

AMS LCT

Software Operation Guide

Class:	User Guide
Product Name:	AMS LCT
Product Version:	4.7.3.4
Doc. No.:	BCD3-TM-E-210502
Doc. Version:	1.4.0
Publish Date:	2008-Dec-30

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. PRODUCT AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL PRODUCT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF PRODUCT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AMS LCT
Software Operation Guide
Text Part Number: 2105-0214

Table of Contents

<u>Chapter 1 Preface.....</u>	<u>1</u>
Purpose.....	1
Organization.....	1
Conventions.....	1
Revision History.....	4
<u>Chapter 2 DAS4 Series Management System Overview.....</u>	<u>10</u>
AMS LCT Overview.....	10
AMS LCT Features.....	10
System Hardware and Software Requirement.....	10
<u>Chapter 3 Getting Started AMS LCT.....</u>	<u>12</u>
Installing the AMS LCT.....	12
Starting a AMS LCT Session.....	13
Navigating of AMS LCT.....	14
Keyboard Commands.....	15
Right Mouse Button.....	15
AMS LCT Window Overview.....	15
Managing the Trap Log View.....	15
Icons and LED Sign Overview.....	17
Error Handling Dialog.....	19
Data Exporting and Graphic Displaying.....	20
<u>Chapter 4 Initiating the NE.....</u>	<u>22</u>
Constructing the NE Objects.....	22
NE SNMP Management.....	28
Configuring the SNMP Trap Manager.....	28
Configuring the SNMP Community.....	30
User Account Management.....	31
Secured Host Management.....	33
NE Date and Time Management.....	34
DNS Server Setting.....	35
Time Server Setting.....	36
Managing the NE Configuration.....	38
Saving NE configuration to Flash.....	38
Erasing NE configuration from Flash.....	38
<u>Chapter 5 Interface Profile Management.....</u>	<u>40</u>
Configuring the xDSL Profile.....	42
ADSL Profile.....	42
SHDSL Profile.....	56
Configuring the VLAN Profile.....	61
IP Traffic Profile.....	61
TV Channel Profile.....	63
Multicast Service Profile.....	65
Configuring the Alarm Definition Profile.....	66
<u>Chapter 6 Interface Port Management.....</u>	<u>70</u>
xDSL Line Interface Management.....	70
GE Network Interface Management.....	73
Link Aggregation (Static / Dynamic).....	76
RSTP Configuration.....	78
CoS Configuration.....	81
Manual VLAN Setting.....	84
Cascaded NE Management.....	85
Configuring the NE Role.....	87
Adding Remote NE.....	88

<u>Chapter 7 Connection Port Management.....</u>	<u>92</u>
VC-to-VLAN Connection Management.....	92
ISP Information for IP over ATM.....	103
Access Control List.....	105
NetBIOS/NetBEUI Packet Filtering.....	105
Source MAC Access Control List.....	105
Packet filter.....	109
Static MAC configuration on xDSL Port.....	117
Multicast Service Management.....	119
Multicast Channel Configuration.....	119
IGMP snooping/IGMP proxy Configuration.....	121
System Services Configuration.....	124
MAC Aging for Bridged Services.....	124
VLAN MAC Limit.....	124
DHCP Service Configuration.....	126
PPPoE Sub-option Configuration.....	129
xDSL Port Agent ID Management.....	129
<u>Chapter 8 Fast Provision Management.....</u>	<u>132</u>
Interface and VC-VLAN Fast Provisioning.....	132
Multicast Service Fast Provisioning.....	142
<u>Chapter 9 Performance Management.....</u>	<u>146</u>
xDSL Line Current Performance Information.....	146
xDSL Line Historical Performance Information.....	149
GE Interface Performance Statistics.....	152
<u>Chapter 10 Fault Management.....</u>	<u>154</u>
NE Alarm Information.....	154
System Alarm Management.....	156
Alarm Synchronization.....	157
Relay Input Alarm Management.....	157
Relay-Output Alarm Management.....	159
Hardware Status Monitoring.....	160
<u>Chapter 11 Diagnosis Management.....</u>	<u>164</u>
xDSL Line Status Diagnosis.....	164
Port Rate Status.....	164
Bits Allocation Monitoring.....	166
Loop Monitoring.....	168
Loop Diagnosis (DELT <Dual-Ended Line Test>).....	171
Loop SELT Test (Single End Loop Test).....	174
xDSL Service Status Diagnosis.....	175
ATM OAM F5 VC Diagnosis.....	175
Bridge Filtering Database.....	176
VLAN Membership.....	183
xDSL MAC Spoofing Status.....	185
Multicast Channel Status.....	186
Multicast Group Membership.....	187
xDSL Downstream Broadcast Forwarding VLANs.....	189
DHCP Session Information.....	189
PPPOE Session Information.....	190
Trunk Current Status Diagnosis.....	192
LACP Diagnosis.....	192
RSTP Diagnosis.....	193
UGE VLAN List.....	196
SFP Information List.....	197
Network Diagnosis.....	199
Ping NE.....	199
Traceroute.....	201

Telnet.....	202
Telnet Timeout.....	203
CLI Prompt Setting.....	203
Check SNMP Connection.....	204
<u>Chapter 12 General System Management.....</u>	206
AMS LCT Options.....	206
Configuring the Alarm Warning Options.....	206
<u>Chapter 13 Administrating and Maintenance.....</u>	208
NE Inventory Information.....	208
NE Configuration Backup and Restore.....	209
NE Firmware Upgrade.....	210
SHDSL LC Firmware Upgrade	212
NE Boot Partition.....	213
Reset the Unit.....	215

List of Figures

Figure 3-1 AMS LCT Login Dialog.....	14
Figure 3-2 AMS LCT Operation Window.....	15
Figure 3-3 AMS LCT Trap Log View.....	16
Figure 3-4 Detailed Alarm & Event Dialog.....	16
Figure 3-5 Trap Log Filter Dialog.....	17
Figure 3-6 Error Handling Message.....	19
Figure 3-7 Export Dialog.....	20
Figure 3-8 2D/3D Data Graph Displaying Dialog.....	21
Figure 4-9 Board Setting List Dialog.....	23
Figure 4-10 xDSL Board Setting Dialog.....	24
Figure 4-11 NC Boarding Setting Dialog	25
Figure 4-12 NE SNMP Manager IP Address List Dialog.....	28
Figure 4-13 Add NE SNMP Manager IP Address Dialog.....	29
Figure 4-14 NE SNMP Community List Dialog.....	30
Figure 4-15 Add NE SNMP Community Dialog.....	31
Figure 4-16 NE User Account List Dialog.....	31
Figure 4-17 NE User Account Setting Dialog.....	32
Figure 4-18 NE Secured Host List Dialog.....	33
Figure 4-19 NE Secured Host Setting Dialog.....	34
Figure 4-20 NE System Time Dialog.....	35
Figure 4-21 DNS Server Setting Dialog.....	36
Figure 4-22 NE Time Server Status Dialog.....	36
Figure 4-23 NE Time Server Setting Dialog.....	37
Figure 4-24 NE Write Flash Confirm Dialog.....	38
Figure 4-25 NE Erase Flash Confirm Dialog.....	39
Figure 5-26 Interrelationship of Data Transport Related Profiles.....	40
Figure 5-27 xDSL Profile List Dialog Function Button.....	42
Figure 5-28 ADSL Profile List – Line Dialog.....	43
Figure 5-29 Add ADSL Line Profile– Transmission Rate Dialog.....	44
Figure 5-30 Add ADSL Line Profile–Line Standard Dialog.....	45
Figure 5-31 Add ADSL Line Profile– SNR Margin Dialog.....	46

Figure 5-32 Add ADSL Line Profile– PSD Dialog.....	48
Figure 5-33 Add ADSL Line Profile– Power Management Dialog.....	50
Figure 5-34 Add ADSL Line Profile– INP Dialog.....	51
Figure 5-35 xDSL Profile List– PM Threshold Dialog.....	53
Figure 5-36 Add ADSL PM Threshold Profile Dialog.....	53
Figure 5-37 xDSL Profile List– Traffic Policing Dialog.....	55
Figure 5-38 Add Traffic Policing Profile Dialog.....	55
Figure 5-39 SHDSL Profile List– Line Dialog.....	56
Figure 5-40 Add SHDSL Line Profile– Transmission Rate Dialog.....	57
Figure 5-41 Add SHDSL Line Profile– SNR Margin Dialog.....	58
Figure 5-42 Add SHDSL Line Profile– Miscellaneous Dialog.....	58
Figure 5-43 SHDSL Profile List– PM Threshold Dialog.....	60
Figure 5-44 Add SHDSL PM Threshold Profile Dialog.....	60
Figure 5-45 VLAN Profile List– IP Traffic Dialog.....	62
Figure 5-46 Add xDSL IP Traffic Profile Dialog.....	63
Figure 5-47 VLAN Profile List– TV Channel Dialog.....	64
Figure 5-48 Add xDSL TV Channel Profile Dialog.....	64
Figure 5-49 VLAN Profile List– Multicast Service Dialog.....	65
Figure 5-50 Add xDSL Multicast Service Profile Dialog.....	65
Figure 5-51 Alarm Definition List Dialog.....	66
Figure 5-52 Modify Alarm Definition Dialog.....	67
Figure 6-53 ADSL Port List Dialog.....	70
Figure 6-54 ADSL Port Modification Dialog.....	72
Figure 6-55 SHDSL Port Modification Dialog.....	73
Figure 6-56 GE Network Interface Packet Forward Illustrate.....	74
Figure 6-57 Illustration of 3 DAS4-Series IP-DSLAMs are connected in a Daisy-Chain topology.....	74
Figure 6-58 Trunk Port Dialog.....	74
Figure 6-59 Trunk Port Configuration Dialog.....	75
Figure 6-60 Typical GE-Channel Configuration.....	76
Figure 6-61 Link Aggregation Setting Dialog.....	77
Figure 6-62 Rapid Spanning Tree Active Topology.....	78
Figure 6-63 Trunk RSTP Setting– Bridge Dialog.....	79

Figure 6-64 Trunk RSTP Setting– Port GE1/Port GE2 Dialog.....	80
Figure 6-65 DiffServ Field.....	82
Figure 6-66 Trunk CoS Mapping and DSCP Re-mapping Dialog.....	84
Figure 6-67 Manual VLAN Setting Dialog	85
Figure 6-68 Illustration of cascading topology.....	86
Figure 6-69 Illustration the IP configuration of NEs in a cascading topology	86
Figure 6-70 Cascaded Management Setting Dialog.....	87
Figure 6-71 Remote NE List Dialog.....	88
Figure 6-72 Remote NE Setting Dialog.....	89
Figure 7-73 VC-to-VLAN Mapping Illustrate.....	92
Figure 7-74 RFC 2684 Route Mode Connection Method.....	93
Figure 7-75 xDSL VC-to-VLAN List Dialog.....	94
Figure 7-76 xDSL VC-to-VLAN Setting – IP Traffic Dialog.....	95
Figure 7-77 xDSL VC-to-VLAN Setting – 802.1Q/1P Dialog (only for the RFC2684 bridged mode).....	95
Figure 7-78 xDSL VC-to-VLAN Setting – 802.1P Dialog (only for the RFC2684 routed mode).....	96
Figure 7-79 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 bridged mode.....	96
Figure 7-80 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 routed mode.....	97
Figure 7-81 xDSL VC-to-VLAN Setting – Next-hop Dialog (only for the RFC2684 routed mode).....	97
Figure 7-82 xDSL VC-to-VLAN Setting – Service Type Dialog.....	98
Figure 7-83 RFC 2684 Route Mode Connection Method.....	103
Figure 7-84 xDSL Next-hop List for IPoA Dialog.....	104
Figure 7-85 Add xDSL Next-hop for IPoA Dialog.....	104
Figure 7-86 Packet Filtering Dialog.....	105
Figure 7-87 VC-to-VLAN Access Control List dialog.....	106
Figure 7-88 Add xDSL Access Control Dialog.....	107
Figure 7-89 xDSL Access Control List.....	108
Figure 7-90 xDSL Slot Selection of Packet Filter.....	110
Figure 7-91 xDSL Packet Filter of Ethernet Type Only.....	110

Figure 7-92 xDSL Packet Filter of Known Protocol.....	111
Figure 7-93 xDSL Fully Configured Packet Filter.....	112
Figure 7-94 xDSL Packet Filter Group for Upstream.....	114
Figure 7-95 xDSL Packet Filter Group for Downstream.....	115
Figure 7-96 Implying the xDSL Packet Filter Group to the specified ADSL port	116
Figure 7-97 xDSL Configured Bridge Filtering Database Entry List dialog	117
Figure 7-98 xDSL Static MAC Address Setting Dialog.....	119
Figure 7-99 xDSL Multicast Channel List Dialog.....	120
Figure 7-100 xDSL Multicast Channel Setting Dialog.....	121
Figure 7-101 IGMP Snooping / IGMP Proxy Setting Dialog.....	122
Figure 7-102 MAC Aging Setting Dialog.....	124
Figure 7-103 VLAN MAC Limit List Dialog.....	125
Figure 7-104 VLAN MAC Limit Configure Dialog.....	126
Figure 7-105 DHCP Setting Dialog.....	127
Figure 7-106 DHCP Server List for DHCP Relay Dialog.....	127
Figure 7-107 DHCP Broadcast Control Dialog.....	128
Figure 7-108 PPPoE Sub-option Setting Dialog.....	129
Figure 7-109 xDSL Port Agent ID List.....	130
Figure 8-110 xDSL Port & VC-to-VLAN Fast Provision – Port Setting Dialog	133
Figure 8-111 xDSL Port & VC-to-VLAN Fast Provision – Channel Setting Dialog.....	133
Figure 8-112 xDSL Port & VC-to-VLAN Fast Provision – IP Traffic Dialog	134
Figure 8-113 xDSL Port & VC-to-VLAN Fast Provision – MAC Control Dialog	134
Figure 8-114 xDSL Port & VC-to-VLAN Fast Provision – Next-hop Dialog (only for the RFC2684 routed mode).....	135
Figure 8-115 xDSL Port & VC-to-VLAN Fast Provision – 802.1P Dialog	135
Figure 8-116 xDSL Port & VC-to-VLAN Fast Provision – Service Type Dialog	136
Figure 8-117 xDSL Fast Provision List Dialog.....	140

Figure 8-118 xDSL Multicast Channel Fast Provision – Multicast Service Profile Dialog.....	143
Figure 8-119 xDSL Multicast Channel Fast Provision – Channel Limit Dialog	143
Figure 8-120 xDSL Multicast Channel Fast Provision List Dialog.....	144
Figure 9-121 xDSL Current PM Port Selection.....	146
Figure 9-122 ADSL Current PM Dialog.....	147
Figure 9-123 SHDSL Current PM Dialog.....	148
Figure 9-124 xDSL History Port Selection Dialog.....	150
Figure 9-125 ADSL History PM Dialog.....	150
Figure 9-126 SHDSL History PM Dialog.....	152
Figure 9-127 Trunk PM Statistics Dialog.....	153
Figure 10-128 Active Alarm & Event List Dialog.....	154
Figure 10-129 Detailed Alarm & Event Dialog.....	156
Figure 10-130 Completed Alarm Sync Dialog.....	157
Figure 10-131 Alarm Input List Dialog.....	157
Figure 10-132 Alarm Input Modification Dialog.....	158
Figure 10-133 Alarm Output List Dialog.....	159
Figure 10-134 Alarm Output Modification Dialog.....	159
Figure 10-135 Hardware Monitoring List Dialog.....	161
Figure 10-136 Hardware Monitoring Threshold Setting Dialog.....	162
Figure 11-137 xDSL Port Selection Dialog.....	164
Figure 11-138 ADSL Port Rate Status Dialog.....	165
Figure 11-139 ADSL Bit Allocation Status Dialog.....	167
Figure 11-140 Graph of Bit Allocation.....	168
Figure 11-141 ADSL Loop Monitoring Dialog.....	169
Figure 11-142 Graph of Loop Monitoring – Magnitude.....	170
Figure 11-143 Graph of Loop Monitoring – Quiet Line Noise PSD....	170
Figure 11-144 ADSL Loop Diagnosis Dialog.....	171
Figure 11-145 Graph of DELT result – Magnitude.....	173
Figure 11-146 Graph of DELT result – Quiet Line PSD.....	173
Figure 11-147 Graph of DELT result – SNR.....	174
Figure 11-148 ADSL Loop SELT Test.....	174

Figure 11-149 TM Loopback OAM Cell Testing.....	176
Figure 11-150 Bridge Filtering Database Entry List Dialog.....	182
Figure 11-151 VLAN Membership List Dialog.....	184
Figure 11-152 MAC Spoofing Status List Dialog.....	185
Figure 11-153 Multicast Channel Status List Dialog.....	187
Figure 11-154 Multicast Group Membership List Dialog	188
Figure 11-155 xDSL Forwarding Broadcast VLANs List.....	189
Figure 11-156 DHCP Session Information List Dialog.....	190
Figure 11-157 PPPOE Session Information List Dialog.....	191
Figure 11-158 Current Status of Link Aggregation Dialog.....	192
Figure 11-159 Current Status of Rapid Spanning Tree Protocol – Bridge Dialog.....	194
Figure 11-160 Current Status of Rapid Spanning Tree Protocol –Port GE1/Port GE2 Dialog.....	195
Figure 11-161 UGE VLAN Status Dialog.....	197
Figure 11-162 Current Status of SFP Information Dialog.....	197
Figure 11-163 Ping NE from Client Dialog.....	200
Figure 11-164 Tracer Route NE from Client Dialog.....	201
Figure 11-165 Telnet Pop-up Window.....	203
Figure 11-166 Telnet Time-out Setting Dialog.....	203
Figure 11-167 CLI Prompt Setting Dialog.....	204
Figure 11-168 Check NE SNMP Connection Dialog.....	204
Figure 12-169 Client Options Dialog – Alarm Warning.....	206
Figure 13-170 Inventory Information List.....	208
Figure 13-171 NE Configuration Backup & Restore File List Dialog .	210
Figure 13-172 NE Firmware Upgrade Dialog.....	211
Figure 13-173 NE SHDSL Firmware Upgrade Dialog.....	212
Figure 13-174 NE Firmware Boot Partition Dialog.....	213
Figure 13-175 NE File System List Dialog.....	214
Figure 13-176 Reset the Unit Dialog.....	215

List of Tables

This page is leave in blank for note or memo use

Chapter 1 Preface

This preface describes the “*AMS LCT 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 AMS (Advanced Management System) LCT (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 D-Link DAS4 Series IP-DSLAM to the network as quickly as possible.

Organization

This guide contains the following chapters:

- Preface
- DAS4 Series Management System Overview
- Getting Started AMS LCT
- Initiating the NE
- Interface Profile Management
- Interface Port Management
- Connection Port Management
- Fast Provision Management
- Performance Management
- Fault Management
- Diagnosis Management
- General System Management
- Administrating and Maintenance
- Quick Configuration Guide for LCT

Conventions

This section describes the conventions used in this guide.

NE/NEs mentioned in this document means DAS4 Series 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.

Revision History

- 1) Revision Date: 2007/5/18
Release version: 1.1.3
Author: Julia Shen
Summary of Change(s):
 - (1) “Figure 3-1 AMS LCT Login Dialog” is changed due to typo-error.
 - (2) “Figure 3-7 Export Dialog” and its corresponding Table 3-2 are changed due to typo-error.
 - (3) “Figure 4-20 NE System Time” and its corresponding Table 4-15 are changed to add parameter “*unit:hour*” in Time Zone
 - (4) “Figure 4-22 NE Time Server Status Dialog” and its corresponding Table 4-17 are changed due to typo-error.
 - (5) “Figure 5-38 Add Traffic Policing Profile Dialog” and its corresponding Table 5-28 are changed to remove the parameter “*PIR*”.
 - (6) “Figure 8-110 xDSL Port & VC-to-VLAN Fast Provision – Port Setting Dialog” and its corresponding Table 8-78 are changed to remove the parameter “*wireless function*”.
 - (7) “Figure 6-61 Link Aggregation Setting Dialog” and its corresponding Table 6-43 are changed due to typo-error.
 - (8) “Figure 6-63 Trunk RSTP Setting– Bridge Dialog” and its corresponding Table 6-44 are changed due to typo-error.
 - (9) “Table 7-68 xDSL Multicast Channel Setting Description” is changed to improve the readability.
 - (10) “Table 8-80 xDSL Multicast Channel Fast Provision Description” is changed to improve the readability.
 - (11) “Table 8-81 xDSL Multicast Channel Fast Provision List Dialog Description” is changed to improve the readability.
 - (12) “Table 10-89 Alarm Input List Dialog Description” and its corresponding are changed due to typo-error.
 - (13) “Table 10-93 Hardware Monitoring List Dialog Description” and its corresponding are changed due to typo-error.
 - (14) “Figure 11-152 MAC Spoofing Status List Dialog” and its corresponding are changed due to typo-error.
 - (15) “Figure 11-154 Multicast Group Membership List Dialog” and its corresponding are changed due to typo-error.
 - (16) The titles of Figure 11-158 and Table 11-117 are changed to improve the readability.
 - (17) “Figure 11-159 Current Status of Rapid Spanning Tree Protocol – Bridge Dialog” and its corresponding Table 11-118 are changed due to typo-error.
 - (18) “Figure 13-173 NE SHDSL Firmware Upgrade Dialog” and its corresponding are changed due to typo-error.

- 2) Revision Date: 2007/5/28
Release version: 1.1.3
Author: Julia Shen
Summary of Change(s):
 - (1) “Figure 6-54 ADSL Port Modification Dialog” and Table 6-39 are changed to improve the readability.
 - (2) “Figure 6-55 SHDSL Port Modification Dialog” and Table 6-40 are changed to improve the readability.
 - (3) “Figure 10-132 Alarm Input Modification Dialog” and Table 10-90 are changed to improve the readability.

- 3) Revision Date: 2007/7/16
Release version: 1.1.4
Author: William Fu
Summary of Change(s):
 - (1) Replace Appendix C “index” with “Quick Configuration Guide for LCT”

- 4) Revision Date: 2007/10/01
Release version: 1.1.5
Author: William Fu
Summary of Change(s):
 - (1) Add descriptions of 802.1Q tagged mode in Section “Constructing the NE Objects” and modify/add the following tables.
 - Table 4-4 Board Setting List Description
 - Table 4-5 Board Setting Dialog Description
 - Table 4-6 The NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.
 - (2) Add sub-section “Manual VLAN Setting” to describe the manual VLAN setting for when the 2nd GE port is enabled to work as a subtended port in Section “GE Network Interface Management”

- 5) Revision Date: 2007/10/12
Release version: 1.1.6
Author: Julia Shen
Summary of Change(s):
 - (1) “Figure 4-16 NE User Account List Dialog” is changed to improve the readability.
 - (2) “Figure 5-34 ADSL Line Profile– INP Dialog” is changed due to typo-error.
 - (3) “Figure 7-102 MAC Aging Setting Dialog” and its corresponding Table 7-70 are changed to remove the parameter “*Admin Srtatus*”. And move “MAC Aging” menu item from “xDSL” to “NE Management”.
 - (4) “Figure 7-103 VLAN MAC Limit List Dialog” is changed to add the option that shows LC’s information and its corresponding Table 7-71 is changed to add the parameter “*Rsfresh*”.
 - (5) “Table 5-36” is changed to improve the readability.
 - (6) Change the name of “ISP server” to “Next-hop” and change the following table and figures.
 - Figure 7-76 xDSL VC-to-VLAN Setting – IP Traffic Dialog-(b).
 - Figure 7-78 xDSL VC-to-VLAN Setting – 802.1P Dialog (only for the RFC2684 routed mode).
 - Figure 7-81 xDSL VC-to-VLAN Setting – Next-hop Dialog (only for the RFC2684 routed mode).
 - Figure 7-82 xDSL VC-to-VLAN Setting – Service Type Dialog-(d).
 - Table 7-53 xDSL VC-to-VLAN Setting Description.
 - Figure 8-111 xDSL Port & VC-to-VLAN Fast Provision – Channel Setting Dialog-(b)
 - Figure 8-114 xDSL Port & VC-to-VLAN Fast Provision – Next-hop Dialog (only for the RFC2684 routed mode)
 - Figure 8-116 xDSL Port & VC-to-VLAN Fast Provision – Service Type Dialog-(d)
 - Table 8-78 xDSL Port & VC-to-VLAN Fast Provision Description
 - Figure 8-117 xDSL Fast Provision List Dialog
 - Table 8-79 xDSL Fast Provision List Dialog Description
 - (7) “Figure 8-116-(a), (b), (c)” are changed to improve the readability.

- (8) Change the name of “Mac Limit” to “Channel Limit” and change the following table and figures.
- Figure 7-100 xDSL Multicast Channel Setting Dialog
 - Table 7-68 xDSL Multicast Channel Setting Description
 - Figure 8-118 xDSL Multicast Channel Fast Provision – Multicast Service Profile Dialog
 - Figure 8-119 xDSL Multicast Channel Fast Provision – Channel Limit Dialog
 - Table 8-80 xDSL Multicast Channel Fast Provision Description
- (9) Change the name of “Stream Count” to “Channel Limit” and change the following table and figures.
- Figure 7-100 xDSL Multicast Channel Setting Dialog
 - Table 7-68 xDSL Multicast Channel Setting Description
 - Figure 8-119 xDSL Multicast Channel Fast Provision – Channel Limit Dialog
 - Table 8-80 xDSL Multicast Channel Fast Provision Description
 - Figure 8-120 xDSL Multicast Channel Fast Provision List Dialog
 - Table 8-81 xDSL Multicast Channel Fast Provision List Dialog Description
- 6) Revision Date: 2007/11/13
 Release version: 1.1.7
 Author: Julia Shen
 Summary of Change(s):
- (1) Add a note in Section “User Account Management” of 4.
 - (2) Add some descriptions in Section “Secured Host Management” of 4.
 - (3) Add a note in Section “NE Date and Time Management” of 4.
 - (4) Add some descriptions in Section “DNS Server Setting” of 4.
 - (5) Add some descriptions in Section “Time Server Setting” of 4.
 - (6) Add some descriptions in Section “Managing the NE Configuration” of 4.
 - (7) Add some descriptions and note in Section “Interface Profile Management” of 5.
 - (8) Add some descriptions and notes in Section “ADSL Profile” of 5.
 - (9) Add some descriptions in Section “PM Threshold Profile” of 5.
 - (10) Add some descriptions in Section “IP Traffic Profile” of 5.
 - (11) Add some descriptions in Section “Configuring the VLAN Profile” of 5.
 - (12) Add some descriptions in Section “GE Network Interface Management” of 6.
 - (13) Add some descriptions and notes in Section “Link Aggregation (Static / Dynamic)” of 6.
 - (14) Add some descriptions in Section “RSTP Configuration” of 6.
 - (15) Add some descriptions and notes in Section “CoS Configuration” of 6.
 - (16) Add some descriptions and notes in Section “VC-to-VLAN Connection Management” of 7.
 - (17) Modify the Note below “Table 7-53 xDSL VC-to-VLAN Setting Description” and “Table 8-78 xDSL Port & VC-to-VLAN Fast Provision Description” to describe clearly the IP/MAC anti spoofing function supported in either one of the following cases.
 - “PPPoE” Service Type is enabled
 - “DHCP” Service Type is enabled
 - “Static IP” Service Type is enabled
 - (18) Add some descriptions and notes in Section “Telnet” of 11.
 - (19) Add a note in section “NE Configuration Backup and Restore” of 13.
 - (20) Add some descriptions in Section “NE Boot Partition” of 13.
- 7) Revision Date: 2007/12/13
 Release version: 1.1.8
 Author: Julia Shen

Summary of Change(s):

- (1) “Figure 3-2 AMS LCT Operation Window” is changed due to typo-error.
 - (2) “Table 3-1” is changed to add icon and LED sign description.
- 8) Revision Date: 2008/01/25
Release version: 1.1.9
Author: Tim Yeh
Summary of Change(s):
- (1) Change the operation path on **Main Menu** in Section “User Account Management” of 4.
 - (2) Change the name of Section “Saving the NE Configuration” to “Managing the NE Configuration” in 4. And add a sub-section “Erasing NE configuration from Flash” to describe the procedure to erase NE configuration from Flash.
 - (3) Add some descriptions and note in Section “Source MAC Access Control List” of 7.
 - (4) Add some descriptions in Section “Multicast Service Management” of 7.
 - (5) Add “Non-aged” mode for the RFC2684 bridged mode and routing mode in the following figures.
 - Figure 7-79 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 bridged mode
 - Figure 7-80 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 routed mode
 - Figure 8-113 xDSL Port & VC-to-VLAN Fast Provision – MAC Control Dialog
 - (6) Add a sub-section “Static MAC configuration on xDSL Port” to depict how to manually add a configured MAC entry in FDB.
 - (7) Modify “Figure 7-99 xDSL Multicast Channel List Dialog” to add a new function of “Multi-Delete”.
 - (8) Rewrite Sub-section “IGMP snooping/IGMP proxy Configuration” to describe the new functions of “Query Version”, “Report/Leave Version” and “Immediate Leave”.
 - (9) Add a new section “Cascaded NE Management” of 7 to depict how to set up the cascaded environment with NEs and its management.
 - (10) Add some descriptions in Section “VLAN MAC Limit” of 7.
 - (11) Add some descriptions in Section “Interface and VC-VLAN Fast Provisioning” of 8.
 - (12) Rename Section “Relay Input Management” to Section “Relay Input Alarm Management” of 10.
 - (13) Add a new section “Relay-Output Alarm Management” of 10 to describe the system relay-out alarm configuration of NE.
 - (14) Add some descriptions and notes in Section “Telnet” of 11.
 - (15) Add some descriptions and update the following figure and table in Section “xDSL MAC Spoofing Status” of 11.
 - Figure 11-152 MAC Spoofing Status List Dialog
 - Table 11-111 MAC Spoofing Status List Dialog Description
 - (16) Add a new section “ATM OAM F5 VC Diagnosis” to 11 to depict the ATM Operation, Administration, and Maintenance (OAM) F5 diagnosis at data connection layer.
 - (17) Rewrite Section “Bridge Filtering Database” of 11 to describe the filtering function of upstream traffic of spoofed MAC.
 - (18) Add a sub-section “DHCP Session Information” of 11 to display the information list of DHCP transaction information on the xDSL ports.
 - (19) Add a sub-section “PPPOE Session Information” of 11 to display the information list of PPPOE session on the xDSL ports.
 - (20) Add a sub-section “SFP Information List” of 11 to display the the current SFP information.
 - (21) Add a sub-section “Telnet Timeout” of 11 to set the telnet time out of the system.
 - (22) Add a sub-section “NE File System List” of 13 to show the new file system list of NE

- (23) Add Table 13-125 to depict the parameters in “Figure 13-170 Inventory Information List”.
- 9) Revision Date: 2008/03/12
 Release version: 1.1.10
 Author: Tim Yeh
 Summary of Change(s):
- (1) Update Appendix C “Quick Configuration Guide for LCT” with following figures
 - Figure 7-79 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 bridged mode
 - Figure 7-101 IGMP Snooping / IGMP Proxy Setting Dialog
- 10) Revision Date: 2008/03/27
 Release version: 1.1.11
 Author: Tim Yeh
 Summary of Change(s):
- (1) Add a note in Section “NE Firmware Upgrade” of 13.
- 11) Revision Date: 2008/07/21
 Release version: 1.2.1
 Author: Tim Yeh
 Summary of Change(s):
- (1) Add a new function “Line Standard” to ADSL profile and depict how to manually select xDSL line standards.
 - (2) Add a note in Section “Configuring the VLAN Profile” of 5.
 - (3) Modify “Figure 6-54 ADSL Port Modification Dialog” to add a new function of “Packet filter Groups”.
 - (4) Modify the following figures to set the “MAC Control” up to 64.
 - Figure 7-79 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 bridged mode
 - Figure 7-80 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 routed mode
 - (5) Modify “Figure 7-82 xDSL VC-to-VLAN Setting – Service Type Dialog” to add a new function of additional service type control.
 - (6) Add some notes in Section “VC-to-VLAN Connection Management” of 7.
 - (7) Add a sub-section “Packet filter” of 7 to depict how to set the packet filter on the specific ADSL line card.
 - (8) Modify the following figures in the section “Interface and VC-VLAN Fast Provisioning” for the new adding functionalities.
 - Figure 8-110 xDSL Port & VC-to-VLAN Fast Provision – Port Setting Dialog
 - Figure 8-113 xDSL Port & VC-to-VLAN Fast Provision – MAC Control Dialog
 - Figure 8-116 xDSL Port & VC-to-VLAN Fast Provision – Service Type Dialog
 - (9) Modify the section “Bridge Filtering Database” of 11 to describe the filtering function of upstream traffic of spoofed MAC learned from the GE1(uplink GE port) or GE2 port(uplink/subtending GE port).
 - (10) Modify “Figure 11-152 MAC Spoofing Status List Dialog” to list the spoofing status between the GE1(uplink GE port) or GE2 port(uplink/subtending GE port).
- 12) Revision Date: 2008/08/07
 Release version: 1.3.0

Author: Paine Peng

Summary of Change(s):

- (1) Add xDSL VC-to-VLAN list dialog.

13) Revision Date: 2008/12/30

Release version: 1.4.0

Author: Paine Peng

Summary of Change(s):

- (1) refer to LCT v4.7.3.4 (2008/12/26)

This page is leave in blank for note or memo use

Chapter 2 DAS4 Series Management System Overview

This chapter describes the AMS LCT user interface. This chapter contains the following sections:

- AMS LCT Overview
- AMS LCT Features
- System Hardware and Software Requirement

AMS LCT Overview

AMS LCT 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 AMS LCT is designed on the PC platform and is compatible to Microsoft Windows 98SE/ME/2000/XP
- Easy to operate. The AMS LCT provides user-friendly configuration interface
- Various alarm severity levels are provided for all possible events/conditions

AMS LCT Features

The AMS LCT 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 DAS4 Series IP-DSLAM.

Real-time System Status Monitoring

The AMS LCT 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 AMS LCT.

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.

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

System Hardware and Software Requirement

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

The recommend hardware & OS for AMS LCT:

- 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 AMS LCT System:

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

Chapter 3 Getting Started AMS LCT

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

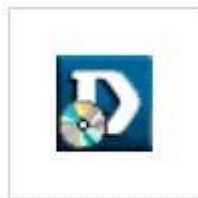
This chapter contains the following sections:

- Installing the AMS LCT
- Starting a AMS LCT Session
- Navigating of AMS LCT
- Managing the Trap Log View
- Icons and LED Sign Overview
- Error Handling Dialog
- Data Exporting and Graphic Displaying

Installing the AMS LCT

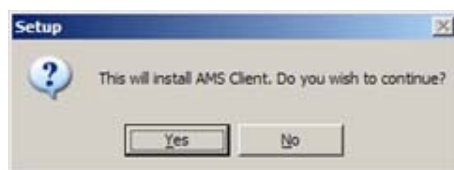
Before installing the AMS LCT software, please make sure both of your requirement of hardware and software are completed with recommend specification list in “Chapter 2 System Hardware and Software Requirement”.

- Step 1** Insert the ‘AMS Installation Package’ CD to your CD/DVD driver, from the directory of ‘AMS_LCT’ double click on the ‘AMS_GUI_LCT_setupVx.x.x.x’ executable file.

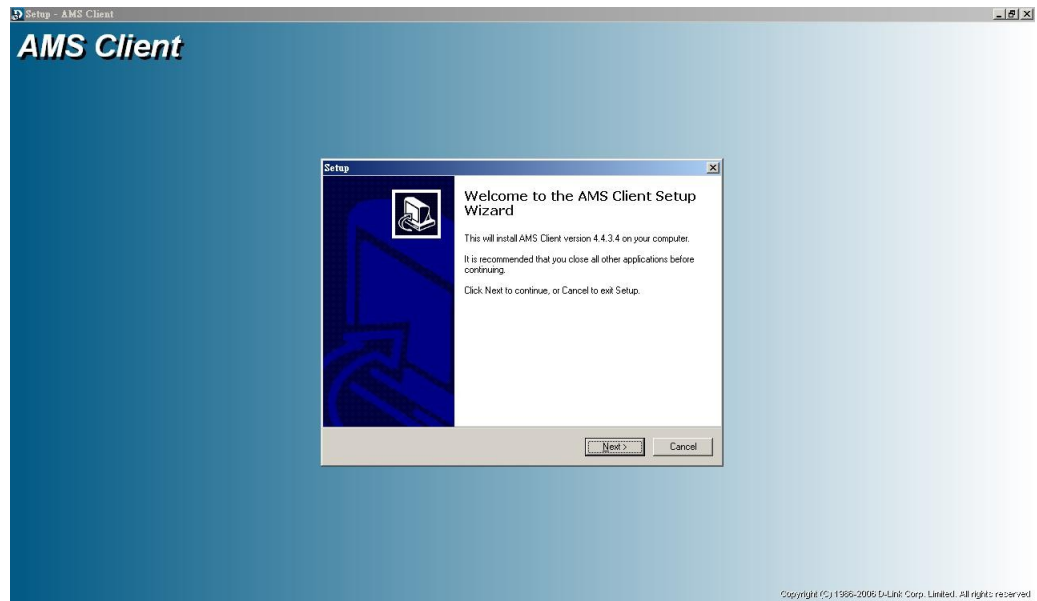


AMS_GUI_LCT_setup

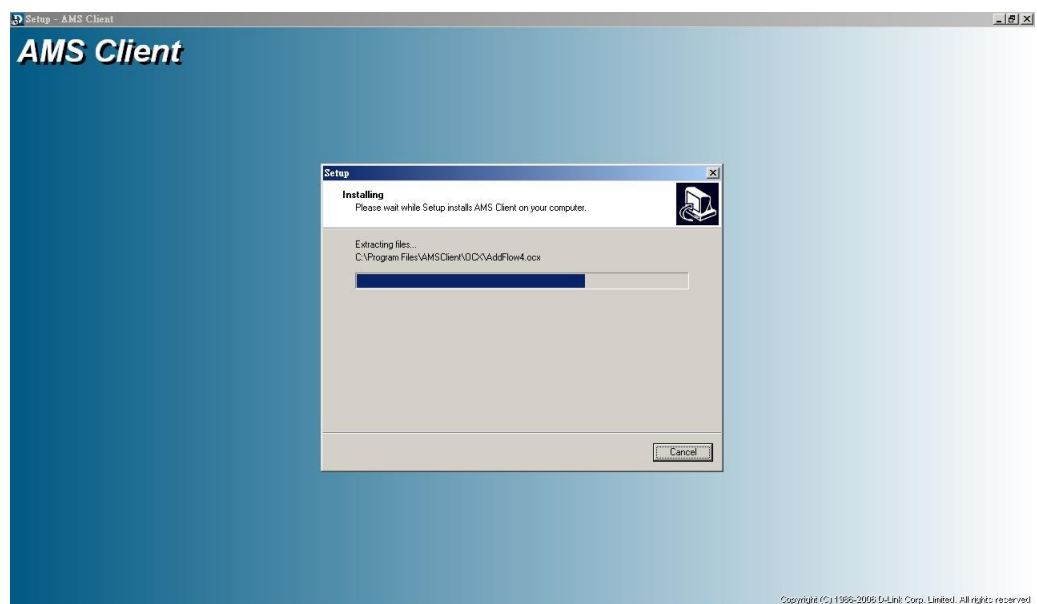
- Step 2** Select ‘Yes’ from the launched window to continuous the installation.



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 'AMS Client' icon on your desktop; double click this icon to run the AMS Client software.

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



Starting a AMS LCT Session

Double click the 'AMS Client' icon on your desktop to launch the AMS LCT 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 AMS LCT.

To start an AMS LCT session, follow these steps.

- Step 1** Open AMS LCT session by double clicking the ‘AMS Client’ icon on the MS-Windows.
The Login window appears.

Figure 3-1 AMS LCT 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 AMS LCT 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 DAS4 Series 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 AMS LCT

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

Keyboard Commands

Certain Keyboard commands are available in AMS LCT. 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

AMS LCT 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.

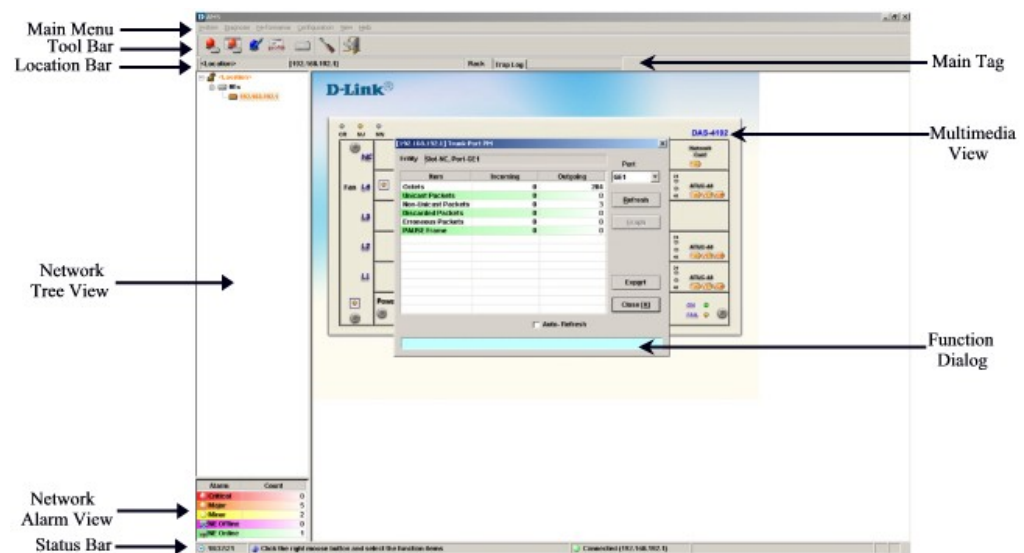


The “NE object” denotes the NE entity, Shelf, Slot/Box, and Port displaying on the Rack tab of Multimedia View area or Network Tree View area.

AMS LCT Window Overview

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

Figure 3-2 AMS LCT Operation Window



Managing the Trap Log View

Click the ‘Trap Log’ tab view to display the system trap (alarm) information.

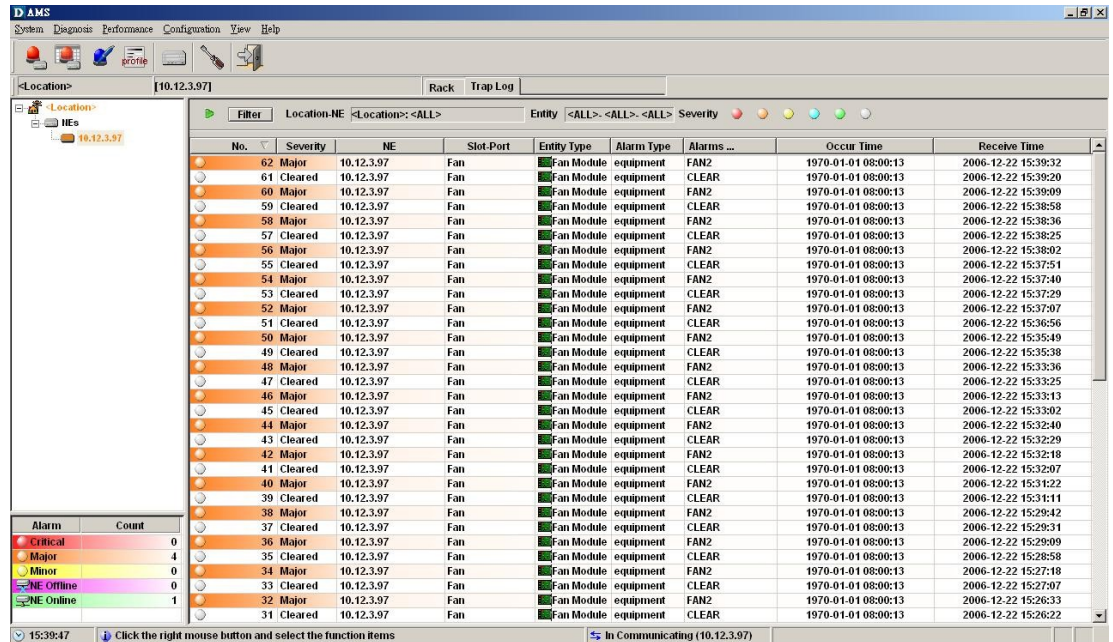
The NE would send SNMP traps to a designated host IP address when there is one or more status

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.

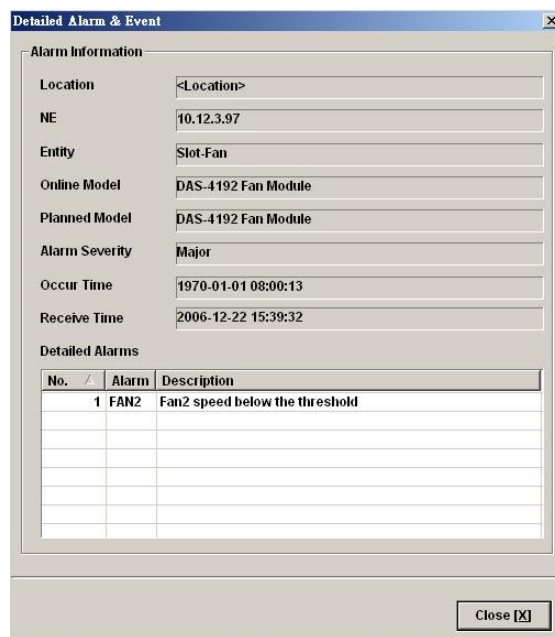
Chapter 4 “Configuring the SNMP Trap Manager” shows you how to configure the SNMP trap station.

Figure 3-3 AMS LCT 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

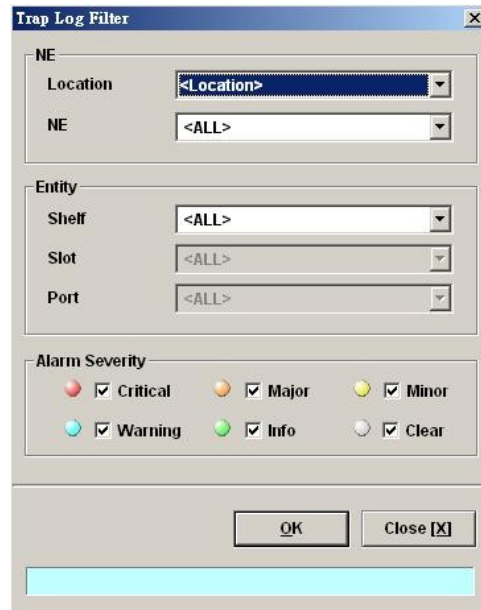


You can also select the ‘Pause’ or ‘Reset’ from launched **Function Menu** to stop refreshing traps or clearing all traps cached in the AMS LCT.

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 AMS LCT.

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.
	AMS LCT Options.
	Exit AMS LCT.

