill the administrative level username of the remote NE.
Login Password	Fill the comparative password of the administrative level username.
Note	This gives a meaningful name to the specified note of the remote NE. The valid value is string of up to 25 characters.

Chapter 7 Connection Port Management

This chapter describes data channel connection and access services filter control.

This chapter contains the following sections:

- VC-to-VLAN Connection Management
- Access Control List
- Multicast Service Management
- Multicast Service
- System Services Configuration

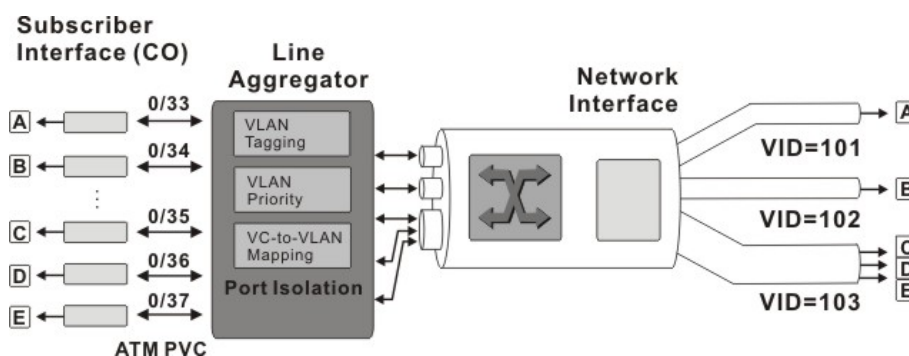
VC-to-VLAN Connection Management

The VC-to-VLAN setting can easily define the multiple to one or one to one mapping; you can group different PVCs to a single VLAN ID as well as single PVC to one VLAN mapping. Figure 7-1 illustrates the basic principle for VLAN assignment in the NCT192 IP-DSLAM. As shown in Figure 7-1, the NE forwards five data flows, A~E, which may be either owned by the same subscriber or by different subscribers. It is noted that these data flows are conveyed in five individual ATM PVCs, and they are grouped into 3 individual VLANs.



The NE supports up to 8 PVCs per xDSL port.
The NE supports up to 4094 VLANs per system.

Figure 7-1 VC-to-VLAN Mapping Illustrate



According to IETF RFC2684, an IP packet is encapsulated in either bridged mode or routed mode. The VC-to-VLAN settings are similar but not the same in these two encapsulation modes. This section depicts their configuration procedures together.

NE Operations in RFC 2684 bridged mode

In the RFC 2684 bridged mode, the NE needs to perform the following functions for the xDSL subscriber to access the Internet.

- For the upstream traffic
 1. Performs the ATM SAR (Segmentation and Reassembly) function to reassemble the ATM cells to get an ATM AAL5 frame.
 2. Strip off the ATM AAL5 trailer to get the RFC2684-encapsulated Ethernet frame.
 3. Strip off the RFC2684 header to get the Ethernet frame.
 4. Add a VLAN tag (Q_s) to the Ethernet frame if required. (see the definition of “ Q_s ” in the

description of Table 4-3)

5. Forward the Ethernet frame from the xDSL subscriber to ISP.
- For the downstream traffic
 1. Strip off the VLAN tag (Q_s) from the Ethernet frame if required. (see the definition of “ Q_s ” in the description of Table 4-3)
 2. Encapsulate the downstream Ethernet frame with RFC2684 header
 3. Append the ATM AAL5 trailer to the RFC2684-encapsulated Ethernet frame to get an ATM AAL5 frame.
 4. Performs the ATM SAR (Segmentation and Reassembly) function to segment the ATM AAL5 frame to get ATM cells.
 5. Forward the Ethernet frame from the ISP to the xDSL subscriber.

NE Operations in RFC 2684 routed mode

In the RFC 2684 routed mode, the NE needs to perform the following functions for the xDSL subscriber to access the Internet.

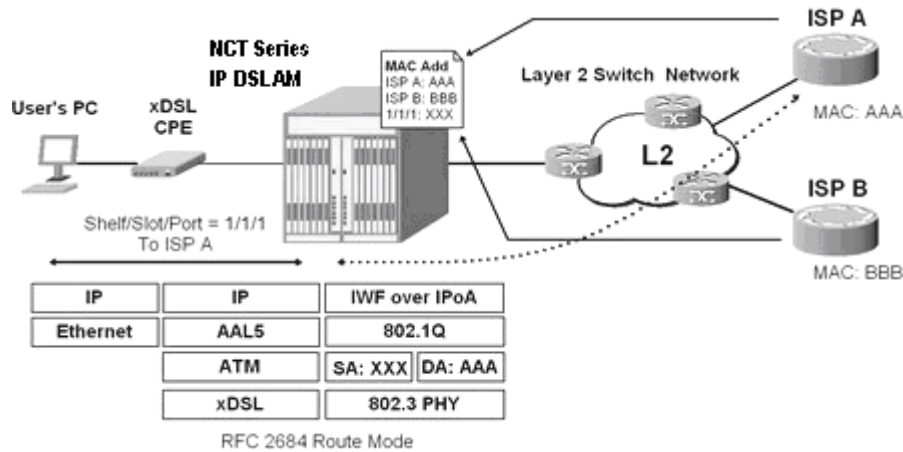
- For the upstream traffic
 1. Performs the ATM SAR (Segmentation and Reassembly) function to reassemble the ATM cells to get an ATM AAL5 frame.
 2. Strip off the ATM AAL5 trailer to get the RFC2684-encapsulated IP packet.
 3. Strip off the RFC2684 header to get the IP packet.
 4. Prefix an Ethernet header to the IP packet. The prefixed Ethernet header is of the following setting.
 Destination MAC = the MAC of Next-hop router toward the ISP's router.
 Source MAC = an unique MAC generated by the NE.
 5. Add a VLAN tag (Q_s) to the Ethernet frame if required. (see the definition of “ Q_s ” in the description of Table 4-3)
 6. Forward the Ethernet frame from the xDSL subscriber to ISP.
- For the downstream traffic
 1. Strip off the VLAN tag (Q_s) from the Ethernet frame if required. (see the definition of “ Q_s ” in the description of Table 4-3)
 2. Strip off the Ethernet header from the IP packet.
 3. Encapsulate the downstream IP packet with RFC2684 header
 4. Append the ATM AAL5 trailer to the RFC2684-encapsulated Ethernet frame to get an ATM AAL5 frame.
 5. Performs the ATM SAR (Segmentation and Reassembly) function to segment the ATM AAL5 frame to get ATM cells.
 6. Forward the Ethernet frame from the ISP to the xDSL subscriber.



In the RFC 2684 routed mode, IP packets are directly encapsulated, i.e., no MAC layer is presented. Through the IWF (Inter-Work Function) of IPoA of IP-DSLAM, it needs to prefix the Ethernet MAC layer for particular subscriber interface. The source MAC address is specially generated by IP-DSLAM, and the destination MAC address is the next-hop router toward the ISP's router. The NE determines the MAC address of next-hop router by the (Address Resolution Protocol (ARP).

Figure 7-2 illustrates an example of the IWF in the case of RFC 2684 routed mode.

Figure 7-2 RFC 2684 Route Mode Connection Method



When you set the IP of “Next Hop”, the NE will send ARP to query the MAC of the “Next Hop”. When the MAC you observe is 00:00:00:00:00:00, it indicates something wrong such that the NE can not get the MAC of the Next-Hop router via ARP.

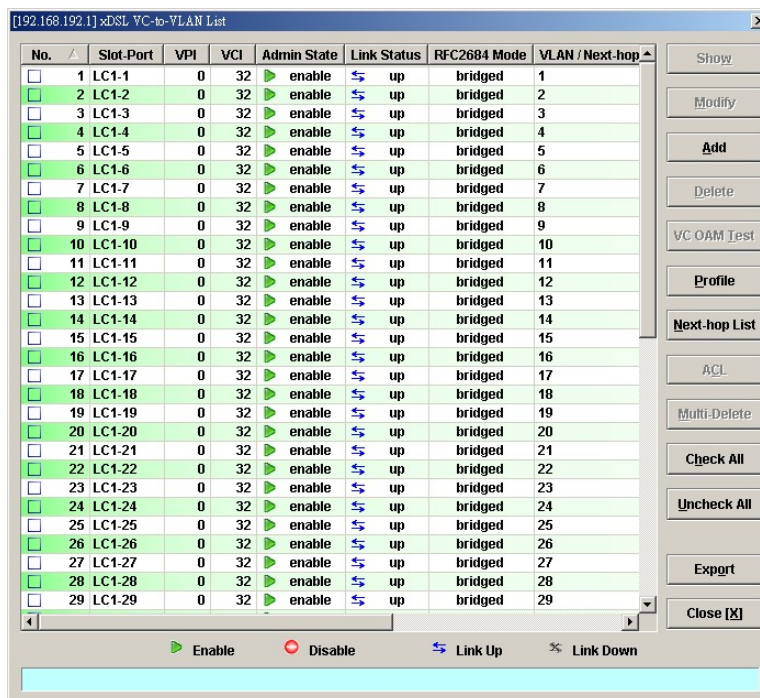


The VC-to-VLAN configuration procedures are the same to both the ADSL port and SHDSL port.

Follow the subsequent procedure to manage your VC-to-VLAN connectivity on a specific xDSL port.

Step 1 Click Configuration → xDSL → VC-to-VLAN on **Main Menu** to open the **xDSL VC-to-VLAN List** Dialog as shown in Figure 7-3.

Figure 7-3 xDSL VC-to-VLAN List Dialog



Step 2 Click on the ‘Add’ button on the right hand side of Figure 7-3 to display the window (Figure 7-4) for adding new PVC and configuring the associated setting. Figure 7-4 ~ Figure 7-10 show the corresponding configuration dialogs in the RFC2684 bridged mode and routed mode. Click either one tab to launch the corresponding dialog to

configure the parameters. Table 7-1 depicts the related configuration parameters



According to IETF RFC2684, an IP packet is encapsulated in either bridged mode or routed mode. The VC-to-VLAN settings are similar but not the same in these two encapsulation modes.

Figure 7-4 xDSL VC-to-VLAN Setting – IP Traffic Dialog

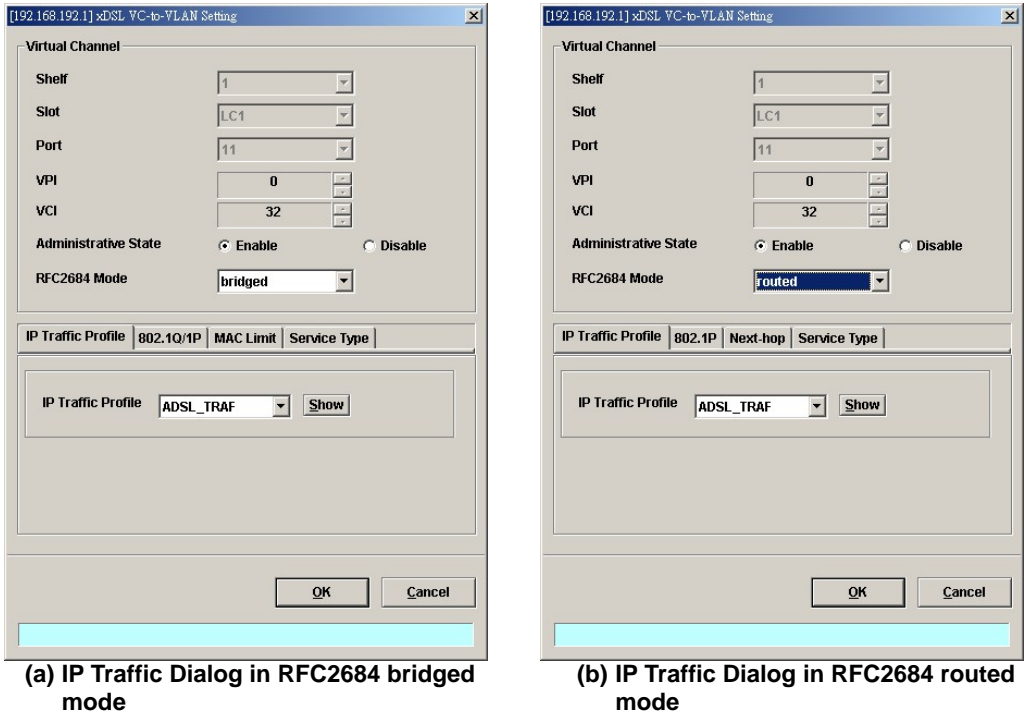


Figure 7-5 xDSL VC-to-VLAN Setting – 802.1Q/1P Dialog (only for the RFC2684 bridged mode)

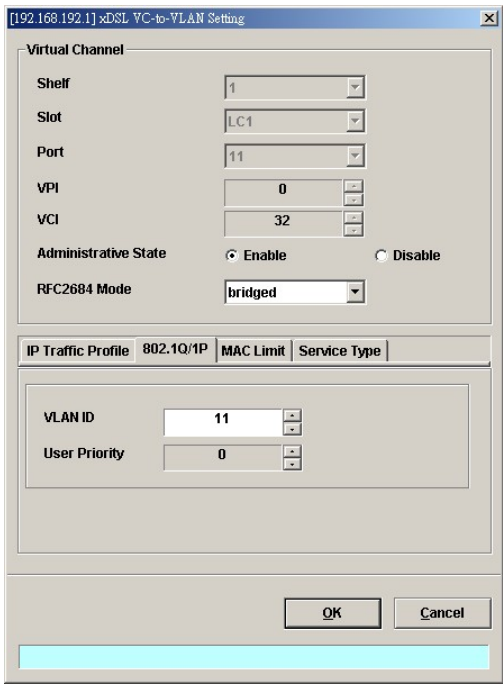
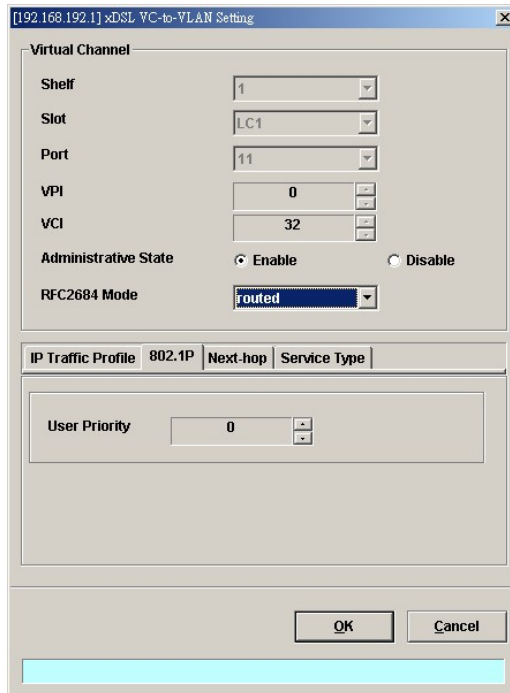
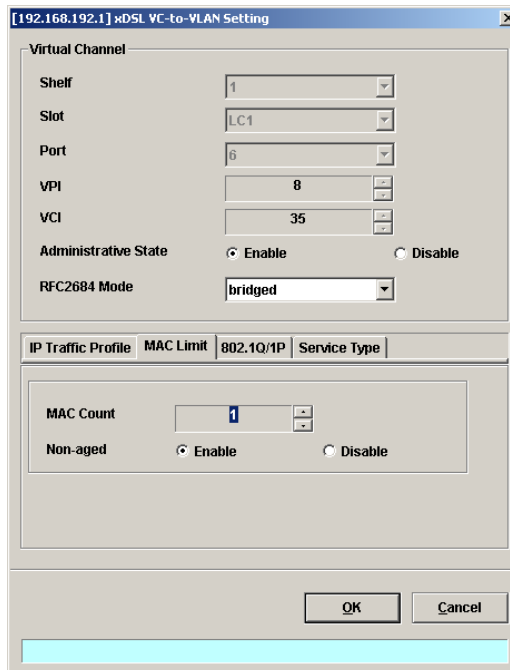


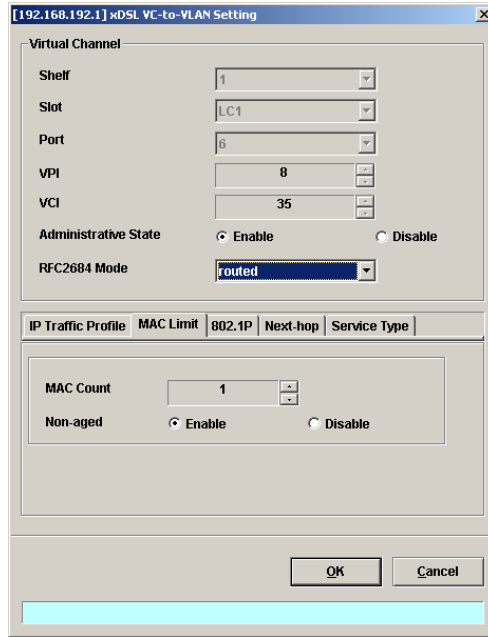
Figure 7-6 xDSL VC-to-VLAN Setting – 802.1P Dialog (only for the RFC2684 routed mode)

The dialog box is titled "[192.168.192.1] xDSL VC-to-VLAN Setting". It contains a "Virtual Channel" section with the following fields: Shelf (1), Slot (LC1), Port (11), VPI (0), and VCI (32). Below these is the "Administrative State" section with "Enable" selected and "Disable" unselected. The "RFC2684 Mode" is set to "routed". A tabbed interface at the bottom shows "IP Traffic Profile", "802.1P", "Next-hop", and "Service Type". The "802.1P" tab is active, showing a "User Priority" of 0. "OK" and "Cancel" buttons are at the bottom right.

Figure 7-7 xDSL VC-to-VLAN Setting – MAC Limit Dialog (only for the RFC2684 bridged mode)

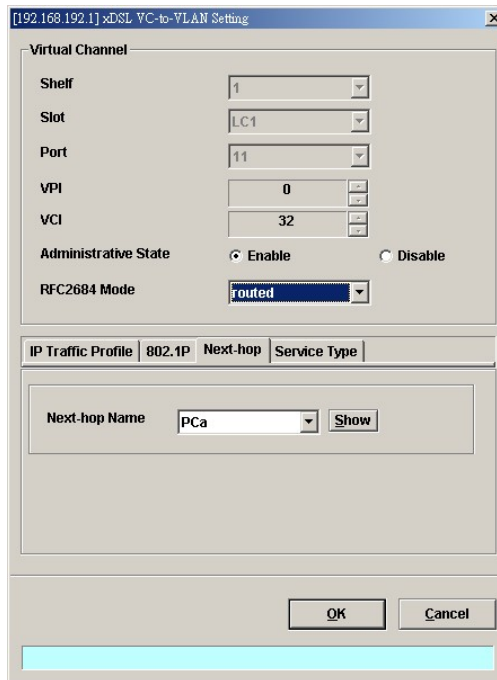
The dialog box is titled "[192.168.192.1] xDSL VC-to-VLAN Setting". It contains a "Virtual Channel" section with the following fields: Shelf (1), Slot (LC1), Port (6), VPI (8), and VCI (35). Below these is the "Administrative State" section with "Enable" selected and "Disable" unselected. The "RFC2684 Mode" is set to "bridged". A tabbed interface at the bottom shows "IP Traffic Profile", "MAC Limit", "802.1Q/1P", and "Service Type". The "MAC Limit" tab is active, showing a "MAC Count" of 1 and "Non-aged" set to "Enable". "OK" and "Cancel" buttons are at the bottom right.

Figure 7-8 xDSL VC-to-VLAN Setting – MAC Limit Dialog for the RFC2684 routed mode



The dialog box is titled "[192.168.192.1] xDSL VC-to-VLAN Setting". It contains a "Virtual Channel" section with the following settings: Shelf (1), Slot (LC1), Port (6), VPI (8), VCI (35), Administrative State (Enable), and RFC2684 Mode (routed). Below this is a tabbed interface with "IP Traffic Profile", "MAC Limit", "802.1P", "Next-hop", and "Service Type" tabs. The "MAC Limit" tab is active, showing "MAC Count" (1) and "Non-aged" (Enable). At the bottom are "OK" and "Cancel" buttons.

Figure 7-9 xDSL VC-to-VLAN Setting – Next-hop Dialog (only for the RFC2684 routed mode)



The dialog box is titled "[192.168.192.1] xDSL VC-to-VLAN Setting". It contains a "Virtual Channel" section with the following settings: Shelf (1), Slot (LC1), Port (11), VPI (0), VCI (32), Administrative State (Enable), and RFC2684 Mode (routed). Below this is a tabbed interface with "IP Traffic Profile", "802.1P", "Next-hop", and "Service Type" tabs. The "Next-hop" tab is active, showing "Next-hop Name" (PCa) and a "Show" button. At the bottom are "OK" and "Cancel" buttons.

Figure 7-10 xDSL VC-to-VLAN Setting – Service Type Dialog

The dialog box is titled "[192.168.192.1] xDSL VC-to-VLAN Setting". It has a "Virtual Channel" section with fields for Shelf (1), Slot (LC1), Port (11), VPI (0), and VCI (32). Below these are "Administrative State" (radio buttons for Enable and Disable, with Enable selected) and "RFC2684 Mode" (a dropdown menu set to "bridged"). A tab bar at the bottom shows "IP Traffic Profile", "802.1Q/1P", "MAC Limit", and "Service Type" (which is selected). The "Service Type" section contains a dropdown menu set to "PPPoE", a "Maximum IP Count" field set to 1, and a "Static IP's Base Address" field set to 0 . 0 . 0 . 0. At the bottom are "OK" and "Cancel" buttons.

(a) PPPoE service in RFC2684 bridged mode

The dialog box is titled "[192.168.192.1] xDSL VC-to-VLAN Setting". It has a "Virtual Channel" section with fields for Shelf (1), Slot (LC1), Port (11), VPI (0), and VCI (32). Below these are "Administrative State" (radio buttons for Enable and Disable, with Enable selected) and "RFC2684 Mode" (a dropdown menu set to "bridged"). A tab bar at the bottom shows "IP Traffic Profile", "802.1Q/1P", "MAC Limit", and "Service Type" (which is selected). The "Service Type" section contains a dropdown menu set to "DHCP", a "Maximum IP Count" field set to 1, and a "Static IP's Base Address" field set to 0 . 0 . 0 . 0. At the bottom are "OK" and "Cancel" buttons.

(b) DHCP service in RFC2684 bridged mode

The dialog box is titled "[192.168.192.1] xDSL VC-to-VLAN Setting". It has a "Virtual Channel" section with fields for Shelf (1), Slot (LC1), Port (11), VPI (0), and VCI (32). Below these are "Administrative State" (radio buttons for Enable and Disable, with Enable selected) and "RFC2684 Mode" (a dropdown menu set to "bridged"). A tab bar at the bottom shows "IP Traffic Profile", "802.1Q/1P", "MAC Limit", and "Service Type" (which is selected). The "Service Type" section contains a dropdown menu set to "static IP", a "Continuous IP Count" field set to 1, and a "Static IP's Base Address" field set to 0 . 0 . 0 . 0. At the bottom are "OK" and "Cancel" buttons.

(c) Static IP service in RFC2684 bridged mode

The dialog box is titled "[192.168.192.1] xDSL VC-to-VLAN Setting". It has a "Virtual Channel" section with fields for Shelf (1), Slot (LC1), Port (11), VPI (0), and VCI (32). Below these are "Administrative State" (radio buttons for Enable and Disable, with Enable selected) and "RFC2684 Mode" (a dropdown menu set to "routed"). A tab bar at the bottom shows "IP Traffic Profile", "802.1P", "Next-hop", and "Service Type" (which is selected). The "Service Type" section contains a dropdown menu set to "static IP", a "Continuous IP Count" field set to 1, and a "Static IP's Base Address" field set to 2 . 3 . 4 . 5. At the bottom are "OK" and "Cancel" buttons.

(d) Static IP service in RFC2684 routed mode

Table 7-1 xDSL VC-to-VLAN Setting Description

Field	Description
Virtual Channel	
Shelf, Slot, Port	This specifies the shelf-slot-port.
VPI	It specifies the VPI value
VCI	It specifies the VCI value
Administrative State	It specifies the state of this VC-VLAN to enable or disable.
RFC2684 Mode	It specifies the RFC 2684 mode, (Bridge or Route)
IP Traffic Profile Dialog	
IP Traffic Profile	This specifies the IP traffic profile
802.1Q/1P Dialog [only for RFC2684 bridged mode]	
VLAN ID	This specifies the VLAN ID value
User Priority	This specifies the VLAN priority
802.1P Dialog [only for RFC2684 routed mode]	
User Priority	This specifies the VLAN priority of corresponding VC-to-VLAN connection.
Next-hopDialog [only for RFC2684 routed mode]	
Next-hop name	It specifies the next-hop name as specified in the section 'ISP Information for IP over ATM' of Chapter 7.
MAC Limit Dialog [only for RFC2684 bridged mode]	
MAC Count	This specifies the number of subscriber's MACs allowed for the corresponding VC-to-VLAN connection.
Non-aged	Enable: The NE never ages out the mac learned on the specific PVCs. Disable: The NE will ages out the mac learned on the specific PVCs.
Service Type Dialog	
Service Type	This specifies the service type to be allowed on the PVC of individual subscriber. In RFC2684 routed mode, the following service type is supported. <ul style="list-style-type: none"> ● Static IP In RFC2684 bridged mode, the following three service types are supported. <ul style="list-style-type: none"> ● PPPoE ● DHCP ● Static IP
Maximum IP Count [only for DHCP Service]	This indicates the number of IP to be allowed while DHCP is selected
Continuous IP Count [only for Static IP Service]	This indicates the number of IP to be allowed while Static IP is selected
Static IP's Basic Address [only for Static IP Service]	This specifies the base of the IP address if the service type is Static IP



Enabling the Service Type Control makes the NE to provide the IP/MAC anti spoofing function. In the case that the subscriber acquires his IP address dynamically via PPPoE or DHCP, the NE will block the subscriber's traffic before a valid IP address assigning. Once the subscriber possesses a valid dynamic or static IP, the NE will just forward the packet of valid source IP/MAC addresses. IN other words, the NE drops the subscriber's traffic of invalid source IP/MAC addresses.



Whenever the service type is specified as "Static IP Service", it is noted that the following relationship should be maintained.

IP Address Increment/Port \geq Continuous IP Count



More than one PVCs can be configured in a xDSL port. Each PVC can be configured with different RFC 2684 mode (either RFC 2684 routed mode or RFC 2684 bridged mode). However, the NE supports only one RFC 2684 mode to be enabled for the PVCs in a xDSL port. Different xDSL ports are allowed to have their PVCs to run with distinct RFC 2684 mode.

