DAS3series LCT

Software Operation Guide

Class:	User Guide
Product Version:	S.W. 1.4.3, LCT R1.5.7
Doc. No.:	BCD3-TM-E-130502
Doc. Version:	1.0
Publish Date:	2007

DAS3series LCT
Software Operation Guide
Text Part Number: 1305-0202

Table of Contents

List of Figures

List of Tables

Chapter 1 Preface

This preface discusses the following topic:

- Purpose
- Organization
- Conventions

Purpose

The purpose of this guide is to provide detailed information and description of DAS3series IP-DSLAM LCT (Local Craft Terminal), which includes software configuration and other specific features.

Organization

This guide contains the following information:

- Preface
- Getting Started the DAS3series LCT
- DAS3series LCT Operation Menus
- Appendix

Conventions

This publication uses the document conventions listed in this section.

NE/NEs mention in this document means DAS3series 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 2 Getting Started the DAS3series LCT

This chapter describes the DAS3series LCT (Local Craft Terminal), the instructions describes how to install the DAS3series LCT software and SNMP Service in your MS Windows.

- Installing the Management and Monitoring Tools
- Install and Uninstall the DAS3series LCT
- Configuring the DAS3series Community

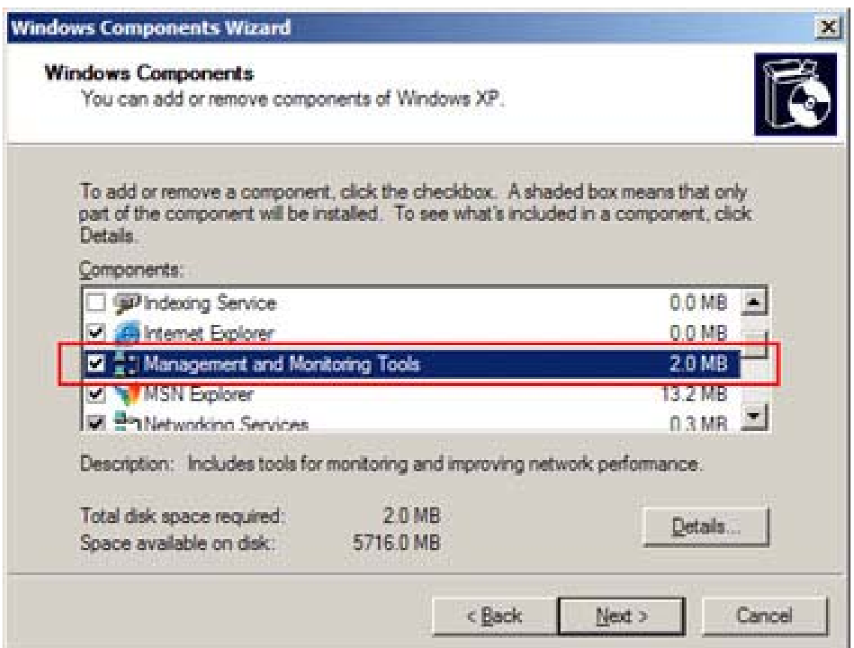
Installing the Management and Monitoring Tools

The management and monitoring tools for MS Windows can be found by the following steps.

Control Panel → Add or remove programs → Add/Remove Windows Components

Windows components wizard dialog appear as show in Figure 2-1, check the '**Management and Monitoring Tools**' at list box and click '**Next**' to install the components.

Figure 2-1 Windows Components Wizard Dialog



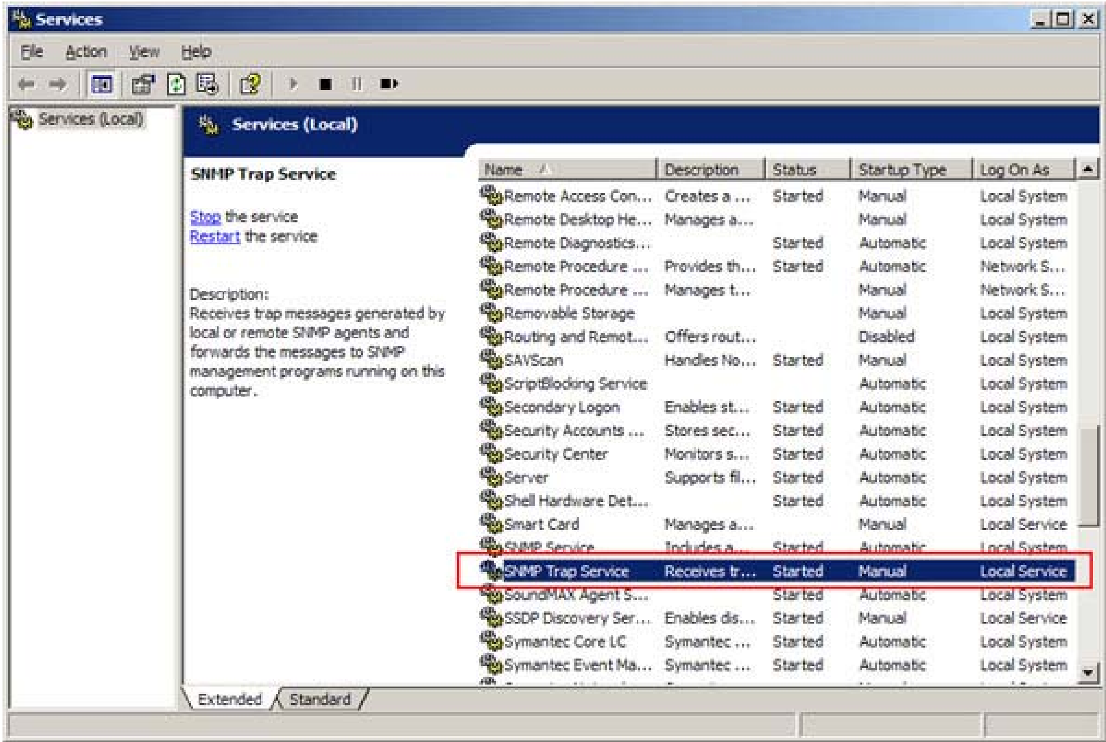
Once the '**Management and Monitoring Tools**' component was installed, you have to manually enable the '**SNMP Trap Service**' from the Service dialog as show in Figure 2-2.

Start → All Programs → Administrative Tools → Services

NOTE

If the '**Administrative Tools**' does not appearing in your All Program menu, point your mouse cursor at '**Start**' button and click right mouse button to pop-up the option menu, select the '**Properties**' customize your Start menu in Advance tag to call the '**System Administrative Tools**'.

Figure 2-2 Windows System Services Dialog



Make sure the SNMP Trap Service is operated in '**Started**' status.

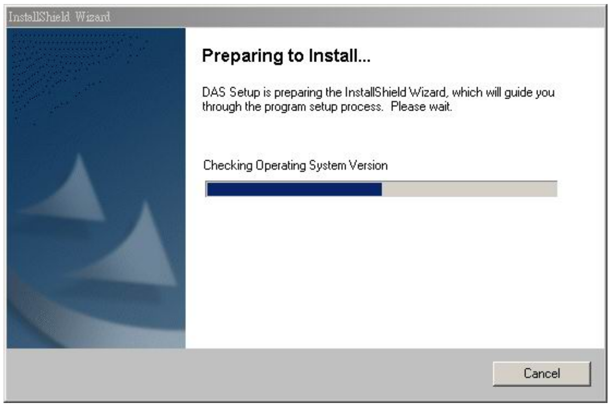
NOTE To ensure DAS3series LCT receive the SNMP traps reported from managed NEs, make sure the '**SNMP Trap Service**' at started status at all time. Some of firewall may block the received traps, configure the UDP port 162 (default) in exception list of your firewall.

Install and Uninstall the DAS3series LCT

Install Software

Double click the executive file to install DAS3series LCT software.

Figure 2-3 Preparing to Install Dialog



Click '**Next**' button to start installation.

Figure 2-4 DAS3series LCT Install Wizard at Welcome

The DAS3series LCT will installed under the directory of '**/Program File/LCT**'.

Figure 2-5 DAS3series LCT Install Wizard at Installing Process

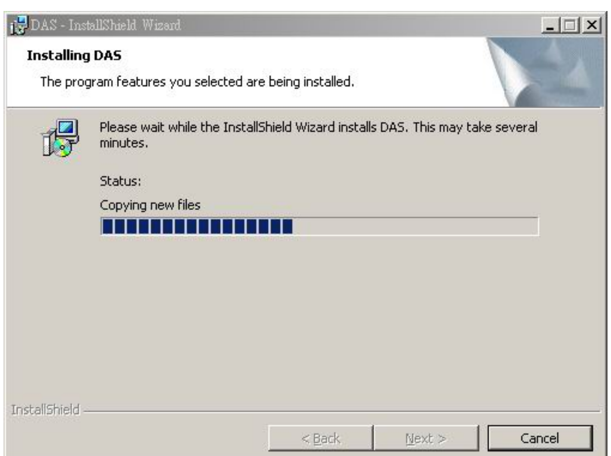
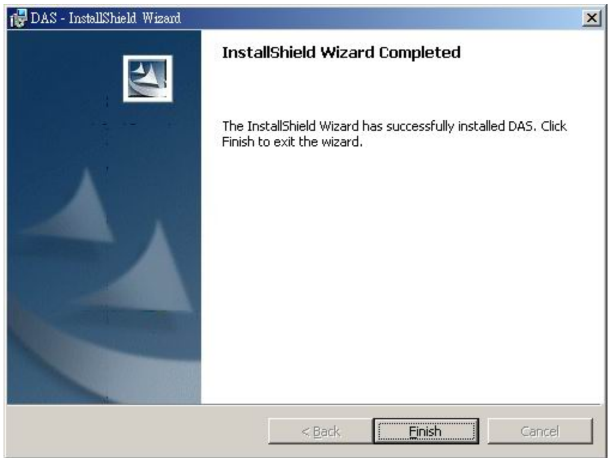


Figure 2-6 DAS3series LCT Install Wizard at Completed



Click '**Finish**' to end the installation,

Uninstall LCT Software

Uninstall the DAS3series LCT software can be done through '**Add or Remove Programs**' at Control Panel.

Execute LCT Software

DAS3series LCT can be accessed through **Start → All Programs → LCT → DAS3series LCT**.

To update the new version of DAS3series LCT, you have to uninstall the previous version before do so.

Configuring the DAS3series Community

This section describes the DAS3series IP-DSLAM network Ethernet IP and SNMP Host/Community initial setting to engage with the DAS3series LCT. Task those setting by access to **CLI Ex** mode.

Access to **CLI Ex** mode via the Console Port can be done using a VT100-compatile terminal directly connected.

To access the **CLI Ex** mode via a direct VT100-compatible terminal connection to the Console Port, use the following procedure:

Table 2-1 DAS3series Console Management Setting

Parameter	Setting
Baud rate	9600
Data bits	8
Parity	None
Start bits	1
Stop bits	1
Flow control	None

Refer to *DAS3series IP-DSLAM System Configuration Guide "Chapter 2 Access via the Console Port"* for detail information.

Two settings of DAS3series need to be initialized before connecting to DAS3series using LCT, the IP address of network Ethernet interface and the SNMP community setting.

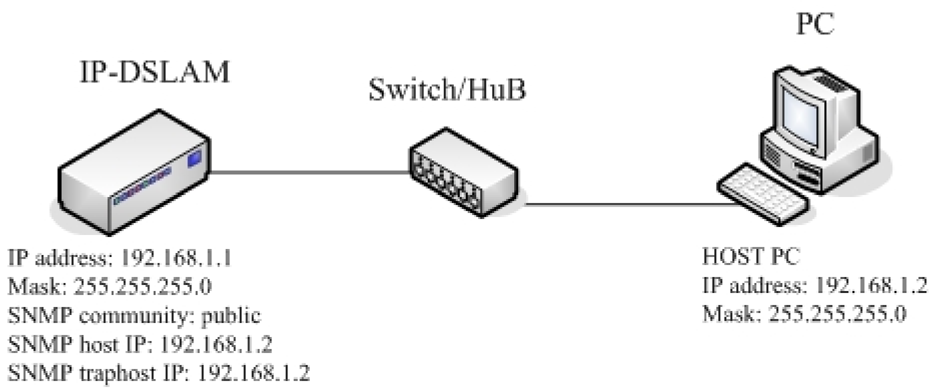
The network Ethernet interface setting refer to *DAS3series IP-DSLAM System Configuration Guide "Chapter 4 Developing the GE Network Management Connection"* for detail information.

The SNMP community setting refer to *DAS3series IP-DSLAM System Configuration Guide "Chapter 3 Configuring the SNMP Status"* for detail information.

Example **DAS3series on-line Initial Setting at CLI Ex mode**

Example below demonstrates the command of default setting to engage with the DAS3series LCT.

Figure 2-7 **Management Connection Example**




```
#wizard ethernet 3 ip 192.168.1.1 mask 255.255.255.0

$create ethernet intf ifname eth-3 ip 192.168.1.1 mask 255.255.255.0

Entry Created

$create snmp comm community public rw

Entry Created

Community          Access
-------------------------
public             RW

$create snmp host ip 192.168.1.2 community public

Entry Created

Host Address              Community
-----------------------------------
192.168.1.2              public

$create snmp traphost ip 192.168.1.2 community public

Entry Created

Ip Address : 192.168.1.2
Community  : public
Port       : 162       Version : v2c
Severity   : critical major minor info
```

> **NOTE** The default SNMP trap community port is 162.