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 (DAS4672 only)
	NC card in standby mode (DAS4672 only)
	NC / LC card type is mismatch
	NC / LC card dose 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)

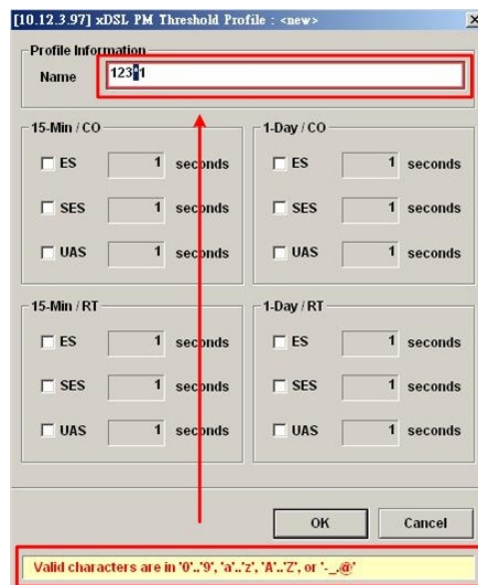
Symbol	Description
Function Dialog	
	Indicates data in list table is active and valid.
	Indicates data in list table is inactive or invalid.
	Indicates the status of specific port in list table is link up.
	Indicates the status of specific port in list table is link down.
	Indicates the status of task 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

AMS LCT 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

AMS LCT provides the data exporting of dialog List Table information.

Figure 3-7 Export Dialog

Field	Value
Title	Active Alarm_Event
NE	10.12.3.107
Entity	<NE>
User	admin
Export data file	C:\AMSLCT Client\CurAlm.txt
Header file	C:\AMSLCT Client\CurAlm.ini
Record count	8

Data file: C:\AMSLCT Client\CurAlm.txt

Add the title and field names at the beginning of file

Append data to the end of file

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

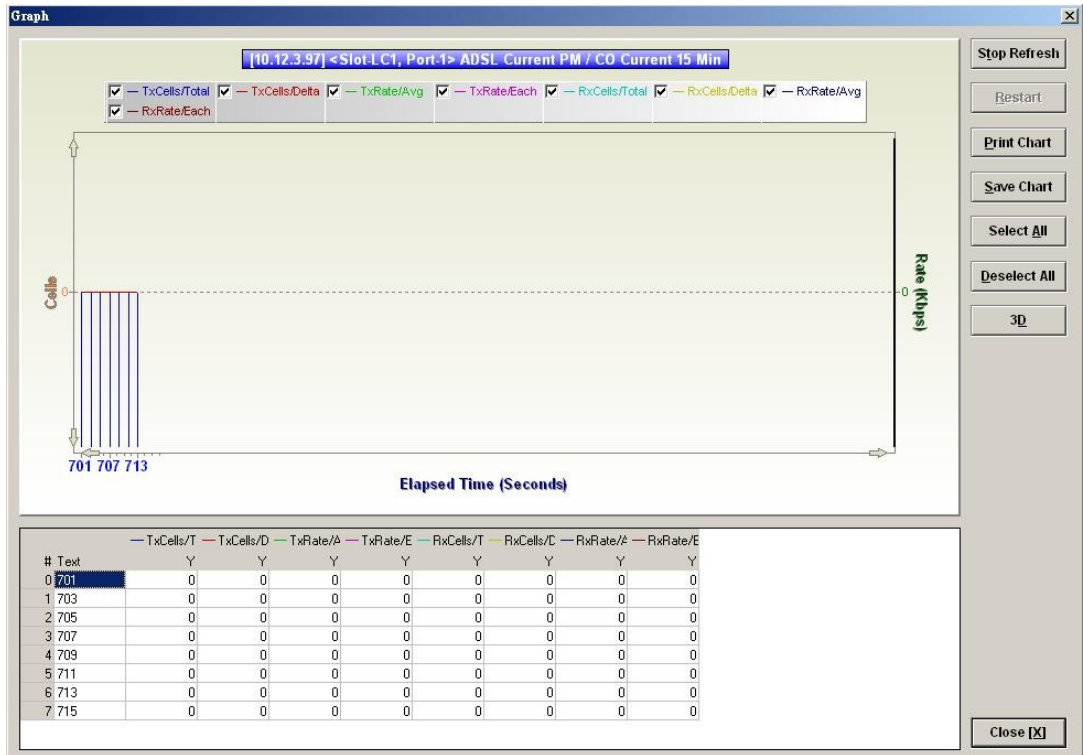


Table 3-3 2D/3D Data Graph Displaying Dialog Description

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 DAS4 Series 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 DAS4 Series 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 DAS4 Series 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 AMS LCT and the configured AMS 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 4-9 and Table 4-4 depicts the related parameters.

Figure 4-9 Board Setting List Dialog

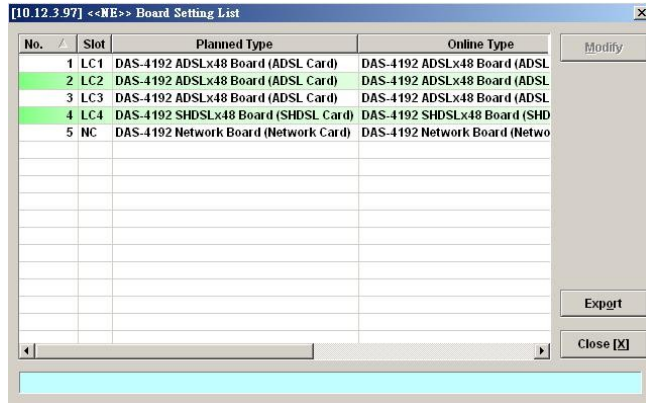


Table 4-4 Board Setting List Description

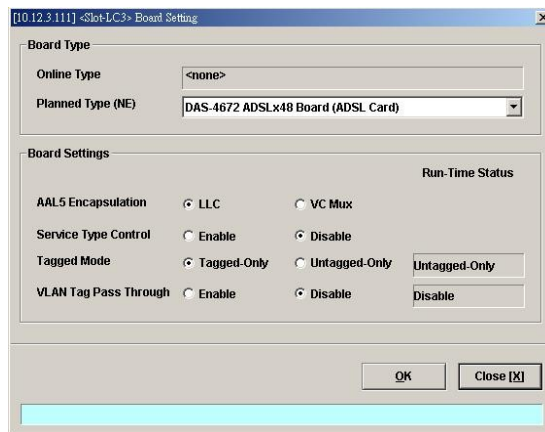
Field	Description
List Table	
No.	This indicates the serial number of entry of the List Table.
Slot	This indicates the location of board.
Planned Type	This indicates the board type planned to be equipped to the slot of DAS4 Series IP-DSLAM. If the planned type is mismatched (removed or type error) with 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 4-6 for the NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.

Table 4-4 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 4-6 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 4-10 and Figure 4-11 for LC and NC setting, respectively. Table 3-1 depicts the related parameters.

Figure 4-10 xDSL Board Setting Dialog



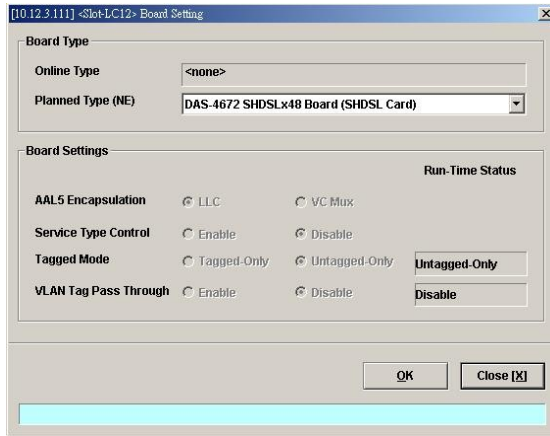


Figure 4-11 NC Boarding Setting Dialog

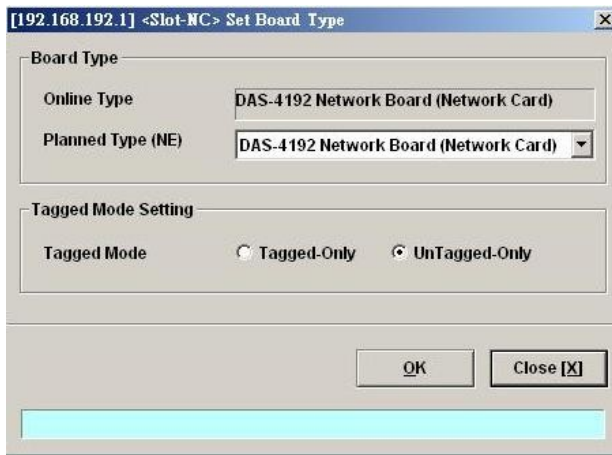


Table 4-5 Board Setting Dialog Description

Field	Description
Board Type	
Planned Type [Modify]	This specifies the board type planned to be equipped to the slot of DAS4 Series 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 4-6 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 4-6 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 4-6 whenever its run-time status changes.



The NC needs to be reset to perform the expected system behavior as depicted in Table 4-6 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 4-6

- 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 4-6 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			
					VLAN-tagging Status of Egress Traffic		Acceptable Ingress Traffic	
Tagged mode	Tagged mode	VTP	Tagged mode	VTP	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 7-77) 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 4-6 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 affect the communication between the AMS LCT and NE, re-login the AMS LCT if the SNMP community has been modified.

Configuring the SNMP Trap Manager

SNMP Trap Manager records the hosts (any SNMP server, like LCT, AMS 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 4-12 and Table 4-7 depicts the related parameters.

Figure 4-12 NE SNMP Manager IP Address List Dialog

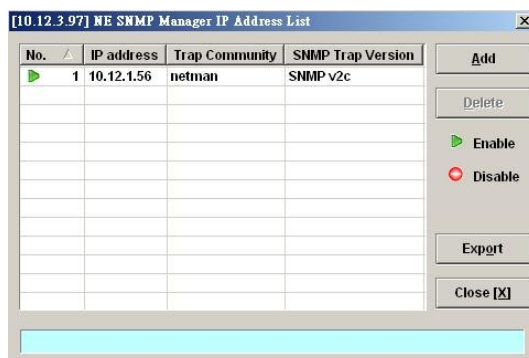


Table 4-7 NE SNMP Manager IP Address List Dialog Description

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 4-13 and Table 4-8 depicts the related parameters.

Figure 4-13 Add NE SNMP Manager IP Address Dialog

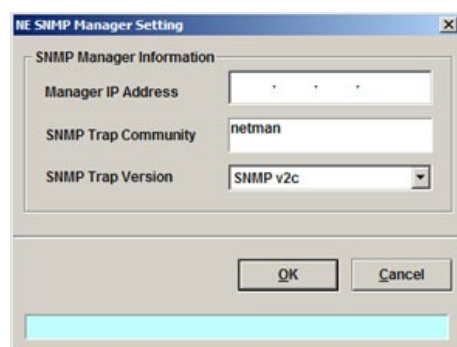


Table 4-8 Add NE SNMP Manager IP Address Dialog Description

Field	Description
Manager IP address	This specifies the IP address (Server / Host IP) of SNMP Manager. Valid values: Any valid class A/B/C address
SNMP 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 AMS LCT 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 4-14 and Table 4-9 depicts the related parameters.

Figure 4-14 NE SNMP Community List Dialog

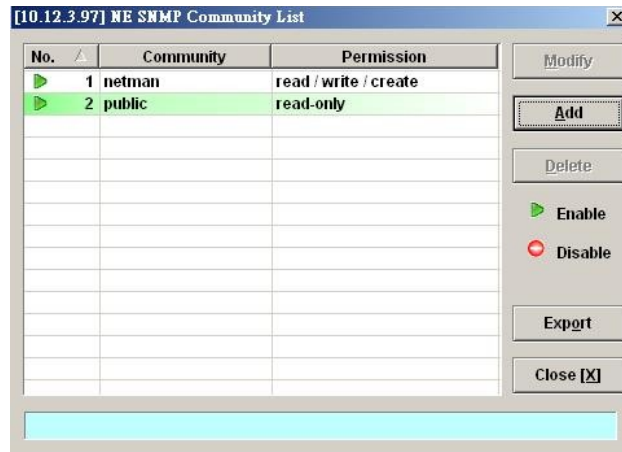


Table 4-9 NE SNMP Community List Dialog Description

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 4-15 and Table 4-10 depicts the related parameters.

Figure 4-15 Add NE SNMP Community Dialog

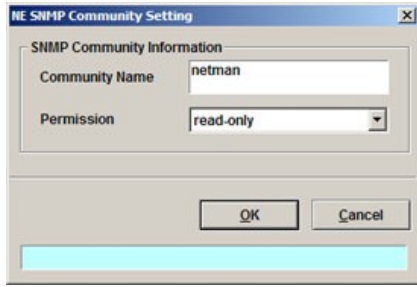


Table 4-10 Add NE SNMP Community Dialog Description

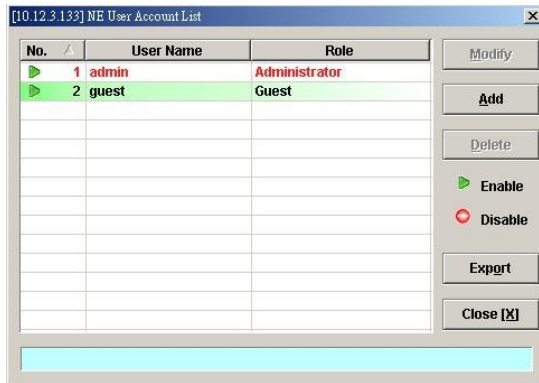
Field	Description
Community Name	This indicates the case-sensitive SNMP community name. Valid values: String of up to 20 characters and any combination of printable characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_', '@').
Permission	This indicates the permission level. Valid values: read-only, read/write/create

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 4-16 and Table 4-11 depicts the related parameters.

Figure 4-16 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 4-17 and Table 4-12 depicts the related parameters.

Table 4-11 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 4-17 NE User Account Setting Dialog

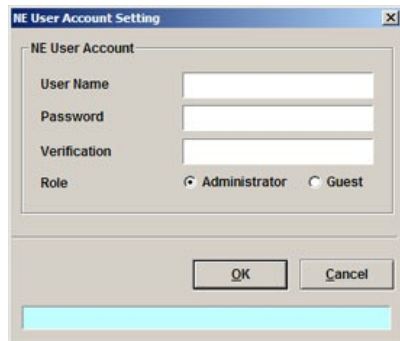


Table 4-12 NE User Account Setting Dialog Description

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 DAS4-Series 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 4-18 and Table 4-13 depicts the related parameters.

Figure 4-18 NE Secured Host List Dialog

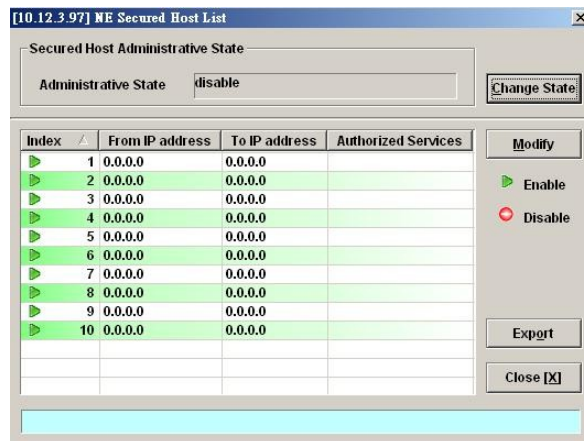


Table 4-13 NE Secured Host List Dialog Description

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 4-19 and Table 4-14 depicts the related parameters.

Figure 4-19 NE Secured Host Setting Dialog

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

Table 4-14 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 4-20 and Table 4-15 depicts the related parameters.

Figure 4-20 NE System Time Dialog

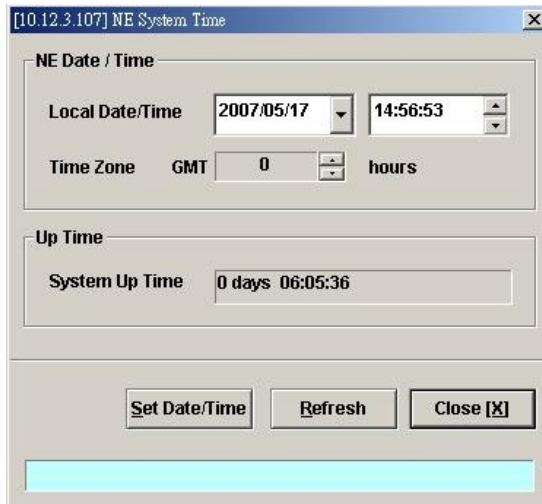


Table 4-15 NE System Time Dialog Description

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 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.cisco.com will receive a reply with the IP address of the web server of Cisco. 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 4-21 and Table 4-16 depicts the related parameters.

Figure 4-21 DNS Server Setting Dialog

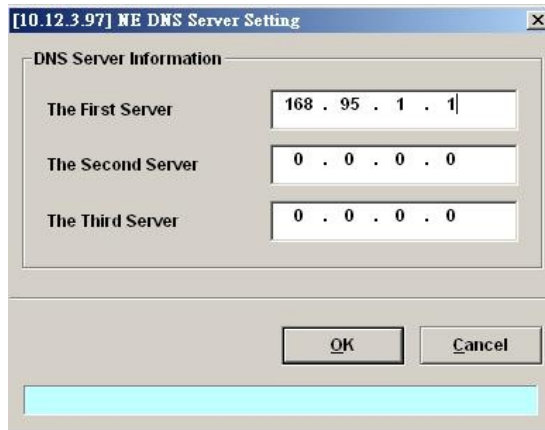


Table 4-16 DNS Server Setting Dialog Description

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 4-22 and Table 4-17 depicts the related parameters.

Figure 4-22 NE Time Server Status Dialog

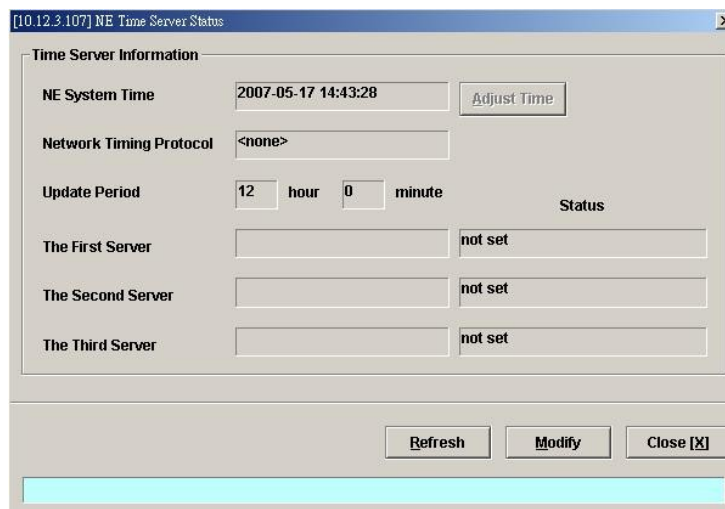


Table 4-17 NE Time Server Status Dialog Description

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 4-23 and Table 4-18 depicts the related parameters.

Figure 4-23 NE Time Server Setting Dialog

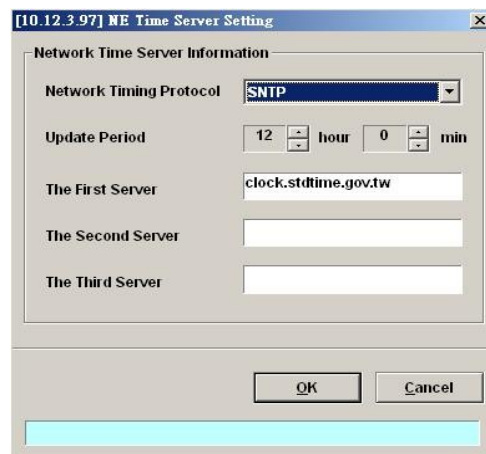


Table 4-18 NE Time Server Setting Dialog Description

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

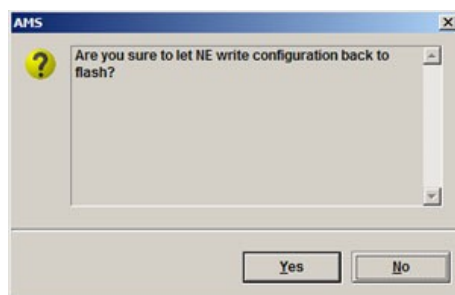
The modified configuration will be lost due to the rebooting of hardware without saving (storing).

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 4-24.

Figure 4-24 NE Write Flash Confirm Dialog

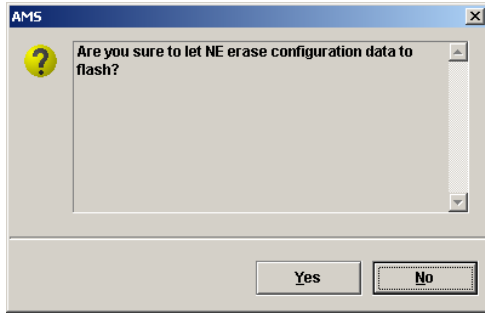


Erasing NE configuration from Flash

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 4-25.

Figure 4-25 NE Erase Flash Confirm Dialog



Chapter 5 Interface 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 5-26 and Table 5-19 help you to understand each profile and their interrelationship.

As shown in Figure 5-26, 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 5-26 Interrelationship of Data Transport Related Profiles

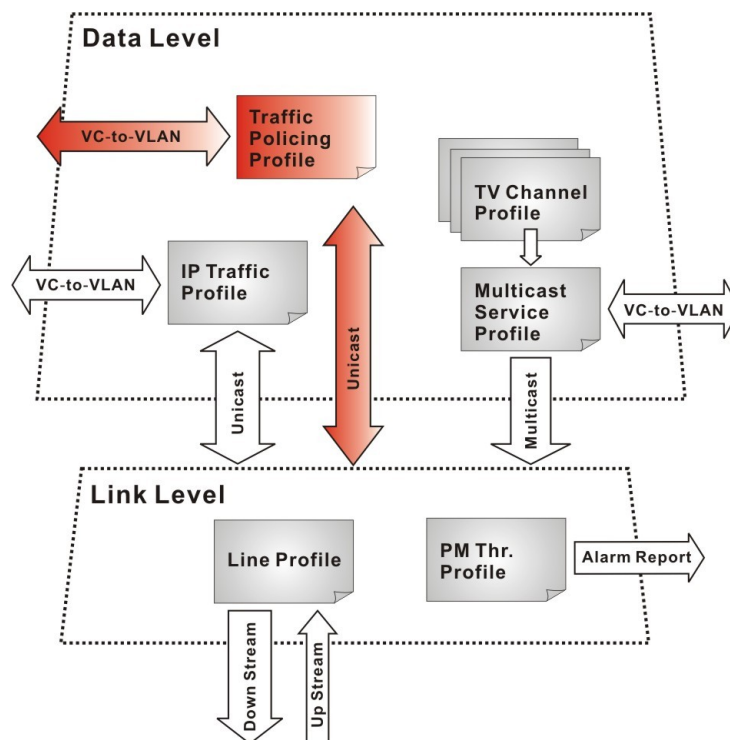


Table 5-19 Data Transport Related Profiles

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 5-28.



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 5-27 indicates the position of the **Function Button** by red rectangle.

Figure 5-27 xDSL Profile List Dialog Function Button

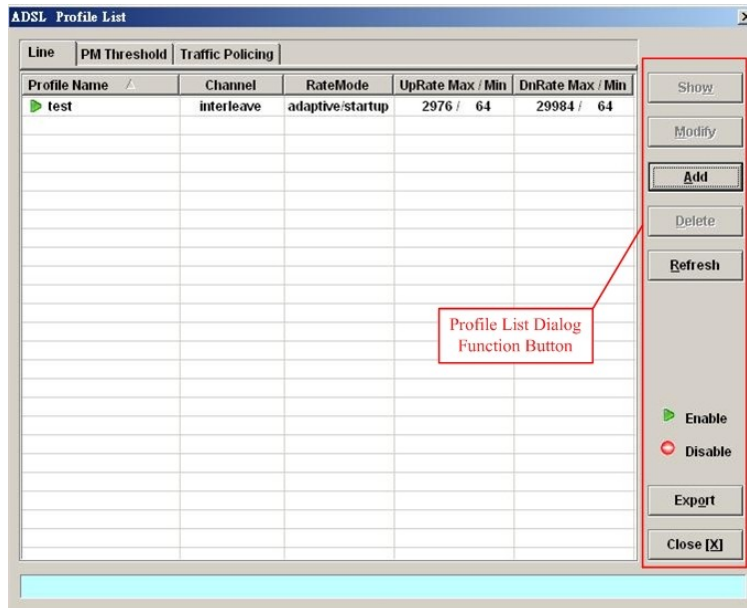


Table 5-20 xDSL Line Profile List Dialog Function Button

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.



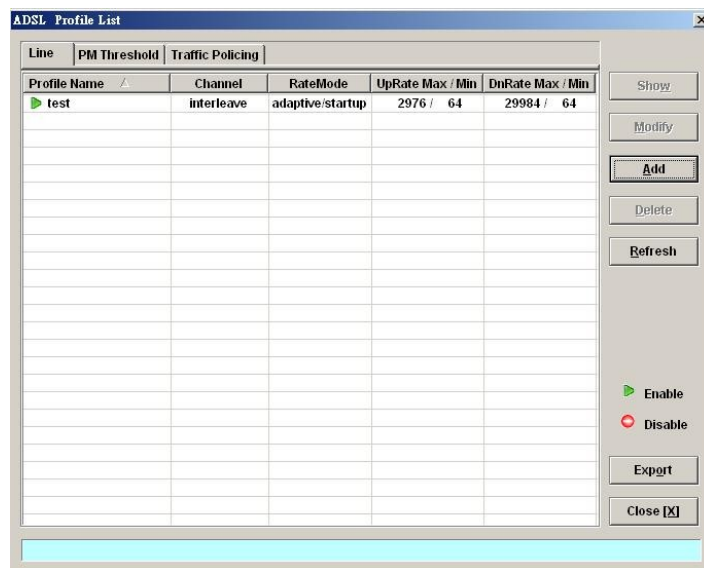
Once the ADSL connection profile is created, the operator can apply it to distinct ADSL line port by the “ADSL Port Modification Dialog” shown in Figure 6-54 for the related command.

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 5-28.

Figure 5-28 ADSL 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 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 5-29. Table 5-21 depicts the related parameters.

Figure 5-29 Add ADSL Line Profile– Transmission Rate Dialog

Table 5-21 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

Line Standard

Click the **Line Standard** tab in **ADSL Line Profile Dialog** to launch the **ADSL Line Profile–Line Standard Dialog** as shown in Figure 5-29. Table 5-21 depicts the related parameters.

Figure 5-30 Add ADSL Line Profile–Line Standard Dialog

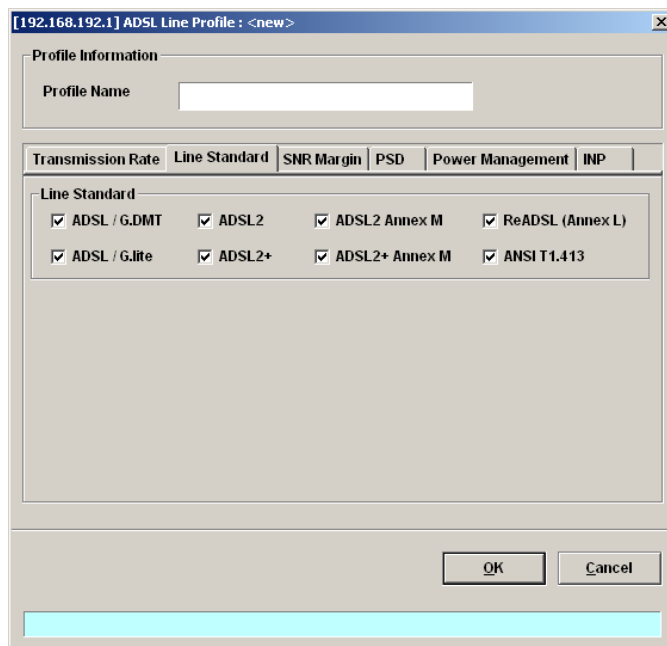


Table 5-22 Add Line Profile– Transmission Rate Dialog Description

Field	Description
Profile Information	
Profile Name	Enter to give a profile name
Line Standard	
ADSL/G.DMT	It specifies the ITU (International Telecommunication Union) G.992.1 standard for ADSL using discrete multitone modulation.
ADSL2	It specifies the ITU G.992.3 standard and optionally extends the capability of basic ADSL in data rates to 12 Mbit/s downstream and 3.5 Mbit/s upstream.
ADSL2+	It specifies the ITU G.992.5 standard and extends the capability of basic ADSL by doubling the number of downstream bits. The data rates can be as high as 24 Mbit/s downstream and 1 Mbit/s upstream depending on the distance from the DSLAM to the customer's home.
ADSL2 Annex M	It specifies the ITU G.992.3 Annex M standard and extends the capability of basic ADSL in data rates to 12 Mbit/s downstream and 3.5 Mbit/s upstream.
ADSL2+ Annex M	It specifies the ITU G.992.5 Annex M standard and extends the capability of basic ADSL2 by doubling the number of upstream bits. The data rates can be as high as 24 Mbit/s downstream and 3.5 Mbit/s upstream depending on the distance from the DSLAM to the customer's home.
ReADSL (Annex L)	It specifies an ADSL2 variant designed to boost the reach and data transfer rate of long-loop multicarrier systems.
ANSI T1.413	It specifies the American National Standards Institute (ANSI) T1.413 standard using discrete multitone modulation.

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 5-31. Table 5-23 depicts the related parameters.

Figure 5-31 Add ADSL Line Profile– SNR Margin Dialog

Table 5-23 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’.



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 5-32. Table 5-24 depicts the related parameters.

Figure 5-32 Add ADSL Line Profile– PSD Dialog

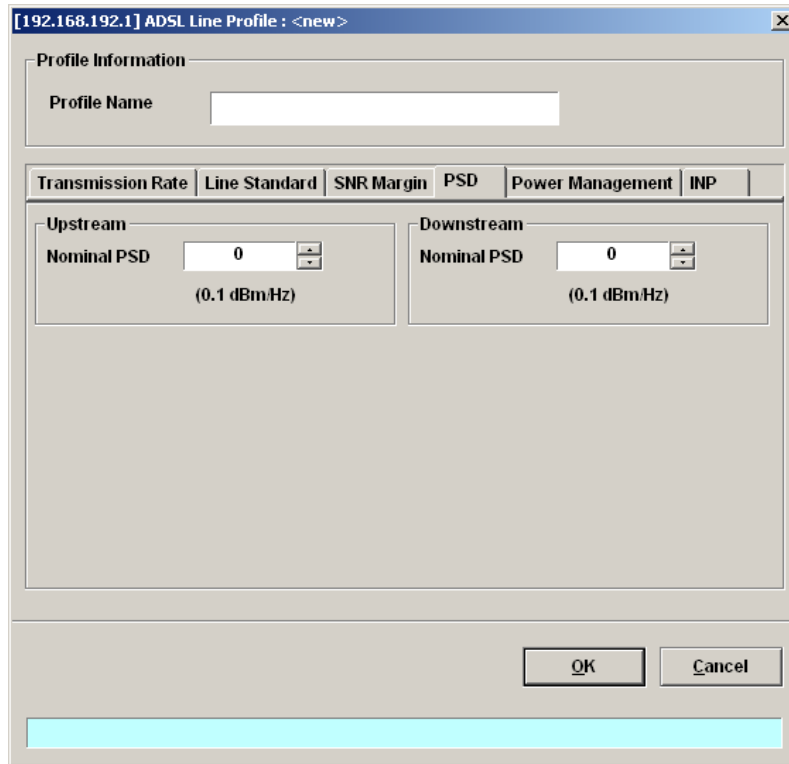


Table 5-24 Add Line Profile – PSD Dialog Description

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 to 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 5-33. Table 5-25 depicts the related parameters.

Figure 5-33 Add ADSL Line Profile– Power Management Dialog

Table 5-25 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 5-34. Table 5-26 depicts the related parameters.

Figure 5-34 Add ADSL Line Profile– INP Dialog

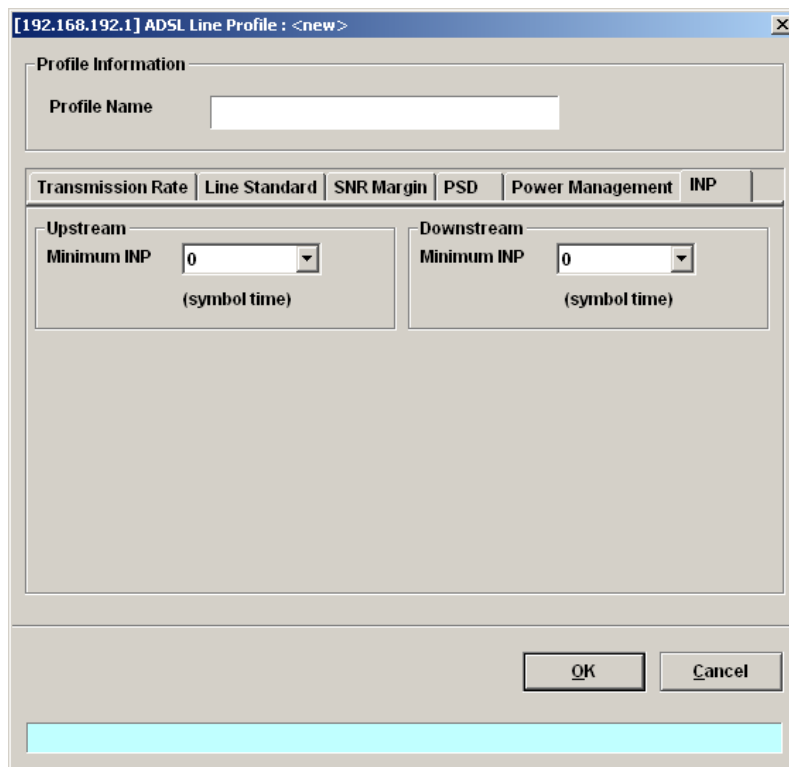


Table 5-26 Add Line Profile – INP Dialog Description

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 AMS LCT 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.

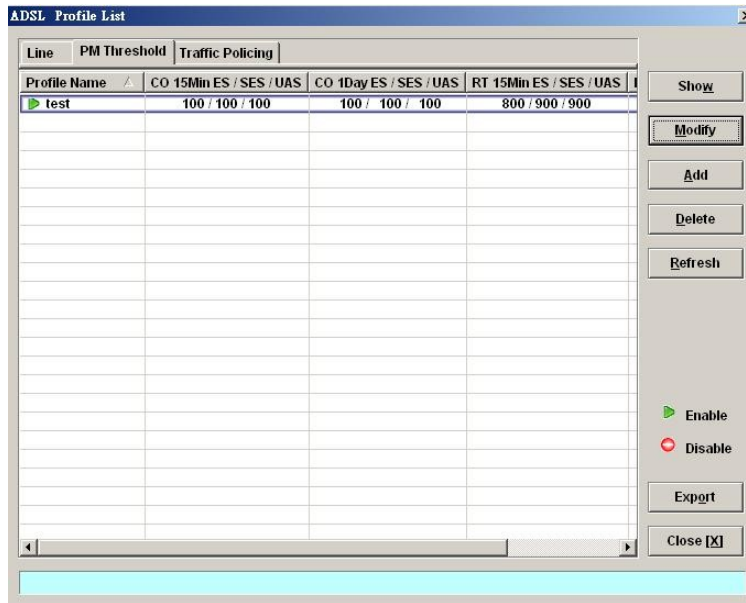
The NE supports to define the Near-End and Far-End thresholds of ES (Errored Seconds), SES (Severely Errored Seconds), and UAS (Unavailable Seconds) conditions in 15 minutes and 1 day interval. The definition of ES, SES and UAS are as follows.

- **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 5-35 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 5-35.

Figure 5-35 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 5-36 shows **Add ADSL PM Threshold Profile Dialog**. Table 5-27 depicts the related parameters.

Figure 5-36 Add ADSL PM Threshold Profile Dialog

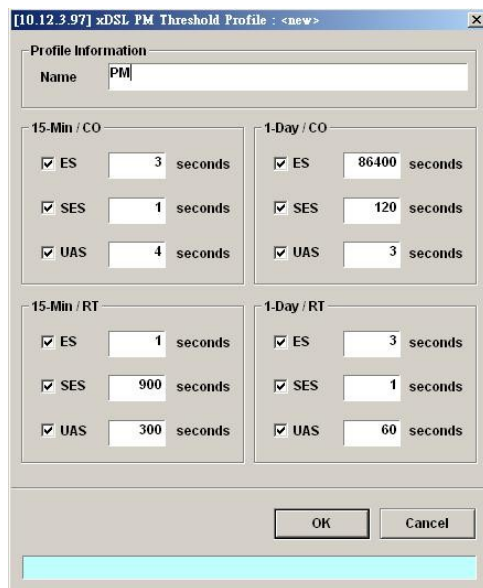


Table 5-27 Add PM Threshold Profile Field Description

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

Field	Description
	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 6-54 for the related command.

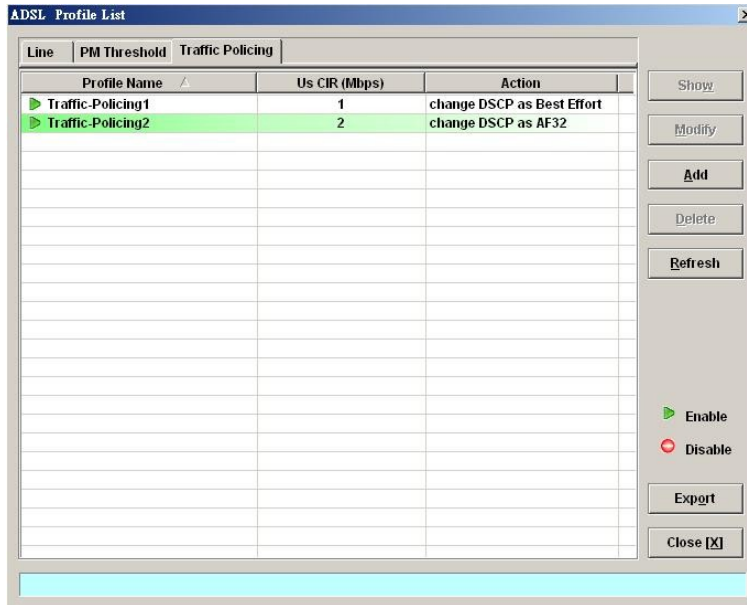
One example of application of traffic policing is as follows.

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 5-37 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 5-38 shows the **Add Traffic Policing Profile Dialog**. Table 5-28 depicts the related parameters.

Figure 5-38 Add Traffic Policing Profile Dialog

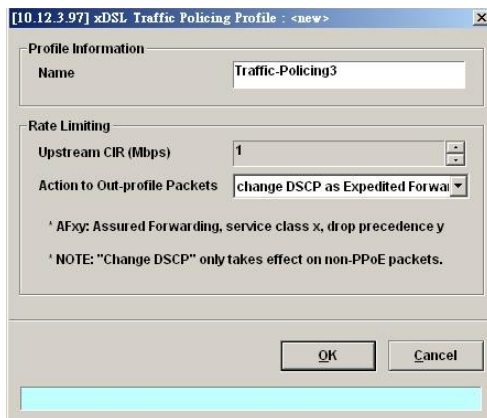


Table 5-28 Add Traffic Policing Profile Field Description

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 6-54).



Please refer to Figure 6-65 for more details of Differentiated Service Code Point.

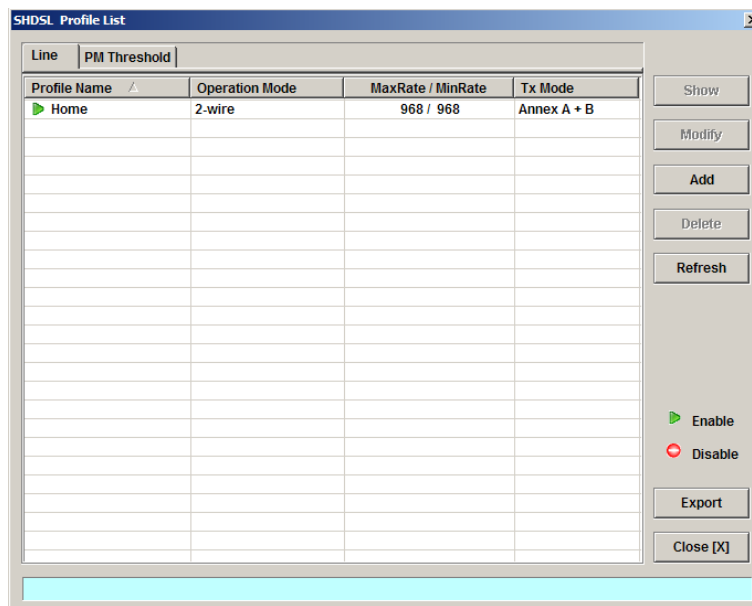
SHDSL Profile

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 5-39.

Figure 5-39 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 5-40. Table 5-29 depicts the related parameters.

Figure 5-40 Add SHDSL Line Profile– Transmission Rate Dialog

Table 5-29 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 5-41. Table 5-30 depicts the related parameters.

Figure 5-41 Add SHDSL Line Profile– SNR Margin Dialog

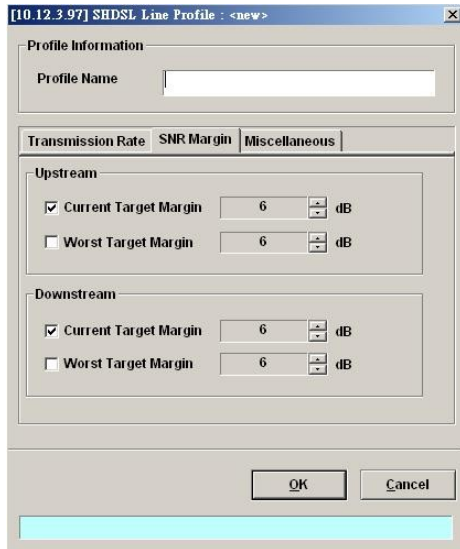


Table 5-30 Add SHDSL Line Profile - SNR Margin Dialog Description

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 5-42. Table 5-31 depicts the related parameters.

Figure 5-42 Add SHDSL Line Profile– Miscellaneous Dialog

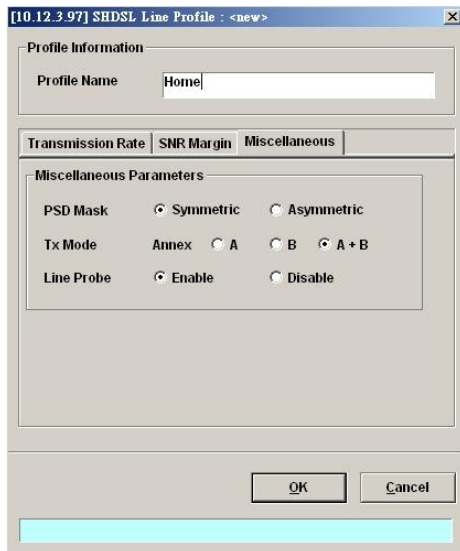


Table 5-31 Add SHDSL Line Profile– Miscellaneous Dialog Description

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 AMS LCT 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.

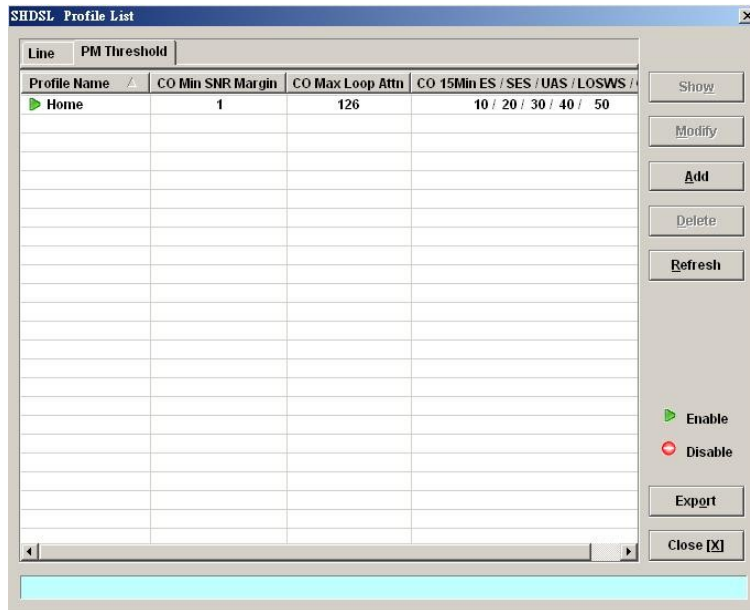
The NE supports to define the Near-End and Far-End thresholds of ES (Errored Seconds), SES (Severely Errored Seconds), and UAS (Unavailable Seconds) conditions in 15 minutes and 1 day interval. The definition of ES, SES and UAS are as follows.

- 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 5-43 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 5-43.

Figure 5-43 SHDSL 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 5-44 shows **Add SHDSL PM Threshold Profile Dialog**. Table 5-32 depicts the related parameters.

Figure 5-44 Add SHDSL PM Threshold Profile Dialog

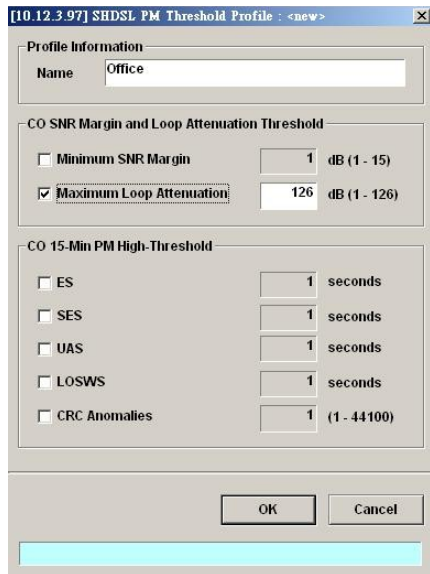


Table 5-32 Add SHDSL PM Threshold Profile Dialog Description

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 5-26, 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 5for 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 configuring 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 5-45.

Figure 5-45 VLAN Profile List- IP Traffic Dialog

Profile Name	Queue	Ds Rate(Kbps)	Us Rate(Kbps)
2M-512K	high	2048	512
Enterprise	highest	29984	<no limit>

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 5-46 shows **Add xDSL IP Traffic Profile Dialog**. Table 5-33 depicts the related parameters.

Figure 5-46 Add xDSL IP Traffic Profile Dialog

Table 5-33 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.



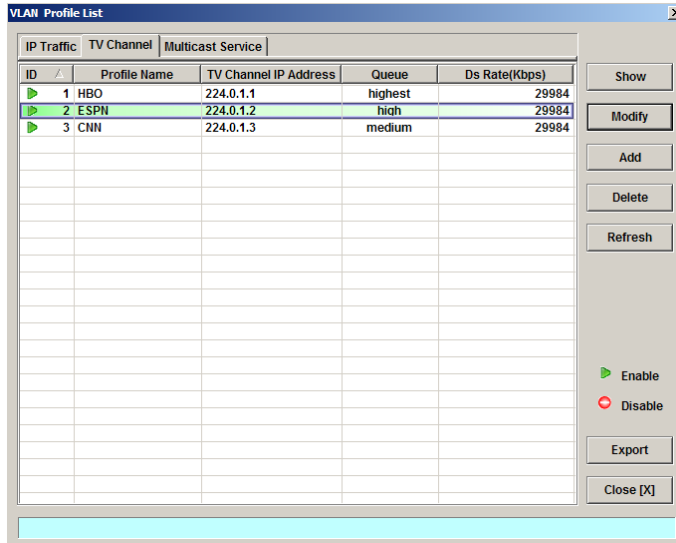
If the IP traffic profile is not configured or configured by mistake, the PVC can not be enabled.