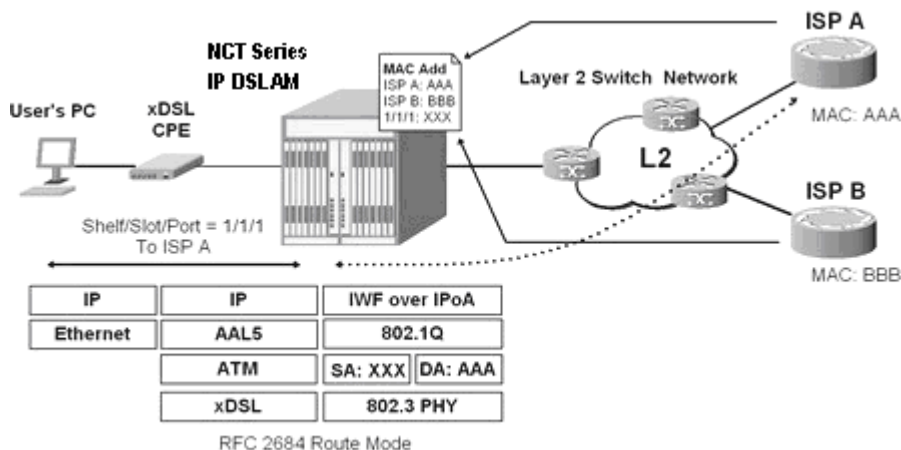


In the RFC 2684 bridged mode, the NE supports to IP counts \leq MAC limit per PVC of xDSL port.

ISP Information for IP over ATM

In the RFC 2684 routed mode, IP packets are directly encapsulated, i.e., no MAC layer is presented. Through the IWF (Inter-Work Function) of IPoA of IP-DSLAM, it needs to append the Ethernet MAC layer for particular subscriber interface, the source MAC address is specially generate by IP-DSLAM, and the destination MAC address is the next-hop router toward the ISP's router. The NE determines the MAC address of next-hop router by the (Address Resolution Protocol (ARP). Figure 7-11 illustrates an example of the IWF in the case of RFC 2684 routed mode.

Figure 7-11 RFC 2684 Route Mode Connection Method



Follow the subsequent procedure to launch the ISP Information dialog to resolve the MAC address by just specifying the Next-hop's IP address.

Step 1 Click Configuration → xDSL → Next-hop Info for IP over ATM on **Main Menu** to open the **Next-hop Info for IP over ATM** Dialog as shown in Figure 7-12 and Table

7-2 depicts the related parameters.

Figure 7-12 xDSL Next-hop List for IPoA Dialog

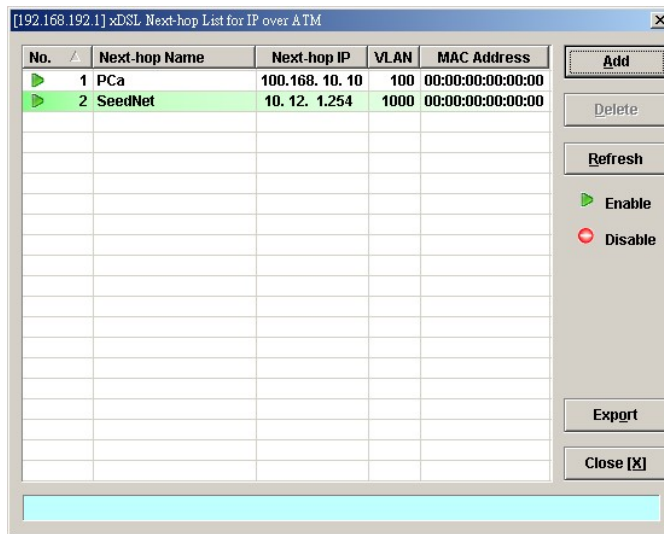


Table 7-2 xDSL Next-hop List for IPoA Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
Next-hop Name	It specifies the Next-hop name.
Next-hop IP	It specifies the Next-hop router IP.
VLAN	It specifies the VLAN grouping number for Next-hop connection.
MAC Address	It specifies the MAC address of the next-hop router toward the ISP's router.
Function Button	
Add	Click this button to add a new Next-hop entry
Delete	Click this button to remove the Next-hop entry
Refresh	Click this button to refresh the List Table
Export	Click this button to save the contents of xDSL Next-hop List for IPoA to the Personal Computer.
Close	Exit the xDSL Next-hop List for IPoA Dialog.

Step 2 Click 'Add' button to launch the **xDSL Next-hop for IPoA Dialog**. Figure 7-13 shows **xDSL Next-hop for IPoA Dialog**, and Table 7-3 depicts the related parameters.

Figure 7-13 Add xDSL Next-hop for IPoA Dialog

The screenshot shows a dialog box titled "[192.168.192.1] xDSL Next-hop Information for IPoA Setting". Inside, there is a section labeled "Next-hop Information" containing three input fields: "Name" with the value "SeedNet", "IP Address" with the value "10 . 12 . 1 . 254", and "VLAN ID" with the value "1000". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Table 7-3 Add xDSL Next-hop for IPoA Dialog Description

Field	Description
Next-hop Information	
Name	This specifies the Next-hop name.
IP Address	This specifies the Next-hop router IP.
VLAN ID	This specifies the VLAN grouping number for Next-hop connection.

Access Control List

The NE supports packet filtering functions allows you to forward or drop subscriber traffics received on the subscriber interfaces.

- NetBIOS/NetBEUI Packet Filtering
- Source MAC Access Control List

NetBIOS/NetBEUI Packet Filtering

The NE allows the operator to configure to forward or drop the name server protocol (NetBIOS and NetBEUI) traffics received on the subscriber interfaces.

Follow the subsequent procedures to configure the related parameters.

Click Configuration → xDSL → Packet Filter on **Main Menu** to open the **Packet Filtering** Dialog as shown in Figure 7-14 and Table 7-4 depicts the related parameters.

Figure 7-14 Packet Filtering Dialog

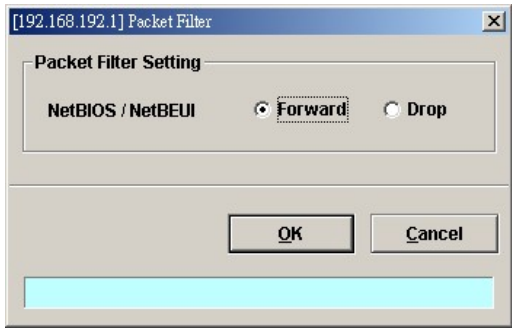


Table 7-4 Packet Filtering Dialog Description

Field	Description
Packet Filtering Setting	
NetBIOS/NetBEUI	Set the packet filtering function to “forward” or “drop” for NetBIOS and NetBEUI packets.

Source MAC Access Control List

The NE supports the VC-to-VLAN ACL function is to provide the operator a tool to manually deny/permit the ADSL subscriber’s upstream Ethernet frame according to their source MAC addresses.

For example, if there are duplicate MAC addresses from two or more individual xDSL subscriber ports, the operator should deny the hacker’s traffic and permit the good guy’s traffic. With the VC-to-VLAN ACL function, the operator can manually set to permit (forward) one of them and deny the rest traffic.

- Step 1

Click Configuration → xDSL → VC-to-VLAN on **Main Menu** to open the **xDSL VC-to-VLAN List** Dialog as shown in Figure 7-3.
- Step 2

Select a port in **VC to VLAN List dialog** and click “ACL” button on the right hand side of Figure 7-3 to configure the Access Control List option of the selected port. Figure 7-15 illustrated the **VC-to-VLAN Access Control List dialog**, and Table 7-5 depicts the related parameters. Figure 7-16 illustrated the window for adding new MAC into the access control list.

Figure 7-15 VC-to-VLAN Access Control List dialog

The screenshot shows a Windows-style dialog box titled "xDSL VC-to-VLAN Access Control List". It is divided into three main sections. The first section, "xDSL PVC", contains a "PVC" label and a text box with the value "LC4-1 0/32". The second section, "Current Control State", contains a "State" label and a dropdown menu currently showing "Permit All Listed Source MACs". The third section, "Controlled Source MAC List", contains a table with a header "Source MAC Address" and one data row with the value "00:00:00:00:00:02". To the right of this table are four buttons: "Add", "Delete", "Refresh", and "Close [X]".

Table 7-5 VC-to-VLAN Access Control List Dialog Description

Field	Description
xDSL PVC	
PVC	This indicates the specified xDSL port and specified PVC.
Current Control State	
State	This indicates the current access control state of the specified PVC.
Controlled Source MAC List	
Source MAC Address	This indicates the MAC address under controlling.
Function Button	
Add	Click this button to add or modify the role of access control.
Delete	Click this button to delete the specified access control entry.
Refresh	Click this button to refresh the access control state.
Close	Exit the Access Control List Dialog.

Step 3 Click 'Add' button to launch the **xDSL Access Control Dialog**. Figure 7-16 shows the **xDSL Access Control Dialog**, and Table 7-6 depicts the related parameters.

Figure 7-16 Add xDSL Access Control Dialog

The screenshot shows the 'xDSL Access Control' dialog box. It has three main sections: 'xDSL PVC', 'Control State', and 'Controlled Source MAC Address'. In the 'xDSL PVC' section, the 'PVC' field contains 'LC1-21 8/35'. In the 'Control State' section, the 'Current State' field contains 'Permit All Listed Source MACs', and the 'New State' section has two radio buttons: 'Permit' (which is selected) and 'Deny'. In the 'Controlled Source MAC Address' section, the 'MAC Address (Hex)' field contains '00:00:00:00:bb'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.



The format “00:00:00:00:00:00” of MAC Address in the xDSL Access Control is not allowed as shown in the following figure.

This screenshot shows the same 'xDSL Access Control' dialog box, but with an error. The 'MAC Address (Hex)' field now contains '00:00:00:00:00:00', which is highlighted with a red border. A yellow error message bar at the bottom of the dialog says 'Format error'. The 'Current State' field now shows '<none>'.

Table 7-6 Add xDSL Access Control Dialog Description

Field	Description
Control State (Add)	
Current State	This indicates the current access control state of the specified PVC.
New State	Check the radio button to select the role of new state.
Controlled Source MAC Address (Add)	
MAC Address (Hex)	This specifies the MAC address under controlling.



The roles of access control function, Deny and Permit, are repulsive, i.e. a “deny” role will be replaced while a new role “permit” is be configured.

Users can review the access control list from the menu combo-box. Follow the subsequent procedures to review the access control list configuration.

Click Configuration → xDSL → Access Control List on **Main Menu** to open the **xDSL Access Control List** Dialog as shown in Figure 7-17 and Table 7-7 depicts the related parameters.

Figure 7-17 xDSL Access Control List

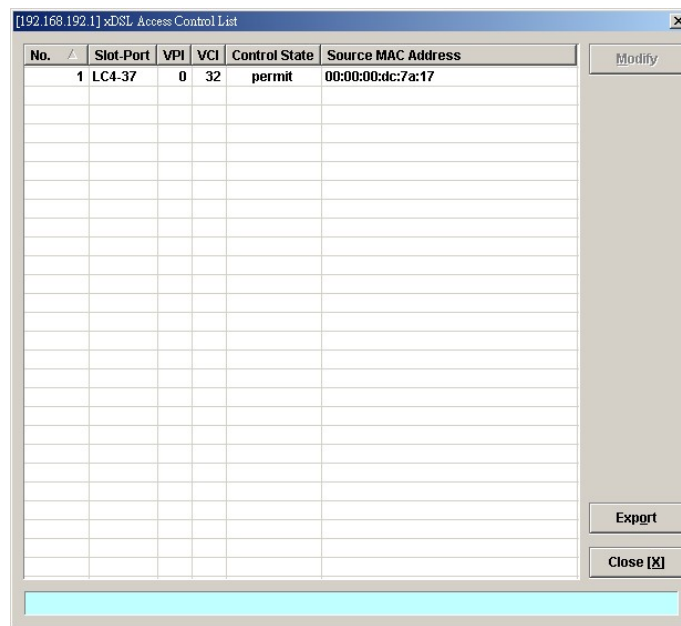


Table 7-7 xDSL Access Control List Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the access control list.
Slot-Port	This indicates the location of xDSL port.
VPI	This indicates the VPI of the specified xDSL subscriber.
VCI	This indicates the VCI of the specified xDSL subscriber.
Control State	This indicates the control state of access control of the specified xDSL subscriber.
Source MAC Address	This indicates the source MAC address which is under controlling of the specified xDSL subscriber.
Function Button	
Modify	Click this button to open the VC-to-VLAN Access Control List.
Export	Click this button to save the contents of xDSL Access Control List to the Personal Computer.
Close	Exit the xDSL Access Control List Dialog.

Static MAC configuration on xDSL Port

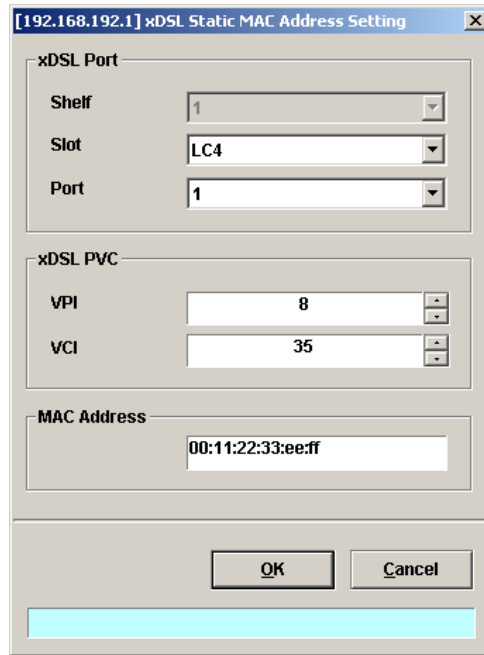
The NE supports the operator to add the “static” MAC addresses to specified xDSL line port manually. In comparison with the the MAC addresses learned from the associate ATM VC, the manually added “static” MAC addresses are never aged out.

- Step 1** Click Configuration → xDSL → Bridge Filtering Database on **Main Menu** to open the **xDSL Configured Filtering Database Entry List** Dialog as shown in Figure 7-18, and Table 7-8 depicts the related parameters.

Table 7-8 xDSL Configured Bridge Filtering Database Entry List Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
Slot-Port	This indicates the location of xDSL port.
VPI	This indicates the VPI of the specified entry.
VCI	This indicates the VCI of the specified entry.
MAC Address	This indicates the MAC address of the specified entry.
Status	<p>This indicates the reason the MAC address appears in this entry. The definitions of status are as follows.</p> <ul style="list-style-type: none"> • Static: It indicates this MAC entry is configured manually in FDB. • ACL Permit: It indicates the NE is to forward the upstream traffic of this indicated source MAC and drops the upstream traffic of other source MAC from the indicated xDSL port. • ACL Deny: It indicates the NE is to drop the upstream traffic of the indicated source MAC and forward the upstream traffic of other source MAC from the indicated xDSL port. • Learned Unique: It indicates the MAC address is learned on the indicated xDSL port dynamically with setting aged time and is a unique one • Learned Non-aged: It indicates the MAC address is learned on the indicated xDSL port dynamically with setting non-aged time and is a unique one. • Learned Spoofed Active: It indicates the spoofed MAC is at the “active” state. That is the NE is to forward the upstream traffic of the spoofed MAC from the the indicated xDSL port. • Learned Spoofed Inactive: It indicates the spoofed MAC is at the “inactive” state. That is the NE is to drop the upstream traffic of the spoofed MAC from the the indicated xDSL port.
Function Button	
Add Static	Click this button to add the static MAC entry to FDB.
Delete	Click this button to delete a specified MAC entry
Refresh	Click this button to refresh the list table.
Export	Click this button to save the contents of xDSL Configured Filtering Database Entry List to the Personal Computer.
Close	Exit the xDSL Configured Filtering Database Entry List Dialog.

Step 2 Click ‘Add’ button to launch the **xDSL Static MAC Address Setting Dialog**. Figure 7-19 shows the **xDSL Static MAC Address Setting Dialog**, and Table 7-9 depicts the related parameters.

Figure 7-19 xDSL Static MAC Address Setting Dialog


The dialog box is titled "[192.168.192.1] xDSL Static MAC Address Setting". It contains three main sections:

- xDSL Port:** Includes dropdown menus for Shelf (set to 1), Slot (set to LC4), and Port (set to 1).
- xDSL PVC:** Includes input fields for VPI (set to 8) and VCI (set to 35).
- MAC Address:** Includes a text field containing the MAC address 00:11:22:33:ee:ff.

At the bottom, there are "OK" and "Cancel" buttons, and a light blue horizontal bar.

Table 7-9 xDSL Configured Filtering Database Entry List Description

Field	Description
xDSL Port	
Shelf	This indicates the shelf of NE.
Slot	This specifies the slot of NE.
Port	This specifies the location of xDSL port.
xDSL PVC	
VPI	This specifies the VPI of the specified xDSL subscriber.
VCI	This specifies the VCI of the specified xDSL subscriber.
MAC Address	This specifies this MAC entry to be configured.

Multicast Service Management

Whenever the subscriber clicks his remote controller to watch a TV channel transmitted via the ADSL line, the set-top-box sends the corresponding IGMP report packet. The NE will forward IGMP packet if its multicast IP hits the associated multicast service profile. Otherwise, the NE drops the IGMP packet. As a result, the subscriber is restricted to watch the TV programs that he booked.

To provide multicast service, the operator needs to properly configure the multicast channel and IGMP snooping /IGMP proxy. This section contains the following two subsections.

- Multicast Channel Configuration
- IGMP snooping/IGMP proxy Configuration

Multicast Channel Configuration

The NE supports to prevent the subscriber to receive un-booked TV channel (multicast channel)

by checking the received “IGMP join” packet with a preconfigured Multicast Service Profile. (A Multicast Service Profile consists of a number of Multicast Channel Profiles.) The subscriber is restricted to receive the TV channels (recorded in the Multicast Channel Profile).

This sub-section depicts the CLI commands to associate the ADSL subscriber with the created Multicast Service Profiles.

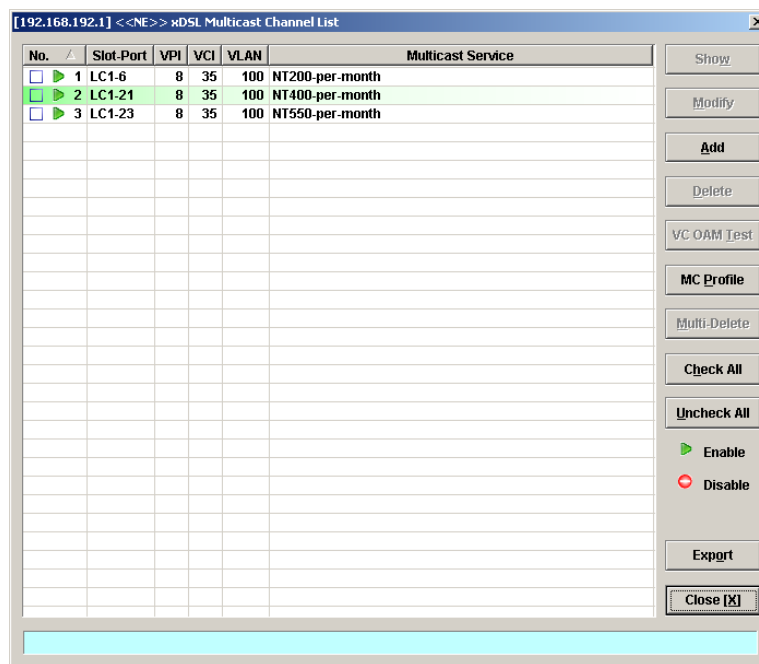
To forward the multicast stream, you are required to establish a VC-to-VLAN tunnel and specify the associated multicast service profile.

Follow the subsequent procedures to configure the related parameters.

- Step 1** Click Configuration → xDSL → Multicast Service on **Main Menu** to open the **xDSL Multicast Channel** Dialog.
- Step 2** Click on the ‘Modify’ or ‘Add’ button on the right hand side of Figure 7-20 to open the window (Figure 7-21) for adding new multicast channel and configure the associated setting.

In Figure 7-21, it is noted that two individual tabs (Multicast Service Profile and MAC Limit) are provided to set the Multicast Channel related parameters. Click either one **tab** to launch the corresponding dialog to configure the parameters. Table 7-10 depicts the related parameters

Figure 7-20 xDSL Multicast Channel List Dialog



The differences between the “Multi-Delete” and “Delete” button on the right hand side of Figure 7-20 are as follows.

“Multi-Delete”: To delete all the checked entries in the list.

“Delete”: To delete a highlighted entry in the list.

Figure 7-21 xDSL Multicast Channel Setting Dialog
Table 7-10 xDSL Multicast Channel Setting Description

Field	Description
Ethernet over ATM	
Shelf, Slot, Port	This specifies the physical connection information.
VPI	This specifies the VPI values.
VCI	This specifies the VCI values.
VLAN ID	This specifies the multicast VLAN ID.
Administrative State	Enable: Apply the specified multicast setting to the indicated PVC Disable: Do not apply specified multicast setting to the indicated PVC
Multicast Service Profile Dialog	
Profile	This specifies the multicast service profile. Please refer to the section “Multicast Service Profile” in Chapter 5.
Channel Limit Dialog	
Channel Limit	This specifies the number of multicast streams allowed to be forwarded via the VC-to-VLAN connection.

IGMP snooping/IGMP proxy Configuration

The NE supports IGMP snooping and IGMP proxy as follows.

- IGMP snooping:
When the IGMP snooping function is enabled,
 1. The NE starts to “listen in” IGMP conversations between hosts and routers.
 2. Once the NE hears an “IGMP join” message on an xDSL interface, it checks the associated Multicast Service Profile to prevent the subscriber to receive un-booked TV channels (multicast channel).
 3. If the multicast group IP of the received “IGMP join” message “hits” the Multicast Service Profile, the NE adds that xDSL interface to the corresponding multicast forwarding table and forwards this “IGMP join” message out of the GE port.

Otherwise, the NE drops the “IGMP join” message.

4. As the NE hears an “IGMP leave” message or the ‘snooping aging-time’ expires, the NE will remove that xDSL interface from the corresponding multicast forwarding table.

- **IGMP proxy:**

When the IGMP proxy function is enabled,

1. The NE starts to “listen in” IGMP conversations between hosts and routers.
2. Once it receives an “IGMP join” message from the subscribers, it checks the associated Multicast Service Profile to prevent the subscriber to receive un-booked TV channels (multicast channel).
3. If the multicast group IP of the received “IGMP join” message “hits” the Multicast Service Profile, the NE adds that xDSL interface to the corresponding multicast forwarding table. And the NE further checks if it already forwards the TV channel requested by this “IGMP join” message. If the answer is YES, the NE drops this “IGMP join” message. Otherwise, the NE sends an “IGMP join” message to request that TV channel via the GE port.
If the multicast group IP of the received “IGMP join” message “misses” the Multicast Service Profile, the NE drops the “IGMP join” message.
4. As the NE receives an “IGMP leave” message or the ‘response-time’ expires, the NE will remove that xDSL interface from the corresponding multicast forwarding table.

Follow the subsequent procedures to configure the IGMP snooping and IGMP proxy related parameters.

Click Configuration → xDSL → IGMP Snooping / Proxy on **Main Menu** to open the **IGMP Snooping / IGMP Proxy Setting** Dialog as shown in Figure 7-22 and Table 7-11 depicts the related parameters.

Figure 7-22 IGMP Snooping / IGMP Proxy Setting Dialog

IGMP Setting

Administrative State: ☐ Disable ☒ Enable Snooping ☐ Enable Proxy

Query Version: ☒ IGMPv2 ☐ IGMPv3 ☐ Auto

Report / Leave Version: ☐ IGMPv2 ☒ IGMPv3 ☐ Auto

IGMP Snooping Settings

Aging Time: 30 seconds

Query Response Interval: 100 1/10 seconds

Query Retries: 2

Immediate Leave: ☒

IGMP Proxy Settings

Query Response Interval: 30 1/10 seconds

Query Retries: 3

Immediate Leave: ☐

OK Cancel

Table 7-11 IGMP Proxy Setting Dialog Description

Field	Description
IGMP Setting → Administrator State	
Disable	This disables the IGMP Snooping and Proxy functionality.
Enable Snooping	This enables the IGMP Snooping functionality. (Default)
Enable Proxy	This enables the IGMP Proxy functionality.
IGMP Setting → Query Version	
IGMP Setting → Report/Leave Version	
IGMPv2	This indicates to force the NE to launch the IGMP packets of version 2 no matter what version of IGMP packet it receives
IGMPv3	This indicates to force the NE to launch the IGMP packets of version 3 no matter what version of IGMP packet it receives
Auto	This indicates to launch/relay the IGMP packets of version the same as the version of IGMP packet it receives.
IGMP Snooping Setting	
Aging Time	This specifies the aging time of snooped legal multicast group MAC address. Available value is 1 ~ 600 (seconds).
Query Response Interval	This specifies the period between the NE send 2 consecutive IGMP queries to the xDSL subscriber. Available value is 1 ~ 6000 (1/10 seconds).
Query Retries	This specifies the IGMP Robustness retry times. Available value is 1 ~ 5 (times).
Immediate Leave	Check the check box to enable the immediate leave function.
IGMP Proxy Setting	
Query Response Interval	This specifies the period between the NE send 2 consecutive IGM queries to the xDSL subscriber. Available value is 1 ~ 6000 (1/10 seconds).
Query Retries	This specifies the IGMP Robustness retry times. Available value is 1 ~ 5 (times).
Immediate Leave	Check the check box to enable the immediate leave function.



- If “Immediate Leave” is enabled:
The NE will stop forwarding the multicast stream once it receives the corresponding IGMP “leave” packet. That is, the TV image should be “freezed” immediately
- If “Immediate Leave” is disabled:
The NE will react on the received IGMP “leave” packet and start the “leave” process as follows.
 1. The NE will re-send the “IGMP query” packet ‘Robustness (Query Retry)’ times if it does not receive “IGMP join”.
 2. The time interval between 2 consecutive “IGMP query” packets is ‘Query Response Interval’ seconds.
 3. During the of “leave” process, if the NE receives the corresponding “IGMP join” packet, it continues to forward the multicast stream and stops the “leave” process.
 4. At the end of “leave” process, the NE will stop forwarding the multicast stream if it does not receive any “IGMP join” packet.

System Services Configuration

The system services configuration covers the following settings.

- MAC Aging for Bridged Services
- VLAN MAC Limit
- DHCP Service Configuration
- PPPoE Sub-option Configuration
- xDSL Port Agent ID

MAC Aging for Bridged Services

The MAC aging time sets the lifetime for the learned MAC address. A specific MAC address will be dropped when aging out until it get learning again.

Click Configuration → NE Mangement → MAC Aging on **Main Menu** to open the **MAC Aging** Dialog as shown in Figure 7-23 and Table 7-12 depicts the related parameters.

Figure 7-23 MAC Aging Setting Dialog



Table 7-12 MAC Aging Setting Dialog Description

Field	Description
Unicast MAC Aging	
Aging Time (seconds)	This specifies the MAC aging time. Default value is 300 seconds. The valid range: 10 ~ 1000.