Chapter 3 DAS3series LCT Operation Menus

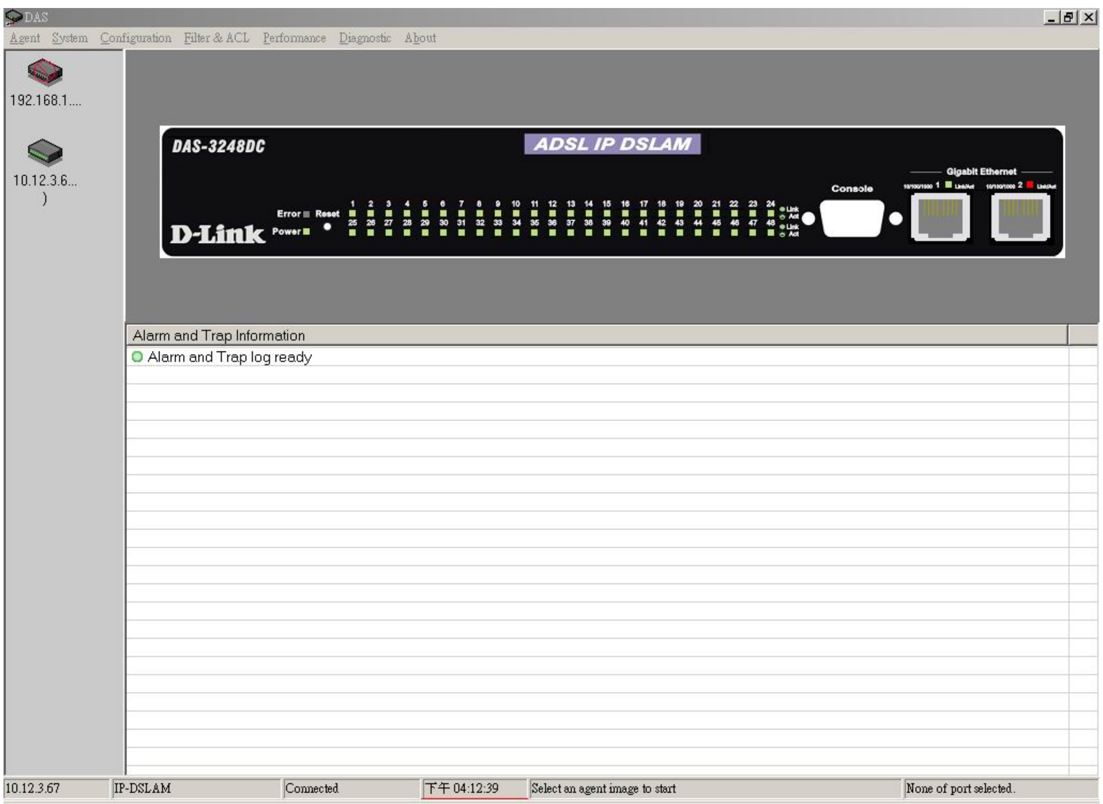
The chapter provides the detail descriptions on software configurations and administrating procedures for DAS3series LCT. This chapter contains the following sections:

- Operation Window Overview
- Agent Menu
- System Menu
- Configuration Menu
- Filter & ACL Menu
- Performance Menu
- Diagnostic Menu

Operation Window Overview

The DAS3series LCT operation window contains main menu, agent list, alarm and trap information list and real-time LED status panel.

Figure 3-1 DAS3series LCT Operation Window



You can point your mouse cursor at the real-time status panel and click right mouse button to pop-up the configuration menu. The pop-up menu will appear the relative menu according to cursor position, i.e. the ADSL port and the network Ethernet port will have different pop-up menu.

Agent Menu

The agent menu allows you to manage your DAS3series IP-DSLAM.

Add an Agent

Open the '**Add an Agent**' from agent menu to add a new DAS3series IP-DSLAM.

Figure 3-2 Add an Agent Dialog

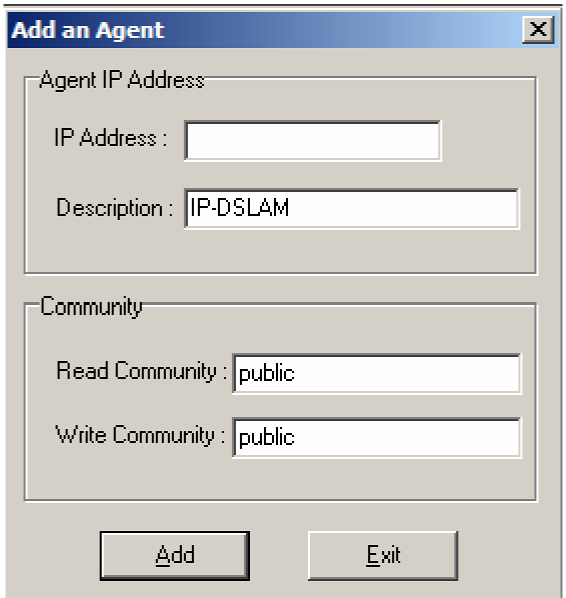


Table 3-1 describe fields appear in the Add an Agent dialog, insert the control information in text box and click '**Add**' to add new DAS3series IP-DSLAM agent, the number of agents can be add is depend on your system memory.

Table 3-1 Configuring the Add an Agent Dialog

Item	Description
Agent IP Address	
IP Address	This specifies the user name and password to be created. **Valid values:** Any valid class A/B/C address
Description	This indicates the privilege level of the user. **Valid values:** String of up to 64 characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_') and any combination of printable characters excluding ';'.
Community	
Read Community	This specifies the community name for read permissions. **Valid values:** String of up to 20 characters (All characters except ';', '?', and empty space)
Write Community	This specifies the community name for write permissions. **Valid values:** String of up to 20 characters (All characters except ';', '?', and empty space)

Delete an Agent

Select an agent from agent list to delete.

Save Agent Configuration

Use this function to save the agent list, all agent created without save will be lost due to exit of DAS3series LCT software.

Ping an Agent

Use this function to Ping selected agent from the agent list. A window will pop-up to display information as it was done manually by using Ping command follow agent IP.

System Menu

System menu contains data information of selected agent (DAS3series).

General Information

You can edit the system information in this dialog.

Figure 3-3 System General Information Dialog

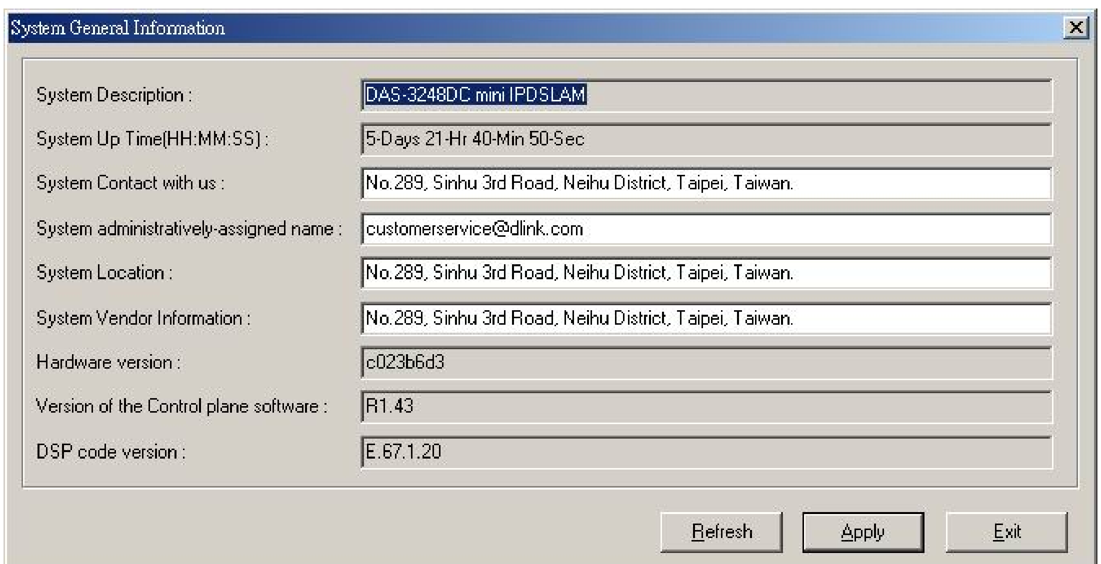


Table 3-2 describes the general information dialog field items.

Table 3-2 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.

Table 3-2 Modifying the System Information

Item	Description
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 ‘;’.
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

User and Password

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

Figure 3-4 User & Password Dialog

Click ‘Add’ button to create a new user.

Figure 3-5 Add New User Dialog

Two users can be adding to a single DAS3series IP-DSLAM.

The users manage in here are only for Telnet access, the '**superUser**' 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. **superUser** – Owns shows, add, delete, and modify privilege. **user** – Owns show privilege only.

Statistics Information

The statistics information dialog monitors current system network status.

Figure 3-6 System Statistics Information Dialog

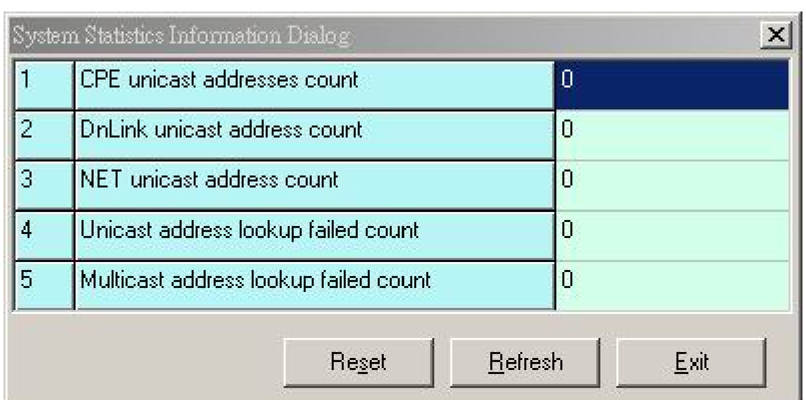


Table 3-4 describes the system (DAS3series) statistics information field items.

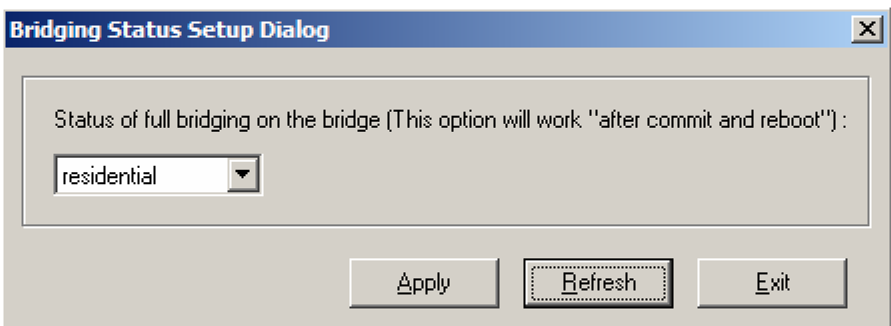
Table 3-4 Monitoring the System Statistics Information

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.

Bridging Status Setup

The bridging status in this field control entire system's bridging behaviors. There are three modes of bridging: **residential**, **restricted**, and **unrestricted**.

Figure 3-7 Bridging Status Setup Dialog



The **residential** bridging will direct packets coming from CPE side to be forwarded to the network side port without a lookup. This is the most commonly used mode.

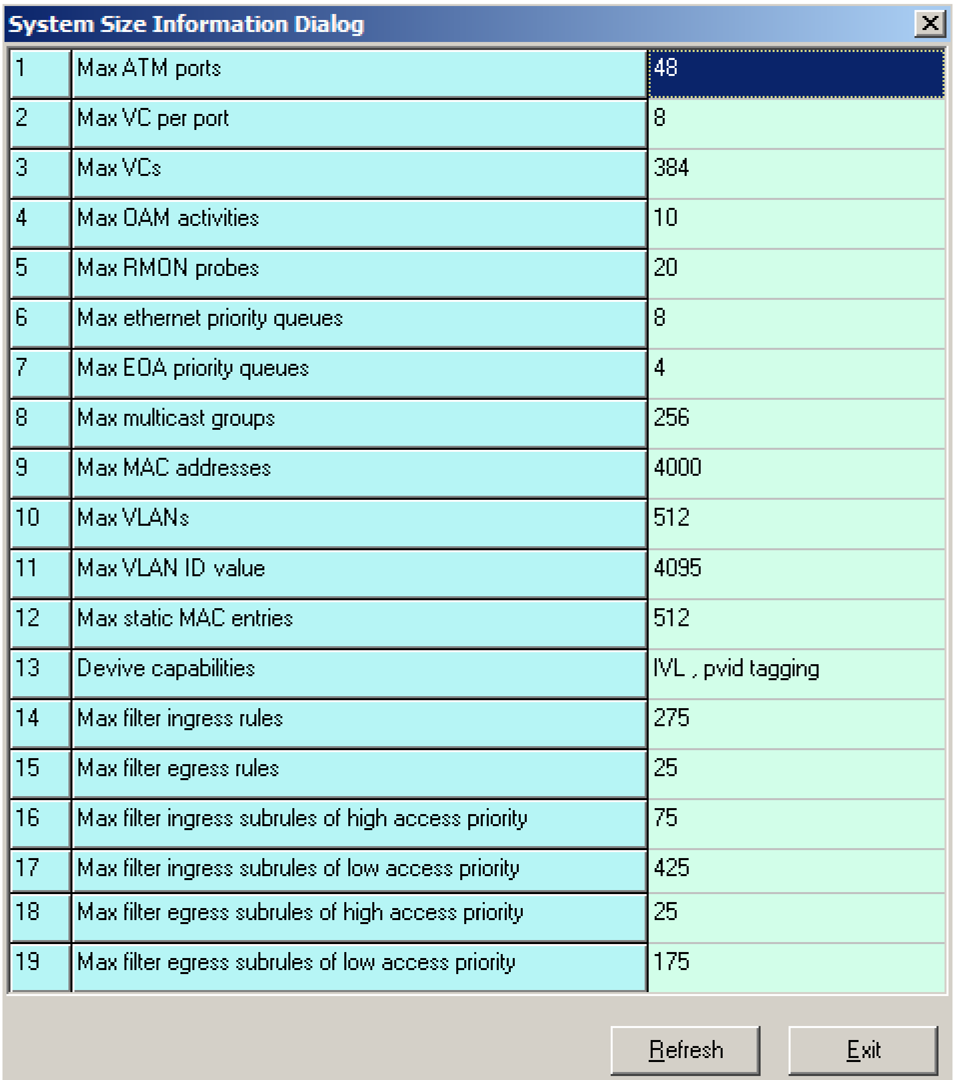
The **restricted** bridging will direct the packets undergo a MAC address lookup and if the destination is another CPE port, the packets would be dropped. Thus, CPE to CPE traffics are not allowed.

The **unrestricted** bridging will force packets to be forwarded based MAC address lookup under all cases.

System Size Information

The system size shows the maximum values of particular field where the system is capable to process.

Figure 3-8 System Size Information Dialog



1	Max ATM ports	48
2	Max VC per port	8
3	Max VCs	384
4	Max OAM activities	10
5	Max RMON probes	20
6	Max ethernet priority queues	8
7	Max EOA priority queues	4
8	Max multicast groups	256
9	Max MAC addresses	4000
10	Max VLANs	512
11	Max VLAN ID value	4095
12	Max static MAC entries	512
13	Devive capabilities	IVL , pvid tagging
14	Max filter ingress rules	275
15	Max filter egress rules	25
16	Max filter ingress subrules of high access priority	75
17	Max filter ingress subrules of low access priority	425
18	Max filter egress subrules of high access priority	25
19	Max filter egress subrules of low access priority	175

Table 3-5 describes the system size information field items.