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 5-47.

Figure 5-47 VLAN Profile List– TV Channel Dialog



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 5-48 shows **Add xDSL TV Channel Profile Dialog**. Table 5-34 depicts the related parameters.

Figure 5-48 Add xDSL TV Channel Profile Dialog

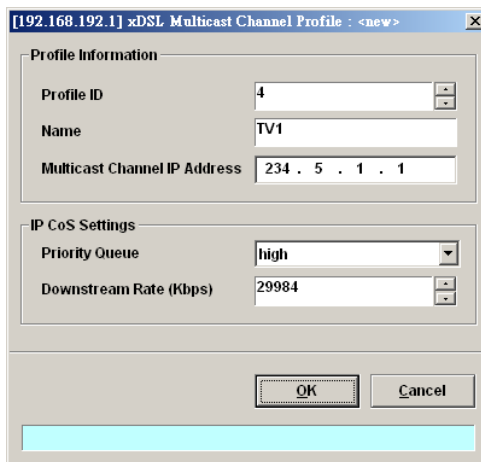


Table 5-34 Add xDSL TV Channel Profile Dialog Description

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.

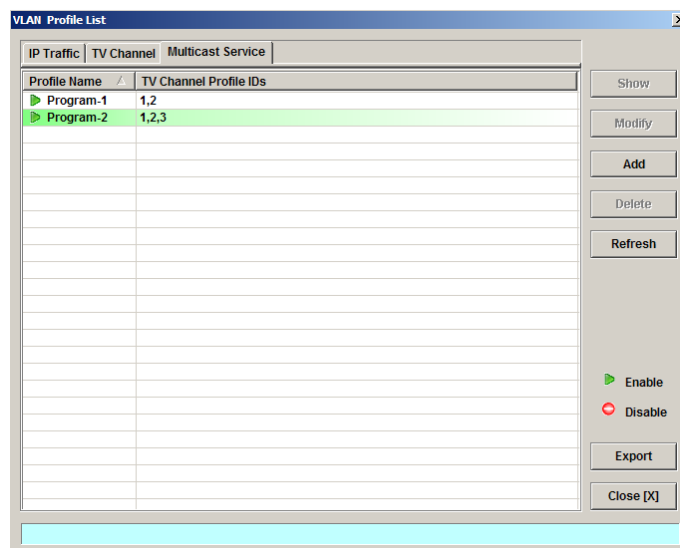
Multicast Service Profile

The multicast service profile is a set of TV channel profiles. Once the TV channel profiles are created, you can generate the multicast service profile to bind suitable TV channel profiles. Each multicast service profile is viewed as a service package for the subscriber to book. The operator then applies the booked multicast service profile to the distinct VC-to-VLAN associated with the subscriber. (see Chapter 7).

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.

Click the **Multicast Service** tab in **VLAN Profile List Dialog** to launch the **VLAN Profile List–Multicast Service Dialog** as shown in Figure 5-49.

Figure 5-49 VLAN Profile List– Multicast Service Dialog



Click ‘Add’ button to generate a multicast service profile, each profile must have its unique profile name. Or select an existent profile and click ‘Modify’ to modify it. Figure 5-50 shows **Add xDSL Multicast Service Profile Dialog**. Table 5-35 depicts the related parameters.

Figure 5-50 Add xDSL Multicast Service Profile Dialog

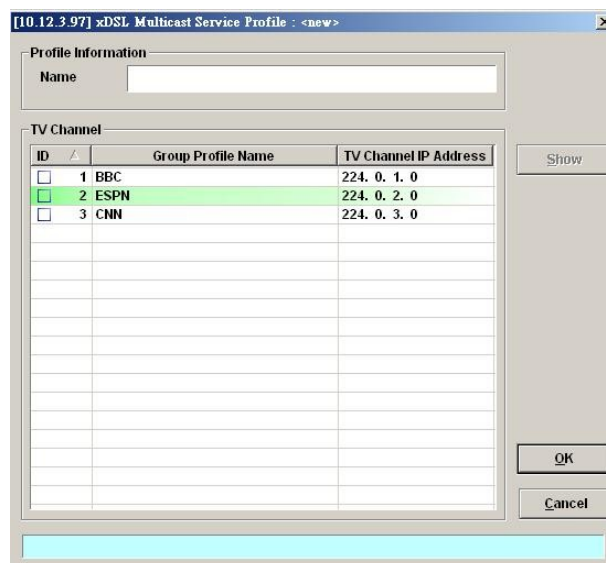


Table 5-35 Add Multicast Service Profile Dialog Description

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.

- Step 1** Click Configuration → Profile → Alarm Definition on **Main Menu** to open the **Alarm Definition List** Dialog as shown in Figure 5-51. Table 5-36 depicts the related parameters.

Figure 5-51 Alarm Definition List Dialog

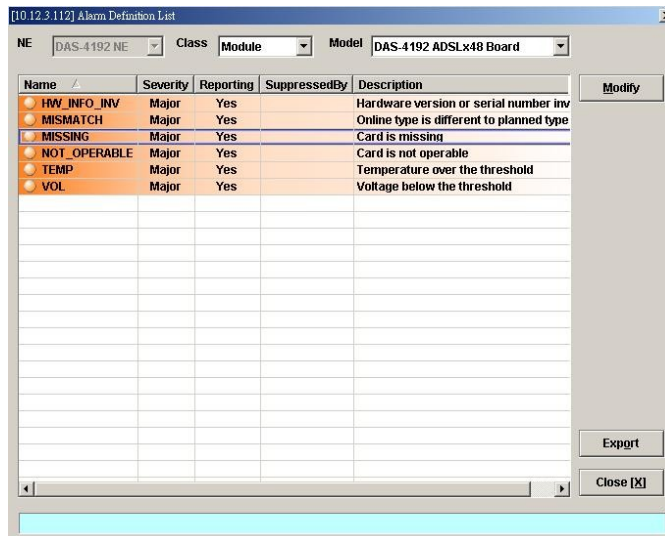


Table 5-36 Alarm Definition List Dialog Description

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.

Field	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 5-52 shows **Modify Alarm Definition Dialog**, and Table 5-37 depicts the related parameters.

Figure 5-52 Modify Alarm Definition Dialog

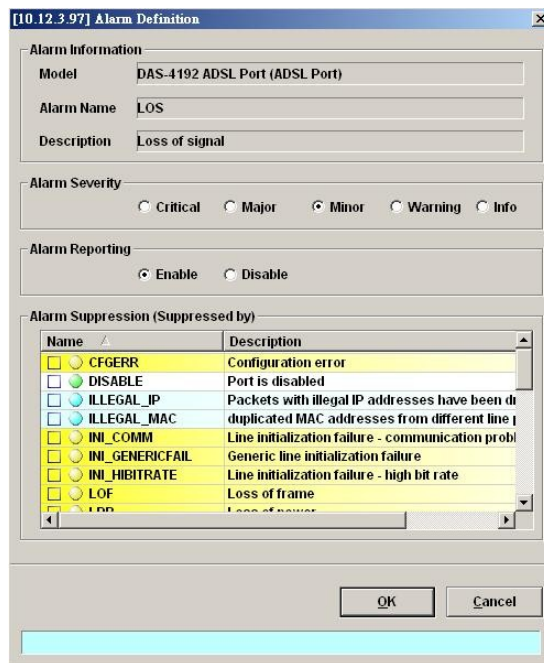


Table 5-37 Modify Alarm Definition Dialog Description

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.

This page is leave in blank for note or memo use

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 6-53. Table 6-38 depicts the related parameters.
 Or
 Click Configuration → xDSL → SHDSL Port Setting on **Main Menu** to open the **SHDSL Port List** Dialog. Table 6-38 depicts the related parameters.

Figure 6-53 ADSL Port List Dialog

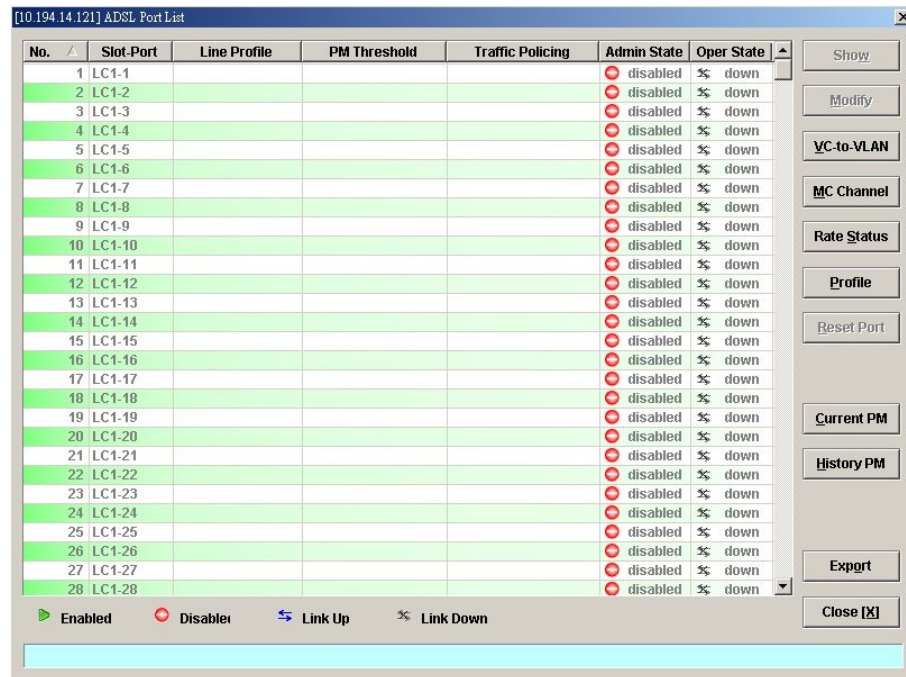


Table 6-38 xDSL Port List Dialog Description

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)
Oper State	It specifies the operational 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 6-54 shows **ADSL Port Modification Dialog**. Table 6-39 depicts the related parameters.

Figure 6-54 ADSL Port Modification Dialog

Table 6-39 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.
Packet Filter Groups	
Upstream/USG1~3:usg1~3	Check the checkbox to select packet filter group for upstream.
Downstream/DSG1~4:dsg1~4	Check the checkbox to select packet filter group for downstream.
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 6-55 shows **SHDSL Port Modification Dialog**. Table 6-40 depicts the related parameters.

Figure 6-55 SHDSL Port Modification Dialog

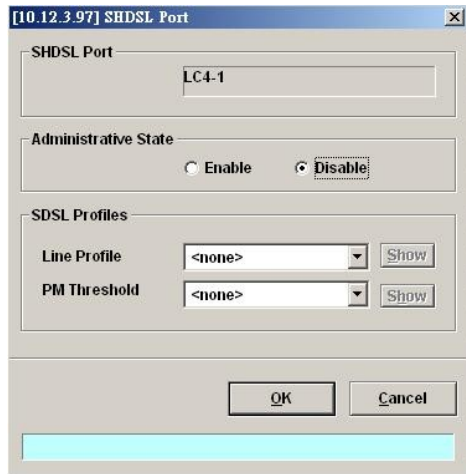


Table 6-40 SHDSL Port Modification Dialog Description

Field	Description
SHDSL Port	This indicates the current SHDSL Port which is under m
Administrative State	Enable or disable the specified SHDSL port.
SHDSL Profiles	
Line Profile	Use this combo-box to select an existent SHDSL line pr
PM Threshold	Use this combo-box to select an existent PM Threshold
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

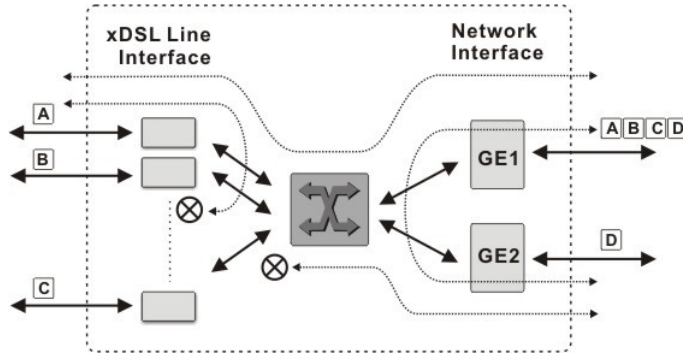
- Traffic Policing
- Service Type Control

GE Network Interface Management

There are two GE network interfaces, GE1 and GE2, for DAS4-Series 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.

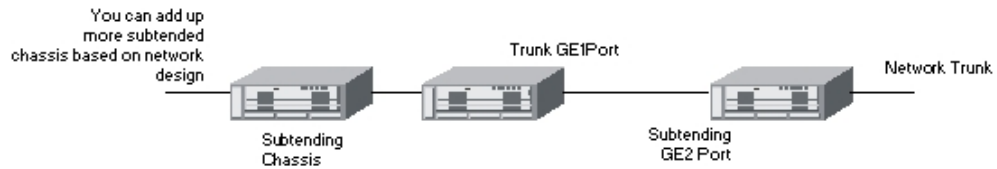
Figure 6-56 shows the packet forwarding diagram. As can be seen, the so-called “Port Isolation” indicates that all xDSL users can not communicate with each other. That is, all traffic from the xDSL line interface is forwarded to the GE1 interface. In the mean time, once the GE2 is configured as a subtended port, all the ingress traffic of GE2 is restricted to be forwarded to GE1.

Figure 6-56 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 6-57. As can be seen in Figure 6-57, three DAS4-Series 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 6-57 Illustration of 3 DAS4-Series 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 6-58 and Table 6-41 depicts the related parameters.

Figure 6-58 Trunk Port Dialog

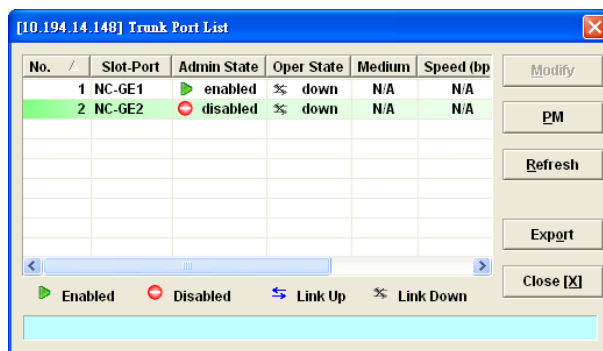


Table 6-41 Trunk Port Dialog Description

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.
Medium	This indicated the UGE medium is fiber or copper
Speed (bps)	An estimate of the interface's current bandwidth in bits per second.
Oper state	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 6-59 shows the **Trunk Port Configuration Dialog**, and Table 6-42 depicts the related parameters.

Figure 6-59 Trunk Port Configuration Dialog

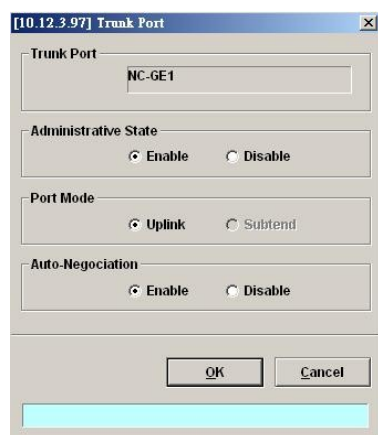


Table 6-42 Trunk Port Configuration Dialog Description

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 6-60 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 6-60, 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.

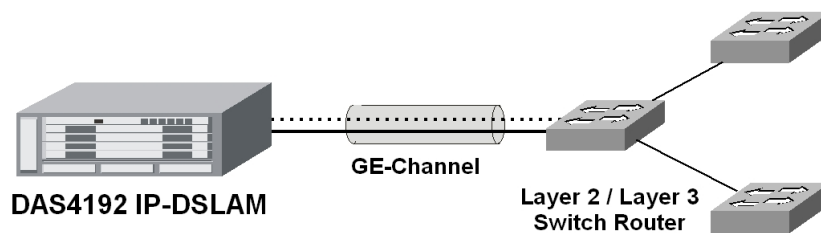
Dynamic link aggregation (LACP)

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 6-60. 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 6-60 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 6-61. Table 6-43 depicts the related parameters.

Figure 6-61 Link Aggregation Setting Dialog

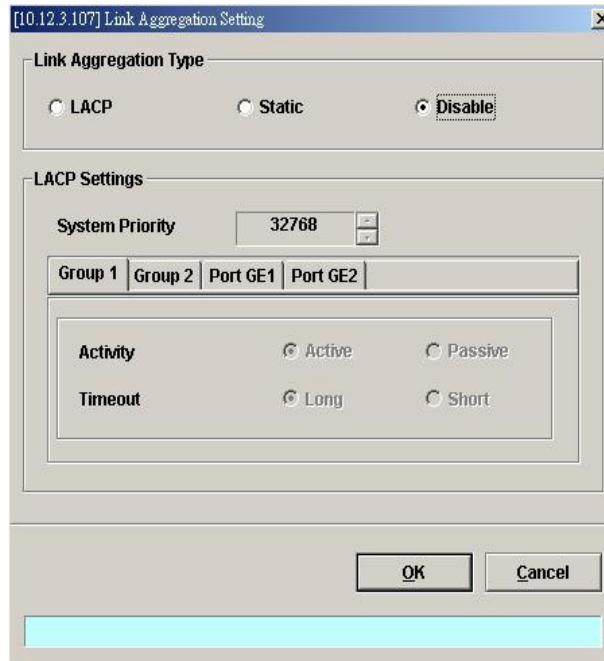


Table 6-43 Link Aggregation Setting Dialog Description

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> <p>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.</p> <p>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.</p>

Table 6-43 Link Aggregation Setting Dialog Description (Continued)

Timeout	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. Its value is either long (30 seconds) or short (1 second).
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

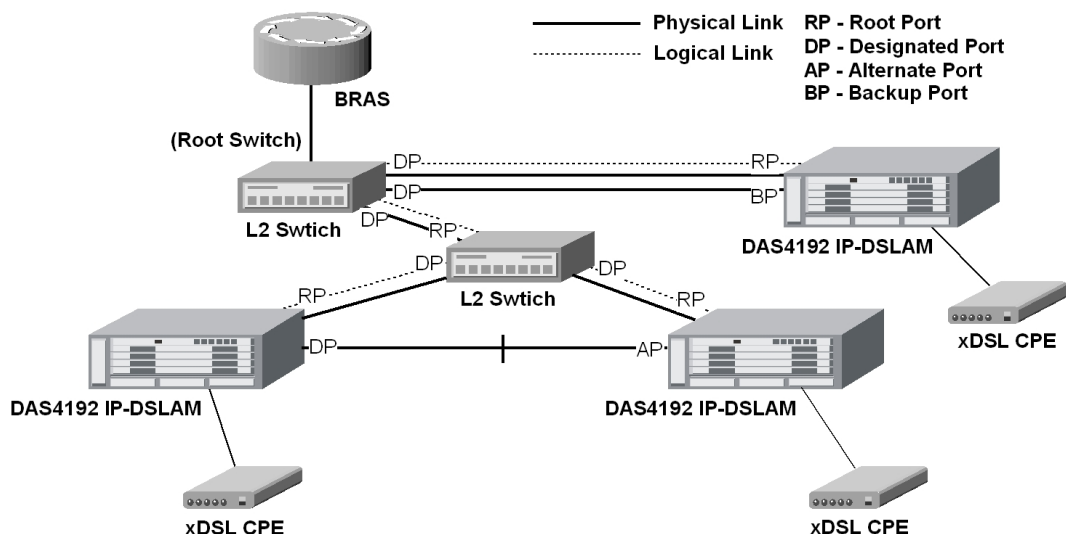
The 802.1D Spanning Tree Protocol (STP) standard was designed at a time when the recovery of connectivity after an outage within a minute or so was considered adequate performance. Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) can be seen as an evolution of the 802.1D standard more than a revolution. 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 DAS4-Series IP-DSLAM is enabled, it assigns their network interface to play one of following port-roles. Figure 6-62 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 6-62 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 6-63. Table 6-44 depicts the related parameters.

Figure 6-63 Trunk RSTP Setting– Bridge Dialog

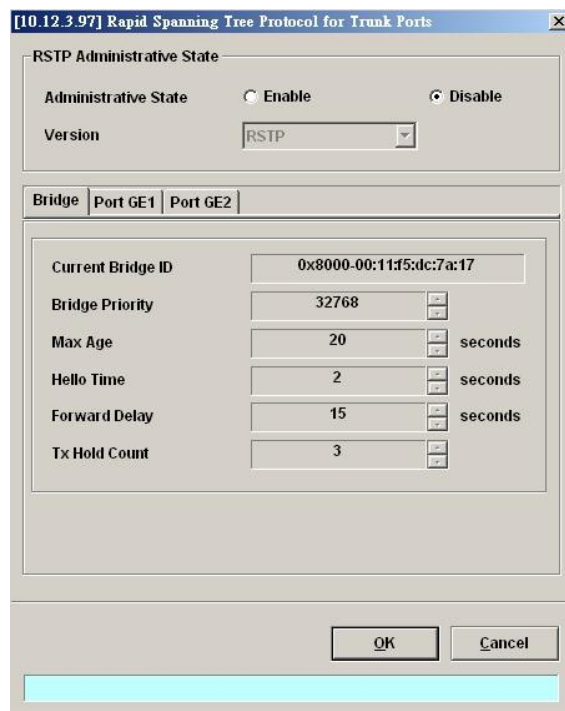


Table 6-44 Rapid Spanning Tree Protocol for Trunk Ports– Bridge Dialog Description

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

Table 6-44 Rapid Spanning Tree Protocol for Trunk Ports– Bridge Dialog Description (continued)

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 6-64. Table 6-45 depicts the related parameters.

Figure 6-64 Trunk RSTP Setting– Port GE1/Port GE2 Dialog

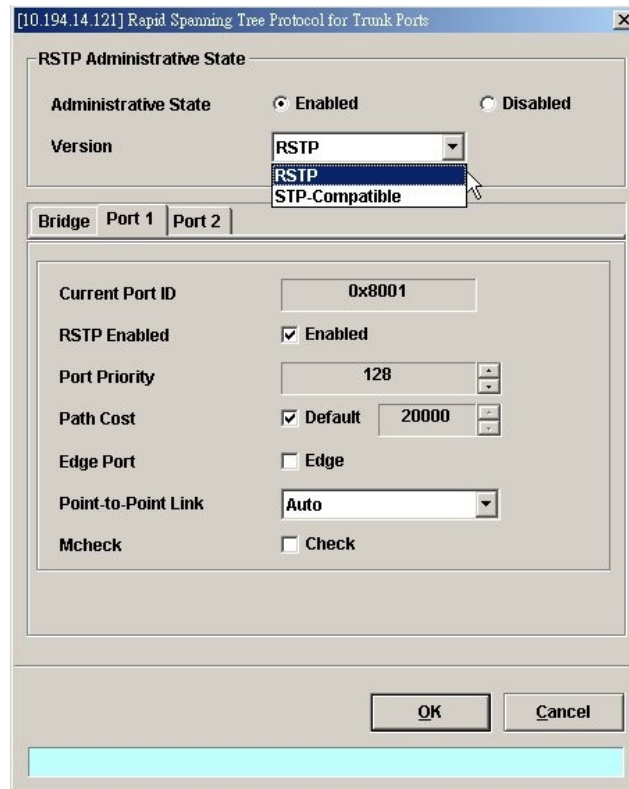


Table 6-45 RSTP for Trunk Ports– Port GE1/Port GE2 Dialog Description

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.
Mcheck (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 6-65 shows the DiffServ field.

Figure 6-65

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 6-46. 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 6-46 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 6-47 indicates the relationship of the 4 AF class.

Table 6-47 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)

The 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 6-66. Table 6-48 depicts the related parameters.

Figure 6-66 Trunk CoS Mapping and DSCP Re-mapping Dialog

802.1p User Priority-CoS Queue Mapping and DSCP Re-mapping

User Priority	Queue (Traffic Class)	DiffServ Code Point (DSCP)
0	3	Best Effort
1	1	Best Effort
2	2	Best Effort
3	4	Best Effort
4	5	Best Effort
5	6	Best Effort
6	7	Best Effort
7	8	Best Effort

* 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 6-48 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 6-59 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 6-67. Table 6-49 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 6-67 Manual VLAN Setting Dialog

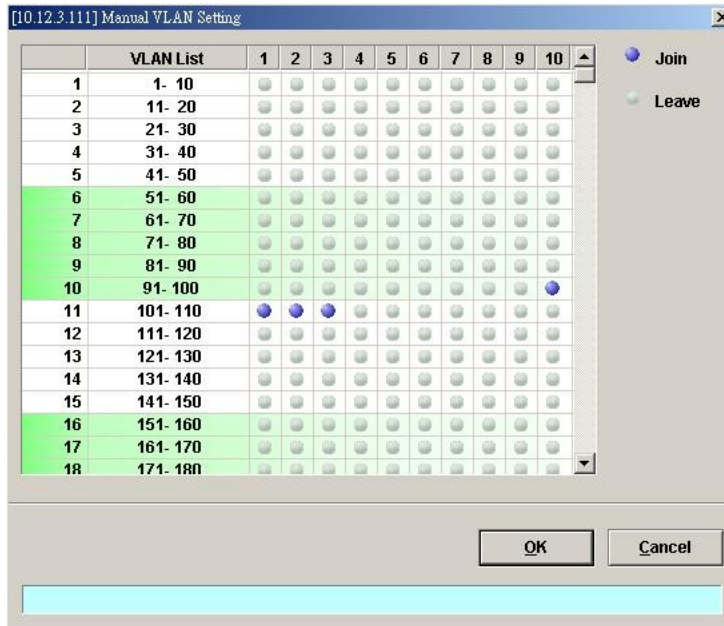


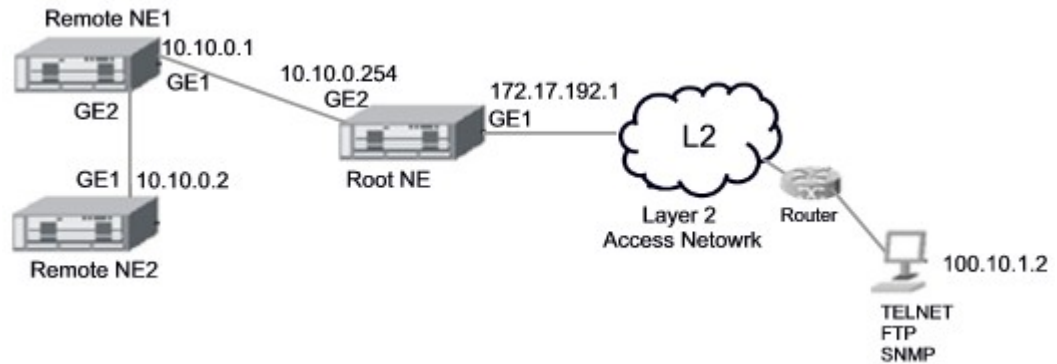
Table 6-49 Manual VLAN Setting Dialog Description

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 6-68 depicts a typical cascading topology.

Figure 6-68 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 6-68. 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 6-68. 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.

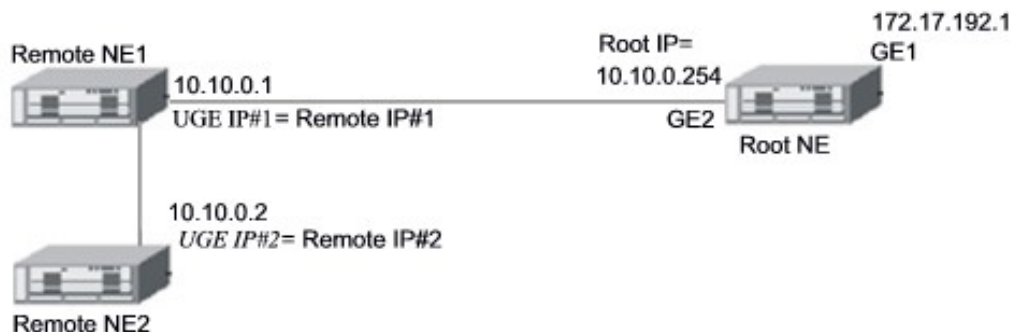
- “remote-ne-ip” of the Root-NE
- “UGE IP” of the Remote-NE

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 6-69, these NEs will work as a single NE which possesses several shelves via the EMS.

Figure 6-69 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.

-
- NOTE** 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.
-
- NOTE** The mini-GBIC and fiber have to be of the same type, either SM or MM.
-
- NOTE** 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 6-70 and Table 6-50 depicts the related parameters.

Figure 6-70 Cascaded Management Setting Dialog

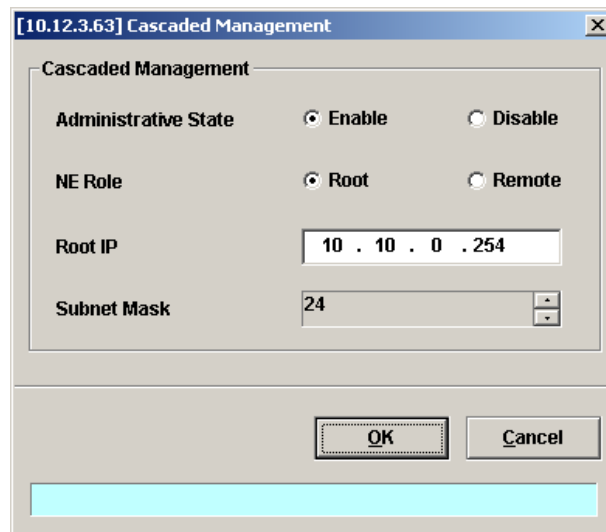


Table 6-50 Cascaded Management Setting Dialog Description

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 6-69)
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 6-69, the IP address of UGE ports of Remote-NE1 and Remote-NE2 have to be setup up first. As can be seen in Figure 6-69, 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 Management → Cascaded Management on **Main Menu** to open the **Cascaded Remote NE List** Dialog as shown in Figure 6-71 and Table 6-51 depicts the related parameters.

Figure 6-71 Remote NE List Dialog

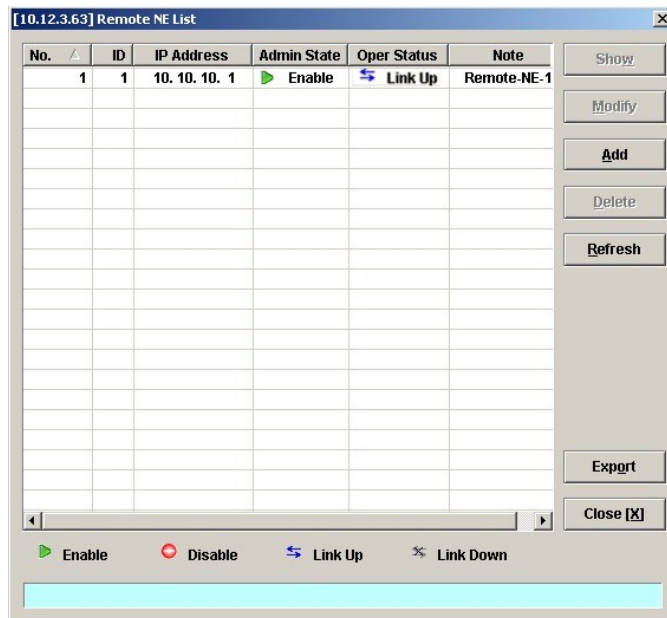


Table 6-51 Remote NE List Dialog Description

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 6-72 to add the new remote NE setting. Table 6-52 depicts the related parameters.

Figure 6-72 Remote NE Setting Dialog

The screenshot shows a dialog box titled "[192.168.192.1] Remote NE Setting". It contains the following fields and controls:

- Remote NE Information** (Section Header)
- ID**: Text input field containing "1".
- Administrative State**: Radio button group with "Enable" selected and "Disable" unselected.
- IP Address**: Text input field containing "10 . 10 . 10 . 1".
- SNMP Community**: Text input field containing "netman".
- Login User Name**: Text input field containing "admin".
- Login Password**: Text input field containing "*****".
- Note**: Text input field containing "Remote-NE-1".
- Buttons**: "OK" and "Cancel" buttons at the bottom.

Table 6-52 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.

This page is leave in blank for note or memo use

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

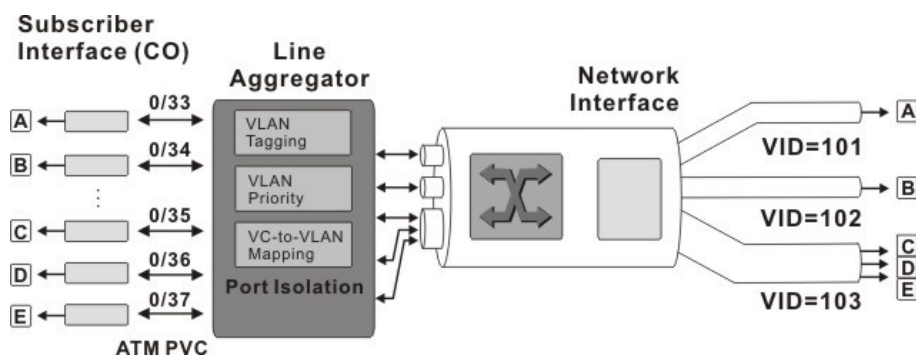
VC-to-VLAN Connection Management

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 7-73 illustrates the basic principle for VLAN assignment in the DAS4 Series IP-DSLAM. As shown in Figure 7-73, 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 7-73 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 (Qs) to the Ethernet frame if required. (see the definition of “Qs” in the description of Table 4-6)
 5. Forward the Ethernet frame from the xDSL subscriber to ISP.
- For the downstream traffic
 1. Strip off the VLAN tag (Qs) from the Ethernet frame if required. (see the definition of “Qs” in the description of Table 4-6)
 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.

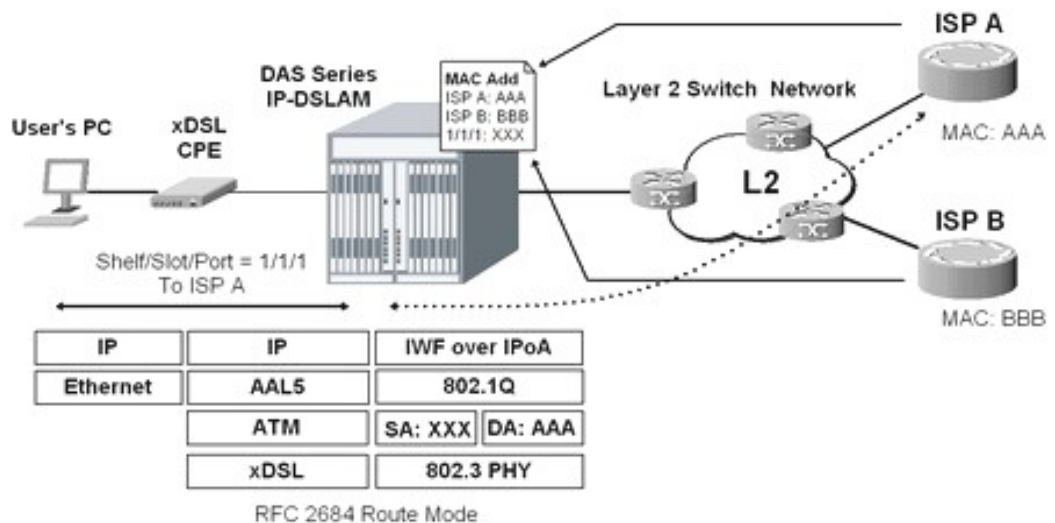
- For the upstream traffic
 1. Performs the ATM SAR (Segmentation and Reassembly) function to reassemble the ATM cells to get an ATM AAL5 frame.
 2. Strip off the ATM AAL5 trailer to get the RFC2684-encapsulated IP packet.
 3. Strip off the RFC2684 header to get the IP packet.
 4. Prefix an Ethernet 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 (Qs) to the Ethernet frame if required. (see the definition of “Qs” in the description of Table 4-6)
 6. Forward the Ethernet frame from the xDSL subscriber to ISP.
- For the downstream traffic
 1. Strip off the VLAN tag (Qs) from the Ethernet frame if required. (see the definition of “Qs” in the description of Table 4-6)
 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 7-74 illustrates an example of the IWF in the case of RFC 2684 routed mode.

Figure 7-74 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 7-75.

Figure 7-75 xDSL VC-to-VLAN List Dialog

No.	Slot-Port	VPI	VCI	Admin State	Link Status	RFC2684 Mode	VLAN / ISP Name
<input type="checkbox"/>	1 LC1-1	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	2 LC1-2	0	32	enable	up	bridged	100
<input type="checkbox"/>	3 LC1-3	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	4 LC1-4	0	32	enable	up	bridged	100
<input type="checkbox"/>	5 LC1-5	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	6 LC1-6	0	32	enable	up	bridged	100
<input type="checkbox"/>	7 LC1-7	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	8 LC1-8	0	32	enable	up	bridged	100
<input type="checkbox"/>	9 LC1-9	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	10 LC1-10	0	32	enable	up	bridged	100
<input type="checkbox"/>	11 LC1-11	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	12 LC1-12	0	32	enable	up	bridged	100
<input type="checkbox"/>	13 LC1-13	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	14 LC1-14	0	32	enable	up	bridged	100
<input type="checkbox"/>	15 LC1-15	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	16 LC1-16	0	32	enable	up	bridged	100
<input type="checkbox"/>	17 LC1-17	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	18 LC1-18	0	32	enable	up	bridged	100
<input type="checkbox"/>	19 LC1-19	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	20 LC1-20	0	32	enable	up	bridged	100
<input type="checkbox"/>	21 LC1-21	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	22 LC1-22	0	32	enable	up	bridged	100
<input type="checkbox"/>	23 LC1-23	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	24 LC1-24	0	32	enable	up	bridged	100
<input type="checkbox"/>	25 LC1-25	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	26 LC1-26	0	32	enable	up	bridged	100
<input type="checkbox"/>	27 LC1-27	0	32	enable	up	bridged	100
<input checked="" type="checkbox"/>	28 LC1-28	0	32	enable	up	bridged	100
<input type="checkbox"/>	29 LC1-29	0	32	enable	up	bridged	100

Buttons on the right: Show, Modify, Add, Delete, VC OAM Test, Profile, ISP List, ACL, Multi-Delete, Check All, Uncheck All, Export, Close [X].

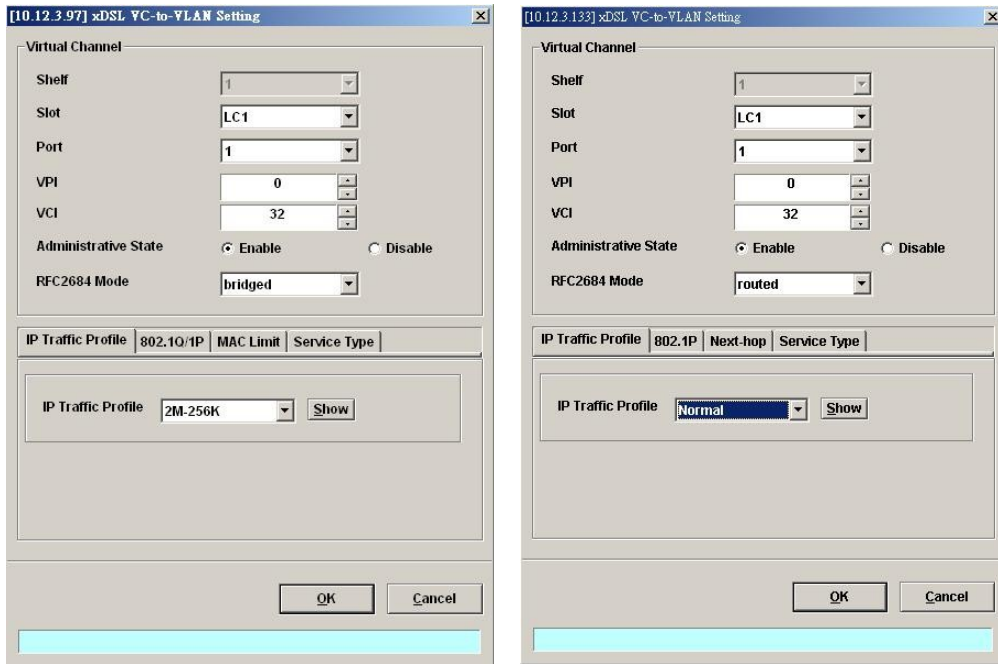
Legend: Enable (green triangle), Disable (red circle), Link Up (blue double arrow), Link Down (grey double arrow).