VLAN MAC Limit

To limit the number of source MAC address learned in a specific VLAN, the users can enable the MAC limiting function and configure the upper limit of allowed MAC for a specific VLAN.

Follow the subsequent procedure to set the VLAN MAC limitation related parameters.

- Step 1** Click Configuration → xDSL → VLAN MAC Limit on **Main Menu** to open the **VLAN MAC Limit** Dialog as shown in Figure 7-24 and Table 7-13 depicts the related parameters.

Figure 7-24 VLAN MAC Limit List Dialog

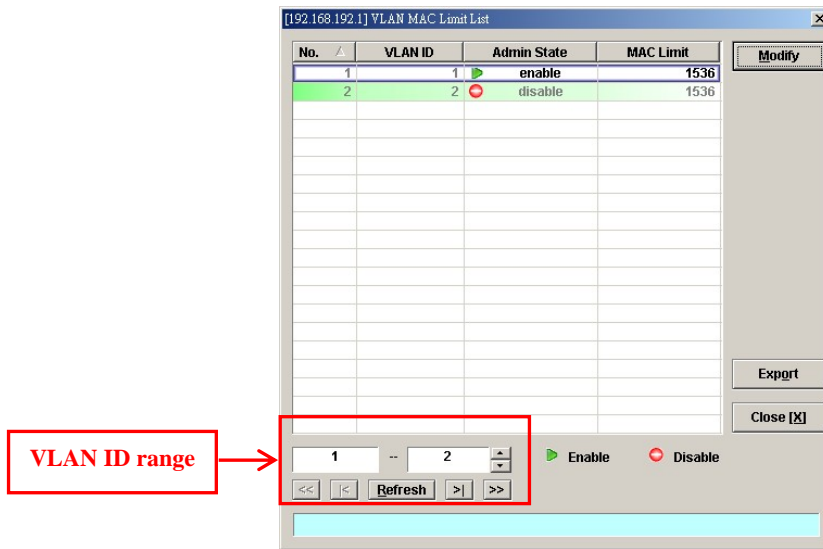


Table 7-13 VLAN MAC Limit List Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
VLAN ID	It specifies the VLAN.
Admin State	It specifies the administrative state.
MAC Limit	It specifies the number of MACs allowed for the corresponding VC-to-VLAN connection.
VLAN ID Range	
Range	Specify the range of VLAN ID as indicated by the red rectangle.
Function Button	
Modify	Click this button to open the MAC limit configure dialog.
Export	Click this button to save the contents of VLAN MAC Limit List to the Personal Computer.
Close	Exit the VLAN MAC Limit List Dialog.
Refresh	Click this button to display the List Table with configured VLAN ID range.

Step 2 Click 'Modify' button to launch the **VLAN MAC Limit Configure Dialog**. Figure 7-25 shows **VLAN MAC Limit Configure Dialog**, and Table 7-14 depicts the related parameters.

Figure 7-25 VLAN MAC Limit Configure Dialog

Table 7-14 VLAN MAC Limit Setting Dialog Description

Field	Description
MAC Limit (Modify)	
VLAN ID	It specifies the VLAN.
Administrative State	Enable or disable the MAC limit function. Default state is “disable”.
MAC Limit	This specifies the number of MAC allowed for the VLAN, from 5 ~ 50000. Default value is 12288.

DHCP Service Configuration

Four dialogs are related to the DHCP Service Configuration.

- DHCP Setting
- DHCP Server List for DHCP Relay
- DHCP Broadcast Control

DHCP Setting

The DHCP relay intercepts the DHCP request packets from subscriber interface and forwards them to the specified DHCP server. In the opposite direction, the DHCP relay transfers the DHCP reply packets from DHCP server to the specified xDSL subscriber.



The setting of DHCP option 82 contents is performed by configuring the xDSL Port Agent ID

Follow the subsequent procedures to configure the related parameters.

Click Configuration → xDSL → DHCP → DHCP Setting on **Main Menu** to open the **DHCP Setting** Dialog as shown in Figure 7-26 and Table 7-15 depicts the related parameters.

Figure 7-26 DHCP Setting Dialog

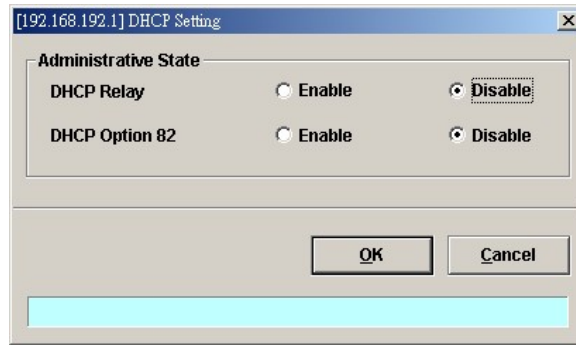


Table 7-15 DHCP Setting Dialog Description

Field	Description
DHCP Relay	Enable or disable the DHCP Relay function.
DHCP Option82	Enable or disable the DHCP option 82 function. Enable: The relayed DHCP packet is to be appended with the configured DHCP option 82 information as specified in the xDSL Port Agent ID List

DHCP Server List for DHCP Relay

Click Configuration → xDSL → DHCP → DHCP Server for DHCP Relay on **Main Menu** to open the **DHCP Server List for DHCP Relay** Dialog as shown in Figure 7-27 and Table 7-16 depicts the related parameters.

Figure 7-27 DHCP Server List for DHCP Relay Dialog

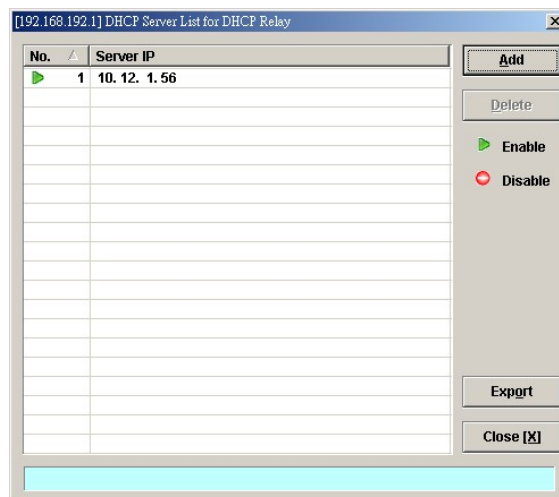


Table 7-16 DHCP Server List for DHCP Relay Dialog Description

Field	Description
Table List	
No.	This indicates the serial number of entry of the List.
Server IP	This specifies the DHCP server IP address.
Function Button	
Add	Click this button to add a new DHCP server IP address.
Delete	Click this button to delete a specified DHCP server.
Export	Click this button to save the contents of DHCP Server List to the Personal Computer.
Close	Exit the DHCP Server List for DHCP Relay table dialog.

DHCP Broadcast Control

Users can set the DHCP broadcast packet rate limit and set the action applied to the out-of-profile traffic on a per NE basis.

Click Configuration → xDSL → DHCP → DHCP Broadcast Control on **Main Menu** to open the **DHCP Broadcast Control s** Dialog as shown in Figure 7-28. Table 7-17 depicts the related parameters.

Figure 7-28 DHCP Broadcast Control Dialog

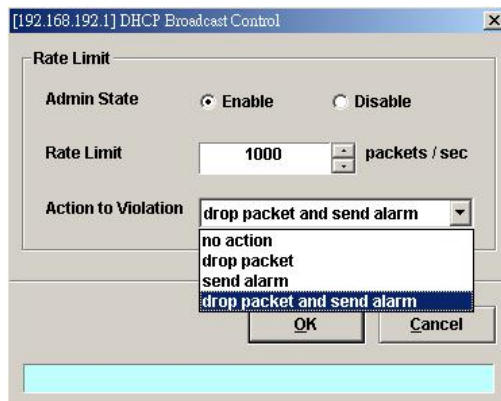


Table 7-17 DHCP Broadcast Control Dialog - Description

Field	Description
Rate Limit	
Admin State	Enable or disable the DHCP broadcast control. The default setting is “disable”.
Rate Limit	This specifies the rate limit based on packets per second. Available value is 1 ~ 100000 (packet per second). Default value is 100 packets per second.
Action to Violation	This specifies the action to be taken for the packets over the limit. “No action”, “Drop packet”, “Send alarm” and “Drop packet and send alarm”.



When the action is set to be either “Send alarm” and “Drop packet and send alarm”, the NE will launch SNMP traps to the SNMP trap managers as specified in the section “Configuring the SNMP Trap Manager” in Chap 4.

PPPoE Sub-option Configuration

PPPoE sub-option has similar mechanism as DHCP option 82. The NE can insert Circuit ID and Remote ID in all upstream PPPoE discovery stage packets, i.e. the PADI, PADR and upstream PADT packets. Figure 7-29 illustrates the enable/disable window for this functionality.



The setting of PPPoE sub-option contents is performed by configuring the xDSL Port Agent ID

Follow the subsequent procedures to configure the related parameters.

Click Configuration → xDSL → PPPoE on **Main Menu** to open the **PPPoE setting** Dialog as shown in Figure 7-29 and Table 7-18 depicts the related parameters.

Figure 7-29 PPPoE Sub-option Setting Dialog



Table 7-18 PPPoE Sub-option Setting Dialog Description

Field	Description
Administrative State	
PPPoE Sub-option 1 & 2	<p>Enable or disable the PPPoE sub-option function.</p> <p>Enable: The relayed PPPoE packet is to be appended with the configured PPPoE Sub-option 1 & 2 information as specified in the xDSL Port Agent ID List</p> <p>Default value is “Disable”.</p>

xDSL Port Agent ID Management

The xDSL Port Agent ID List keeps the Agent Circuit ID (intended for circuits terminated by the system hosting the Relay agent) and Agent Remote ID (intended to identify the remote host end of a circuit). The NE allows the operator to specify Agent Remote ID with an ASCII string of up to 63 characters. As to the Agent Circuit ID, it is not permitted to be modified. The format of Agent Circuit ID is as follows.

“NE-InbandIP-userSrcMAC atm slot-port:VPI.VCI”

Here is one example Agent Agent Circuit ID

“IP_DSLAM-100.168.3.97-00:11:d8:80:93:23 atm 3-1:100.33”,

which represents

NE’s inband IP=100.168.3.97,

MAC address of subscriber’s personal computer (or the CPE)= 00:11:d8:80:93:23,
slot = 3, port = 1, vpi = 100, vci = 33.



xDSL Port Agent ID is to be inserted into either all upstream DHCP messages sent by the client and all upstream PPPoE discovery stage packets

Follow the subsequent procedures to configure the xDSL Port Agent ID.

- Step 1** Click Configuration → xDSL → Port Agent ID on **Main Menu** to open the **xDSL Port Agent IDs** Dialog as shown in Figure 7-30 and Table 7-19 depicts the related parameters. To modify the
- Step 2** Click and highlight a row and click ‘**Modify**’ button to modify the Agent Remote ID.

Figure 7-30 xDSL Port Agent ID List

No.	Slot-Port	Agent Circuit ID	Agent Remote ID
1	LC1-1	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/1:0.0	
2	LC1-2	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/2:0.0	
3	LC1-3	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/3:0.0	
4	LC1-4	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/4:0.0	
5	LC1-5	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/5:0.0	
6	LC1-6	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/6:0.0	
7	LC1-7	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/7:0.0	
8	LC1-8	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/8:0.0	
9	LC1-9	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/9:0.0	
10	LC1-10	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/10:0.0	
11	LC1-11	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/11:0.0	
12	LC1-12	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/12:0.0	
13	LC1-13	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/13:0.0	
14	LC1-14	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/14:0.0	
15	LC1-15	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/15:0.0	
16	LC1-16	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/16:0.0	
17	LC1-17	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/17:0.0	
18	LC1-18	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/18:0.0	
19	LC1-19	IP_DSLAM-100.168.1.31-00:00:00:00:00:00 atm 1/19:0.0	

Table 7-19 xDSL Port Agent IDs Dialog Description

Field	Description
Table List	
No,	This indicates the number of Table List.
Slot-Port	This indicates the slot-port address.
Agent Circuit ID	This indicates the agent circuit ID of the specified xDSL subscriber. Its format is as follows. “NE-InbandIP-userSrcMAC atm slot-port:VPI.VCI”
Agent Remote ID	This indicates the agent remote ID of the specified xDSL subscriber. It is an ASCII string of up to 63 characters.
Function Button	
Modify	Click this button to modify the selected xDSL port’s agent ID.
Export	Click this button to save the contents of xDSL Port Agent ID List to the Personal Computer.
Close	Exit the xDSL Port Agent ID List Dialog.

Chapter 8 Fast Provision Management

This chapter describes the Fast Provision function. Through this function, you are able to efficiently apply the profiles to a mass of xDSL subscriber ports.

This chapter contains the following sections:

- Interface and VC-VLAN Fast Provisioning
- Multicast Service Fast Provisioning

Interface and VC-VLAN Fast Provisioning

The NCT192 provides a fast provision function that helps you to build-up the principal connection setting of interface ports in fast and efficient way. Through this function, you can apply the profile and VC-to-VLAN setting to a mass of xDSL subscriber interfaces simultaneously, instead of configuring the individual subscriber interfaces one by one.

Follow the subsequent procedure to configure the interface fast provision.

Step 1 Click Configuration → xDSL → Fast Provision → Port & VC-to-VLAN on **Main Menu** to open the **xDSL Port & VC-to-VLAN Fast Provision** Dialog as shown in Figure 8-1.

Note that the configuration tabs are not exact the same for the RFC2684 bridged mode and routed mode. Figure 8-1 ~ Figure 8-7 show the corresponding configuration dialogs. Click either one tab to launch the corresponding dialog to configure the parameters. As to the description of the configuration parameters, please refer to Table 8-1.



It is noted that the configuration dialog may be different between the RFC2684 bridged mode and routed mode. If the configuration dialogs are the same for both the bridged mode and routed mode, Figure 8-1 ~ Figure 8-7 only show the ones in the bridged mode without any additional description. Otherwise, Figure 8-1 ~ Figure 8-7 show the configuration dialogs with description to indicate it. The rule of description also applies to Table 8-1.

Figure 8-1 xDSL Port & VC-to-VLAN Fast Provision – Port Setting Dialog

Module Criteria

	From	To
Shelf	1	1
Slot	LC1	LC1
Type	NCT1901 ADSLx48 Board	
RFC2684 Mode	bridged	

Port Setting | Channel Setting | MAC Limit | IP Traffic Profile | 802.1Q

Admin State: ☒ Enable ☐ Disable

Line Profile: <none> [Show]

PM Threshold: <none> [Show]

Traffic Policing: <none> [Show]

[List] [Cancel]

Figure 8-2 xDSL Port & VC-to-VLAN Fast Provision – Channel Setting Dialog

Module Criteria

	From	To
Shelf	1	1
Slot	LC1	LC1
Type	NCT1901 ADSLx48 Board	
RFC2684 Mode	bridged	

Port Setting | Channel Setting | MAC Limit | IP Traffic Profile | 802.1Q

Admin State: ☒ Enable ☐ Disable

VPI: 0 [Start] [Increment]

VCI: 32 [Start] [Increment]

VLAN ID: 1 [Start] [Increment]

PVCs / Port: 1 [Start] [Increment]

VLAN ID is continuous among ports: ☐

[List] [Cancel]

(a) Channel setting in RFC2684 bridged mode

Module Criteria

	From	To
Shelf	1	1
Slot	LC1	LC1
Type	NCT1901 ADSLx48 Board	
RFC2684 Mode	routed	

Port Setting | Channel Setting | IP Traffic Profile | 802.1Q | Next-h

Admin State: ☒ Enable ☐ Disable

VPI: 0 [Start] [Increment]

VCI: 32 [Start] [Increment]

PVCs / Port: 1 [Start] [Increment]

[List] [Cancel]

(b) Channel setting in RFC2684 routed mode

Figure 8-3 xDSL Port & VC-to-VLAN Fast Provision – IP Traffic Dialog

The screenshot shows a dialog box titled "[192.168.192.1] xDSL Port & VC-to-VLAN Fast Provision". It has a tabbed interface with tabs for "Port Setting", "Channel Setting", "MAC Limit", "IP Traffic Profile", and "802". The "IP Traffic Profile" tab is selected. Under "Module Criteria", the "From" and "To" columns are both set to "1" for Shelf, "LC1" for Slot, "NCT1901 ADSLx48 Board" for Type, and "bridged" for RFC2684 Mode. In the "IP Traffic Profile" section, the "IP Traffic Profile" dropdown is set to "ADSL_TRAF" and the "Show" button is visible. At the bottom, there are "List" and "Cancel" buttons.

Figure 8-4 xDSL Port & VC-to-VLAN Fast Provision – MAC Limit Dialog (only for the RFC2684 bridged mode)

The screenshot shows the same dialog box as Figure 8-3, but with the "MAC Limit" tab selected. The "Module Criteria" are the same. In the "MAC Limit" section, the "MAC Count" is set to "1" and the "Non-aged" radio button is selected under the "Enable" group. The "Disable" radio button is also visible. At the bottom, there are "List" and "Cancel" buttons.

Figure 8-5 xDSL Port & VC-to-VLAN Fast Provision – Next-hop Dialog (only for the RFC2684 routed mode)

The dialog box is titled "[192.168.192.1] xDSL Port & VC-to-VLAN Fast Provision". It features a "Module Criteria" section with the following fields:

	From	To
Shelf	1	1
Slot	LC1	LC1
Type	NCT1901 ADSLx48 Board	
RFC2684 Mode	routed	

Below the criteria is a tabbed interface with "Channel Setting", "IP Traffic Profile", "802.1P", "Next-hop", and "Service Ty". The "Next-hop" tab is active, showing a "Next-hop Name" dropdown set to "SeedNet" and a "Show" button. At the bottom are "List" and "Cancel" buttons.

Figure 8-6 xDSL Port & VC-to-VLAN Fast Provision – 802.1P Dialog

The dialog box is titled "[192.168.192.1] xDSL Port & VC-to-VLAN Fast Provision". It features a "Module Criteria" section with the following fields:

	From	To
Shelf	1	1
Slot	LC1	LC1
Type	NCT1901 ADSLx48 Board	
RFC2684 Mode	bridged	

Below the criteria is a tabbed interface with "Channel Setting", "MAC Limit", "IP Traffic Profile", "802.1P", and "Service 1". The "802.1P" tab is active, showing a "User Priority" spinner set to 0. At the bottom are "List" and "Cancel" buttons.

Figure 8-7 xDSL Port & VC-to-VLAN Fast Provision – Service Type Dialog

The dialog box is titled "[192.168.192.1] xDSL Port & VC-to-VLAN Fast Provision". It has a "Module Criteria" section with fields for "Shelf" (1), "Slot" (LC1), "Type" (NCT1901 ADSLx48 Board), and "RFC2684 Mode" (bridged). Below this is a tabbed interface with "IP Traffic Profile", "802.1P", "MAC Limit", and "Service Type" tabs. The "Service Type" tab is active, showing "Service Type" (PPPoE), "Maximum IP Count" (1), "Static IP's Base Address" (11 . 21 . 33 . 0), and "IP Address Increment / Port" (1). At the bottom are "List" and "Cancel" buttons.

(a) PPPoE service in RFC2684 bridged mode

The dialog box is titled "[192.168.192.1] xDSL Port & VC-to-VLAN Fast Provision". It has a "Module Criteria" section with fields for "Shelf" (1), "Slot" (LC1), "Type" (NCT1901 ADSLx48 Board), and "RFC2684 Mode" (bridged). Below this is a tabbed interface with "IP Traffic Profile", "802.1P", "MAC Limit", and "Service Type" tabs. The "Service Type" tab is active, showing "Service Type" (DHCP), "Maximum IP Count" (1), "Static IP's Base Address" (11 . 21 . 33 . 0), and "IP Address Increment / Port" (1). At the bottom are "List" and "Cancel" buttons.

(b) DHCP service in RFC2684 bridged mode

The dialog box is titled "[192.168.192.1] xDSL Port & VC-to-VLAN Fast Provision". It has a "Module Criteria" section with fields for "Shelf" (1), "Slot" (LC1), "Type" (NCT1901 ADSLx48 Board), and "RFC2684 Mode" (bridged). Below this is a tabbed interface with "IP Traffic Profile", "802.1P", "MAC Limit", and "Service Type" tabs. The "Service Type" tab is active, showing "Service Type" (static IP), "Continuous IP Count" (1), "Static IP's Base Address" (11 . 21 . 33 . 0), and "IP Address Increment / Port" (1). At the bottom are "List" and "Cancel" buttons.

(c) Static IP service in RFC2684 bridged mode

The dialog box is titled "[192.168.192.1] xDSL Port & VC-to-VLAN Fast Provision". It has a "Module Criteria" section with fields for "Shelf" (1), "Slot" (LC1), "Type" (NCT1901 ADSLx48 Board), and "RFC2684 Mode" (routed). Below this is a tabbed interface with "IP Traffic Profile", "802.1P", "Next-hop", and "Service Type" tabs. The "Service Type" tab is active, showing "Service Type" (static IP), "Continuous IP Count" (1), "Static IP's Base Address" (11 . 21 . 33 . 0), and "IP Address Increment / Port" (1). At the bottom are "List" and "Cancel" buttons.

(d) Static IP service in RFC2684 routed mode

Table 8-1 xDSL Port & VC-to-VLAN Fast Provision Description

Field	Description
Module Criteria	
Shelf	This specifies the location of shelf. It is obsolete in the current release.
Slot	It specifies the location of the line card.
Type	It specifies the board type of line card.
RFC2684 Mode	It specifies the RFC 2684 encapsulation mode (Bridged or Routed mode)
Port Setting Dialog	
Admin State	It specifies the administrative state. (enable or disable)
Line Profile	It specifies the line profile. (xDSL Profile)
PM Threshold	It specifies the PM threshold profile.
Traffic Policing	It specifies the Traffic Policing profile. [Only for the ADSL port]
Channel Setting Dialog	
Start – Identify the number of starting value.	
Increment – Identify the number to be increment if more then one PVCs / Port is defined.	
Admin State	It specifies the administrative state. (enable or disable)
VPI (Start, Increment)	It specifies the VPI value of PVCs.
VCI (Start, Increment)	It specifies the VCI value of PVCs.
VLAN ID (Start, Increment)	It specifies the VLAN ID value of corresponding VC-to-VLAN connections.
PVCs / Port	It specifies the number of PVCs to be applied to each xDSL port.
VLAN ID is continuous among port	Check to sequentially increase the VLAN ID values to be assigned to the PVCs.
IP Traffic Profile Dialog	
IP Traffic Profile	This specifies the IP Traffic Profile of corresponding VC-to-VLAN connection.
802.1P Dialog	
User Priority	This specifies the VLAN priority of corresponding VC-to-VLAN connection.
Next-hop Dialog [only for RFC2684 routed mode]	
Next-hop Name	It specifies the next-hop name as specified in the section ‘ISP Information for IP over ATM’ of Chapter 7.
MAC Limit Dialog [only for RFC2684 bridged mode]	
MAC Count	It specifies the number of subscriber’s MACs allowed for the corresponding VC-to-VLAN connection.

Table 8-1 xDSL Port & VC-to-VLAN Fast Provision Description (Continued)

Field	Description
Service Type Dialog	
Service Type	This specifies the service type to be allowed on the PVC of individual subscriber. The following three service types are supported now. <ul style="list-style-type: none"> ● PPPoE ● DHCP ● Static IP
Maximum IP Count [only for DHCP Service]	This indicates the number of IP to be allowed while DHCP is selected
Continuous IP Count [only for Static IP Service]	This indicates the number of IP to be allowed while Static IP is selected
Static IP's Basic Address [only for Static IP Service]	This specifies the base of the IP address if the service type is Static IP
IP Address Increment/Port [only for Static IP Service]	This indicates the increment of IP address between two consecutive ports while Static IP is selected and Continuous IP Count is greater than 1.



Enabling the Service Type Control makes the NE to provide the IP/MAC anti spoofing function.

- **In the case that the subscriber acquires his IP address dynamically via PPPoE**
The NE will block the subscriber's traffic before a valid IP address assignment. Once the subscriber possesses a valid dynamic IP, the NE will just forward the packet of valid source MAC addresses. In other words, the NE drops the subscriber's traffic of invalid source MAC addresses
- **In the case that the subscriber acquires his IP address dynamically via DHCP**
The NE will block the subscriber's traffic before a valid IP address assignment. Once the subscriber possesses a valid dynamic IP, the NE will just forward the packet of valid source IP/MAC addresses. In other words, the NE drops the subscriber's traffic of invalid source IP/MAC addresses.
- **In the case that the subscriber possesses static IP address**
The NE will just forward the packet of valid source IP/MAC addresses. In other words, the NE drops the subscriber's traffic of invalid source IP/MAC addresses.



Whenever the service type is specified as "Static IP Service", it is noted that the following relationship should be maintained.

IP Address Increment/Port \geq Continuous IP Count

Step 2 Click 'List' button to launch the **xDSL Fast Provision List** dialog. Figure 8-8 summarizes what you set via the **xDSL Port & VC-to-VLAN Fast Provision** dialog. As shown in Figure 8-8, it depicts the list of subscriber ports you wish to apply to. If you do not want to apply the setting to any port or PVC, just remove it from the List Table by clearing the corresponding check-box.

Table 8-2 depicts the related parameters.

Step 3 Click 'Go' button to apply the given setting to all ports in the List Table. The checks are removed when the setting is successfully applied. Click 'Stop' to stop the fast provisioning immediately if you want.