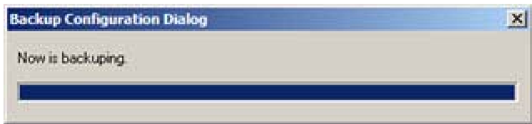
Table 3-5 Monitoring the System Size Information

Item	Description
Max ATM Ports	Maximum number of ATM ports
Max VC per Port	Maximum number of VCs possible per ATM port
Max VCs	Maximum number of VCs possible in the system.
Max OAM activities	Maximum number of OAM activities that are active at a time.
Max RMON probes	Maximum number RMON probes that can be applied simultaneously in the system.
Max Eth Priority queues	This specifies the max number of priority queues that can be configured on a bridge port created over an Ethernet interface.
Max EOA Priority queues	This specifies the max number of priority queues that can be configured on a bridge port created on EOA interface.
Max Multicast groups	Maximum number of multicast groups that are configured in the system.
Max MAC addresses	Maximum number of MAC addresses that are learned by the system.
Max VLANs	Maximum number of VLANs supported.
Max VLAN Id Value	Maximum values of VLAN ID that the bridge can support.
Max static Mac entries	Maximum number of static unicast entries.
Device Capabilities	Device capabilities of the bridge.
Max filter ingress rules	Maximum number of generic filter ingress rules that can be created.
Max filter egress rules	Maximum number of generic filter egress rules that can be created.
Max filter ingress subrules of high access priority	Maximum number of generic filter ingress sub rules of high access priority that can be created.
Max filter ingress subrules of low access priority	Maximum number of generic filter ingress sub rules of low access priority that can be created.
Max filter egress subrules of high access priority	Maximum number of generic filter egress sub rules of high access priority that can be created.
Max filter egress subrules of low access priority	Maximum number of generic filter egress sub rules of low access priority that can be created.

Backup Configuration

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

Figure 3-9 Backup Configuration Dialog



Restore Configuration

Use Restore Configuration function to retrieve the configuration data from exterior device to system.

Figure 3-10 Configuration Restore 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 3-11 System Commit Dialog

Commit action takes around 20 seconds to accomplish.

Reboot System

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

Figure 3-12 System Reboot Dialog

Restore Factory Configuration

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

Figure 3-13 Restore Factory Configuration

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

Table 3-6 DAS3series System Factory Default Parameters

Item	Description
ADSL Layer	
VPCI (VPI/VCI)	0/35 for each ADSL port interface.
Encapsulation	LLCMUX
Standard	ADSL2plus
Bridge Layer and Ethernet IP	
Bridge mode	Residential bridged mode
Ethernet port 1 IP address	192.168.1.1 / 255.255.255.0, Uplink
Ethernet port 2 IP address	0.0.0.0 / 0.0.0.0, Downlink
Management	
SNMP community	public (re-write privilege)
Telnet Username / Password	dnld / dnld

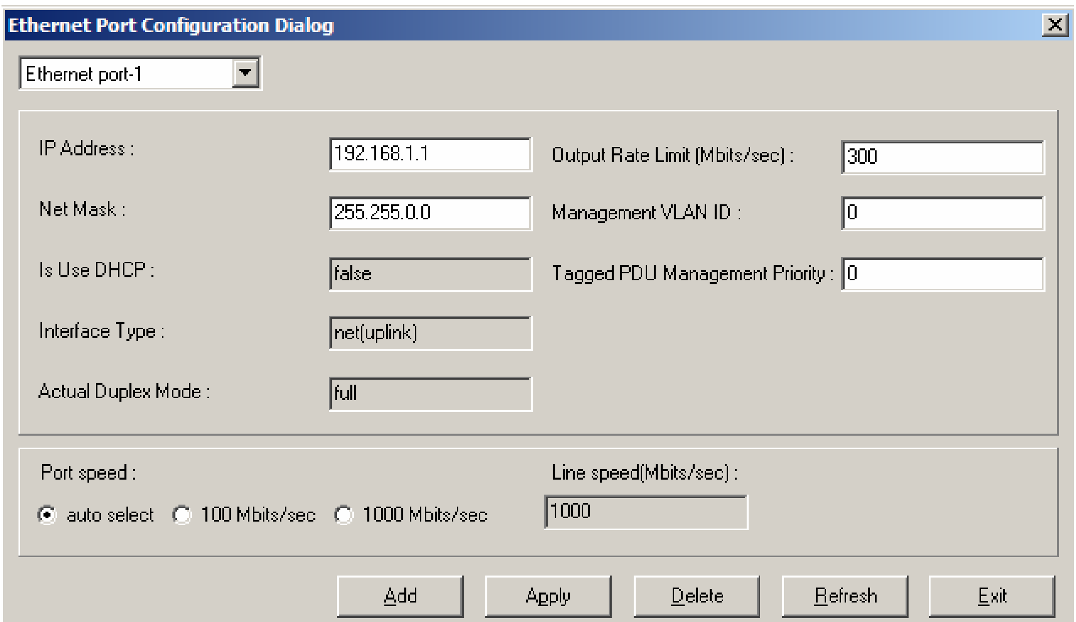
Configuration Menu

The Configuration menu contains physical interface setting, network Ethernet and ADSL port, as well as unicast and multicast for up layer service setting.

Ethernet Interface

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

Figure 3-14 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.

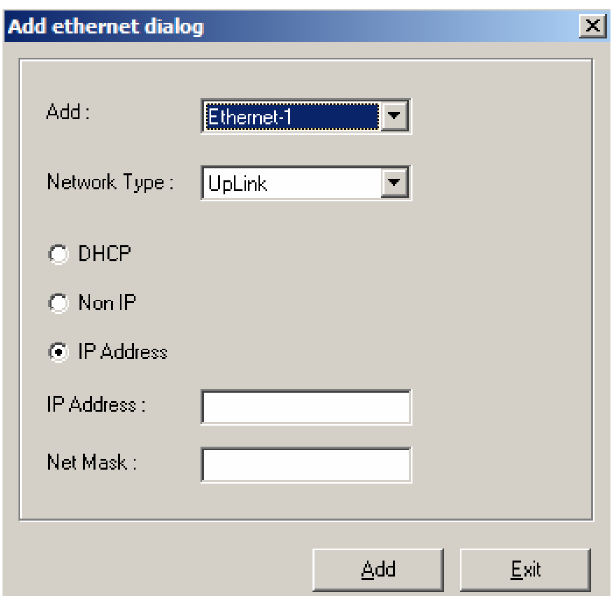
Table 3-7 Monitoring the Ethernet Port

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, uplink or downlink.
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

Table 3-7 Monitoring the Ethernet Port

Item	Description
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 'Is used 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
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 'Is used 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.

Figure 3-15 Add Ethernet Port Dialog



DAS3series IP-DSLAM supports two Ethernet interfaces. The IP address is only for management purpose and each Ethernet interface can apply its own IP address.

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 3-8 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.
DHCP	The DHCP is not support due to entity is managed under DAS3series LCT.
Non IP	Select Non IP to restrict the IP management activity.
IP Address	
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

PVC Management

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

ATM (Asynchronous Transfer Mode) is more efficient than synchronous technologies like time-division multiplexing (TDM). With TDM, each station or users is pre-assigned some time slots, and no other station can send in that time slot. With ATM being asynchronous in nature, time slots are available on demand.

ATM supports integrated voice, data, and video communications. In ATM the information to be transmitted in divided into short 53 byte packets or cells, which have a 5 byte header. The reason for such a short cell length is that ATM must deliver real time service at low bit rates and thus it minimizes packetization delay. ATM networks are connection oriented with virtual channels and virtual paths. The virtual channel carries one connection while a virtual path may carry a group of virtual channels. This ensures that cell sequence is maintained throughout the network. The virtual channel is identified by the Virtual Channel Identifier, (VCI), and the virtual path is identified by the Virtual Path Identifier, (VPI). Both the VCI and VPI may change within the network and they are stored in the header of the cell.

AAL (ATM Adaptation Layer) makes the ATM layer services more adaptable to specific services. The specific services may include user services, control services and management services. The AAL is the layer above the ATM layer and it is responsible for converting the information from the higher layers into 48 byte lengths so that the ATM layer can add the 5 byte header to make the 53 byte cell. The two main functions of this AAL are to provide functions needed to support applications and to break up information into units that will fit into cells. There are five AAL layers and each layer is loosely associated with the class of traffic to be carried. AAL1 is designed to support constant bit rate, connection oriented, and synchronous traffic such as uncompressed video transmission. AAL2 is never completed, but it was envisioned to be assigned for variable bit rate, connection-oriented, synchronous traffic. AAL3/4 supports variable bit rate, connection oriented, and asynchronous traffic or connectionless packet data. AAL5 is the primary AAL for data and supports both connection oriented and connectionless data.

Figure 3-16 PVC Management Dialog

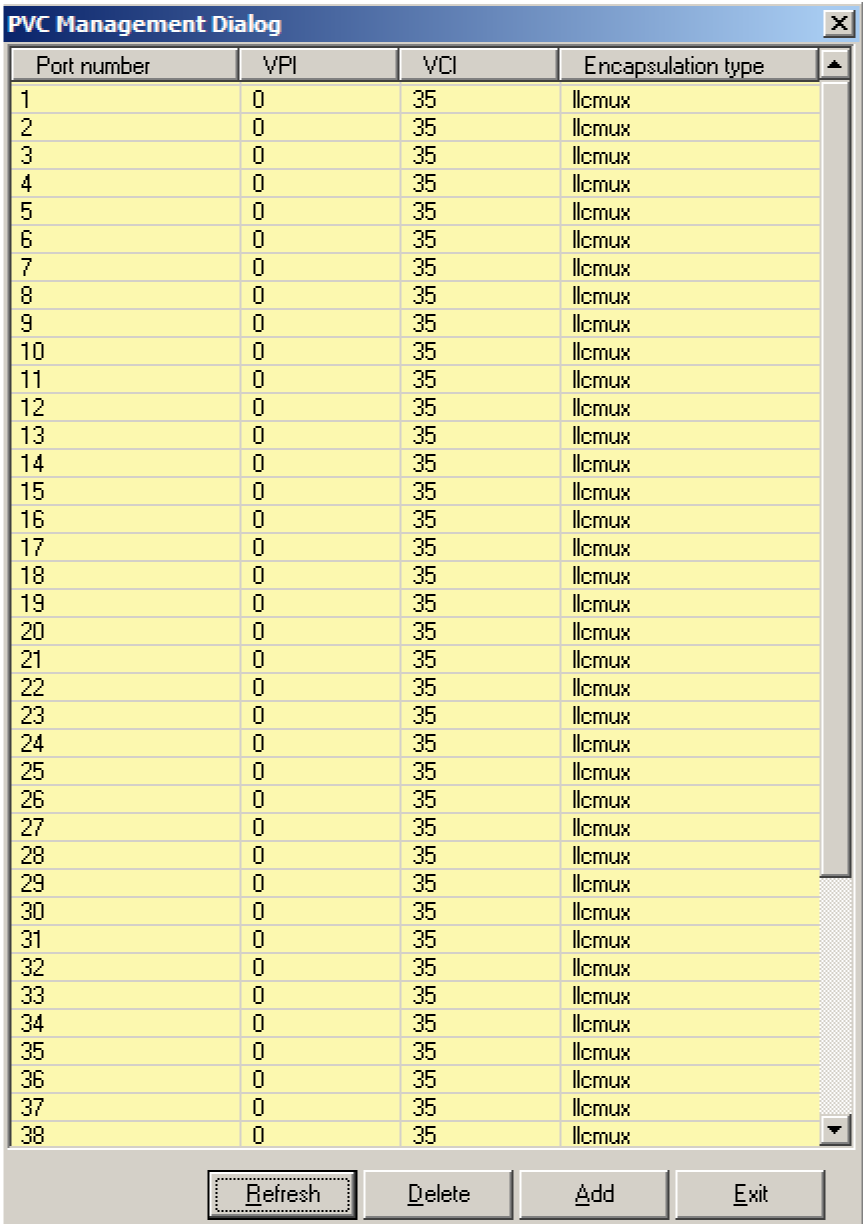


Table 3-9 describes the column status of PVC management dialog.

Table 3-9 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.

Table 3-9 Monitoring the PVC Management

Column Item	Description
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.

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 3-17 Port & PVC Add Dialog

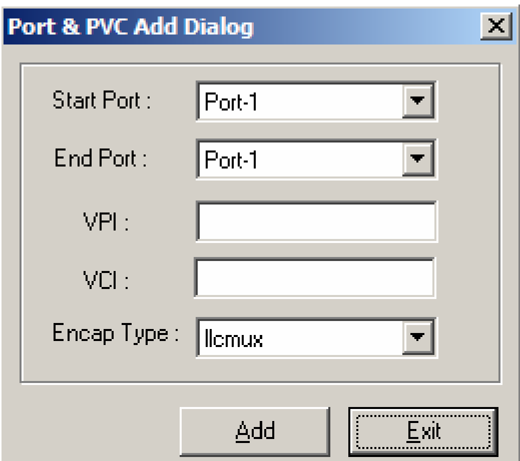


Table 3-10 describes the Port & PVC Add dialog field items.

Table 3-10 Creating the Port PVC

Item	Description
Start Port	This specifies the starting ADSL port interface for ATM PVC configuration.
End Port	This specifies the ending 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)

Table 3-10 Creating the Port PVC

Item	Description
Encap 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.

Enable / disable port

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

Figure 3-18 Enable / Disable port Dialog

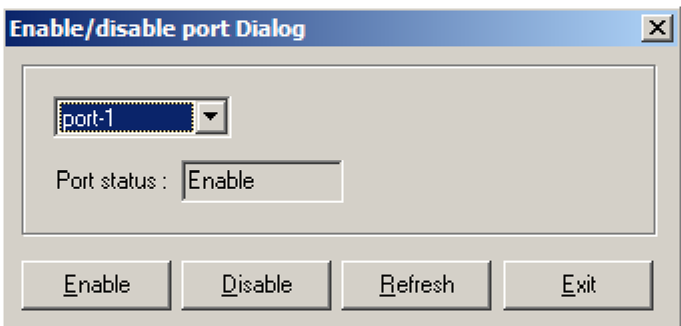


Table 3-11 Enable / Disable port

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

Line 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 ADSL port. Enter the control values to the text box and click '**Apply**' to activate.