- Step 2** Click on the ‘Add’ button on the right hand side of Figure 7-75 to display the window (Figure 7-76) for adding new PVC and configuring the associated setting. **Figure 7-76** ~ **Figure 7-82** 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 7-53 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 7-76 xDSL VC-to-VLAN Setting – IP Traffic Dialog



(a) IP Traffic Dialog in RFC2684 bridged mode

(b) IP Traffic Dialog in RFC2684 routed mode

Figure 7-77 xDSL VC-to-VLAN Setting – 802.1Q/1P Dialog (only for the RFC2684 bridged mode)

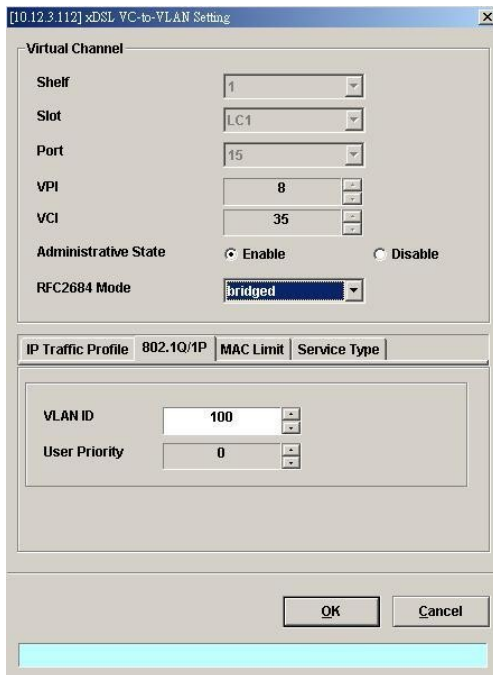


Figure 7-78 xDSL VC-to-VLAN Setting – 802.1P Dialog (only for the RFC2684 routed mode)

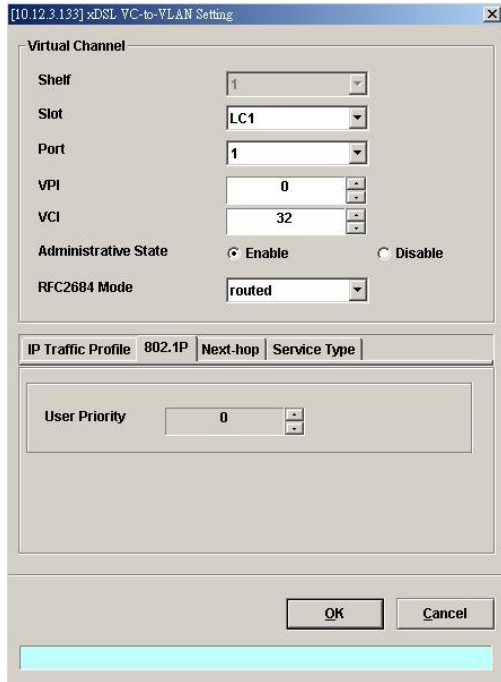


Figure 7-79 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 bridged mode

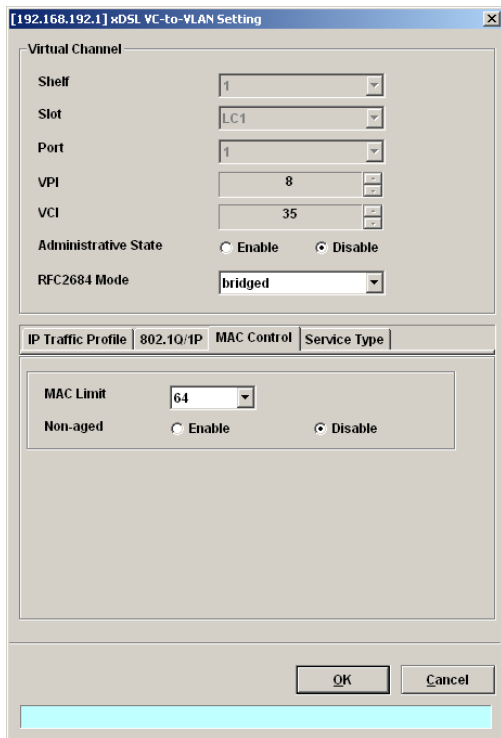


Figure 7-80 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 routed mode

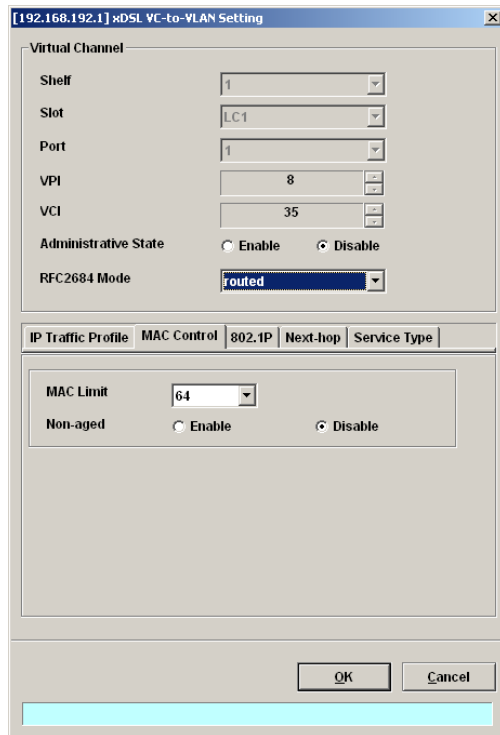


Figure 7-81 xDSL VC-to-VLAN Setting – Next-hop Dialog (only for the RFC2684 routed mode)

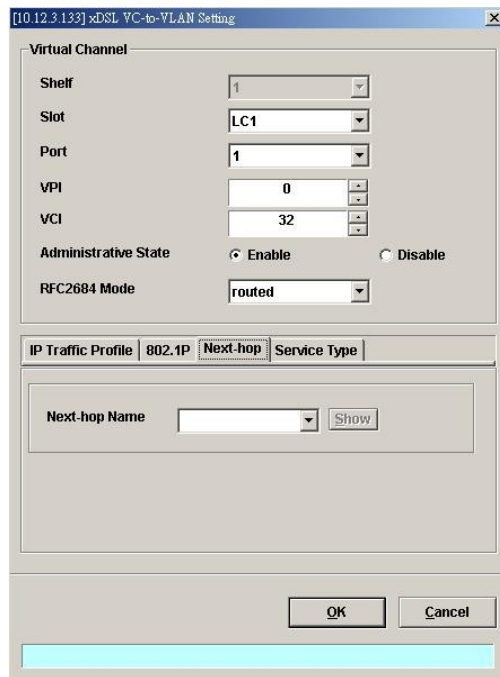


Figure 7-82 xDSL VC-to-VLAN Setting – Service Type Dialog

Virtual Channel

Shelf: 1
Slot: LC1
Port: 1
VPI: 8
VCI: 35
Administrative State: Enable Disable
RFC2684 Mode: bridged

IP Traffic Profile: 802.1Q/IP | MAC Control | Service Type

Service Type: PPPoE
DHCP IP Limit: 8
Static IP's Base / Limit:

IP base	Count

Buttons: Modify, Add, Delete, OK, Cancel

(a) PPPoE service in RFC2684 bridged mode

Virtual Channel

Shelf: 1
Slot: LC1
Port: 1
VPI: 8
VCI: 35
Administrative State: Enable Disable
RFC2684 Mode: bridged

IP Traffic Profile: MAC Control | 802.1Q/IP | Service Type

Service Type: DHCP
DHCP IP Limit: 8
Static IP's Base / Limit:

IP base	Count

Buttons: Modify, Add, Delete, OK, Cancel

(b) DHCP service in RFC2684 bridged mode

Virtual Channel

Shelf: 1
Slot: LC1
Port: 1
VPI: 8
VCI: 35
Administrative State: Enable Disable
RFC2684 Mode: bridged

IP Traffic Profile: MAC Control | 802.1Q/IP | Service Type

Service Type: static IP
DHCP IP Limit: 8
Static IP's Base / Limit:

IP base	Count
10.10.10.1	1

Buttons: Modify, Add, Delete, OK, Cancel

(c) Static IP service in RFC2684 bridged mode

Virtual Channel

Shelf: 1
Slot: LC1
Port: 1
VPI: 8
VCI: 35
Administrative State: Enable Disable
RFC2684 Mode: routed

IP Traffic Profile: MAC Control | 802.1P | Next-hop | Service Type

Service Type: static IP
DHCP IP Limit: 8
Static IP's Base / Limit:

IP base	Count
10.10.10.1	1

Buttons: Modify, Add, Delete, OK, Cancel

(d) Static IP service in RFC2684 routed mode

Virtual Channel

Shelf: 1
Slot: LC1
Port: 1
VPI: 8
VCI: 35
Administrative State: Enable Disable
RFC2684 Mode: bridged

IP Traffic Profile | 802.1Q/IP | MAC Control | Service Type

Service Type: PPPoE+DHCP
DHCP IP Limit: 1
Static IP's Base / Limit

IP base	Count

Modify Add Delete

OK Cancel

(e) PPPoE + DHCP service in RFC2684 bridged mode

Virtual Channel

Shelf: 1
Slot: LC1
Port: 1
VPI: 8
VCI: 35
Administrative State: Enable Disable
RFC2684 Mode: bridged

IP Traffic Profile | 802.1Q/IP | MAC Control | Service Type

Service Type: PPPoE+static IP
DHCP IP Limit: 1
Static IP's Base / Limit

IP base	Count
10.10.10.1	1

Modify Add Delete

OK Cancel

(f) PPPoE + Static IP service in RFC2684 bridged mode

Virtual Channel

Shelf: 1
Slot: LC1
Port: 1
VPI: 0
VCI: 32
Administrative State: Enabled Disabled
RFC2684 Mode: bridged

IP Traffic Profile | MAC Control | 802.1Q/IP | Service Type

Service Type: transparent
DHCP IP Limit: 1
Client Limit: 1
Static IP's Base / Limit

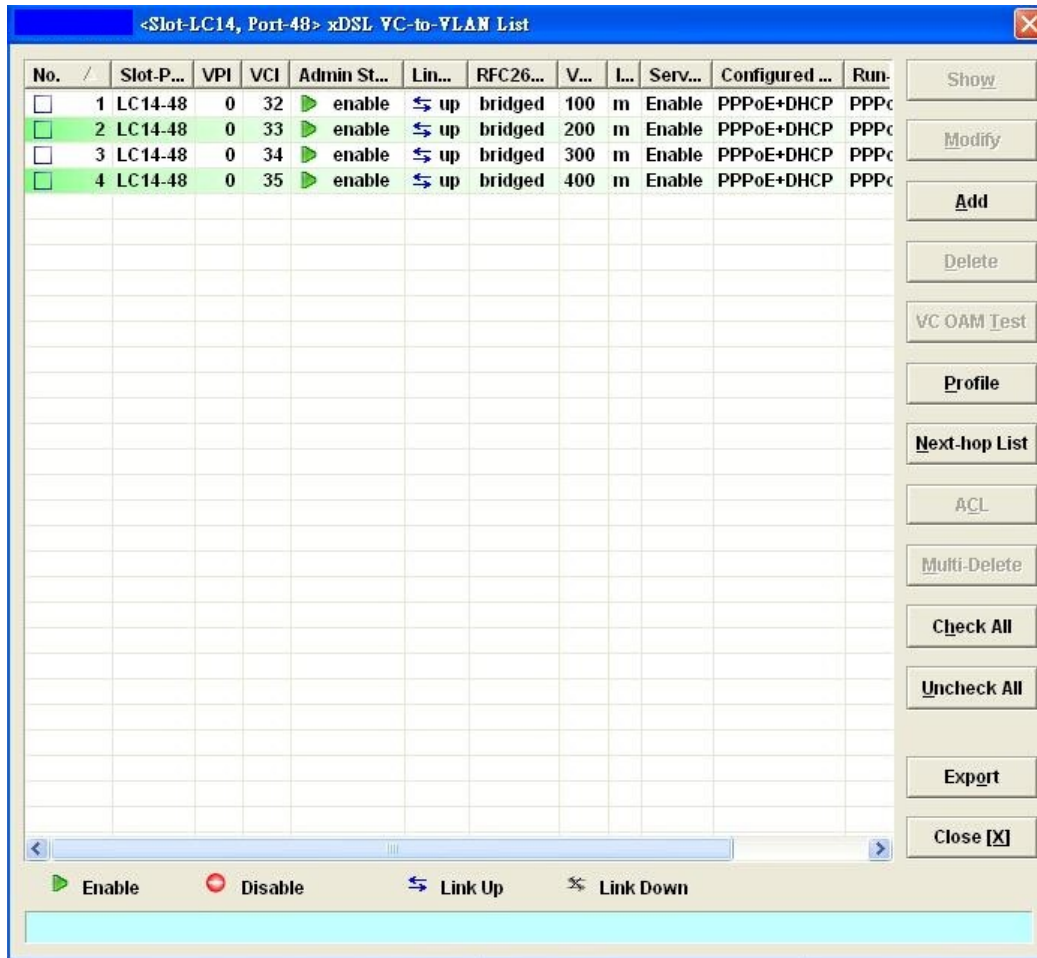
IP base	Count

Modify Add Delete

OK Cancel

(g) Transparent service in RFC2684 bridged mode





(g) Show service type configuration of different PVCs per port

Table 7-53 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/IP 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.

Field	Description
MAC Control Dialog	
MAC Limit	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 ● PPPoE+DHCP ● PPPoE+Static IP ● Transparent
DHCP IP Limit [only for DHCP Service]	This indicates the number of IP to be allowed while DHCP or DHCP+PPPoE is selected
Client Limit [only for Transparent Service]	This attribute limits the number of Transparent client per PVC. It can not be bigger than MAC limit if service type is Transparent; otherwise it can not be bigger than 64.
Static IP's Basic/Limit [only for Static IP Service]	This specifies the base of the IP address and its range if the service type is Static IP or PPPoE+Static IP
Function Button	
Modify	Click this button to modify the IP address range of IP base.
Add	Click this button to add the IP address range of IP base.
Delete	Click this button to delete the IP address range of IP base.



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 ≥ Continuous IP Count



More than one PVCs can be configured in an 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 an 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 ≤ MAC limit per PVC of xDSL port.



In the RFC 2684 both bridged and routed mode, the NE supports to the amount of MAC limit in enabled PVCs ≤ 384 in each line card.



In the RFC 2684 bridged mode, the NE supports to the max numbers of MAC address per PVC of xDSL port which is located on the range in 1~16, 32, 40, 48, 56, 64. The setting is caused by the hardware limitation.



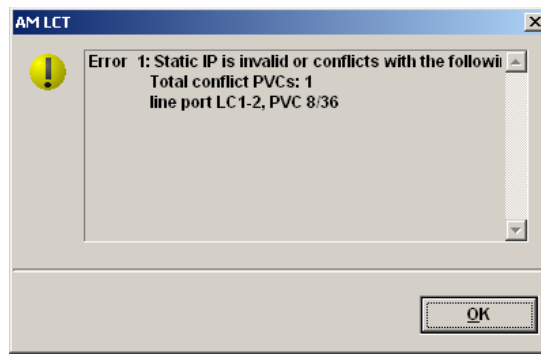
In the RFC 2684 bridged mode/routed mode, the NE supports to the amount of Service Type Control (STC) IP count ≤ 105 in each line card. The amount of Service Type Control (STC) IP count includes Static IP range, DHCP IP limit count, PPPoE session (1 occupied) and the count of the routed mode distributed in each port.



In the RFC 2684 bridged mode/routed mode, the NE supports eight IP base for each PVCs.



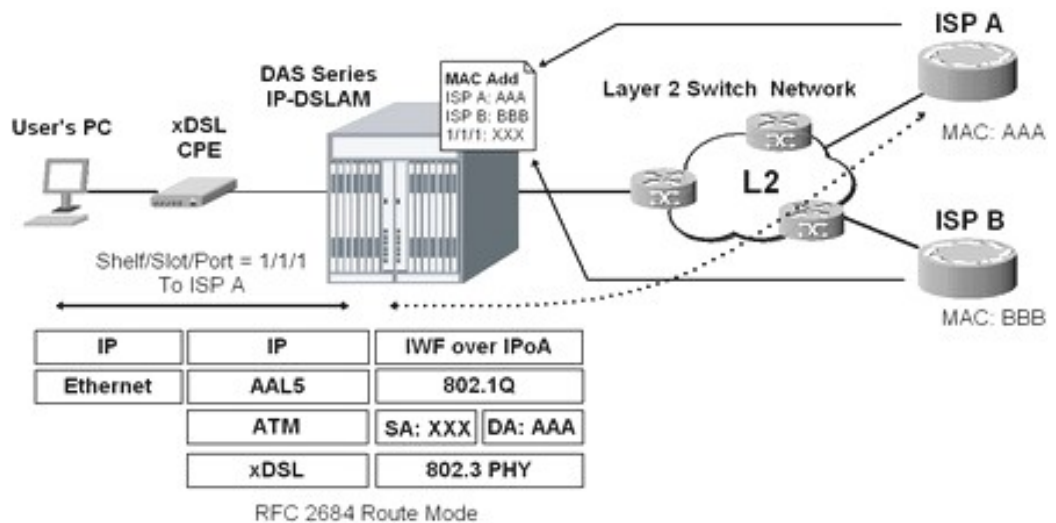
The error message with IP confliction is shown as following figure.



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 7-83 illustrates an example of the IWF in the case of RFC 2684 routed mode.

Figure 7-83 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 7-84 and Table 7-54 depicts the related parameters.

Figure 7-84 xDSL Next-hop List for IPoA Dialog

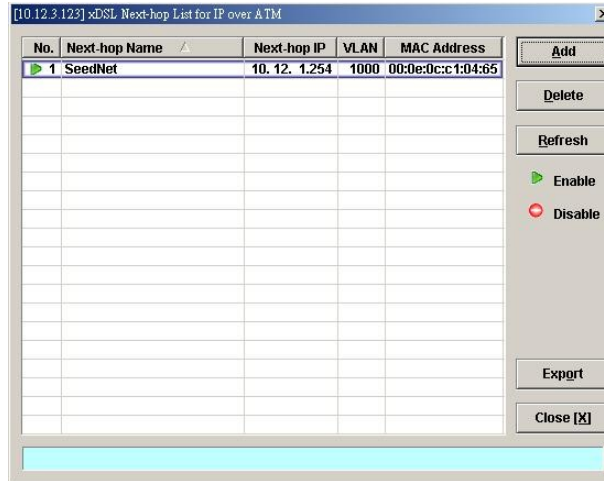


Table 7-54 xDSL Next-hop List for IPoA Dialog Description

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 7-85** shows **xDSL Next-hop for IPoA Dialog**, and **Table 7-55** depicts the related parameters.

Figure 7-85 Add xDSL Next-hop for IPoA Dialog

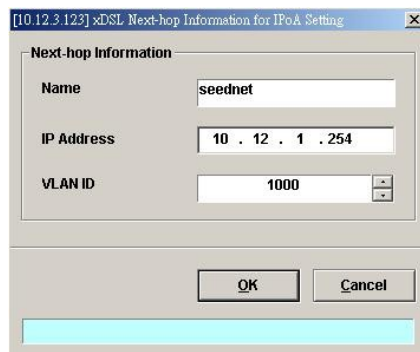


Table 7-55 Add xDSL Next-hop for IPoA Dialog Description

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.



If the “next-hop” is not configured or configured by mistake, the PVC can not be RFC 2684 routed mode.

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
- Packet filter

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 7-86 and Table 7-56 depicts the related parameters.

Figure 7-86 Packet Filtering Dialog

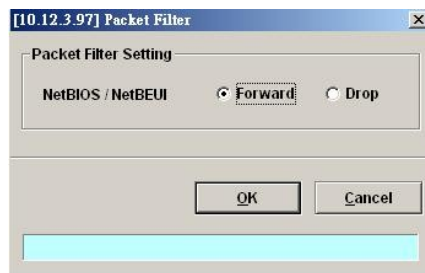


Table 7-56 Packet Filtering Dialog Description

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 7-75.
- Step 2** Select a port in **VC to VLAN List dialog** and click “ACL” button on the right hand side of Figure 7-75 to configure the Access Control List option of the selected port. Figure 7-87 illustrated the **VC-to-VLAN Access Control List dialog**, and Table 7-57 depicts the related parameters. Figure 7-88 illustrated the window for adding new MAC into the access control list.

Figure 7-87 VC-to-VLAN Access Control List dialog

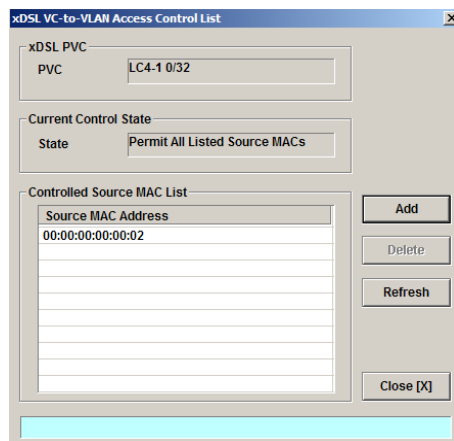
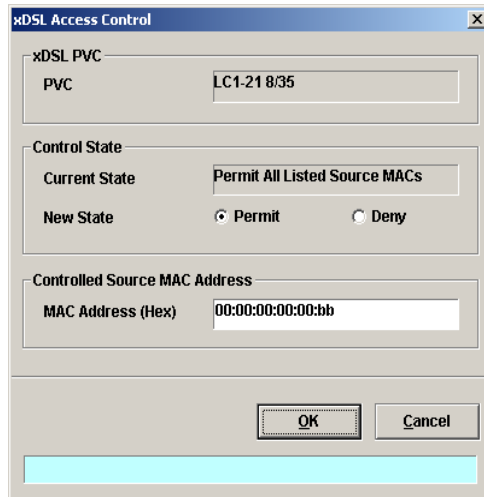


Table 7-57 VC-to-VLAN Access Control List Dialog Description

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 7-88** shows the **xDSL Access Control Dialog**, and Table 7-58 depicts the related parameters.

Figure 7-88 Add xDSL Access Control Dialog



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.

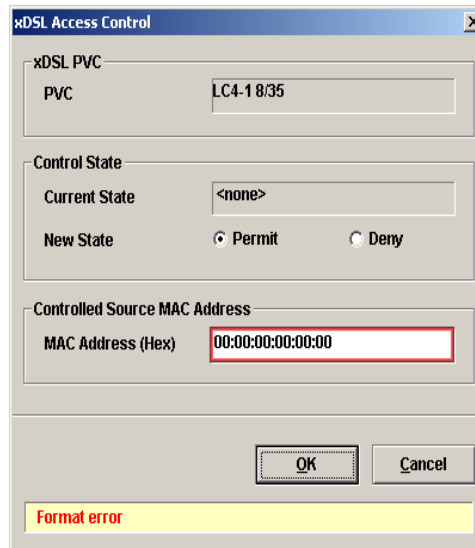


Table 7-58 Add xDSL Access Control Dialog Description

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 7-89 and Table 7-59 depicts the related parameters.

Figure 7-89 xDSL Access Control List

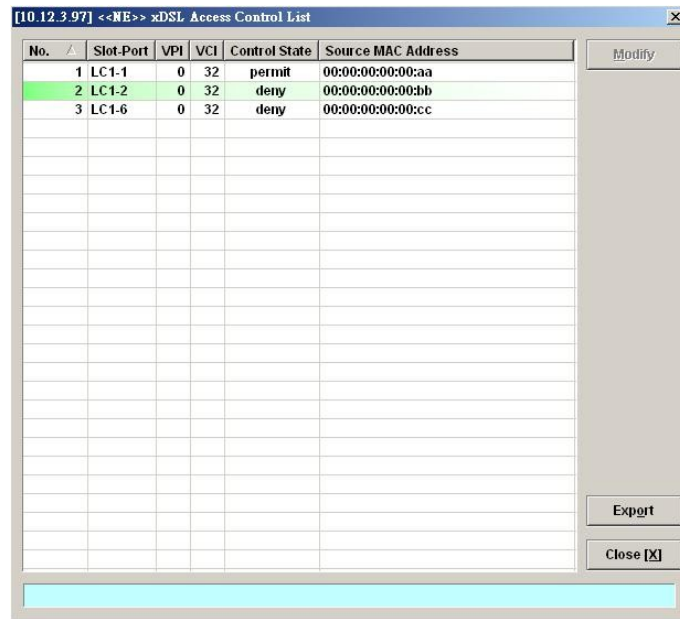


Table 7-59 xDSL Access Control List Description

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.

Packet filter

The DAS4-Series system supports various combinations of packet filtering functionality to provide the operator a method to permit/deny the ADSL subscriber's upstream/downstream Ethernet frame according to manually setting up the packet filtering functionality.

The types of packet filter functionality in DAS4-Series device are described as follows.

- Fully configured filter (FCF)
The FCF is the fully filter configuration to filter upstream or downstream incoming packet according to Ethernet type, IP protocol, transport source port and transport destination port on the specified ADSL line card.
- Ether type only filter (EOF)
The EOF is the packet filter configuration to filter upstream or downstream incoming packet only according to Ethernet type on the specified ADSL line card.
- Known filter (KF)
The KF is the packet filter configuration to filter upstream incoming packet according to some known protocols defined as BOOTP, (R)ARP, PPPoE, IGMP and multicast on the specified ADSL line card.

The actions of packet filter functionality in DAS4-Series device are described as follows

- "match-forward"
If the incoming packet matches the configured filter, the packet will be forwarded.
- "match-drop"
If the incoming packet matches the configured filter, the packet will be dropped.
- "no-match-drop"
If the incoming packet doesn't match the configured filter, the packet will be dropped.

- Step 1** Click Configuration → xDSL → Packet Filter on **Main Menu** to open the **Packet Filter** Dialog as shown in Figure 7-90.
- Step 2** Select a slot in **xDSL Slot Selection** Dialog and click "OK" button on the right hand side of Figure 7-90 to configure the packet filter of the selected ADSL line card. Figure 7-91 illustrated the **xDSL Packet Filter of Ethernet Type Only** Dialog and Table 7-60 depicts the related parameters. Figure 7-92 illustrated the **xDSL Packet Filter of Known Protocol** Dialog, and Table 7-61 depicts the related parameters. Figure 7-93 illustrated the **xDSL Fully Configured Packet Filter** Dialog, and Table 7-62 depicts the related parameters.
- Step 3** Select a slot in **xDSL Slot Selection** Dialog and click "OK" button on the right hand side of Figure 7-90 to configure the packet filter group of the selected ADSL line card. Figure 7-97 illustrated the **xDSL Packet Filter Group for Upstream** Dialog, and Table 7-66 depicts the related parameters. Figure 7-98 illustrated the **xDSL Packet Filter Group for Downstream** Dialog, and Table 7-64 depicts the related parameters.
- Step 4** Click Configuration → xDSL → ADSL Port Setting on **Main Menu** to open the **ADSL Port List** Dialog as shown in Figure 6-53 and choice an ADSL port then click 'Modify' button to select the packet filter groups applying to the specific ADSL port. Figure 7-96 shows **ADSL Port Modification Dialog**. Table 7-65 depicts the related parameters.

Figure 7-90 xDSL Slot Selection of Packet Filter

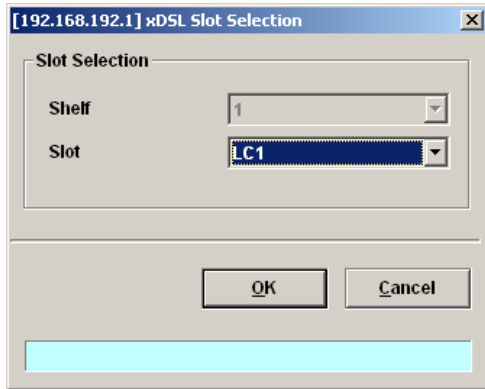


Figure 7-91 xDSL Packet Filter of Ethernet Type Only

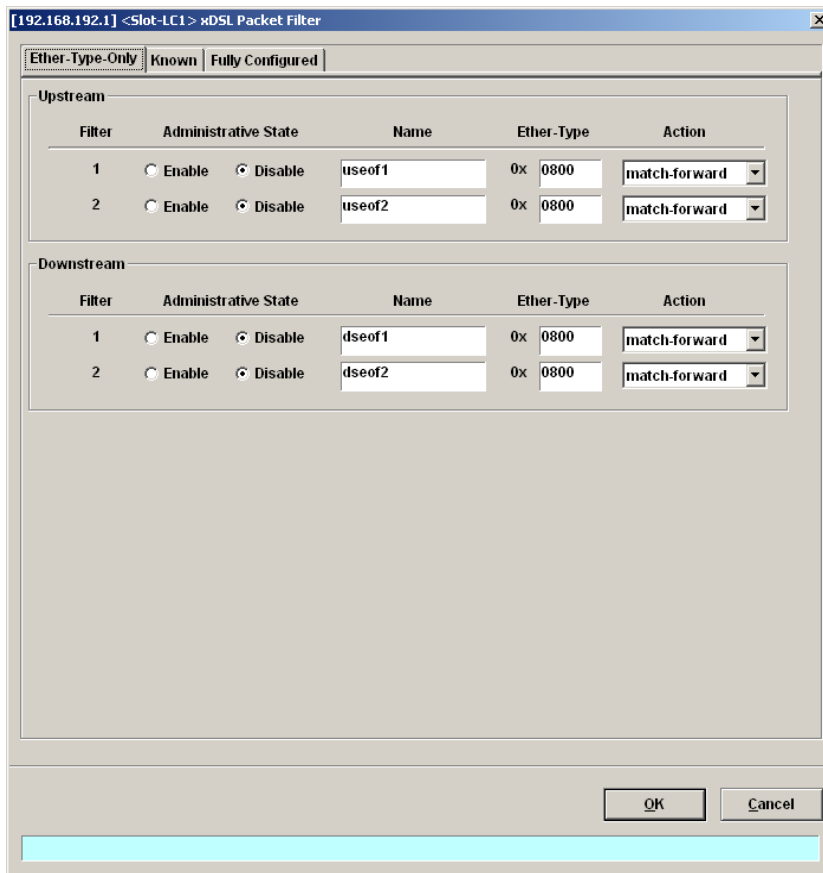


Table 7-60 xDSL Packet Filter Setting Description of Ethernet Type Only

Field	Description
Upstream/Downstream	
Administrative State	Enable: Apply the specified packet filter setting to the specified ADSL line card. Disable: Do not apply specified packet filter setting to the specified ADSL line card.
Name	This specifies the packet filter name according to the Ethernet type for upstream/downstream on the specified ADSL line card.
Ether-Type	This specifies the ethernet type of packets in a string format '0xNNNN' where N is a hex-decimal number between 0 to f.
Action	This indicates the actions if the packet filter functionality is enabled. The definitions of actions are as follows. <ul style="list-style-type: none"> • match-forward: It indicates that if the incoming packet matches the configured filter, the packet will be forwarded. The filter priority is the highest. • match-drop: It indicates that if the incoming packet matches the configured filter, the packet will be dropped. • unmatch-drop: It indicates that if the incoming packet doesn't match the configured filter, the packet will be dropped.

Figure 7-92 xDSL Packet Filter of Known Protocol

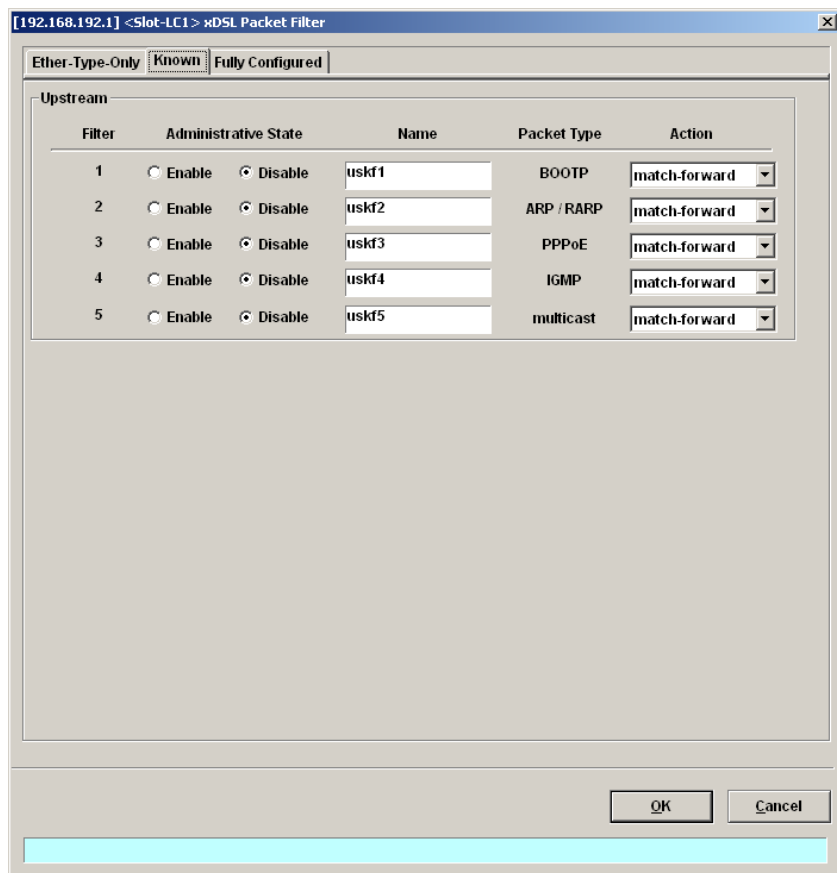


Table 7-61 xDSL Packet Filter Setting Description of Known Protocol

Field	Description
Upstream	
Administrative State	Enable: Apply the specified packet filter setting to the specified ADSL line card. Disable: Do not apply specified packet filter setting to the specified ADSL line card.
Name	This specifies the packet filter name according to the known protocols for upstream on the specified ADSL line card.
Action	This indicates the actions if the packet filter functionality is enabled. The definitions of actions are as follows. <ul style="list-style-type: none"> • match-forward: It indicates that if the incoming packet matches the configured filter, the packet will be forwarded. The filter priority is the highest. • match-drop: It indicates that if the incoming packet matches the configured filter, the packet will be dropped. • unmatch-drop: It indicates that if the incoming packet doesn't match the configured filter, the packet will be dropped.

Figure 7-93 xDSL Fully Configured Packet Filter

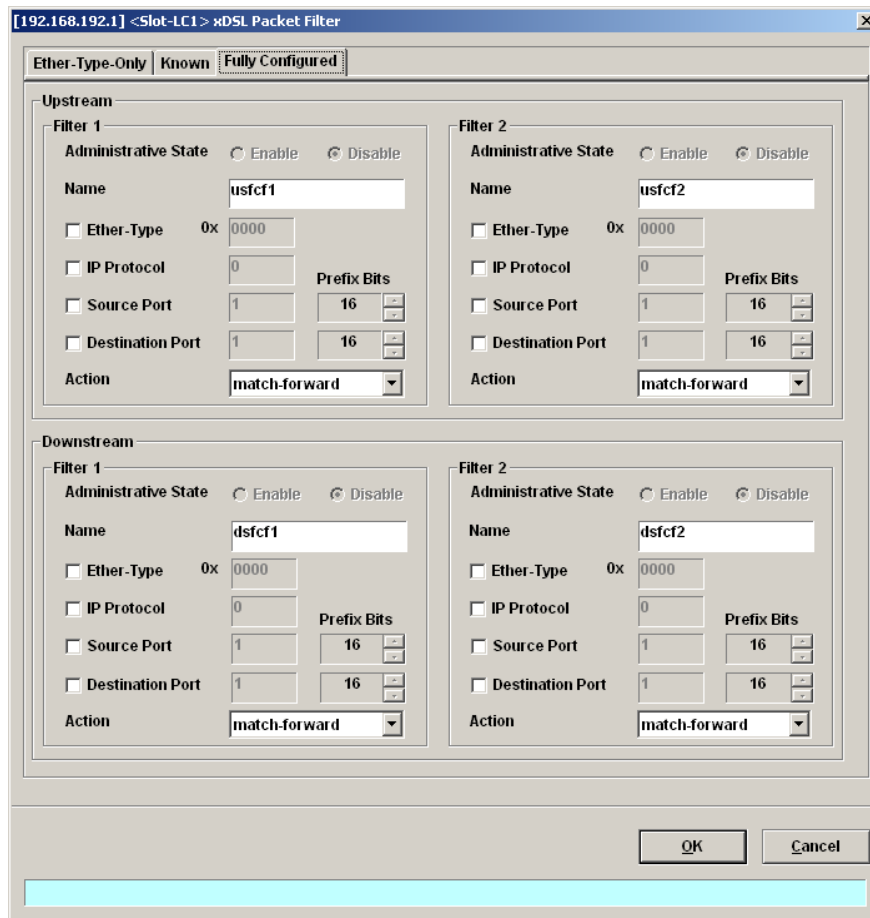


Table 7-62 xDSL Fully Configured Packet Filter Setting Description

Field	Description
Upstream-Filter 1~2/Downstream-Filter 1~2	
Administrative State	Enable: Apply the specified packet filter setting to the specified ADSL line card. Disable: Do not apply specified packet filter setting to the specified ADSL line card.
Name	This specifies the fully configured packet filter name for upstream/downstream on the specified ADSL line card.
Ether-Type	This specifies the ethernet type of packets in a string format '0xNNNN' where N is a hex-decimal number between 0 to f.
IP Protocol	This specifies the IP protocols of packet filter to allow or deny forwarding the packets within the matched IP protocol where the IP protocol number is a decimal number from 0 to 255. (Refer to Appendix D)
Source Port	This specifies the packet filter according to the source port of incoming packets where the source port number is a decimal number from 0 to 65535, disabled is -1.
Destination Port	This specifies the packet filter according to the source port of incoming packets where the source port number is a decimal number from 0 to 65535, disabled is -1.
Prefix Bits	This specifies the range of source port or destination port by prefix length mask configured in packet filter where the range of prefix bit is from 11 to 16.
Action	This indicates the actions if the packet filter functionality is enabled. The definitions of actions are as follows. <ul style="list-style-type: none"> • match-forward: It indicates that if the incoming packet matches the configured filter, the packet will be forwarded. The filter priority is the highest. • match-drop: It indicates that if the incoming packet matches the configured filter, the packet will be dropped. • unmatch-drop: It indicates that if the incoming packet doesn't match the configured filter, the packet will be dropped.

Figure 7-94 xDSL Packet Filter Group for Upstream

Filter	Administrative State	Name
<input type="checkbox"/> Ether-Type-Only Filter 1	disabled	useof1
<input type="checkbox"/> Ether-Type-Only Filter 2	disabled	useof2
<input type="checkbox"/> Fully Configured Filter 1	disabled	usfcf1
<input type="checkbox"/> Fully Configured Filter 2	disabled	usfcf2
<input type="checkbox"/> Known Filter 1	disabled	uskf1
<input type="checkbox"/> Known Filter 2	disabled	uskf2
<input type="checkbox"/> Known Filter 3	disabled	uskf3
<input type="checkbox"/> Known Filter 4	disabled	uskf4
<input type="checkbox"/> Known Filter 5	disabled	uskf5

Table 7-63 xDSL Packet Filter Group Setting Description for Upstream

Field	Description
USG1~3/Upstream Filter Group 1	
Administrative State	Enable: Apply the specified packet filter setting to the specified ADSL line card. Disable: Do not apply specified packet filter setting to the specified ADSL line card.
Name	This specifies the packet filter group name for upstream on the specified ADSL line card.
Upstream Packet Filters	
Ether-Type-Only Filter 1~2	Check the checkbox to select the Ethernet type packet filter for upstream on the specified ADSL line card.
Fully Configured Filter 1~2	Check the checkbox to select the fully configured packet filter for upstream on the specified ADSL line card.
Known Filter 1~5	Check the checkbox to select the known protocols packet filter for upstream on the specified ADSL line card.
Function Button	
Filter	Click this button to open the setting dialog of packet filter.
OK	Click this button to imply the setting of packet filter group.
Cancel	Click this button to cancel the setting of packet filter group.

Figure 7-95 xDSL Packet Filter Group for Downstream

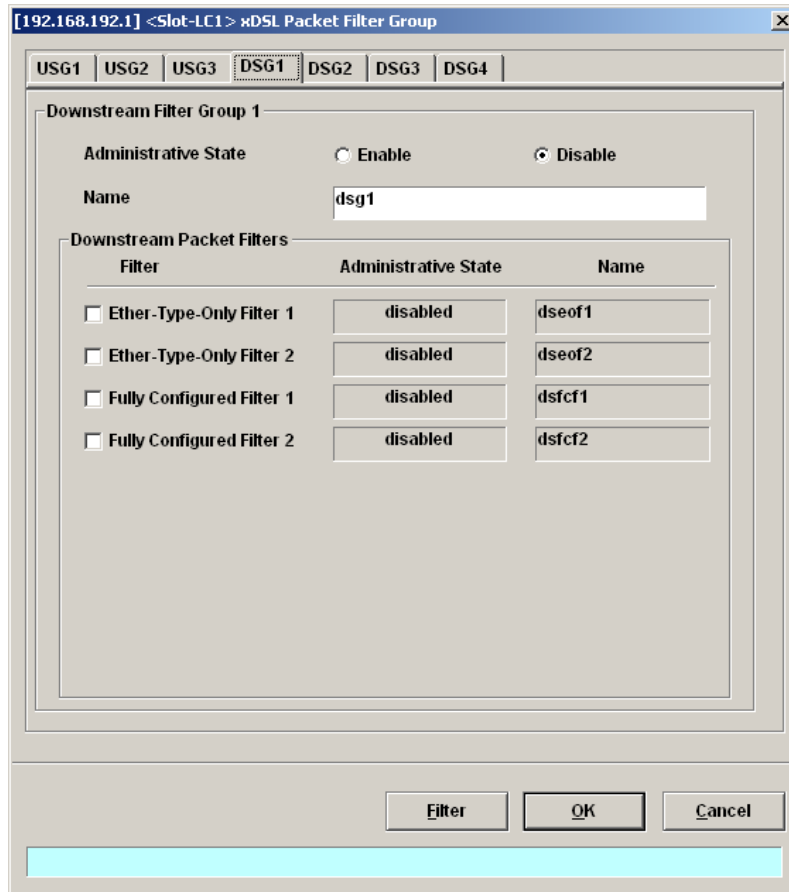


Table 7-64 xDSL Packet Filter Group Setting Description for downstream

Field	Description
DSG1~4/Downstream Filter Group 1	
Administrative State	Enable: Apply the specified packet filter setting to the specified ADSL line card. Disable: Do not apply specified packet filter setting to the specified ADSL line card.
Name	This specifies the packet filter group name for downstream on the specified ADSL line card.
Upstream Packet Filters	
Ether-Type-Only Filter 1~2	Check the checkbox to select the Ethernet type packet filter for downstream on the specified ADSL line card.
Fully Configured Filter 1~2	Check the checkbox to select the fully configured packet filter for downstream on the specified ADSL line card.
Function Button	
Filter	Click this button to open the setting dialog of packet filter.
OK	Click this button to imply the setting of packet filter group.
Cancel	Click this button to cancel the setting of packet filter group.

Figure 7-96 Implying the xDSL Packet Filter Group to the specified ADSL port

Table 7-65 xDSL Packet Filter Group Setting Description to the specified ADSL port

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.
Packet Filter Groups	
Upstream/USG1~3:usg1~3	Check the checkbox to select packet filter group for upstream.
Downstream/DSG1~4:dsg1~4	Check the checkbox to select packet filter group for downstream.
Function Button	
OK	Press this button to commit setting.
Cancel	Press this button to cancel setting.

Table 7-66 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 7-98** shows the **xDSL Static MAC Address Setting Dialog**, and **Table 7-67** depicts the related parameters.

Figure 7-98 xDSL Static MAC Address Setting Dialog

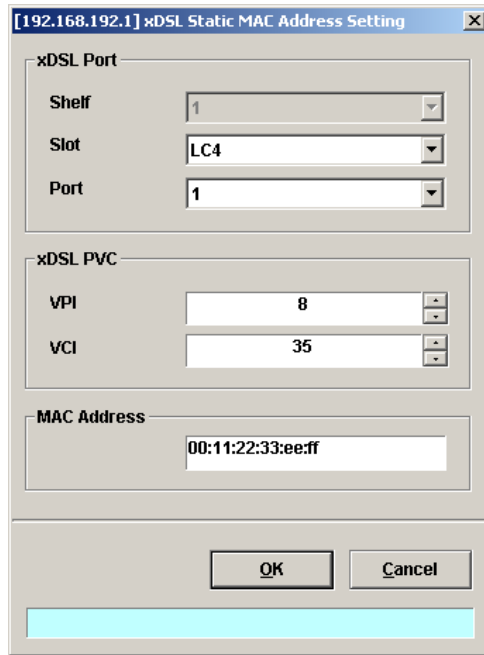


Table 7-67 xDSL Configured Filtering Database Entry List Description

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.

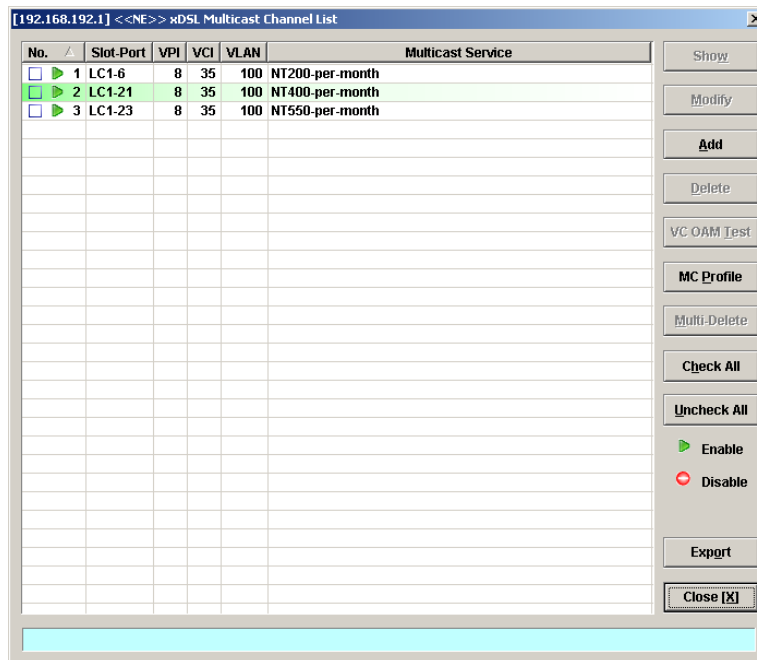
Here, a Multicast Service Profile represents a set of Multicast (TV) Channel Profiles. Each Multicast (TV) Channel Profile describes the attributes of a multicast stream (TV channel). In other words, the subscriber is restricted to receive the TV channels described recorded in the Multicast Service Profile.

Follow the subsequent procedures to to associate the ADSL subscriber with the created Multicast Service Profiles.

- 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 7-99 to open the window (Figure 7-100) for adding new multicast channel and configure the associated setting.

In Figure 7-100, it is noted that two individual tabs (Multicast Service Profile and Channel Limit) are provided to set the Multicast Channel related parameters. Click either one **tab** to launch the corresponding dialog to configure the parameters. Table 7-68 depicts the related parameters

Figure 7-99 xDSL Multicast Channel List Dialog



The differences between the “Multi-Delete” and “Delete” button on the right hand side of Figure 7-99 are as follows.

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

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

Figure 7-100 xDSL Multicast Channel Setting Dialog

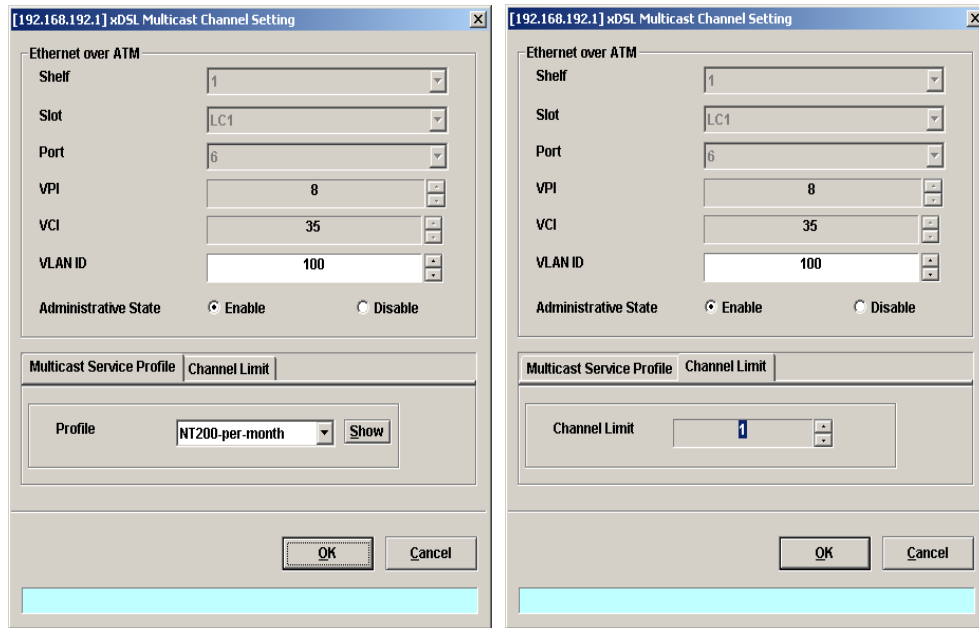


Table 7-68 xDSL Multicast Channel Setting Description

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 5.
Channel Limit Dialog	
Channel Limit	This specifies the allowed number of multicast streams 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 7-101 and Table 7-69 depicts the related parameters.

Figure 7-101 IGMP Snooping / IGMP Proxy Setting Dialog

The screenshot shows a configuration dialog box for IGMP Snooping and Proxy. The title bar reads "[192.168.192.1] IGMP Snooping / IGMP Proxy Setting". The dialog is divided into three main sections:

- 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:

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

Table 7-69 IGMP Snooping / 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 “frozen” 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. Disable this function will keep the learned MAC addresses permanent in the learning table.

Click Configuration → NE Management → MAC Aging on **Main Menu** to open the **MAC Aging** Dialog as shown in Figure 7-102 and Table 7-70 depicts the related parameters.

Figure 7-102 MAC Aging Setting Dialog

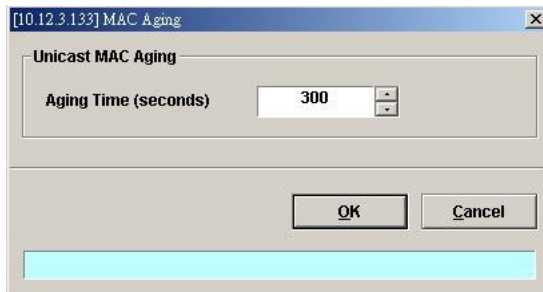


Table 7-70 MAC Aging Setting Dialog Description

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 7-103 and Table 7-71 depicts the related parameters.

Figure 7-103 VLAN MAC Limit List Dialog

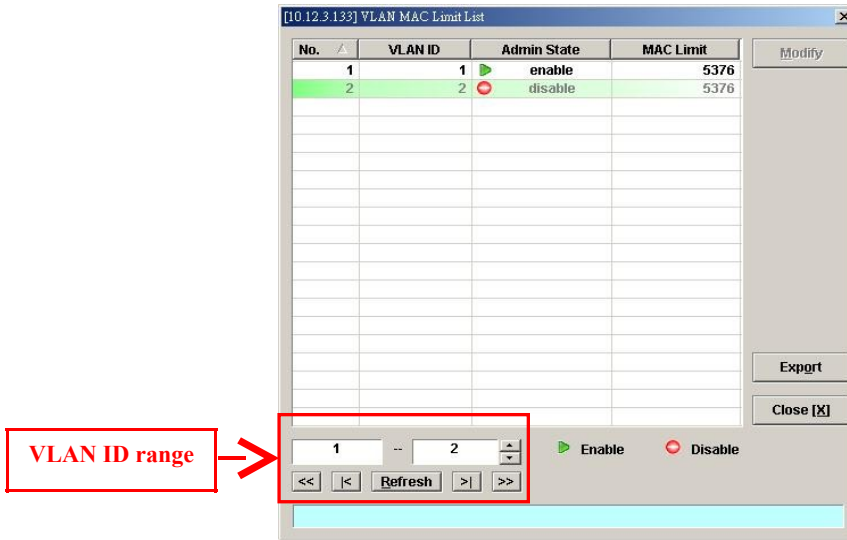


Table 7-71 VLAN MAC Limit List Dialog Description

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 7-104** shows **VLAN MAC Limit Configure Dialog**, and **Table 7-72** depicts the related parameters.

Figure 7-104 VLAN MAC Limit Configure Dialog

Table 7-72 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

Three 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 7-105 and Table 7-73 depicts the related parameters.

Figure 7-105 DHCP Setting Dialog



Table 7-73 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 7-106 and Table 7-74 depicts the related parameters.