Figure 8-8 xDSL Fast Provision List Dialog

[192.168.192.1] NCT1901 ADSLx48 Board - Fast Provision List

☒ Port Setting

Administrative State
enable

Line Profile

PM Threshold Profile

Traffic Policing Profile

☒ VC-to-VLAN

Administrative State
enable

Encapsulation Mode
bridged

User Priority
0

IP Traffic Profile
ADSL_TRAF

MAC Count Limit
1

Service Type
PPPoE

No.	Slot-Port	VPI	VCI	VLAN / Next-hop	Base IP / Count
1	LC1-1	0	32		1
2	LC1-2	0	32		1
3	LC1-3	0	32		1
4	LC1-4	0	32		1
5	LC1-5	0	32		1
6	LC1-6	0	32		1
7	LC1-7	0	32		1
8	LC1-8	0	32		1
9	LC1-9	0	32		1
10	LC1-10	0	32		1
11	LC1-11	0	32		1
12	LC1-12	0	32		1
13	LC1-13	0	32		1
14	LC1-14	0	32		1
15	LC1-15	0	32		1
16	LC1-16	0	32		1
17	LC1-17	0	32		1

Go Stop Export Close [X]

(a) List Dialog in the RFC2684 bridged mode

[192.168.192.1] NCT1901 ADSLx48 Board - Fast Provision List

☒ Port Setting

Administrative State
enable

Line Profile

PM Threshold Profile

Traffic Policing Profile

☒ VC-to-VLAN

Administrative State
enable

Encapsulation Mode
routed

User Priority
0

IP Traffic Profile
ADSL_TRAF

MAC Count Limit
1

Service Type
Static IP

No.	Slot-Port	VPI	VCI	VLAN / Next-hop	Base IP / Count
1	LC1-1	0	32	PCa	0.0.1.1 / 1
2	LC1-2	0	32	PCa	0.0.1.2 / 1
3	LC1-3	0	32	PCa	0.0.1.3 / 1
4	LC1-4	0	32	PCa	0.0.1.4 / 1
5	LC1-5	0	32	PCa	0.0.1.5 / 1
6	LC1-6	0	32	PCa	0.0.1.6 / 1
7	LC1-7	0	32	PCa	0.0.1.7 / 1
8	LC1-8	0	32	PCa	0.0.1.8 / 1
9	LC1-9	0	32	PCa	0.0.1.9 / 1
10	LC1-10	0	32	PCa	0.0.1.10 / 1
11	LC1-11	0	32	PCa	0.0.1.11 / 1
12	LC1-12	0	32	PCa	0.0.1.12 / 1
13	LC1-13	0	32	PCa	0.0.1.13 / 1
14	LC1-14	0	32	PCa	0.0.1.14 / 1
15	LC1-15	0	32	PCa	0.0.1.15 / 1
16	LC1-16	0	32	PCa	0.0.1.16 / 1
17	LC1-17	0	32	PCa	0.0.1.17 / 1

Go Stop Export Close [X]

(b) List Dialog in the RFC2684 routed mode

Table 8-2 xDSL Fast Provision List Dialog Description

Field	Description
Condition	
Port Setting – Check to allow the correspondent setting to be applied to the ports in List Table.	
VC-to-VLAN – Check to allow the correspondent setting to be applied to the ports in List Table.	
Administrative State	This specifies the administrative state. (enable or disable)
Line Profile	This specifies the line profile. (xDSL Profile)
PM Threshold Profile	This specifies the PM threshold profile.
Traffic Policing Profile	This specifies the Traffic Policing profile. [Only for the ADSL port]
Encapsulation Mode	This specifies the RFC2684 encapsulation mode of corresponding PVC.
User Priority	This specifies the VLAN priority of corresponding VC-to-VLAN connection.
IP Traffic Profile	This specifies the IP traffic profile of corresponding VC-to-VLAN connection.
MAC Count Limit	It specifies the number of subscriber's MACs allowed for the corresponding VC-to-VLAN connection. [only for RFC2684 bridged mode]
Service Type	This specifies the service type of corresponding VC-to-VLAN connection. The following three service types are supported now. <ul style="list-style-type: none"> ● PPPoE ● DHCP ● Static IP
List Table	
No.	This indicates the serial number of entry of the List Table.
Slot-Port	This specifies the location of subscriber port.
VPI	This specifies the VPI value of PVC.
VCI	This specifies the VCI value of PVC.
VLAN / Next-hop	This specifies the VLAN ID (in RFC2684 bridged mode) or Next-hop name (in RFC2684 routed mode) of corresponding VC-to-VLAN connection.
Base IP / Count	This specifies the IP Base address and count of IP address of corresponding VC-to-VLAN connection. It applies whenever the Service Type Control is enabled and Static IP or DHCP is selected
Function Button	
Go	Click this button to start fast provisioning.
Stop	Click this button to force the fast provision terminating.
Export	Click this button to save the contents of xDSL Fast Provision List to the Personal Computer.
Close	Exit this xDSL Fast Provision List Dialog.

Multicast Service Fast Provisioning

The multicast service fast provision function helps you to build-up the multicast connection and the associated service profile efficiently.

Follow the subsequent procedures to configure the multicast service fast provision.

Step 1 Click Configuration → xDSL → Fast Provision → Multicast Channel on **Main Menu** to open the **xDSL Multicast Channel Fast Provision** Dialog, as shown in Figure 8-9 and Table 8-3 depicts the related parameters.

In Figure 8-9, it is noted that two individual tabs (Multicast Service Profile and Channel Limit) are provided to set the Multicast Service Fast Provision related parameters. Figure 8-9 ~ Figure 8-10 show the corresponding configuration Dialog. Click either one tab to launch the corresponding dialog to configure the parameters. As to the description of the configuration parameters, please refer to Table 8-3.

Figure 8-9 xDSL Multicast Channel Fast Provision – Multicast Service Profile Dialog

The screenshot shows the 'xDSL Multicast Channel Fast Provision' dialog box. The title bar indicates the IP address [192.168.192.1]. The dialog is divided into two main sections. The top section, titled 'Ethernet over ATM', contains fields for 'From' and 'To' (Shelf, Slot, Type, VPI, VCI, VLAN ID) and an 'Admin State' (Enable/Disable). The bottom section, titled 'Multicast Service Profile', has a 'Profile' dropdown menu set to 'ms83100' and a 'Show' button. At the bottom of the dialog are 'List' and 'Cancel' buttons.

Figure 8-10 xDSL Multicast Channel Fast Provision – Channel Limit Dialog

The screenshot shows the 'xDSL Multicast Channel Fast Provision' dialog box, with the 'Channel Limit' tab selected. The top section, titled 'Ethernet over ATM', contains fields for 'From' and 'To' (Shelf, Slot, Type, VPI, VCI, VLAN ID) and an 'Admin State' (Enable/Disable). The bottom section, titled 'Channel Limit', has a 'Channel Limit' dropdown menu set to '1' and a 'Show' button. At the bottom of the dialog are 'List' and 'Cancel' buttons.

Table 8-3 xDSL Multicast Channel Fast Provision Description

Field	Description
Ethernet over ATM	
Shelf	This specifies the shelf ID.
Slot	It specifies the slot range.
Type	It specifies the LC board type.
VPI	It specifies the VPI value.
VCI	It specifies the VCI value.
VLAN ID	It specifies the VLAN ID value.
Admin State	Enable: Apply the specified multicast setting to the indicated PVCs Disable: Do not apply specified multicast setting to the indicated PVCs
Multicast Service Profile Dialog	
Show – Click this button to display the details of multicast service profile collocated.	
Profile	It specifies the Multicast Service Profile
Channel Limit Dialog	
Channel Limit	This specifies the allowed number of concurrent multicast streams to be forwarded via each VC-to-VLAN connection.

Step 2 Click 'List' button to launch the **xDSL Multicast Channel Fast Provision List** dialog. Figure 8-11 summarizes what you set via the **xDSL Multicast Channel Fast Provision** dialog. As shown in Figure 8-11, it depicts the list of subscriber ports you wish to apply to. If you do not want to apply the setting to any port in the list table, just clear the corresponding check-box

Table 8-4 depicts the related parameters.

Step 3 Click 'Go' button to apply the given setting to all ports listing in the List Table. The checks are removed when the setting is successfully applied. Click 'Stop' to stop the fast provision immediately if you want.

Figure 8-11 xDSL Multicast Channel Fast Provision List Dialog

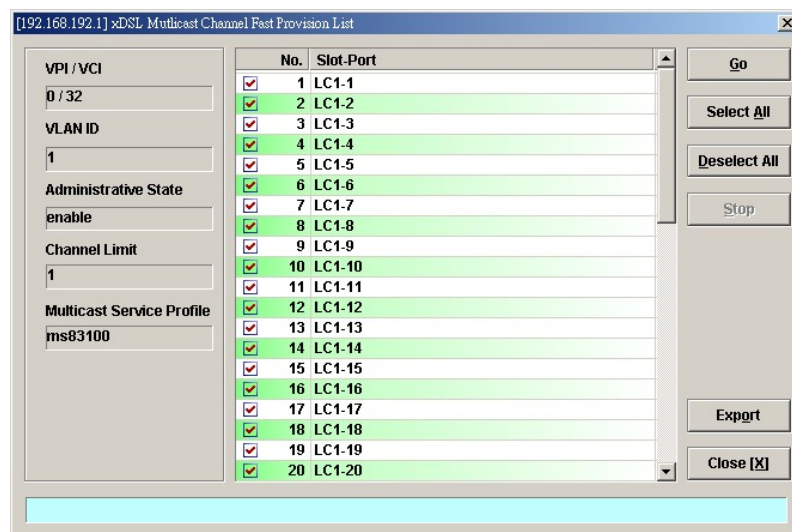


Table 8-4 xDSL Multicast Channel Fast Provision List Dialog Description

Field	Description
Condition	
VPI / VCI	This specifies the VPI / VCI value of corresponding PVC.
VLAN ID	This specifies the VLAN ID value of corresponding VC-to-VLAN connection.
Administrative State	Enable: Apply the specified multicast setting to the indicated PVCs Disable: Do not apply specified multicast setting to the indicated PVCs
Channel Limit	This specifies the allowed number of multicast streams to be forwarded via each VC-to-VLAN connection.
Multicast Service Profile	This specifies the multicast service profile.
List Table	
No.	This indicates the serial number of entry of the List Table.
Slot-Port	This specifies the location of subscriber port.
Function Button	
Go	Click this button to start fast provisioning.
Select All	Click this button to select all rows from List Table.
Deselect All	Click this button to deselect all rows from List Table
Stop	Click this button to force the fast provision terminating.
Export	Click this button to save the contents of xDSL Multicast Channel Fast Provision List to the Personal Computer.
Close	Exit the xDSL Multicast Channel Fast Provision List Dialog.

Chapter 9 Performance Management

This chapter describes system performance monitoring and related management.

This chapter contains the following sections:

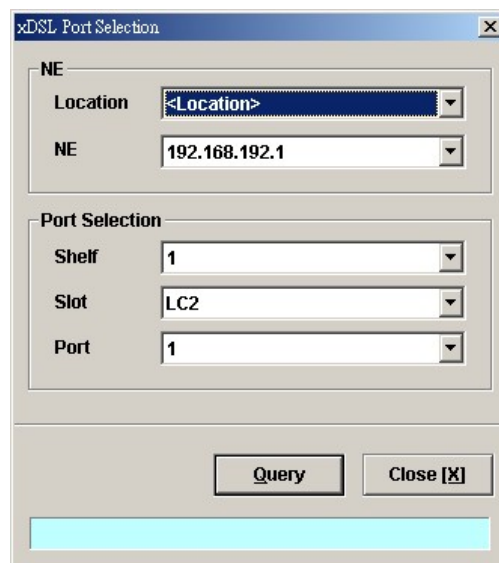
- xDSL Line Current Performance Information
- xDSL Line Historical Performance Information
- GE Interface Performance Statistics

xDSL Line Current Performance Information

Follow the subsequent procedure to obtain data for evaluating the current xDSL line performance.

- Step 1** Click Performance → xDSL Current PM on **Main Menu** to open the **xDSL Current PM Port Selection** Dialog as shown in Figure 9-1.
- Step 2** Select the port you want to show and press Query button to get the current PM data. Depending on the type of selected port, the current PM dialog looks different. Figure 9-2 shows the ADSL Current PM Dialog. The corresponding descriptions are depicted in Table 9-1. As to the SHDSL Current PM Dialog, it is shown in Figure 9-3. The corresponding descriptions are depicted in Table 9-2.

Figure 9-1 xDSL Current PM Port Selection



The image shows a software dialog box titled "xDSL Port Selection". It contains several input fields and buttons. At the top, there is a section for "NE" (Network Element) with a "Location" dropdown menu showing "<Location>" and an "NE" dropdown menu showing "192.168.192.1". Below this is a "Port Selection" section with three dropdown menus: "Shelf" showing "1", "Slot" showing "LC2", and "Port" showing "1". At the bottom of the dialog, there are two buttons: "Query" and "Close [X]". A light blue horizontal bar is visible at the very bottom of the dialog box.

Figure 9-2 ADSL Current PM Dialog

Time Interval	Side	LOSs	ESs	SESs	UASs	Tx Cells / Rate (Kbps)	Rx Cells
Current 15 Min	CO	0	0	0	848	0 / 0.0	
	RT	0	0	0	848	---	
Current 1 Day	CO	0	0	0	24248	0 / 0.0	
	RT	0	0	0	24248	---	
Previous 1 Day	CO	0	0	0	86400	0 / 0.0	
	RT	0	0	0	86400	---	

15Min Elapsed Seconds: 848 / 900 ☐ Auto-Refresh

1-Day Elapsed Seconds: 24248 / 86400

Table 9-1 ADSL Current PM Dialog Description

Field	Description
List Table	
Time Interval	This indicates the PM time interval
Side	This indicates the location where the PM parameters are observed. (Either central side (CO) or remote side (RT))
LOSs	This indicates the count of Loss of Signal Second during the current accumulated period.
ESs	This indicates the count of Error Second during the current accumulated period.
SESs	This indicates the count of Severely Error Second during the current accumulated period.
UASs	This indicates the count of Unavailable Error Second during the current accumulated period.
Tx Cells / Rate (Kbps)	This indicates the transmitted number of ATM cells and net data rate during the current accumulated period.
Rx Cell / Rate (Kbps)	This indicates the received number of ATM cells and net data rate during the current accumulated period.

Table 9-1 ADSL Current PM Dialog Description (Continued)

CVs	This indicates the count of Code Violation during the current accumulated period.
FullInits	This indicates the count of the total number of full initializations attempted on the line (successful and failed) during the current accumulated period.
FailedInits	This indicates the total number of failed full initializations during the current accumulated period. A failed full initialization is when showtime is not reached at the end of the full initialization procedure, e.g., when: <ul style="list-style-type: none"> • A CRC error is detected. • A time-out occurs. • Unexpected message content is received.
TxBlks	This indicates the transmitted number of FEC block during the current accumulated period.
RxBlks	This indicates the received number of FEC block during the current accumulated period.
CrtBlks	This indicates the count of all blocks received with errors that were corrected during the current accumulated period.
UncrtBlks	This indicates the count of all blocks received with uncorrectable errors during the current accumulated period.
Function Button	
Refresh	Click this button to refresh the List Table
Graph	Click this button to draw the 2D/3D diagram
Export	Click this button to save the contents of ADSL Current PM List to the Personal Computer.
Close	Exit the ADSL Current PM Dialog.

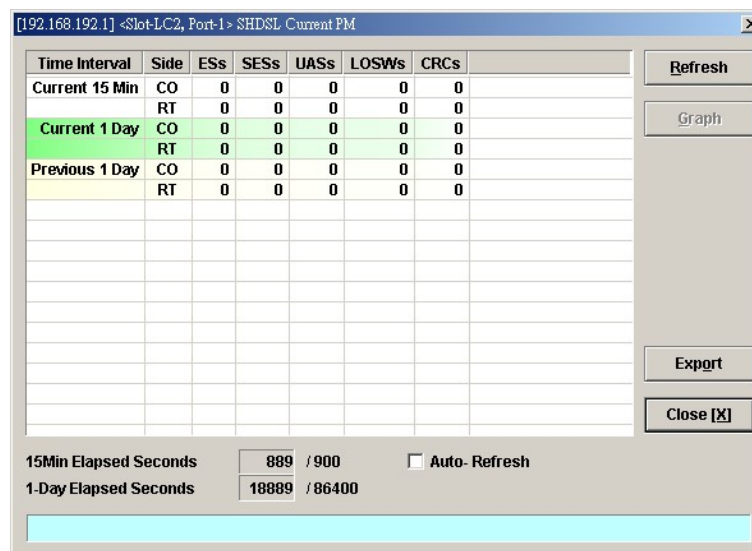
Figure 9-3 SHDSL Current PM Dialog

Table 9-2 SHDSL Current PM Dialog Description

Field	Description
List Table	
Time Interval	This indicates the PM time interval
Side	This indicates the location where the PM parameters are observed. (Either central side (CO) or remote side (RT))
ESs	This indicates the count of Error Second during the current accumulated period.
SESSs	This indicates the count of Severely Error Second during the current accumulated period.
UASs	This indicates the count of Unavailable Error Second during the current accumulated period.
LOSWS	This indicates the count of LOSW second during the current accumulated period.
CRCs	This indicates the count of the SHDSL CRC anomalies occurring during the current accumulation period.
Function Button	
Refresh	Click this button to refresh the List Table
Graph	Click this button to draw the 2D/3D diagram
Export	Click this button to save the contents of SHDSL Current PM List to the Personal Computer.
Close	Exit the SHDSL Current PM Dialog .

xDSL Line Historical Performance Information

Follow the subsequent procedure to obtain data for evaluating the history xDSL line performance.

- Step 1** Click Performance → xDSL History PM on **Main Menu** to open the **xDSL History PM Port Selection** Dialog as shown in Figure 9-4.
- Step 2** Select the port you want to show and press Query button to get the historical PM data. Depending on the type of selected port, the historical PM dialog looks different. Figure 9-5 shows the ADSL History PM Dialog. The corresponding descriptions are depicted in Table 9-3. As to the SHDSL History PM Dialog, it is shown in Figure 9-6. The corresponding descriptions are depicted in Table 9-4.

Figure 9-4 xDSL History Port Selection Dialog

xDSL Port Selection

NE

Location

<Location>

NE

192.168.192.1

Port Selection

Shelf

1

Slot

LC1

Port

1

Query

Close [X]

Figure 9-5 ADSL History PM Dialog

[192.168.192.1] <Slot-LC1, Port-1> ADSL History PM

Create Time	Side	LOSs	ESs	SESs	UASs	TxCells / Rate (Kbps)
10-30 14:45	CO	0	0	0	900	0 / 0.0
10-30 14:45	RT	0	0	0	900	---
10-30 15:00	CO	0	0	0	900	0 / 0.0
10-30 15:00	RT	0	0	0	900	---
10-30 15:15	CO	0	0	0	900	0 / 0.0
10-30 15:15	RT	0	0	0	900	---
10-30 15:30	CO	0	0	0	900	0 / 0.0
10-30 15:30	RT	0	0	0	900	---
10-30 15:45	CO	0	0	0	900	0 / 0.0
10-30 15:45	RT	0	0	0	900	---
10-30 16:00	CO	0	0	0	900	0 / 0.0
10-30 16:00	RT	0	0	0	900	---
10-30 16:15	CO	0	0	0	900	0 / 0.0
10-30 16:15	RT	0	0	0	900	---
10-30 16:30	CO	0	0	0	900	0 / 0.0
10-30 16:30	RT	0	0	0	900	---
10-30 16:45	CO	0	0	0	900	0 / 0.0
10-30 16:45	RT	0	0	0	900	---

Graph

Export

Close [X]

Table 9-3 ADSL History PM Dialog Description

Field	Description
List Table	
Create Time	This indicates the time when the xDSL historical PM is recorded.
Side	This indicates the location where the PM parameters are observed. (Either central side(CO) or remote side(RT))
LOSs	This indicates the count of Loss of Signal Second during the indicated period.
ESs	This indicates the count of Error Second during the indicated period.
SEs	This indicates the count of Severely Error Second during the indicated period.
UASs	This indicates the count of Unavailable Error Second during the indicated period.
Tx Cells / Rate (Kbps)	This indicates the transmitted number of ATM cells and net data rate during the indicated period.
Rx Cell / Rate (Kbps)	This indicates the received number of ATM cells and net data rate during the indicated period.
CVs	This indicates the count of Code Violation during the indicated period.
FullInits	This indicates the count of the total number of full initializations attempted on the line (successful and failed) during the indicated period.
FailedInits	<p>This indicates the total number of failed full initializations during the indicated period.</p> <p>A failed full initialization is when showtime is not reached at the end of the full initialization procedure, e.g., when:</p> <ul style="list-style-type: none"> • A CRC error is detected. • A time-out occurs. • Unexpected message content is received.
Function Button	
Graph	Click this button to draw the 2D/3D diagram
Export	Click this button to save the contents of ADSL History PM to the Personal Computer.
Close	Exit the ADSL History PM Dialog.

Figure 9-6 SHDSL History PM Dialog

Create Time	Side	ESs	SESs	UASs	LOSs	CRC
10-30 16:00	CO	0	0	0	0	0
10-30 16:00	RT	0	0	0	0	0
10-30 16:15	CO	0	0	0	0	0
10-30 16:15	RT	0	0	0	0	0
10-30 16:30	CO	0	0	0	0	0
10-30 16:30	RT	0	0	0	0	0
10-30 16:45	CO	0	0	0	0	0
10-30 16:45	RT	0	0	0	0	0
10-30 17:00	CO	0	0	0	0	0
10-30 17:00	RT	0	0	0	0	0
10-30 17:15	CO	0	0	0	0	0
10-30 17:15	RT	0	0	0	0	0
10-30 17:30	CO	0	0	0	0	0
10-30 17:30	RT	0	0	0	0	0
10-30 17:45	CO	0	0	0	0	0
10-30 17:45	RT	0	0	0	0	0
10-30 18:00	CO	0	0	0	0	0
10-30 18:00	RT	0	0	0	0	0

Table 9-4 SHDSL History PM Dialog Description

Field	Description
List Table	
Create Time	This indicates the time when the PM is reported
Side	This indicates the location where the PM parameters are observed. (Either central side (CO) or remote side (RT))
ESs	This indicates the count of Error Second during the indicated period.
SESs	This indicates the count of Severely Error Second during the indicated period.
UASs	This indicates the count of Unavailable Error Second during the indicated period.
LOSs	This indicates the count of LOSW second during the indicated period.
CRCs	This indicates the count of the SHDSL CRC anomalies occurring during the current accumulation period.
Function Button	
Graph	Click this button to draw the 2D/3D diagram
Export	Click this button to save the contents of SHDSL History PM List to the Personal Computer.
Close	Exit the SHDSL History PM Dialog .

GE Interface Performance Statistics

Follow the subsequent procedure to obtain data for evaluating the GE interface performance.

Click Performance → Trunk Port PM on **Main Menu** to open the **Trunk Port PM Dialog** as shown in Figure 9-7. Table 9-5 depicts the related parameters.

Figure 9-7 Trunk PM Statistics Dialog

Entity: Slot-NC, Port-GE1

Item	Incoming	Outgoing
Octets	0	204
Unicast Packets	0	0
Non-Unicast Packets	0	3
Discarded Packets	0	0
Erroneous Packets	0	0
PAUSE Frame	0	0

Port: GE1

Buttons: Refresh, Graph, Export, Close [X]

Auto-Refresh: ☐

Table 9-5 Trunk PM Dialog Description

Field	Description
List Table	
Octets	This indicates the numbers of incoming/outgoing octets via the specified GE port.
Unicast Packets	This indicates the numbers of incoming/outgoing unicast packets via the specified GE port.
Non-Unicast Packets	This indicates the numbers of incoming/outgoing non-unicast packets via the specified GE port.
Discarded Packets	This indicates the numbers of incoming/outgoing discarded packets on the specified GE port per RFC1213.
Erroneous Packets	This indicates the numbers of incoming/outgoing erroneous packets on the specified GE port per RFC1213.
PAUSE Frame	This indicates the numbers of incoming/outgoing IEEE 802.3x pause frames on the specified GE port.
Function Button	
Port	Select the GE port you want to observe.
Refresh	Click this button to refresh the List Table
Graph	Click this button to draw the 2D/3D diagram
Export	Click this button to save the contents of Trunk Port PM to the Personal Computer.
Close	Exit the Trunk Port PM Dialog.

Chapter 10 Fault Management

This chapter describes the system fault management. The NCT192 supports real time monitoring of the NE.

This chapter contains the following sections:

- NE Alarm Information
- System Alarm Management

NE Alarm Information

NCT192 detects alarms from the NE system and interface card modules. Alarm detection is accomplished by way of either polling NE actively or receiving SNMP trap passively.

NCT192 allows you to temporarily isolate a subset of event messages and display them in the List Table. By applying condition filters at top of dialog, the List Table will only contain the events that meet the specified filter criteria.

Follow the subsequent procedure to observe the current alarm information.

- Step 1** Click Diagnosis → NE Alarm → Active Alarm on **Main Menu** to open the **Active Alarm & Event** dialog, or alternative select the object form **Rack Tab** and use right mouse button to bring out the menu, select the **Alarm** → **Active Alarm**, as shown in Figure 10-1. Table 10-1 depicts the definition of fields..
- Step 2** Select the event from the List Table and click 'Detail' button to view the detail of a specific event, as shown in Figure 10-2 and Table 10-2 depicts the related parameters.

Figure 10-1 Active Alarm & Event List Dialog

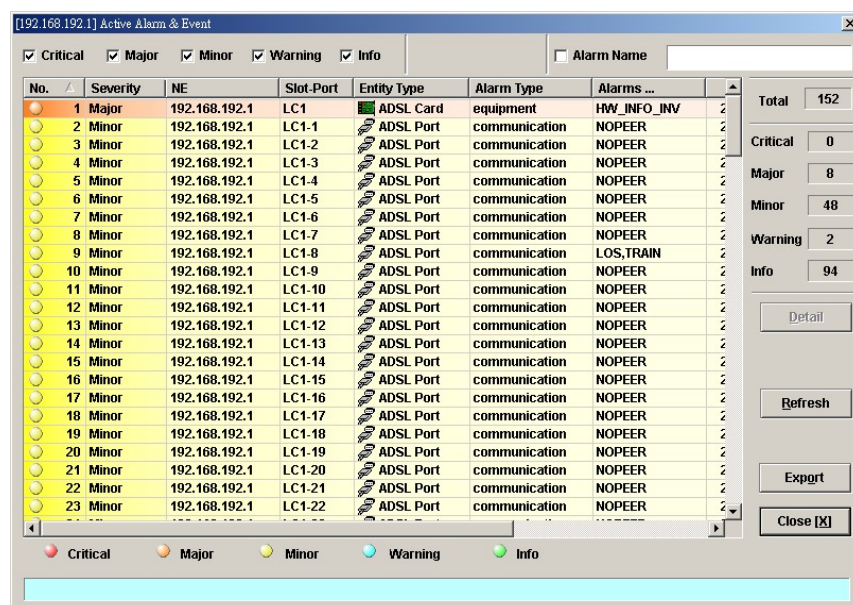


Table 10-1 Active Alarm & Event List Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the Table List.
Severity	This indicates the severity of the specified alarm/event.
NE	This indicates the NE IP address.
Slot-Port	This indicates where the alarm/event occurred.
Entity Type	This indicates the hardware type of the entity where the alarm/event occurred.
Alarm Type	This indicates the alarm type.
Alarms	This indicates the description of alarm.
Occur Time	This indicates the time when the indicated alarm/event occurs at the NE.
Receive Time	This indicates the time when the indicated alarm/event received by the NCT192.
Function Button	
Detail	Click this button to display the detail information of the specified alarm/event.
Refresh	Click this button to refresh the List Table
Export	Click this button to save the contents of Active Alarm & Event List to the Personal Computer.
Close	Exit the Active Alarm & Event List Dialog.



The right-hand side of dialog provides a summary of all the active alarm status under the selected object (Slot-Port), with a display of the alarm of severity.



The List Table of Active Alarm & Event dialog displays the selected object. The title of dialog shows the scope of selecting object.

