DAS3 Series Web Management

Operation Guide

Class:	Operation Guide
Product Version:	S.W. R2.5, Internet Explorer 6.0
Doc. No.:	BCD3-TM-E-120502
Doc. Version:	2.0
Publish Date:	2008-10-31

DAS3 Series Web Management
Operation Guide
Text Part Number: 1205-0220

Table of Contents

List of Figures

List of Tables

This page is leave in blank for note or memo use

Preface

This preface discusses the following topic:

- Purpose
- Organization
- Conventions

Purpose

The purpose of this guide is to provide detailed information and description of DAS3 Series IP-DSLAM web management, which includes web interface configuration and other specific features.

Organization

This guide contains the following information:

- Preface
- Getting Started Web Management
- System Menu
- Status and Performance
- Deployment Menu
- Access Control
- Protocol Menu
- Diagnostic Menu
- Abbreviations and Acronyms

Conventions

This publication uses the document conventions listed in this section.

NE/NEs mention in this document means DAS3 Series IP-DSLAM

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

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

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

This sign indicate 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.

This page is leave in blank for note or memo use

Chapter 1Getting Started Web Management

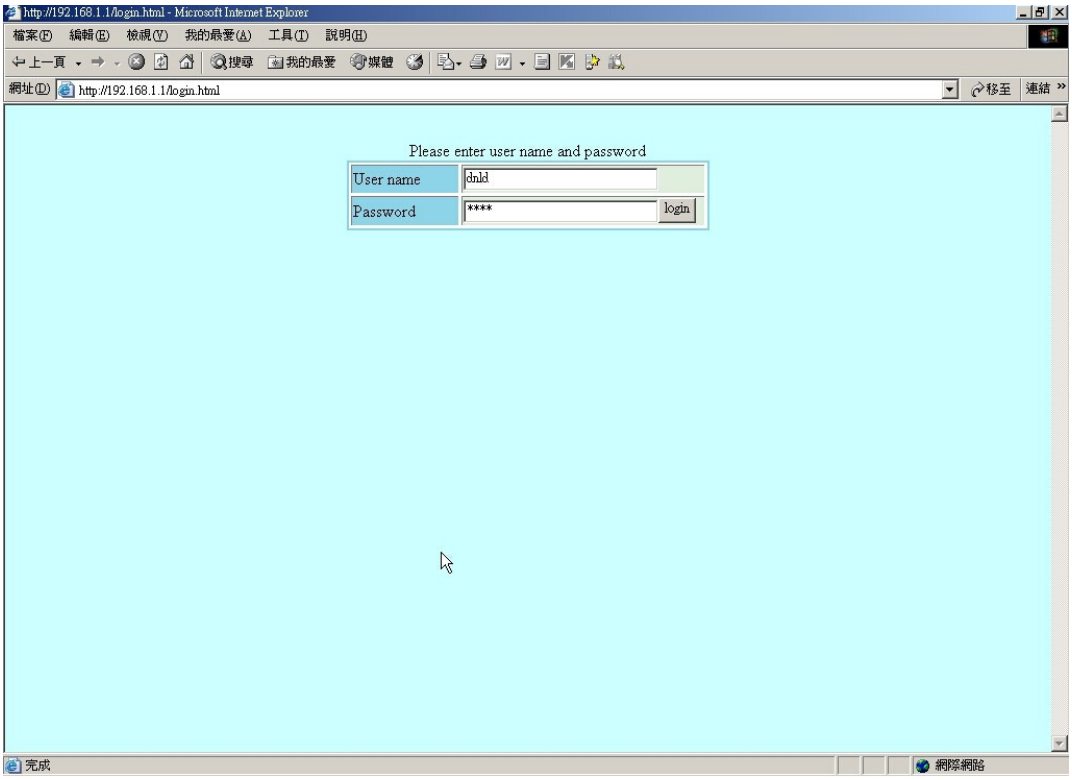
This chapter provides the descriptions to start the web management in your network.
This chapter contains the following sections:

- Login Window
- Operation Window Overview

Login Window

Launch your web browser, and go to http://192.168.1.1 via management port. The following screen appears.
The login window to use User name/Password = **Admin** / **Admin** then click “login” button to login.

Figure 2-1 DAS3 Series Web Management Login Window



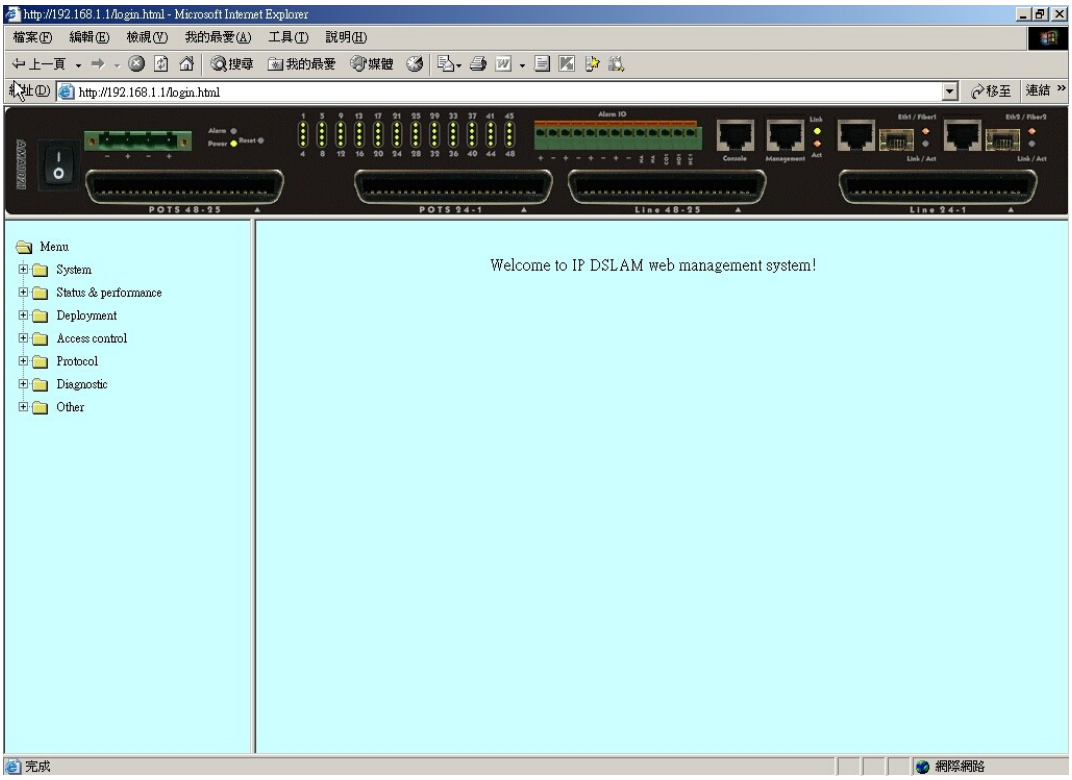
Even though you can connect to the IP-DSLAM Eth1/Fiber1 (uplink) or Eth2/Fiber2 (downlink), it is recommended that you connect your computer to management port for initial configuration.

The DAS3 Series web management login User name/Password = **Admin** / **Admin** of default value.

Operation Window Overview

The DAS3 Series web management window contains main menu, operate window and real-time LED status panel.

Figure 2-2 DAS3 Series Web Management Operation Window



Chapter 2System Menu

This chapter provides the detail system menu that contains data information of web managed agent (DAS3 Series). This chapter contains the following sections:

- General Information
- Statistics Information
- User and Password
- Bridge Mode
-
- Firmware Upgrade
- Commit and Reboot
- Hardware Information

General Information

You can edit the system information in this dialog.

Figure 3-3 System General Information Dialog

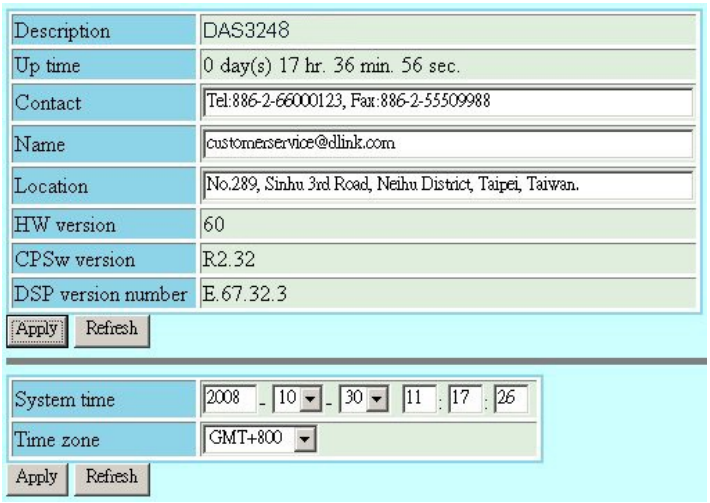


Table 3-1 describes the general information dialog field items.

Table 3-1 Modifying the System Information

Item	Description
System Description	This is a text description of the entity.
System Up Time (HH:MM:SS)	This shows the time in seconds since the system is up.
System Contact with us	This specifies the textual identification of the contact person for this managed node, together with the information on how to contact this person. **Valid values:** String of up to 100 characters (‘A’ – ‘Z’, ‘a’ – ‘z’, ‘0’ – ‘9’, ‘-’, ‘_’) and any combination of printable characters excluding ‘;’.

Table 3-1 Modifying the System Information

Item	Description
System administratively-assigned name	This specifies administrator-specific information. **Valid values:** String of up to 100 characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_') and any combination of printable characters excluding ';'.
System Location	This specifies the physical location of this node. **Valid values:** String of up to 100 characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_') and any combination of printable characters excluding ';'.
System Vendor Information	This indicates the vendor-specific information. **Valid values:** String of up to 100 characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_') and any combination of printable characters excluding ';'.
Hardware version	This indicates the hardware and firmware information.
Version of the control plane software	This indicates the software version of control plane.
DSP code version	The Version number of Digital Signal Processor

Statistics Information

The statistics information dialog monitors current system network status.

Figure 3-4 System Statistics Information Dialog

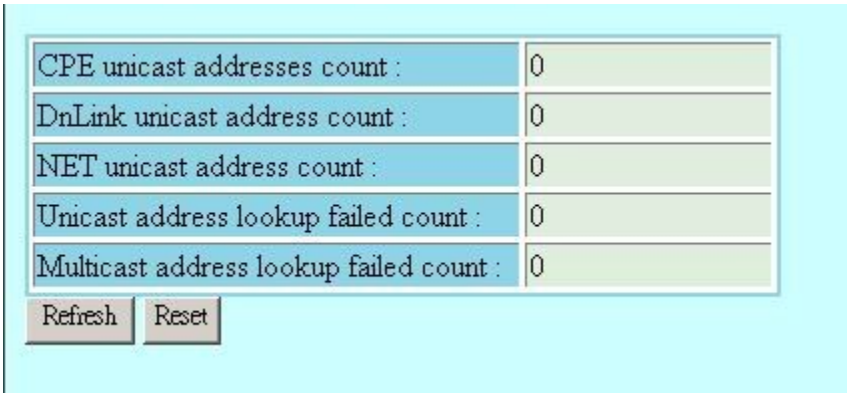


Table 3-2 describes the system (DAS3 Series) statistics information.

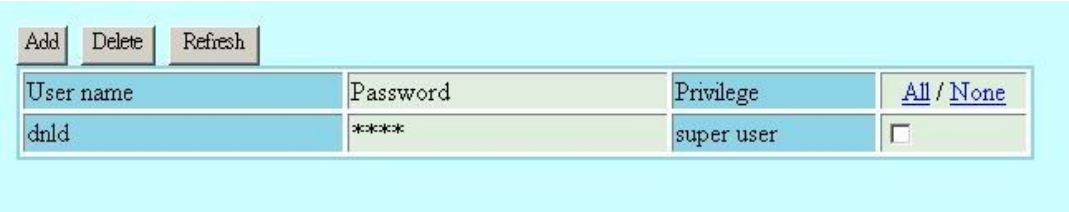
Table 3-2 Monitoring the System Statistics Information

Item	Description
CPE Ucast Addr Count	Number of unicast addresses, which were learned from the CPE ports.
DnLink Ucast Addr Count	Number of unicast addresses, which were learned from the downlink port.
Net Ucast Addr Count	Number of unicast addresses, which were learned from the network ports.
Ucast Lookup Fail Count	Number of times unicast address lookup failed.
Mcast Lookup Fail Count	Number of times multicast address lookup failed.

User and Password

The User and Password Dialog window displays information of all the users. Password is hidden in '*'.

Figure 3-5 User & Password Dialog



Click 'Add' button to create a new user.

Figure 3-6 Add New User Dialog

Two users can be adding to a single DAS3 Series IP-DSLAM.

The users manage in here are only for Telnet access, the '**super user**' owns full privilege while '**user**' has only monitoring privilege.

Table 3-3 Configuring the Add New User

Item	Description
User Name	This specifies the user name to be created. **Valid values:** String of up to 20 characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_') and any combination of printable characters excluding ';'.
Password	This specifies the password required by this user to login to the unit. **Valid values:** String of up to 20 characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_') and any combination of printable characters excluding ';'.
Privilege	This indicates the privilege level of the user. **super user** – Owns show, add, delete and modify privilege. **user** – Owns show privilege only.

Bridge Mode

The bridge configuration allows you to control the system bridging parameters.

Figure 3-7 Bridge Mode Dialog

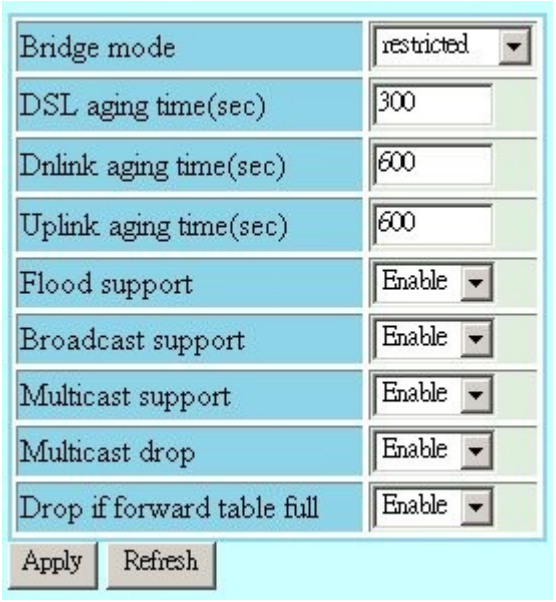


Table 3-4 Bridge Configuration Dialog Description

Item	Description
Bridge mode	This specifies the current state of full bridging on the bridge. The bridge can be set to residential bridging, restricted full bridging or unrestricted full bridging. * **Residential bridging**, all packets from a CPE side port are sent to Net side port without doing a lookup in the forwarding table. * **Restricted bridging**, there is a lookup and a packet coming from a CPE port destined for another CPE port is dropped. Hence, CPE-CPE switching is not permitted. * **Unrestricted bridging**, all traffic is forwarded based on lookup.
Aging Time	The timeout period, in seconds, for aging out dynamically learned forwarding information from CPEs. The value 0 can be configured when aging is to be stopped. **Valid values:** 10 ~ 1,000,000
Uplink Aging Time	The timeout period, in seconds, for aging out dynamically learned forwarding information from uplink side port. This is used only for **full bridge** configuration. The value 0 can be configured when aging is to be stopped. Default is set to 600 sec. **Valid values:** 10 ~ 1,000,000
Dnlink (Slave) Aging Time	The timeout period, in seconds, for aging out dynamically learned forwarding information learned from the downlink device. The value 0 can be configured when aging is to be stopped. Default is set to 600 sec. **Valid values:** 10 ~ 1,000,000
Flood Support	This is used to specify whether the unknown unicast packets are to be flooded or not. The value for this is used along with per VLAN configuration for flood support to determine if flooding has to be done for unknown unicast packet.