Figure 3-19 Line Profile Configuration Dialog

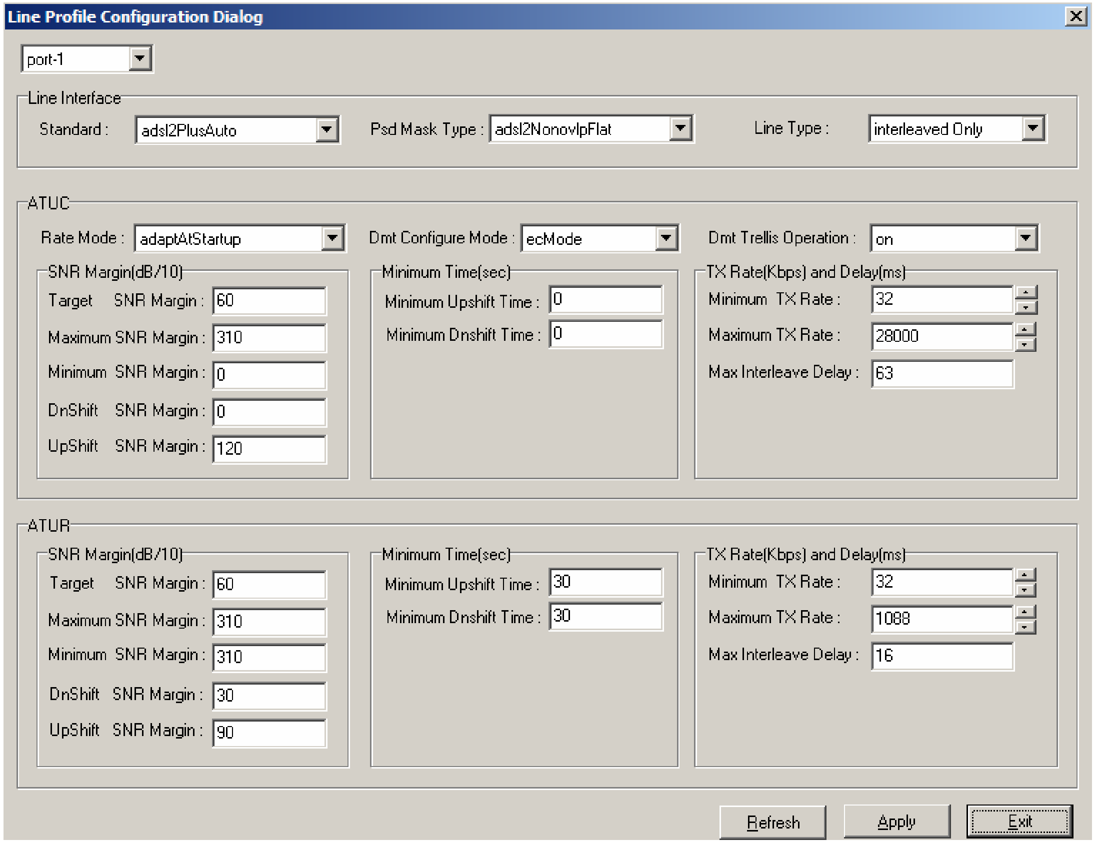


Table 3-12 describes the full ADSL connection parameters, click '**Enable Port**' button to activate the select ADSL port interface, the connection will not be able to establish in disabled status.

Table 3-12 Configuring Line Profile

Item	Description
Line Interface	
Standard	Preferred standard compliance. Outcome is dependent upon standard support of the remote unit.
Psd Mask Type	This parameter selects the PSD mask option to be used.
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.
ATUC	
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.
Dmt Configure Mode	This specifies the DMT configure mode. **ecMode** – Echo Cancellation Mode. The up-stream signal **overlaps** the lower spectrum of the down-stream signals. The overlap is resolved by Echo Cancellation. **fdmMode** – Frequency Division Multiplexing. Three separate bands are allocated to POTS, Upstream and Down-stream.
Dmt Trellis Operation	This parameter enables/disables Trellis coding. Trellis coding should always be enabled for its clear performance advantage.
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)
DnShift SNR Margin	Configured Signal/Noise Margin for rate downshift. If the noise margin falls below this level, the modem should attempt to decrease it's transmit rate. In the case that RADSL mode is not present, the value will be 0. **Valid values:** 0 ~ 310 (dB/10)

Table 3-12 Configuring Line Profile

Item	Description
UpShift SNR Margin	Configured Signal/Noise Margin for rate upshift. If the noise margin rises above this level, the modem should attempt to increase it's transmit rate. In the case that RADSL is not present, the value will be 0. **Valid values:** 0 ~ 310 (dB/10)
Minimum Time (ATUC/ATUR)	
Minimum Upshift Time	Minimum time that the current margin is above UpshiftSnrMgn before an upshift occurs. In the case that RADSL is not present, the value will be 0. **Valid values:** 0 ~ 16383
Minimum Dnshift Time	Minimum time that the current margin is below DownshiftSnrMgn before a downshift occurs. In the case that RADSL is not present, the value will be 0. **Valid values:** 0 ~ 16383
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)
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)
Select a port	Select the ADSL port interface to be display with relative parameters.

Power Management

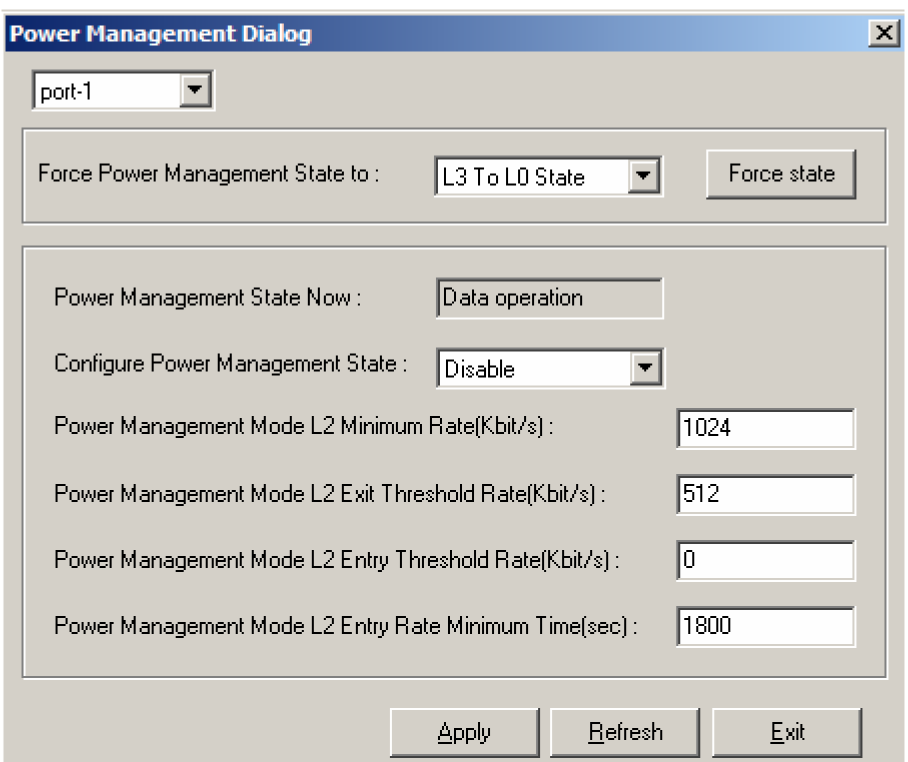
The power management allows you to furnish the efficiency of ADSL power output.

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 reduce overall power consumption while maintaining ADSL's "always-on" functionality for the user. These modes include 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 re-initializing and entering into steady-state communication mode.

Figure 3-20 Power Management Dialog



Click '**Apply**' button to submit the control values of selected ADSL port.

Table 3-13 Configuring the Power Management

Item	Description
Port selection pull down menu	Select the ADSL port interface to be display with relative parameters.
Force Power Management State to	Power management state forced. Defines the line states to be forced by the near-end (ATU-C) on this line.
Power Management State Now	The Line Power Management status, not available for ADSL connection. **Status:** Data Operation, Idle Operation, L2 Operation
Configure Power Management State	PM-related parameter used by ATU-C to set the allowed link states. Both bit values can be given simultaneously in the input.
Power Management Mode L2 Minimum Rate	PM 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)
Power Management Mode L2 Exit Threshold Rate	PM configuration parameter. L2 state **exit** data rate. **Valid values:** 0 ~ 30000
Power Management Mode L2 Entry Threshold Rate	PM configuration parameter. L2 state **entry** data rate. **Valid values:** 0 ~ 30000
Power Management Mode L2 Entry Rate Minimum Time	PM configuration parameter. Min L2 **entry** rate time **Valid values:** 900 ~ 65535

Alarm Profile Configuration

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 specific option reach the given values (in seconds), the system will send the SNMP trap.

Figure 3-21 Alarm Profile Dialog

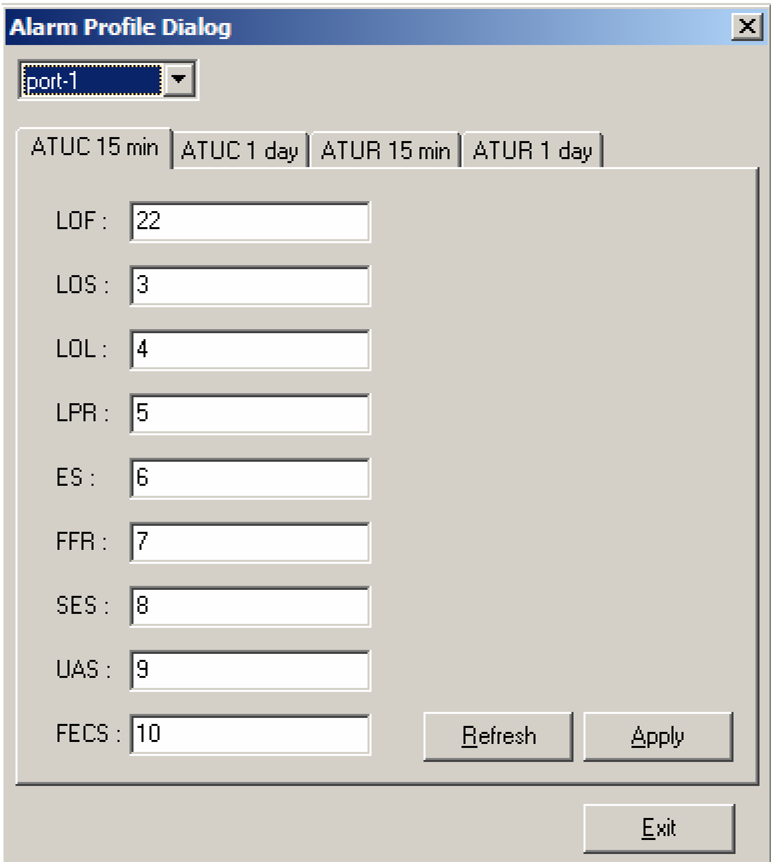


Table 3-14 describes the alarm profile dialog option items.

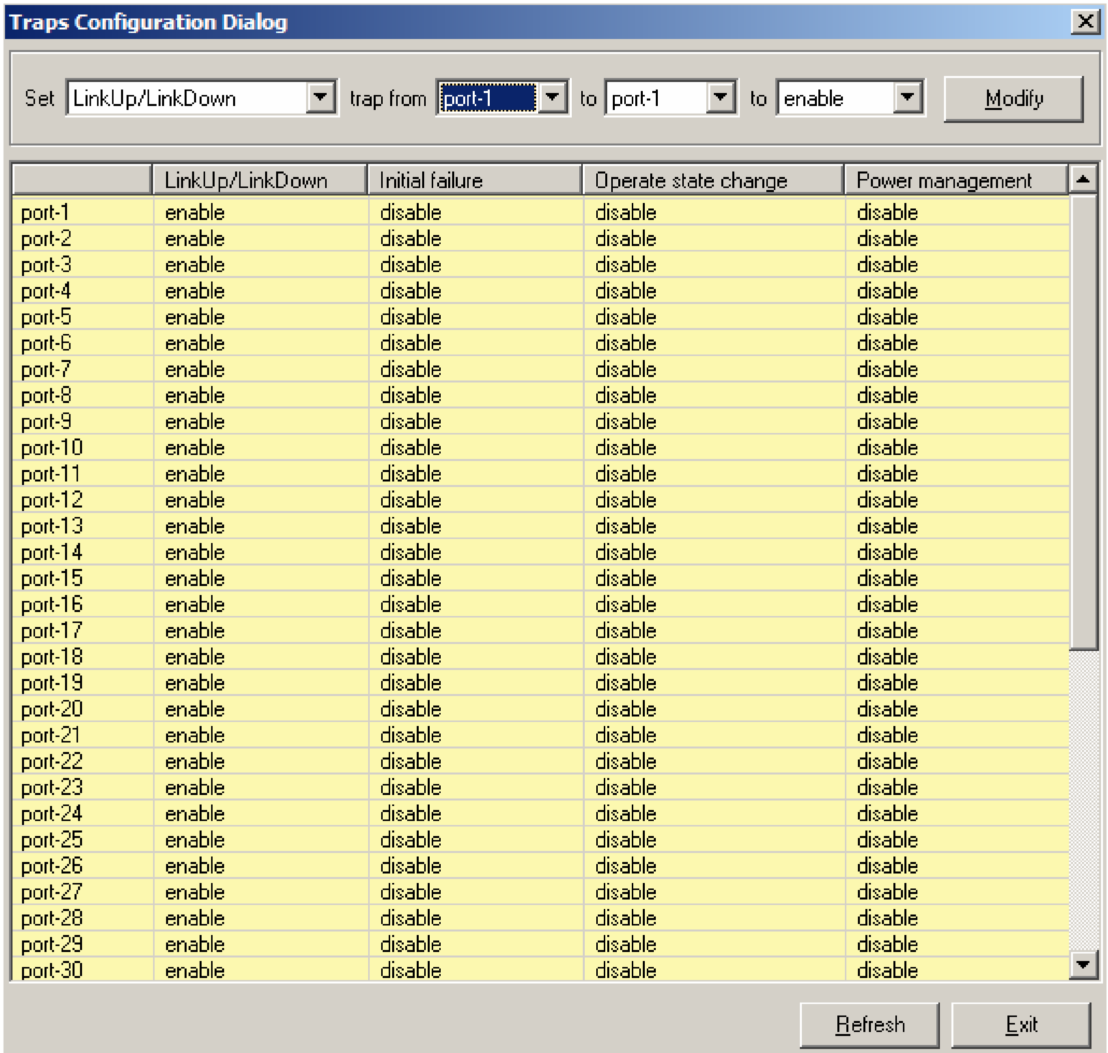
Table 3-14 Configuring the Alarm Profile