Figure 10-2 Detailed Alarm & Event Dialog

Detailed Alarm & Event

Alarm Information

Location: <Location>

NE: 192.168.192.1

Entity: Slot-LC1, Port-10

Online Model: NCT1901 ADSL Port

Planned Model: NCT1901 ADSL Port

Alarm Severity: Minor

Occur Time: 2007-10-26 10:13:01

Receive Time: 2007-10-31 10:03:06

Detailed Alarms

No.	Alarm	Description
1	NOPEER	No peer detected

Close [X]

Table 10-2 Detailed Alarm & Event Dialog Description

Field	Description
Alarm Information	
Location	This indicates the location of the NE
NE	This indicates the NE IP address.
Entity	This indicates the module where the alarm/event occurred.
Online Model	This indicates the online model name associated with the “Entity”.
Planned Model	This indicates the planned model name associated with the “Entity”.
Alarm Severity	This indicates the severity of the observed alarm/event.
Occur Time	This record occur time of the observed alarm/event.
Receive Time	This record receives time of the specified alarm/event.
Detailed Alarm	This describes the detailed alarm information.

System Alarm Management

The system alarm management allows you to manually gather the alarm information from NE. You can also configure the system alarm relay input and monitor the NE hardware operation status (like voltage, temperature).

.This section contains the following three subsections.

- Alarm Synchronization
- Relay-Input Alarm Management
- Relay-Output Alarm Management
- Hardware Status Monitoring

Alarm Synchronization

The NCT192 provides automatic alarm synchronization. However, since the NCT192 polls the NE periodically, the polling may not reflect the real-time status. To supplement this issue, the NCT192 supports the real-time manually alarm synchronization function.

Follow the subsequent procedure to perform the alarm synchronization function.

Click Diagnosis → NE Alarm → Alarm Sync on **Main Menu** to process the alarm synchronization, as shown in Figure 10-3.

Figure 10-3 Completed Alarm Sync Dialog



Relay-Input Alarm Management

The NCT192 support housekeep alarm relays for input signals. The system relay-in alarm management allows you to define the alarm relay input. Please see “*System Installation Guide*” for the definition. Once the normal status of input signal is different from the current status, the NE will launch an “abnormal status” alarm of the specified relay input to LCT.

Follow the subsequent procedure to manage the alarm relay-in.

Step 1 Click Diagnosis → NE Alarm → Alarm Input on **Main Menu** to open the **Alarm Input** Dialog as shown in Figure 10-4 . Table 10-3 depicts the related parameters.

Figure 10-4 Alarm Input List Dialog

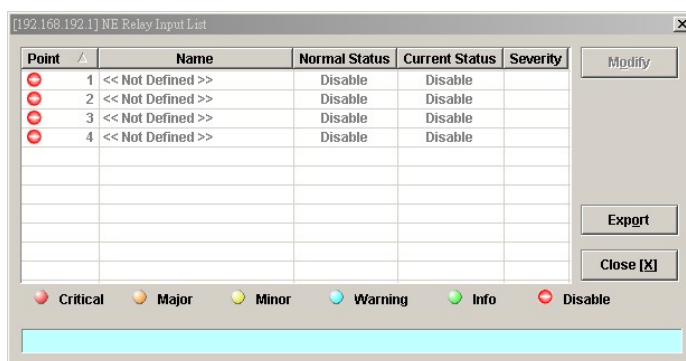


Table 10-3 Alarm Input List Dialog Description

Field	Description
List Table	
Index	This indicates the location of the relay-in alarm port.
Name	This indicates the name of the relay-in alarm port.
Admin State	This indicates the administrative status of the specified alarm relay-in.
Current State	This indicates the current status of the specified alarm relay-in.
Normal State	This indicates the normal status of the specified alarm relay-in that configured by operator.
Severity	This indicates the alarm severity while the status is abnormal.

Step 2 Select the row and click ‘**Modify**’ button to modify the normal status of the alarm input port as shown in Figure 10-5. Table 10-4 depicts the related parameters.

Figure 10-5 Alarm Input Modification Dialog
Table 10-4 Alarm Input Modification Dialog Description

Field	Description
Relay Input Setting	
Name	This gives a meaningful name to the specified alarm relay-in. The valid value is string of up to 32 characters
Administrator State	
Enable	Check this radio button to enable the specified alarm relay-in.
Disable	Check this radio button to disable the specified alarm relay-in.
Normal Status	
Closed	Check this radio button to define normal status of the specified alarm relay-in as “closed circuit”.
Opened	Check this radio button to define normal status of the specified alarm relay-in as “open circuit”.

Relay-Output Alarm Management

The NE support housekeeping alarm relays to trigger the external device such as speaker or light to launch warning signal.

Follow the subsequent procedure to manage the alarm relay-in.

- Step 1
- Click Diagnosis → NE Alarm → Alarm output on **Main Menu** to open the **Alarm Output** Dialog as shown in Figure 10-6. Table 10-5 depicts the related parameters.

Figure 10-6 Alarm Output List Dialog

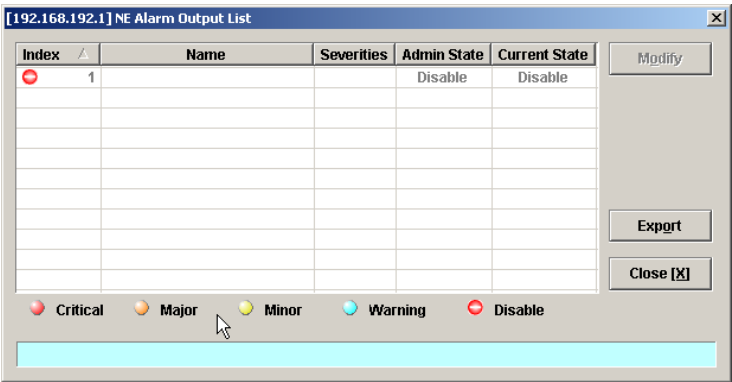


Table 10-5 Alarm Output List Dialog Description

Field	Description
List Table	
Index	This indicates the location of the relay-in alarm port.
Name	This indicates the name of the relay-in alarm port.
Severities	This indicates the alarm severity while the status is abnormal.
Admin Status	This indicates the administrative status of the specified alarm relay-out that configured by operator.
Current Status	This indicates the current status of the specified alarm relay-out.

- Step 2
- Select the row and click ‘**Modify**’ button to modify the normal status of the alarm output port as shown in Figure 10-7. Table 10-6 depicts the related parameters.

Figure 10-7 Alarm Output Modification Dialog

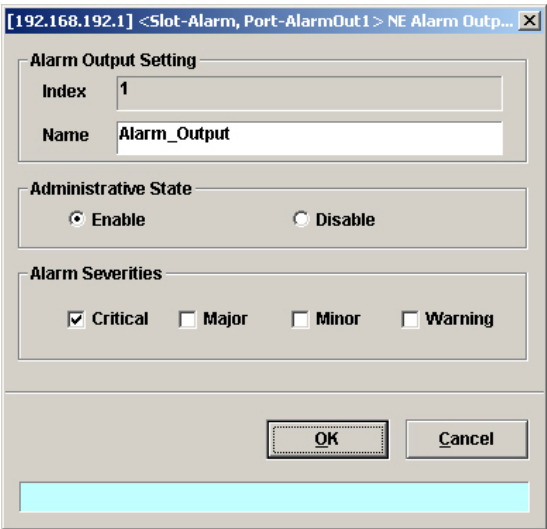


Table 10-6 Alarm Input Modification Dialog Description

Field	Description
Alarm Output Setting	
Index	This indicates the location of the relay-out alarm port.
Name	This gives a meaningful name to the specified alarm relay-out. The valid value is string of up to 32 characters
Administrator State	
Enable	Check this radio button to enable the specified alarm relay-out.
Disable	Check this radio button to disable the specified alarm relay-out.
Alarm Severities	
Critical	Check this check-box button to define alarm severity of the specified alarm relay-out as “Critical”.
Major	Check this check-box button to define alarm severity of the specified alarm relay-out as “Major”.
Minor	Check this check-box button to define alarm severity of the specified alarm relay-out as “Minor”.
Warning	Check this check-box button to define alarm severity of the specified alarm relay-out as “Warning”.

Hardware Status Monitoring

In the hardware monitoring list dialog, you can monitor the temperature and voltage status of any specific card module.

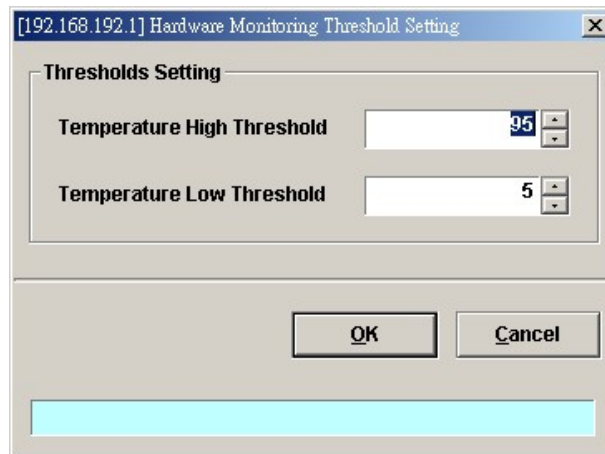
- Step 1** Click Diagnosis → NE Alarm → Hardware Monitoring on **Main Menu** to open the **Hardware Monitoring List** Dialog as shown in Figure 10-8. Table 10-7 depicts the related parameters.
- Step 2** Select the row and click ‘**Modify**’ button to the system temperature threshold value as shown in Figure 10-9.

Figure 10-8 Hardware Monitoring List Dialog

No.	Slot	Name	Current Value	Reference Value	Threshold
1	LC1	Voltage sensor1 (0.01 voltage)	1178	1200	
2	LC1	Voltage sensor2 (0.01 voltage)	117	120	
3	LC1	Voltage sensor3 (0.01 voltage)	177	180	
4	LC1	Voltage sensor4 (0.01 voltage)	314	320	
5	LC1	Voltage sensor5 (0.01 voltage)	0	0	
6	LC1	Voltage sensor6 (0.01 voltage)	146	150	
7	LC1	Voltage sensor7 (0.01 voltage)	249	250	
8	LC1	Voltage sensor8 (0.01 voltage)	314	320	
9	LC1	Temperature sensor1 (1 degree centigrade)	40	--	
10	LC1	Temperature sensor2 (1 degree centigrade)	38	--	
11	LC1	Temperature sensor3 (1 degree centigrade)	34	--	
12	LC1	Temperature sensor4 (1 degree centigrade)	31	--	
13	LC2	Voltage sensor1 (0.01 voltage)	1196	1200	
14	LC2	Voltage sensor2 (0.01 voltage)	148	150	
15	LC2	Voltage sensor3 (0.01 voltage)	178	180	
16	LC2	Voltage sensor4 (0.01 voltage)	319	330	
17	LC2	Voltage sensor5 (0.01 voltage)	0	0	
18	LC2	Voltage sensor6 (0.01 voltage)	0	0	
19	LC2	Voltage sensor7 (0.01 voltage)	247	250	
20	LC2	Voltage sensor8 (0.01 voltage)	317	330	
21	LC2	Temperature sensor1 (1 degree centigrade)	35	--	
22	LC2	Temperature sensor2 (1 degree centigrade)	36	--	
23	LC2	Temperature sensor3 (1 degree centigrade)	41	--	
24	LC2	Temperature sensor4 (1 degree centigrade)	35	--	
25	LC3	Voltage sensor1 (0.01 voltage)	1184	1200	

Table 10-7 Hardware Monitoring List Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Tale.
Slot	This indicates the location of line card or other card model.
Name	This indicates the name of sensor.
Current Value	This indicates the current value of the specified sensor.
Reference Value	This indicates the normal value of the specified sensor.
Threshold – Low/High	This indicates the low-high threshold value of the specified sensor.
Function Button	
Modify	Click this button to modify the system temperature threshold value as shown in Figure 10-9.
Refresh	Click this button to refresh the table list.
Export	Click this button to save the contents of Hardware Monitoring List to the Personal Computer.
Close	Exit the Hardware Monitoring List dialog.

Figure 10-9 Hardware Monitoring Threshold Setting Dialog

Chapter 11 Diagnosis Management

This chapter describes the diagnosis of xDSL line interface, GE interface, and system network connectivity.

This chapter contains the following sections:

- xDSL Line Interface Diagnosis
- xDSL Service Status Diagnosis
- Trunk Current Status Diagnosis
- Network Diagnosis

xDSL Line Status Diagnosis

The NE supports the following five xDSL line status related diagnosis functions.

- Port Rate Status
- Bits Allocation Monitoring
- Loop Monitoring
- Loop Diagnosis (DELT <Dual-Ended Line Test>)
- Loop SELT Test (Single End Loop Test)

Port Rate Status

Follow the subsequent procedure to monitor the ADSL current rate status.

- Step 1** Click Diagnosis → xDSL Current Status → Port Rate Status on **Main Menu** to open the **xDSL Port Selection Dialog** as shown in Figure 11-1.
- Step 2** Select the port you want to show and press Query button on the **xDSL Port Selection Dialog** to observe the current ADSL port status as shown in Figure 11-2. Table 11-1 depicts the related parameters.

Figure 11-1 xDSL Port Selection Dialog

Figure 11-2 ADSL Port Rate Status Dialog

Item	Downstream	Upstream
Current Tx Rate (Kbps)	0	0
Previous Tx Rate (Kbps)	0	0
Attainable Rate (Kbps)	0	0
SNR Margin (dB)	0.0	0.0
Attenuation (dB)	0.0	0.0
Output Power (dBm)	0.0	0.0
Interleave Delay (msec)	0	0
Data Block Length (byte)	0	0
Line Standard	G.992.1 AnnexA	--
Power Management Mode	Manual	--
Power State	L0	--
Current INP (0.01 symbol time)	0	0

Table 11-1 ADSL Port Rate Status Dialog Description

Field	Description
List Table	
Current Tx Rate (Kbps)	This indicates the current DS/US transmit rate in unit of Kbps. (in the current show-time)
Previous Tx Rate (Kbps)	This indicates the previous DS/US transmit rate in unit of Kbps. (in the last show-time)
Attainable Rate (Kbps)	This indicates the DS/US attainable rate in unit of Kbps.
SNR Margin (dB)	This indicates the DS/US SNR margin in unit of dB.
Attenuation (dB)	This indicates the DS/US attenuation in unit of dB.
Output Power (dBm)	This indicates the DS/US output power in unit of dBm.
Interleave Delay (msec)	This indicates the DS/US interleave delay whenever the line is in the interleaved mode.
Data Block Length (byte)	This indicates the DS/US ADSL data block length in unit of octet.
Line Standard	This indicates the adopted for the current ADSL connection.
Power Management Mode	This indicates the power management mode, either manual or. Automatic.
Power State	This indicates the power management state of this subscriber port per ITU-T 992.3.
Current INP (0.01 symbol time)	This indicates the DS/US INP (Impulse Noise Protection) symbol time in unit of (0.01 symbol time).

Table 11-1 ADSL Port Rate Status Dialog Description (Continued)

Field	Description
Function Button	
Refresh	Click this button to refresh the specified threshold value.
Next	Click this button to display the next subscriber port.
Previous	Click this button to display the previous subscriber port.
First	Click this button to go to the first subscriber status.
Last	Click this button to go to the last subscriber status.
Transit to L0	Click this button to force the power management state to L0 per ITU-T 992.3.
Transit to L2	Click this button to set the power management state to L2 per ITU-T 992.3.
Transit to L3	Click this button to set the power management state to L3 per ITU-T 992.3.
Export	Click this button to save the contents of ADSL Current Rate Status List to the Personal Computer.
Close	Exit the ADSL Current Rate Status Dialog.



Please refer to ITU-T 992.3 for the details of state transition among the power management state L0, L2 and L3.

Bits Allocation Monitoring

The bit allocation monitoring function allows the operator to observe the number of bits carried on each tone of ADSL line in show-time.

Follow the subsequent procedure to monitor the bit allocation status on the specified ADSL connection.

- Step 1** Click Diagnosis → xDSL Current Status → Bits Allocation on **Main Menu** to open the **xDSL Port Selection Dialog** as shown in Figure 11-1.
- Step 2** Select the port you want to show and press Query button on the **xDSL Port Selection Dialog** to open the **xDSL Bit Allocation** Dialog as shown in Figure 11-3. Table 11-2 depicts the related parameters.

Figure 11-3 ADSL Bit Allocation Status Dialog

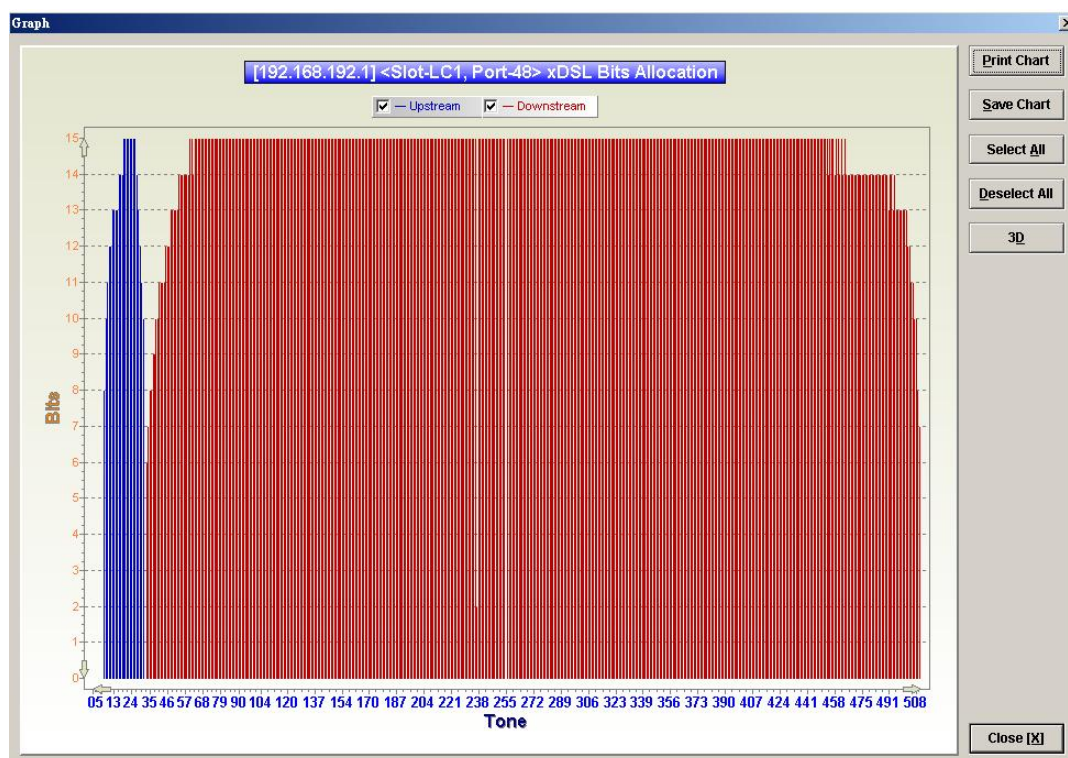


Table 11-2 ADSL Bit Allocation Status Dialog Description

Field	Description
List Table	
Tone	This indicates number of tone index.
Upstream	This indicates the upstream bit allocation of the specified tone.
Downstream	This indicates the downstream bit allocation of the specified tone.
Function Button	
Refresh	Click this button to refresh the bit allocation list table.
Graph	Click this button to display the graph for the bit allocation.
Export	Click this button to save the contents of ADSL Bit Allocation Status List to the Personal Computer.
Close	Exit the ADSL Bit Allocation Status Dialog .

Step 3 Click “Graph” to show the graph of Bit Allocation as shown in Figure 11-4.

Figure 11-4 Graph of Bit Allocation



Loop Monitoring

The loop monitoring function provides the records of ADSL loop characteristics and Quiet Line Noise (QLN) measured during the last training. It is noted that the measured results are only available in the show-time.

- Step 1** Click Diagnosis → xDSL Current Status → Bits Allocation on **Main Menu** to open the **xDSL Port Selection Dialog** as shown in Figure 11-1.
- Step 2** Select the port you want to show and press Query button on the **xDSL Port Selection Dialog** to open the **ADSL Loop Monitoring Dialog** as shown in Figure 11-5. Table 11-3 depicts the related parameters.
- Step 3** Press Start button to get starting.
- Step 4** Click “Graph” button to show the graph of Magnitude as shown in Figure 11-6 or show the graph of Quiet Line PSD as shown in Figure 11-7



Please refer to ITU-T 992.3 for the details of loop monitoring parameters.



In comparison with the DELT, the ADSL loop is not corrupted whenever the operator performs the loop monitoring function.

Figure 11-5 ADSL Loop Monitoring Dialog

Tone	Upstream (dB)	Downstream (dB)
0	-42.5	-59.0
1	NA	-121.5
2	NA	-139.0
3	NA	-137.5
4	NA	-23.0
5	-140.0	-23.0
6	-145.0	-148.0
7	-93.5	-23.0
8	-52.5	-40.0
9	-40.5	-40.0
10	-38.0	-34.5
11	-35.5	-40.0
12	-34.0	-40.0
13	-33.0	-34.5
14	-33.0	-40.0
15	-34.5	-34.5
16	-36.0	-34.5
17	-38.5	-68.0
18	-41.5	-52.5
19	-45.5	-76.5

Table 11-3 ADSL Loop Monitoring Dialog Description

Field	Description
Status	This indicates the status of the loop monitoring.
Reason for Failure	This indicates the result of failure case.
Magnitude Dialog	
Tone	This indicates the serial number of tone.
Upstream	This indicates the magnitude of transfer function per tone of the upstream channel.
Downstream	This indicates the magnitude of transfer function per tone of the downstream channel.
Quiet Line PSD Dialog	
Tone	This indicates the serial number of tone.
Upstream	This indicates the quiet line noise PSD per tone of the upstream channel.
Downstream	This indicates the quiet line noise PSD per tone of the downstream channel.
Function Button	
Start	Click this button to start the loop monitoring function.
Graph	Click this button to display the resultant graph of loop monitoring.
Export	Click this button to save the contents of xDSL Loop Monitoring List to the Personal Computer.
Close	Exit the xDSL Loop Monitoring List Dialog.



Please refer to ITU-T 992.3 for the details of loop monitoring parameters.

Figure 11-6 Graph of Loop Monitoring – Magnitude

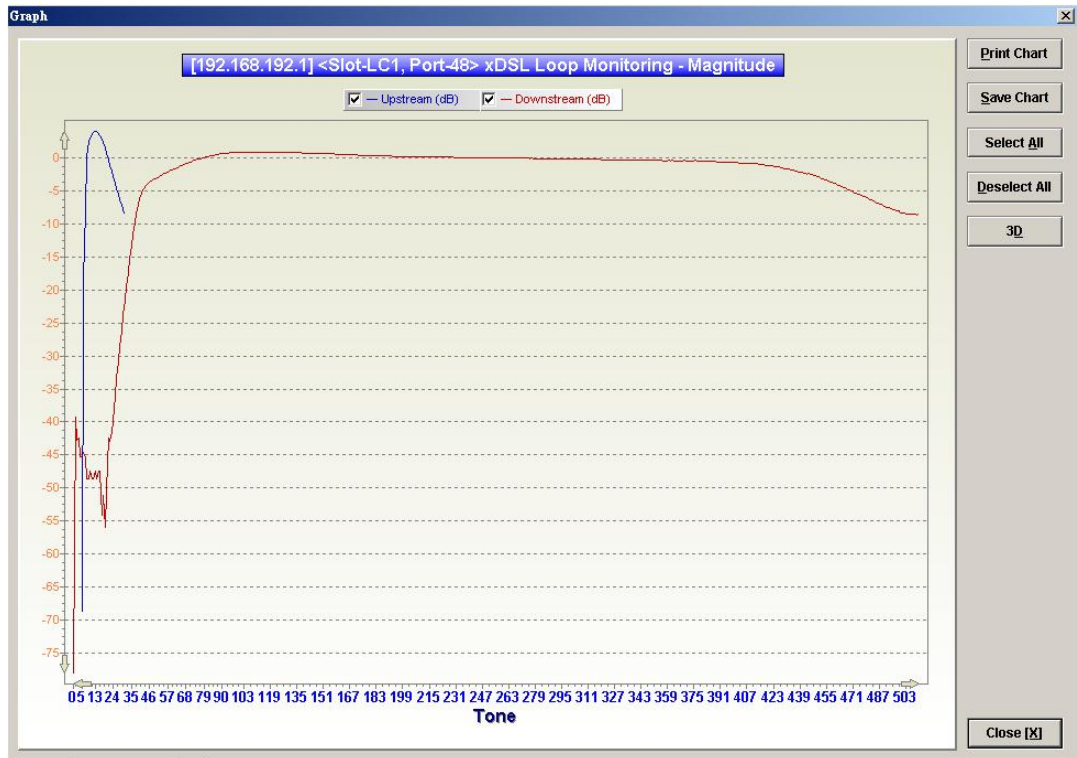
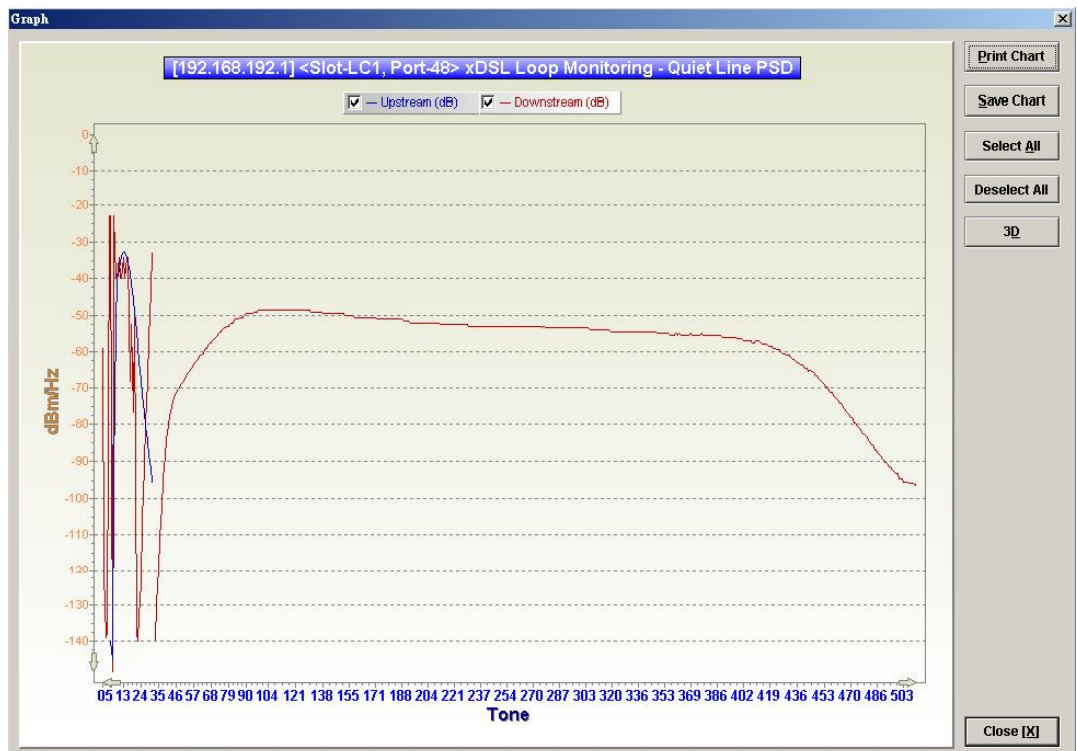


Figure 11-7 Graph of Loop Monitoring – Quiet Line Noise PSD



Loop Diagnosis (DELT <Dual-Ended Line Test>)

The DELT loop diagnosis function provides mechanism to measure the ADSL loop quality. This action will interrupt the ADSL connection. However, more detailed inform are gathered in comparison with the aforementioned loop monitoring function.