Table 3-4 Bridge Configuration Dialog Description

Item	Description
Broadcast Support	This is used to specify whether the broadcasting is supported or not. The value for this is used along with per VLAN configuration broadcast support, to determine if broadcasting has to be done for the broadcast packet.
Multicast Support	Used to specify whether the multicast is supported or not.
Multicast Drop	If multicast is not supported, this setting can specify whether the multicast packets are to be dropped, or to be forwarded.
Drop if Forwarding Table Full	This specifies if the frame for which learning could not be done because of forwarding table limit being reached, is to be dropped. If this is enabled, the frame for which learning could not be done because of limit exceeded shall be dropped, else forwarded based on bridge forwarding logic. This being enabled shall reduce flooding, as when a response to such a frame from which learning could not be done shall come the frame shall be flooded, as the entry for that unicast address, shall not be found in forwarding table.

Backup and Restore

Backup and Restore function allows operator to save current network element configuration. The file will be saved at the folder of local host PC.

Backup Configuration

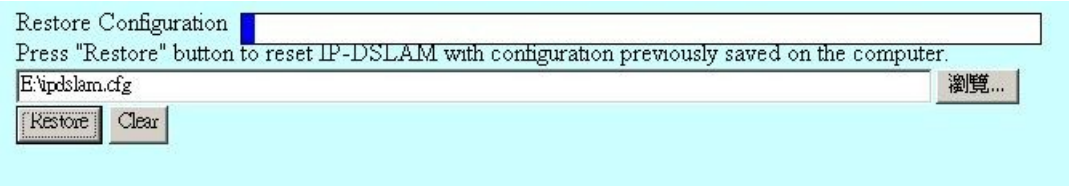
Use Backup Configuration function to save all configured setting from system to exterior device.

Figure 3-8 Backup Configuration Dialog

Restore Configuration

Use Restore Configuration function to retrieve the configuration data from other devices to system.

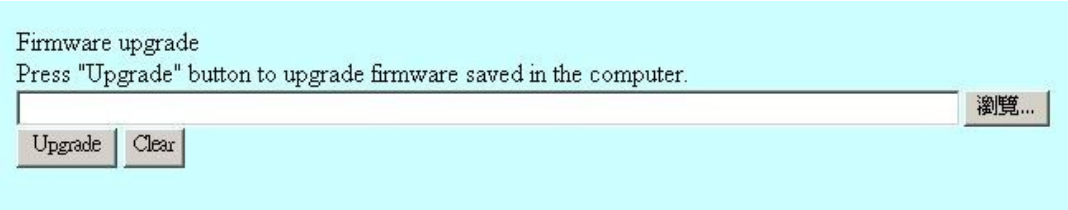
Figure 3-9 Configuration Restore Dialog



Firmware Upgrade

The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three minutes. After a successful upload, the system must reboot.

Figure 3-10 Firmware Upgrade Dialog



The following table describes the labels in this screen.

NOTE The DAS3 Series web management Firmware Upgrade file name must be “TEImage.bin.gz”.

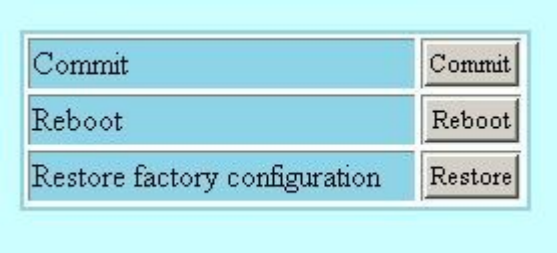
Table 3-5 Firmware Upgrade Description

Item	Description
Browse…	Type in the location of the file you want to upload in this field or click **Browse…** to find the “.bin.gz” file.
Upgrade	Click this to begin the upgrade process. This process may take up to three minutes.
Clear	Click this to clear the location of the file in this field.

Commit and Reboot

The commit and reboot configuration dialog allows you to commit, reboot or restore factory configuration the system.

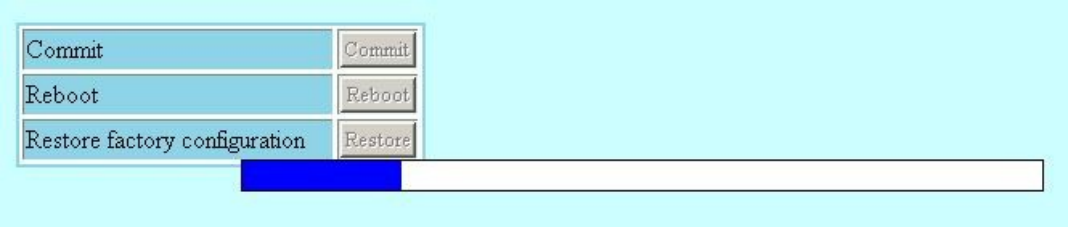
Figure 3-11 Commit & Reboot Configuration Dialog



Commit Configuration

Commit the system to save all configuration information from NVRAM to Flash, all variables change without commit will be lost due to system (hardware) reboot or power-off.

Figure 3-12 System Commit

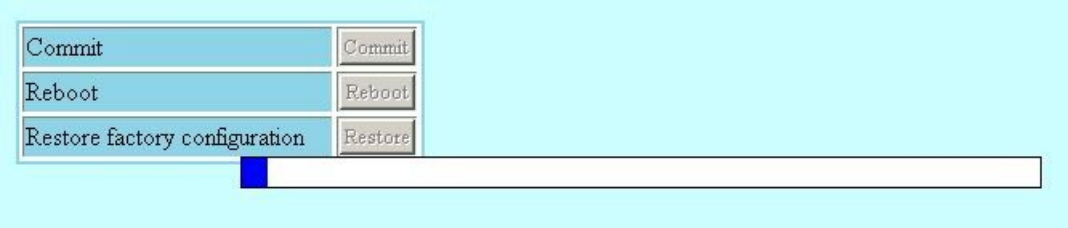


Commit action takes around 20 seconds to accomplish.

Reboot System

Reboot system (restart) takes around 90 seconds to accomplish.

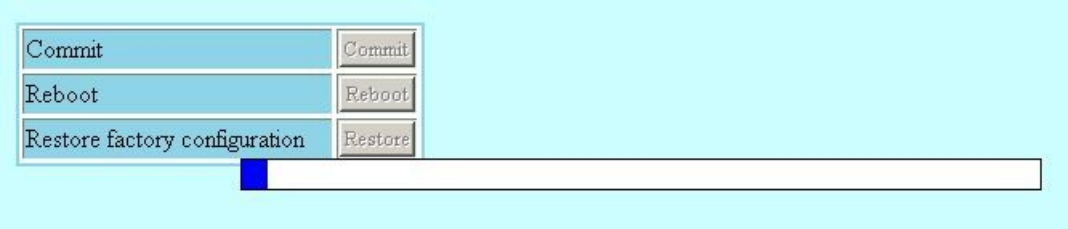
Figure 3-13 System Reboot



Restore Factory Configuration

Use restore factory configuration to restore configuration parameters of factory default values.

Figure 3-14 Restore Factory Configuration



The restore factory default parameters are list in Table 3-6.

Table 3-6 DAS3 Series System Factory Default Parameters

Item	Description
ADSL Layer	
VPCI (VPI/VCI)	8/35 for each ADSL port interface.
Encapsulation	LLCMUX
Standard	ADSL2plus

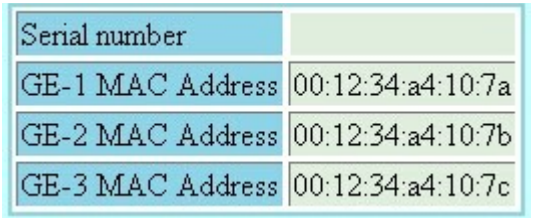
Table 3-6 DAS3 Series System Factory Default Parameters

Item	Description
Bridge Layer and Ethernet IP	
Bridge mode	Restricted bridge mode
Ethernet port 1 IP address	0.0.0.0 / 0.0.0.0, Uplink
Ethernet port 2 IP address	0.0.0.0 / 0.0.0.0, Downlink
Ethernet port 3 IP address	192.168.1.1 / 255.255.255.0, management port
Management	
SNMP community	public (re-write privilege)
SNMP host	192.168.1.2
Telnet, Console and Web management Username / Password	Admin / Admin

Hardware Information

The hardware information dialog monitors Ethernet MAC addresses.

Figure 3-15 Hardware Information Dialog



Chapter 3Status and Performance

In the Status and Performance menu, operator can view the ADSL line performance parameters and Ethernet statistics as well as the ADSL channel performance parameters and Ethernet statistics. This chapter contains the following sections:

- DSL Status
- Layer Information
- PVC Statistics
- Ethernet Statistics
- GBIC Information
- Line 15min Performance
- Line 1day Performance
- Unicast Forwarding Table
- Multicast Forwarding Table
- Alarm Sensor
- Active Alarm
- Active Alarm Log

DSL Status

The line status shows the ADSL line information.

Figure 4-16 DSL Status Dialog

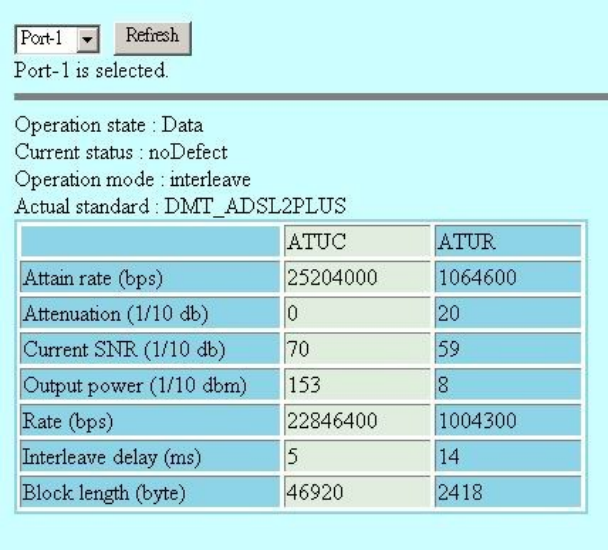


Table 4-7 DSL Status Dialog Description

Item	Description
Port selection menu	Select the ADSL port interface to be display with relative parameters.
Operation state	Operational state of the DSL port.

Table 4-7 DSL Status Dialog Description

Item	Description
Current status	Indicates current state of the DSL line. This is a bit-map of possible conditions.
Operation mode	Operation mode used by the DSL port.
Actual standard	Actual standard used for connection, based on the outcome of the negotiation with the ATU-R
Attain rate (bps)	Indicates the maximum currently attainable data rate by the ATU-x. This value will be equal to, or greater than the current line rate.
Attenuation (1/10 db)	Measured difference in the total power transmitted by the peer ATU-x and the total power received by this ATU-x.
Current SNR (1/10 db)	Noise Margin as seen by this ATU-x with respect to its received signal in tenth dB.
Output power (1/10 dbm)	Measured total output power transmitted by this ATU-x. This is the measurement that was reported during the last activation sequence.
Rate (bps)	Actual transmit rate on this channel.
Interleave delay (ms)	Interleave delay for this channel.
Block length (byte)	Indicates the length of the channel data-block, on which the CRC operates.

Layer Information

The Layer Information will display ATM and Channel layer information.

Figure 4-17 Layer Information Dialog

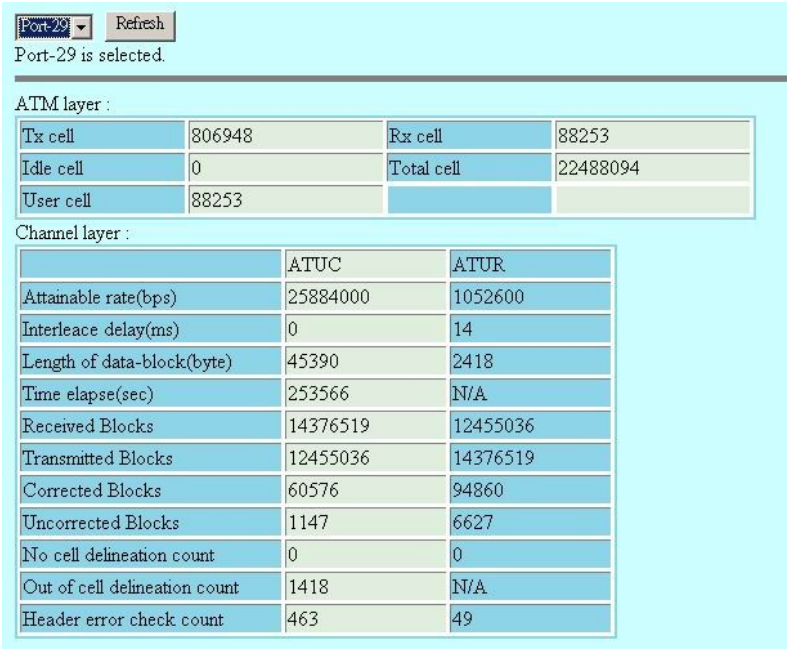


Table 4-8 Layer Information Dialog Description

Item	Description
Port selection menu	Select the ADSL port interface to be display with relative parameters.
Tx cell	Provides Tx ATM cell counter.
Rx cell	Provides Rx ATM cell counter.
Idle cell	Number of idle cells.
Total cell	Number of total cell
User cell	Number of user cell
Attain rate (bps)	Indicates the maximum currently attainable data rate by the ATU-x. This value will be equal to, or greater than the current line rate.
Interleave delay (ms)	Interleave delay for this channel.
Block length (byte)	Indicates the length of the channel data-block, on which the CRC operates.
Time elapse (sec)	Total time elapsed in seconds.
Received Blocks	Count of all encoded blocks received on this channel since agent was reset.
Transmitted Blocks	Count of all encoded blocks transmitted on this channel since agent was reset.
Corrected Blocks	Count of all encoded blocks received with corrected error on this channel since agent reset.
Uncorrected Blocks	Count of all encoded blocks received with uncorrected error on this channel since agent was reset.
No cell delineation count	Number of packets with NCD (No Cell Delineation) error.
Out of cell delineation count	Number of packets with OCD (Out of Cell Delineation) error.
Header error check count	Number of packets with HEC (Header Error Check) error.

PVC Statistics

PVC statistics will display input output frame information for vpi/vci of each port.

Figure 4-18 PVC Statistics Dialog

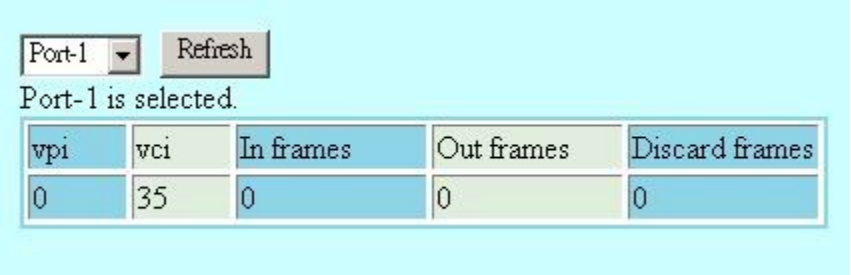


Table 4-9 PVC Statistics Description

Item	Description
VPI/VCI	This indicates the VPI/VCI of the specified entry.
In frames	The number of frames that have been received by this port from its segment.
Out frames	The number of frames that have been transmitted by this port from its segment.
Discard frames	Count of valid frames received, which were discarded (i.e., filtered) by the Forwarding Process.

Ethernet Statistics

The Ethernet interface statistics allows you to check the packets information of selected Ethernet port.