Item	Description
ATUC 15 min / ATUR 15 min	
	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 performance data collection period.
LOS(sec)	The number of Loss of Signal Seconds encountered by an ADSL interface, within any given 15 minutes performance data collection period.
LOL (sec)	The number of Loss of Link Seconds encountered by an ADSL interface, within any given 15 minutes performance data collection period.
LPR (sec)	The number of Loss of Power Seconds encountered by an ADSL interface, within any given 15 minutes performance data collection period.
ES (sec)	The number of Error Seconds encountered by an ADSL interface, within any given 15 minutes performance data collection period.
FFR (sec)	The number of failed retrains encountered by an ADSL interface within any given 15 minute performance data collection period, which causes adslAtucFailedFastRTrap.
SES (sec)	The number of Severe error seconds encountered by an ADSL interface within any given 15 minute performance data collection period, which causes adslAtucSesLTrap.
UAS (sec)	The number of unavailable error seconds encountered by an ADSL interface within any given 15 Minute performance data collection period, which causes adslAtucUasLThreshTrap.
FECS (sec)	The number of Forward error correction seconds encountered by an ADSL interface within any given 15 Minute performance data collection period, which causes adslAtucPerfFecsLThreshTrap.
ATUC 1 day / ATUR 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 1 day performance data collection period.'
LOS(sec)	The number of Loss of Signal Seconds encountered by an ADSL interface, within any given 1 day performance data collection period.
LOL (sec)	The number of Loss of Link Seconds encountered by an ADSL interface, within any given 1 day performance data collection period.
LPR (sec)	The number of Loss of Power Seconds encountered by an ADSL interface, within any given 1 day performance data collection period.
ES (sec)	The number of Error Seconds encountered by an ADSL interface, within any given 1 day performance data collection period.
SES (sec)	The number of Severe Error Seconds encountered by an ADSL interface within any given 1 Day performance data collection period, which causes adslAtucSesLTrap.
UAS (sec)	The number of unavailable error seconds encountered by an ADSL interface within any given 1 Day performance data collection period, which causes adslAtucUasLThreshTrap.
FECS (sec)	The number of Forward error correction seconds encountered by an ADSL interface within any given 1 Day performance data collection period, which causes adslAtucPerfFecsLThreshTrap.

Traps Configuration

The trap configuration allows you to administrate the specific ADSL trap report.

Figure 3-22 Traps Configuration Dialog



	LinkUp/LinkDown	Initial failure	Operate state change	Power management
port-1	enable	disable	disable	disable
port-2	enable	disable	disable	disable
port-3	enable	disable	disable	disable
port-4	enable	disable	disable	disable
port-5	enable	disable	disable	disable
port-6	enable	disable	disable	disable
port-7	enable	disable	disable	disable
port-8	enable	disable	disable	disable
port-9	enable	disable	disable	disable
port-10	enable	disable	disable	disable
port-11	enable	disable	disable	disable
port-12	enable	disable	disable	disable
port-13	enable	disable	disable	disable
port-14	enable	disable	disable	disable
port-15	enable	disable	disable	disable
port-16	enable	disable	disable	disable
port-17	enable	disable	disable	disable
port-18	enable	disable	disable	disable
port-19	enable	disable	disable	disable
port-20	enable	disable	disable	disable
port-21	enable	disable	disable	disable
port-22	enable	disable	disable	disable
port-23	enable	disable	disable	disable
port-24	enable	disable	disable	disable
port-25	enable	disable	disable	disable
port-26	enable	disable	disable	disable
port-27	enable	disable	disable	disable
port-28	enable	disable	disable	disable
port-29	enable	disable	disable	disable
port-30	enable	disable	disable	disable

Table 3-15 describes the trap configuration field items.

Table 3-15 Configuring the Traps

Item	Description
Set traps pull down menu	There are four choices of traps: LinkUp/LinkDown, Initial Failure, Operate State Change and Power Management. **LinkUp/LinkDown** : Indicates whether linkUp/linkDown traps should be generated for this interface. **Initial Failure** : ATUC initialization failed. **Operate State Change** : Enables/disables trap indicating a change in op state. **Power Management** : PM state change trap used for ADSL2 / ADSL2plus PM operation. This trap is not valid for ADSL mode.

Table 3-15 Configuring the Traps

Item	Description
from	This specifies the ADSL starting port interface.
to	This specifies the ADSL ending port interface.
Enable/disable	To enable or disable the trap on the specified port range.

SNMP Community Configuration

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 3-23 SNMP Community Configuration Dialog

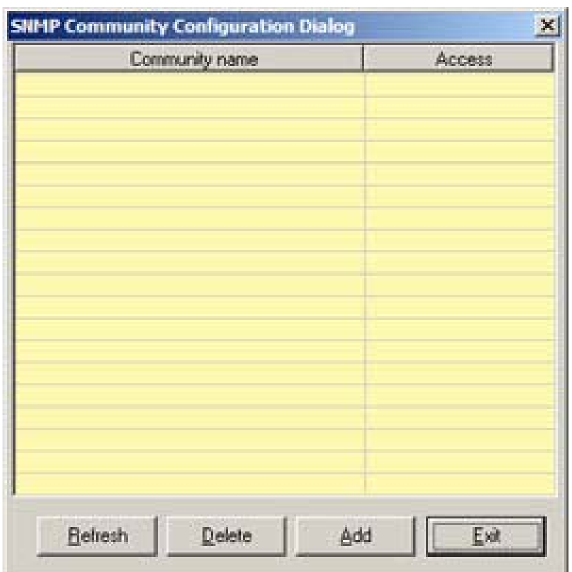


Figure 3-24 Add Community Dialog

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 3-16 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 Configuration

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

Figure 3-25 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 LCT. It is recommended to limit the number of host device.

Figure 3-26 Add Host IP Address Dialog

Table 3-17 describes fields in the Add Host IP Address Dialog.

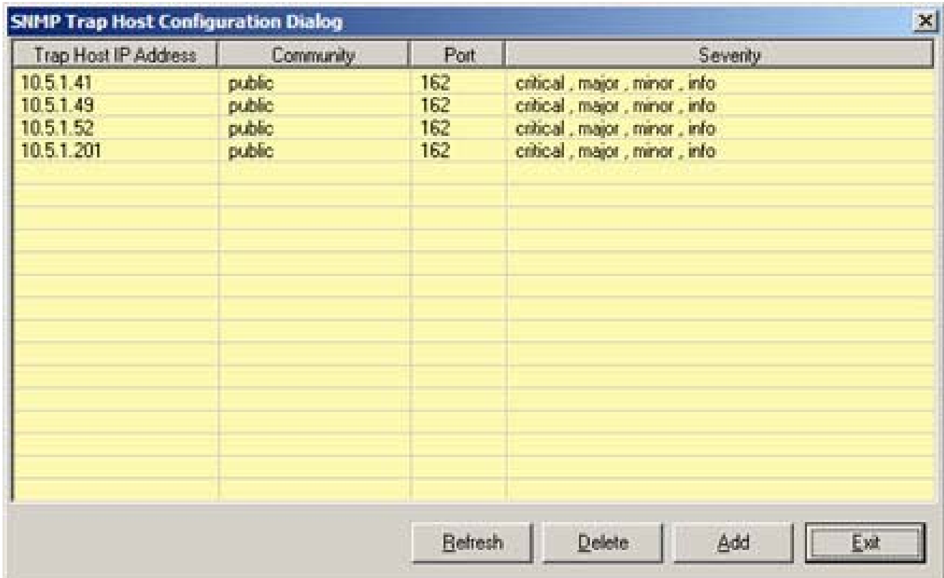
Table 3-17 Configure Host IP

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 Configuration

The SNMP trap configuration provides the management of SNMP trap host (at most 8 hosts).

Figure 3-27 SNMP Trap Configuration Dialog



Click '**Add**' button to create a new Trap host IP address.

Figure 3-28 Add Trap Host IP Dialog

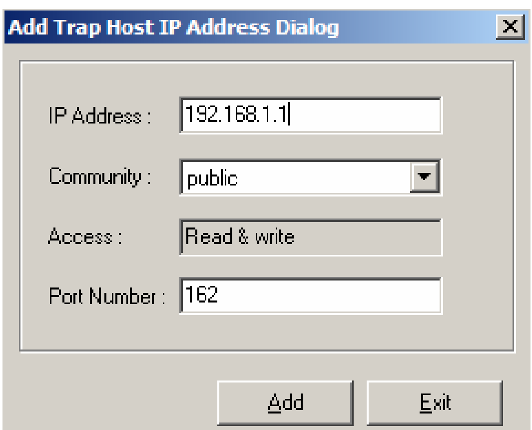


Table 3-18 Configuring Trap Host IP

Item	Description
IP Address	This specifies the IP address of the manager where trap is to be sent.
Community	This specifies the Community name used in the trap.
Access	This specifies the access permissions given to managers with this community name. 'ro' implies Read Only permissions and 'rw' implies Read-Write permissions.
Port Number	This specifies the Port at which the trap is to be sent.

Table 3-18 Configuring Trap Host IP

Item	Description
Severity	This specifies the severity level of the trap. It can be: CRITICAL ALARM MAJOR ALARM WARNING STATUS ALARM

VLAN Management

The VLAN management dialog list the existing VLAN and its configuration.

Introduction to VLAN and VLAN Tag

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 DAS3series is capable of passing tagged or untagged frames.

Each port has its own Ingress rule. If Ingress rule accept tagged frames only, the switch port will drop all incoming non-tagged frames. If Ingress rule accept all frame type, the switch port simultaneously allow the incoming tagged and untagged frames. An untagged frame doesn't carry any VID to which it belongs. When an untagged frame is received, Ingress Process insert a tag contained the PVID into the untagged frame. Each physical port has a default VID called PVID (Port VID). PVID is assigned to untagged frames or priority tagged frames (frames with null (0) VID) received on this port.

Figure 3-29 VLAN Management Dialog

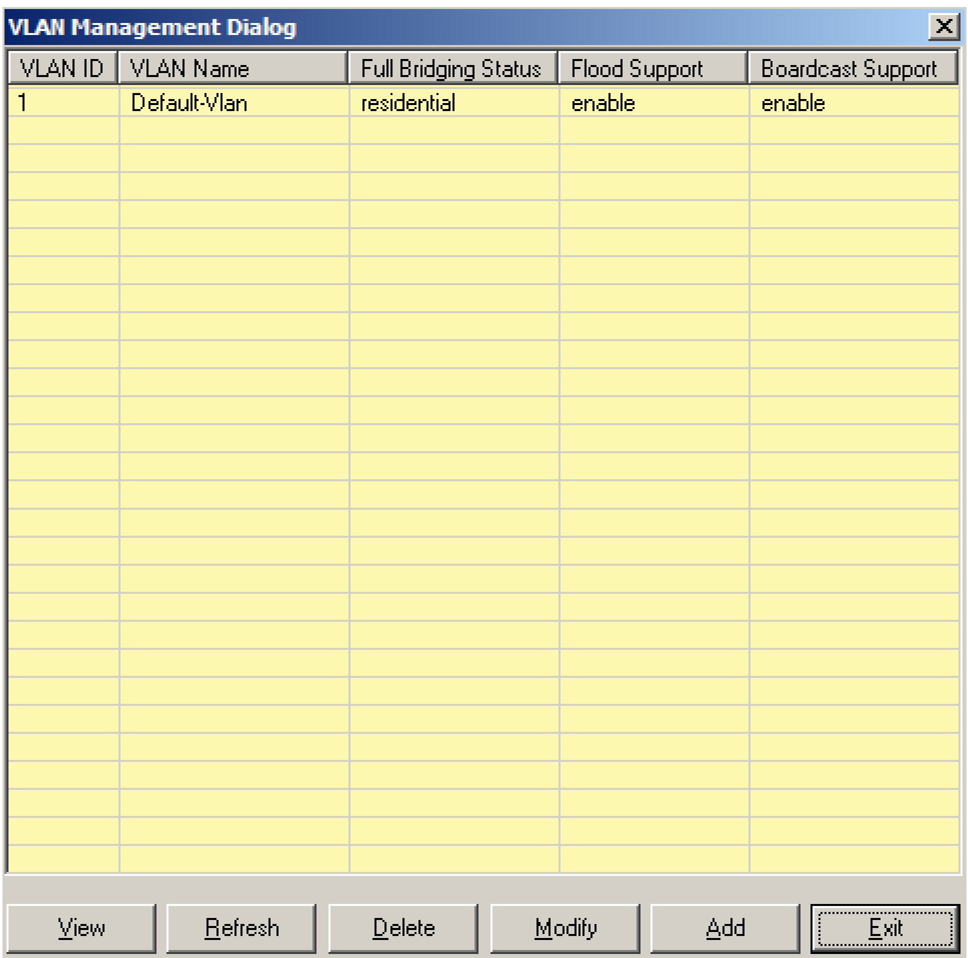


Table 3-19 Monitoring the VLAN Management

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]**
VLAN Name	An administratively assigned string, which may be used to identify the VLAN. This is mandatory in the case of create command line environment. In case of get/modify/delete - either vlan name or vlan id can be given. **Valid values:** 1 ~ 63 characters
Full Bridging Status	This specifies the state of bridging status for the VLAN. There can be three values associated with this. These values can be restricted bridging, unrestricted full bridging and residential bridging. [see **bridge status setup** for further details]
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.
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.

Click ‘**View**’ button to monitoring the selected VLAN information.