This function is available on ADSL2 and ADSL2+ connection only, the ADSL CPE who did not complied with ITU-T standard G.992.3, G.992.4, and G.992.5 may not be able to perform the loop diagnostics.

- Step 1** Click Diagnosis → xDSL Current Status → Bits Allocation on **Main Menu** to open the **xDSL Port Selection Dialog** as shown in Figure 11-1.
- Step 2** Select the port you want to show and press Query button on the **xDSL Port Selection Dialog** to open the **ADSL Loop Diagnosis Dialog** as shown in Figure 11-8. Table 11-4 depicts the related parameters.
- Step 3** Press Start button to get starting.
- Step 4** Click “Graph” button to show the graph of Magnitude as shown in Figure 11-9 or the graph of Quiet Line PSD as shown in Figure 11-10 or the graph of SNR as shown in Figure 11-11.



In comparison with the loop monitoring function, the ADSL loop is corrupted whenever the operator performs the DELT.



It is suggested to view the graphical presentation of the DELT diagnosis via the NCT192 or NCT192 client.

Figure 11-8 ADSL Loop Diagnosis Dialog

Item	Downstream	Upstream
Attainable Rate (bps)	27276000	1280000
Loop Attenuation (0.1 dB)	0	2
Signal Attenuation (0.1 dB)	0	0
SNR Margin (0.1 dB)	0	60
Tx Power (0.1 dBm)	113	123

The above dialog lists the loop diagnostics parameters that display, see the ITU-T's G.992.3 and G.992.5 for more information.

Table 11-4 ADSL Loop Diagnosis Dialog Description

Field	Description
Line Profile	Use this combo-box to select the line profile to test.
Status	This indicates the status of the DELT.
Reason for Failure	This indicates the result of failure case.
Rate Dialog	
Attainable Rate (bps)	This displays the attainable rate of DELT.
Loop Attenuation (0.1dB)	This displays the loop attenuation of DELT.
Signal Attenuation (0.1dB)	This displays the signal attenuation of DELT.
SNR Margin (0.1dB)	This displays the SNR margin value of DELT.
Tx Power (0.1dB)	This displays the transmit power value of DELT.
Magnitude Dialog (The magnitude of ADSL line transfer function)	
Tone	This indicates the number of the tone.
Upstream	This indicates the upstream magnitude of the specified tone.
Downstream	This indicates the downstream magnitude of the specified tone.
Quiet Line PSD Dialog (PSD of Quiet Line Noise)	
Tone	This indicates the number of the tone.
Upstream	This indicates the upstream PSD of Quiet Line Noise of the specified tone.
Downstream	This indicates the downstream PSD of Quiet Line Noise of the specified tone.
SNR Dialog	
Tone	This indicates the number of the tone.
Upstream	This indicates the upstream SNR of the specified tone.
Downstream	This indicates the downstream SNR of the specified tone.
Function Button	
Show	Click this button to display the selected line profile.
Start	Click this button to start the DELT function.
Graph	Click this button to display the result graph of DELT.
Export	Click this button to save the results of ADSL Loop Diagnosis (DELT) to the Personal Computer.
Close	Exit the ADSL Loop Diagnosis (DELT) Dialog.



Please refer to ITU-T 992.3 for the details of DELT.



‘Upshift Noise Margin’, ‘Downshift Noise Margin’, ‘Upshift Time’ and ‘Downshift Time’ are only applied to the Rate Mode ‘Adaptive at Run-Time’.

Figure 11-9 Graph of DELT result – Magnitude

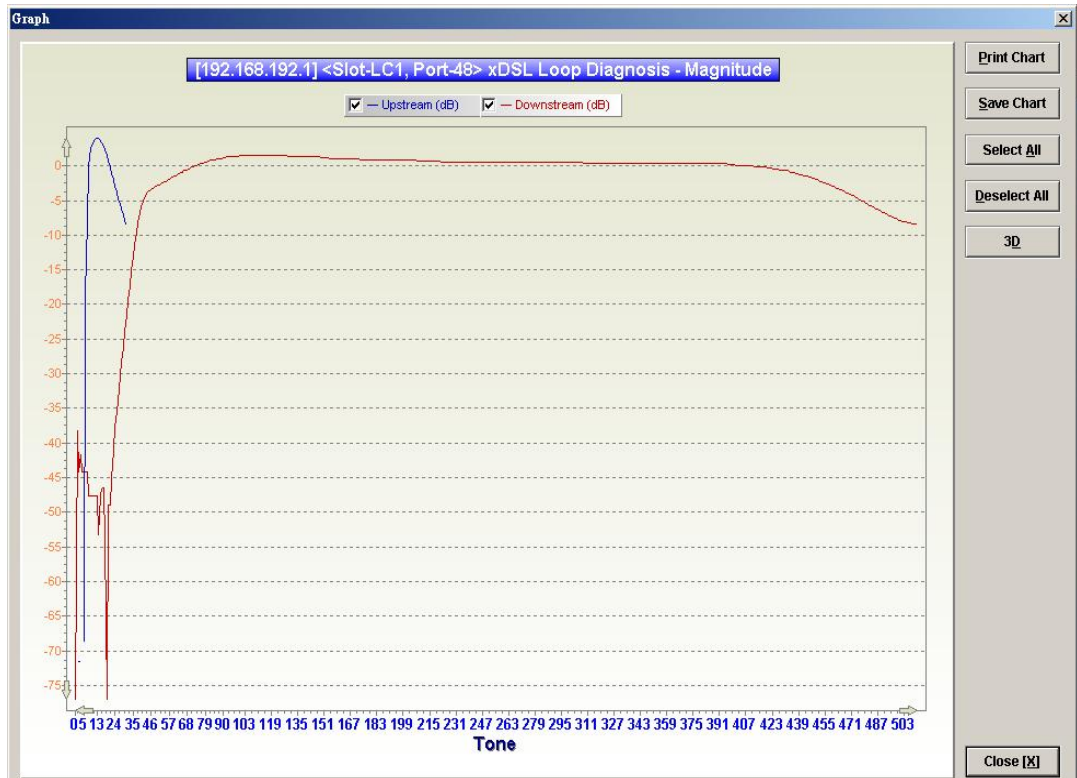


Figure 11-10 Graph of DELT result – Quiet Line PSD

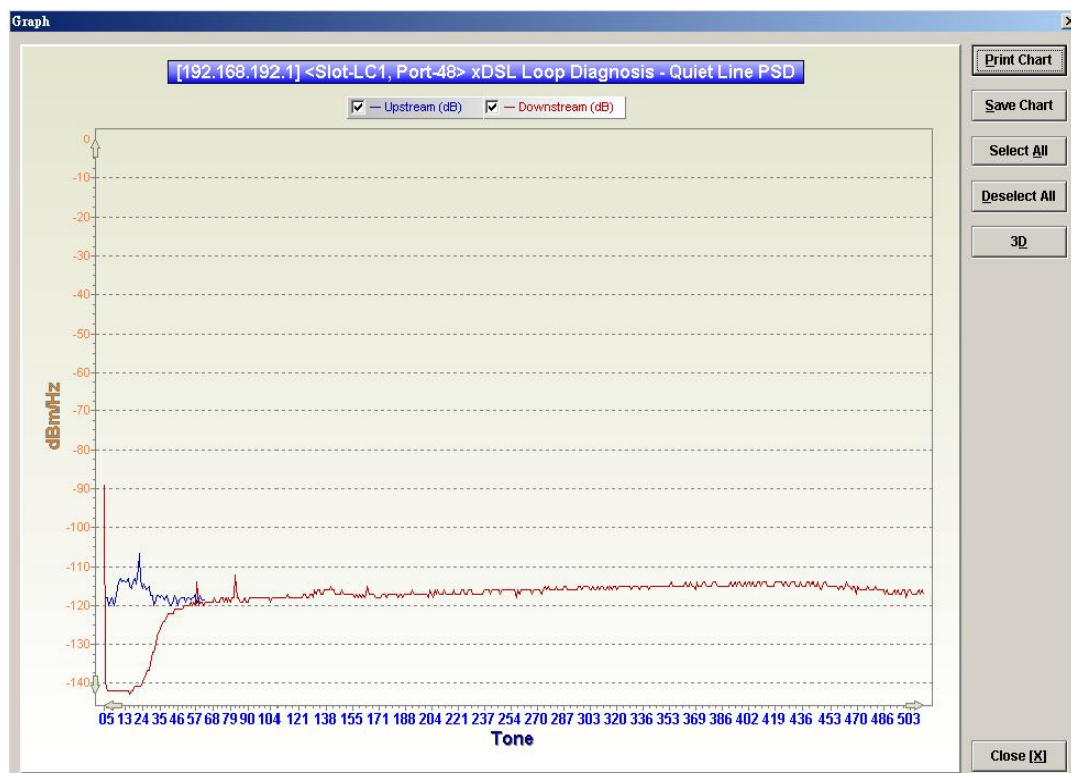
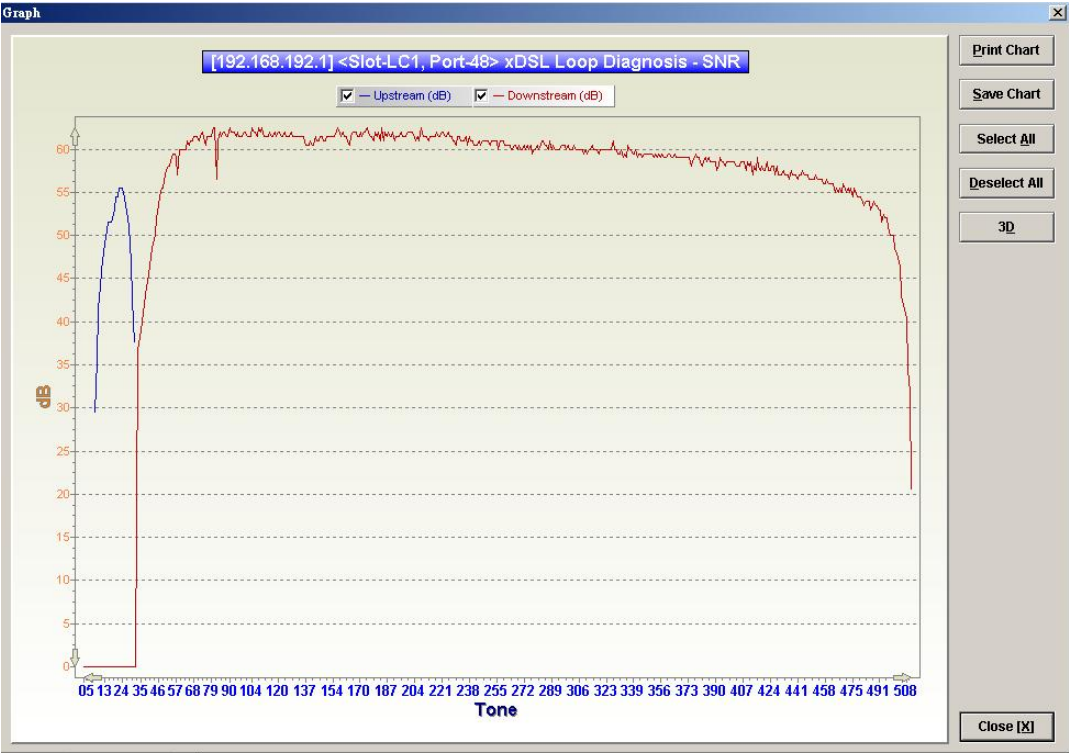


Figure 11-11 Graph of DELT result – SNR



Loop SELT Test (Single End Loop Test)

The SELT loop function diagnosis function is to estimate the distance of the DSL connection from the NE to the subscriber’s location without connecting a subscriber device.

- Step 1** Click Diagnosis → xDSL Current Status → Bits Allocation on **Main Menu** to open the **xDSL Port Selection Dialog** as shown in Figure 11-1.
- Step 2** Select the port you want to show and press Query button on the **xDSL Port Selection Dialog** to open the **ADSL Loop SELT Test Dialog** as shown in Figure 11-12 and Table 11-5 depicts the related parameters.
- Step 3** Press Start button to get starting.

Figure 11-12 ADSL Loop SELT Test

Table 11-5 ADSL Loop SELT Test Dialog Description

Field	Description
Status	This indicates the status of the SELT.
Reason for Failure	This indicates the result of failure case.
Test Result	
Cable Type	This displays the estimated cable type.
Reach Length (ft.)	This displays the estimated cable length.
Function Button	
Start	Click this button to start the SELT.
Close	Exit the SELT dialog.



Please refer to ITU-T 992.3 for the details of SELT.

xDSL Service Status Diagnosis

The NE supports the following six xDSL service status related diagnosis functions.

- ATM OAM F5 VC Diagnosis
- Bridge Filtering Database
- VLAN Membership
- xDSL MAC Spoofing Statu
- Multicast Channel Status
- Multicast Group Membership
- xDSL Downstream Broadcast Forwarding VLANs
- DHCP Session Information
- PPPOE Session Information

ATM OAM F5 VC Diagnosis

In order to diagnose and fix problem, the NE supports to perform the ATM Operation, Administration, and Maintenance (OAM) F5 diagnosis at data connection layer.

Via ATM OAM F5 loopback diagnosis, the operator is able to diagnose the health of existant ATM VC connection between the NE and ADSL CPE in intrest.

Follow the subsequent procedure to manage the VC-to-VLAN connectivity on a specific xDSL port.

Step 1 Click Configuration → xDSL → VC-to-VLAN on **Main Menu** to open the **xDSL VC-to-VLAN List** Dialog as shown in Figure 7-3.

Step 2 Click on the 'VC OAM Test' button to to launch the **ATM Loopback OAM Cell Testing** as shown in and Table 11-6 depicts the related parameters.

Figure 11-13 TM Loopback OAM Cell Testing

Table 11-6 ATM Loopback OAM Cell Testing

Field	Description
Virtual Channel	
VPI	This indicates the VPI of the specified entry.
VCI	This indicates the VCI of the specified entry.
Loopback OAM Cell Type	
Segment	This indicates to send the segment OAM F5 cells which are processed by the next segment
End-to-End	This indicates to send the end-to-end OAM F5 cells which are only processed by end stations terminating an ATM link
Both	This indicates to send both the end-to-end and segment OAM F5 cells.
Function Button	
Test	Click this button to send OAM F5 cells.
Close	Exit the ATM Loopback OAM Cell Testing Dialog.

Bridge Filtering Database

The FDB (filtering Database) of NCT192 system stores the following MAC entries

- the manually configured MAC addresses on an ATM VC of xDSL port.
- the MAC addresses learned from the associate ATM VC of xDSL port.

According to the nature of stored MAC entry, each entry possesses “status” field. The definitions of “status” field are as follows.

- **“AD”** : the abbreviation of “ACL Deny”,
It means the NE is to drop the upstream traffic of the indicated source MAC and forward the upstream traffic of other source MAC from the indicated xDSL port.
- **“AP”** : the abbreviation of “ACL Permit”,
It means the NE is to forward the upstream traffic of this indicated source MAC and drops the upstream traffic of other source MAC from the indicated xDSL port.
- **“S”**: the abbreviation of “Static”,
It means this MAC entry is configured manually in FDB.
- **“LU”**: the abbreviation of “Learned Unique”,
It means this MAC is learned on the indicated xDSL port dynamically with setting aged time and is a unique one.
- **“LUN”**: the abbreviation of “Learned Unique, non-aged”,

It means this MAC is learned on the indicated xDSL port dynamically with setting non-aged time and is a unique one.

- **“LR”** : the abbreviation of “Learned Routed”,
It means this MAC is inserted by the xDSL LC in the case that the indicated xDSL port is in the RFC2684 routed mode.
- **“LSI”**: the abbreviation of “Learned Spoofed Inactive”,
It means the following identities.
 - This MAC is learned on the indicated xDSL port.
 - The NE learns the same MAC on the xDSL ports other than the indicated xDSL port. That is, this MAC is spoofed.
 - This spoofed MAC is at the “inactive” state. That is the NE is to drop the upstream traffic of the spoofed MAC from the the indicated xDSL port.
- **“LSA”** : the abbreviation of “Learned Spoofed Active”,
It means the following identities.
 - This MAC is learned on the indicated xDSL port.
 - The NE also learns the same MAC on the xDSL ports other than the indicated xDSL port. That is, this MAC is spoofed.
 - This spoofed MAC is at the “active” state. That is the NE is to forward the upstream traffic of the spoofed MAC from the the indicated xDSL port.

Table 11-7 shows how the NE treats the upstream Ethernet frame whenever its source MAC hits the PVC_FDB. Here, the “PVC_FDB” indicates the the FDB associated with the specified ATM PVC.

Table 11-8 shows the conditions the NE will not learn the source MAC of upstream traffic.

- When the status of existent MAC entry in PVC_FDB is **“AP”**.

Table 11-7 The treatment of an upstream Ethernet frame of source MAC hitting the PVC_FDB

Status of hitted MAC entry in PVC_FDB	S	AD	AP	LU	LUN	LR	LSA	LSI
Forward (F) /Drop (D) packets of the same source MAC	F	D	F	F	F	F	F	D

Table 11-8 The conditions the NE does not learn additional source MAC of upstream traffic

Status of existent MAC entry in PVC_FDB	S	AD	AP	LU	LUN	LR	LSA	LSI
Allow (Y) /Deny (N) learning any additional MAC	Y	Y	N	Y	Y	NA	Y	Y

The NE may add a MAC entry to FDB due to either one of the following cases.

- The operator intends to manually add a MAC ACL entry.
- The operator intends to manually add a static MAC entry.
- The NE executes the basic “learning process of a bridge”.

Depending on the status of existent MAC entries in FDB, the NE may take some or all of the following actions when it is to add a MAC entry to FDB

- Change the status of existent MAC entries of the same MAC.
- Reject to add this new MAC entry.
- Allow to add this new MAC entry but assign it some different status.

Table 11-9~Table 11-11 depicts the expected status of hitted MAC entry as well as the status of new added MAC entry in the aforementioned cases with the follwoing notations.

- Dif_Port_FDB = The MAC entries of FDB associated with different port
- Dif_PVC_FDB = The MAC entries of FDB associated with the same port but different PVC

- PVC_FDB = The MAC entries of FDB associated with the same port and the same PVC
- o : Permit x : Reject # : Clear LU/LUN Entry
- c : Clear AP Entry & : Clear non-AP Entry r : Replacement

Table 11-9 The expected status of hitted MAC entry as well as the status of new added MAC entry in the case that the MAC entry to be added hits the entry of Dif_Port_FDB

The reason to add a MACentry Status of matched MAC entry of Dif_Port_FDB	Manual addition			Dynamicaly learning on ATM PVC of		
	a static MAC	a MAC ACL Permit MAC	a MAC ACL Deny MAC	RFC2684 routed mode	“aged” RFC2684 bridged mode	“non-aged” RFC2684 bridged mode
S	S x	S x	S o	NA	S LSI	S LSI
AP	AP x	AP x	AP o	NA	AP LSI	AP LSI
AD	AD o	AD o	AD o	NA	AD LU	AD LUN
LR	LR x	LR x	LR x	NA	LR LSI	LR LSI
LU	LU x	LU x	LU o	NA	LSA LSI	LSA LSI
LUN	LUN x	LUN x	LUN o	NA	LUN LSI	LUN LSI
LSA	LSA x	LSA x	LSA o	NA	LSA LSI	LSA LSI
LSI	LSI x	LSI x	LSI o	NA o	LSI LSI	LSI LSI



NA indicates “Not Applicable”. As the NE reserves MACs for routed PVC. It’s not possible for NE to dynamicaly learn such a MAC address on an ATM PVC of RFC2684 routed mode.



Whenever the following 3 cases hold simultaneously.

- NE learns a new MAC entry on a ATM PVC of “non-aged”/“aged” RFC2684 bridged mode,
- This new MAC is the same as the one of FDB associated with different port
- The status of the MAC entry associated with different port is “LUN”.

The NE will keep the status of the MAC entry associated with different port as “LUN”.

Table 11-10 The expected status of hitted MAC entry as well as the status of new added MAC entry in the case that the MAC entry to be added hits the entry of Dif_PVC_FDB

The reason to add a MACentry Status of matched MAC entry of Dif_PVC_FDB	Manual addition			Dynamically learning on ATM PVC of		
	a static MAC	a MAC ACL Permit MAC	a MAC ACL Deny MAC	RFC2684 routed mode	“aged” RFC2684 bridged mode	“non-aged” RFC2684 bridged mode
S	S / 0	S / 0	S / 0	NA	S / LU	S / LUN
AP	AP / 0	AP / 0	AP / 0	NA	AP / LU	AP / LUN
AD	AD / 0	AD / 0	AD / 0	NA	AD / LU	AD / LUN
LR	LR / x	LR / x	LR / x	NA	NA	NA
LU	LU / 0	LU / 0	LU / 0	NA	LU / x	LU / x
LUN	LUN / 0	LUN / 0	LUN / 0	NA	LUN / x	LUN / x
LSA	LSA / x	LSA / x	LSA / x	NA	LSA / x	LSA / x
LSI	LSI / x	LSI / x	LSI / x	NA	LSI / x	LSI / x

Table 11-11 The expected status of hitted MAC entry as well as the status of new added MAC entry in the case that the MAC entry to be added hits the entry of PVC_FDB

The reason to add a MACentry Status of matched MAC entry of PVC_FDB	Manual addition			Dynamically learning on ATM PVC of		
	a static MAC	a MAC ACL Permit MAC	a MAC ACL Deny MAC	RFC2684 routed mode	“aged” RFC2684 bridged mode	“non-aged” RFC2684 bridged mode
S	S / x	S / x	S / x	NA	S / x	S / x
AP	AP / x	AP / x	AP / x	NA	AP / x	AP / x
AD	AD / x	AD / x	AD / x	NA	AD / x	AD / x
LR	LR / x	LR / x	LR / x	LR / 0	NA	NA
LU	LU / r	LU / r+&	LU / r+c	NA	LU / x	NA
LUN	LUN / r	LUN / r+&	LUN / r+c	NA	NA	LUN / x
LSA	LSA / x	LSA / x	LSA / x	NA	LSA / x	NA
LSI	LSI / x	LSI / x	LSI / x	NA	LSI / x	LSI / x

Table 11-12 Bridge Filtering Database Entry List Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
Slot-Port	This indicates the location of xDSL port.
VPI	This indicates the VPI of the specified entry.
VCI	This indicates the VCI of the specified entry.
MAC Address	This indicates the MAC address of the specified entry.
Status	<p>This indicates the reason the MAC address appears in this entry. The definitions of status are as follows.</p> <ul style="list-style-type: none"> • Static: It indicates this MAC entry is configured manually in FDB. • ACL Permit: It indicates the NE is to forward the upstream traffic of this indicated source MAC and drops the upstream traffic of other source MAC from the indicated xDSL port. • ACL Deny: It indicates the NE is to drop the upstream traffic of the indicated source MAC and forward the upstream traffic of other source MAC from the indicated xDSL port. • Learned Unique: It indicates the MAC address is learned on the indicated xDSL port dynamically with setting aged time and is a unique one • Learned Non-aged: It indicates the MAC address is learned on the indicated xDSL port dynamically with setting non-aged time and is a unique one. • Learned Spoofed Active: It indicates the spoofed MAC is at the “active” state. That is the NE is to forward the upstream traffic of the spoofed MAC from the the indicated xDSL port. • Learned Spoofed Inactive: It indicates the spoofed MAC is at the “inactive” state. That is the NE is to drop the upstream traffic of the spoofed MAC from the the indicated xDSL port.
Function Button	
Slot	Use this combo-box to select the line card.
Port	Use this combo-box to select the xDSL port.
Refresh	Click this button to refresh the list table.
Export	Click this button to save the contents of Filtering Database Entry List to the Personal Computer.
Close	Exit the Filtering Database Entry List Dialog.

VLAN Membership

The VLAN membership displays the list of xDSL ports belonging to a VLAN of particular VLAN ID.

Click Diagnosis → xDSL Current Status → VLAN Membership on **Main Menu** to open the **VLAN Membership List** Dialog as shown in Figure 11-15. Table 11-13 depicts the related parameters.

Figure 11-15 VLAN Membership List Dialog

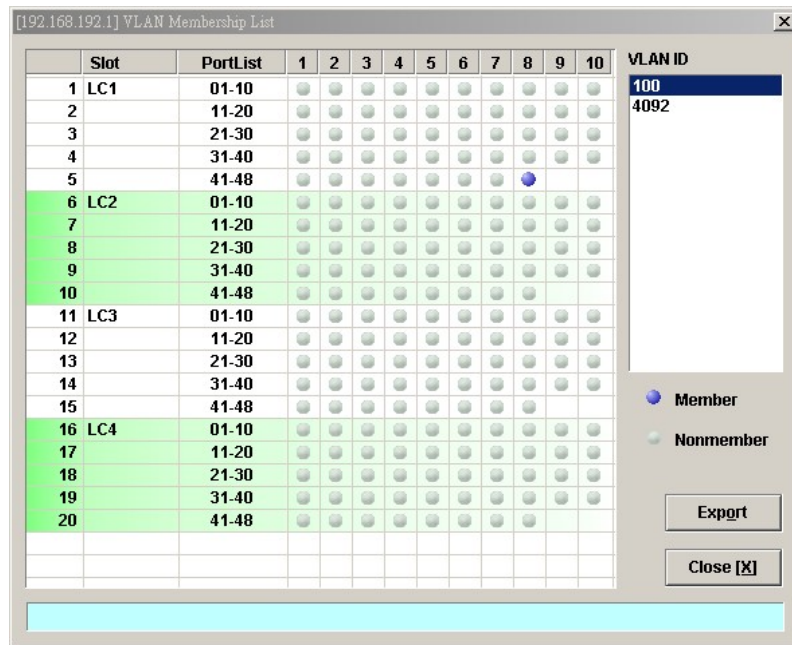


Table 11-13 VLAN Membership List Dialog Description

Field	Description
List Table	
Slot	This indicates the location of line card.
Port-List	This indicates the location of xDSL port. The blue point indicates that the corresponding port is a member port of a VLAN of the specified VLAN ID.
VLAN ID	This specifies the VLAN ID of the VLAN to show its members ports. Change the VLAN ID by clicking VLAN ID value with left button on mouse.
Function Button	
Export	Click this button to save the contents of VLAN Membership List to the Personal Computer.
Close	Exit the VLAN Membership List Dialog.

xDSL MAC Spoofing Status

The xDSL MAC Spoofing displays the duplicate MAC address from two or more individual xDSL subscriber ports. Moreover, the NE supports to prevent forwarding the upstream traffic of duplicated MAC address from xDSL subscribers as they may be maybe opportunist or hacker

When the NE learns two or more duplicated MAC addresses from xDSL subscriber side learned at the same time, the NE's default action is to **allow the first MAC address and block all the others.**

However, the illegal user's MAC address may be learned firstly. To provide the operator a tool to cure the aforementioned situation, the NE supports to manually set the action to the the upstream traffic of spoofed source MAC.