Figure 4-19 Ethernet Statistics Dialog

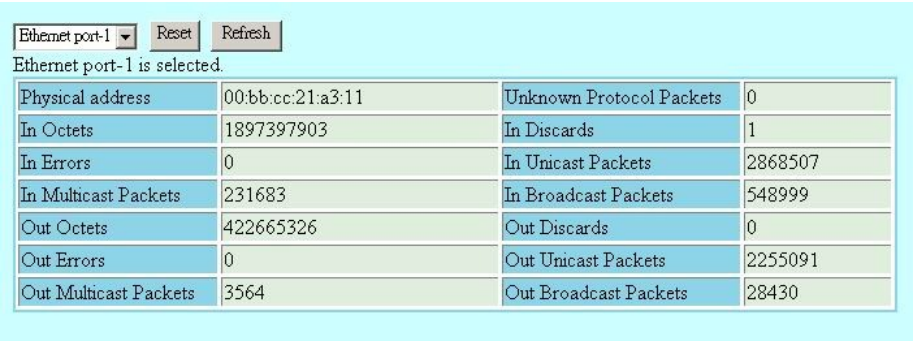


Table 4-10 Ethernet Statistics Dialog Description

Item	Description
Ethernet port selection menu	Select the Ethernet interface to display relative parameters.
Physical address	The MAC address used by this Ethernet interface, when it must be referred to, in a unique fashion.
Unknown Protocol Packets	The number of packets received by the interface, which were discarded because

Table 4-10 Ethernet Statistics Dialog Description

Item	Description
	of an unknown or unsupported protocol.
In Octets	The total number of octets received on the interface, including the framing characters. For Ethernet interface, this will have the lower 32 bits of HC in octets.
Out Octets	The total number of octets transmitted out the interface, including the framing characters. For Ethernet interface, this will have the lower 32 bits of HC out octets.
In Discards	The number of inbound packets, which were discarded, though no errors were detected.
Out Discards	The number of outbound packets chosen to be discarded even though there were no errors.
In Errors	The number of inbound packets, which were not delivered to upper layers because of errors.
Out Errors	The number of outbound packets to be discarded because there were errors.
In Unicast Packets	The number of unicast packets delivered to a higher layer protocol.
Out Unicast Packets	The number of packets requested to be sent to unicast addresses, by upper layer protocol.
In Multicast Packets	The number of multicast packets delivered to a higher layer protocol.
Out Multicast Packets	The number of packets requested to be sent to multicast addresses, by upper layer protocol.
In Broadcast Packets	The number of broadcast packets delivered to a higher layer protocol.
Out Broadcast Packets	The number of packets requested to be sent to broadcast addresses, by upper layer protocol.

GBIC Information

View the current status of small form-factor pluggable (SFP) in GE ports.

Figure 4-20 GBIC Information Dialog

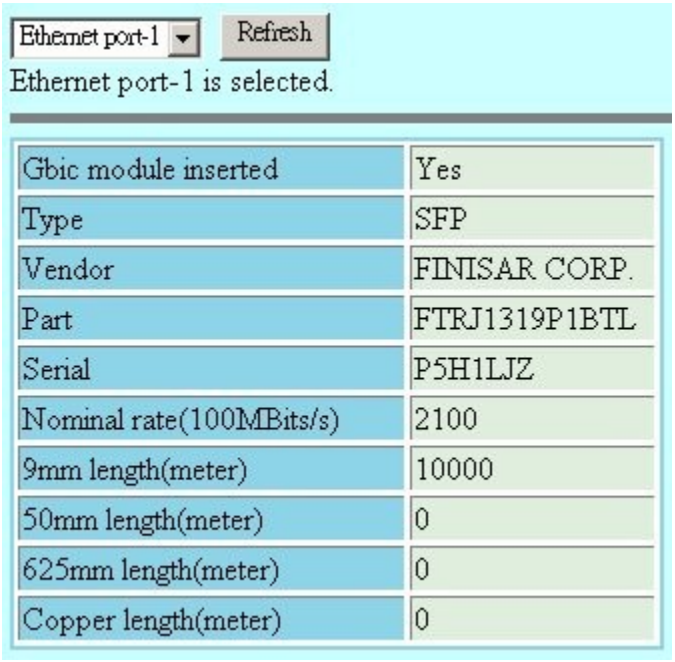


Table 4-11 GBIC Information Description

Item	Description
GBIC module inserted	It indicates whether the GBIC module inserted or not.
Type	It indicates the type specifies the physical device.
Vendor	It indicates the full name of the corporation, a commonly abbreviation of the corporation name will be accepted.
Part	It indicates the vendor part number or product name.
Serial	It indicates the vendor serial number for the GBIC.
Nominal rate(100MBits/s)	It indicates the nominal bit rate (BR, nominal) in units of 100 Megabits per second, rounded off to the nearest 100 Megabits per second.
9mm Length(meter)	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 millimeter.
50mm Length(meter)	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.
625mm Length(meter)	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(meter)	It indicates the minimum link length that is supported by the GBIC while operating in compliance with the applicable standards using copper cable.

Line 15min Performance

The ATU line 15min performance data represents line performance related data for a particular channel associated with a particular ATU-C/ATU-R.

Figure 4-21 ADSL Line 15min Performance Dialog

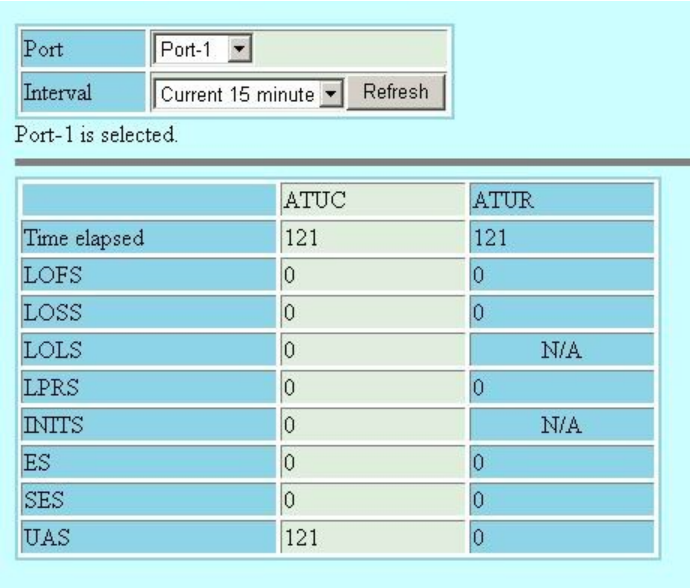


Table 4-12 Line 15min Performance Dialog Description

Item	Description
Port selection menu	Select the ADSL port interface to display relative parameters.
LOFS	Loss of Frame Second. This specifies the second which no corrected frame is received.
LOSS	Loss of Signal Second. This specifies the second which no signal is received.
LOLS	Loss of Link Second. This specifies the second which the link appears to be failed.
LPRS	Loss of Power Resource Second. This specifies the second which the power is cut off.
ES	Error Second. This specifies the second which error occurs and can not be recovered from CRC bit.
INITS	Initialization Second. This specifies the second which initialization has occurred.
SES	Severely Error Second. This specifies the second which LOS, LOF, LOL have occurred.
UAS	Unavailable Second. This specifies the second which the link is abnormal for 10 seconds.

Line 1day Performance

The ATU line 1day performance data represents line performance related data for a particular channel associated with a particular ATU-C/ATU-R.

Figure 4-22 ADSL Line 1day Performance Dialog

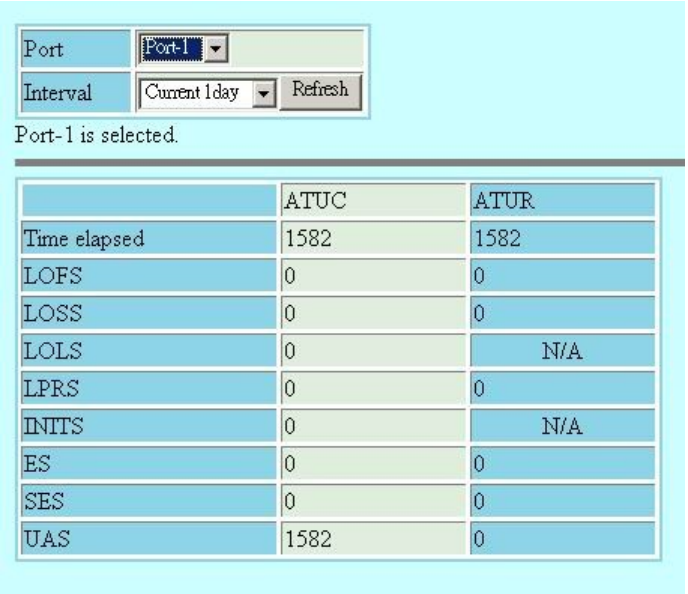


Table 4-13 Line 1day Performance Dialog Description

Item	Description
Port selection menu	Select the ADSL port interface to display relative parameters.
LOFS	Loss of Frame Second. This specifies the second which no corrected frame is received.
LOSS	Loss of Signal Second. This specifies the second which no signal is received.
LOLS	Loss of Link Second. This specifies the second which the link appears to be failed.
LPRS	Loss of Power Resource Second. This specifies the second which the power is cut off.
ES	Error Second. This specifies the second which error occurs and can not be recovered from CRC bit.
INITS	Initialization Second. This specifies the second which initialization has occurred.
SES	Severely Error Second. This specifies the second which LOS, LOF, LOL have occurred.
UAS	Unavailable Second. This specifies the second which the link is abnormal for 10 seconds.

Unicast Forwarding Table

The unicast forwarding table of DAS3 Series system stores the following MAC entries

- The manually configured MAC addresses on an ADSL port.
- The MAC addresses learned from the associate ADSL port.
- The MAC addresses learned from the GE1 (uplink GE port) or GE2 port (uplink/subtending GE port).

Figure 4-23 Unicast Forwarding Table Dialog

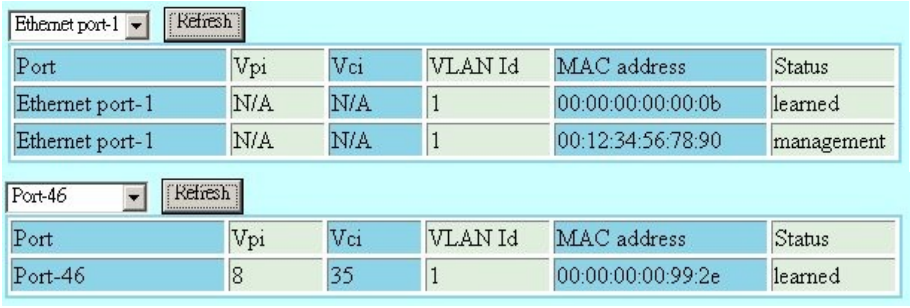


Table 4-14 Unicast Forwarding Table Description

Item	Description
Port	This indicates the location ADSL port.
Vpi/Vci	This indicates the VPI/VCI of the specified entry.
VLAN ID	This specifies the VLAN ID.
MAC address	This indicates the MAC address of the specified entry.
Status	This indicates the reason the MAC address appears in this entry. The definitions of status are as follows. • **Learned:** It indicates this MAC entry is learned from ADSL or GE port • **Management:** It indicates this MAC entry is configured manually in FDB.

Multicast Forwarding Table

The multicast forwarding table of DAS3 Series system stores the multicast following MAC entries

- The manually configured MAC addresses on an ADSL port.
- The MAC addresses learned from the associate subscriber port.
- The MAC addresses learned from the GE1 (uplink GE port) or GE2 port (uplink/subtending GE port).

Figure 4-24 Multicast Forwarding Table Dialog

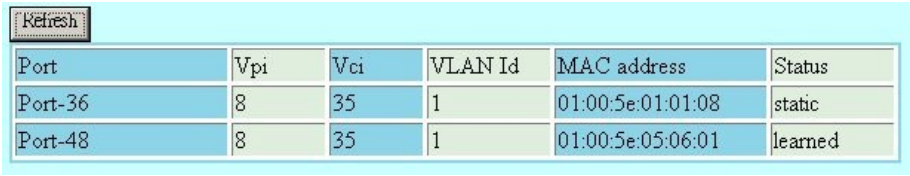


Table 4-15 Multicast Forwarding Table Description

Item	Description
Port	This indicates the location ADSL port.
Vpi/Vci	This indicates the VPI/VCI of the specified entry.
VLAN ID	This specifies the VLAN ID.

Table 4-15 Multicast Forwarding Table Description

Item	Description
MAC address	This indicates the multicast MAC address of the specified entry.
Status	This indicates the reason the MAC address appears in this entry. The definitions of status are as follows. • **Learned:** It indicates this multicast MAC entry is learned from ADSL port. • **Static:** It indicates the multicast MAC entry is configured manually in table.

Alarm Sensor

In the alarm sensor dialog, you can monitor the temperature and Fan status of NCT480 IP-DSLAM.

Figure 4-25 Alarm Sensor Dialog

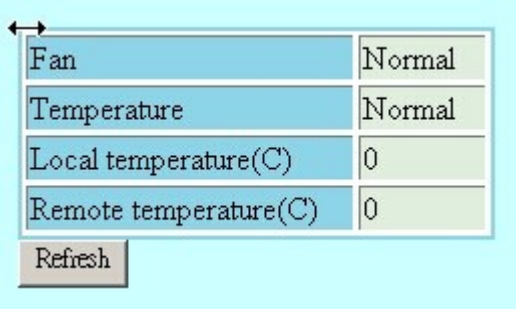


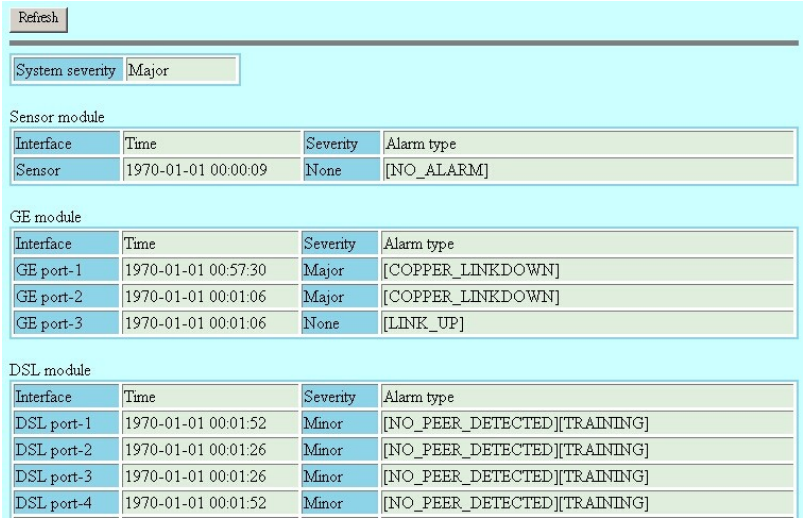
Table 4-16 Alarm Sensor Description

Item	Description
Fan	This specifies the Fan alarm status.
Temperature	This specifies the Temperature alarm status.
Local temperature (°C)	This specifies the local temperature.
Remote temperature (°C)	This specifies the remote temperature.

Active Alarm

Web management detects alarms from system and alarm sensor modules. Alarm detection is accomplished by way of either polling NE actively or receiving SNMP trap passively.

Figure 4-26 Active Alarm Dialog



Refresh

System severity	Major

Sensor module

Interface	Time	Severity	Alarm type
Sensor	1970-01-01 00:00:09	None	[NO_ALARM]

GE module

Interface	Time	Severity	Alarm type
GE port-1	1970-01-01 00:57:30	Major	[COPPER_LINKDOWN]
GE port-2	1970-01-01 00:01:06	Major	[COPPER_LINKDOWN]
GE port-3	1970-01-01 00:01:06	None	[LINK_UP]

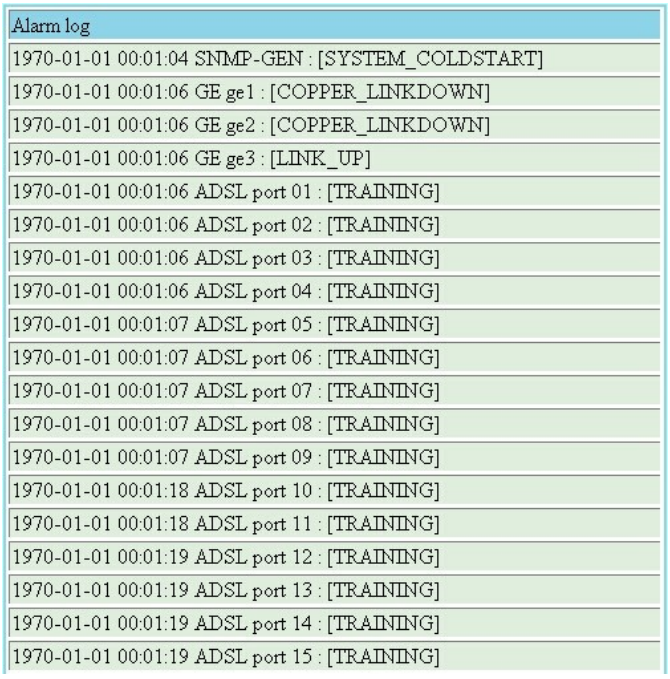
DSL module

Interface	Time	Severity	Alarm type
DSL port-1	1970-01-01 00:01:52	Minor	[NO_PEER_DETECTED][TRAINING]
DSL port-2	1970-01-01 00:01:26	Minor	[NO_PEER_DETECTED][TRAINING]
DSL port-3	1970-01-01 00:01:26	Minor	[NO_PEER_DETECTED][TRAINING]
DSL port-4	1970-01-01 00:01:52	Minor	[NO_PEER_DETECTED][TRAINING]

Active Alarm Log

The active alarm log dialog displays the last alarm messages.