Figure 3-30 VLAN View Configuration Dialog

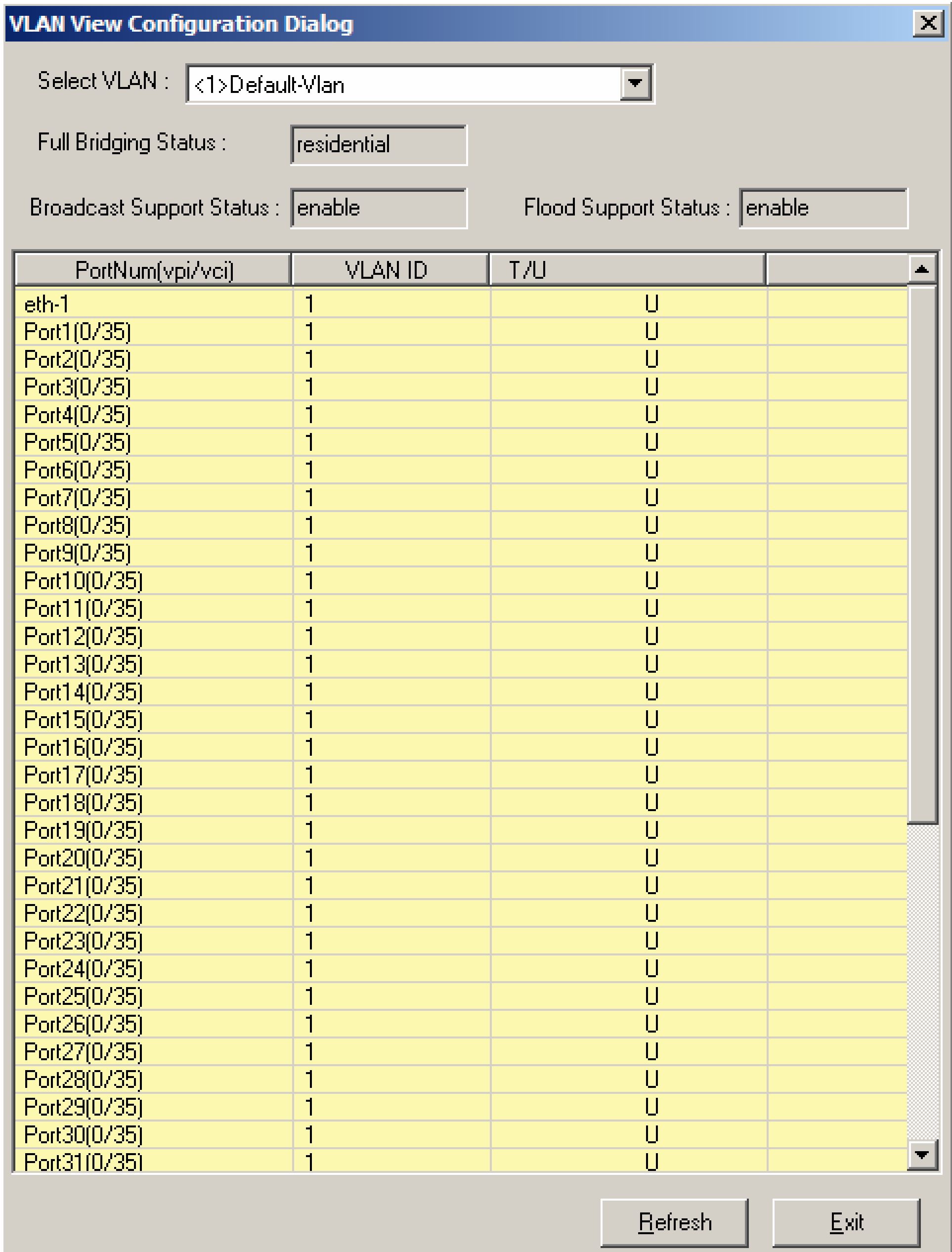


Table 3-20 Monitoring the VLAN View Configuration

Item	Description
Select VLAN	Select desired VLAN to show VLAN configuration
Full bridge status	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 full bridging, all traffic is forwarded based on lookup.
Broadcast support status	This is used to specify whether broadcast 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.
Flood support status	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.
PortNum(vpi/vci)	Display port number and its path, circuit identifier number.
VLAN ID	The corresponding VLAN ID for each port.
T/U	This setting determines a specific port to receive tagged (T) or untagged (U) frame.

Click ‘**Add**’ button to set the new VLAN with associate port interface.

Figure 3-31 VLAN Set Configuration Dialog

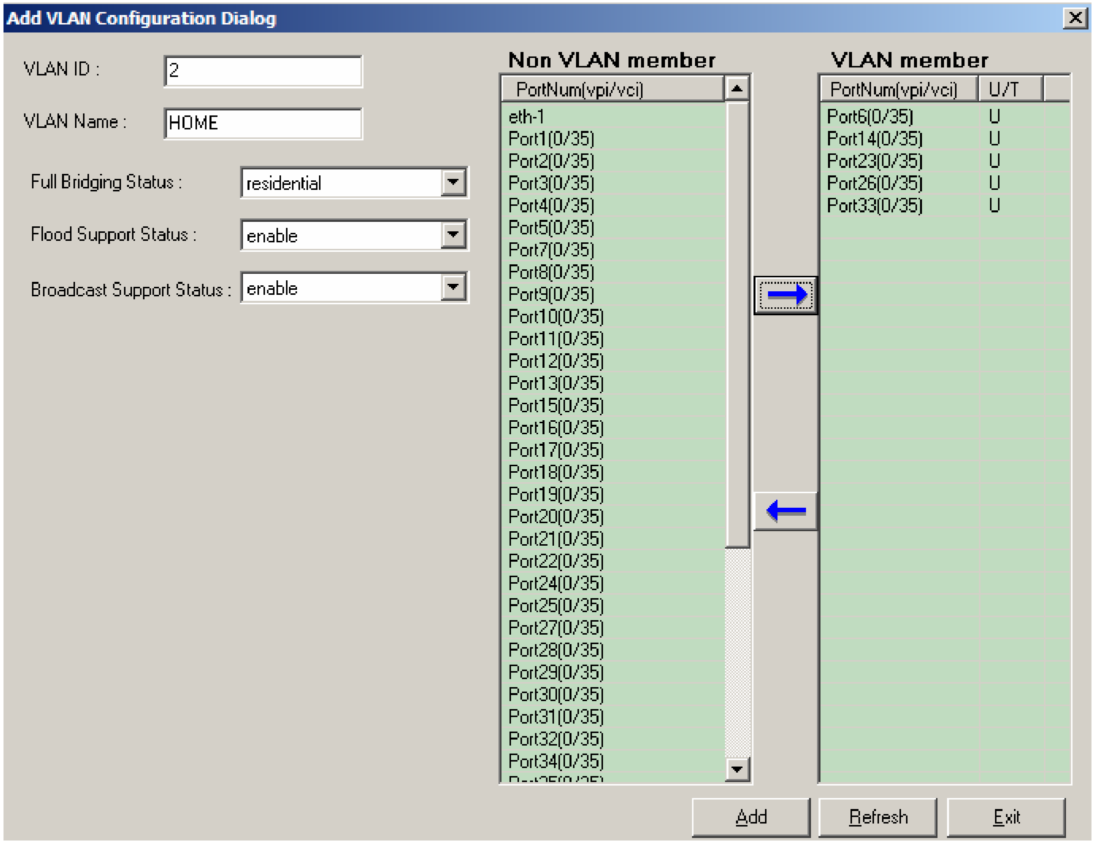


Table 3-21 Configuring VLAN Port Member

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]**
VLAN Name	An administratively assigned string, which may be used to identify the VLAN. This is mandatory in the case of create command line environment. In case of get/modify/delete - either vlan name or vlan id can be given. **Valid values:** 1 ~ 63 characters
Full Bridging Status	This specifies the state of bridging status for the VLAN. There can be three values associated with this. These values can be restricted bridging, unrestricted full bridging and residential bridging. [see **bridge status setup** for further details]
Flood Support Status	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.
Broadcast Support Status	This is used to specify whether broadcast 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.
Non VLAN member	All candidate ports, which can be selected to be in the new VLAN, displayed in PortNum(vpi/vci) format.
VLAN member	All candidate ports, which can be included in the new VLAN, displayed in PortNum(vpi/vci) format.

Table 3-21 Configuring VLAN Port Member

Item	Description
U/T	This setting determines a specific port to receive tagged (T) or untagged (U) frame. Click on the U to rotate between U and T.
	Please use arrow button to add or remove ports.

VLAN Ports Management

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

Figure 3-32 VLAN Ports Management Dialog

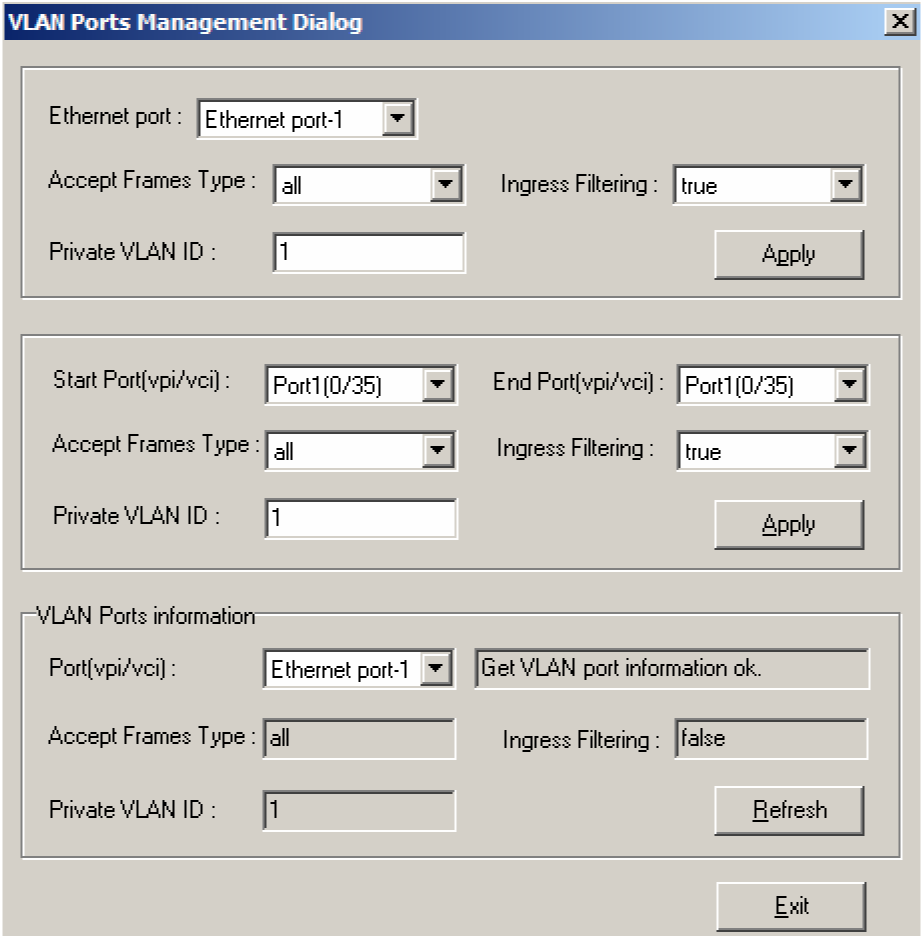


Table 3-22 VLAN Ports Management

Item	Description
Ethernet port	This specifies the network Ethernet port interface.
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.
Private VLAN ID	The VLAN Identifier.
	Press the '**Apply**' button to confirm the setting.
Start Port(vpi/vci)	This specifies the ADSL starting port interface.
End Port(vpi/vci)	This specifies the ADSL ending port interface.
Accept Frames Type	This field specifies whether the port(s) will accept tag only frames or all frames. When this is **Tagged**, the device will discard untagged frames or priority-tagged

Table 3-22 VLAN Ports Management

Item	Description
	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 not discard frames base on VLAN ID.
Private VLAN ID	The VLAND ID to be assigned if untagged frames are accepted.
	Press the '**Apply**' button to confirm the setting.
VLAN Ports information	Use this field to monitoring the VLAN information correspond to ADSL port or Ethernet port interface.
Port(vpi/vci)	This specifies the ADSL or network Ethernet interface.
Accept Frames Type	This displays the accept frames types of selected port interface.
Ingress Filtering	This displays the ingress filtering status of selected port interface.
Private VLAN ID	This display the VLAN identify of selected port interface.
	Press the '**Refresh**' button to acquire desired port information.

GVRP Ports Management

The GVRP ports management allows you to view and change the GVRP administrate status.
GVRP is a GARP application that provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports.

Figure 3-33 GVRP Ports Management Dialog

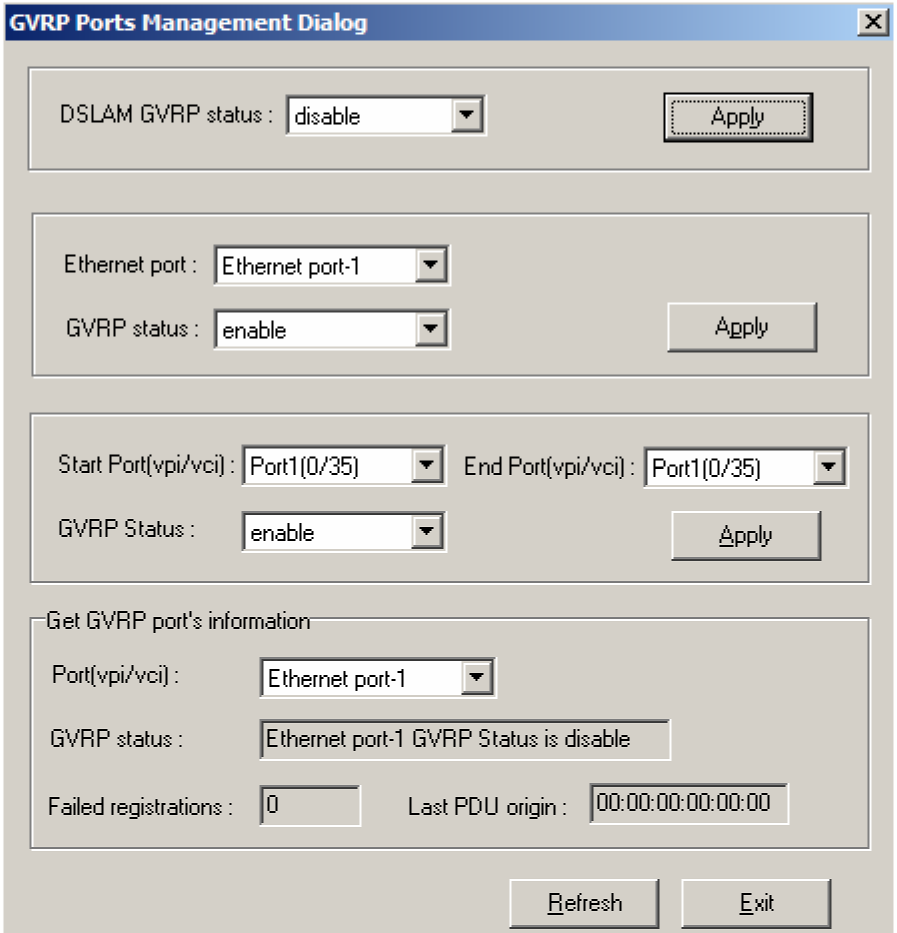


Table 3-23 Configuring GVRP Ports Management

Item	Description
DSLAM GVRP status	The administrative status to be set by operator for GVRP
	Press the '**Apply**' button to confirm the setting.
Ethernet port	This specifies the network Ethernet port interface.
Ethernet port's GVRP Status	This displays the Ethernet port's GVRP status.
	Press the '**Apply**' button to confirm the setting.
Start Port(vpi/vci)	This specifies the ADSL starting port interface in Port(vpi/vci) format
End Port(vpi/vci)	This specifies the ADSL ending port interface in Port(vpi/vci) format
GVRP Status	The administrative status requested by management for GVRP.
	Press the '**Apply**' button to confirm the setting.
Get GVRP port's information	
Port(vpi/vci)	This specifies the ADSL or network Ethernet interface.