Click Diagnosis → xDSL Current Status → MAC Spoofing Status on **Main Menu** to open the **MAC Spoofing Status List** Dialog as shown in Figure 11-16. Table 11-14 depicts the related parameters.

Figure 11-16 MAC Spoofing Status List Dialog

No.	Slot-Port	VPI	VCI	MAC Address	VLAN ID	Status
1	LC1-6	8	35	00:00:00:00:00:11	100	Learned Spoofed Inactive
2	LC1-23	8	35	00:00:00:00:00:11	1	Learned Spoofed Active

Table 11-14 MAC Spoofing Status List Dialog Description

Field	Description
Spoofed MAC Address	This displays the current spoofed MAC address.
List Table	
No.	This indicates the serial number of entry of the List Table.
Slot-Port	This indicates the location of xDSL port where the spoofed MAC address is observed.
VPI	This indicates the VPI of the PVC where the spoofed MAC address is observed.
VCI	This indicates the VCI of the PVC where the spoofed MAC address is observed.
MAC Address	This indicates the spoofed MAC address
Status	<p>This indicates the current status of the recorded MAC address. The definition of possible statuses is as follows.</p> <ul style="list-style-type: none"> • Learned Spoofed Active: It indicates the dynamically learned MAC address is spoofed. The NE forwards the packet from this subscriber port as it appears first. • Learned Spoofed Inactive: It indicates the dynamically learned MAC address is spoofed. The NE drop the packet from this subscriber port as it does not appears first.
Function Button	
Refresh	Click this button to refresh the Spoofed MAC Address list.
Export	Click this button to save the contents of Spoofed MAC Address List to the Personal Computer.
Close	Exit the Spoofed MAC Address List Dialog.



Whenever the NE detects spoofed MAC address, the NE launches a SNMP traps to the SNMP trap managers as specified in the section “Configuring the SNMP Trap Manager” in Chap 4.

Multicast Channel Status

Whenever the subscriber clicks his remote controller to watch a TV channel transmitted via the ADSL line, the set-top-box sends the corresponding IGMP report packet. The NE inspects the received IGMP report packet to check whether its multicast IP hits the associated multicast service profile (MSP) or not. If the multicast IP hits the associated MSP, the NE forwards the IGMP packet. In the meantime, the NE also records the multicast IP in the **Multicast Channel Status List** s shown in Figure 11-17. Refer the related information to the section “Multicast Service Profile” in Chapter 5.

Click Diagnosis → xDSL Current Status → Multicast Channel Status on **Main Menu** to open the **Multicast Channel Status List** Dialog as shown in Figure 11-17. Table 11-15 depicts the related parameters.

Figure 11-17 Multicast Channel Status List Dialog

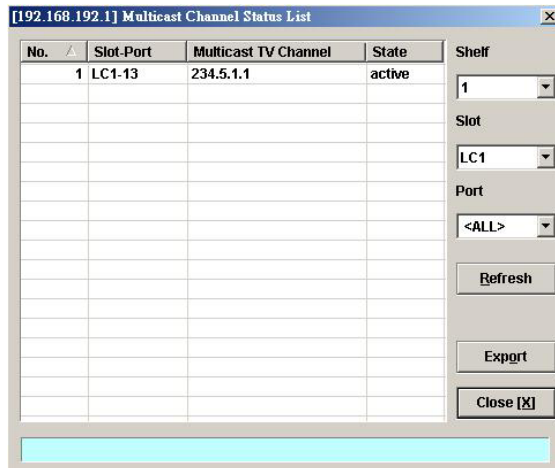


Table 11-15 Multicast Channel Status List Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
Slot-Port	This indicates the location of xDSL port.
Multicast TV Channel	This indicates that recorded multicast channel group IP address which the NE has received the corresponding IGMP report (Join) packet.
Status	<p>This indicates the current status of the multicast channel group. The definition of possible statuses is as follows.</p> <ul style="list-style-type: none"> • Active: The NE received the subscriber's IGMP report. • Poll: The NE does not receive the subscriber's IGMP report which responds to the IGMP server/proxy's IGMP query packet. • Idle: The NE retries to query the subscriber for "IGMP Robustness retry" times, but it does not get the response. In fact, the LCT will not show the entries of status equal to Idle.
Function Button	
Shelf	Use this combo-box to select the NE.
Slot	Use this combo-box to select the line card.
Port	Use this combo-box to select the xDSL ports, either one port or all ports.
Refresh	Click this button to refresh the multicast channel status.
Export	Click this button to save the contents of Multicast Channel Status List to the Personal Computer.
Close	Exit the Multicast Channel Status List Dialog.

Multicast Group Membership

The multicast group membership list displays the list of xDSL subscriber ports from which the NE has received the IGMP report (Join) packets to join a particular multicast TV channel. In other word, the multicast group membership list shows the xDSL member ports of a particular multicast TV Channel.

Click Diagnosis → xDSL Current Status → Multicast Group Membership on **Main Menu** to open the **Multicast Group Membership List** Dialog as shown in Figure 11-18. Table 11-16 depicts the related parameters.

Figure 11-18 Multicast Group Membership List Dialog

Slot	PortList	1	2	3	4	5	6	7	8	9	10
1 LC1	01-10										
2	11-20										
3	21-30										
4	31-40										
5	41-48										
6 LC2	01-10										
7	11-20										
8	21-30										
9	31-40										
10	41-48										
11 LC3	01-10										
12	11-20										
13	21-30										
14	31-40										
15	41-48										
16 LC4	01-10										
17	11-20										
18	21-30										
19	31-40										
20	41-48										
21 NC	GE										

Table 11-16 Multicast Group Membership List Dialog Description

Field	Description
Multicast TV Channel	Use this list to select the multicast TV Channel to display its members.
Last Reporter	This indicates the last xDSL subscriber launches an IGMP report to join the specified multicast TV channel. Its representation includes the location of the subscriber as well as its IP address.
Member Count	This indicates the number of xDSL subscribers currently join the specified multicast TV channel.
Up Time (sec)	This indicates the time period since the NE received the first IGMP report to join the specified multicast TV channel.
List Table	
Slot	This indicates the location of line card.
Port-List	<p>This indicates the port list number. The blue point means that the specified port is a member of the specified multicast channel.</p> <p>Note: In the case that the RSTP is disabled, “Subtend” indicates the port GE2.</p> <p>Note: In the case that the RSTP is enabled, “Subtend” indicates the “designated port” (either port GE1 or port GE2).</p>
Function Button	
Refresh	Click this button to refresh the multicast group membership list.
Export	Click this button to save the contents of Multicast Group Membership List to the Personal Computer.
Close	Exit the Multicast Group Membership List Dialog.

xDSL Downstream Broadcast Forwarding VLANs

The xDSL Downstream Broadcast Forwarding VLANs List displays the list of VLANs which are allowed to forward the downstream broadcast traffic.

Click Diagnosis → xDSL Current Status → Broadcast Filter Status on **Main Menu** to open the **xDSL Forwarding Broadcast VLANs List** Dialog as shown in Figure 11-19 and Table 11-17 depicts the related parameters.

Figure 11-19 xDSL Forwarding Broadcast VLANs List

Table 11-17 xDSL Forwarding Broadcast VLANs List Description

Field	Description
List Table	This displays current VLAN ID of VLAN which forwards the broadcast packets.
Function Button	
Slot	Use this combo-box to select the location of xDSL line card.
Refresh	Click this button to refresh the Forwarding Broadcast VLANs list.
Export	Click this button to save the contents of xDSL Forwarding Broadcast VLANs List to the Personal Computer.
Close	Exit the xDSL Forwarding Broadcast VLANs List Dialog.

DHCP Session Information

The DHCP session information list displays the DHCP transaction information on the xDSL ports.

Click Diagnosis → xDSL Current Status → DHCP Session Information on **Main Menu** to open the **DHCP Session Information** Dialog as shown in Figure 11-20. Table 11-18 depicts the related parameters.

Trunk Current Status Diagnosis

This section contains the following two subsections.

- LACP Diagnosis
- RSTP Diagnosis
- UGE VLAN List
- SFP Information List

LACP Diagnosis

Follow the subsequent procedures to view the current LACP status.

Click **Diagnosis** → **Trunk Current Status** → **Link Aggregation Status** on **Main Menu** to open the **Current Status of Link Aggregation Dialog**. Figure 11-22 shows **Current Status of Link Aggregation Dialog**, and Table 11-20 depicts the related parameters.

Figure 11-22 Current Status of Link Aggregation Dialog

Link Aggregation Type

Administrative State: disabled Refresh

Port GE1 Port GE2

Item	Current Status
Aggregator ID	
Actor System Priority	
Actor System ID	
Actor Key	
Actor Port Priority	
Actor Port ID	
Actor Operation State	
Partner System Priority	
Partner System ID	
Partner Key	
Partner Port Priority	
Partner Port ID	
Partner Operation State	

Export Close [X]

Operation State:
A: Active LACP, C: Collection Enabled, D: Distribution Enabled, E: Expired,
F: Defaulted Partner Information, G: Aggregable, S: IN_SYNC, T: Short Timeout

Table 11-20 Current Status of Link Aggregation Dialog Description

Field	Description
Link Aggregation Type	
Administrative State	This indicates the current setting of the field Link Aggregation Type of LACP for Trunk Ports Dialog .
Port GE1/ Port GE2 (Tab)	
Aggregator ID	It indicates the ID of aggregation group which the port belongs to.
Actor System Priority	It indicates the system priority configured for the LACP running on the NE.
Actor System ID	It indicates a 6-octet unique system ID for the LACP running on the NE. It is the MAC address of one of the GE port.
Actor Key	It indicates a 2-octet operational Key value of the GE port for the LACP running on the NE.
Actor Port Priority	It indicates a 2-octet port priority configured for the LACP running on the NE.
Actor Port ID	It indicates the port ID for the LACP running on the NE.
Actor Operation State	It indicates the current port status of the LACP on the NE per the IEEE 802.3 Annex 30C.6. A: lacpActivity, T: lacpTimeout(1), G: aggregation(2), S: synchronization(3), C: collecting(4), D: distributing(5), F: defaulted(6), E: expired(7)
Partner System Priority	It indicates the system priority of the peer LACP partner.
Partner System ID	It indicates a 6-octet unique system ID of the peer LACP partner.
Partner Key	It indicates a 2-octet operational Key value of GE port of the peer LACP partner.
Partner Port Priority	It indicates a 2-octet GE port priority of the peer LACP partner.
Partner Port ID	It indicates the port ID of GE port of the peer LACP partner.
Partner Operation State	It indicates the current GE port status of the peer LACP partner per the IEEE 802.3 Annex 30C.6. A: lacpActivity, T: lacpTimeout(1), G: aggregation(2), S: synchronization(3), C: collecting(4), D: distributing(5), F: defaulted(6), E: expired(7)

RSTP Diagnosis

Follow the subsequent procedures to view the current RSTP-Bridge status.

Click Diagnosis→ Trunk Current Status → RSTP Status on **Main Menu** to open the **Current**

Status of Rapid Spanning Tree Protocol– Bridge Dialog as shown in Figure 11-23. Table 11-21 depicts the related parameters.

Figure 11-23 Current Status of Rapid Spanning Tree Protocol – Bridge Dialog

Item	Configured Value / Current Status
Bridge ID	0x8000-00:11:f5:dc:7a:17
Bridge Priority	32768
Bridge Max Age	20 seconds
Bridge Hello Time	2 seconds
Bridge Forward Delay	15 seconds
Tx Hold Count	3 seconds
Time Since Last Topology Change	0 days 00:00:00
Topology Change Count	0
Designated Root ID	0x8000-00:11:f5:dc:7a:17
Root Cost	0
Root Port	--
Root Max Age	20 seconds
Root Hello Time	2 seconds
Root Forward Delay	15 seconds

Table 11-21 Current Status of Rapid Spanning Tree Protocol – Bridge Dialog Description

Field	Description
RSTP State	This indicates the enable/disable the RSTP function at GE ports.
Version	This indicates the RSTP version the NE runs.
Bridge (Tab)	
Bridge ID	It indicates an unique 8-octet bridge ID which consists of a 2-octet Bridge Priority and a 6-octet MAC address.
Bridge Priority	It indicates the configured 2-octet bridge priority.
Bridge Max Age	It indicates the configured maximum age of STP/RSTP.
Bridge Hello Time	It indicates the configured amount of time between the transmission of configuration bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so.
Bridge Forward Delay	It indicates the configured time value that controls how fast a port changes its spanning state when moving towards the Forwarding state.
Tx Hold Count	It indicates the configured Bridge Tx Hold Count.
Time Since Last Topology Change	It indicates the time since last topology change.
Topology Change Count	It indicates the count of topology changes.
Designated Root ID	It indicates the Root Bridge ID once the RSTP selects a bridge as a root bridge.
Root Cost	It indicates the total cost from the NE to the root bridge.
Root Port	It indicates the port toward the root bridge
Root Max Age	It indicates the Max Age determined by RSTP.
Root Hello Time	It indicates the Hello Time determined by RSTP.
Root Forward Delay	It indicates the Forward Delay determined by RSTP.

Port GE1/Port GE2

Follow the subsequent procedures to view the current RSTP- Port GE1/Port GE2 status.

Click the **Port GE1/Port GE2** tab in **Current Status of Rapid Spanning Tree Protocol Dialog** to launch the **Current Status of Rapid Spanning Tree Protocol –Port GE1/Port GE2 Dialog** as shown in Figure 11-24. Table 11-22 depicts the related parameters.

Figure 11-24 Current Status of Rapid Spanning Tree Protocol –Port GE1/Port GE2 Dialog

Item	Configured Value / Current Status
Port ID	0x8001
RSTP Enable State	enable
Priority	128
Configured Path Cost	default
Configured Edge Port	no
Configured Point-to-Point Link	auto
Current Operation State	broken
Forward Transitions	0
Current Path Cost	20000
Current Edge Port State	no
Current Point-to-Point Link State	yes
Designated Root ID	0x0000-00:00:00:00:00:00
Designated Cost	0
Designated BridgeID	0x0000-00:00:00:00:00:00
Designated Port ID	0x8001

Table 11-22 Current Status of Rapid Spanning Tree Protocol –Port GE1/Port GE2 Dialog Description

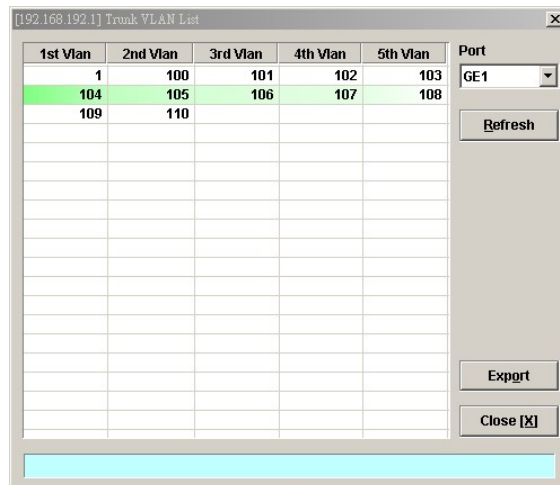
Field	Description
RSTP State	This indicates the enable/disable the RSTP function at GE ports.
Version	This indicates the RSTP version the NE runs.
Port GE 1 / Port GE 2 (Tab)	
Port ID	It indicates the port ID the GE port.
RSTP Port Enable State	It indicates the current RSTP enabled/disabled status of the GE port.
Priority	It indicates the configured port priority the GE port.
Configured Path Cost	It indicates the configured path cost of the GE port.
Configured Edge Port	It indicates whether the GE port is configured as Edge Port or not.
Configured Point-to-Point Link	It indicates the configured status of the LAN segment attached to this GE port. <ul style="list-style-type: none"> • Yes: It indicates that this port should always be treated as if it is connected to a point-to-point link. • No: It indicates that this port should be treated as having a shared media connection • Auto-detection: It indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
Current Operation State	It indicates the current operation state of GE port.
Forward Transitions	It indicates the number of times this port has transitioned from the Learning state to the Forwarding state.
Current Path Cost	It indicates the configured numerical path cost of the GE port.
Current Edge Port State	It indicates whether the GE port is edge port or not.
Current Point-to-Point Link State	It indicates whether the GE port connects with point-to-point link or not.
Designated Root ID	It indicates the unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the designated Bridge for the segment to which the port is attached.
Designated Cost	It indicates the path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path cost field in received bridge BPDUs
Designated Bridge ID	It indicates the Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port's segment.
Designated Port ID	The Port Identifier of the port on the Designated Bridge for this port's segment.

UGE VLAN List

Follow the subsequent procedures to view the current UGE VLAN status.

Click Diagnosis → Trunk Current Status → UGE VLAN Status on **Main Menu** to open the **UGE VLAN Status Dialog** as shown in Figure 11-25.

Figure 11-25 UGE VLAN Status Dialog



SFP Information List

Follow the subsequent procedures to view the current status of small form-factor pluggable (SFP) in GE ports.

Click **Diagnosis** → **Trunk Current Status** → **SFP Information** on **Main Menu** to open the **SFP Information Dialog** as shown in Figure 11-26.

Figure 11-26 Current Status of SFP Information Dialog

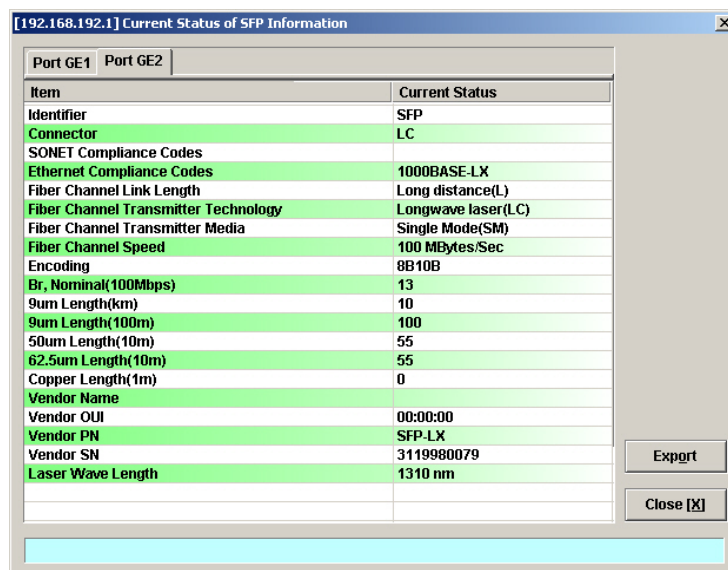


Table 11-23 Current Status of SFP Information –Port GE1/Port GE2 Dialog Description

Field	Description
Port GE 1 / Port GE 2 (Tab)	
Identifier	It indicates the identifier value specifies the physical device.
Connector	It indicates the external connector type
SONET Compliance Codes	It indicates the SONET compliance codes. (It is of no use when the SFP is of Ethrenet type.)
Ethrenet Compliance Codes	It indicates the Ethrenet compliance codes.
Fiber Channel Link Length	It indicates fiber channel link length <ul style="list-style-type: none"> • Long distance(L) • Intermediate distance(I) • Short distance(S) • Very long distance(V)
Fiber Channel Transmitter Technology	It indicates the fiber channel transmitter technology <ul style="list-style-type: none"> • Electrical inter-enclosure(EL) • Low cost long wave laser(LC) • Long wave laser (LL) • Short wave laser w/ OFC (SL) • Short wave laser w/o OFC (SN) • Electrical intra-enclosure (EL)
Fiber Channel Transmitter Media	It indicates fiber channel transmitter media <ul style="list-style-type: none"> • Single Mode (SM) • Multi-mode, 50 m (M5) • Multi-mode, 62.5m (M6) • Video Coax (TV) • Miniature Coax (MI) • Shielded Twisted Pair (TP) • Twin Axial Pair (TW)
Fiber Channel Speed	It indicates fiber channel speed. <ul style="list-style-type: none"> • 100 MBytes/Sec • 200 MBytes/Sec • 400 MBytes/Sec
Encoding	It indicates the serial encoding mechanism that is the nominal design target of the particular GBIC. <ul style="list-style-type: none"> • value 0 – Unspecified • value 1 - 8B10B • value 2 - 4B5B • value 3 – NRZ • value 4 – Manchester • value 5 - SONET Scrambled
Br, Nominal (100Mbps)	It indicates the nominal bit rate (BR, nominal) in units of 100 Megabits per second, rounded off to the nearest 100 Megabits per second.

Table 11-23 Current Status of SFP Information –Port GE1/Port GE2 Dialog Description (Continued)

Field	Description
Port GE 1 / Port GE 2 (Tab)	
9um Length(km)	It indicates the link length that is supported by the GBIC while operating in compliance with the applicable standards using single mode fiber. The value is in units of kilo-meters.
9um Length(100m)	It indicates the link length that is supported by the GBIC while operating in compliance with the applicable standards using single mode fiber. The value is in units of 100 meters.
50um Length(10m)	It indicates the link length that is supported by the GBIC while operating in compliance with the applicable standards using 50 micron multi-mode fiber.
62.5um Length(10m)	It indicates the link length that is supported by the GBIC while operating in compliance with the applicable standards using 62.5 micron multi-mode fiber.
Copper Length(1m)	It indicates the minimum link length that is supported by the GBIC while operating in compliance with the applicable standards using copper cable.
Vendor Name	It indicates the full name of the corporation, a commonly abbreviation of the corporation name will be accepted.
Vendor OUI	It indicates the vendor organizationally unique identifier that contains the IEEE Company Identifier for the vendor.
Vendor PN	It indicates the vendor part number or product name.
Vendor SN	It indicates the vendor serial number for the GBIC.
Laser Wave Length	It indicates the fibre channel transmitter wave laser length (nm).

Network Diagnosis

The NCT192 supports the following three network related diagnosis functions to check the connection between the NCT192 and NE.

- Ping NE
- Traceroute
- Telnet
- Telnet Timeout
- Check SNMP Connection

Ping NE

Use the 'Ping NE' echo to check the NE connection from NCT192 host.

Click Diagnosis → NE Connection → Ping NE on **Main Menu** to open the **Ping NE** Dialog as shown in Figure 11-27 and Table 11-24 depicts the related parameters.

Figure 11-27 Ping NE from Client Dialog

The screenshot shows a Windows-style dialog box titled "Ping NE from Client". It is divided into several sections:

- NE Section:** Contains three fields: "Location" (a dropdown menu showing "<Location>"), "NE" (a dropdown menu showing "192.168.192.1"), and "IP" (a text field showing "192 . 168 . 192 . 1").
- Ping Parameters Section:** Contains six fields: "Count" (4), "Wait (second)" (4), "Data Size (byte)" (32), "TTL" (128), "ToS" (0), and a "Don't fragment" checkbox (which is unchecked).
- Result Section:** A large, empty rectangular area for displaying the ping results.
- Buttons:** At the bottom right, there are three buttons: "Ping", "Clear", and "Close [X]".

Table 11-24 Ping NE from Client Dialog Description

Field	Description
NE	
Location	Use this combo-box to select location.
NE	Use this combo-box to select NE.
IP	This indicates the IP address of the selected NE.
Ping Parameters	
Count	Use this field to select the number of ICMP ping packets to be launched by the LCT. Valid value is 1 ~ 99.
Wait (second)	Use this field to select the waiting time of ICMP packet. Valid value is 1 ~ 30.
Data Size (byte)	Use this field to select the payload size of ICMP ping packet. Valid value is 32 ~ 9996.
TTL	Use this field to select the TTL (Time To Live) of ICMP ping packet. Valid value is 1 ~ 255.
ToS	Use this field to select the ToS (Type of Service) of ICMP ping packet. Valid value is 0 ~ 255.
Don't fragment	Check this check box to set the "Do not fragment"-bit of ICMP ping packet.
Function Button	
Ping	Start sending ICMP packets.
Clear	Clear all the result above.
Close	Exit the Ping dialog.

Traceroute

Use the “Traceroute” to check the NE connection from NCT192 host.

Click Diagnosis → NE Connection → Traceroute on **Main Menu** to open the **Traceroute NE** Dialog as shown in Figure 11-28. Table 11-25 depicts the related parameters.

Figure 11-28 Tracer Route NE from Client Dialog

The screenshot shows a dialog box titled "Traceroute NE from Client". It contains the following sections:

- NE Section:**
 - Location:** A dropdown menu with the text "<Location>".
 - NE:** A dropdown menu with the value "192.168.192.1".
 - IP:** A text field with the value "192.168.192.1".
- Traceroute Parameters Section:**
 - Ping Count:** A spin box with the value "4".
 - Max Hops:** A spin box with the value "30".
 - Wait (sec):** A spin box with the value "4".
 - ToS:** A spin box with the value "0".
 - Data Size (byte):** A spin box with the value "32".
 - Don't Fragment:** An unchecked checkbox.
- Result Section:** A large, empty text area for displaying the traceroute results.
- Buttons:** At the bottom, there are three buttons: "Trace", "Clear", and "Close [X]".

Table 11-25 Trace Route NE from Client Dialog Description

Field	Description
NE	
Location	Use this combo-box to select location.
NE	Use this combo-box to select NE.
IP	This indicates the IP address of the selected NE.
Ping Parameters	
Ping Count	Use this field to select the number of ICMP packets to be launched by the LCT. Valid value is 1 ~ 99.
Wait (second)	Use this field to select the waiting time of ICMP packet. Valid value is 1 ~ 30.
Data Size (byte)	Use this field to select the payload size of ICMP packet. Valid value is 32 ~ 9996.
Max Hops	Use this field to select the maximum number of hops of tracing. Valid value is 1 ~ 255.
ToS	Use this field to select the ToS (Type of Service) of ICMP packet. Valid value is 0 ~ 255.
Do not fragment	Check this check box to set the “Do not fragment”-bit of ICMP packet.
Function Button	
Trace	Start Traceroute by sending ICMP packets.
Clear	Clear all the result above.
Close	Exit the Trace Route dialog.