Figure 4-27 Active Alarm Log Dialog



Alarm log
1970-01-01 00:01:04 SNMP-GEN : [SYSTEM_COLDSTART]
1970-01-01 00:01:06 GE ge1 : [COPPER_LINKDOWN]
1970-01-01 00:01:06 GE ge2 : [COPPER_LINKDOWN]
1970-01-01 00:01:06 GE ge3 : [LINK_UP]
1970-01-01 00:01:06 ADSL port 01 : [TRAINING]
1970-01-01 00:01:06 ADSL port 02 : [TRAINING]
1970-01-01 00:01:06 ADSL port 03 : [TRAINING]
1970-01-01 00:01:06 ADSL port 04 : [TRAINING]
1970-01-01 00:01:07 ADSL port 05 : [TRAINING]
1970-01-01 00:01:07 ADSL port 06 : [TRAINING]
1970-01-01 00:01:07 ADSL port 07 : [TRAINING]
1970-01-01 00:01:07 ADSL port 08 : [TRAINING]
1970-01-01 00:01:07 ADSL port 09 : [TRAINING]
1970-01-01 00:01:18 ADSL port 10 : [TRAINING]
1970-01-01 00:01:18 ADSL port 11 : [TRAINING]
1970-01-01 00:01:19 ADSL port 12 : [TRAINING]
1970-01-01 00:01:19 ADSL port 13 : [TRAINING]
1970-01-01 00:01:19 ADSL port 14 : [TRAINING]
1970-01-01 00:01:19 ADSL port 15 : [TRAINING]

This page is leave in blank for note or memo use

Chapter 4Deployment Menu

The deployment menu contains DSL profile, physical interface setting, network Ethernet and ADSL port.
This chapter contains the following sections:

- DSL Port Enable
- DSL Profile Configuration
- DSL Profile Mapping
- DSL Alarm Profile
- Power Management Mode
- PVC Setting
- IPoA Route
- Ethernet Port Enable
- Ethernet Setting
- SNMP Community
- SNMP Host
- SNMP Trap Host
- Alarm I/O Control
- Remote DSLAM

DSL Port Enable

This section describes how to enable and disable port through Enable/disable dialog.

Figure 5-28 DSL Port Configuration Dialog

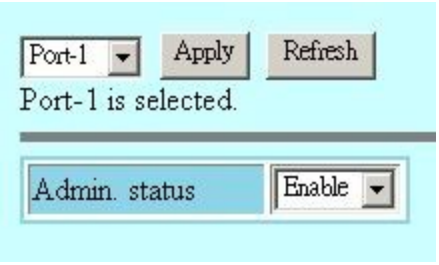


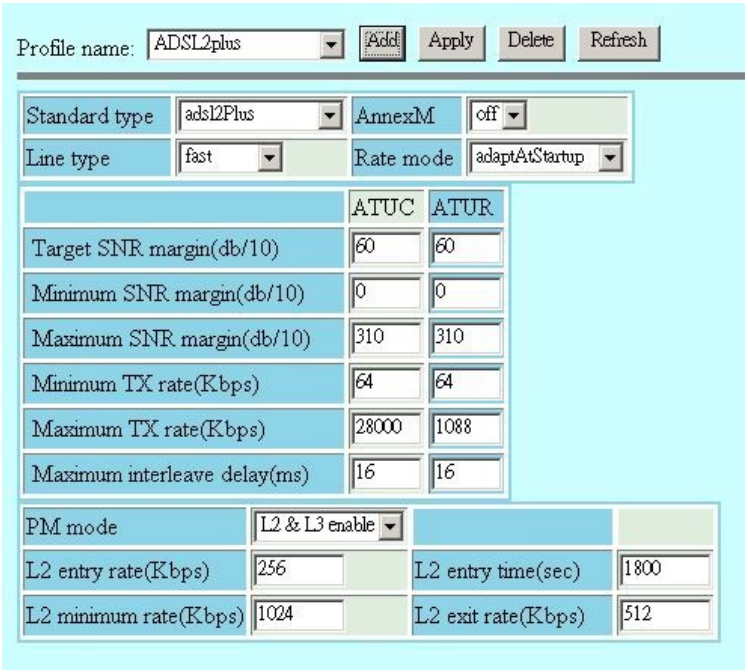
Table 5-17 Enable / Disable port

Item	Description
Port selection pull down menu	Select port to be enabled or disabled
Admin status	Display port status

DSL Profile Configuration

This section describes the static Line (ADSL) profile configuration. Line Profile Configuration dialog allows you to modify the ADSL connection parameters of each DSL profile.

Figure 5-29 DSL Profile Configuration



Add DSL Profile

Add DSL profile dialog allows you to create the ADSL connection parameters. Enter the control values to the text box and click '**Add**' to activate

Figure 5-30 Add DSL Profile Dialog

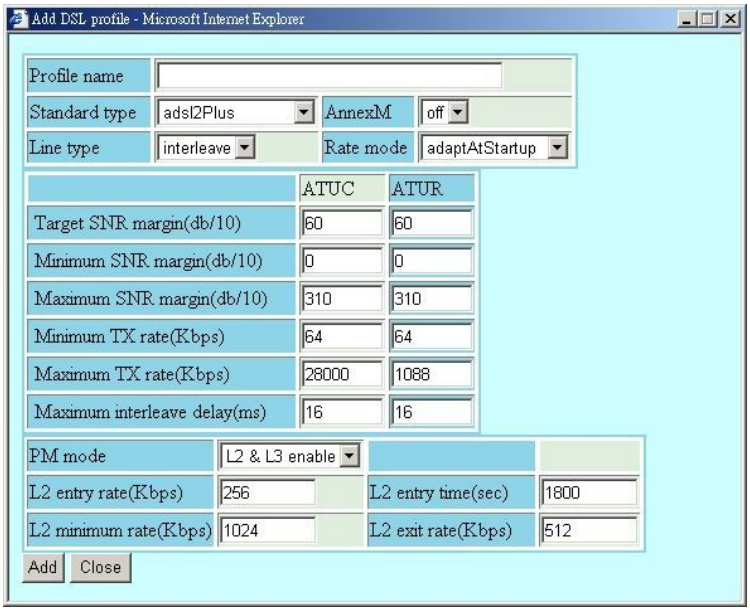


Table 5-18 Monitoring Line Profile Configuration

Item	Description
Profile name	Select a DSL profile to display relative parameters.
Line Interface	
Standard type	Preferred standard compliance. Outcome is dependent upon standard support of the remote unit.
AnnexM	This extends the capability of basic ADSL2 by doubling the number of upstream bits.
Line Type	This specifies the type of channel on which the ATM VC's cells have to be transmitted and received. Possible choice: Interleave Only/Fast Only * **Interleave mode** is used when transmission error correction is necessary due to a less than ideal telephone line. * **Fast mode** will result in faster transmission rate.
Rate Mode	This specifies what form of transmission rate adaptation is configured on this port. **fixed** – Connect over the fixed speed given by 'Tx Rate' field, the connection gets fail if it can not reach the lengths and qualities of lines **adaptAtStartup** – Connect over the range of speed given by 'Tx Rate' field, the connection gets retrain due to varying qualities of lines. **adaptAtRuntime** – Connect over the range of speed given by 'Tx Rate' field, the connection is auto rearrange seamlessly due to varying qualities of lines.
SNR Margin (ATUC/ATUR)	
Target SNR Margin	This specifies Target SNR Margin which the ATU-R must achieve with a BER of 10 to the power -7 or better, to successfully complete initialization. **Valid values:** 0 ~ 310 (dB/10)
Maximum SNR Margin	This specifies Maximum SNR Margin which the ATU-R receiver shall try to sustain. If the noise margin is above this level, the ATU-R shall request the ATU-C to reduce the transmit power to get a noise margin below this limit. **Valid values:** 0 ~ 310 (dB/10)
Minimum SNR Margin	This specifies Minimum Noise Margin which the ATU-R receiver shall tolerate. If the noise margin falls below this level, the ATU-R shall request the ATU-C to increase the ATU-C transmit power. If an increase to ATU-C transmit power is not possible, a loss-of-margin (LOM) defect occurs, the ATU-R shall fail and attempt to reinitialize. **Valid values:** 0 ~ 310 (dB/10)
Tx Rate and Delay (ATUC/ATUR)	
Minimum Tx Rate	Configured Minimum Transmit rate for ADSL line channels, in bps. **Valid values (ATU-C Downstream):** 32 ~ 28000 (kbps) **Valid values (ATU-R Upstream):** 32 ~ 2784 (kbps)
Maximum Tx Rate	Configured Minimum Transmit rate for ADSL line channels, in bps. **Valid values (ATU-C Downstream):** 64 ~ 28000 (kbps) **Valid values (ATU-R Upstream):** 0 ~ 2784 (kbps)

Table 5-18 Monitoring Line Profile Configuration

Item	Description
Maximum Interleave Delay	Configured maximum Interleave Delay for this channel. Interleave delay applies only to the interleave channel and defines the mapping (relative spacing) between subsequent input bytes at the interleave 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. **Valid values:** 0 ~ 255 (mSec)
Power Management	
Power Management mode	Power Management-related parameter used by ATU-C to set the allowed link states. Both bit values can be given simultaneously in the input.
L2 Entry Rate (Kbps)	Power Management configuration parameter. L2 state **entry** data rate. **Valid values:** 0 ~ 30000
L2 Minimum Rate (Kbps)	Power Management configuration parameter, related to the L2 low power state. This parameter specifies the minimum net data rate during the low power state (L2). **Valid values:** 8 ~ 1024 (kbps)
L2 Entry Time (sec)	Power Management configuration parameter. Min L2 **entry** rate time **Valid values:** 900 ~ 65535
L2 Exit Rate (Kbps)	Power Management configuration parameter. L2 state **exit** data rate. **Valid values:** 0 ~ 30000

DSL Profile Mapping

This section helps you to attach the DSL profile to the ADSL line interface.

Figure 5-31 DSL Profile Mapping Dialog

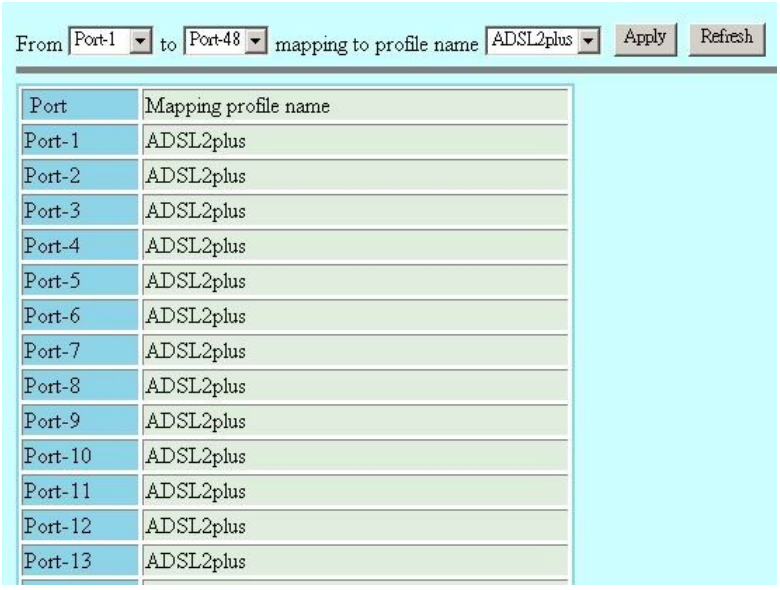


Table 5-20 If DSL profile chose 'None', the default parameter values

Table 5-19 DSL Profile Mapping

Item	Description
From	This specifies the starting ADSL port interface for ATM PVC configuration.
To	This specifies the ending ADSL port interface for ATM PVC configuration.
Profile Name	This specifies the profile name. (DSL Profile)

Table 5-20 Default DSL Profile Setting

Item	Setting
Line Interface	
Standard type	ADSL2Plus
AnnexM	off
Line Type	interleave
Rate Mode	adaptAtStartup
SNR Margin (ATUC/ATUR)	
Target SNR Margin (db/10)	60
Minimum SNR Margin (db/10)	0
Maximum SNR Margin (db/10)	310
Tx Rate and Delay (ATUC/ATUR)	
Minimum Tx Rate (Kbps)	64
Maximum Tx Rate (Kbps)	ATUC: 28000 ATUR: 1088
Maximum Interleave Delay (ms)	16
Power Management	
Power Management mode	L2 & L3 enable
L2 Entry Rate (Kbps)	256
L2 Minimum Rate (Kbps)	1024
L2 Entry Time (sec)	1800
L2 Exit Rate (Kbps)	512

DSL Alarm Profile

The alarm profile configuration controls the PM threshold values of ADSL line parameters.

Click on the text column to edit the threshold seconds, if the value reach the threshold (in seconds), the system will send the SNMP trap.

Figure 5-32 DSL Alarm Profile Dialog

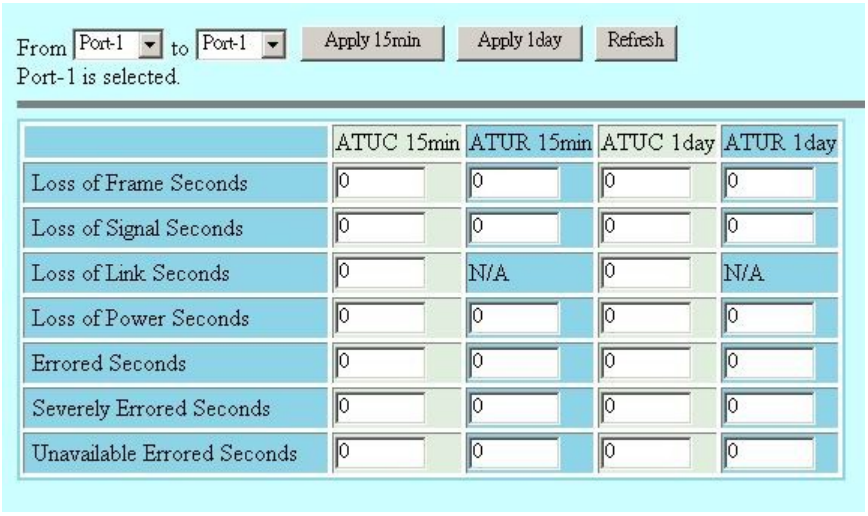


Table 5-21 describes the alarm profile dialog option items.

Table 5-21 DSL Alarm Profile Dialog Description

Item	Description
ATUC 15 min / 1 day	Set Value to zero to disable traps
LOF(sec)	The number of Loss of Frame Seconds encountered by an ADSL interface within any given 15 minutes or 1 day performance data collection period.
LOS(sec)	The number of Loss of Signal Seconds encountered by an ADSL interface, within any given 15 minutes or 1 day performance data collection period.
LOL (sec)	The number of Loss of Link Seconds encountered by an ADSL interface, within any given 15 minutes or 1 day performance data collection period.
LOP (sec)	The number of Loss of Power Seconds encountered by an ADSL interface, within any given 15 minutes or 1 day performance data collection period.
ES (sec)	The number of Error Seconds encountered by an ADSL interface, within any given 15 minutes or 1 day performance data collection period.
SESL (sec)	The number of Severe error seconds encountered by an ADSL interface within any given 15 minute or 1 day performance data collection period, which causes adslAtucSesLTrap.
UASL (sec)	The number of unavailable error seconds encountered by an ADSL interface within any given 15 Minute or 1 day performance data collection period, which causes adslAtucUasLThreshTrap.
ATUR 15 min / 1 day	Set Value to zero to disable traps
LOF(sec)	The number of Loss of Frame Seconds encountered by an ADSL interface within any given 15 Minute or 1 day performance data collection period.'