Table 3-23 Configuring GVRP Ports Management

Item	Description
GVRP Status	The state of the GVRP operation on this port. The value **'enable'** indicates that GVRP is enabled on this port. When this is **'disable'**, GVRP will be 'disable' on this port. In such a case, any GVRP packet received will be silently discarded and no GVRP registrations will be propagated from other ports.
Failed Registration	The total number of failed GVRP registrations, for any reason, on this port.
Last PDU origin	The Source MAC Address of the last GVRP message received on this port.

Limit MAC Number

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

Figure 3-34 Limit MAC Number Dialog

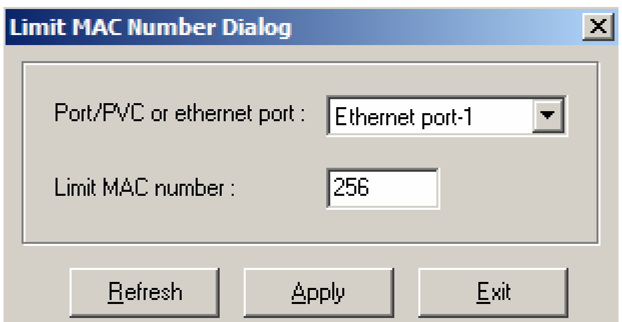


Table 3-24 shows the limit MAC number field items.

Table 3-24 Configuring the MAC Number

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. **Valid values:** 0 ~ 256
Selected port's MAC number	This displays the selected port's limit MAC number.

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.

Figure 3-35 Set Spanning Tree Protocol Dialog

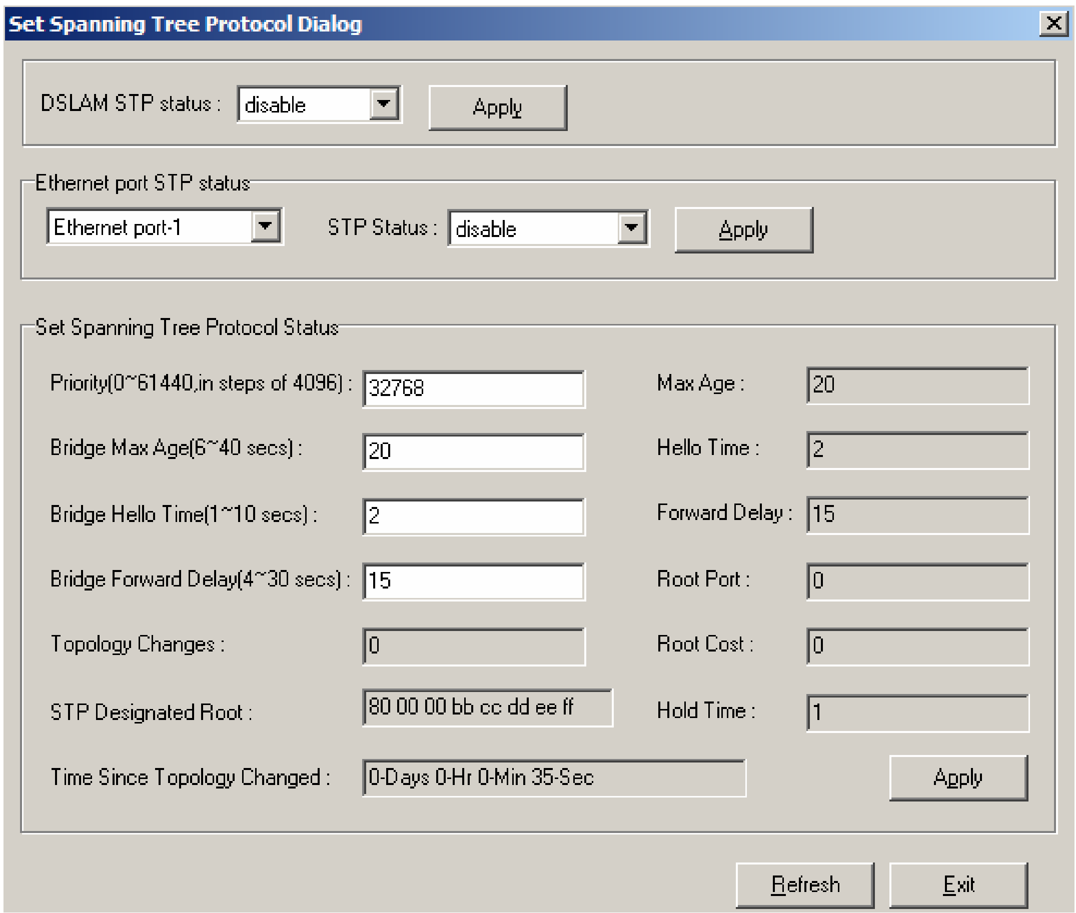


Table 3-25 describes the spanning tree parameters field items.

Table 3-25 Configuring the Spanning Tree Protocol

Item	Description
DSLAM STP status	Spanning Tree Protocol to be enabled on the Bridge or not.
	Press the '**Apply**' button to confirm the setting.
Ethernet port STP status	
Select an Ethernet Port	This specifies the STP status of network Ethernet interface.

Table 3-25 Configuring the Spanning Tree Protocol

Item	Description
STP Status	This specifies the Spanning Tree Protocol status of selected Ethernet port.
	Press the '**Apply**' button to confirm the setting.
Set Spanning Tree Protocol Status	
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 STP 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
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)
Topology Change	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
STP Designated Root	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Time Since Topology Changed	The time (in second) since the last time a topology change was detected by the bridge entity.
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 Hello Time 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 the root.
Root Port	The port number of the port which offers the lowest cost path from this bridge to the root bridge.
Root Cost	The cost of the path to the root as seen from this bridge.
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.
	Press the '**Apply**' button to confirm the setting.

Bridge Information

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

Figure 3-36 Bridge Information Dialog

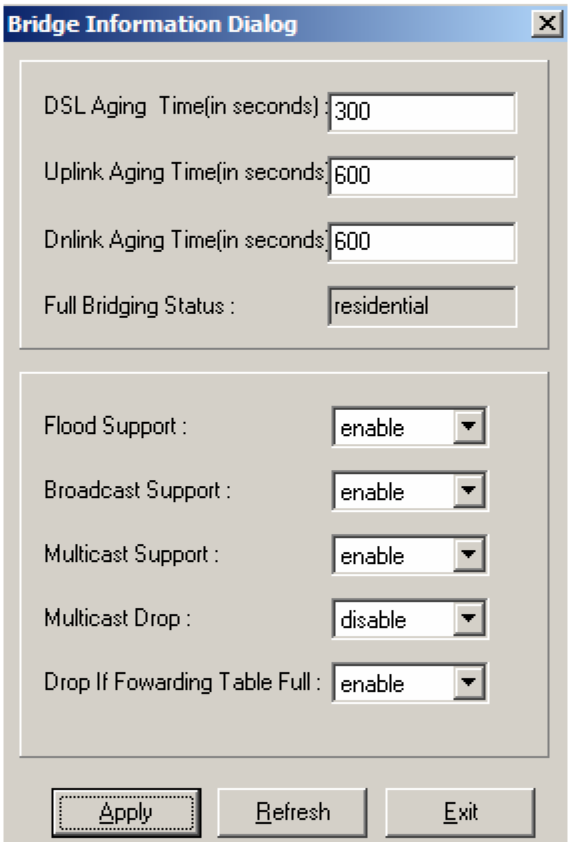


Table 3-26 Configuring the Bridge Information

Item	Description
DSL 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 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

Table 3-26 Configuring the Bridge Information

Item	Description
Full Bridging Status	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 full bridging, all traffic is forwarded based on lookup.
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.
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.

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 3-37 IGMP Snooping Dialog

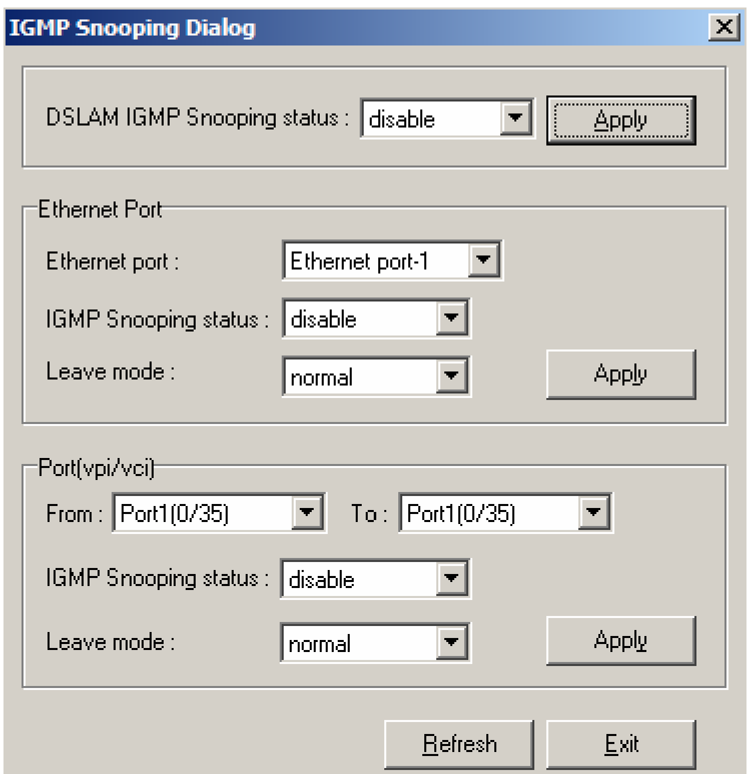


Table 3-27 Configuring IGMP Snooping

Item	Description
DSLAM IGMP Snooping Status	Specified whether or not IGMP Snooping is to be enabled in the system.
	Press the '**Apply**' button to confirm the setting.
Ethernet Port	

Table 3-27 Configuring IGMP Snooping

Item	Description
Ethernet Port	This specifies the network Ethernet port interface.
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.
	Press the '**Apply**' button to confirm the setting.
Port(vpi/vci)	
From	This specifies the ADSL starting port interface in port (vpi/vci) format.
To	This specifies the ADSL ending port interface in port (vpi/vci) format.
IGMP Snooping Status	Specifies whether or not IGMP Snooping is to be enabled on the port.
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.

DHCP Relay Configuration

The DHCP Relay configuration provides DHCP Relay Option 82 function.

DHCP allows individual computers on an IP network to extract their configurations from DHCP server. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address. Information can be added into client TCP/IP configuration requests that IP-DSLAM relays to a DHCP server. This helps provide authentication about the source of the request. Please refer to RFC 3046 for further details.

Figure 3-38 DHCP Relay Configuration Dialog.

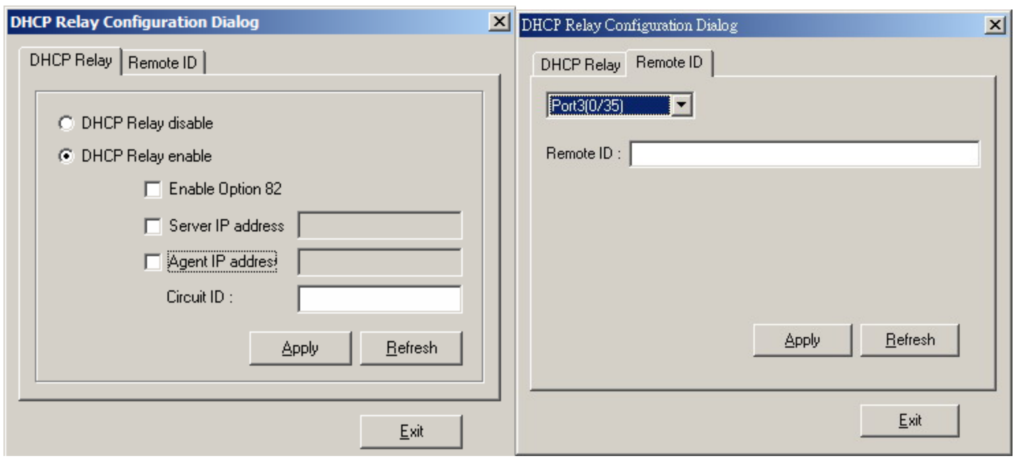


Table 3-28 Configuring DHCP Relay Configuration

Item	Description
DHCP Relay	
DHCP Relay disable	To disable the DHCP relay function.
DHCP Relay enable	This enables the DHCP relay function.
Enable Option 82	This enables the DHCP relay with option 82.
Server IP Address	This specifies the DHCP Server IP address.
Agent IP address	This specifies the relay agent IP address.
Circuit ID	This field will be included in Option 82 message to identify relay agent.
	Press the '**Apply**' button to confirm the setting.
Remote ID	
Port (vpi/vci) pull down menu	Please select a Port (vpi/vci) pair to set remote ID.
Remote ID	This field will be included in Option 82 message to identify relay agent.

Filter & ACL Menu

The Filter & ACL functionalities allow system administrator to build packet filter and access control list.

Filter Wizard

Filter Wizard can guide administrator to set up rules and sub rule for the filter.