Figure 7-106 DHCP Server List for DHCP Relay Dialog

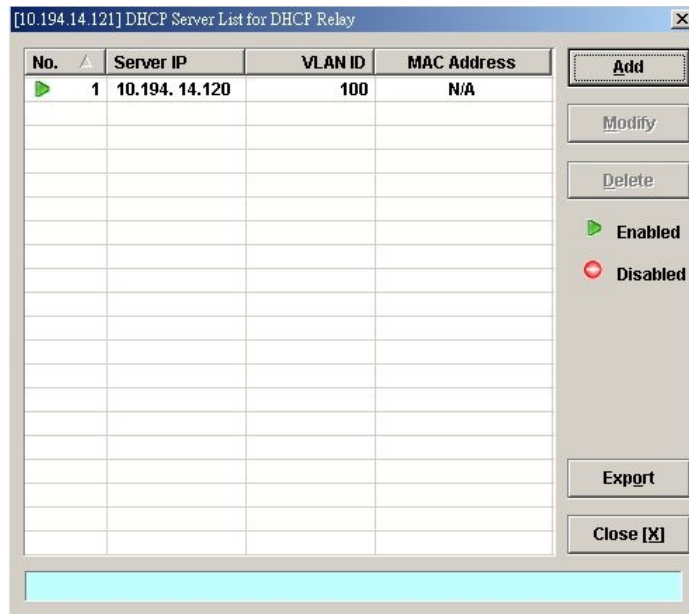


Table 7-74 DHCP Server List for DHCP Relay Dialog Description

Field	Description
Table List	
No.	This indicates the serial number of entry of the List.
Server IP	This specifies the DHCP server IP address. Hide: only have 4 relay server data for DHCP relay server table.
VLAN ID	This specifies the VLAN ID for this DHCP server.
MAC Address	This specifies the MAC address of DHCP server.
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.

Click Configuration → xDSL → DHCP → DHCP Broadcast Control on **Main Menu** to open the **DHCP Broadcast Control** Dialog as shown in Figure 7-107. Table 7-75 depicts the related parameters.

Figure 7-107 DHCP Broadcast Control Dialog

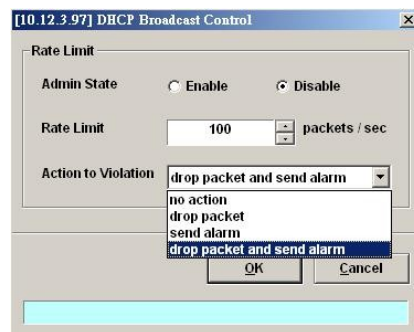


Table 7-75 DHCP Broadcast Control Dialog - Description

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 7-108 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 7-108 and Table 7-76 depicts the related parameters.

Figure 7-108 PPPoE Sub-option Setting Dialog

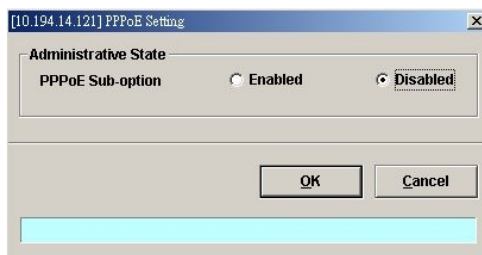


Table 7-76 PPPoE Sub-option Setting Dialog Description

Field	Description
Administrative State	
PPPoE Sub-option	Enable or disable the PPPoE sub-option function. 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 Default value is “Disable”.

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 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 7-109 and Table 7-77 depicts the related parameters.
- Step 2** Click and highlight a row and click ‘**Modify**’ button to modify the Agent Remote ID.

Figure 7-109 xDSL Port Agent ID List

No.	Slot-Port	Agent Circuit ID	Agent Remote ID
1	LC1-1	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/1:0.0	
2	LC1-2	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/2:0.0	
3	LC1-3	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/3:0.0	
4	LC1-4	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/4:0.0	
5	LC1-5	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/5:0.0	
6	LC1-6	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/6:0.0	
7	LC1-7	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/7:0.0	
8	LC1-8	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/8:0.0	
9	LC1-9	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/9:0.0	
10	LC1-10	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/10:0.0	
11	LC1-11	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/11:0.0	
12	LC1-12	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/12:0.0	
13	LC1-13	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/13:0.0	
14	LC1-14	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/14:0.0	
15	LC1-15	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/15:0.0	
16	LC1-16	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/16:0.0	
17	LC1-17	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/17:0.0	
18	LC1-18	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/18:0.0	
19	LC1-19	IP_DSLAM-100.168.3.97-00:00:00:00:00:00 atm 1/19:0.0	

Table 7-77 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.

This page is leave in blank for note or memo use

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 AMS LCT 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 8-110.

Note that the configuration tabs are not exact the same for the RFC2684 bridged mode and routed mode. Figure 8-110 ~ Figure 8-116 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 8-78.



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 8-110 ~ Figure 8-116 only show the ones in the bridged mode without any additional description. Otherwise, Figure 8-110 ~ Figure 8-116 show the configuration dialogs with description to indicate it. The rule of description also applies to Table 8-78.

Figure 8-110 xDSL Port & VC-to-VLAN Fast Provision – Port Setting Dialog

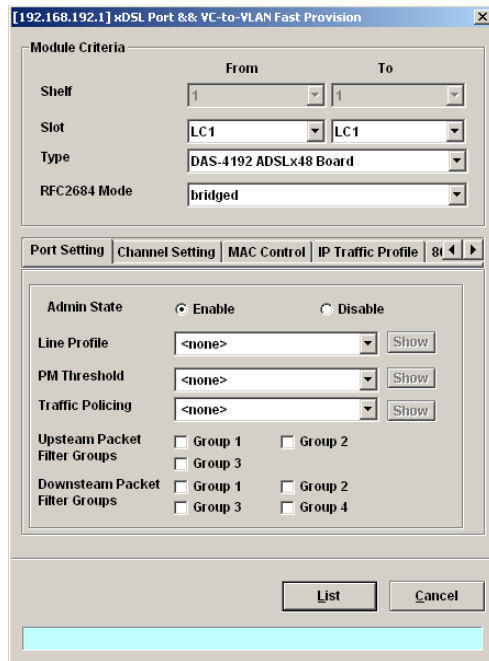


Figure 8-111 xDSL Port & VC-to-VLAN Fast Provision – Channel Setting Dialog

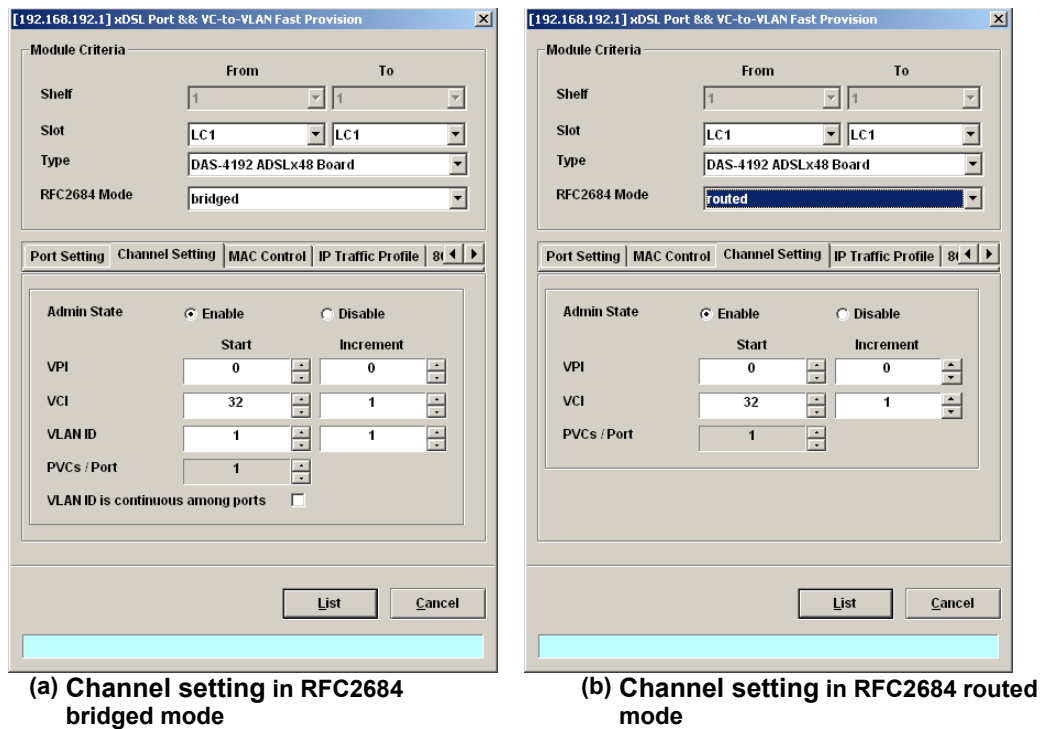
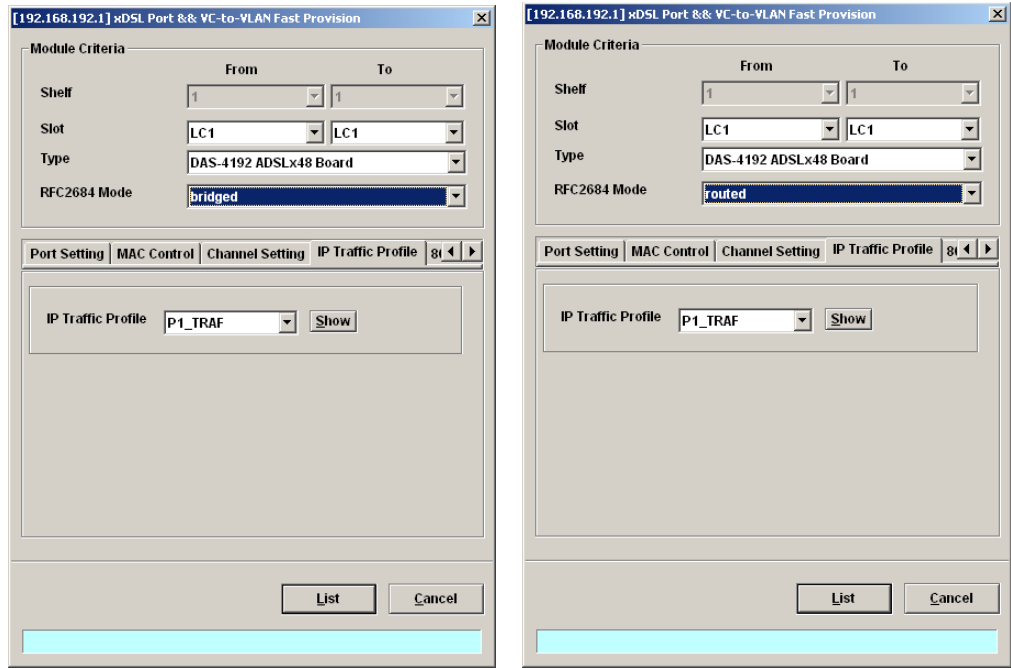


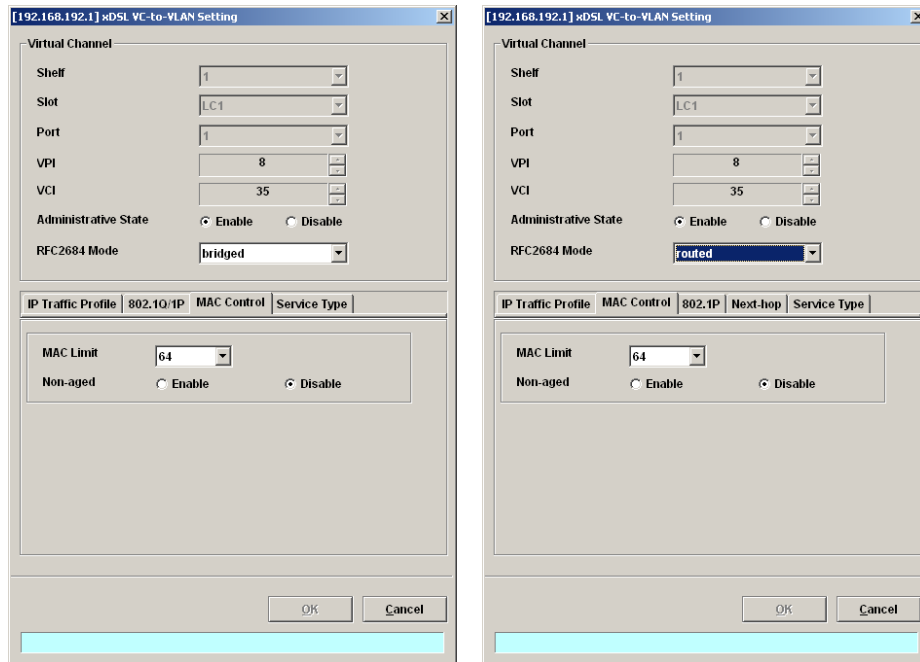
Figure 8-112 xDSL Port & VC-to-VLAN Fast Provision – IP Traffic Dialog



(a) IP traffic setting in RFC2684 bridged mode

(b) IP traffic setting in RFC2684 routed mode

Figure 8-113 xDSL Port & VC-to-VLAN Fast Provision – MAC Control Dialog



(a) MAC control setting in RFC2684 bridged mode

(b) MAC control setting in RFC2684 routed mode

Figure 8-114 xDSL Port & VC-to-VLAN Fast Provision – Next-hop Dialog (only for the RFC2684 routed mode)

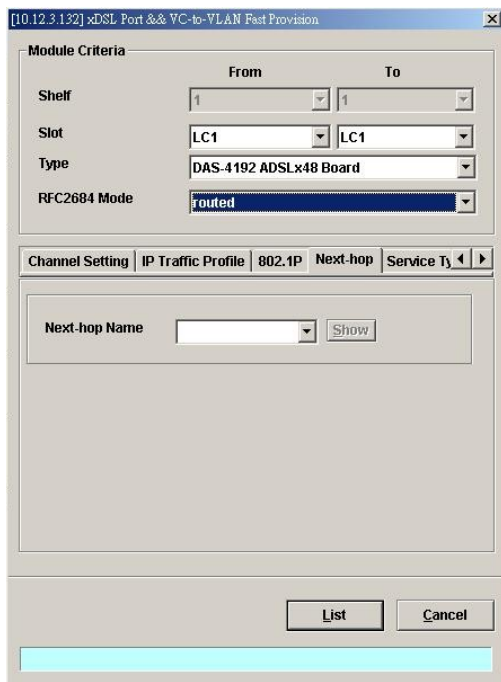
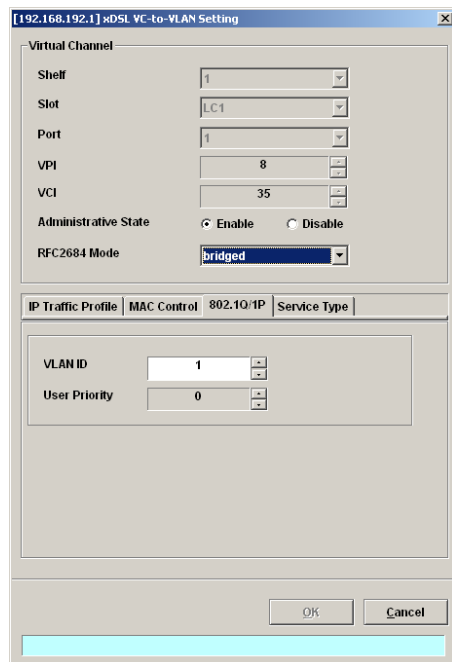
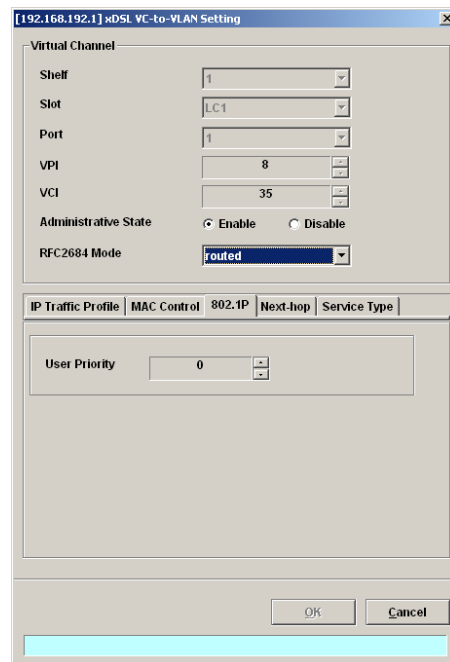


Figure 8-115 xDSL Port & VC-to-VLAN Fast Provision – 802.1P Dialog



(a) 802.1P setting in RFC2684 bridged mode



(b) 802.1P setting in RFC2684 routed mode

Figure 8-116 xDSL Port & VC-to-VLAN Fast Provision – Service Type Dialog

Module Criteria

	From	To
Shelf	1	1
Slot	LC1	LC1
Type	DAS-4192 ADSLx48 Board	
RFC2684 Mode	bridged	

Channel Setting | IP Traffic Profile | 802.1P | Service Type

Service Type: PPPoE

DHCP IP Limit: 1

Static IP's Base Address: 0 . 0 . 0 . 0

Static IP's Limit: 1

IP Address Increment / Port: 256

List Cancel

(a) PPPoE service in RFC2684 bridged mode

Module Criteria

	From	To
Shelf	1	1
Slot	LC1	LC1
Type	DAS-4192 ADSLx48 Board	
RFC2684 Mode	bridged	

Channel Setting | IP Traffic Profile | 802.1P | Service Type

Service Type: DHCP

DHCP IP Limit: 1

Static IP's Base Address: 0 . 0 . 0 . 0

Static IP's Limit: 1

IP Address Increment / Port: 256

List Cancel

(b) DHCP service in RFC2684 bridged mode

Module Criteria

	From	To
Shelf	1	1
Slot	LC1	LC1
Type	DAS-4192 ADSLx48 Board	
RFC2684 Mode	bridged	

Channel Setting | IP Traffic Profile | 802.1P | Service Type

Service Type: PPPoE+DHCP

DHCP IP Limit: 1

Static IP's Base Address: 11 . 21 . 33 . 0

Static IP's Limit: 1

IP Address Increment / Port: 256

List Cancel

(c) PPPoE + DHCP service in RFC2684 bridged mode

Module Criteria

	From	To
Shelf	1	1
Slot	LC1	LC1
Type	DAS-4192 ADSLx48 Board	
RFC2684 Mode	bridged	

Channel Setting | IP Traffic Profile | 802.1P | Service Type

Service Type: PPPoE+static IP

DHCP IP Limit: 1

Static IP's Base Address: 11 . 21 . 33 . 0

Static IP's Limit: 1

IP Address Increment / Port: 256

List Cancel

(d) PPPoE + Static IP service in RFC2684 bridged mode

(e) Static IP service in RFC2684 bridged mode

(f) Transparent service in RFC2684 bridged mode

Table 8-78 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 Control Dialog	
MAC Limit	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 ● PPPoE+DHCP ● PPPoE+Static IP ● Transparent
DHCP IP Limit	This indicates the number of IP to be allowed while DHCP or DHCP+PPPoE is selected
Client Limit [only for Transparent Service]	This attribute limits the number of Transparent client per PVC. It can not be bigger than MAC limit if service type is Transparent; otherwise it can not be bigger than 64.
Static IP's Basic Address	This specifies the base of the IP address if the service type is Static IP
Static IP's Limit [only for Static IP Service]	This specifies the base of the IP address and its range if the service type is Static IP or PPPoE+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.
- **In the case that the subscriber acquires his IP address dynamically via PPPoE+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 MAC addresses via PPPoE or IP/MAC addresses via DHCP. In other words, the NE drops the subscriber's traffic of invalid source MAC addresses or IP/MAC addresses.
- **In the case that the subscriber acquires his IP address dynamically via PPPoE+Static IP**
The NE will block the subscriber's traffic before a valid IP address assignment. Once the subscriber possesses a valid dynamic IP or source IP/MAC addresses, the NE will just forward the packet of valid source IP via Static IP or source IP/ MAC addresses via PPPoE. In other words, the NE drops the subscriber's traffic of invalid source IP or source IP/MAC addresses.



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

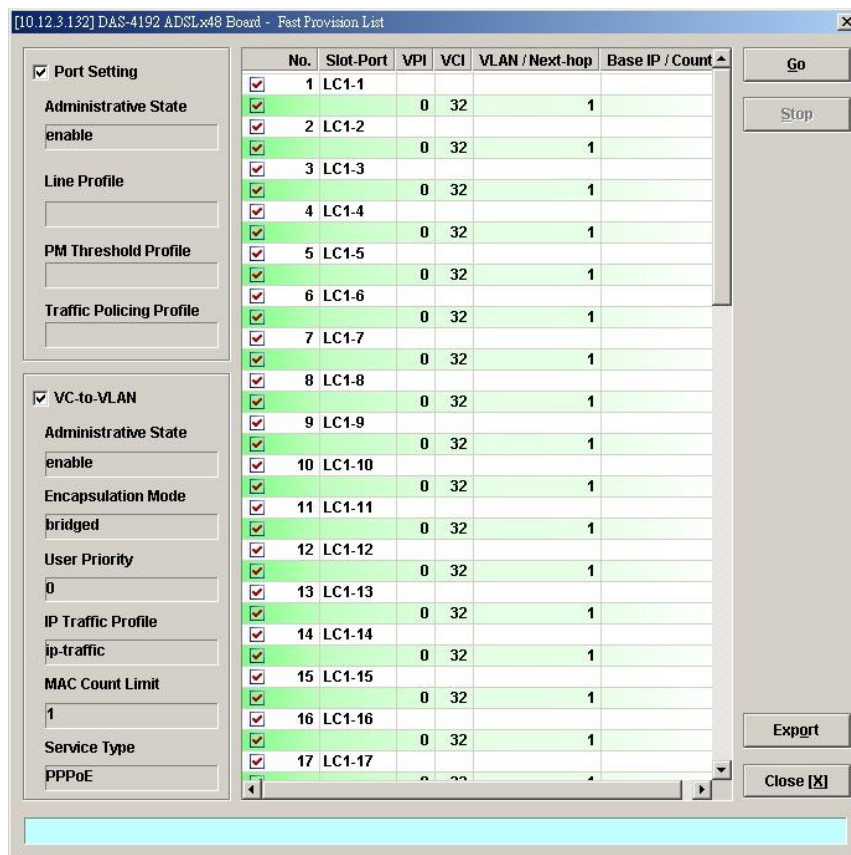
IP Address Increment/Port \geq Continuous IP Count

- Step 2** Click ‘List’ button to launch the **xDSL Fast Provision List** dialog. Figure 8-117 summarizes what you set via the **xDSL Port & VC-to-VLAN Fast Provision** dialog. As shown in Figure 8-117, 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.

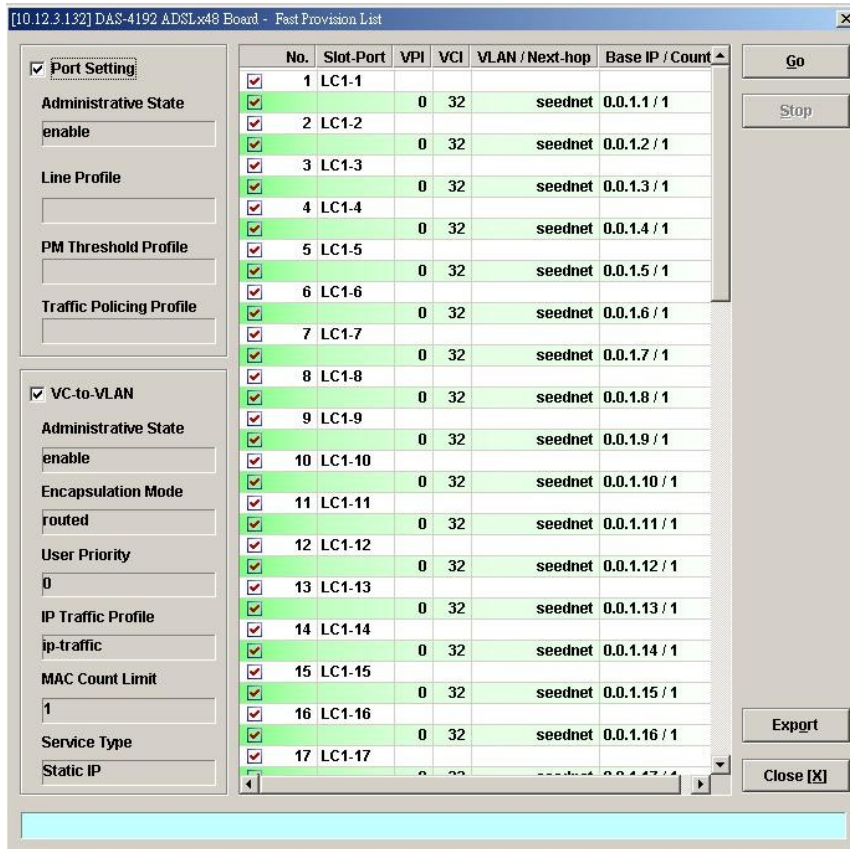
Table 8-79 depicts the related parameters.

- 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 8-117 xDSL Fast Provision List Dialog



(a) List Dialog in the RFC2684 bridged mode



(b) List Dialog in the RFC2684 routed mode

Table 8-79 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.

Table 8-79 xDSL Fast Provision List Dialog Description(Continued)

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 ● PPPoE+DHCP ● PPPoE+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 8-118 and Table 8-80 depicts the related parameters.

In Figure 8-118, it is noted that two individual tabs (Multicast Service Profile and Channel Limit) are provides to set the Multicast Service Fast Provision related parameters. Figure 8-118 ~ Figure 8-119 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 8-80.

Figure 8-118 xDSL Multicast Channel Fast Provision – Multicast Service Profile Dialog

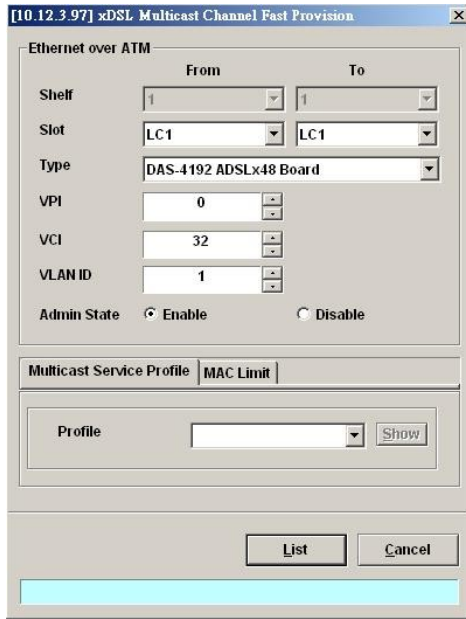


Figure 8-119 xDSL Multicast Channel Fast Provision – Channel Limit Dialog

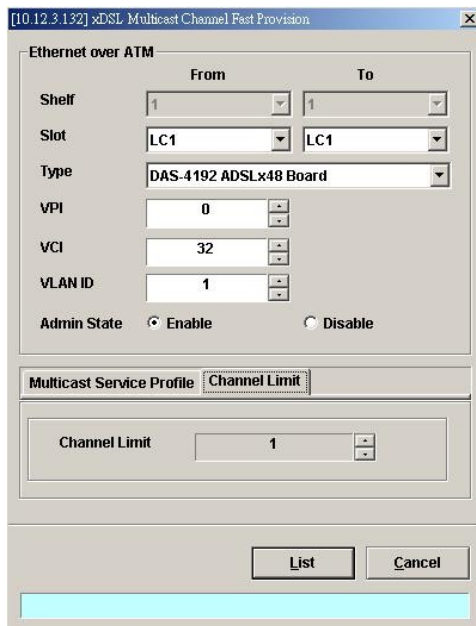


Table 8-80 xDSL Multicast Channel Fast Provision Description

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 8-120 summarizes what you set via the **xDSL Multicast Channel Fast Provision** dialog. As shown in Figure 8-120, 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 8-81 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 8-120 xDSL Multicast Channel Fast Provision List Dialog

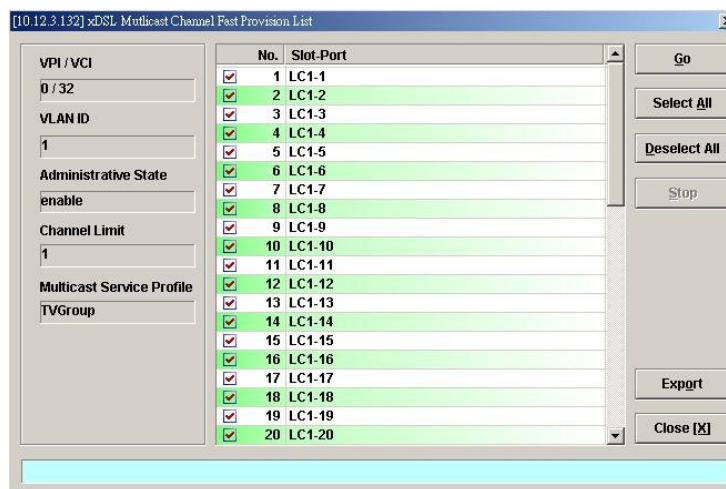


Table 8-81 xDSL Multicast Channel Fast Provision List Dialog Description

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 9-121.
- 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 9-122 shows the ADSL Current PM Dialog. The corresponding descriptions are depicted in Table 9-82. As to the SHDSL Current PM Dialog, it is shown in Figure 9-123. The corresponding descriptions are depicted in Table 9-83.

Figure 9-121 xDSL Current PM Port Selection

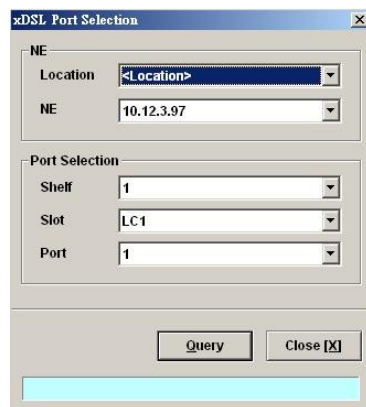


Figure 9-122 ADSL Current PM Dialog

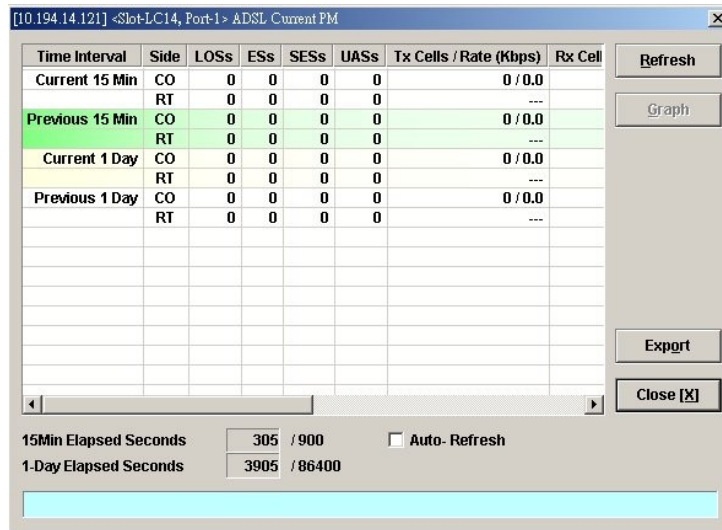


Table 9-82 ADSL Current PM Dialog Description

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.
CVs	This indicates the count of Code Violation during the current accumulated period.

Table 9-82 ADSL Current PM Dialog Description (Continued)

Field	Description
List Table	
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 9-123 SHDSL Current PM Dialog

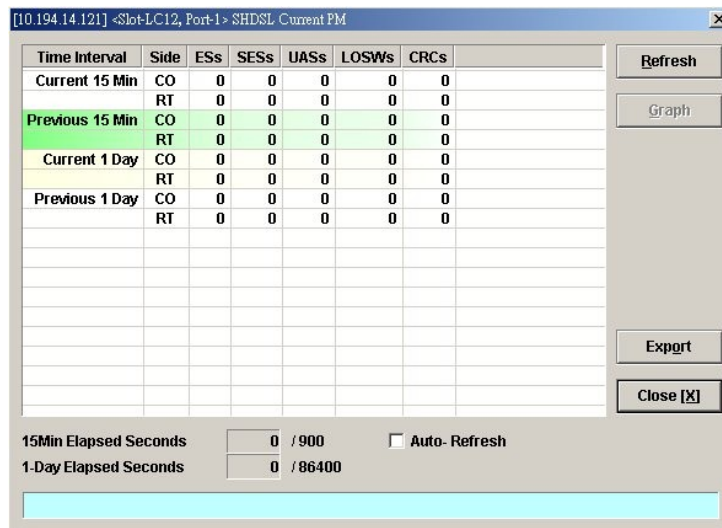


Table 9-83 SHDSL Current PM Dialog Description

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.
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.
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 9-124.
- 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 9-125 shows the ADSL History PM Dialog. The corresponding descriptions are depicted in Table 9-84. As to the SHDSL History PM Dialog, it is shown in Figure 9-126. The corresponding descriptions are depicted in Table 9-85.

Figure 9-124 xDSL History Port Selection Dialog

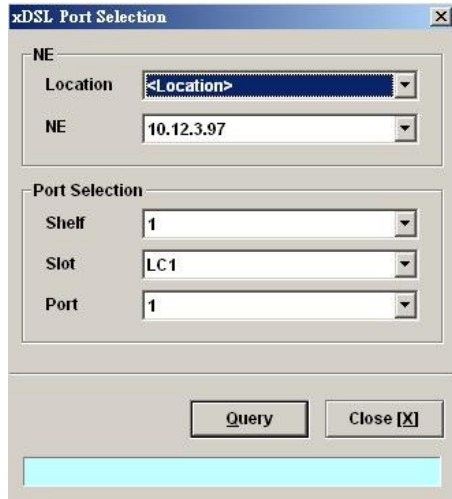


Figure 9-125 ADSL History PM Dialog

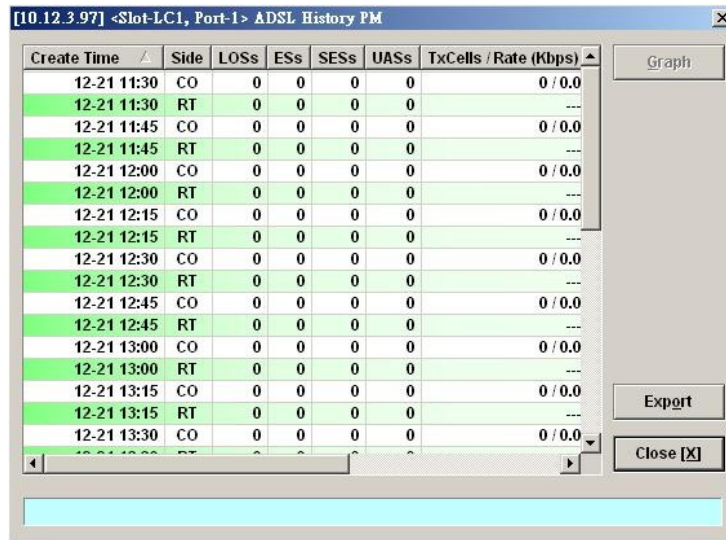


Table 9-84 ADSL History PM Dialog Description

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.
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.
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	This indicates the total number of failed full initializations during the indicated 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.
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 9-126 SHDSL History PM Dialog

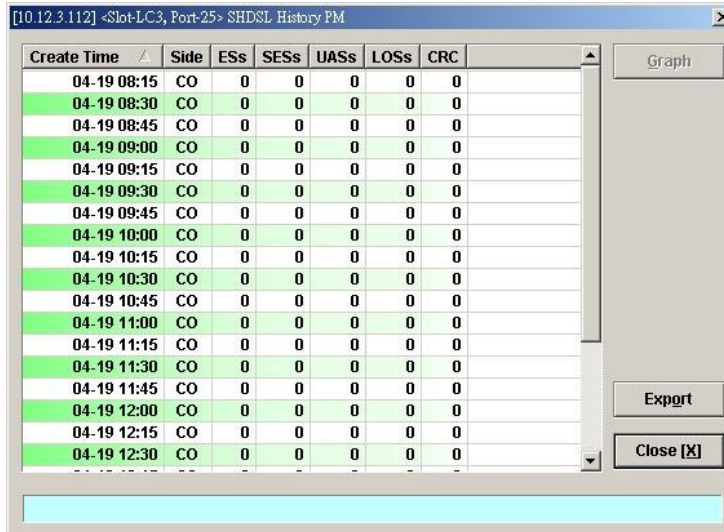


Table 9-85 SHDSL History PM Dialog Description

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 9-127. Table 9-86 depicts the related parameters.

Figure 9-127 Trunk PM Statistics Dialog

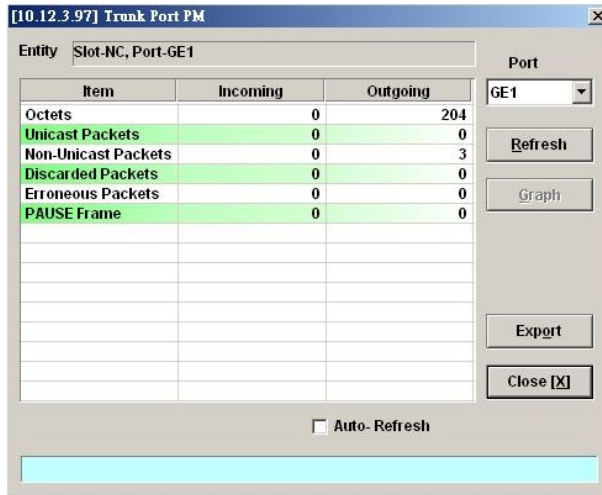


Table 9-86 Trunk PM Dialog Description

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 AMS LCT supports real time monitoring of the NE.

This chapter contains the following sections:

- NE Alarm Information
- System Alarm Management

NE Alarm Information

AMS LCT 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.

AMS LCT 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 10-128. Table 10-87 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 10-129 and Table 10-88 depicts the related parameters.

Figure 10-128 Active Alarm & Event List Dialog

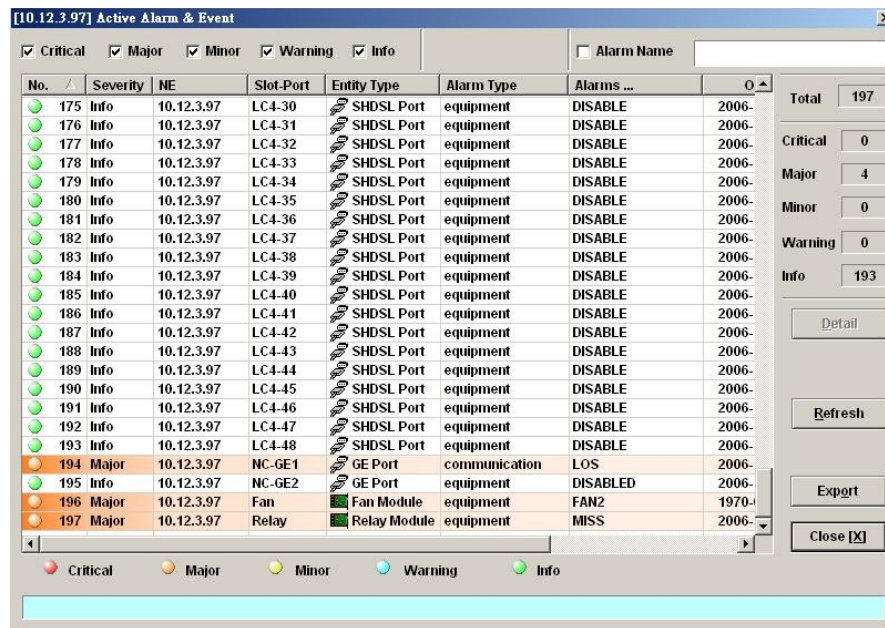



Table 10-87 Active Alarm & Event List Dialog Description

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 AMS LCT.
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 10-129 Detailed Alarm & Event Dialog

Alarm Information		
Location	<Location>	
NE	10.12.3.97	
Entity	Slot-NC, Port-GE1	
Online Model	DAS-4192 GE Port	
Planned Model	DAS-4192 GE Port	
Alarm Severity	Major	
Occur Time	2006-12-25 10:51:50	
Receive Time	2006-12-25 10:53:40	
Detailed Alarms		
No.	Alarm	Description
1	LOS	Loss of signal

Table 10-88 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

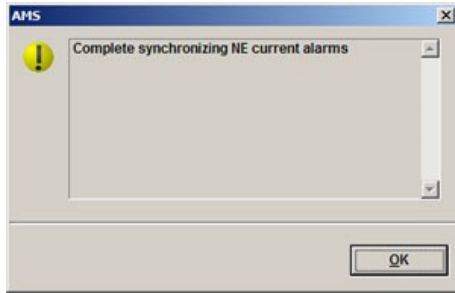
Alarm Synchronization

The AMS LCT provides automatic alarm synchronization. However, since the AMS LCT polls the NE periodically, the polling may not reflect the real-time status. To supplement this issue, the AMS LCT 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 10-130.

Figure 10-130 Completed Alarm Sync Dialog



Relay Input Alarm Management

The NE 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 10-131 . Table 10-89 depicts the related parameters.

Figure 10-131 Alarm Input List Dialog

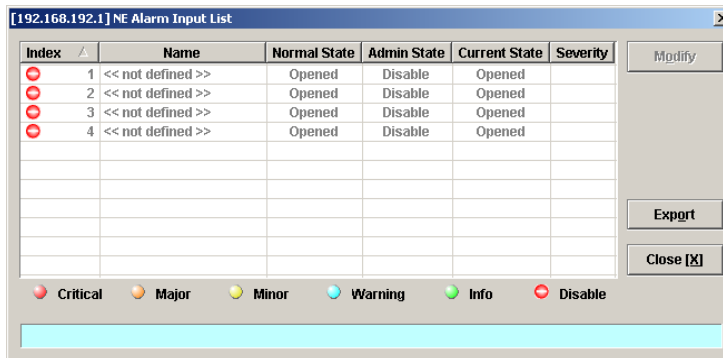


Table 10-89 Alarm Input List Dialog Description

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 10-132. Table 10-90 depicts the related parameters.

Figure 10-132 Alarm Input Modification Dialog

Table 10-90 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 10-133. Table 10-91 depicts the related parameters.

Figure 10-133 Alarm Output List Dialog

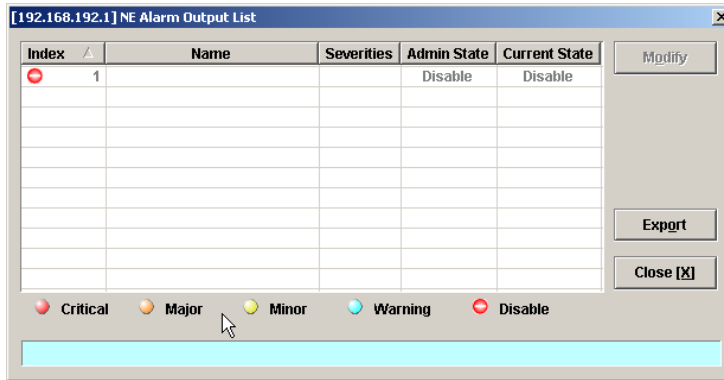


Table 10-91 Alarm Output List Dialog Description

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 10-134. Table 10-92 depicts the related parameters.

Figure 10-134 Alarm Output Modification Dialog

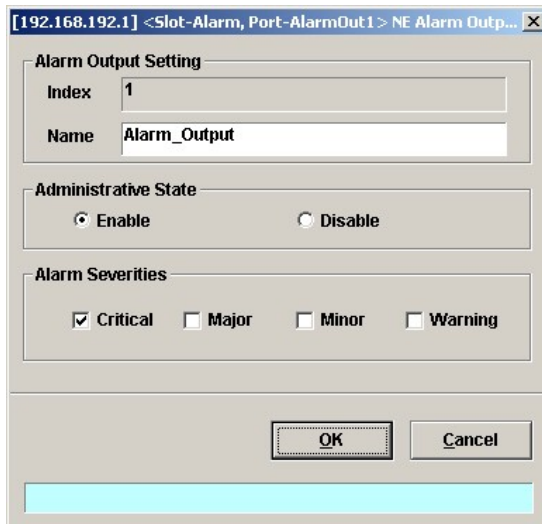


Table 10-92 Alarm Input Modification Dialog Description

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 10-135. Table 10-93 depicts the related parameters.
- Step 2** Select the row and click ‘**Modify**’ button to the system temperature threshold value as shown in Figure 10-136.

Figure 10-135 Hardware Monitoring List Dialog

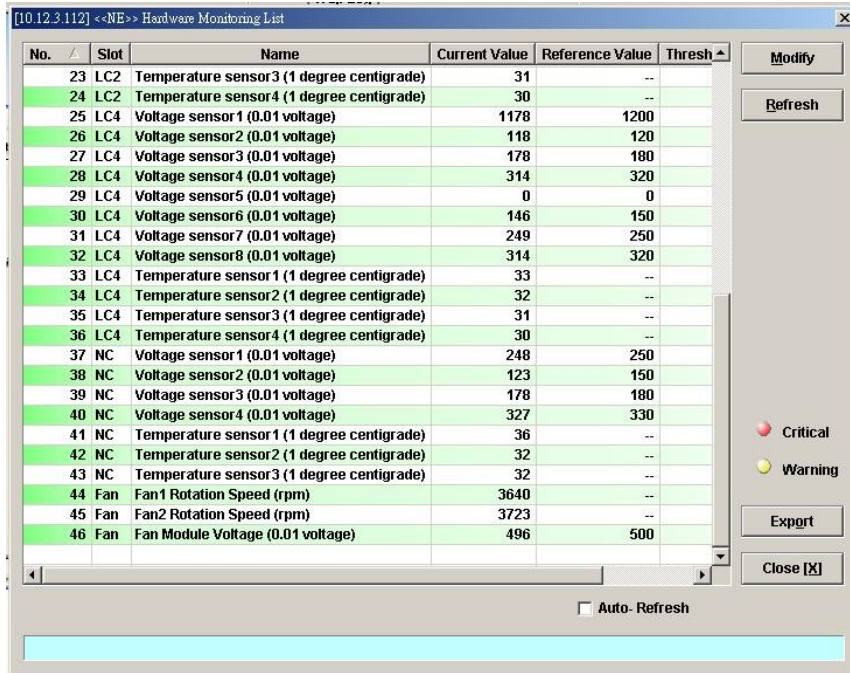
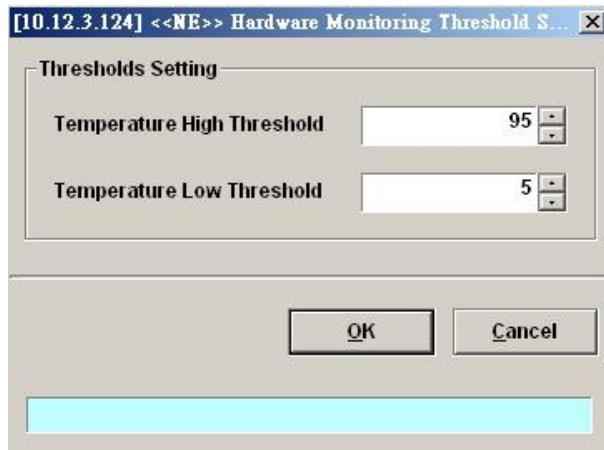


Table 10-93 Hardware Monitoring List Dialog Description

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 10-136.
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 10-136 Hardware Monitoring Threshold Setting Dialog



This page is leave in blank for note or memo use

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 Status 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 11-137**.
- 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 11-138. Table 11-94 depicts the related parameters.