Table 5-21 DSL Alarm Profile Dialog Description

Item	Description
LOS(sec)	The number of Loss of Signal Seconds encountered by an ADSL interface, within any given 15 Minute or 1 day performance data collection period.
LOP (sec)	The number of Loss of Power Seconds encountered by an ADSL interface, within any given 15 Minute or 1 day performance data collection period.
ES (sec)	The number of Error Seconds encountered by an ADSL interface, within any given 15 Minute or 1 day performance data collection period.
SESL (sec)	The number of Severe Error Seconds encountered by an ADSL interface within any given 15 Minute or 1 Day performance data collection period, which causes adslAtucSesLTrap.
UASL (sec)	The number of unavailable error seconds encountered by an ADSL interface within any given 15 Minute or 1 Day performance data collection period, which causes adslAtucUasLThreshTrap.

Power Management Mode

The power management allows you to furnish the efficiency of ADSL power output.

First-generation ADSL transceivers operate in full-power mode (L0) day and night, even when not in use. To address these concerns, the ADSL2 standard brings in two power management modes that help to reduce overall power consumption while maintaining ADSL's "always-on" functionality for the user. These modes are the L2 and L3 power modes.

The L2 low-power mode enables statistical powers savings at the ADSL transceiver unit in the central office (ATU-C) by rapidly entering and exiting low power mode based on Internet traffic running over the ADSL connection. When large files are being downloaded, ADSL2 operates in full power mode (called "L0" power mode) in order to maximize the download speed. When Internet traffic decreases, such as when a user is reading a long text page, ADSL2 systems can transition into L2 low power mode, in which the data rate is significantly decreased and overall power consumption is reduced. While in L2, the ADSL2 system can instantly re-enter L0 and increase to the maximum data rate as soon the user initiates a file download. The L2 entry/exit mechanisms and resulting data rate adaptations are accomplished without any service interruption or even a single bit error, and as such, are not noticed by the user.

The L3 power modem on the other hand, enables overall power savings at both the ATU-C and the remote ADSL transceiver unit (ATU-R) by entering into sleep mode when the connection is not being used for extended periods of time. L3 is a sleep mode where traffic cannot be communicated over the ADSL connection when the user is not online. When the user returns to go on-line the ADSL transceivers require at least 2 to 3 seconds to re-initialize and to enter into steady-state communication mode.

Figure 5-33 Power Management Forced State

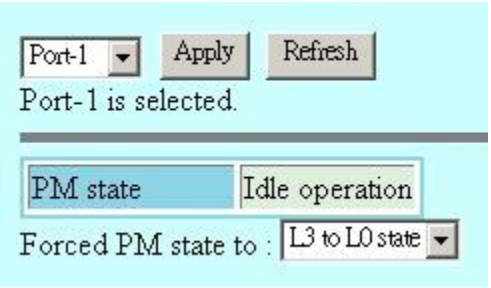


Table 5-22 Force Power Management

Item	Description
Port selection pull down menu	Select port to be applied.
Forced PM state to	L3 to L0 state L0 to L2 state To L3 state L2 to L0 state

PVC Setting

The PVC Management dialog has the ability to configure the ATM PVC on ADSL port interface.

Figure 5-34 PVC Setting Dialog

Table 5-23 describes the column status of PVC setting dialog.

Table 5-23 Monitoring the PVC Management

Column Item	Description
Port	This indicates the physical DSL port interface.
VPI	The virtual path identifier of correspond DSL port interface.
VCI	The virtual circuit identifier of correspond DSL port interface.
Encapsulation type	This specifies the data multiplexing method to be used over the AAL5 layer, adjacent CPE must use the same encapsulation to establish the connection. Possible choice: LLCMux* or VCMux*. * LLC encapsulation enables one Virtual Channel to carry multiple protocols with each packet header containing protocol identifying information. VC encapsulation engages each protocol with a specific virtual channel.

Add Port & PVC

Click '**Add**' button to create a new PVC of single or range of ADSL port interface.
Total eight PVCs will be allowed under a single port.

Figure 5-35 Add Port & PVC Dialog

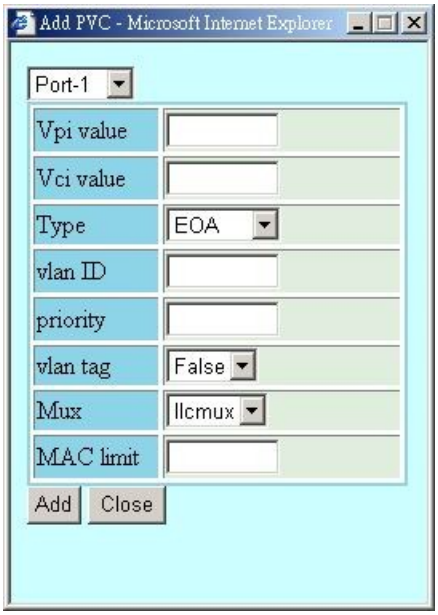


Table 5-24 describes the Port & PVC Add dialog field items.

Table 5-24 Creating the Port PVC

Item	Description
Port selection pull down menu	This specifies the ADSL port interface for ATM PVC configuration.
VPI	This specifies the virtual path identifier for use at DSL port interface. **Valid values:** 0 ~ 255
VCI	This specifies the virtual circuit identifier for use at DSL port interface. **Valid values:** 1 ~ 65535 (1 ~ 31 are reserved)
Type	Be sure to use the encapsulation method required by the ATU-R. The DAS3 Series IP-DSLAM supports the following methods. **EOA:** Ethernet over ATM. EoA benefits from SONET/SDH protection but has been criticized for being expensive and having scalability issues. EoA offers smooth roll out of Ethernet-based services in existing Asynchronous Transfer Mode ATM network and optimizes the use of spare capacity in the ATM network. **IPOA:** Existing CPE devices have IPoA interfaces towards the WAN side. These interfaces need to be supported and retained by the service providers. Also DSLAMs are moving from ATM to Packet mode and hence support for these interfaces on the CPE side becomes essential. In order to provide this flexibility in the route mode firmware release R2.0, RFC 2684 Routed (IPoA) interfaces along with the existing RFC 2684 Bridged Ethernet interfaces shall be supported. **PPPOA:** PPPoA stands for Point to Point Protocol over ATM Adaptation Layer5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The DAS3 Series IP-DSLAM encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the CPEs. Please refer to RFC2364 for more information on PPPoA. Refer to RFC1661 for more information on PPP.

Table 5-24 Creating the Port PVC

Item	Description
VLAN ID	This specifies the VLAN ID value. The VC-to-VLAN setting can easily define in multiple to one or one to one mapping; you can group different PVC to a single VLAN ID as well as single PVC to one VLAN mapping.
Priority	This specify the VLAN priority
VLAN tag	This specify the VLAN tag or untag
Mux (For EOA)	This specifies the data multiplexing method to be used over the AAL5 layer, adjacent CPE must use the same encapsulation to establish the connection. Possible choice: LLCMux* or VCMux*. * LLC encapsulation enables one Virtual Channel to carry multiple protocols with each packet header containing protocol identifying information. VC encapsulation engages each protocol with a specific virtual channel.
MAC limit (For EOA)	The number of MAC addresses that can be learned by the specific port interface. **Valid values:** 1 ~ 16
IP (For IPOA)	The creation of the above downstream route actually assigns an IP address to the IPoE interface. Also it specifies that for IP routing, IP address <E.F.G.H>. Using all this information, an ARP request for the IP address specified in the gateway IP address of the default route. BRAS shall respond the ARP request from the NET side. Also due to source MAC address based learning, an entry in the MAC address-forwarding table will get created, which is required for the upstream forwarding. Hence, the upstream traffic can flow.
MAC (For IPOA)	MAC address profile is a generic way for assigning MAC addresses to interfaces. A MAC address can be associated with a profile and that profile can be attached to the interface. Currently a maximum of 48 profiles are supported in the system.

Set PPPoA MAC

The PPPoA MAC address to be used in the PPPoE packets from DSLAM to the BRAS is configurable. One MAC address can be assigned to multiple PPPoA terminations. The PPPoE session identifier is additionally used to perform the de-multiplexing in the BRAS to customer direction.

Figure 5-36 Set PPPoA MAC Dialog

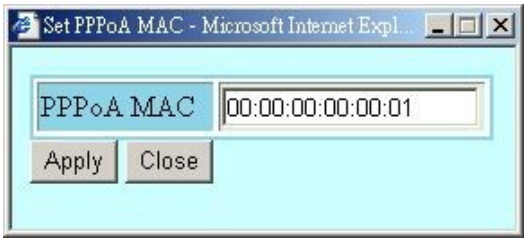


Table 5-25 Add PPPoA MAC

Item	Description
PPPoA MAC	Configure the MAC address to be used by the PPPoE tunnel interface.

IPoA Route

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

Figure 5-37 Display the Routing Table

Ethernet Port Enable

This section describes how to enable and disable Ethernet port through Enable/disable dialog.

Figure 5-38 Ethernet port Configuration Dialog

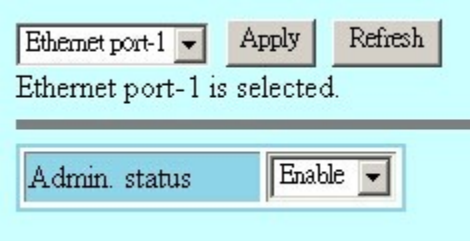


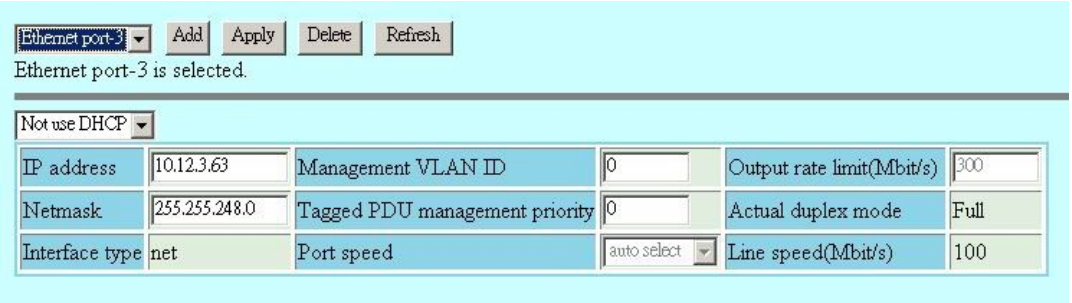
Table 5-26 Enable / Disable Ethernet port

Item	Description
Port selection pull down menu	Select Ethernet port to be enabled or disabled
Admin status	Display Ethernet port status

Ethernet Setting

The Ethernet Interface allows you to manage the network Ethernet port.

Figure 5-39 Ethernet Port Configuration Dialog



Select an Ethernet Port to show the parameters, edit the control value in text box and click '**Apply**' to modify or click '**Add**' to create a new Ethernet port.

Table 5-27 Monitoring the Ethernet Port

Item	Description
Ethernet Port pull down menu	Select the Ethernet port from pull down menu.
IP Address	This specifies the network IP address of given Ethernet interface. This IP address is for system management use only. **Valid values:** Any valid class A/B/C address
Net Mask	This specifies the network mask configured for the interface. **Valid values:** 255.0.0.0 ~ 255.255.255.255
Is use DHCP	This indicates whether a DHCP client is to be triggered to obtain an IP address for this Ethernet interface.
Interface Type	The type of Ethernet interface, net or slave.
Actual Duplex Mode	The duplex mode use by the Ethernet interface.
Output Rate Limit	This parameter specifies the output rate limiting value to be applied on this interface. The unit is in Mbits/sec. This setting will have effect on receiving data rate of specified port. **Valid values:** 0 ~ 300 Mbps
Management VLAN ID	VLAN for management traffic on this interface. Nonzero value of this field is valid only if either 'IP Address' field is non-zero or 'does use DHCP' field is true. If no Management VLAN ID is specified (in the create operation) or its value is set to zero (either in create or modify operation) then the system shall use the value of 'private VLAN ID' associated with the bridge port created on this interface as the Management VLAN ID. In case the management VLAN (i.e. 'Management VLAN ID' or the associated 'private VLAN ID', if 'Management VLAN ID' is zero) does not exist on the system then IP based management on this management VLAN shall not happen on the interface till the corresponding VLAN is created with the Network side port as its member. **Default values:** 0 **Valid values:** 0 ~ 4094

Table 5-27 Monitoring the Ethernet Port

Item	Description
Tagged PDU Management Priority	Priority to be set in Tagged Ethernet PDUs sent on Management VLAN over this interface. This field is valid only if either 'IP Address' field is non-zero or 'does use DHCP' field is true. **Valid values:** 0 ~ 7
Port Speed	This specifies the port speed for the Network Ethernet interfaces. The 'auto select' specifies that the interface will determine the line speed using auto-negotiation.

Add Ethernet Interface

DAS3 Series IP-DSLAM supports two Ethernet interfaces and one management port (Ethernet port-3). The IP address is only for management purpose and each Ethernet interface can apply its own IP address.

Figure 5-40 Add Ethernet Interface Dialog

Network type '**downlink**' is for system stacking and relevant port will not need an IP address.

Beware when select on the '**Non IP**' option and '**Delete**' button, the management connection may be loss due to those setting.

Table 5-28 Creating the Ethernet Port

Item	Description
Select an Ethernet port to add	Select the Ethernet port from pull down menu.
Network Type	This specifies the type of the Ethernet interfaces. The uplink is towards the Network side (2 at most) and downlink is towards the physical interface connected to the slave device. For uplink type, IP address can not be null, if 'Is use DHCP' is false.
Use DHCP	If this mode is selected, the IP will be automatically obtained from DHCP server.
Non-IP	Select Non IP to restrict the IP management activity.

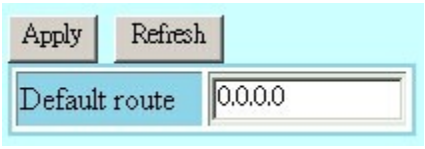
Table 5-28 Creating the Ethernet Port

Item	Description
IP address & netmask	
IP Address	This specifies the network IP address of given Ethernet interface, this IP address use for only system management. **Valid values:** Any valid class A/B/C address
Net Mask	This specifies the network mask configured for the interface. **Valid values:** 255.0.0.0 ~ 255.255.255.255

Default Route

This link takes you to screens where you can configure static routes. A static route defines how the DSLAM should forward traffic by configuring the TCP/IP parameters manually.

Figure 5-41 Default Route Setting

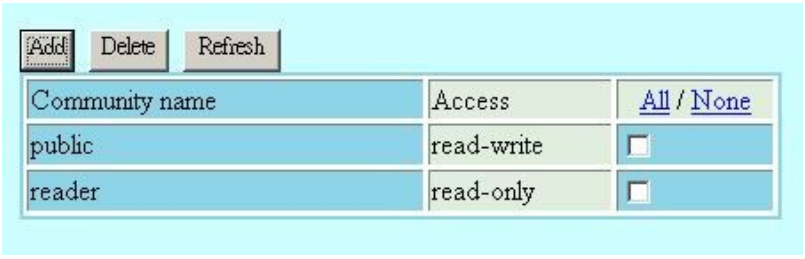


SNMP Community

The SNMP community configuration dialog allows you to manage the SNMP community access privilege.

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. The Trap operation is used by agents to asynchronously inform the NMS of a significant event.

Figure 5-42 SNMP Community Configuration Dialog



Click '**Add**' button to create a new SNMP community name and access permission.

Figure 5-43 Add Community Dialog

The community access has relationship to the mapping Host IP, changed the community access option will change the access privilege of specifics Host IP.

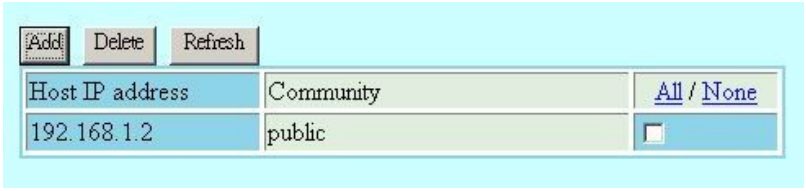
Table 5-29 Configuring the SNMP Community

Item	Description
Community name	This specifies the community name. **Valid values:** String of up to 20 characters (All characters except ';', '?', and empty space)
Community Access	This specifies the access permissions given to managers with this community name in Read only or Read-write permissions.