Telnet

The NCT192 allows operator to launch a Telnet window in the LCT environment.

Click Diagnosis → NE Connection → Telnet on **Main Menu** to launch the Telnet window as shown in Figure 11-29.



If the IP address of NCT192 is changed during configuration, the Telnet session will be broken. The operator needs to build a new Telnet session to continue the configuration process.



If the assigned IP has been changed and forgotten, locally access NE via Console port to retrieve the IP address assigned to the system.

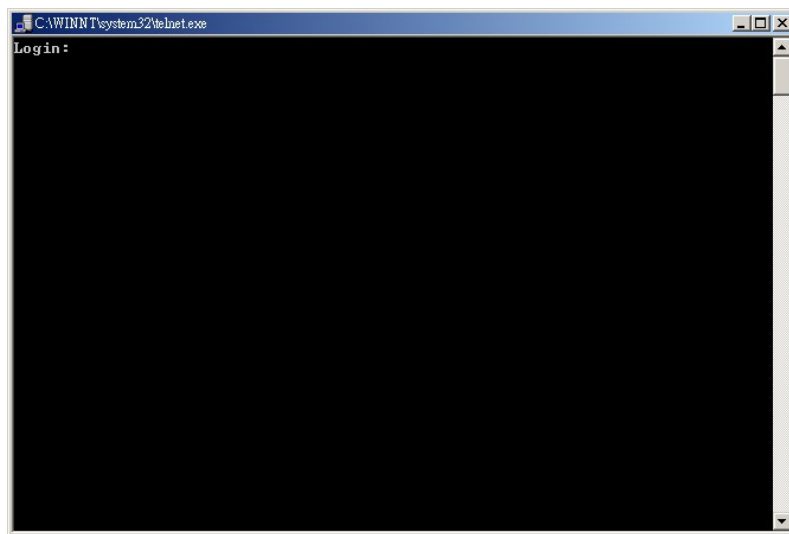


The IP address assigned must be unique in use with the device on the network segment.



A single NE supports up to 12 concurrent telnet sessions. Only one concurrent telnet session is allowed to enter by admin account user at a time (Console access included), the default “**admin**” account user is with administrator privilege level, see Section “User Account Management” of Chapter 4 for detail information.

Figure 11-29 Telnet Pop-up Window

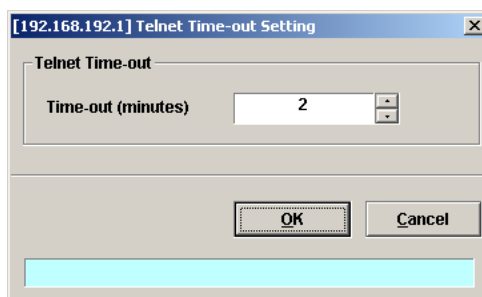


Telnet Timeout

Use the 'Telnet Time-out' to set the telnet time out of the system.

Click Configuration → NE Management → NE Connection → **Telnet Time-out** on **Main Menu** to open the **Telnet Time-out Setting** Dialog as shown in Figure 11-30.

Figure 11-30 Telnet Time-out Setting Dialog



The range of telnet timeout is from 2 minutes to 1440 minutes. The default value is 2 minutes.

Check SNMP Connection

Use the 'SNMP Connection' to check whether the connection between NE and NCT192 host is normal or not.

Click Diagnosis → NE Connection → SNMP Connection on **Main Menu** to open the **SNMP Connection** Dialog as shown in Figure 11-31 and Table 11-26 depicts the related parameters.

Figure 11-31 Check NE SNMP Connection Dialog

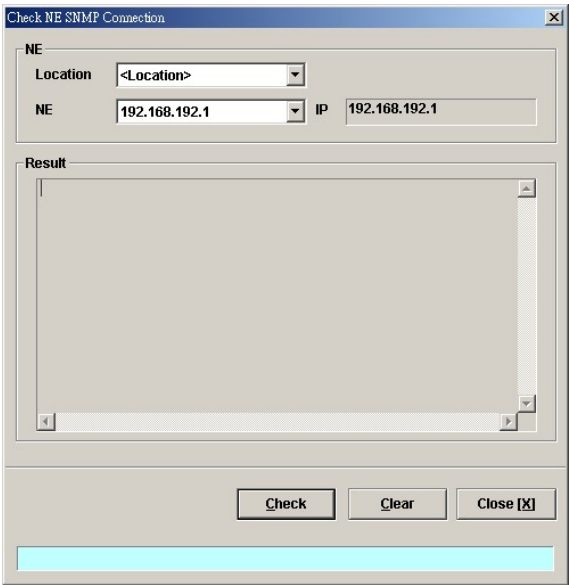


Table 11-26 Check NE SNMP Connection Dialog Description

Field	Description
NE	
Location	Use this combo-box to select location.
NE	Use this combo-box to select NE.
IP	This indicates the IP address of the selected NE.
Function Button	
Check	Start checking the SNMP connection.
Clear	Clear all the result above.
Close	Exit the Check NE SNMP Connection Dialog.

Chapter 12 General System Management

This chapter details the various operations that need to be carried out to setup and start services.

- NCT192 Options

NCT192 Options

Configuring the Alarm Warning Options

The NCT192 supports to notify the operators whenever there is an alarm sent from the NE. The operator is allowed to control the NCT192 to notify by flashing the alarm on the multimedia view (see Figure 3-2) and/or playing a audio file.

Click System → Option on **Main Menu** to open the **Client Options** Dialog as shown in Figure 12-1. Table 12-1 depicts the related parameters.

Figure 12-1 Client Options Dialog – Alarm Warning

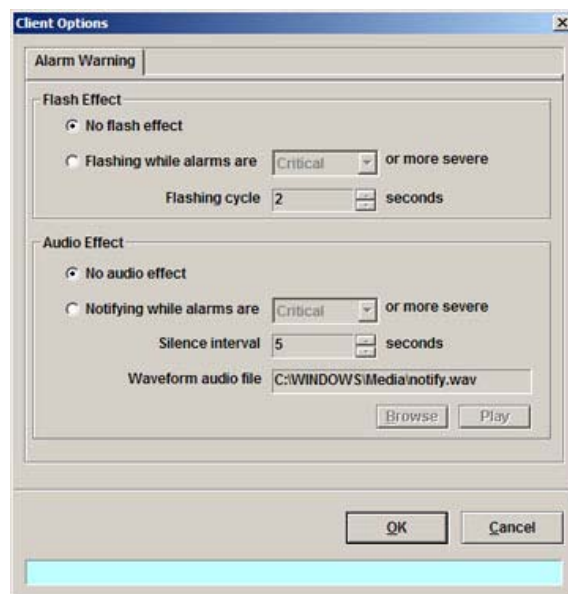


Table 12-1 Client Options Dialog – Alarm Warning Description

Field	Description
Flash Effect	
No flash effect	This option button disables the alarm warning flash effect.
Flashing condition and cycle	This option button enables the alarm warning flash effect. You can control the alarm severity and flashing cycles.
Audio Effect	
No audio effect	This option button disables the audio effect.
Notifying condition and interval	This option button enables the audio effect. You can control the alarm severity and the silence interval between two audio notifications.

Field	Description
Waveform audio file	This specifies the sound file of audio effect. Click 'Browse' button to select file and click 'Play' to test.

Table 13-1 Inventory Information List Dialog Description

Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
Slot	This indicates the location of board.
Planned Type	This indicates the board type planned to be equipped to the slot of NCT192 IP-DSLAM. If the planned type is mismatched (removed or type error) with online type detected from the system, the board mismatch alarm message will be reported.
Online Type	This indicates the observed board type of the card module in the slot (current type).
System Up Time	This indicates the system up time of NE.
Software Version	This indicates the software version of NC and LC.
Hardware Version	This indicates the hardware version of NC and LC.
Serial Number	This indicates the serial number of NC and LC.
Function Button	
Refresh	Click this button to refresh the inventory information.
Export	Click this button to save the contents of Inventory Information List to the Personal Computer.
Close	Exit the Inventory Information List Dialog Dialog.

NE Configuration Backup and Restore

Follow the subsequent procedure to backup and restore the configuration data file of NE on local LCT PC through FTP.

- Step 1** Click Configuration → NE Management → Backup & Restore on **Main Menu** to open the **NE Configuration Backup & Restore** Dialog as shown in Figure 13-2 and Table 13-2 depicts the related parameters.
- Step 2** To backup the configuration file, please input a valid administrative level username/password and give your backup file a file name, then click '**Backup**' button.
- Step 3** To restore the configuration file, click '**Browse**' and choose the target file from the backup file directory, then click '**Restore**' button.
- Step 4** After restoring the configuration data, it is noted that the NE needs to be rebooted to make the configuration data take effect.



You can also select and highlight the NE from the **Network Tree View** to progress the NE configuration Backup & Restore by right click of pop-up menu, NE Management → NE Backup & Restore.



It is noted that login device via FTP must be used the read-write authorization. The default username/password is **admin/admin**.

Figure 13-2 NE Configuration Backup & Restore File List Dialog

Table 13-2 NE Configuration Backup & Restore File List Dialog Description

Field	Description
FTP Login	
FTP User Name	Fill the administrative level username of FTP.
FTP Password	Fill the comparative password of the administrative level username.
Local Backup File	
Browse	Click this button to open the file choice window.
Function Button	
Backup	Start to backup the configuration data file of NE by saving it as the specified file on the local LCT PC through FTP.
Restore	Start to restore the configuration of NE by sending the specified NE configuration file to NE from the the local LCT PC via FTP.
Close	Exit the Configuration Backup & Restore Dialog.

NE Firmware Upgrade

NCT192 provides the “NE Firmware Upgrade” dialog to upgrade the NC/ADSL LC firmware image to NE through FTP.

Follow the subsequent procedure to upgrade the NC/ADSL LC firmware image. It is noted that the NE needs to be rebooted to execute the new image.

- Step 1** Click Configuration → NE Management → Firmware Upgrade on **Main Menu** to open the **NE Firmware Upgrade** Dialog as shown in Figure 13-3. Table 13-3 depicts the related parameters.
- Step 2** Click ‘**Browse**’ button to choose the suitable code file from host directory.
- Step 3** Click ‘**Upgrade**’ button to process.
- Step 4** Reset the NC or ADSL LC to execute the upgraded firmware.

Figure 13-3 NE Firmware Upgrade Dialog

The screenshot shows the 'NE Firmware Upgrade & Backup' dialog box. It is divided into three main sections. The first section, 'FTP Login', contains two input fields: 'FTP User Name' with the value 'admin' and 'FTP Password'. The second section, 'Local Firmware File', contains a 'File Name' input field, a 'Browse' button, a 'Firmware Type' dropdown menu currently set to 'Network board firmware', and a 'Detail' button. The third section, 'NE Boot Partition', contains three input fields: 'Backup / Restore Partition' with 'opCodeA', 'Current Boot Partition' with 'opCodeB', and 'Next Time Boot Partition' with 'opCodeB'. There is a 'Change' button next to the 'Next Time Boot Partition' field. At the bottom of the dialog are three buttons: 'Backup', 'Upgrade', and 'Close [X]'. A status bar at the very bottom is highlighted in light blue.



Make sure the source image file that you select is accordant to the NE model; else the NE may not run well with the upgraded firmware image after rebooting.

Table 13-3 NE Firmware Upgrade Dialog Description

Field	Description
FTP Login	
FTP User Name	This indicates the user name of NE with administrator right.
FTP Password	This indicates the password of FTP to access NE with administrator right.
Local Firmware File	
File Name	Click the 'Browse' button to select a file of NC firmware or an ADSL LC firmware from your local host.
Firmware Type	This indicates the firmware type for upgrade. Click 'Detail' button to display the information of selected file.
NE Boot Partition (also refer to NE Boot Partition)	
Backup / Restore Partition	This specifies the boot partition where the upgraded file to be placed to or backup from.
Current Boot Partition	This specifies the current boot partition.
Next Time Boot Partition	This indicates the partition of NE for next booting. Click 'Change' button to change boot partition.
Function Button	
Backup	Start to backup the NC/ADSL LC firmware image of NE by saving it as the specified file on the local LCT PC through FTP.
Upgrade	Start to upgrade the NC/ADSL LC firmware image of NE by sending the specified file on the local LCT PC through FTP.
Close	Exit the Configuration Backup & Restore Dialog.

Table 13-4 NE SHDSL Firmware Upgrade Dialog Description

Field	Description
FTP Login	
FTP User Name	This indicates the user name of NE with administrator right.
FTP Password	This indicates the password of NE with administrator right.
Local SHDSL Firmware File	
File Name	Click the 'Browse' button to select a file of SHDSL firmware from your local host.
FTP	Click this button to upload SHDSL firmware to the NC.
Current Upgrading Status	This indicates the status of SHDSL line card. Upgrading is available only when the status is "initial".
Upgrade	Click this button to upgrade the new image from NC to SHDSL LC.
Refresh	Click this button to refresh the status during firmware updating.
Export	Click this button to save the contents of NE SHDSL Firmware Upgrade to the local LCT PC.
Close	Exit the NE SHDSL Firmware Upgrade Dialog.

NE Boot Partition

The NE supports two boot sections 'opCodeA' and 'opCodeB', each contains the necessary firmware for the system. With 2 boot sections, the original NE firmware can be kept as it is. As a result, the operator is able to recover the NE whenever it fails to upgrade NE firmware due to any reason (ex. the upgraded firmware is corrupted due to network failure.)

To this end, it is recommended the operator to upload the new firmware to the 'opCodeA' if the current boot partition is 'opCodeB'.

Follow the subsequent procedure to select boot partition when the NC reboots.

- Step 1** Click Configuration → NE Management → Boot Partition on **Main Menu** to open the **NE Firmware Boot Partition** Dialog as shown in Figure 13-5 .Table 13-5 depicts the related parameters.
- Step 2** Select the boot partition form 'Next Time Boot Partition' field to decide the booting image the NE will run whenever it is rebooted.

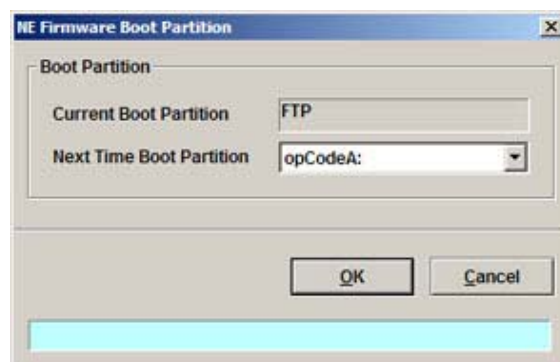
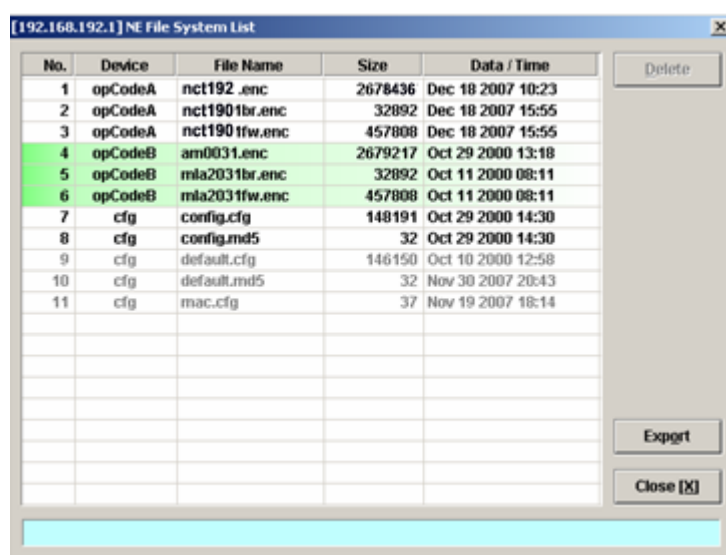
Figure 13-5 NE Firmware Boot Partition Dialog

Table 13-5 NE Firmware Boot Partition Dialog Description

Field	Description
Current Boot Partition	This indicates the current boot partition.
Next Time Boot Partition	Use this combo-box to select the next boot partition.
Function Button	
OK	Commit the configuration.
Cancel	Cancel the setting.

NE File System List

Click Configuration → NE Management → File System List, on **Main Menu** to open the **NE File System List** Dialog as shown in Figure 13-6. Table 13-6 depicts the related parameters.

Figure 13-6 NE File System List Dialog**Table 13-6 NE File System List Dialog Description**

Field	Description
Device	This indicates the boot partitions (opCodeA and opCodeB) and the configuration partition (cfg).
File Name	This indicates the filename of firmware where Device is either “opCodeA” or “opCodeB”. In the column where Device is “cfg”, it indicates the filename of NE’s configuration files.
Size	This indicates the file size
Date/Time	This indicates the time when the file is saved (or uploaded).
Function Button	
Delete	Click this button to delete the selected file.
Export	Click this button to save the contents of NE File System List to the local LCT PC.
Close	Exit the NE File System List Dialog.



It is noted that the following files can not be deleted via CLI/LCT.

default.cfg
default.md5
mac.cfg



Two kinds of .cfg files, config.cfg and default.cfg, are kept in the NE for the NE to boot up with a set of deterministic configuration parameters. In order to guarantee these .cfg files are not corrupted, the NE also protect them by MD5 encryption.

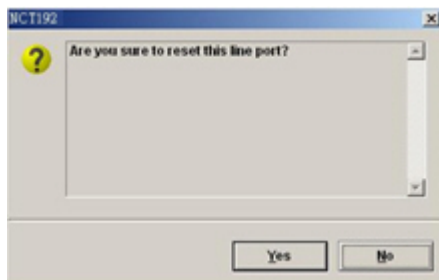
Whenever the NE boots up, it executes the following procedure.

1. The NE first reads and checks config.cfg and try to rebuild the previous configuration accordingly.
2. If the config.cfg is absent or is corrupted, the NE will read and check default.cfg and try to rebuild the default configuration accordingly.
3. If the default.cfg is absent or is corrupted, the NE will use its internal setting to rebuild the factory-default configuration accordingly

Reset the Unit

Select the NC/LC or Port object, use right mouse button to bring out the menu, select the 'Reset' option to launch the **Reset the Unit Dialog** as shown in Figure 13-7.

Figure 13-7 **Reset the Unit Dialog**



Appendix A Abbreviations and Acronyms

The abbreviations and acronyms used in this document.

Table A-1 Abbreviations and Acronyms Table

Abbreviations	Full Name
AAL	ATM Adaptation Layer
ADSL	Asymmetric Digital Subscriber line
AIS	Alarm Indication Signal
ATM	Asynchronous Transfer Mode
ATU-C	ADSL Transceiver Unit at the central office end
ATU-R	ADSL Transceiver Unit at the remote end
CBR	Constant Bit Rate
CV	Coding Violation
DSLAM	Digital Subscriber line Access Multiplexer
ES	Error Seconds
EOA	Ethernet over ATM
GE	Gigabit Ethernet
IP	Internet Protocol
LAN	Local Area Network
LOF	Loss of Frame
LOS	Loss of Signal
LPR	Loss of Power
OAM	Operation, Administration, and Maintenance
PADI	PPPoE active discovery initiation
PADR	PPPoE active discovery request
PADT	PPPoE active discovery terminate
PCR	Peak Cell Rate
PSD	Power Spectral Density
PVC	Permanent Virtual Channel
rtVBR	Real time Variable Bit Rate
SCR	Sustainable Cell Rate
SNR	Signal-to Noise Ratio
SNMP	Simple Network Management Protocol
UAS	Unavailable Seconds
UBR	Unspecified Bit Rate
VC	Virtual Channel
VCI	Virtual Channel Identify
VCL	Virtual Channel Link
VDSL	Very high-speed Digital Subscriber line
VLAN	Virtual Local Area Network
VP	Virtual Path
VPI	Virtual Path Identifier
VTU-O	VDSL Transmission Unit at the Optical network interface
VTU-R	VDSL Transmission Unit at the remote end
WAN	Wide Area Network

Abbreviations	Full Name
xDSL	ADSL/VDSL

Appendix B Alarm Definition

Describe all the alarm in the NCT192 Alarm Definition.

Table B-1 Alarm Definition

NE Model	Module Name	Alarm Name	Default Severity	Alarm Description
All	noEntity	EMPTY	No	Neither plan type nor on-line type configured
NCT192	CPU Module	MISSING	Major	CPU Module is off-line
		TEMP	Major	Temperature is over the threshold
		VOL	Major	Voltage is below the threshold
		MISMATCH	Major	Planned type and online type are mismatched
		TCA_DHCP_BC	Warning	DHCP broadcast request rate threshold-crossing alert
	ADSL Module	MISSING	Major	ADSL module is off-line
		TEMP	Major	Temperature is over the threshold
		VOL	Major	Voltage is below the threshold
		MISMATCH	Major	Planned type and online type are mismatched
		NOT_OPERABLE	Major	ADSL line card is not operable
	Power Module	MISSING	Major	Power module is off-line
		NOT_OPERABLE	Major	Power card is not operable
	Fan Module	MISSING	Major	Fan module is off-line
		FAN1_SPEED	Major	Fan1 speed is below the threshold
		FAN2_SPEED	Major	Fan2 speed is below the threshold
		VOL	Major	Voltage is below the threshold
	ADSL Port	ES_NE_15_MIN	Minor	15 min near end ES is over threshold
		SES_NE_15_MIN	Minor	15 min near end SES is over threshold
		UAS_NE_15_MIN	Minor	15 min near end UAS is over threshold
		ES_FE_15_MIN	Minor	15 min far end ES is over threshold
		SES_FE_15_MIN	Minor	15 min far end SES is over threshold
		UAS_FE_15_MIN	Minor	15 min far end UAS is over threshold
		ES_NE_1_DAY	Minor	1 day near end ES is over threshold
		SES_NE_1_DAY	Minor	1 day near end SES is over threshold
		UAS_NE_1_DAY	Minor	1 day near end UAS is over threshold
		ES_FE_1_DAY	Minor	1 day far end ES is over threshold
		SES_FE_1_DAY	Minor	1 day far end SES is over threshold
		UAS_FE_1_DAY	Minor	1 day far end UAS is over threshold
		LOS	Minor	Loss of signal
		LOF	Minor	Loss of frame
		LPWR	Warning	CPE loss of power
		GEN_LINE_INIT_FAIL	Minor	Generic line initialization failure
		CONFIG_ERROR	Minor	Line initialization failure - configuration error
		HIGH_BIT_RATE	Minor	Line initialization failure - high bit rate

NE Model	Module Name	Alarm Name	Default Severity	Alarm Description
		COMM_PROBLEM	Minor	Line initialization failure - communication problem
		NO_PEER_DETECTED	Minor	No peer detected
		TRAINING	Warning	Port is under training
		NO_CONFIG	Information	Port is not configured
		PS_L2_MANUAL	Information	ADSL2/ADSL2+ Power State transfers to L2 by manual mode
NCT192	ADSL Port	PS_L2_AUTO	Information	ADSL2/ADSL2+ Power State transfers to L2 by automatic mode
		PS_L3_CO	Information	ADSL2/ADSL2+ Power State transfers to L3 by CO side
		PS_L3_CPE	Information	ADSL2/ADSL2+ Power State transfers to L3 by CPE side
		ILLEGAL_IP	Warning	Packets with illegal IP addresses have been dropped
		ILLEGAL_MAC	Warning	duplicate MAC addresses from different line ports are made out
		DISABLED	Information	The port is disabled
	GE Port	MISSING	Major	GE Port is off-line
		NOT_OPERABLE	Major	GE Port is not operable
		STP_LEARN	Information	GE port is transited to STP-learning state
		STP_BLOCK	Information	GE port is transited to STP-blocking state
		DISABLED	Information	GE port is disabled
	Alarm Relay Module	MISSING	Major	Alarm relay module is off-line
	Alarm Relay Port	MISSING	Major	Alarm relay port is off-line
		RELAY_ABNORMAL	Major	The alarm relay port is under abnormal status
		DISABLED	Information	The alarm relay port is disabled
	SHDSL Module	MISSING	Major	SHDSL module is off-line
		TEMP	Major	Temperature is over the threshold
		VOL	Major	Voltage is below the threshold
		MISMATCH	Major	Planned type and online type are mismatched
		NOT_OPERABLE	Major	Line card is not operable
	SHDSL Port	TCA_ES_NE_15_MIN	Minor	15-min near end ES is over the threshold
		TCA_SES_NE_15_MIN	Minor	15-min near end SES is over the threshold
		TCA_UAS_NE_15_MIN	Minor	15-min near end UAS is over the threshold
		TCA_CRC_NE_15MIN	Minor	15-min near end CRC is over the threshold
		TCA_LOSW_NE_15MIN	Minor	15-min near end LOSW is over the threshold
		TCA_SNR_NE	Minor	Near end SNR margin is over the threshold
		TCA_ATTN_NE	Minor	Near end loop attenuation is over the threshold
		OPI	Information	Operation state change indication
		LOS	Minor	Loss of signal (FOH lost bit)
		SEGA	Minor	Segment anomaly - CRC anomaly (FOH sega bit)
		LPR	Minor	Loss of power - power status (FOH ps bit)
		SEGD	Minor	Segment defect - LOSW defect (FOH segd bit)
		PBO_NE	Minor	Near end enhanced power back off
		DEVFAULT_NE	Minor	Near end device fault - Diagnostic or self-test fault

NE Model	Module Name	Alarm Name	Default Severity	Alarm Description
		DCCONT_NE	Minor	Near end DC continuity fault - interfere with span powering
		LOSW_NE	Minor	Near end LOSW failure
		INI_CFG_NE	Minor	Near end indicates Far end not able to support requested configuration
		INI_PROTOCOL_NE	Minor	Near end indicates incompatible protocol used by Far end
		NOPEER	Minor	No peer detected
		PBO_FE	Minor	Far end enhanced power back off
		DEVFAULT_FE	Minor	Far end device fault - Diagnostic or self-test fault
		DCCONT_FE	Minor	Far end DC continuity fault - interfere with span powering
NCT192	SHDSL Port	LOSW_FE	Minor	Far end LOSW failure
		INI_CFG_FE	Minor	Far end indicates Near end not able to support requested configuration
		INI_PROTOCOL_FE	Minor	Far end indicates incompatible protocol used by Near end
		DISABLED	Information	The port is disabled

Appendix C: 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

Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website www.netcomm.com.au.

Technical Support

If you have any technical difficulties with your product, please refer to the support section of our website.

www.netcomm.com.au/support

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 the User Guide or contact a Network Specialist.

NetComm®
www.netcomm.com.au

NETCOMM LIMITED PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: sales@netcomm.com.au **W:** www.netcomm.com.au

 **Dynalink**
www.dynalink.co.nz

DYNALINK NZ 224b Bush Road, Albany, Auckland, New Zealand
P: 09 448 5548 **F:** 09 448 5549
E: sales@dynalink.co.nz **W:** www.dynalink.co.nz