Figure 11-137 xDSL Port Selection Dialog

The screenshot shows a dialog box titled "xDSL PortSelection". It contains the following fields and controls:

- NE Section:**
 - Location:** A dropdown menu with the text "<Location>" selected.
 - NE:** A text input field containing "10.12.3.112".
- Port Selection Section:**
 - Shelf:** A dropdown menu with "1" selected.
 - Slot:** A dropdown menu with "LC1" selected.
 - Port:** A dropdown menu with "1" selected.
- Buttons:** "Query" and "Close [X]" buttons are located at the bottom of the dialog.

Figure 11-138 ADSL Port Rate Status Dialog

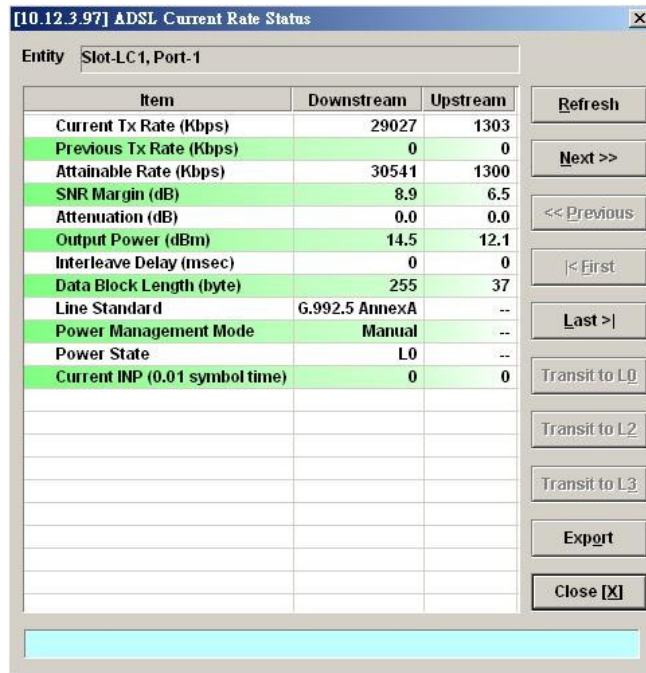


Table 11-94 ADSL Port Rate Status Dialog Description

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 11-137**.
- 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 11-139. Table 11-95 depicts the related parameters.

Figure 11-139 ADSL Bit Allocation Status Dialog

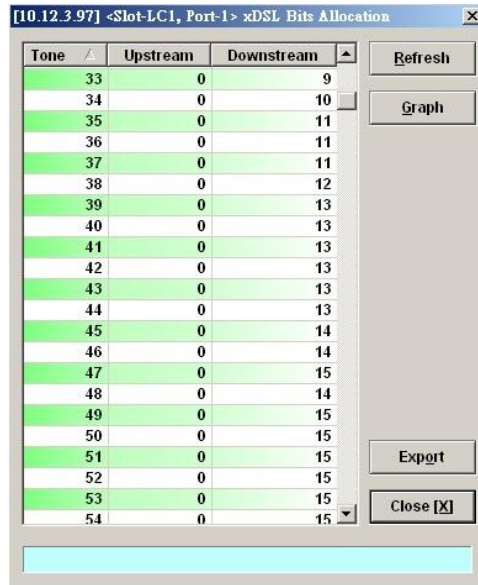
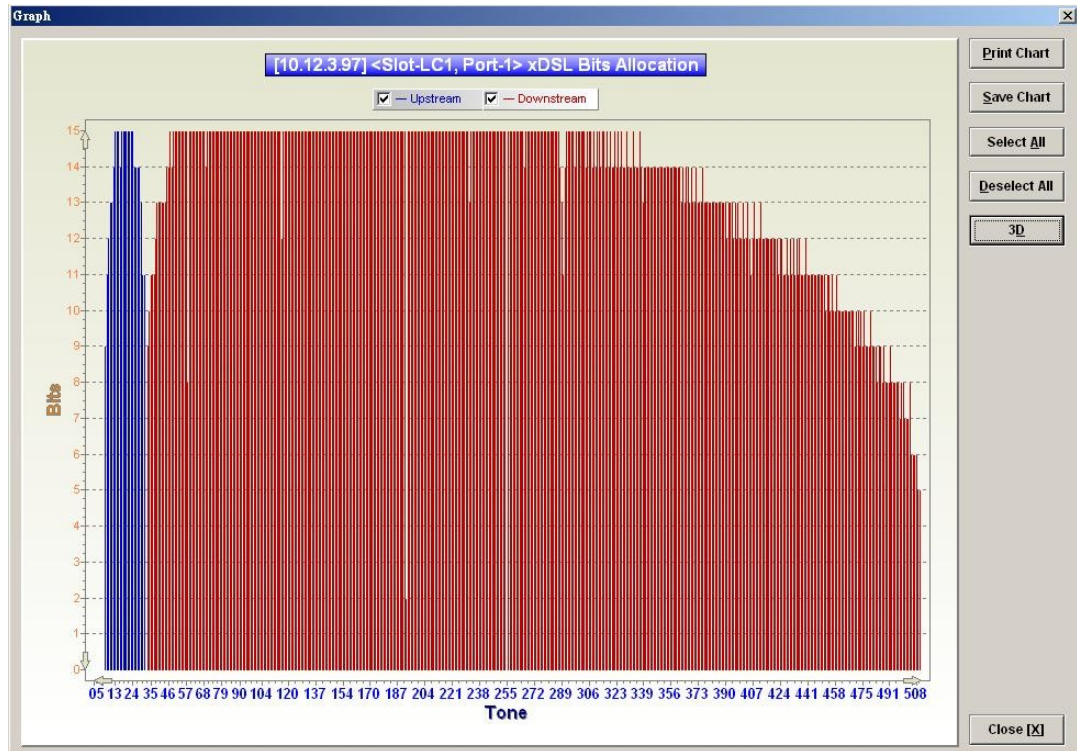


Table 11-95 ADSL Bit Allocation Status Dialog Description

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 11-140.

Figure 11-140 Graph of Bit Allocation



Loop Monitoring

The loop monitoring function provides the records of ADSL loop characteristics 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 11-137**.
- 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 11-141**. **Table 11-96** 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 11-142** or show the graph of Quiet Line PSD as shown in **Figure 11-143**



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 11-141 ADSL Loop Monitoring Dialog

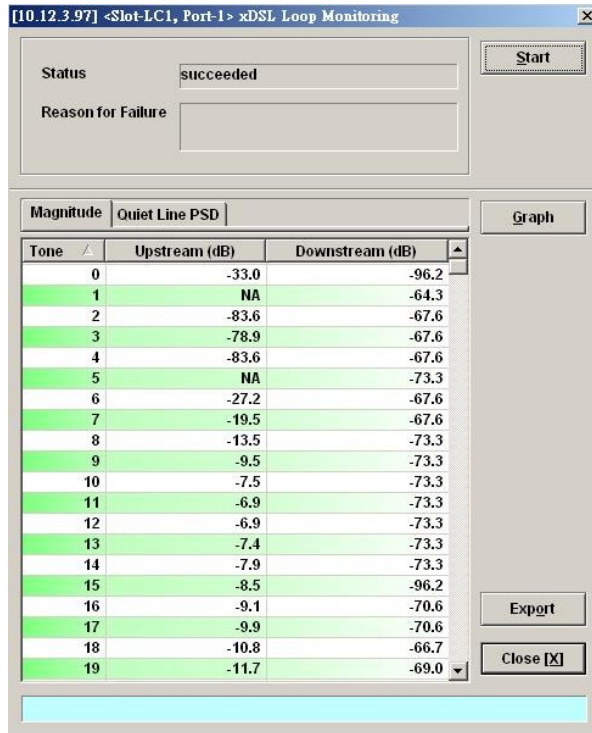


Table 11-96 ADSL Loop Monitoring Dialog Description

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 11-142 Graph of Loop Monitoring – Magnitude

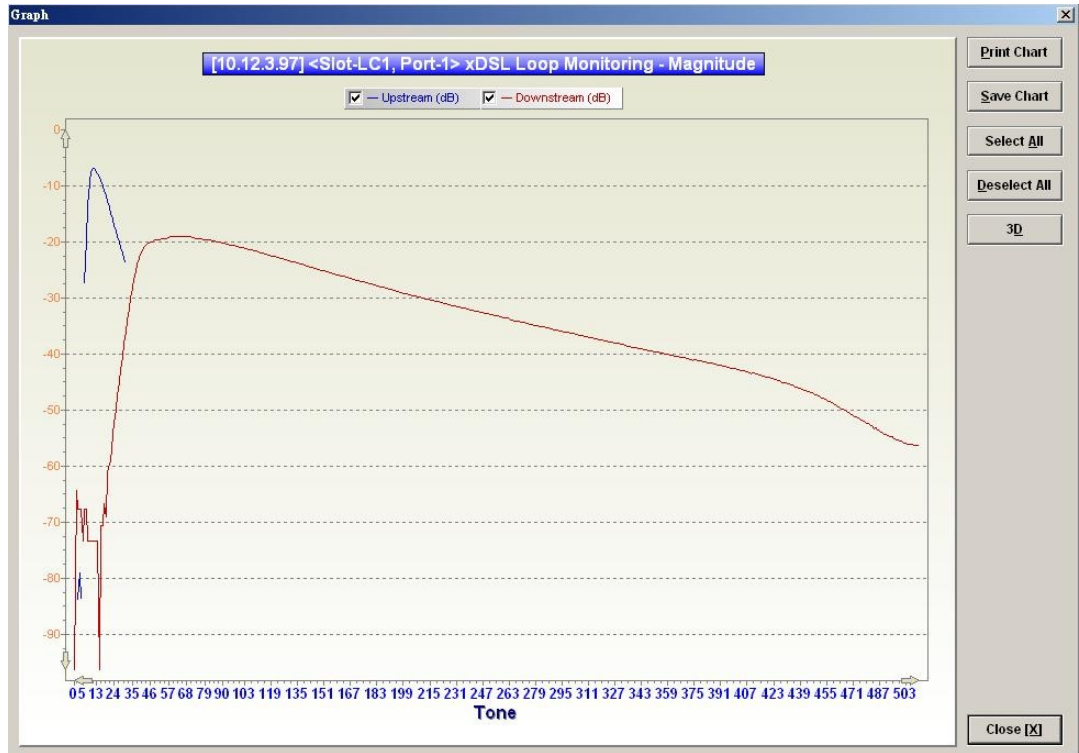


Figure 11-143 Graph of Loop Monitoring – Quiet Line Noise PSD



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

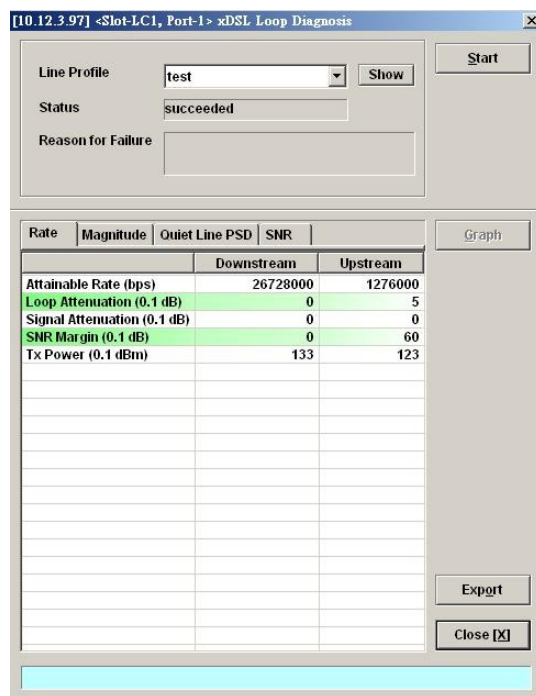
The DELT loop diagnosis function provides mechanism to measure the ADSL loop quality. This action will interrupt the ADSL connection. However, more detailed inform are gathered in comparison with the aforementioned loop monitoring function.

- Step 1** Click Diagnosis → xDSL Current Status → Bits Allocation on **Main Menu** to open the **xDSL Port Selection Dialog** as shown in **Figure 11-137**.
- 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 11-144. Table 11-97 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 11-145 or the graph of Quiet Line PSD as shown in Figure 11-146 or the graph of SNR as shown in Figure 11-147.



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

Figure 11-144 ADSL Loop Diagnosis Dialog



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 11-97 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 11-145 Graph of DELT result – Magnitude

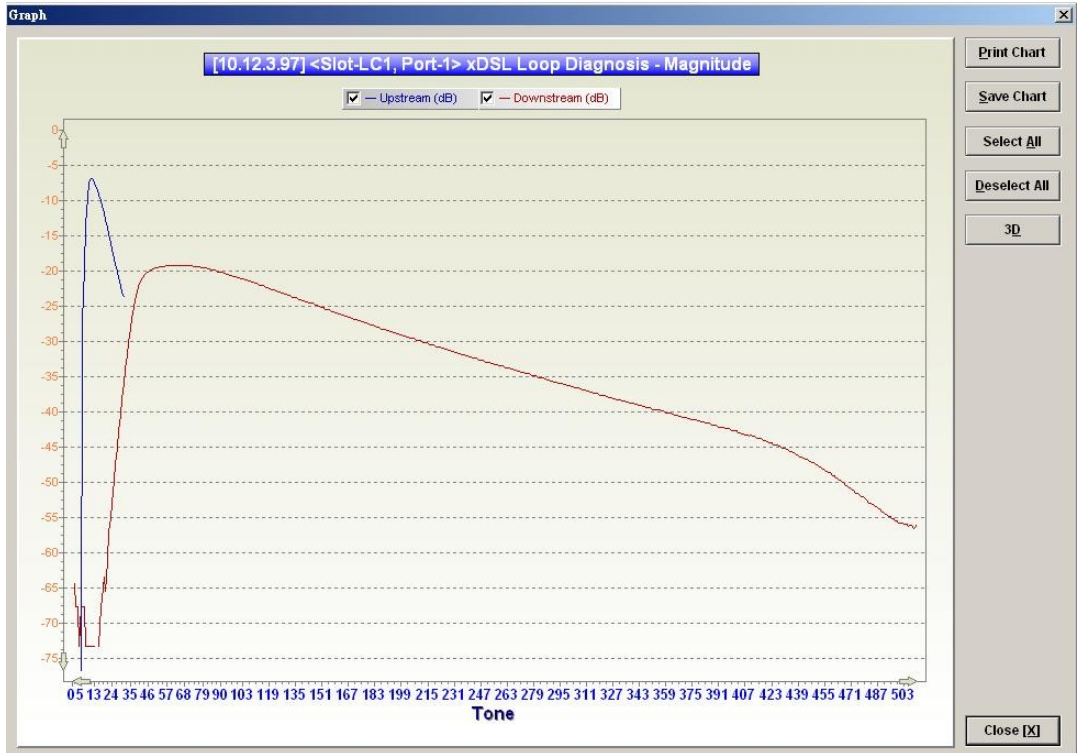


Figure 11-146 Graph of DELT result – Quiet Line PSD

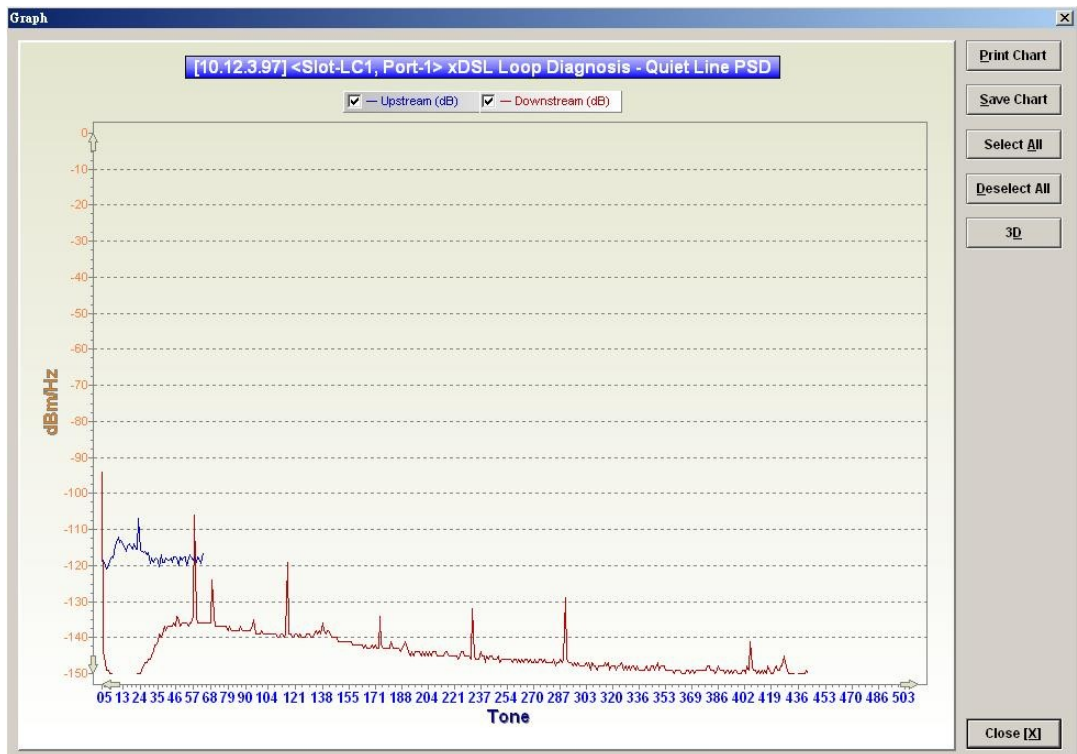
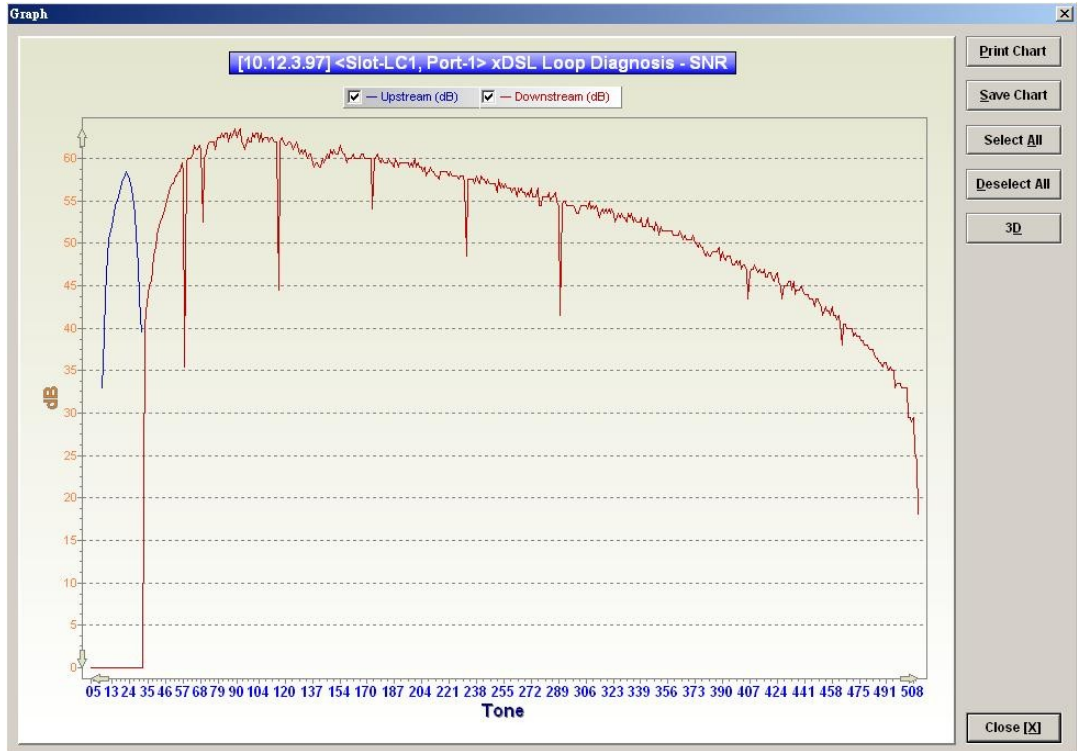


Figure 11-147 Graph of DELT result – SNR



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 11-137**.
- 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 11-148 and Table 11-98 depicts the related parameters.
- Step 3** Press Start button to get starting.

Figure 11-148 ADSL Loop SELT Test

Table 11-98 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 7-75.
- Step 2** Click on the 'VC OAM Test' button to to launch the **ATM Loopback OAM Cell Testing** as shown in and Table 11-99 depicts the related parameters.

Figure 11-149 TM Loopback OAM Cell Testing

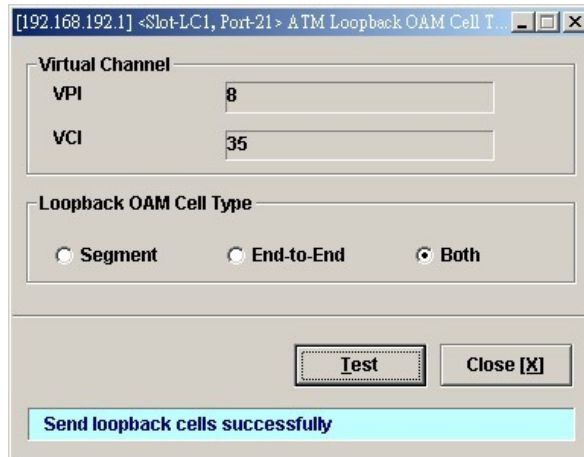


Table 11-99 ATM Loopback OAM Cell Testing

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 DAS4-Series 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.
- the MAC addresses learned from the GE1(uplink GE port) or GE2 port(uplink/subtending GE 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 11-100 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 11-101 shows the conditions the NE will not learn the source MAC of upstream traffic.

Table 11-100 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 11-101 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 11-102~Table 11-104 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
- c-u: Clear the uge spoofed table

Table 11-102 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 11-103 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	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 11-104 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	Manual addition		
	a static MAC	a MAC ACL Permit MAC	a MAC ACL Deny MAC
S	S X	S X	S X
AP	AP X	AP X	AP X
AD	AD X	AD X	AD X
LR	LR X	LR X	LR X
LU	LU #+0	LU &+0	LU #+0
LUN	LUN #+0	LUN &+0	LUN #+0
LSA	LSA X	LSA X	LSA X
LSI	LSI X	LSI X	LSI X

Table 11-105 The expected spoofed status between the xDSL line port and uplink (uge1) port

The reason to add a MAC entry	Manual addition			Dynamically learning on the line port of		
	a static MAC	a MAC ACL Permit MAC	a MAC ACL Deny MAC	LR	LU	LUN
Status of matched uplink (uge1) port						
LU	S LU	AP LU	AD LU	NA	LU c-u	LUN c-u
LSA	X LSA	X LSA	AD LSA	NA	LSI LSA	LSI LSA

The reason to add a MAC entry	Dynamically learning on the uplink (uge1) port of	
	LU	
Status of matched xDSL line port		
S	S	LSA
AP	AP	LSA
AD	AD	LU
LR	LR	X
LU	LSA	LSA
LUN	LUN	LSA
LSA	LSA	LSA
LSI	LSI	LSA

Table 11-106 The expected spoofed status between the xDSL line port and subbanding (uge2)port

The reason to add a MAC entry	Manual addition			Dynamically learning on the line port of		
	a static MAC	a MAC ACL Permit MAC	a MAC ACL Deny MAC	LR	LU	LUN
Status of matched subbanding (uge2) port						
LU	S LU	AP LU	AD LU	NA	LU c-u	LUN c-u
LSA	X LSA	X LSA	AD LSA	NA	LSI LSA	LSI LSA

The reason to add a MAC entry	Dynamically learning on the subtending (uge2) port of	
Status of matched xDSL line port	LU	
S	S	LSA
AP	AP	LSA
AD	AD	LU
LR	LR	X
LU	LSA	LSA
LUN	LUN	LSA
LSA	LSA	LSA
LSI	LSI	LSA

Table 11-107 The expected spoofed status between uplink(uge1) port and subtending(uge2)port

The reason to add a MAC entry	Dynamically learning on uplink (uge1) port of	
Status of matched subtending (uge2) port	LU	
LU	c-u	LU
LSA	LSA	LSA

The reason to add a MAC entry	Dynamically learning on subtending (uge2) port of	
Status of matched uplink (uge1) port	LU	
LU	c-u	LU
LSA	LSA	LSA

Table 11-108 The expected spoofed status between uplink(uge1) port and uplink (uge2)port

The reason to add a MAC entry	Dynamically learning on uplink (uge1) port of	
Status of matched uplink (uge2) port	LU	
LU	c-u	LU
LSA	LSA	LSA

The reason to add a MAC entry	Dynamically learning on uplink (uge2) port of	
Status of matched uplink (uge1) port	LU	
LU	c-u	LU
LSA	LSA	LSA

Click Diagnosis → xDSL Current Status → Bridge Filtering Database on **Main Menu** to open the **Filtering Database Entry List** Dialog as shown in Figure 11-150. Table 11-109 depicts the related parameters.

Figure 11-150 Bridge Filtering Database Entry List Dialog

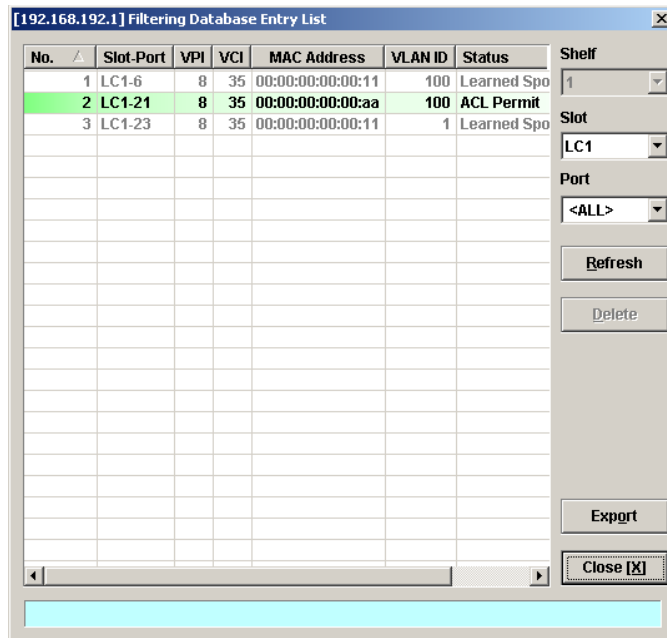


Table 11-109 Bridge Filtering Database Entry List Dialog Description

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 11-151. Table 11-110 depicts the related parameters.

Figure 11-151 VLAN Membership List Dialog

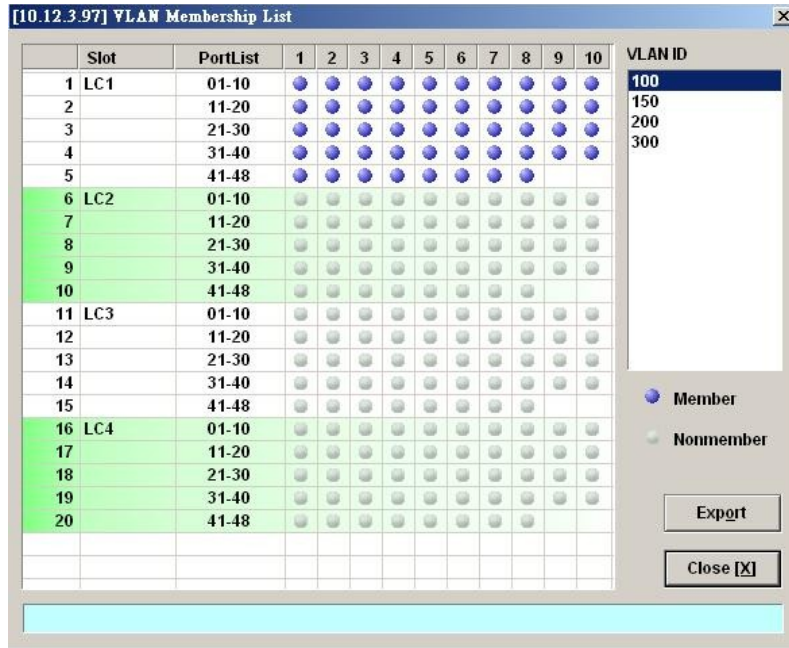


Table 11-110 VLAN Membership List Dialog Description

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 11-152. Table 11-111 depicts the related parameters.

Figure 11-152 MAC Spoofing Status List Dialog

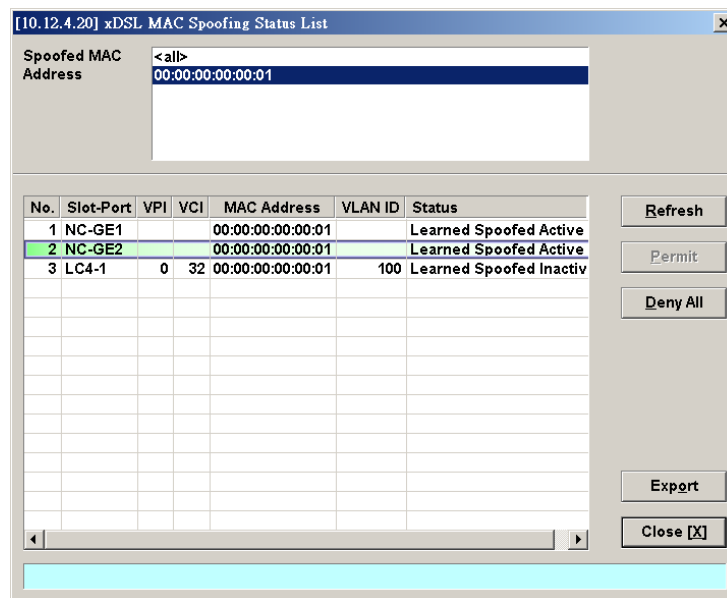


Table 11-111 MAC Spoofing Status List Dialog Description

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	This indicates the current status of the recorded MAC address. The definition of possible statuses is as follows. <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 11-153. Refer the related information to the section “Multicast Service Profile” in 5.

Click Diagnosis → xDSL Current Status → Multicast Channel Status on **Main Menu** to open the **Multicast Channel Status List** Dialog as shown in Figure 11-153. Table 11-112 depicts the related parameters.

Figure 11-153 Multicast Channel Status List Dialog

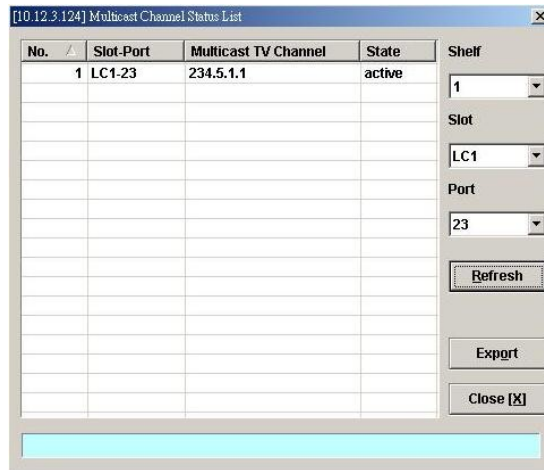


Table 11-112 Multicast Channel Status List Dialog Description

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	This indicates the current status of the multicast channel group. The definition of possible statuses is as follows. <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 11-154. Table 11-113 depicts the related parameters.

Figure 11-154 Multicast Group Membership List Dialog

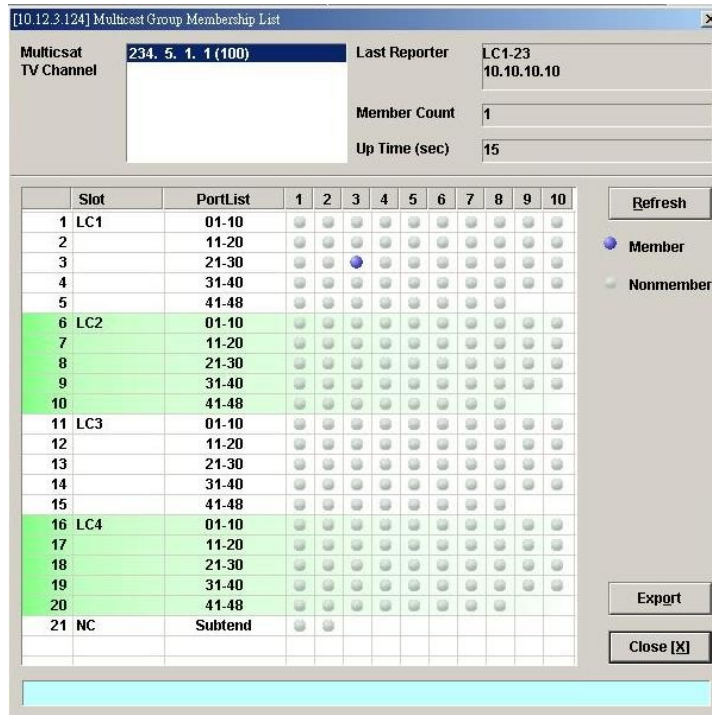


Table 11-113 Multicast Group Membership List Dialog Description

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	This indicates the port list number. The blue point means that the specified port is a member of the specified multicast channel. Note: In the case that the RSTP is disabled, "Subtend" indicates the port GE2. Note: In the case that the RSTP is enabled, "Subtend" indicates the "designated port" (either port GE1 or port GE2).
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 11-155 and Table 11-114 depicts the related parameters.

Figure 11-155 xDSL Forwarding Broadcast VLANs List

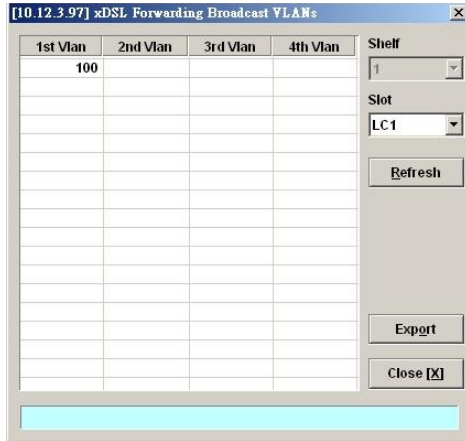


Table 11-114 xDSL Forwarding Broadcast VLANs List Description

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 11-156. Table 11-115 depicts the related parameters.

Figure 11-156 DHCP Session Information List Dialog

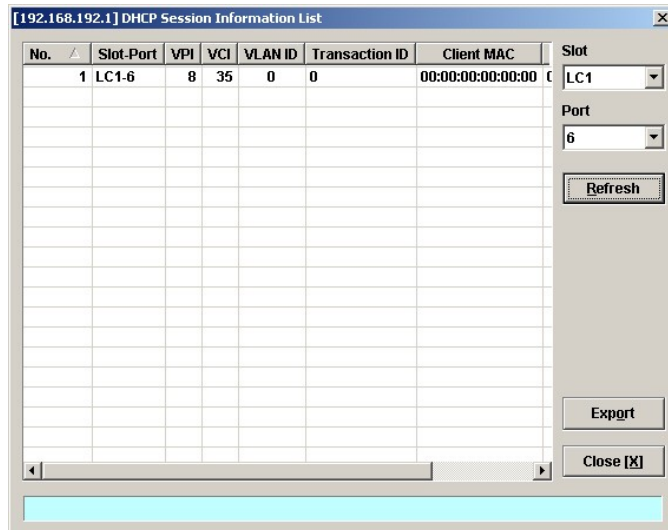


Table 11-115 DHCP Session Information List Dialog Description

Field	Description
List Table	
No.	This indicates the index of DHCP session information.
Slot-Port	This indicates the location of xDSL slot-port.
VPI	This indicates the VPI value of the PVC where the DHCP transaction resides.
VCI	This indicates the VCI value of the PVC where the DHCP transaction resides.
VLAN ID	This indicates the VLAN ID associated with the PVC specified by (VPI, VCI).
Transaction ID	This indicates the DHCP transaction ID.
Client MAC	This indicates the MAC address of client.
Assigned IP	This indicates the IP address assigned to this client.
Status	This indicates the DHCP transaction state <ul style="list-style-type: none"> • Init (1) • Select (2) • Bound (3) • Renew (4) • Unknown (5)
Function Button	
Refresh	Click this button to refresh the information list
Export	Click this button to save the contents of DHCP Session Information List to the Personal Computer.
Close	Exit the DHCP Session Information List Dialog.

PPPOE Session Information

The PPPOE session information list displays the PPPOE session information on the xDSL ports.

Click Diagnosis → xDSL Current Status → PPPOE Session Information on **Main Menu** to open the **PPPOE Session Information** Dialog as shown in Figure 11-157. Table 11-116 depicts the

related parameters.

Figure 11-157 PPPOE Session Information List Dialog

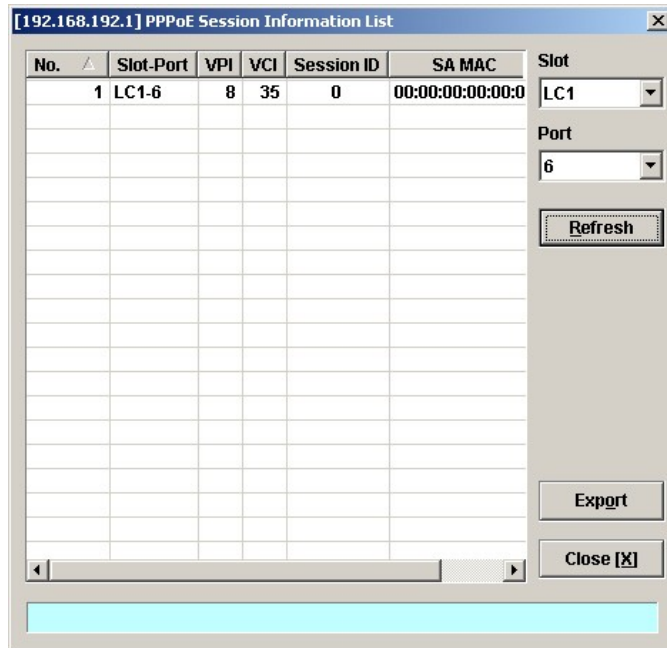


Table 11-116 PPPOE Session Information List Dialog Description

Field	Description
List Table	
No.	This indicates the indx of DHCP session information.
Slot-Port	This indicates the location of xDSL slot-port.
VPI	This indicates the VPI value of the PVC where the PPPOE session resides.
VCI	This indicates the VCI value of the PVC where the PPPOE session resides.
Session ID	This indicates the PPPOE session ID.
SA MAC	This indicates the source MAC address of client.
Status	This indicates the PPPOE session state <ul style="list-style-type: none"> • Idle (1) • Init (2) • Session (3) • Poll (4)
Function Button	
Refresh	Click this button to refresh the information list
Export	Click this button to save the contents of PPPOE Session Information List to the Personal Computer.
Close	Exit the PPPOE Session Information List Dialog.

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 11-158 shows **Current Status of Link Aggregation Dialog**, and Table 11-117 depicts the related parameters.

Figure 11-158 Current Status of Link Aggregation Dialog

The screenshot shows a dialog box titled "[10.12.3.107] Current Status of Link Aggregation". At the top, there is a section for "Link Aggregation Type" with a sub-section "Administrative State" containing a text box with the value "disabled" and a "Refresh" button to its right. Below this is a tabbed interface with two tabs: "Port GE1" and "Port GE2". The main area contains a table with two columns: "Item" and "Current Status". The table lists the following items: 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, and Partner Operation State. The rows for Actor System Priority, Actor Key, Actor Port ID, Partner System Priority, Partner Key, and Partner Port ID are highlighted in green. To the right of the table are buttons for "Export" and "Close [X]". At the bottom of the dialog, there is a legend for "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. Below the legend is an empty light blue text box.

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	

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 11-117 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 11-159. Table 11-118 depicts the related parameters.

Figure 11-159 Current Status of Rapid Spanning Tree Protocol – Bridge Dialog

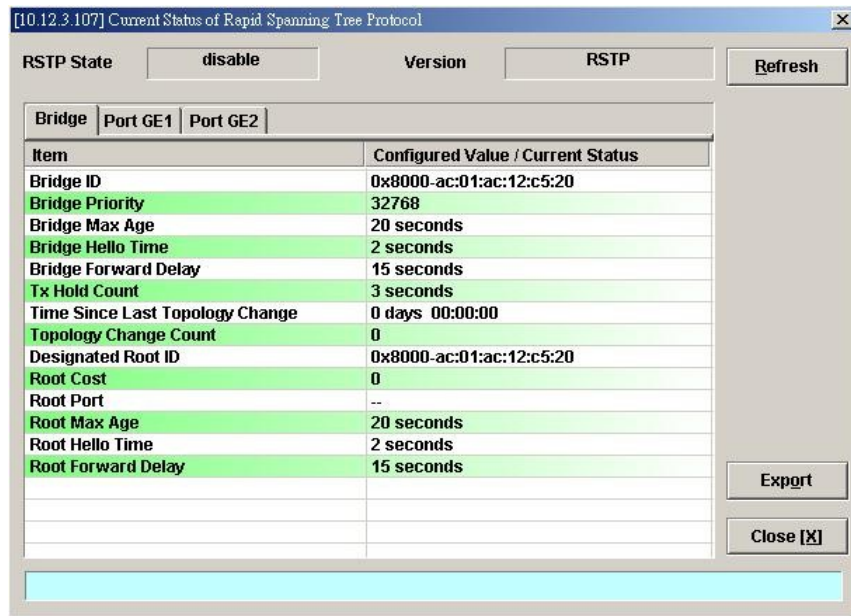


Table 11-118 Current Status of Rapid Spanning Tree Protocol – Bridge Dialog Description

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 11-160. Table 11-119 depicts the related parameters.

Figure 11-160 Current Status of Rapid Spanning Tree Protocol –Port GE1/Port GE2 Dialog

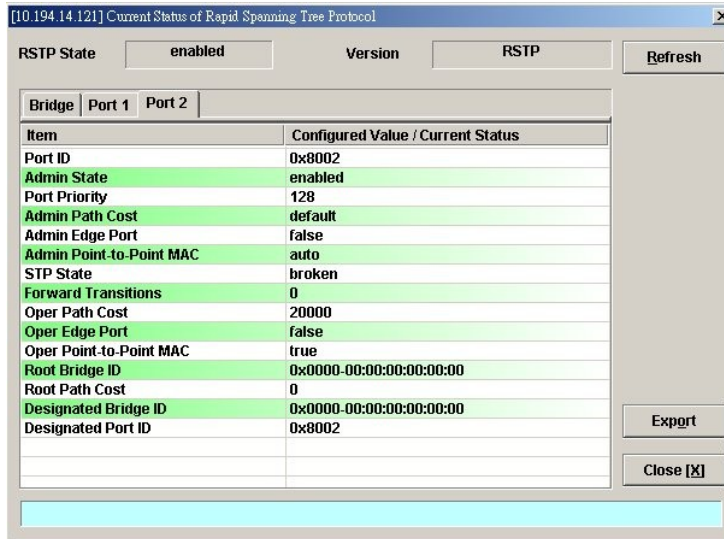


Table 11-119 Current Status of Rapid Spanning Tree Protocol –Port GE1/Port GE2 Dialog Description

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"> ture: It indicates that this port should always be treated as if it is connected to a point-to-point link. false: 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 11-161.

Table 11-120 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 11-120 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 AMS LCT supports the following three network related diagnosis functions to check the connection between the AMS LCT and NE.

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

Ping NE

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

Click Diagnosis → NE Connection → Ping NE on **Main Menu** to open the **Ping NE** Dialog as shown in Figure 11-163 and Table 11-121 depicts the related parameters.

Figure 11-163 Ping NE from Client Dialog

Table 11-121 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 AMS LCT host.

Click Diagnosis → NE Connection → Traceroute on **Main Menu** to open the **Traceroute NE** Dialog as shown in Figure 11-164. Table 11-122 depicts the related parameters.

Figure 11-164 Tracer Route NE from Client Dialog

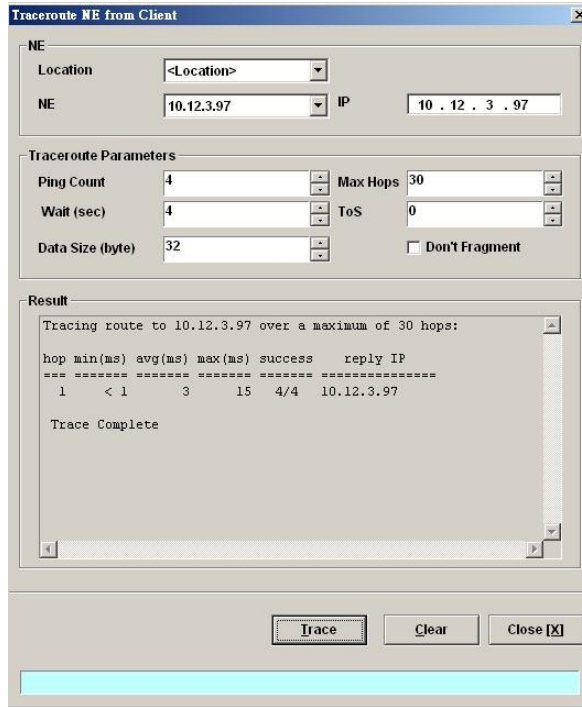


Table 11-122 Trace Route NE from Client Dialog Description

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 AMS LCT 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 11-165.



If the IP address of NE 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.

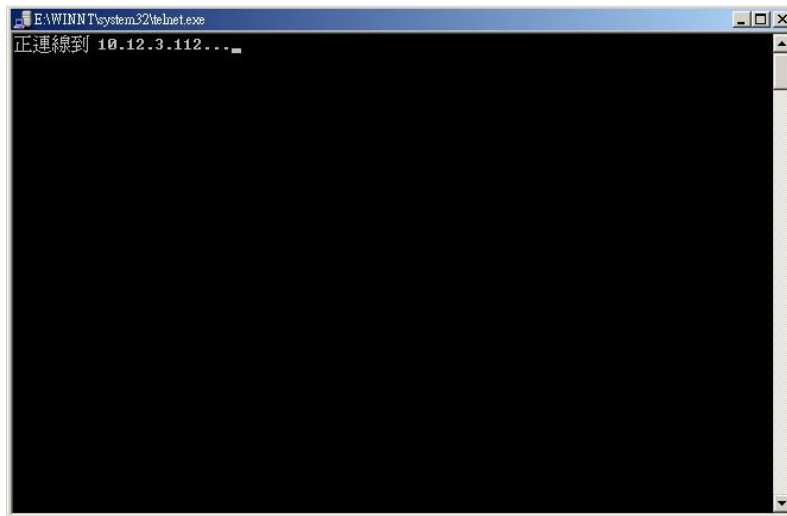


The IP address assigned must be unique in use with the device on the network segment.



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 4 for detail information.

Figure 11-165 Telnet Pop-up Window

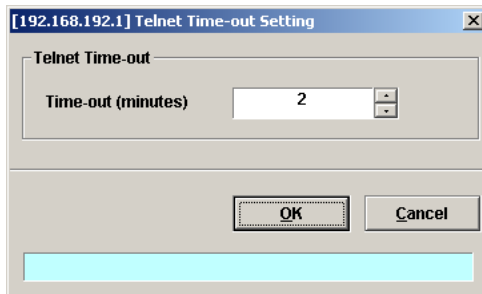


Telnet Timeout

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

Click Configuration → NE Management → NE Connection → CLI Setting → **Telnet Time-out** on **Main Menu** to open the **Telnet Time-out Setting** Dialog as shown in Figure 11-166.