SNMP Host

The SNMP Host configuration dialog allows you to manage the Host IP and corresponded SNMP community.

Figure 5-44 SNMP Host Configuration Dialog



Click '**Add**' button to create a new SNMP Host IP address.

The Host IP is the device (PC) IP address allowed to manage the IP-DSLAM via AMS (Advanced Management Service). It is recommended to limit the number of host device.

Figure 5-45 Add Host IP Address Dialog

Table 5-30 describes fields in the Add Host IP Address Dialog.

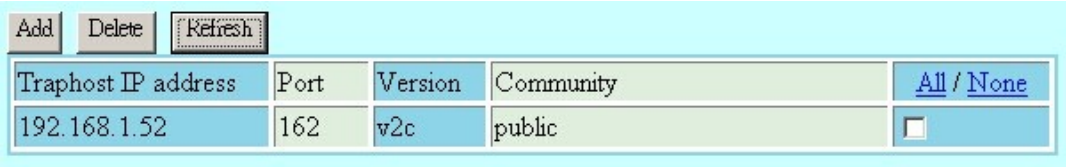
Table 5-30 Configure Host IP

Item	Description
IP Address	This specifies the IP address of the manager that has access permissions. **Valid values:** Any valid class A/B/C address
Community	This indicates the community name specify on community configuration.
Access	This indicates the access permissions given to managers with this community name.

SNMP Trap Host

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.

Figure 5-46 SNMP Trap Host Setting Dialog



Alarm I/O Control

The alarm I/O control allows you to define the alarm input and output. Please see "*System Installation Guide*" for the definition. Once the normal status of input signal is different from the current status, the DAS3 Series will launch an "abnormal status" alarm of the specified output to terminal or administrator.

Figure 5-47 Alarm I/O Control Dialog

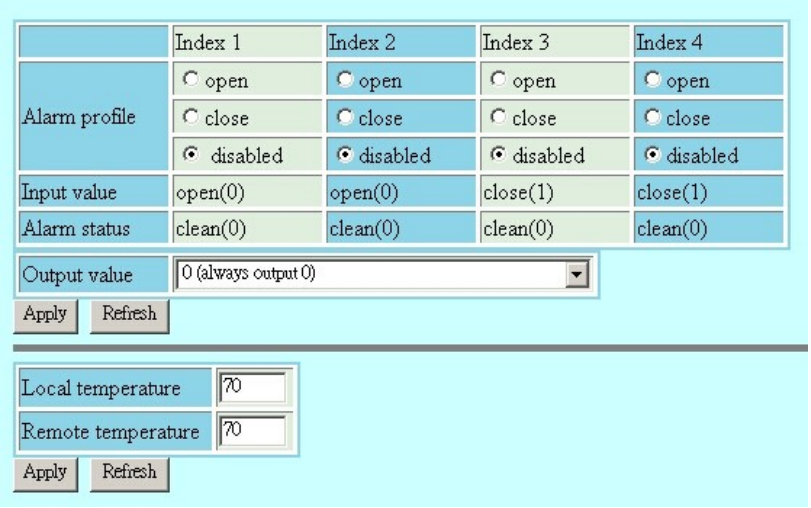


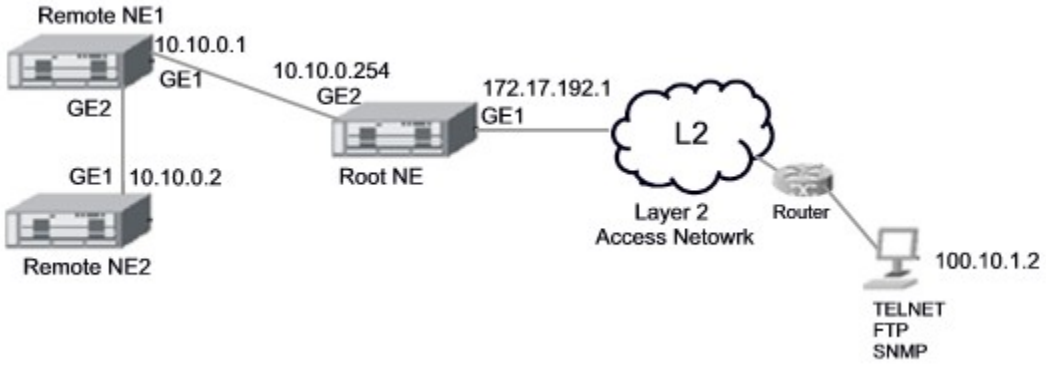
Table 5-31 Alarm I/O Control

Item	Description
Index 1~4	This indicates the location of relay input ports (1 ~ 4).
Alarm profile	This indicates the alarm profile of the specified relay input that configured by operator.
Input value	This indicates the current status of the specified relay input.
Alarm status	This indicates the alarm status.
Output value	This specifies the status of out alarm configuration. 0: always output 0 1: always output 1 0alarm: usually output 1, output 0 when alarm occur 1alarm: usually output 0, output 1 when alarm occur
Local temperature	This specifies the local alarm temperature value.
Remote temperature	This specifies the remote alarm temperature value.

Remote DSLAM

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(Network Equipment) 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 5-48 depicts a typical cascading topology.

Figure 5-48 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 5-48. The Root-NE possesses 2 IP addresses.
  - UGE IP: “UGE IP” is for the communication with the EMS server, Web management and Telnet hosts.
  - Root IP: “root IP” is for the communication with the Remote-NE. It is invisible to the network operator.
- Remote-DSLAM

  The Remote-NE indicates the NE which is not directly connected to the L2 access network as shown in Figure 5-48. 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 as shown in Figure 5-48, the operator needs to set them to run in the cascade mode. After appropriate configurations on the Root-NE and Remote-NEs, these NEs will work as a single NE which possesses several shelves via the EMS.

Figure 5-49 Remote DSLAM Configuration Dialog

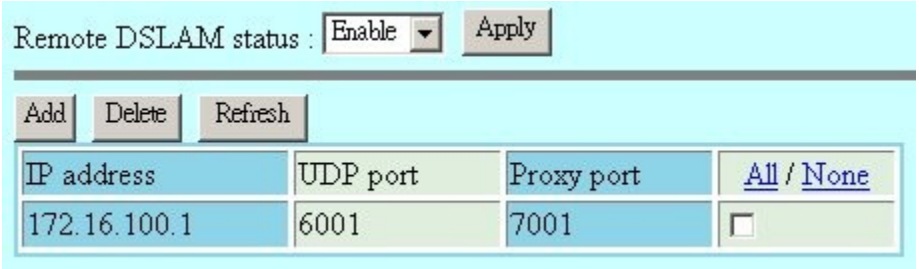


Table 5-32 Remote DSLAM Configuration

Item	Description
Remote DSLAM status	Specified whether or not Remote DSLAM status is to be enabled in the system.
IP address	This indicates the IP address of the remote NE.
UDP port	This specifies the UDP port number.
Proxy port	This specifies the proxy port number.

This page is leave in blank for note or memo use

Chapter 5Access Control

The access control functionalities allow system administrator to build packet filter and access control list.
This chapter contains the following sections:

- MAC Limit
- Port ACL
- Global ACL

MAC Limit

Limit MAC number control the total number of MAC addresses learning from independent port interface (Ethernet and ADSL).

Figure 6-50 MAC Limit Dialog

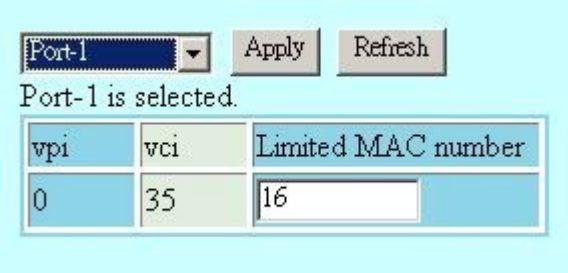


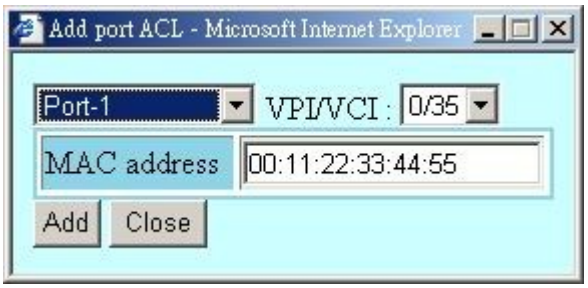
Table 6-33 Configuring the MAC Limit

Item	Description
Port selection menu	This specifies the Ethernet interface and ADSL port interface.
Limit MAC number	The number of MAC addresses that can be learned by the specific port interface. **Ethernet valid values:** 1 ~ 256 **DSL valid values:** 1 ~ 16
Selected port's MAC number	This displays the selected port's limit MAC number.

Port ACL

The per port access control list allow the MAC addresses to entry the system.

Figure 6-51 Port ACL Configuration Dialog



Enter the MAC address at 'Allow MAC Address' text box and click '**Add**' to submit. MAC address in format of xx:xx:xx:xx:xx:xx up to maximum 8 sets per port interface.

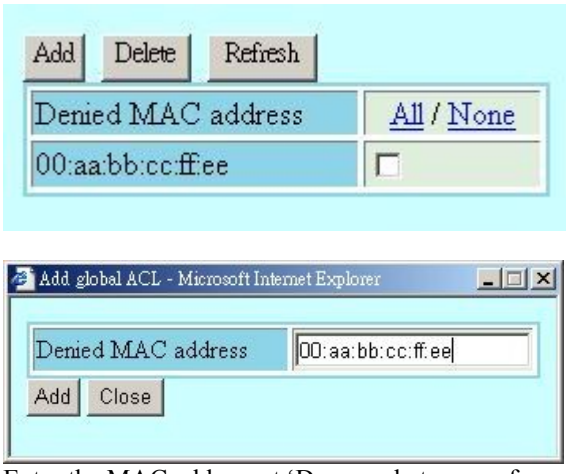
Table 6-34 Configuring Port(vpi/vci) Access Control List

Item	Description
Port(vpi/vci)	Select the ADSL port interface to be display with relative parameters.
Allow MAC Address	This specifies MAC address to be allowed for the port, vpi, and vci pair.

Global ACL

The global access control list denies the MAC addresses pass-through the system at all port interface.

Figure 6-52 Global ACL Configuration Dialog



Enter the MAC address at 'Drop packets come from the MAC Address' text box and click '**Add**' to submit. MAC address in format of xx:xx:xx:xx:xx:xx up to maximum 256 sets per system.

Table 6-35 Configuring Global Access Control List

Item	Description
Deny MAC Address	Source MAC address to be dropped

Chapter 6Protocol Menu

Protocol menu contains setting for VLAN, SNTP, IGMP, DHCP/PPPoE relay configuration, Rapid Spanning Tree Protocol and Multicast related.
This chapter contains the following sections:

- Port VLAN
- Ethernet VLAN Membership
- DHCP & PPPoE Relay
- Spanning Tree Protocol
- Rapid Spanning Tree Protocol
- SNTP Protocol
- IGMP Snooping
- Multicast Profile
- Multicast VLAN Registration

Port VLAN

The VLAN port management allows you to control the accept frame type and ingress filtering status of port interface.

Figure 7-53 Port VLAN Management Dialog

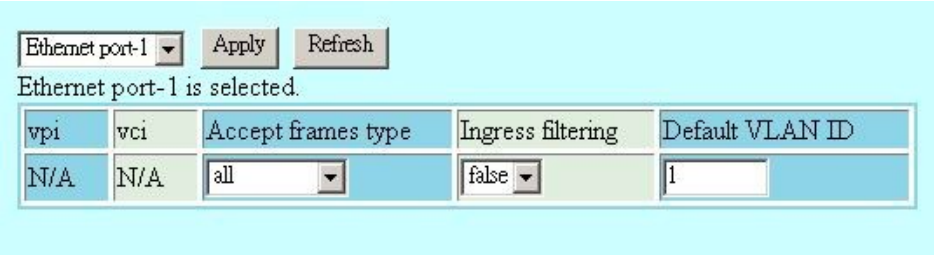


Table 7-36 VLAN Ports Management Dialog Description

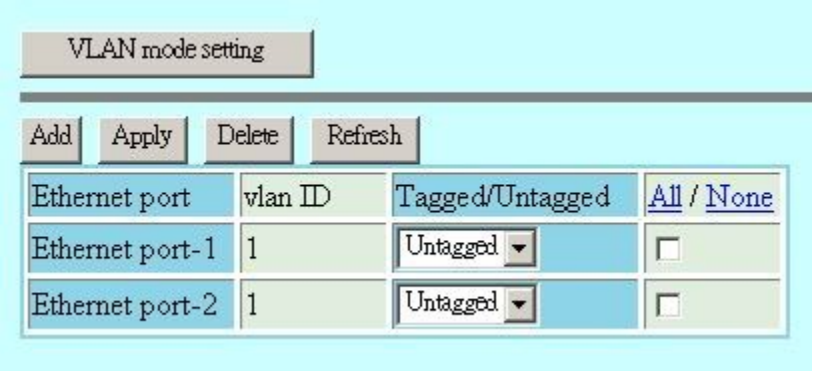
Item	Description
Accept Frames Type	The set of ports, which are transmitting traffic for this VLAN, as either tagged or untagged frames. When this is **Tagged**, the device will discard untagged frames or priority-Tagged frames received on this port. When **All**, untagged frames or Priority-Tagged frames received on this port will be accepted and assigned to the PVID for this port.
Ingress Filtering	When this is **true**, the device will discard incoming frames for VLANs, which do not include this Port in its Member set. When **false**, the port will accept all incoming frames.
Default VLAN ID	The VLAND ID to be assigned if untagged frames are accepted.
	Press the **'Apply'** button to confirm the setting.

Ethernet VLAN Membership

The Ethernet VLAN Membership dialog lists the existing trunk VLAN and its configuration.

A VLAN allows a physical network to be divided into several logical networks. A device can belong to more than one VLAN group. Devices that are not in the same VLAN groups can not talk to each other. VLAN can provide isolation and security to users and increase performance by limiting broadcast domain. VLAN tag can be added to the MAC header to identify the VLAN membership of a frame across bridges. A tagged frame is four bytes longer than an untagged frame. Each port of DAS3 Series is capable of passing tagged or untagged frames.

Figure 7-54 Ethernet VLAN Membership Dialog



Click '**Add**' button to set the new Ethernet VLAN membership with associate port interface.

Add Trunk VLAN

Figure 7-55 Add Trunk VLAN Dialog

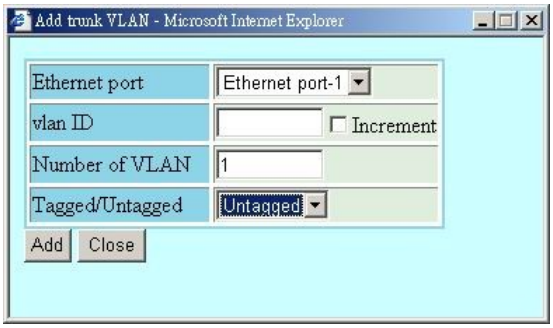


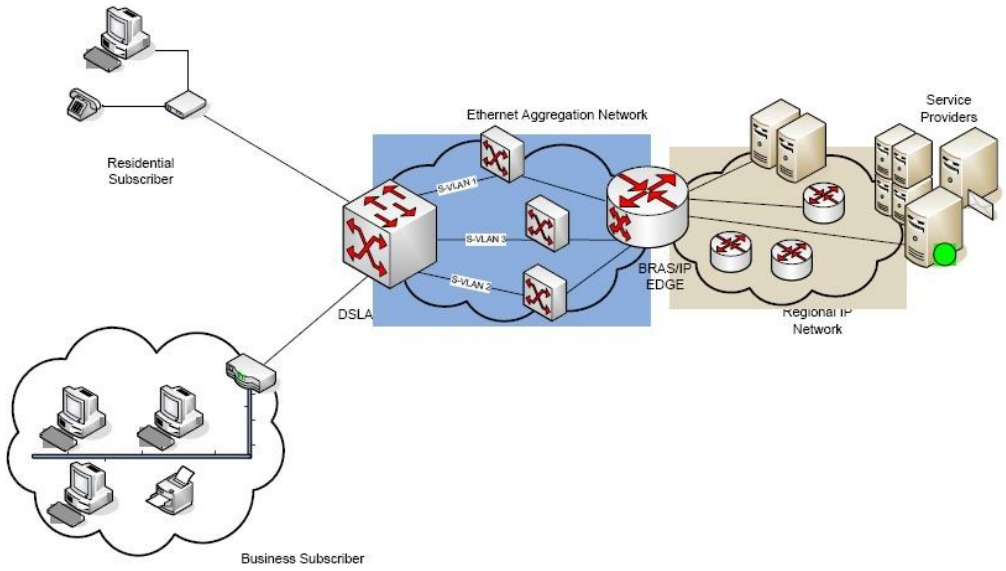
Table 7-37 Configuring VLAN Port Member

Item	Description
VLAN ID	The VLAN identifier assigned to a specific VLAN. VLAN 1 is the default VLAN **Valid values: 0~4095. [0 is reserved for priority tag, 4095 is reserved]**
Number of VLAN	This indicates the VLAN ID increment number.
Tagged/Untagged	This setting determines a specific port to receive tagged or untagged frame.

VLAN Mode Setting

With the Ethernet becoming cheaper and more popular, the Ethernet networks are expanding to cover metros. This is leading to deployment of MEN (Metropolitan Ethernet network). The existing support for VLAN as standardized in IEEE 802.1Q is not able to scale to MEN deployment, because of limited 4095 VLANs and hence the requirement for VLAN Stacking.
VLAN Stacking, also known as Q in Q, is the mechanism where one VLAN (Virtual Local Area Network) may be encapsulated within another VLAN. This allows a carrier to partition the network among several national ISPs, while allowing each ISP to still utilize VLANs to their full extent. It is very important to logically separate all traffic between ISPs – for security, for offering different levels of service to prospective ISP customers and the ability to utilize full VLAN space.
In a typical network scenario Columbia is on edge of provider network (Ethernet Aggregation Network), the location of DSLAM as shown in Figure 7-56 depicting Network Scenario.

Figure 7-56 Network Scenario



With VLAN stacking, if one ISP provisioned an end user into “VLAN 1”, and another ISP provisioned one of their end users into “VLAN 1”, the two end users would not receive each other’s traffic.

Figure 7-57 VLAN Mode Setting Dialog

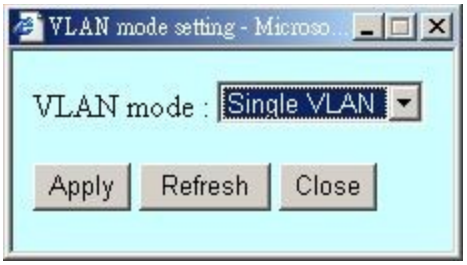


Table 7-38 VLAN Mode Setting Description

Item	Description
VLAN mode	Single VLAN: The single VLAN Mode confirms to the normal 802.1Q VLAN support and the system will continue to work as is in the current model without VLAN stacking. Double VLAN: VLAN used in VLAN aware networks based on 802.1Q bridging is called C-VLAN (Customer-VLAN), and can be uniquely identified by a C-VLAN tag VLAN that encapsulates Customer traffic in Provider network is called S-VLAN or Service VLAN and is identified by an S-VLAN ID, used as second VLAN tag. In this mode the features can be used to meet custom VLAN stacking requirements.
	Press the '**Apply**' button to confirm the setting.

DHCP & PPPoE Relay

The DHCP Relay configuration provides DHCP Relay Option 82 function.

Modern high-speed public Internet access technologies call for an ISP/NSP Switch/Router to have a local area network (LAN) attachment to one or more customer premise hosts. It is advantageous to use the Dynamic Host Configuration Protocol (DHCP) as defined in IETF RFC-2131 to assign customer premise host IP addresses in this environment. However, a number of security and scaling problems arise with such normal DHCP use.

To solve the aforementioned problems, IETF RFC-3046 defines the Relay Agent Information option (Option82). The DHCP relay agent inserts this optional tag when forwarding client-originated DHCP packets to a DHCP Server. Server can use this information to assign IP addresses, perform access control, set quality of service (QoS) and security policies (or other parameter-assignment policies) for each subscriber of a service-provider network. The DHCP Server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

Two sub-options of option 82 are defined in RFC 3046:
• Agent Circuit ID (intended for circuits terminated by the system hosting the Relay agent)
• Agent Remote ID (intended to identify the remote host end of a circuit)

Figure 7-58 DHCP & PPPoE Relay Dialog

Table 7-39 DHCP & PPPoE Relay Configuration

Item	Description
Circuit ID	
Prefix string	The flexible syntax is concatenation of a configurable prefix string of circuit ID.
Access node identifier	It is a character string and can be configured. If its value is auto, the access node identifier is derived from MAC address of access node
Chassis No.	This specifies the chassis string and can be configured.
Rack No.	This specifies the rack string and can be configured.
Frame No.	This specifies the frame string and can be configured.
Slot No.	This specifies the slot string and can be configured.
Sub slot No.	This specifies the sub slot string and can be configured.
L2 type	1. Determined automatically from the type of layer. 2. Two types are possible – atm and eth.
Port	In can be configured on a DRA (DHCP Relay Agent) instance. If not configured, then atm interface id, corresponding to DRA instance is used for this purpose.
VPI/VCI	Determined automatically from the VPI/VCI corresponding to the DRA instance.
Remote ID	Agent Remote id is a character string and can be configured on a DRA Instance.
Encapsulation type	In a TR-59 based architecture, the BRAS is responsible for shaping downstream traffic to the DSL line rate, or the service rate (which may be less than the line rate). If this is not done, then significant and indiscriminate packet loss can result. In the Ethernet aggregation scenario described by this recommendation, the BNG (broadband network gateway) will be shaping at the IP level, but the Layer 2 encapsulation added at the IP-DSLAM can increase packet overhead to the point where the physical line rate is exceeded. If the BNG knows the nature of this encapsulation, then the IP shaping rate can be adjusted accordingly. This section describes sub-options for use with the PPPoE VSA Tag / DHCP option-82 to signal the access loop encapsulation from the IP-DSLAM to the BNG.
Access loop characteristic	This solution is designed as an extension of the role of a Layer2 DHCP Relay Agent or a PPPoE Intermediate Agent in an IP-DSLAM, inserting the appropriate access loop characteristics (e.g. syncrate and interleaving delay) values while forwarding DHCP or PPPoE messages.

Spanning Tree Protocol

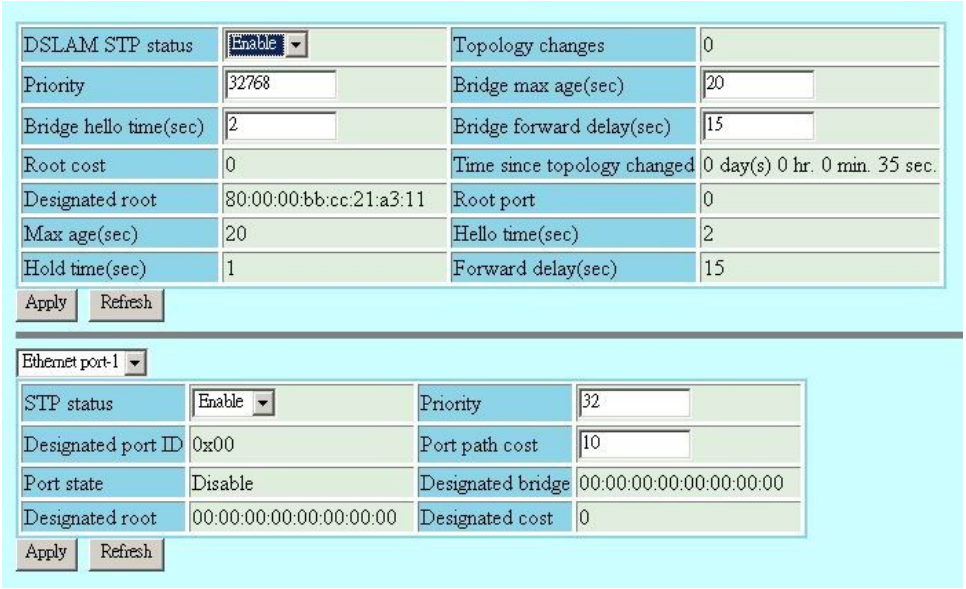
The spanning tree protocol allows you to configure the STP parameters on network Ethernet interface.

Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations. Multiple active paths between stations cause loops in the network. If a loop exists in the network topology, the potential exists for duplication of messages. When loops occur, some switches see stations appear on both sides of the switch. This condition confuses the forwarding algorithm and allows duplicate frames to be forwarded.

To provide path redundancy, Spanning-Tree Protocol defines a tree that spans all switches in an extended network. Spanning-Tree Protocol forces certain redundant data paths into a standby (blocked) state. If one network segment in the Spanning-Tree Protocol becomes unreachable, or if Spanning-Tree Protocol costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and reestablishes the link by activating the standby path.

STP is a technology that allows bridges to communicate with each other to discover physical loops in the network. The protocol then specifies an algorithm that bridges can use to create a loop-free logical topology. In other words, STP creates a tree structure of loop-free leaves and branches that spans the entire Layer 2 network.

Figure 7-59 Spanning Tree Protocol Setting Dialog



Refer to Table 7-40 Spanning Tree Protocol Dialog Description

Rapid Spanning Tree Protocol

Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol (802.1D standard) and provides for faster spanning tree convergence after a topology change.

Figure 7-60 Rapid Spanning Tree Protocol Setting Dialog

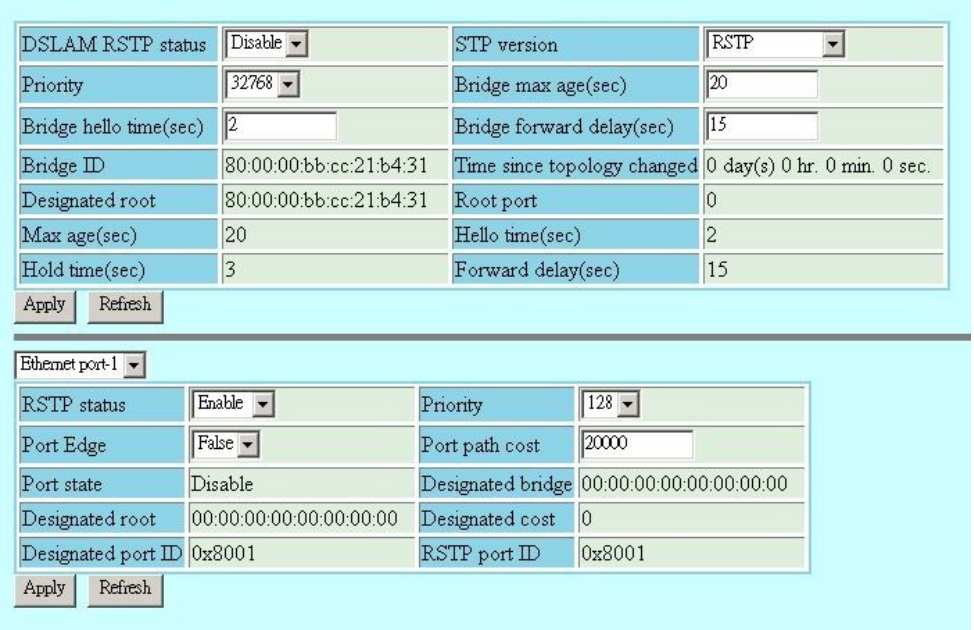


Table 7-40 Spanning Tree Protocol Dialog Description

Table 7-40 Spanning Tree Protocol Dialog Description

Item	Description
DSLAM STP status	Spanning Tree Protocol to be enabled on the Bridge or not.
Ethernet Port STP status	This specifies the STP status of Gigabit Ethernet interface.
	Press the '**Apply**' button to confirm the setting.
Set Spanning Tree Protocol Status	
STP Priority	This value can determine if the IP-DSLAM will be root switch among all known switches. The switch with the highest priority (lowest numeric value) becomes the Spanning Tree root switch. MAC address (the lowest numeric value) is used to decide root switch if priority is the same. **Valid values:** 0 ~ 61440 in steps of 4096
Time Since Top Changed	The time elapsed since the root node of the Spanning Tree has changed. The change of the root node will cause the Spanning Tree to reconfigure.
Top Changed	The count which the root node has changed in the existing Spanning Tree.
Designated Root	The root of current Spanning Tree indicating by its MAC address.
Root Cost	The cost configured in the DSLAM contributing to the path cost leading to the root
Root Port	The port number of the port which offers the lowest cost path from this bridge to the root bridge.
Max Age	The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of seconds, when this bridge is the root of the spanning tree.
Hello Time	The value that all bridges use for HelloTime when this bridge is acting as the root.
Forward Delay	The value that all bridges use for Forward Delay when this bridge is acting as

Table 7-40 Spanning Tree Protocol Dialog Description

Item	Description
	the root.
Hold Time	This time value determines the interval length during which no more than two Configuration bridge PDUs shall be transmitted by this node, in units of seconds.
Bridge Max Age	The maximum age time of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of seconds. **Valid values:** 6 ~ 40 (Seconds)
Bridge Hello Time	The amount of time between the transmission of Configuration BPDU (Bridge Protocol Data Units) by this node on any port when it is the root of the spanning tree or trying to become so, in units of second. **Valid values:** 1 ~ 30 (Seconds)
Bridge Forward Delay	This value, measured in units of seconds, controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used, when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database. **Valid values:** 4 ~ 30 (Seconds)
	Press the '**Apply**' button to confirm the setting.

SNTP Protocol

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 DAS3 Series 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.

Figure 7-61 SNTP Protocol Setting Dialog

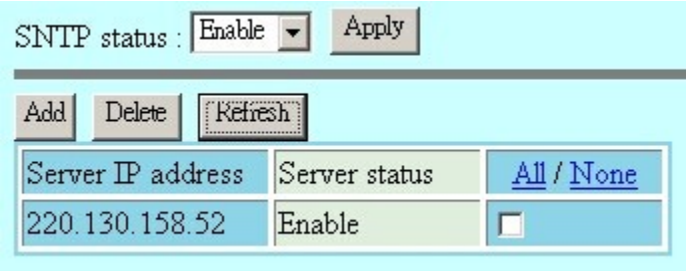


Table 7-41 SNTP Protocol Description

Item	Description
SNTP status	This indicates connection status between the DSLAM and the time server.
Server IP address	This indicates the time server the DSLAM tries to synchronize with.

IGMP Snooping

The IGMP Snooping allows you to view and change the IGMP Snooping administrate status.

IP traffic can be transmitted in one of either three ways: unicast (one sender to one receiver), broadcast (one sender to all members on the network) or multicast (one sender to a group of hosts). IGMP is a session-layer (layer-3) protocol used to establish membership in a multicast group.

Multicast addresses are Class D IP address, from 224.0.0.0 to 239.255.255.255. These addresses are also referred to as Group Destination Address (GDA). Each GDA address is associated with one MAC address. The GDA MAC address is constructed by joining 01:00:5E and the last 23 bits of the GDA multicast IP address in Hex. For example, GDA 224.1.1.1 corresponds to MAC address 01:00:5E:01:01:01

A layer-2 switch supported IGMP snooping can passively snoop on IGMP Query, Report and Leave packets transferred between Routers/Switches and hosts to learn the IP Multicast group membership. It snoops IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly.