Figure 11-166 Telnet Time-out Setting Dialog



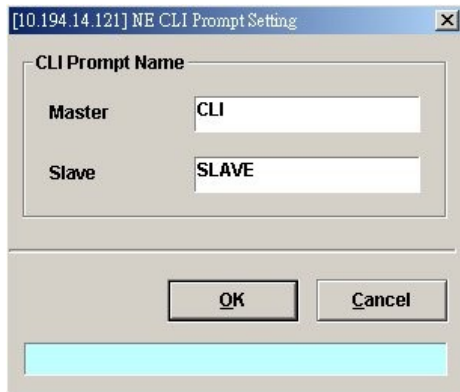
The range of telnet timeout is from 2 minutes to 1440 minutes. The default value is 2 minutes.

CLI Prompt Setting

Use the ‘CLI prompt setting’ to set the CLI prompt of the system.

Click Configuration → NE Management → NE Connection → CLI Setting → **CLI Prompt Setting** on **Main Menu** to open the **Telnet Time-out Setting** Dialog as shown in Figure 11-166.

Figure 11-167 CLI Prompt Setting Dialog



Check SNMP Connection

Use the ‘SNMP Connection’ to check whether the connection between NE and AMS LCT host is normal or not.

Click Diagnosis → NE Connection → SNMP Connection on **Main Menu** to open the **SNMP Connection** Dialog as shown in Figure 11-168 and Table 11-123 depicts the related parameters.

Figure 11-168 Check NE SNMP Connection Dialog

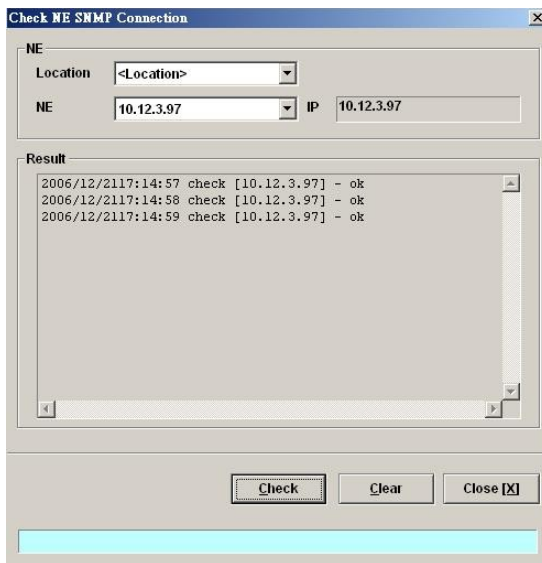


Table 11-123 Check NE SNMP Connection Dialog Description

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.

This page is leave in blank for note or memo use

Chapter 12 General System Management

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

- AMS LCT Options

AMS LCT Options

Configuring the Alarm Warning Options

The AMS LCT supports to notify the operators whenever there is an alarm sent from the NE. The operator is allowed to control the AMS LCT 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 12-169. Table 12-124 depicts the related parameters.

Figure 12-169 Client Options Dialog – Alarm Warning

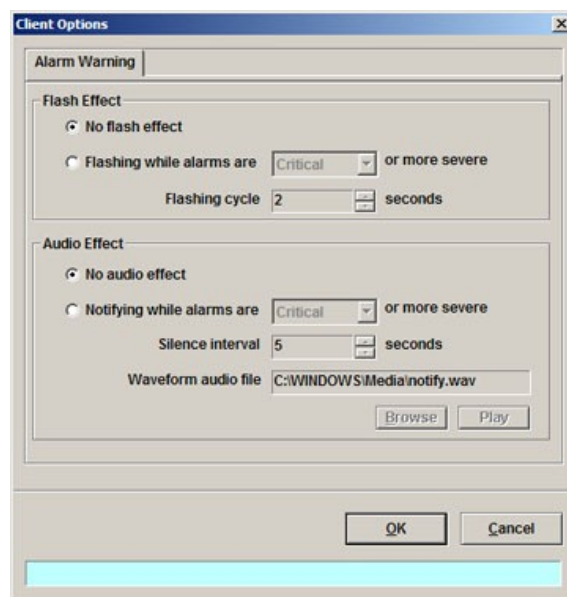


Table 12-124 Client Options Dialog – Alarm Warning Description

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

Chapter 13 Administrating and Maintenance

AMS supports the NE firmware and NE inventory management as follows.

This chapter contains the following sections:

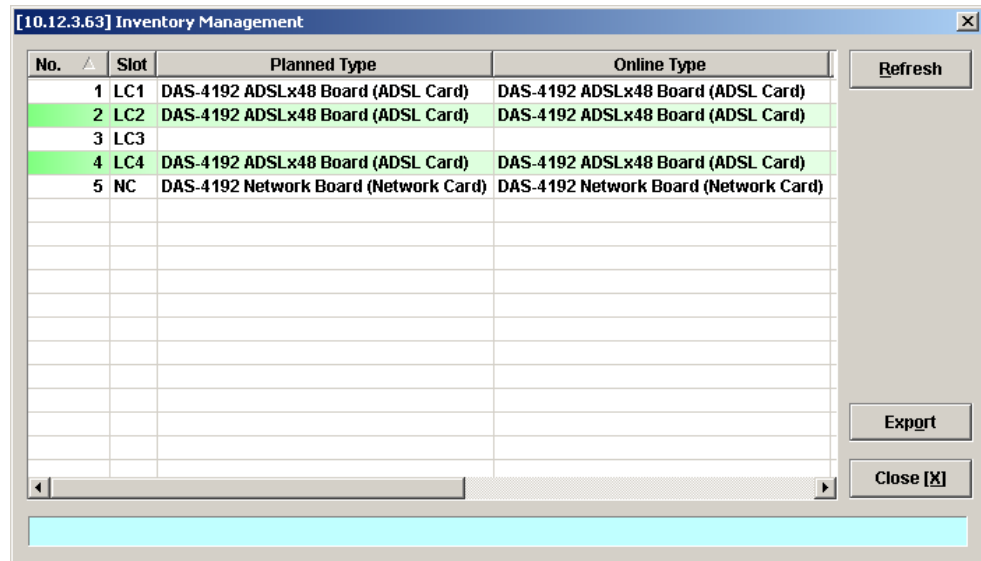
- NE Inventory Information
- NE Configuration Backup and Restore
- NE Firmware Upgrade
- SHDSL LC Firmware Upgrade
- NE Boot Partition
- NE File System List
- Reset the Unit

NE Inventory Information

Follow the subsequent procedure to display the inventory information of NE software/ hardware version, card serial number, card type and so on

Step 1 Click Diagnosis → Inventory on **Main Menu** to open the **Inventory Information List** as shown in Figure 13-170. Table 13-125 depicts the related parameters.

Figure 13-170 Inventory Information List



No.	Slot	Planned Type	Online Type	Refresh
1	LC1	DAS-4192 ADSLx48 Board (ADSL Card)	DAS-4192 ADSLx48 Board (ADSL Card)	
2	LC2	DAS-4192 ADSLx48 Board (ADSL Card)	DAS-4192 ADSLx48 Board (ADSL Card)	
3	LC3			
4	LC4	DAS-4192 ADSLx48 Board (ADSL Card)	DAS-4192 ADSLx48 Board (ADSL Card)	
5	NC	DAS-4192 Network Board (Network Card)	DAS-4192 Network Board (Network Card)	
				Export
				Close [X]

Table 13-125 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 DAS4 Series 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 13-171 and Table 13-126 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 of the read-write authorization. The default username/password is **admin/admin**.

Figure 13-171 NE Configuration Backup & Restore File List Dialog

Table 13-126 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.

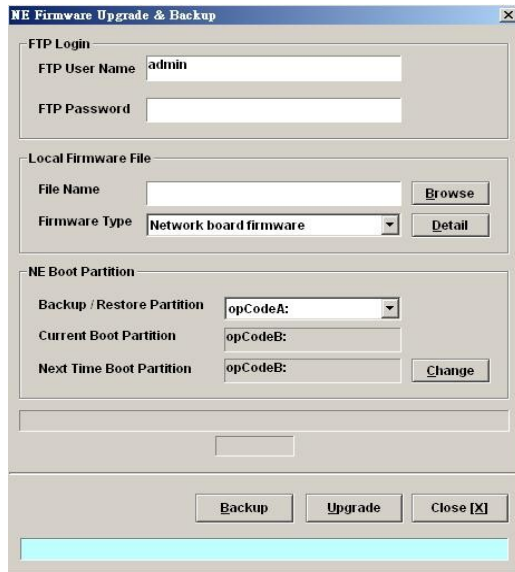
NE Firmware Upgrade

AMS LCT 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 13-172. Table 13-127 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 13-172 NE Firmware Upgrade Dialog



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 13-127 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.

SHDSL LC Firmware Upgrade

AMS LCT provides the “NE SHDSL Firmware Upgrade” dialog to upgrade the SHDSL LC firmware image to NE through FTP.

Follow the subsequent procedure to upgrade the SHDSL LC firmware image. It is noted that the NE needs to be rebooted to execute the new image.

AMS LCT provides the “NE SHDSL Firmware Upgrade” dialog to upload the firmware image to NC through FTP and then upgrade the new image from NC to SHDSL card. Follow the subsequent procedures to upgrade your SHDSL line card if necessary.

- Step 1** Click Configuration → NE Management → NE SHDSL Firmware Upgrade on **Main Menu** to open the **NE SHDSL Firmware Upgrade** Dialog as shown in Figure 13-173. Table 13-128 depicts the related parameters.
- Step 2** Click ‘**Browse**’ button to choose the suitable code file from host directory.
- Step 3** Click ‘**FTP**’ button to upload new firmware to NC card.
- Step 4** Mark the SHDSL LC which you want to upgrade firmware, and then click “**Upgrade**” to be proceed.
- Step 5** Reset the SHDSL LC to execute the upgraded firmware.



In comparison with the NC/ADSL LC firmware upgrade procedure, you need take one more step (**Step 4**) to upgrade the SHDSL firmware.



It is noted that the SHDSL LC must be reset at the completion of **Step 4**.

Figure 13-173 NE SHDSL Firmware Upgrade Dialog

No.	Slot	Current Upgrading Status
<input type="checkbox"/>	1 LC4	Finished

Table 13-128 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 13-174 .Table 13-129 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 13-174 NE Firmware Boot Partition Dialog

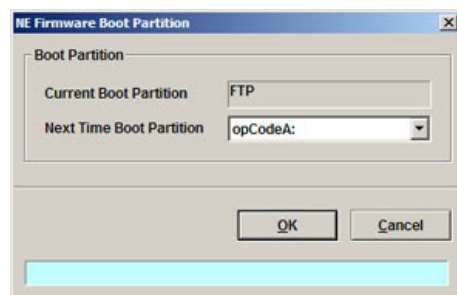


Table 13-129 NE Firmware Boot Partition Dialog Description

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 13-175. Table 13-130 depicts the related parameters.

Figure 13-175 NE File System List Dialog

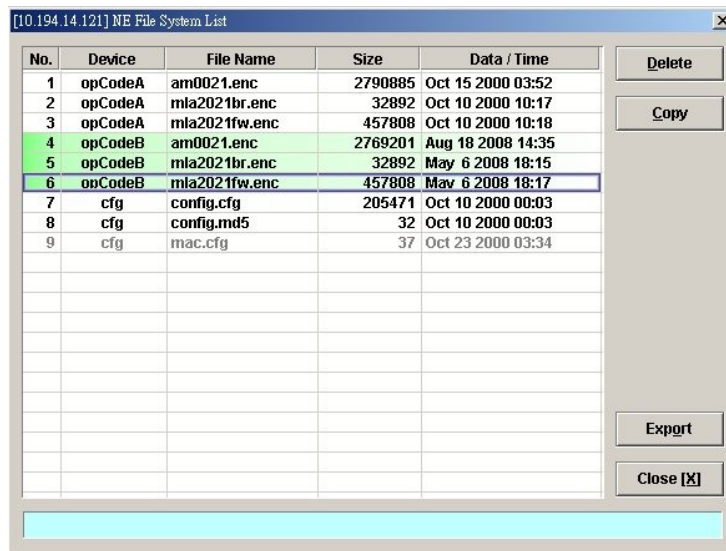


Table 13-130 NE File System List Dialog Description

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 seleted file.
Copy	Click this button to copy the seleted 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.

Administrating and Maintenance



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.

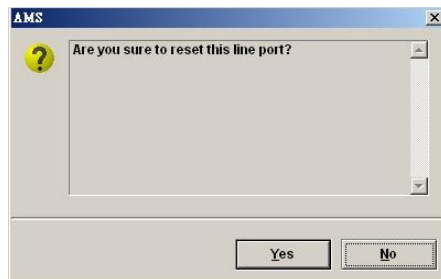
Whenever the NE boots up, it executes the following procedure.

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 13-176.

Figure 13-176 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
xDSL	ADSL/VDSL

This page is leave in blank for note or memo use

Appendix B Alarm Definition

Describe all the alarm in the AMS.

Table B-2 Alarm Definition

NE Model	Module Name	Alarm Name	Default Severity	Alarm Description
All	noEntity	EMPTY	No	Neither plan type nor on-line type configured
DAS4192	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
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		

NE Model	Module Name	Alarm Name	Default Severity	Alarm Description
DAS4192	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	uplicated 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 repay 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
		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		

NE Model	Module Name	Alarm Name	Default Severity	Alarm Description
DAS4192	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
DAS4672	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
		NOT_OPERABLE	Major	CPU card is not operable
		TCA_DHCP_BC	Warning	DHCP broadcast request rate threshold-crossing alert
		STANDBY	Information	Running in standby mode
		HW_VERSION	Major	Hardware version is inconsistent
	ADSL Module	SWAP	Information	Standby CPU module has been changed as active.
		MISSING	Major	ADSL module is off-line
		TEMP	Major	Temperature is over the threshold
		VOL	Major	Voltage is below the threshold
	Fan Module	MISMATCH	Major	Planned type and online type are mismatched
		NOT_OPERABLE	Major	Line card is not operable
		MISSING	Major	Fan module is off-line
		FAN1_SPEED	Major	Fan1 speed is below the threshold
	ADSL Port	FAN2_SPEED	Major	Fan2 speed is below the threshold
		FAN3_SPEED	Major	Fan3 speed is below the threshold
		VOL	Major	Voltage is below the threshold
		ES_NE_15_MIN	Minor	15 min near end ES is over the threshold
		SES_NE_15_MIN	Minor	15 min near end SES is over the threshold
		UAS_NE_15_MIN	Minor	15 min near end UAS is over the threshold
		ES_FE_15_MIN	Minor	15 min far end ES is over the threshold
		SES_FE_15_MIN	Minor	15 min far end SES is over the threshold
		UAS_FE_15_MIN	Minor	15 min far end UAS is over the threshold
		ES_NE_1_DAY	Minor	1 day near end ES is over the threshold
		SES_NE_1_DAY	Minor	1 day near end SES is over the threshold
		UAS_NE_1_DAY	Minor	1 day near end UAS is over the threshold
		ES_FE_1_DAY	Minor	1 day far end ES is over the threshold
		SES_FE_1_DAY	Minor	1 day far end SES is over the threshold
		UAS_FE_1_DAY	Minor	1 day far end UAS is over the 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	
	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	
	ADSL Port	PS_L2_MANUAL	Information	ADSL2/ADSL2+ Power State transfers to L2 by manual mode.
		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	

NE Model	Module Name	Alarm Name	Default Severity	Alarm Description	
DAS4672	GE Port	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 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	
	SHDSL Port	NOT_OPERABLE	Major	Line card is not operable	
		ES_NE_15_MIN	Minor	15-min near end ES is over the threshold	
		SES_NE_15_MIN	Minor	15-min near end SES is over the threshold	
		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	Minor	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	
		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	
		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	
		Chassis	PWR1_FAIL	Warning	Power1 failed
			PWR2_FAIL	Warning	Power2 failed
			PWR1_NOT_OPERABLE	Major	Power1 is not operable
			PWR2_NOT_OPERABLE	Major	Power2 is not operable

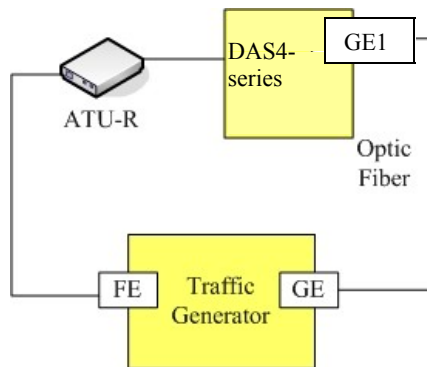
Appendix C Quick Configuration Guide for LCT

This appendix contains the following “How to” for the operator to be familiar with the DAS4-series product.

- HowTo 1. How to configure to provide a unicast/broadcast and bridged data service on the DAS4-series series IP-DSALM
- HowTo 2. How to configure to provide a multicast and bridged data service on the DAS4-series series IP-DSALM
- HowTo 3. How to configure to provide a Trunk CoS Mapping on the DAS4-series series IP-DSALM
- HowTo 4. How to backup and restore the NE Configuration
- HowTo 5. How to download the NE firmware via the out-band port

HowTo 1. How to configure to provide a unicast/broadcast and bridged data service on the DAS4-series series IP-DSALM

Environment



Set Up via AMS LCT

Step	Procedure and example of parameter value (Procedure with blue background, Example with yellow background)

Step 4 Add DSL line profile to system..

Follow the procedures in Section “Configuring the xDSL Profile” to set the profiles by filling the indicated dialogs as follows

Line Profile (Please refer the corresponding OID definition in Table F-)

1. Figure 5-29 Add ADSL Line Profile– Transmission Rate Dialog
2. Figure 5-31 Add ADSL Line Profile– SNR Margin Dialog
3. Figure 5-32 Add ADSL Line Profile– PSD Dialog
4. Figure 5-33 Add ADSL Line Profile– Power Management Dialog
5. Figure 5-34 Add ADSL Line Profile– INP Dialog

PM Threshold Profile (optional) (Please refer the corresponding OID definition in Table F-)

1. Figure 5-36 Add ADSL PM Threshold Profile Dialog

Traffic Policing Profile (Please refer the corresponding OID definition in Table F-)

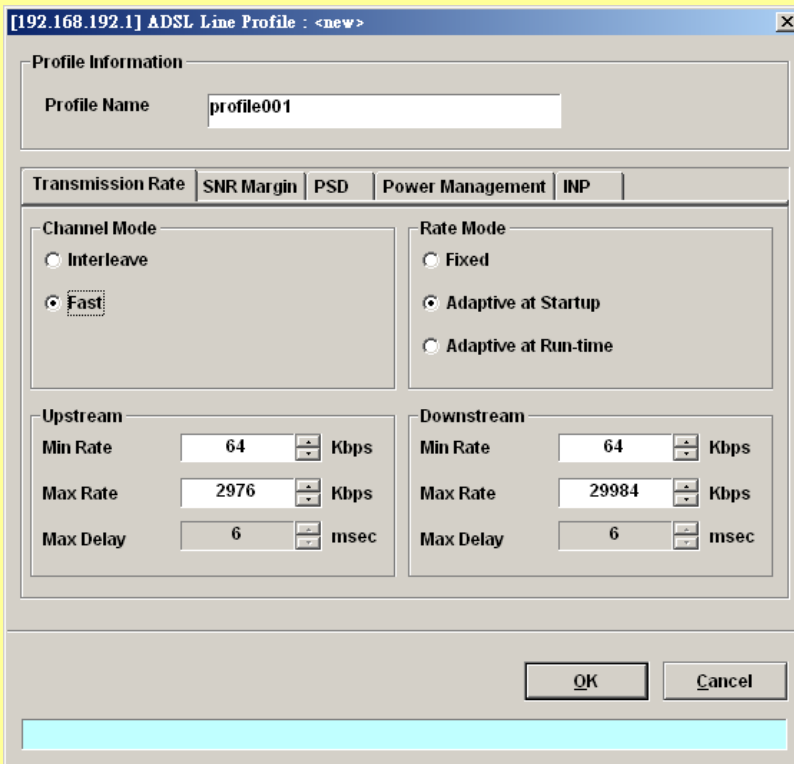
1. Figure 5-38 Add Traffic Policing Profile Dialog

Example:

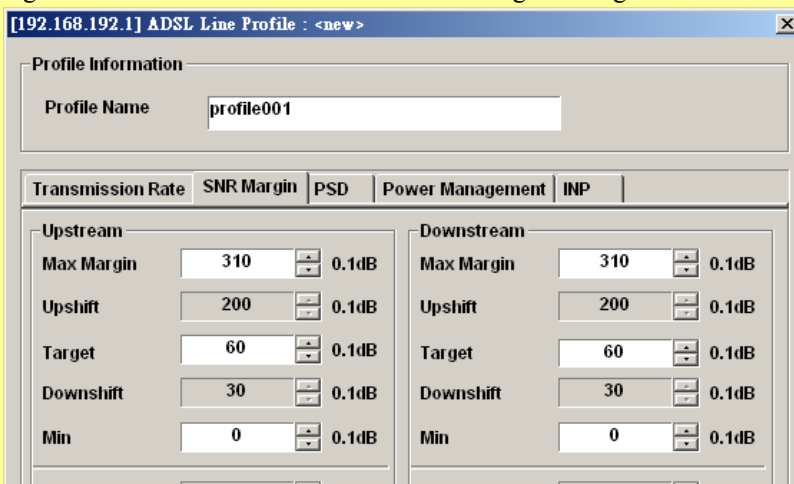
Please see the example setting as follows.

Line Profile

1. Figure 5-29 Add ADSL Line Profile– Transmission Rate Dialog



2. Figure 5-31 Add ADSL Line Profile– SNR Margin Dialog



3. Figure 5-32 Add ADSL Line Profile– PSD Dialog

[192.168.192.1] ADSL Line Profile : <new>

Profile Information

Profile Name

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

Upstream

Nominal PSD (0.1 dBm/Hz)

Downstream

Nominal PSD (0.1 dBm/Hz)

OK Cancel

4. Figure 5-33 Add ADSL Line Profile– Power Management Dialog

[192.168.192.1] ADSL Line Profile : <new>

Profile Information

Profile Name

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

Management Mode

Automatic

Manual

Trigger Criteria of State Transition

L2 State Min & Low Rate Kbps

L2 State Max Rate Kbps

L0 State Min Time to Start Monitoring sec

L2 State Low Rate Min Contiguous Time sec

CPE L3 State Request Accept Reject

OK Cancel

5. Figure 5-34 Add ADSL Line Profile– INP Dialog

[192.168.192.1] ADSL Line Profile : <new>

Profile Information

Profile Name profile001

Transmission Rate SNR Margin PSD Power Management INP

Upstream Minimum INP 0 (symbol time)

Downstream Minimum INP 0 (symbol time)

OK Cancel

PM Threshold Profile (optional)

1. Figure 5-36 Add ADSL PM Threshold Profile Dialog

Profile Information

Name: PM

15-Min / CO

ES 1 seconds

SES 1 seconds

UAS 1 seconds

1-Day / CO

ES 1 seconds

SES 1 seconds

UAS 1 seconds

15-Min / RT

ES 1 seconds

SES 1 seconds

UAS 1 seconds

1-Day / RT

ES 1 seconds

SES 1 seconds

UAS 1 seconds

OK Cancel

Traffic Policing Profile

1. Figure 5-38 Add Traffic Policing Profile Dialog

Profile Information

Name: Traffic-Policing3

Rate Limiting

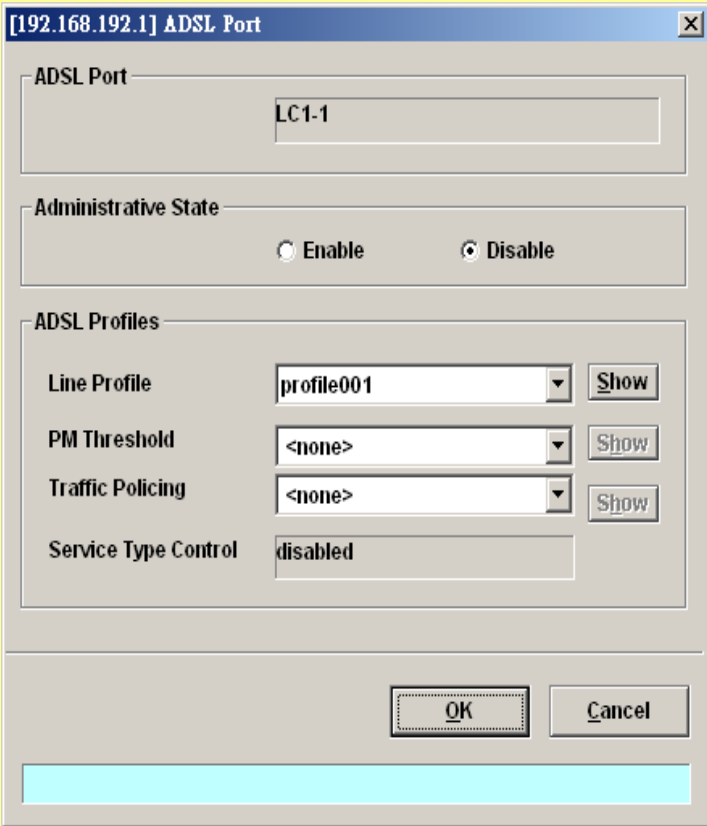
Upstream CIR (Mbps): 1

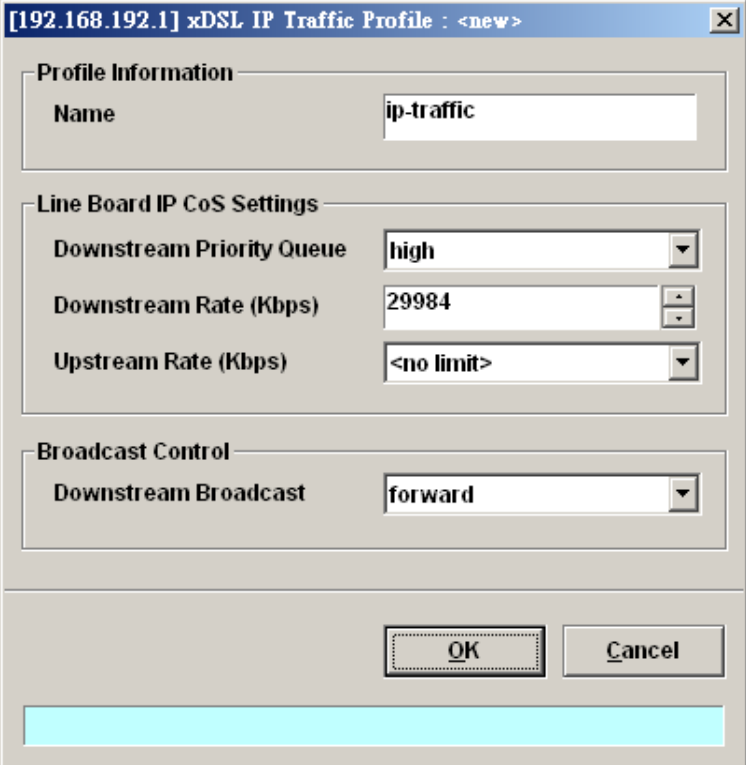
Action to Out-profile Packets: change DSCP as Expedited Forwarding

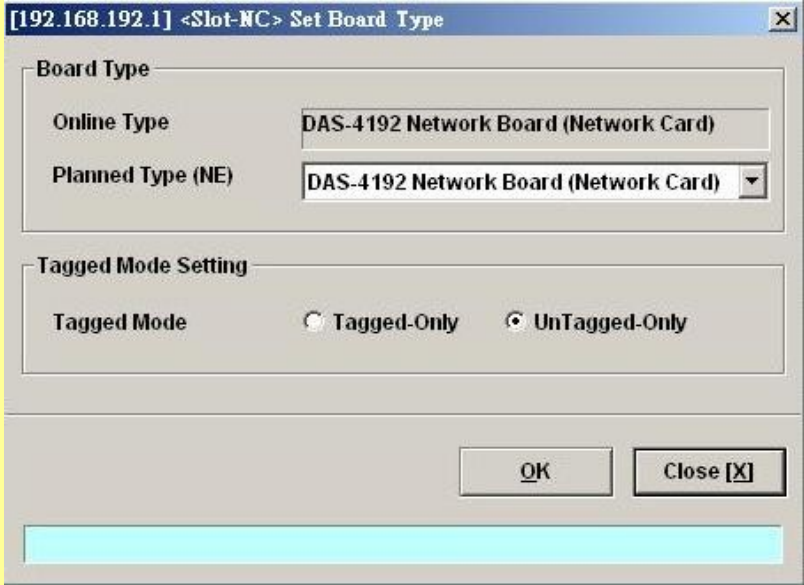
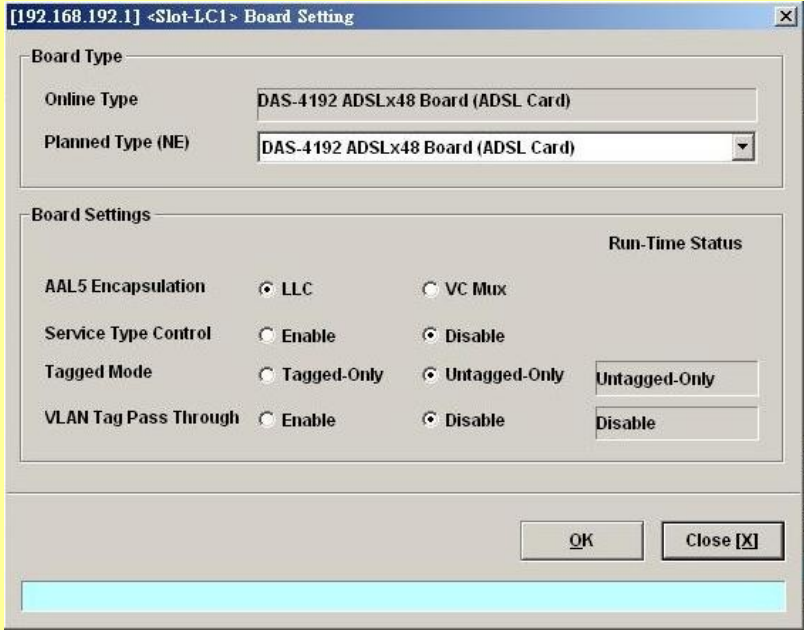
* AFxy: Assured Forwarding, service class x, drop precedence y

* NOTE: "Change DSCP" only takes effect on non-PPoE packets.

OK Cancel

Step 2	<p>Assign ADSL line profile to a ADSL subscriber and enable it.</p> <p>Follow the procedures in Section “xDSL Line Interface Management” to modify the configuration of target ADSL port by filling the following dialog.</p> <ol style="list-style-type: none">1. Figure 6-54 ADSL Port Modification Dialog (Please refer the corresponding OID definition in Table F-) <p>Example: Please see the example setting as follows.</p> <ol style="list-style-type: none">1. Figure 6-54 ADSL Port Modification Dialog 
--------	---

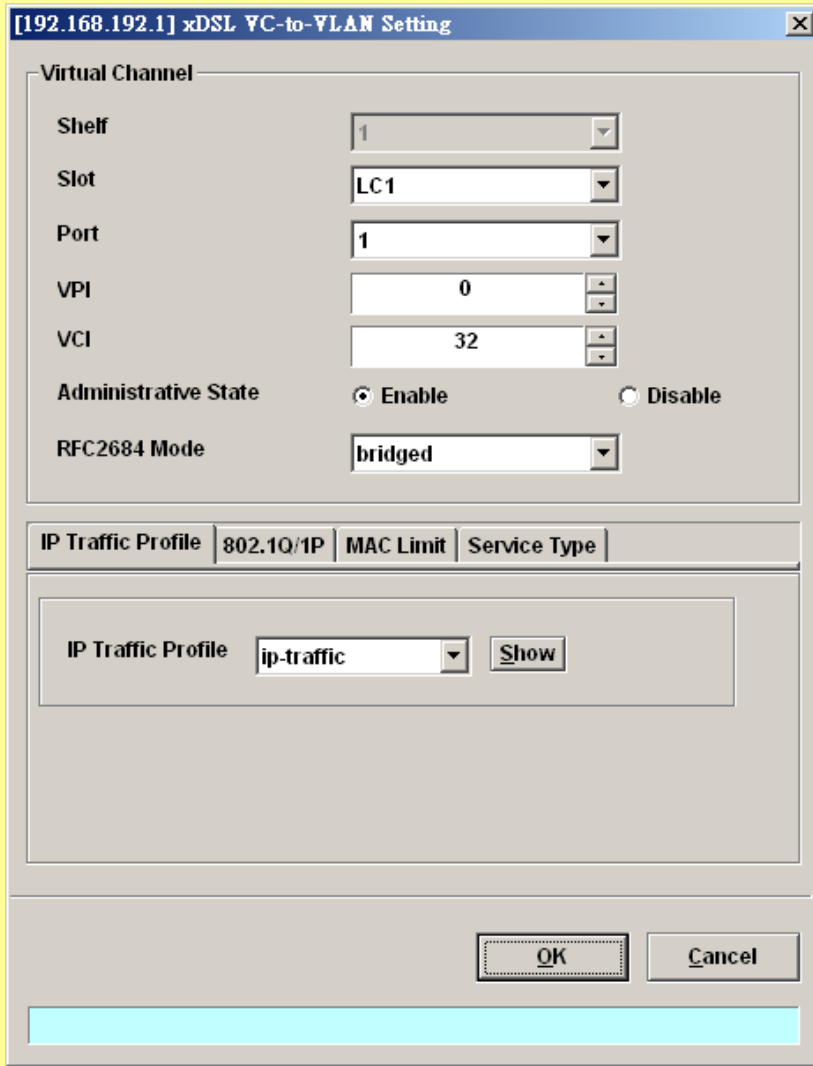
Step 3	Add an IP traffic profile to system.
	<p>Follow the procedures in Section “Traffic Profile” to set the following profiles</p> <p>IP Traffic Profile</p> <ol style="list-style-type: none"> Figure 5-46 Add xDSL IP Traffic Profile Dialog (Please refer the corresponding OID definition in Table F-)
	<p>Example:</p> <p>Please see the example setting as follows.</p> <ol style="list-style-type: none"> Figure 5-46 Add xDSL IP Traffic Profile Dialog 

<p>Step 4</p>	<p>Set the tag mode of NC/LC. (optional)</p> <p>Follow the procedures in Section “Network Interface Administrating” of Chapter 6 to set the tag mode of NC/LC</p> <p>Set the tag mode of NC</p> <ol style="list-style-type: none"> Figure 4-11 NC Boarding Setting Dialog <p>Set the tag mode of target LC</p> <ol style="list-style-type: none"> Figure 4-10 xDSL Board Setting Dialog <p>Example: Please see the example setting as follows.</p> <p>Set the tag mode of NC</p> <ol style="list-style-type: none"> Figure 4-11 NC Boarding Setting Dialog  <p>Set the tag mode of target LC</p> <ol style="list-style-type: none"> Figure 4-10 xDSL Board Setting Dialog 
---------------	--

Step 5	<p>Create a bidirectional PVC between IP-DSLAM and ATU-R</p> <p>Follow the procedures in Section “VC-to-VLAN Connection Management” to fill the following dialogs Add xDSL IP Traffic Profile Dialog (Please refer the corresponding OID definition in Table F-)</p> <ol style="list-style-type: none"> 1. Figure 7-76 xDSL VC-to-VLAN Setting – IP Traffic Dialog 2. Figure 7-77 xDSL VC-to-VLAN Setting – 802.1Q/IP Dialog (only for the RFC2684 bridged mode) 3. Figure 7-79 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 bridged mode 4. Figure 7-82 xDSL VC-to-VLAN Setting – Service Type Dialog
--------	--

Example:
 Please see the example setting as follows.

1. Figure 7-76 xDSL VC-to-VLAN Setting – IP Traffic Dialog (Bridged Mode)



- 2. Figure 7-77 xDSL VC-to-VLAN Setting – 802.1Q/IP Dialog (only for the RFC2684 bridged mode)

The screenshot shows a dialog box titled "[192.168.192.1] xDSL VC-to-VLAN Setting". It has a "Virtual Channel" section with the following settings: Shelf (1), Slot (LC1), Port (1), VPI (0), VCI (32), Administrative State (Enable), and RFC2684 Mode (bridged). Below this is a tabbed interface with "IP Traffic Profile", "802.1Q/IP", "MAC Limit", and "Service Type" tabs. The "802.1Q/IP" tab is active, showing "VLAN ID" (100) and "User Priority" (0). At the bottom are "OK" and "Cancel" buttons.

- 3. Figure 7-79 xDSL VC-to-VLAN Setting – MAC Control Dialog for the RFC2684 bridged mode

The screenshot shows the same dialog box as above, but with the "MAC Limit" tab selected. The "MAC Count" is set to 4, and "Non-aged" is set to Disable. The "Virtual Channel" and "802.1Q/IP" sections remain the same. At the bottom are "OK" and "Cancel" buttons.

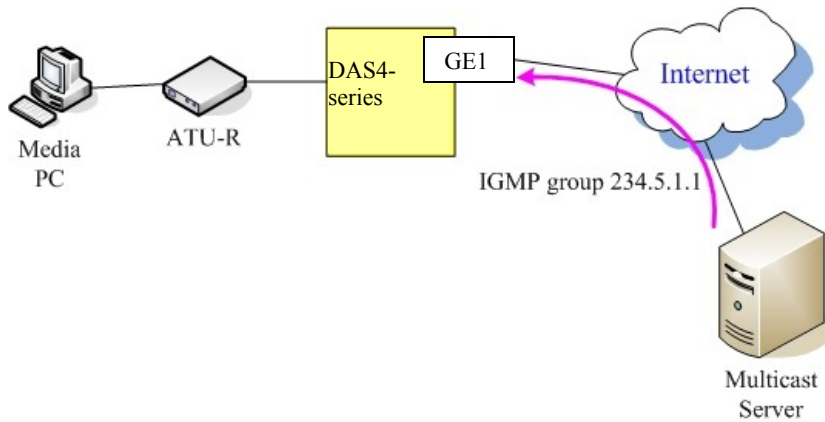
4. Figure 7-82 xDSL VC-to-VLAN Setting – Service Type Dialog

The screenshot shows a dialog box titled "[192.168.192.1] xDSL VC-to-VLAN Setting". It has a "Virtual Channel" section with the following settings: Shelf (1), Slot (LC1), Port (1), VPI (0), VCI (32), Administrative State (Enable), and RFC2684 Mode (bridged). Below this is a tabbed interface with "IP Traffic Profile", "802.1Q/IP", "MAC Limit", and "Service Type" tabs. The "Service Type" tab is active, showing Service Type (PPPoE), Continous IP Count (1), and Static IP's Base Address (1 . 1 . 1 . 1). At the bottom are "OK" and "Cancel" buttons.

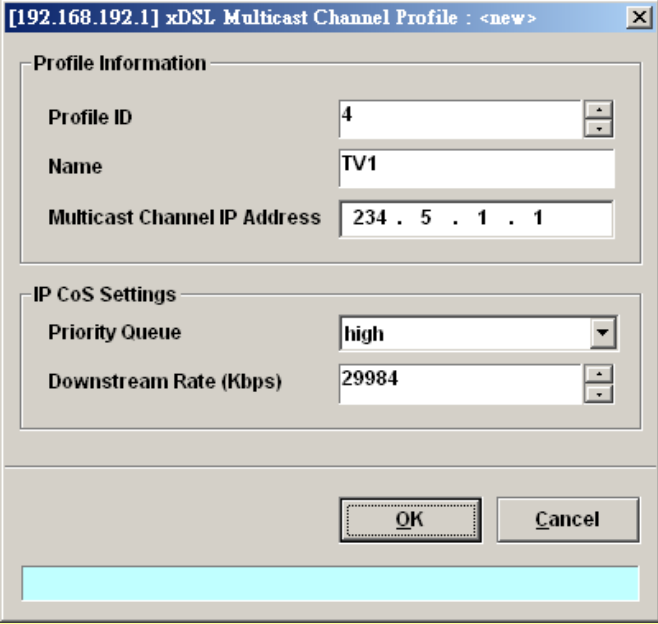
The screenshot shows the same dialog box as above, but with the "Service Type" tab set to "DHCP". The "Continous IP Count" field is now labeled "Maximum IP Count" and remains set to 1. The "Static IP's Base Address" field remains set to 1 . 1 . 1 . 1. All other settings in the "Virtual Channel" section and the tabs are identical to the previous screenshot.

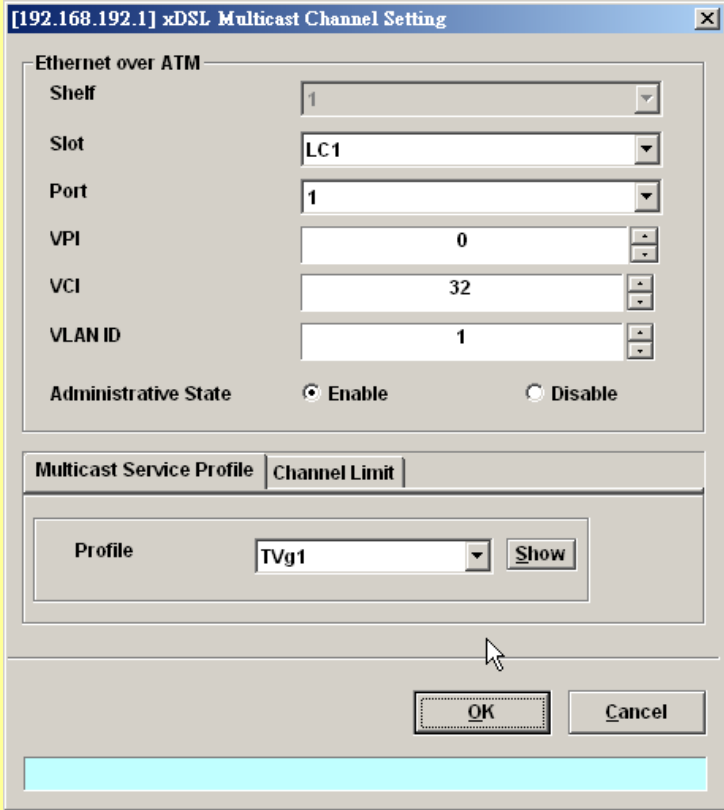
HowTo 2. How to configure to provide a multicast and bridged data service on the DAS4-series series IP-DSALM

Environment



Set Up via AMS LCT

Step	Procedure and example of parameter value (Procedure with blue background, Example with yellow background)
Step 1	<p>Add a TV (multicast) channel profile to system.</p> <p>Follow the procedures in Section “TV Channel Profile” to set the following profiles TV Channel Profile (Please refer the corresponding OID definition in Table F-)</p> <ol style="list-style-type: none"> Figure 5-48 Add xDSL TV Channel Profile Dialog <p>Example: Please see the example setting as follows.</p> <ol style="list-style-type: none"> Figure 5-48 Add xDSL TV Channel Profile Dialog 

Step 3	LCT setup as same as step 1~4 in HowTo 1
Step 4	Create a meau (multicast conditional access unit) on xDSL subscriber.
	Follow the procedures in Section “Multicast Channel Configuration” to fill the following dialogs (Please refer the corresponding OID definition in Table F-)
	1. Figure 7-100 xDSL Multicast Channel Setting Dialog
	<p>Example: Please see the example setting as follows.</p> <p>1. Figure 7-100 xDSL Multicast Channel Setting Dialog</p> 

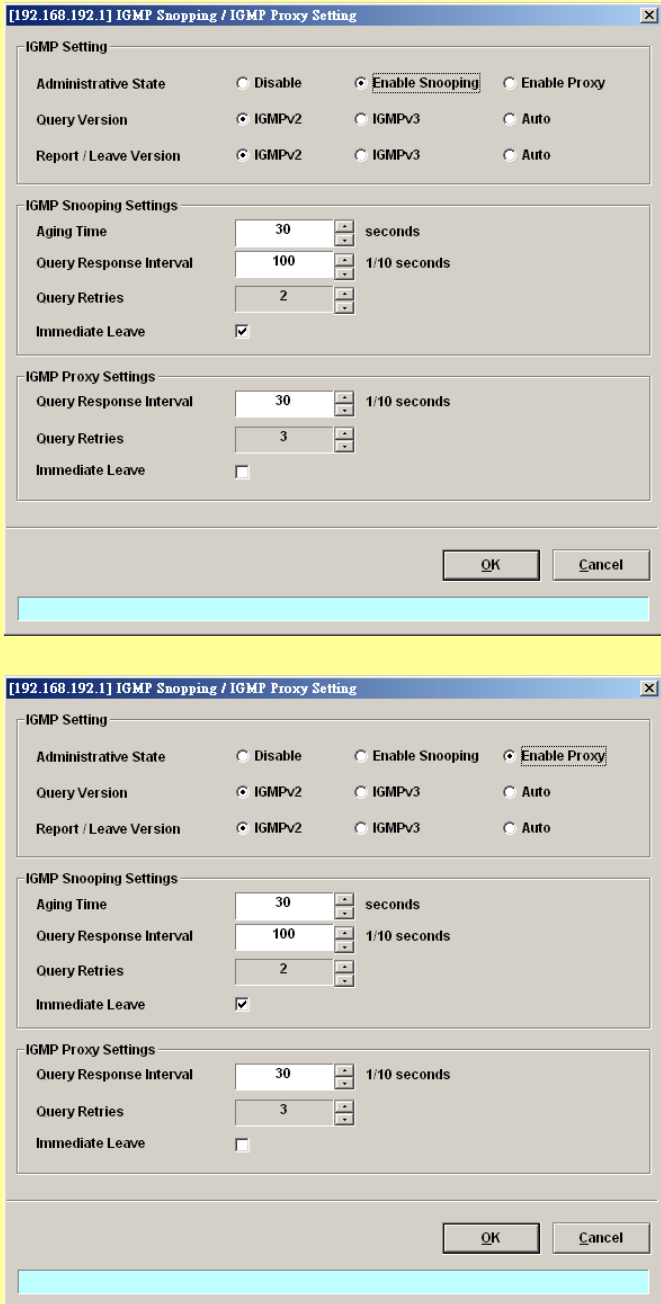
Step 5 Enable IGMP snoopy function on IP-DSLAM.

Follow the procedures in Section “IGMP snooping/IGMP proxy Configuration” to fill the following dialogs (Please refer the corresponding OID definition in Table F-)

- Figure 7-101 IGMP Snooping / IGMP Proxy Setting Dialog

Example:
Please see the example setting as follows.