Figure 7-62 IGMP Snooping Dialog

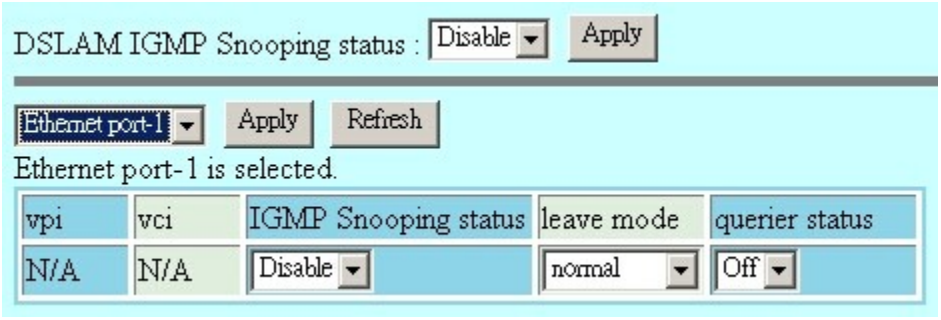


Table 7-42 IGMP Snooping Description

Item	Description
DSLAM IGMP Snooping Status	Specified whether or not IGMP Snooping is to be enabled in the system.
(Ethernet) Port ID	This specifies the network port interface.
VPI/VCI	This specifies the virtual path, circuit identification for the PVC in the port.
IGMP Snooping Status	A Bridge Port, for which IGMP Snooping needs to be enabled or disabled.
Leave Mode	IGMP Snooping Leave message processing mode for the port. If the mode is set to **'Normal'**, the Leave message is forwarded to the Querier and then based on the Query received from Querier the Leave processing is triggered. If the mode is set to **'Fast'**, the port is immediately deleted from that multicast group on Leave message reception and then the Leave message is forwarded. The mode should be set to 'Fast' for a port only if there is one host behind the port. This is because if there are multiple hosts behind the port then it will lead to traffic disruption for other hosts who might still be listening to that multicast group. If mode is set to **'FastNormal'**, the Leave message is forwarded and the Leave processing is triggered immediately without waiting for any trigger from the Querier. 'FastNormal' mode thus saves the delay (equal to the time taken for Leave message to reach router and Querier processing time for it and the time taken for Query to reach IGMP Snoop module) in Leave processing.
Querier Status (Ethernet port only)	This specifies whether the Ethernet port can become querier or no.

Multicast Profile

The DAS3 Series 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.

The multicast channel profile sets value of multicast group IP, it is a menu list of the Multicast Channel (multicast group; i.e. a TV channel) provided by the Content Service Provider (CSP) or Application Service Provider (ASP).

Figure 7-63 Multicast Profile Dialog

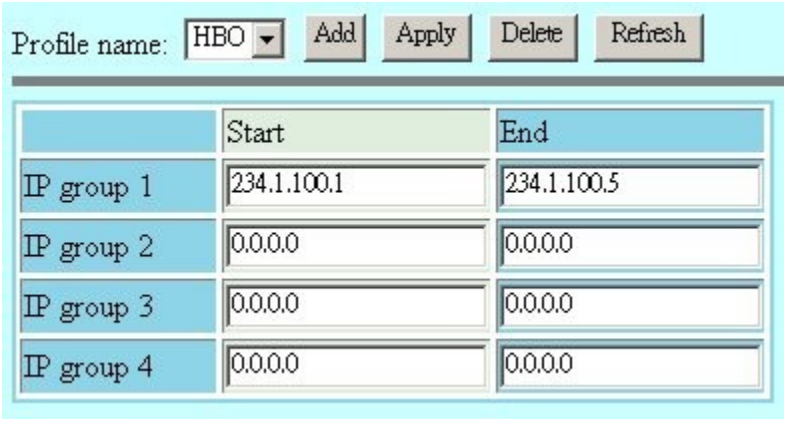


Table 7-43 Multicast Profile Description

Item	Description
Profile name	This specifies the multicast profile name.
IP group 1~4	This specifies the IP group 1~4.
Start	This specifies the ip address range group start.
End	This specifies the ip address range group end.

Multicast Profile Mapping

This section helps you to attach the multicast profile to the ADSL line interface.

Figure 7-64 Multicast Profile Mapping Dialog

Multicast VLAN Registration

DAS3 Series supports multicast VLAN, which is a concept of sending multicast traffic on one or more designated VLANs identified for multicast. A multicast VLAN is used for receiving downstream multicast, tagging, sending upstream IGMP reports, and creating layer 2 filtering entries.

A multicast VLAN provides efficient layer 2 replication in the aggregation network by using N:1 VLANs. Instead of coming on the same VLAN, the IGMP reports come on a 1:1 VLAN mapping and an edge device translates the VLANs of such IGMP reports to multicast VLAN. The learning is done based on the multicast VLAN, which is used for egress VLAN and corresponding tag when forwarding reports upstream. In the DSL deployment, the edge device acts as the access node. In the absence of this mapping, the upstream reports goes on 1:1 VLANs and learning also happen based on same. The downstream multicast streams for the same group is replicated for different subscribers as

the 1:1 VLANs are different for them in absence of multicast VLAN mapping.

Determination of a multicast VLAN is based on the incoming VLAN (virtual VLAN in case of VLAN stacking mode), Group IP, Source IP of multicast server, and subscriber port. The identification of a multicast VLAN for IGMP reports coming from subscribers over 1:1 subscriber VLANs is done by Columbia, where an upstream report is sent over the multicast VLAN. The downstream multicast as well as the query is received on the multicast VLAN and data is forwarded based on multicast filtering entries in the Data plane/ Forwarding plane while the query is appropriately handled by Protocol support on Control plane. Therefore, the learning of layer 2 filtering multicast entries is done based on the multicast VLAN.

A multicast VLAN allows source-based filtering in an aggregation network, which is a layer 2 network. In the aggregation network, the multicast entries are created at layer 2 by using the VLAN and multicast MAC addresses mapped from a group. Since, each source can be mapped to a corresponding multicast VLAN; entries can be made different for each source. Due to such entries in the aggregation network, and thus multicast VLANs also contribute to source-based filtering of multicast streams within layer 2 device.

MVR Channel

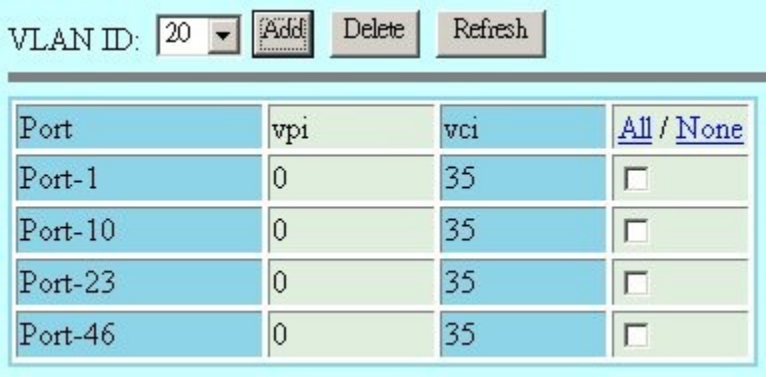
Configure multicast VLAN and group IP address.

Figure 7-65 MVR Channel Dialog

MVR VLAN

Configure member in multicast VLAN.

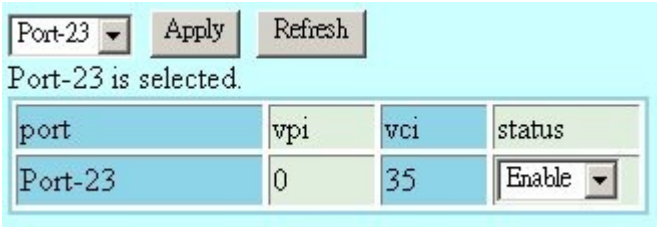
Figure 7-66 MVR VLAN Dialog



MVR PVC Enable

Enable or Disable PVC's MVR status.

Figure 7-67 MVR PVC Enable Dialog



This page is leave in blank for note or memo use

Chapter 7Diagnostic Menu

The diagnostic menu provides test function from ADSL physical layer to ATM layer. This chapter contains the following sections:

- DSL Bin Information
- ATM OAM Test
- ADSL2 DELT Test

DSL Bin Information

The allocation table shows both upstream and downstream bin bits and bin SNR status.

Figure 8-68 DSL Bin Information Dialog

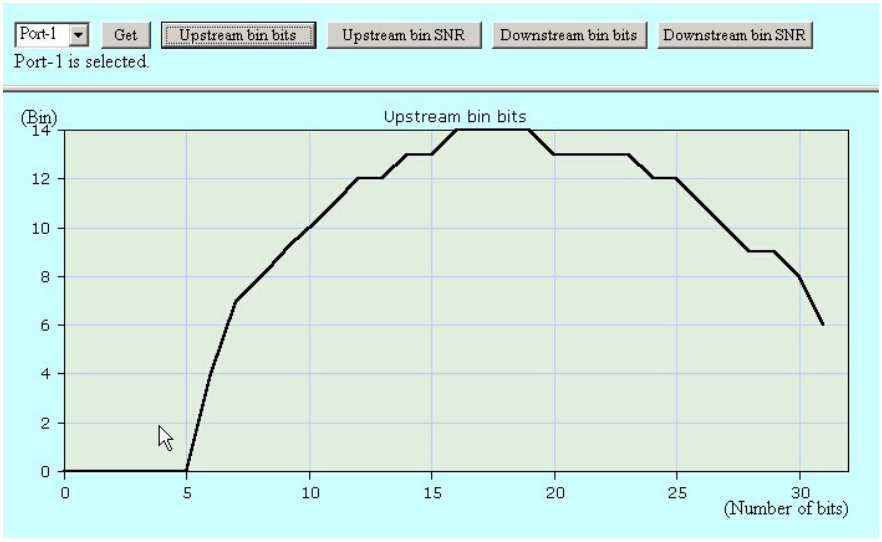


Table 8-44 describes the bin allocation tap items.

Table 8-44 DSL Bin Information Dialog

Item	Description
Get	Press '**Get**' button to get the DSL bin information, then press others button to show.
Upstream Bin Bits	Number of downstream bits/ bin for the bin indexed by this element of the string. The 0th element contains the number of bits per bin for 0, through the 31st element, which contains the number bits for bin 31. (upstream)
Upstream Bin SNR	The DELT-related parameter that provides an array of real downstream SNR (f) values in dB (Not available for ADSL and ADSL2plus)
Downstream Bin Bits	Number of upstream bits/ bin for the bin indexed by this element of the string. The 0th element contains the number of bits per bin for 0, through the 31st element, which contains the number bits for bin 31. (Downstream)
Downstream Bin SNR	The DELT-related parameter that provides an array of real upstream SNR (f) values in dB (Not available for ADSL and ADSL2plus)

ATM OAM Test

The ATM OAM test generates the ATM F5 loop-back to diagnose the ADSL port interface.

Operation Administration and Maintenance (OA&M) - OA&M is defined for supervision, testing, and performance monitoring. It uses loop-back for maintenance and ITU TS standard CMIP, with organization into 5 hierarchical levels: Virtual Channel (F5 - Between VC endpoints), Virtual Path (F4- between VP endpoints), and Transmission Path (F3- Between elements that perform assembling, disassembling of payload, header, or control), Digital Section (F2 Between section end-points, performs frame synchronization) and Regenerator Section (F1- Between regeneration sections).

Figure 8-69 ATM OAM Test Dialog

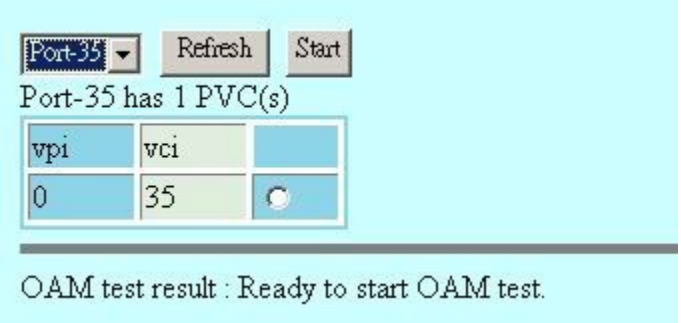


Table 8-45 describes the OAM test field items.

Table 8-45 ATM OAM Test Dialog

Item	Description
Port(vpi/vci)	Loop-back source id assigned to the ATM port. The ATM port will respond to all loop-back cells, which carry this OAM id. This parameter specifies the interface, virtual path, and virtual circuit for which information is desired.
Result	Use this command to display result of previous OAM loopback command. This specifies the result of the loop back test. It may be Result Unavailable, Seg Succeeded, Seg Failed, E2e Succeeded, E2e Failed, Test Aborted, or Test In Progress.

ADSL2 DELT Test

DELT is primarily used for reactive tests on a loop after a CPE has been deployed, either to help troubleshoot a line or to capture a baseline of loop characteristics at the time of installation.

DELT can determine the ADSL2+ data rate (up/down), loop attenuation (up/down), SNR (up/down), and noise (up/down).

Figure 8-70 ADSL2 DELT Run & Report Dialog

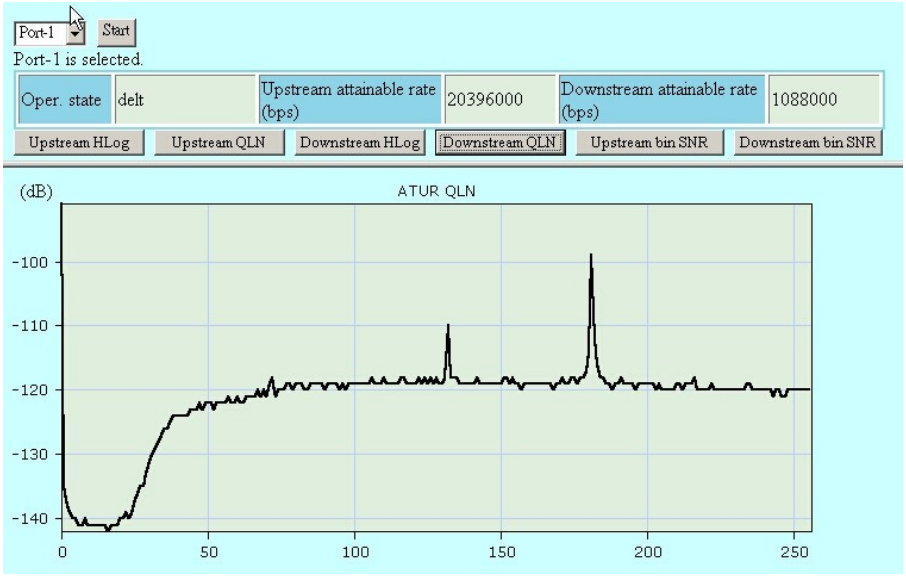


Table 8-46 Monitoring DELT Run & Report

Item	Description
Port selection menu	Please select a port to perform DELT.
Operation State	This object identifies the high level operational state for the ATU. Here is the state flow: data (Click START) → handshake → discovery → delt Training → delt (Diagram is displayed) ->handshake -> discovery → Training → data
ATUC Attainable net data rate	Indicates the maximum currently attainable data rate by the ATU. This value will be equal to, or greater than the current line rate. (Downstream)
ATUR Attainable net data rate	Indicates the maximum currently attainable data rate by the ATU. This value will be equal to, or greater than the current line rate. (upstream)
Upstream HLIN	The DELT-related parameter that provides an array of complex downstream Hlin (f) values in linear scale. (Not available for ADSL and ADSL2plus)
Upstream HLOG	The DELT-related parameter that provides an array of real downstream Hlog (f) values in dB. (Not available for ADSL and ADSL2plus)
Upstream QLN	The DELT-related parameter that provides an array of real downstream QLN (f) values in dB. (Not available for ADSL and ADSL2plus)
Downstream HLIN	The DELT-related parameter that provides an array of complex upstream Hlin (f) values in linear scale. (Not available for ADSL and ADSL2plus)
Downstream HLOG	The DELT-related parameter that provides an array of real upstream Hlog (f) values in dB. (Not available for ADSL and ADSL2plus)
Downstream QLN	The DELT-related parameter that provides an array of real upstream QLN (f) values in dB. (Not available for ADSL and ADSL2plus)

This page is leave in blank for note or memo use

1. 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
CPE	Customer Premises Equipment
CV	Coding Violation
DELT	Dual End Loop Testing
DSLAM	Digital Subscriber line Access Multiplexer
ES	Error Seconds
EOA	Ethernet over ATM
GE	Gigabit Ethernet
IP	Internet Protocol
LAN	Local Area Network
LCT	Local Craft Terminal
LOF	Loss of Frame
LOS	Loss of Signal
LPR	Loss of Power
OAM	Operation, Administration, and Maintenance
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
VDSL	Very high-speed Digital Subscriber line
VLAN	Virtual Local Area Network
VP	Virtual Path
VPI	Virtual Path Identifier
ATU-O	ADSL Transmission Unit at the Optical network interface
ATU-R	ADSL Transmission Unit at the remote end
WAN	Wide Area Network
xDSL	ADSL/VDSL

2. Index