- Figure 7-101 IGMP Snooping / IGMP Proxy Setting Dialog



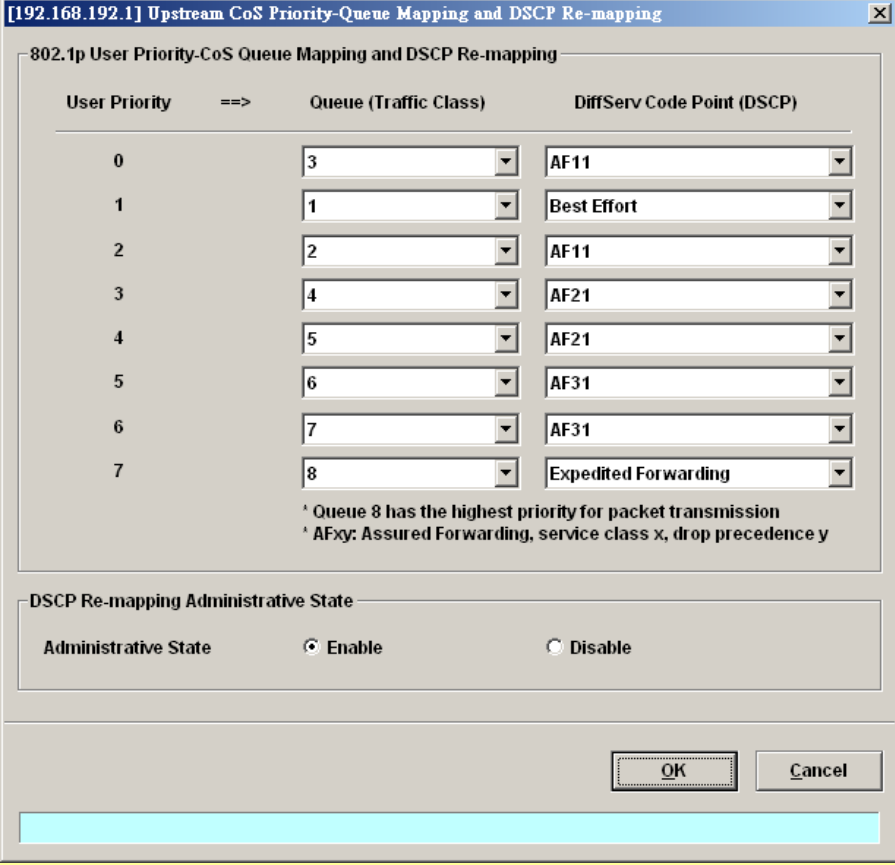
The figure shows two screenshots of the 'IGMP Snooping / IGMP Proxy Setting' dialog box. The first screenshot shows the 'Administrative State' section with 'Enable Snooping' selected. The second screenshot shows the 'Administrative State' section with 'Enable Proxy' selected. Both screenshots show the same configuration for the 'IGMP Snooping Settings' and 'IGMP Proxy Settings' sections.



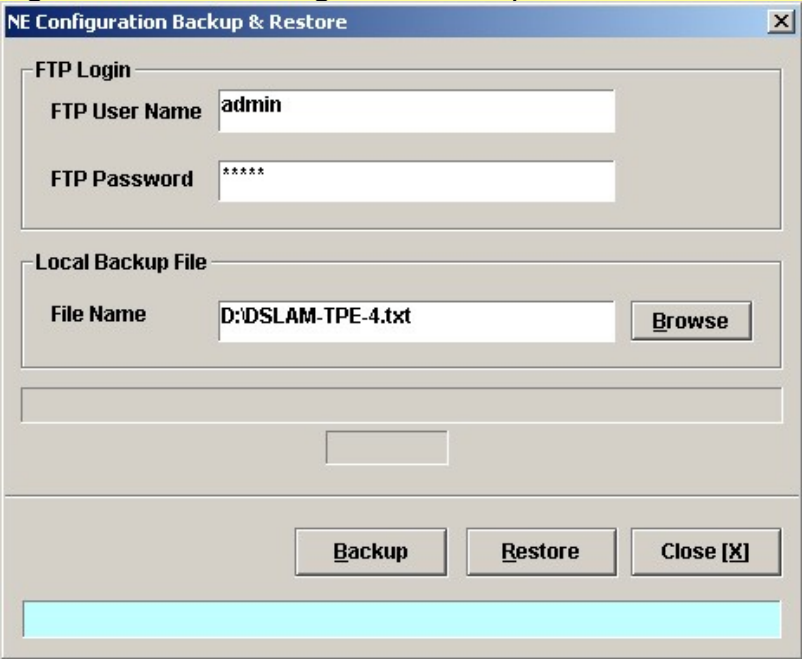
As shown in the above figure, the default **Aging Time** is 30 seconds. However, the aging time setting should be large enough to prevent the spooned multicast IP MAC from being aged out. It is suggested to set the **Aging Time** to be 600 seconds.

HowTo 3. How to configure to provide a Trunk CoS Mapping on the DAS4-series series IP-DSALM

Set Up via AMS LCT

Step	Procedure and example of parameter value (Procedure with blue background, Example with yellow background)
Step 1	<p>Add a Trunk CoS Mapping and DSCP Re-mapping to system.</p> <p>Follow the procedures in Section “CoS Configuration” to fill the following dialogs (Please refer the corresponding OID definition in Table F-)</p> <ol style="list-style-type: none"> Figure 6-66 Trunk CoS Mapping and DSCP Re-mapping Dialog <p>Example: Please see the example setting as follows.</p> <ol style="list-style-type: none"> Figure 6-66 Trunk CoS Mapping and DSCP Re-mapping Dialog 

HowTo 4. How to backup and restore the NE Configuration
Backup and Restore the NE Configuration via AMS LCT

Step	Procedure and example of parameter value (Procedure with blue background, Example with yellow background)
Step 1	<p>Backup the configuration from the NE and restore the configuration to the NE.</p> <p>Follow the procedures in Section “NE Configuration Backup and Restore” to fill the following dialogs.</p> <ol style="list-style-type: none"> Figure 13-171 NE Configuration Backup & Restore File List Dialog <p>Example: Please see the example setting as follows.</p> <ol style="list-style-type: none"> Figure 13-171 NE Configuration Backup & Restore File List Dialog 



It is noted that the NE configuration is saved in “default.cfg” on the NE. The LCT allows to backup the “default.cfg” and save it with a different filename on the local host. In the mean time, the LCT also allows to restore the “default.cfg” with a NE configuration different filename on the local host.

Set Up via CLI

NE provides NC/ADSL LC backup and restore related CLI commands to backup or restore the NE configuration via FTP. The backup procedures are as following:

Step 1 Open the DOS prompt window (or environment) on personal computer (PC).

Step 2 Go to the directory where the backup file is saved, and then login the

DAS4-Series by FTP

Step 3 Get the configuration file from NE to the target partition via FTP by following

commands:

```
ftp> cd cfg:
ftp> get default.cfg
```

or
ftp> put default.cfg



It is noted that login device via FTP must be used the read-write authorization. The default username/password is **admin/admin**.



It is noted that the NE configuration is saved in “default.cfg” on the NE. The operator can backup the “default.cfg” and save it with a different filename on the local host. However, the operator has to restore (by the ftp “put” command) the NE configuration with filename of “default.cfg”.

The following example shows how to backup the configurations from NE.

```

1.
2.D:\>ftp 10.12.3.160
3.Connected to 10.12.3.160.
4.220-=====
5.220-          Welcome to the IP-DSLAM FTP Server          -
6.220-          -
7.220- CAUTION: It's your responsibility to use the FTP service correctly -
8.220-          , please put the right files into the right file system. -
9.220 =====
10.User (10.12.3.160:(none)): admin
11.331 Password required
12.Password:
13.230 User logged in
14.ftp> cd cfg:
15.250 Changed directory to "cfg:/"
16.ftp> get default.cfg D:\DSLAM-TPE-4.txt
17.200 Port set okay
18.150 Opening BINARY mode data connection
19.226 Transfer complete
20.ftp: 152231 bytes received in 0.45Seconds 335.31Kbytes/sec.
21.ftp> bye
22.221 Bye...see you later
23.
24.D:\>

```

The following example shows how to restore the configurations to NE.

```

25.
26.D:\>ftp 10.12.3.160
27.Connected to 10.12.3.160.
28.220-=====
29.220-          Welcome to the IP-DSLAM FTP Server          -
30.220-          -
31.220- CAUTION: It's your responsibility to use the FTP service correctly -
32.220-          , please put the right files into the right file system. -
33.220 =====
34.User (10.12.3.160:(none)): admin

```

```
35.331 Password required
36.Password:
37.230 User logged in
38.ftp> cd cfg:
39.250 Changed directory to "cfg:/"
40.ftp> put DSLAM-TPE-4.cfg default.cfg
41.200 Port set okay
42.150 Opening BINARY mode data connection
43.226- CAUTION:Please wait for 120 seconds or check the Flash LED -
44.226 Transfer complete
45.ftp: 152231 bytes sent in 0.80Seconds 191.01Kbytes/sec.
46.ftp> bye
47.221 Bye...see you late
```

HowTo 5. How to download the NE firmware via the out-band port

The NE supports to use FTP to download the NE firmware from a local host (PC, for example) to the NE via the out-band port (i.e. nme). To this end, this section depicts the procedures on the local host side and the NE side as follows.

On the local host side:

The local host should be equipped with a FTP Server (WFTP for example) and the NE firmware in demand. The configuration of WFTP is as follows.

Step 1 Execute the wftp32.exe

Step 2 Click Users/rights under the Security sub-menu. (Refers to Figure 1)

Step 3 Click New User to create username and password. (Refers to Figure 2)

Step 4 Input the full path in “Home Directory” and finish it by clicking ‘Done’.
(Refers to Figure 2)



The NE firmware must be placed in the “Home Directory” of host PC as set in Figure 2. Otherwise, the NE will fail to download the NE firmware.

Figure 1 The setting of WFTP: To open the Users/rights dialog

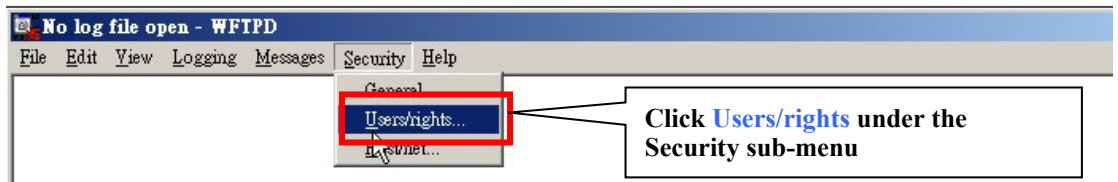
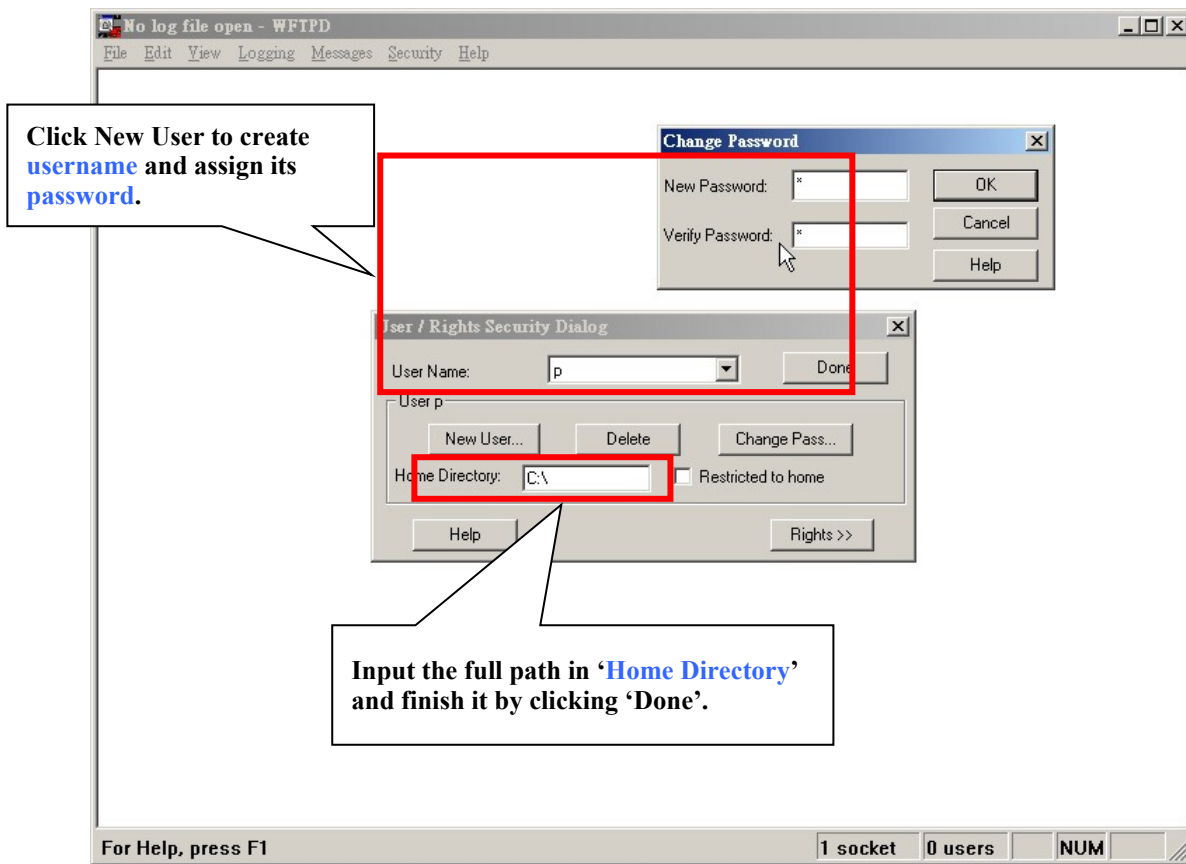


Figure 2 The setting of WFTP: Create User and assign its password.

**On the NE side:**

Example 1 depicts the procedure on the NE side.

Step 1 Power up the NE and press any key to enter the “VxWorks Boot” mode.

Step 2 Change the boot configuration by the command ‘c’. (Refers to Example 1)

Step 3 Change to the values marked in red rectangles as shown in Example 1.

(Refers Table 1 for the description of the mandatory parameters in Example 1)

Step 4 Enter command ‘p’ to show and confirm the new setting of NE boot configuration as shown in Example 2.

Step 5 Enter command ‘@’ to load the NE firmware from the local host and execute it.



After loading the firmware from the local host via FTP, the boot partition must be changed to ‘opCodeA’ or ‘opCodeB’. Such that the NE reboots from the non-volatile memory instead of the local host.

For the related commands, please refer to Chapter 3 in “IP-DSLAM System Configuration Guide” or Chapter 13 in “LCT Software Operation Guide”



If the operator does not press any key. The NE will load NE firmware from the partition 'opCodeA' or 'opCodeB' of its non-volatile memory)



A summarization of commands use in the [VxWorks Boot] mode.

'p' : Show the current setting

'c' : Change the setting

'@' : Start to load the NE firmware and execute it.

Example 1 Change the setting of [VxWorks Boot]

```
[VxWorks Boot]: c

'. ' = clear field; '^' = go to previous field; ^D = quit

boot device      : opCodeA rtl
processor number  : 0
host name       : MCI2021
file name       : am00xx.enc am0031.enc
inet on ethernet (e) : 192.168.192.1 10.12.3.92
inet on backplane (b):
host inet (h)    : 10.12.3.11 10.12.3.92
gateway inet (g) :
user (u)        : a p
ftp password (pw) (blank = use rsh): a p
flags (f)       : 0x0 ^
target name (tn) :
startup script (s) :
other (o)       : rtl
```

Example 2 Show the current setting of [VxWorks Boot]

```
[VxWorks Boot]: p

boot string      : 255
boot device      : rtl
unit number      : 0
processor number  : 0
host name       : MCI2021
file name       : am0031.enc
inet on ethernet (e) : 10.12.1.251
host inet (h)    : 10.12.3.92
user (u)        : p
ftp password (pw) : p
flags (f)       : 0x0
other (o)       : rtl

[VxWorks Boot]: @
```

Table 1 Description of the mandatory parameters shown in the [VxWorks Boot] mode

Parameters	Task
boot device	<p>This specifies the place to load NE firmware.</p> <ul style="list-style-type: none"> The 'opCodeA' and 'opCodeB' indicate the boot partitions of non-volatile memory. 'rtl' indicates the out-band port of NE. <p>Type: Mandatory Valid values: opCodeA, opCodeB, rtl</p>
file name	<p>This specifies the filename of firmware</p> <p>Type: Mandatory Valid values: am0021.enc am0031.enc</p>
inet on ethernet (e)	<p>This specifies the IP address of out-band port of NE.</p> <p>Type: Mandatory Valid values: Any valid class A/B/C address Default value: 192.168.192.1</p>
host inet (h)	<p>This specifies the IP address of local host (PC).</p> <p>Type: Mandatory Valid values: Any valid class A/B/C address</p>
user (u)	<p>This specifies the username of FTP server.</p> <p>Type: Mandatory Valid values: String of up to 16 characters ('A' - 'Z', 'a' - 'z', '0' - '9', '-', '_', '.', '@')</p>
ftp password (pw)	<p>This specifies the password of FTP server.</p> <p>Type: Mandatory Valid values: String of up to 16 characters ('A' - 'Z', 'a' - 'z', '0' - '9', '-', '_', '.', '@')</p>



The configured IP addresses of 'inet on ethernet (e)' and 'host inet (h)' must be in the same subnet.

This page is leave in blank for note or memo use

Appendix D Reference to Internet Protocol Numbers

Table D-3 Internet Protocol Numbers Definition

Decimal	Keyword	Protocol	References
0	HOPOPT	IPv6 Hop-by-Hop Option	[RFC1883]
1	ICMP	Internet Control Message	[RFC792]
2	IGMP	Internet Group Management	[RFC1112]
3	GGP	Gateway-to-Gateway	[RFC823]
4	IP	IP in IP (encapsulation)	[RFC2003]
5	ST	Stream	[RFC1190][RFC1819]
6	TCP	Transmission Control	[RFC793]
7	CBT	CBT	[Ballardie]
8	EGP	Exterior Gateway Protocol	[RFC888][DLM1]
9	IGP	any private interior gateway	[IANA]
10	BBN-RCC-MON	BBN RCC Monitoring	[SGC]
11	NVP-II	Network Voice Protocol	[RFC741][SC3]
12	PUP	PUP	[PUP][XEROX]
13	ARGUS	ARGUS	[RWS4]
14	EMCON	EMCON	[BN7]
15	XNET	Cross Net Debugger	[IEN158][JFH2]
16	CHAOS	Chaos	[NC3]
17	UDP	User Datagram	[RFC768][JBP]
18	MUX	Multiplexing	[IEN90][JBP]
19	DCN-MEAS	DCN Measurement Subsystems	[DLM1]
20	HMP	Host Monitoring	[RFC869][RH6]
21	PRM	Packet Radio Measurement	[ZSU]
22	XNS-IDP	XEROX NS IDP	[ETHERNET][XEROX]
23	TRUNK-1	Trunk-1	[BWB6]
24	TRUNK-2	Trunk-2	[BWB6]
25	LEAF-1	Leaf-1	[BWB6]
26	LEAF-2	Leaf-2	[BWB6]
27	RDP	Reliable Data Protocol	[RFC908][RH6]
28	IRTP	Internet Reliable Transaction	[RFC938][TXM]
29	ISO-TP4	ISO Transport Protocol Class 4	[RFC905][RC77]
30	NETBLT	Bulk Data Transfer Protocol	[RFC969][DDC1]
31	MFE-NSP	MFE Network Services Protocol	[MFENET][BCH2]
32	MERIT-INP	MERIT Internodal Protocol	[HWB]
33	DCCP	Datagram Congestion Control Protocol	[RFC4340]
34	3PC	Third Party Connect Protocol	[SAF3]
35	IDPR	Inter-Domain Policy Routing Protocol	[MXS1]
36	XTP	XTP	[GXC]
37	DDP	Datagram Delivery Protocol	[WXC]
38	IDPR-CMTP	IDPR Control Message Transport Protocol	[MXS1]
39	TP++	TP++ Transport Protocol	[DXF]

Decimal	Keyword	Protocol	References
40	IL	IL Transport Protocol	[Presotto]
41	IPv6	Ipv6	[Deering]
42	SDRP	Source Demand Routing Protocol	[DXE1]
43	IPv6-Route	Routing Header for IPv6	[Deering]
44	IPv6-Frag	Fragment Header for IPv6	[Deering]
45	IDRP	Inter-Domain Routing Protocol	[Hares]
46	RSVP	Reservation Protocol	[Braden]
47	GRE	General Routing Encapsulation	[Li]
48	DSR	Dynamic Source Routing Protocol	[RFC4728]
49	BNA	BNA	[Salamon]
50	ESP	Encap Security Payload	[RFC2406]
51	AH	Authentication Header	[RFC2402]
52	I-NLSP	Integrated Net Layer Security TUBA	[GLENN]
53	SWIPE	IP with Encryption	[JI6]
54	NARP	NBMA Address Resolution Protocol	[RFC1735]
55	MOBILE	IP Mobility	[Perkins]
56	TLSP	Transport Layer Security Protocol	[Oberg]
57	SKIP	SKIP	[Markson]
58	IPv6-ICMP	ICMP for IPv6	[RFC1883]
59	IPv6-NoNxt	No Next Header for IPv6	[RFC1883]
60	IPv6-Opts	Destination Options for IPv6	[RFC1883]
61		any host internal protocol	[IANA]
62	CFTP	CFTP	[CFTP] [HCF2]
63		any local network	[IANA]
64	SAT-EXPAK	SATNET and Backroom EXPAK	[SHB]
65	KRYPTOLAN	Kryptolan	[PXL1]
66	RVD	MIT Remote Virtual Disk Protocol	[MBG]
67	IPPC	Internet Pluribus Packet Core	[SHB]
68		any distributed file system	[IANA]
69	SAT-MON	SATNET Monitoring	[SHB]
70	VISA	VISA Protocol	[GXT1]
71	IPCV	Internet Packet Core Utility	[SHB]
72	CPNX	Computer Protocol Network Executive	[DXM2]
73	CPHB	Computer Protocol Heart Beat	[DXM2]
74	WSN	Wang Span Network	[VXD]
75	PVP	Packet Video Protocol	[SC3]
76	BR-SAT-MON	Backroom SATNET Monitoring	[SHB]
77	SUN-ND	SUN ND PROTOCOL-Temporary	[WM3]
78	WB-MON	WIDEBAND Monitoring	[SHB]
79	WB-EXPAK	WIDEBAND EXPAK	[SHB]
80	ISO-IP	ISO Internet Protocol	[MTR]
81	VMTP	VMTP	[DRC3]
82	SECURE-VMTP	SECURE-VMTP	[DRC3]

Decimal	Keyword	Protocol	References
83	VINES	VINES	[BXH]
84	TTP	TTP	[JXS]
85	NSFNET-IGP	NSFNET-IGP	[HWB]
86	DGP	Dissimilar Gateway Protocol	[DGP][ML109]
87	TCF	TCF	[GAL5]
88	EIGRP	EIGRP	[CISCO][GXS]
89	OSPFIGP	OSPFIGP	[RFC1583][JTM4]
90	Sprite-RPC	Sprite RPC Protocol	[SPRITE][BXW]
91	LARP	Locus Address Resolution Protocol	[BXH]
92	MTP	Multicast Transport Protocol	[SXA]
93	AX.25	AX.25 Frames	[BK29]
94	IPIP	IP-within-IP Encapsulation Protocol	[JI6]
95	MICP	Mobile Internetworking Control Protocol	[JI6]
96	SCC-SP	Semaphore Communications Sec. Protocol	[HXH]
97	ETHERIP	Ethernet-within-IP Encapsulation	[RFC3378]
98	ENCAP	Encapsulation Header	[RFC1241,RXB3]
99	GMTP	GMTP	[RXB5]
100	IFMP	Ipsilon Flow Management Protocol	[Hinden]
101	PNNI	PNNI over IP	[Callon]
102	PIM	Protocol Independent Multicast	[Farinacci]
103	ARIS	ARIS	[Feldman]
104	SCPS	SCPS	[Durst]
105	QNX	QNX	[Hunter]
106	A/N	Active Networks	[Braden]
107	IPComp	IP Payload Compression Protocol	[RFC2393]
108	SNP	Sitara Networks Protocol	[Sridhar]
109	Compaq-Peer	Compaq Peer Protocol	[Volpe]
110	IPX-in-IP	IPX in IP	[Lee]
111	VRRP	Virtual Router Redundancy Protocol	[RFC3768]
112	PGM	PGM Reliable Transport Protocol	[Speakman]
113		any 0-hop protocol	[IANA]
114	L2TP	Layer Two Tunneling Protocol	[Aboba]
115	DDX	D-II Data Exchange (DDX)	[Worley]
116	IATP	Interactive Agent Transfer Protocol	[Murphy]
117	STP	Schedule Transfer Protocol	[JMP]
118	SRP	SpectraLink Radio Protocol	[Hamilton]
119	UTI	UTI	[Lothberg]
120	SMP	Simple Message Protocol	[Ekblad]
121	SM	SM	[Crowcroft]
122	PTP	Performance Transparency Protocol	[Welzl]
123	ISIS over IPv4		[Przygienda]
124	FIRE		[Partridge]
125	CRTP	Combat Radio Transport Protocol	[Sautter]

Decimal	Keyword	Protocol	References
126	CRUDP	Combat Radio User Datagram	[Sautter]
127	SSCOPMCE		[Waber]
128	IPLT		[Hollbach]
129	SPS	Secure Packet Shield	[McIntosh]
130	PIPE	Private IP Encapsulation within IP	[Petri]
131	SCTP	Stream Control Transmission Protocol	[Stewart]
132	FC	Fibre Channel	[Rajagopal]
133	RSVP-E2E-IGNORE		[RFC3175]
134	Mobility Header		[RFC3775]
135	UDPLite		[RFC3828]
136	MPLS-in-IP		[RFC4023]
137	manet	MANET Protocols	[RFC-ietf-manet-iana-07.txt]
138	HIP	Host Identity Protocol	[RFC5201]
139		Unassigned	[IANA]
140-252		Use for experimentation and testing	[RFC3692]
253		Use for experimentation and testing	[RFC3692]
254	Reserved		[IANA]
255	Reserved		[IANA]

Appendix E Invalid IP Address Definition

Table E-4 Invalid IP Address Definition

Restrictions	Range	Descriptions
Format error	x.x.x.255 0.x.x.x x.x.x.0	This indicates the invalid IP format
Reserved	224.0.0.0~239.255.255.255 127.0.0.0~127.255.255.255 172.31.254.0 ~ 172.31.254.67	This indicates the IP addresses to be reserved for specific usage, such as NME IP, UGE IP, gateway IP, Root-IP and interface IP.
Multicast	224.0.1.0~239.255.255.255	This indicates the IP addresses to be reserved for the multicast application, such as IGMP, video on demand (MOD).
Netmask	255.255.255.254 255.255.255.255 255.0.0.1 0.0.0.0	This indicates the IP addresses to be reserved for IP netmask.

This page is leave in blank for note or memo use

Appendix FMIB files of DAS4 Series

Table F-5 The mapping of ADSL line profile related parameters and their corresponding OID

Parameters	MIB File	OID-number	OID-Name	Task
Profile Name	rfc2662	.1.3.6.1.2.1.10.94.1.1.14.1.1	adslLineConfProfileName	This specifies the ADSL line profile name Type: Mandatory Valid values: String of up to 32 characters ('0'-'9', 'A'-'Z', 'a'-'z', '-', '_', '!', '@').
Upstream Min Rate	rfc2662	.1.3.6.1.2.1.10.94.1.1.14.1.25 or .1.3.6.1.2.1.10.94.1.1.14.1.26	adslAturChanConfFastMinTxRate (see Note ¹) or adslAturChanConfInterleaveMinTxRate (see Note ²)	Defines upstream minimum transmit rate, this parameter is available for adaptive and dynamic rate mode. Type: Mandatory Valid values: 64 ~ 2976 (multiple of 32 kbps) Default value: 64 kbps (due to profile generated)
Upstream Max Rate	rfc2662	.1.3.6.1.2.1.10.94.1.1.14.1.27 or .1.3.6.1.2.1.10.94.1.1.14.1.28	adslAturChanConfFastMaxTxRate (see Note 1) or adslAturChanConfInterleaveMaxTxRate (see Note 2)	Defines upstream maximum transmit rate, this parameter is available for adaptive and dynamic rate mode. Type: Mandatory Valid values: 64 ~ 2976 (multiple of 32 kbps) Default value: 64 kbps (due to profile generated)
Downstream Min Rate	rfc2662	.1.3.6.1.2.1.10.94.1.1.14.1.11 or .1.3.6.1.2.1.10.94.1.1.14.1.12	adslAtucChanConfFastMinTxRate (see Note 1) or adslAtucChanConfInterleaveMinTxRate (see Note 2)	Defines downstream minimum transmit rate, this parameter is available for adaptive and dynamic rate mode. Type: Mandatory Valid values: 64 ~ 29984 (multiple of 32 kbps) Default value: 64 kbps (due to profile generated)
Downstream Max Rate	rfc2662	.1.3.6.1.2.1.10.94.1.1.14.1.13 or .1.3.6.1.2.1.10.94.1.1.14.1.14	adslAtucChanConfFastMaxTxRate (see Note 1) or adslAtucChanConfInterleaveMaxTxRate (see Note 2)	Defines downstream maximum transmit rate, this parameter is available for adaptive and dynamic rate mode. Type: Mandatory Valid values: 64 ~ 29984 (multiple of 32 kbps) Default value: 64 kbps (due to profile generated)
Upstream Min Rate	rfc2662	.1.3.6.1.2.1.10.94.1.1.14.1.25 or .1.3.6.1.2.1.10.94.1.1.14.1.26	adslAturChanConfFastMinTxRate (see Note 1) or adslAturChanConfInterleaveMinTxRate (see Note 2)	Defines upstream transmit rate, this parameter is available for fixed rate mode. Type: Mandatory Valid values: 64 ~ 2976 (multiple of 32 kbps) Default value: 64 kbps (due to profile generated)
Downstream Min Rate	rfc2662	.1.3.6.1.2.1.10.94.1.1.14.1.11 or .1.3.6.1.2.1.10.94.1.1.14.1.12	adslAtucChanConfFastMinTxRate (see Note 1) or adslAtucChanConfInterleaveMinTxRate (see Note 2)	Defines downstream transmit rate, this parameter is available for fixed rate mode. Type: Mandatory Valid values: 64 ~ 29984 (multiple of 32 kbps) Default value: 64 kbps (due to profile generated)
Upstream Downshift Time	rfc2662	.1.3.6.1.2.1.10.94.1.1.14.1.24	adslAturConfMinDownshiftTime	It defines the minimum time interval during which the upstream noise margin should stay below the Downshift SNR below the ATU-R triggers the SRA process to decrease the line rate. Type: Mandatory Valid values: 0 ~ 16384 (seconds) Default value: 0 sec (due to profile generated)
Upstream Upshift Time	rfc2662	.1.3.6.1.2.1.10.94.1.1.14.1.23	adslAturConfMinUpshiftTime	It defines the minimum time interval during which the upstream noise margin should stay above the Upshift SNR before the ATU-R triggers the SRA process to increase the line rate. Type: Mandatory Valid values: 0 ~ 16384 (seconds) Default value: 0 sec (due to profile generated)
Downstream Downshift Time	rfc2662	.1.3.6.1.2.1.10.94.1.1.14.1.10	adslAtucConfMinDownshiftTime	It defines the minimum time interval during which the downstream noise margin should stay below the Downshift SNR before the ATU-C

¹Note . Applicable when the channel mode is fast path.²Note . Applicable when the channel mode is interleaved path.

³Note . Applicable when applying to set the upstream SNR margin.

⁴Note . Applicable when applying to set the downstream SNR margin.

Table F-6 **The mapping of PM Threshold profile related parameters and their corresponding
OID**

Parameters	MIB File	OID-number	OID-Name	Task
Name	rfc2662	.1.3.6.1.2.1.10.94.1.1.15.1.1	adslLineAlarmConfProfileName	This specifies the PM Threshold (performance alarm) profile name Type: Mandatory Valid values: String of up to 32 characters ('0'-'9', 'A'-'Z', 'a'-'z', '-', '_', ',', '@').
15-Min/CO: ES or 15-Min/RT: ES	rfc2662	.1.3.6.1.2.1.10.94.1.1.15.1.6 or .1.3.6.1.2.1.10.94.1.1.15.1.15	adslAtucThresh15MinESs or adslAturThresh15MinESs	When the keyword “near” is set, This field indicates the threshold of Errored Seconds (ES) on the CO (Central Office) side during the last 15 minutes. 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. When the keyword “far” is set, This field indicates the threshold of Errored Seconds (ES) on the RT side (CPE) during the last 15 minutes. 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. Type: Mandatory Valid values: 0 ~ 900 Default value: 0 (due to profile generated)
15-Min/CO: SES or 15-Min/RT: SES	rfc3440	.1.3.6.1.2.1.10.94.3.1.23.1.2 or .1.3.6.1.2.1.10.94.3.1.23.1.4	adslAtucThreshold15MinSesL or adslAturThreshold15MinSesL	When the keyword “near” is set, This field indicates the threshold of Errored Seconds (SES) on the CO (Central Office) side during the last 15 minutes. 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. When the keyword “far” is set, This field indicates the threshold of Severely Errored Seconds (SES) on the RT side (CPE) during the last 15 minutes. 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. Type: Mandatory Valid values: 0 ~ 900 Default value: 0 (due to profile generated)
15-Min/CO: UAS or 15-Min/RT: UAS	rfc3440	.1.3.6.1.2.1.10.94.3.1.23.1.3 or .1.3.6.1.2.1.10.94.3.1.23.1.5	adslAtucThreshold15MinUasL or adslAturThreshold15MinUasL	When the keyword “near” is set, This field indicates the threshold of Unavailable Seconds (UAS) on the CO (Central Office) side during the last 15 minutes. 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. When the keyword “far” is set, This field indicates the threshold of Unavailable Seconds (UAS) on the RT side (CPE) during the last 15 minutes. 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. Type: Mandatory Valid values: 0 ~ 900 Default value: 0 (due to profile generated)
1-Day/CO: ES or	askeyADSL	.1.3.6.1.4.1.3646.1300.2.2.1.1.1. 1 or	adslAtucThreshold1DayEsL or	When the keyword “near” is set, This field indicates the threshold of

Table F-7 The mapping of Traffic Policing profile related parameters and their corresponding OID

Parameters	MIB File	OID-number	OID-Name	Task
Name	ASKEY-QOS-MIB	.1.3.6.1.4.1.3646.1300.2.16.3.1.1.1	trafficPolicingName	This specifies the traffic policing profile name Type: Mandatory Valid values: String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
Upstream CIR (Mbps)	ASKEY-QOS-MIB	.1.3.6.1.4.1.3646.1300.2.16.3.1.1.2	trafficPolicingCIR	Defines the committed information rate of traffic policing profile. Type: Mandatory Valid values: 1 ~ 1000 (mbps)
Action to Out-profile Packets	ASKEY-QOS-MIB	.1.3.6.1.4.1.3646.1300.2.16.3.1.1.4	trafficPolicingAction	This identifies to which value will DSCP be replace, drop packets or do nothing when user's upstream traffic exceeds CIR. Type: Mandatory Valid values: no-action(0) drop(1) BE(2) AF11(3) AF12(4) AF13(5) AF21(6) AF22(7) AF23(8) AF31(9) AF32(10) AF33(11) AF41(12) AF42(13) AF43(14) EF(15)

Table F-8 The mapping of ADSL port configuration parameters and their corresponding OID

Parameters	MIB File	OID-number	OID-Name	Task
Administrative State	rfc2233	.1.3.6.1.2.1.2.2.1.7	ifAdminStatus	This specifies the desired state of the interface. Type: Mandatory Valid values: Enable Disable
Line Profile	rfc2662	.1.3.6.1.2.1.10.94.1.1.1.1.4	adslLineConfProfile	This specifies the ADSL line profile name Type: Mandatory Valid values: String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
PM Threshold (Profile)	rfc2662	.1.3.6.1.2.1.10.94.1.1.1.1.5	adslLineAlarmConfProfile	This specifies the PM Threshold (performance alarm) profile name Type: Mandatory Valid values: String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
Traffic Policing (Profile)	ASKEY-QOS-MIB	.1.3.6.1.4.1.3646.1300.2.16.1.1.1.1	askeyQoSLineTrafficPolicing	This specifies the traffic policing profile name Type: Mandatory Valid values: String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').

Table F-9 The mapping of IP Traffic profile related parameters and their corresponding OID

Parameters	MIB File	OID-number	OID-Name	Task
Name	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.2.2.1.1	ipTrafficProfileName	This specifies the IP traffic profile name Type: Mandatory Valid values: String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
Upstream Rate (Kbps)	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.2.2.1.2	ipTrafficProfileUsRateLimit	This specifies the rate limit for the upstream IP traffic on the PVC of a specific ADSL port where the IP traffic profile is applied to. Type: Mandatory Valid values: nolimit 32k 64k 128k 256k 384k 512k 768k
Downstream Rate (Kbps)	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.2.2.1.3	ipTrafficProfileMaxDsRate	This specifies the rate limit for the downstream IP traffic on the PVC of a specific ADSL port where the IP traffic profile is applied to. Type: Mandatory Valid values: 0 ~ 29984 kbps (multiple of 32 kbps)
Downstream Priority Queue	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.2.2.1.4	ipTrafficProfileDsPriority	This defines the downstream priority of the PVC of a specific ADSL port where the IP traffic profile is applied to. It is noted that the lower the priority of the applied PVC, the higher the chance to get drop due to traffic congestion. Type: Mandatory Valid values: low(0) medium(1) high(2) highest(3)
Downstream Broadcast	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.2.2.1.6	ipTrafficProfileDsBcastFilter	This specifies to drop or to forward downstream broadcast on the PVC of a specific ADSL port where the IP traffic profile is applied to. Type: Mandatory Valid values: drop(2) forward(3)

Table F-10 The mapping of xDSL VC-to-VLAN Setting related parameters and their corresponding OID

Parameters	MIB File	OID-number	OID-Name	Task
VPI	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.1	vcVlanEntryVpi	Defines the VPI (Virtual Path Identifier) value. Type: Mandatory Valid values: 0 ~ 255
VCI	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.2	vcVlanEntryVci	Defines the VCI (Virtual Channel Identifier) value. Type: Mandatory Valid values: 1 ~ 65535 (1 ~ 31 are reserved)
Administrative State	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.13	vcVlanEntryRowStatus	This specifies the desired state of the vc-vlan connection. Type: Mandatory Valid values: Enable Disable
RFC2684 Mode	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.6	vcVlanEntryRfc2684Mode	This specifies the RFC2684 encapsulation mode for the packet on the PVC. Type: Mandatory Valid values: routed mode bridged mode
IP Traffic Profile	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.8	vcVlanEntryIPTrafficProfile	Defines the created IP traffic profile name. Type: Mandatory Valid values: The name of “IP traffic profile”
802.1Q/IP: VLAN ID	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.3	vcVlanEntryVlanId	This specifies the VLAN-ID value of VLAN-tag to be added to the upstream traffic on the PVC. Type: Mandatory Default value: 1 Valid values: 1 ~ 4093
802.1Q/IP: User Priority	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.4	vcVlanEntry8021pPriority	This specifies the User Priority of VLAN-tag to be added to the upstream traffic on the PVC when it is in the RFC 2684 bridged mode. Type: Mandatory Default value: 0 Valid values: 0 ~ 7 (low ~ high)
802.1P: User Priority	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.4	vcVlanEntry8021pPriority	This specifies the User Priority of VLAN-tag to be added to the upstream traffic on the PVC when it is in the RFC 2684 routed mode. Type: Mandatory Default value: 0 Valid values: 0 ~ 7 (low ~ high)
Next-hop Name	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.7	vcVlanEntryRoutedModeNexthop	It specifies the Next-hop name. The NE will use ARP to get its corresponding MAC address. The NE then use this MAC address as the MAC DA of upstream Ethernet frame when the VC-VLAN connection is in the RFC 2684 routed mode. Type: Mandatory Valid values: The name of “ISP Server”
MAC Limit: MAC Count	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.5	vcVlanEntryMacLimit	Defines the limit of MAC address learned on the applied PVC when it is in the RFC 2684 bridged mode. It is noted that each xDSL line port allows maximum of 8 MAC addresses to be learned. Type: Mandatory Default value: 1 Valid values: 1 ~ 8
Service Type	askeyVcVlan	.1.3.6.1.4.1.3646.1300.2.11.1.1.9	vcVlanEntryServiceType	This specifies the service type to

Table F-11 The mapping of TV Channel Profile related parameters and their corresponding OID

Parameters	MIB File	OID-number	OID-Name	Task
Profile ID	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.1.2.1.1	mProfileId	This specifies the multicast channel profile identifier. Type: Mandatory Valid values:
Name	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.1.2.1.2	mProfileName	This specifies the multicast channel profile name Type: Mandatory Valid values: String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
TV Channel IP Address	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.1.2.1.3	mProfileIpAddr	This specifies class D IP address of the multicast stream. Type: Mandatory Valid values: 224.0.1.0 ~ 239.255.255.255
Priority Queue	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.1.2.1.5	mProfilePriority	Defines the downstream forwarding priority of the multicast stream. Type: Mandatory Valid values: low(0) medium(1) high(2) highest(3)
Downstream Rate (Kbps)	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.1.2.1.4	mProfileRate	Defines the downstream transmission rate limit of multicast stream. Type: Mandatory Valid values: 0 ~ 29984 kbps

Table F-12 The mapping of Multicast Service Profile related parameters and their corresponding OID

Parameters	MIB File	OID-number	OID-Name	Task
Name	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.3.2.1.1	mcastServiceProfileName	This specifies the multicast service profile name Type: Mandatory Valid values: String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
TV Channel	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.3.2.1.2	mcastServiceProfileBitMap	This specifies the multicast group profile name. Each service profile may book a set of 800 program at most , we use 100 octets to save what it books. Type: Mandatory Valid values: String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').

Table F-13 The mapping of Multicast Channel Configuration related parameters and their corresponding OID

Parameters	MIB File	OID-number	OID-Name	Task
VPI	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.2.1.1	mConfigVpi	Defines the VPI (Virtual Path Identifier) value for multicast channel. Type: Mandatory Default value: 8 Valid values: 0 ~ 255
VCI	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.2.1.2	mConfigVci	Defines the VCI (Virtual Channel Identifier) value for multicast channel.. Type: Mandatory Default value: 35 Valid values: 1 ~ 65535 (1 ~ 31 are reserved)
VLAN ID	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.2.1.3	mConfigVlanId	This specifies the VLAN-ID value of VLAN-tag to be added to the upstream IGMP report packets on the PVC. Type: Mandatory Default value: 1 Valid values: 1 ~ 4093
Administrative State	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.2.1.6	mConfigRowStatus	This specifies the desired state of the interface. Type: Mandatory Valid values: Enable Disable
Multicast Service Profile	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.2.1.5	mConfigServiceProfile	This specifies the multicast service profile. Internally, each line may book 256 program set, we use 256 bits to save what they booked Type: Mandatory Valid values: String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
Channel Limit: Channel Limit	askeyMcast	.1.3.6.1.4.1.3646.1300.2.5.2.1.4	mConfigStreamNum	This specifies the allowed number of multicast streams to be forwarded via the VC-to-VLAN connection. Type: Mandatory Valid values: 1~ 5

Table F-14 The mapping of IGMP snooping/IGMP proxy Configuration related parameters and their corresponding OID

Parameters	MIB File	OID-number	OID-Name	Task
Disable IGMP snooping and IGMP proxy / Enable IGMP snooping / Enable IGMP proxy	askeySystemMib	.1.3.6.1.4.1.3646.1300.2.1.16.3	askeySystemManagementIgm p	These three parameters correspond to the same OID “askeySystemManagementIgm p” As their names imply, the operator selects one among them. Type: Mandatory Valid values: enableIgm snoop(1), enableIgm pproxy(2), disableIgm p(3)
Enable IGMP snooping: MAC Aging Time (seconds)	askeyIgm pSnoop	.1.3.6.1.4.1.3646.1300.2.3.1.3	askeyMcastAgingTime	Defines the IGMP snooping aging time which the timeout period in seconds for aging out Multicast Groups dynamically learned with IGMP Snooping. Note that aging operates on a per interface per VLAN per multicast group basis. This interval is also used to age out ports that have received IGMP Router Query PDUs on a per VLAN basis. Type: Mandatory Valid values: 30 ~ 3600 (sec.) Default value: 300 (sec.)
Enable IGMP proxy: Robustness(Query Retry)	askeyIGM pprox y	.1.3.6.1.4.1.3646.1300.2.14.2	askeyIgm pProxyRobust	Defines the retry count for the NE to re-send IGMP Query message to the subscriber in the case that the subscriber does not respond. After sending “retry count” of IGMP Query messages, if he NE does not receive any response, the NE will treat the subscriber as ‘leave’ and hence will stop forwarding the multicast stream to the particular link. Type: Mandatory Valid values: 1 ~ 5 Default value: 3 (count.)
Enable IGMP proxy: Query Response Interval	askeyIGM pprox y	.1.3.6.1.4.1.3646.1300.2.14.3	askeyIgm pProxyQueryInterva l	This specifies the period between the NE send 2 consecutive IGMP queries to the xDSL subscriber. Type: Mandatory Valid values: 1 ~ 30 (sec.) Default value: 30 (sec.)
Enable IGMP proxy: Immediate Leave	askeyIGM pprox y	.1.3.6.1.4.1.3646.1300.2.14.4	askeyIgm pProxyImmediatedL eaveEnable	This specifies to enable the “immediate leave” function or not.. Type: Mandatory Valid values: Enable Disable

Table F-15 The mapping of Trunk CoS Mapping and DSCP Re-mapping related parameters and their corresponding OID

Parameters	MIB File	OID-number	OID-Name	Task
User Priority	askeySystemMib	.1.3.6.1.4.1.3646.1300.2.1.18.1.1.1	askeyCosQueueMapping8021p	This indicates the 802.1p user priority as configured in the VC-to-VLAN configuration Type: Mandatory Valid values: 0~7
Queue (Traffic Class)	askeySystemMib	.1.3.6.1.4.1.3646.1300.2.1.18.1.1.2	askeyCosQueueIndex	For a specified User Priority (802.1p) value of received Ethernet packet, this indicates the corresponding CoS queue on the uplink trunk GE port Type: Mandatory Valid values: 1~8
DiffServ Code Point (DSCP)	ASKEY-QOS-MIB	.1.3.6.1.4.1.3646.1300.2.16.2.2.1.1	diffServDSCP	For a specified User Priority (802.1p) value of received subscriber's Ethernet packet, this indicates the new DSCP value on the subscriber's IP frame to be forwarded via the uplink trunk GE port. Type: Mandatory Valid values: be (0), af11 (1), af12 (2), af13 (3), af21 (4), af22 (5), af23 (6), af31 (7), af32 (8), af33 (9), af41 (10), af42 (11), af43 (12), ef (13)
Administrative State	ASKEY-QOS-MIB	.1.3.6.1.4.1.3646.1300.2.16.2.1	diffServAdminStatus	Enable or disable the DSCP Re-mapping function. Type: Mandatory Valid values: Enable(0) Disable(2)