Figure 3-39 Filter Wizard Add Rule Dialog

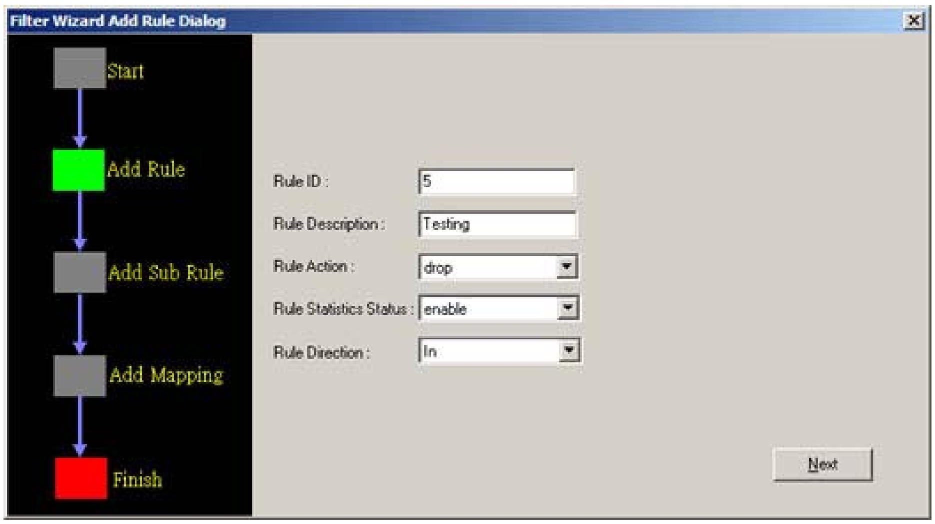


Table 3-29 Filter Wizard Add Rule Dialog

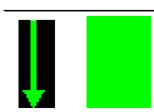
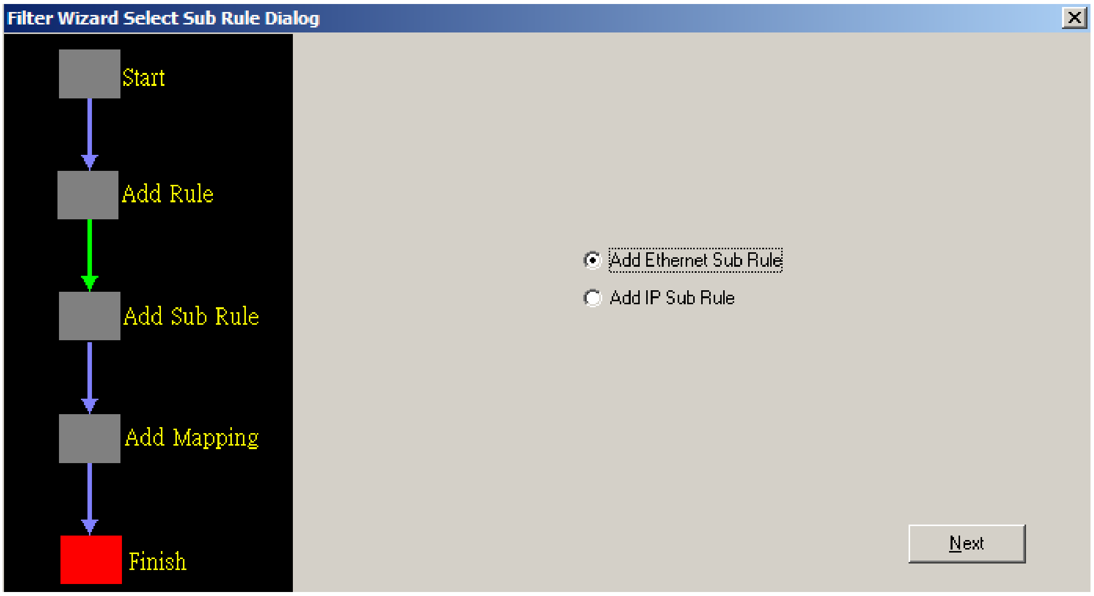
Item	Description
Start	
Rule ID	Unique identifier of a filter rule. **Valid values:** 2 ~ 300, 1 reserved for IGMP Snooping
Rule Description	Description of the application that receives packets matching this rule. **Valid values:** 1 ~ 100 characters
Rule Action	Action to be applied for the packets matching this filter rule. Possible choice: [drop | allow | set priority | send to control | retag priority | copy to control | go to next rule | forward exit]
Rule Statistics Status	Enable or disable this rule.
Rule Direction	Specifies whether the rule will be applied on incoming interfaces (ingress) or outgoing interfaces (egress).
	The green highlight indicates the ongoing step.
Next	Click '**Next**' to advance to '**Add Rule**' step

Figure 3-40 Filter Wizard Select Sub Rule Dialog



Click ‘**Next**’ to configure the Ethernet sub rule or IP sub rule filtering.

Table 3-30 Filter Wizard Select Sub Rule Dialog

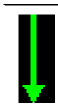
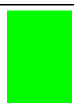
Item	Description
Add Rule	
Add Ethernet Sub Rule	Add sub rule for Ethernet interface
Add IP Sub Rule	Add sub rule for IP Interface
 	The green highlight indicates the ongoing step.
Next	Confirm the selection and go to next step.

Figure 3-41 Filter Wizard Add Ethernet Sub Rule Dialog

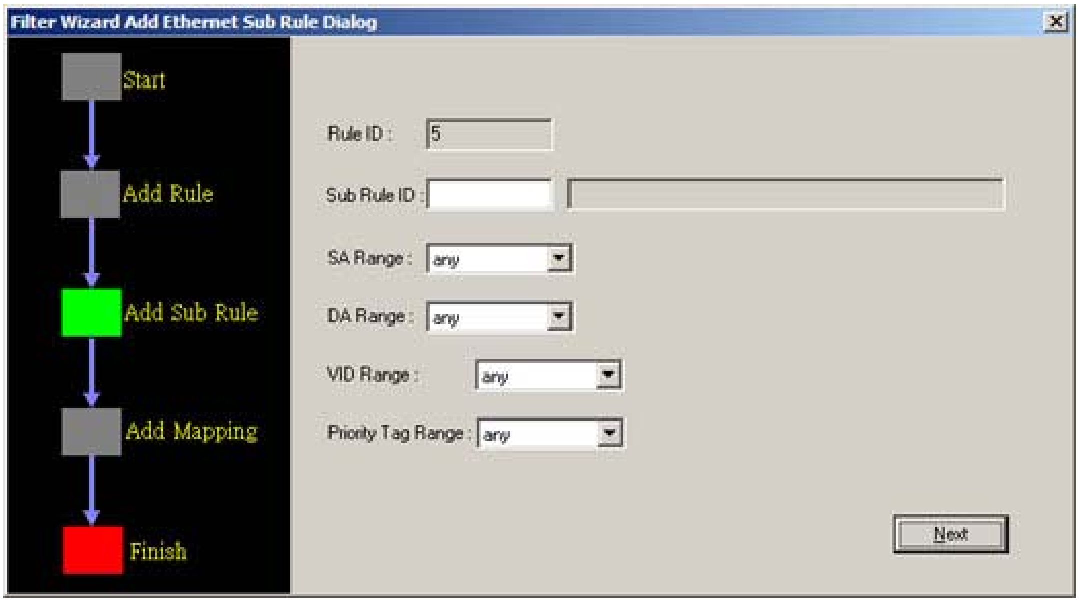


Table 3-31 Filter Wizard Add Ethernet Sub Rule Dialog

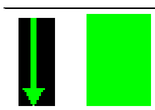
Item	Description
Add Sub Rule (Ethernet)	
Rule ID	Corresponding Rule ID for current Sub Rule ID
Sub Rule ID	Unique identifier of a filter rule. **Valid values:** 2 ~ 300
Sub Rule ID	Unique identifier of a filter sub rule **Valid values:** 1 ~ 1,000,000
SA Range	This specifies the Source address range. possible choice: [equal | unequal | any | in range | out range]
DA Range	This specifies the Destination address range. possible choice: [equal | unequal | any | in range | out range]
VID Range	This specify the VLAN ID range possible choice: [equal | unequal | any | in range | out range]
Priority Tag Range	This specifies the priority tag range. possible choice: [equal | unequal | any | in range | out range]
	The green highlight indicates the ongoing step.

Figure 3-42 Filter Wizard Add IP Sub Rule Dialog

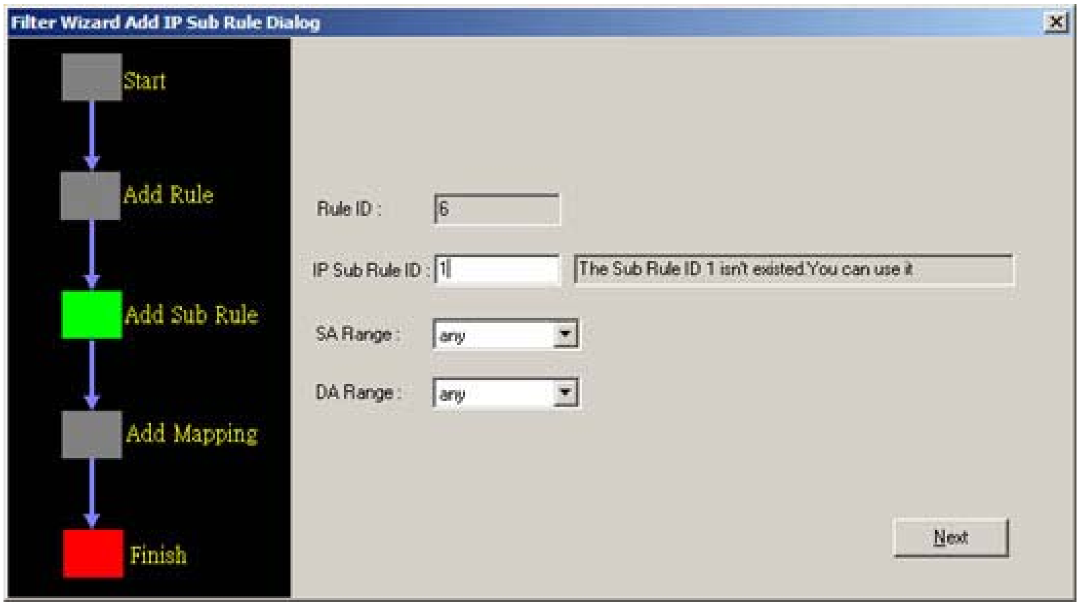


Table 3-32 Filter Wizard Add IP Sub Rule Dialog

Item	Description
Add Sub Rule (IP)	
Rule ID	Corresponding Rule ID for current Sub Rule ID
Sub Rule ID	Unique identifier of a filter rule. **Valid values:** 2 ~ 300
IP Sub Rule ID	Unique identifier of a filter sub rule **Valid values:** 1 ~ 1,000,000
SA Range	This specifies the Source address range. possible choice: [equal | unequal | any | in range | out range]
DA Range	This specifies the Destination address range. possible choice: [equal | unequal | any | in range | out range]
DA Range	This specifies the Destination address range. possible choice: [equal | unequal | any | in range | out range]
	The green highlight indicates the ongoing step.

Figure 3-43 Filter Wizard Add Mapping Dialog

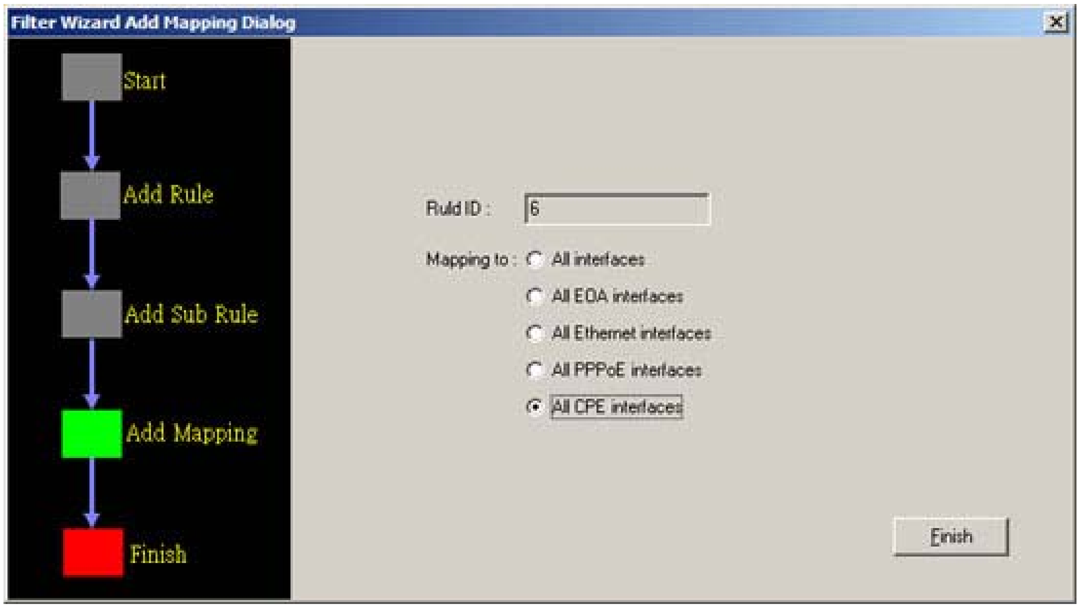


Table 3-33 Filter Wizard Add Mapping Dialog

Item	Description
Rule ID	The Rule which is being created.
Mapping to	Source MAC address comparison type Name of the interface whose mapping is being created. Only EOA, PPPoE, and Ethernet interfaces are allowed. If the value of this field is 'All interfaces', it indicates all interfaces. 'All EOA interfaces' indicates all 'EOA' interfaces and 'All Ethernet interfaces' indicates all 'Ethernet' interfaces. ‘All PPPoE interfaces' indicates all 'PPPoE ' interfaces and 'All CPE interfaces' indicates all EOA and PPPoE interfaces.

Filter Configuration

The setting allow administrator to review created filters and modify their configuration.

Filter Rule

Figure 3-44 Filter Rule Configuration Dialog

Table 3-34 Management the Filter Rule

Item	Description
Rule ID	Unique identifier of a filter rule. **Valid values:** 2 ~ 300, 1 reserved for IGMP Snooping
Description	Description of the application that receives packets matching this rule. This field can be modified only if 'Status' has the value 'disable'.
Action	Action to be applied for the packets matching this filter rule. This field can be modified only if 'status' has the value 'disable'.
Set Priority	Start priority tag of the range of priority tags. Invalid, if the direction of the rule for which this sub-rule is being created is 'out'.
Status	Admin status of the rule.
Direction	Specifies whether the rule will be applied on incoming interfaces (ingress) or outgoing interfaces.
Packet Type	This field specifies the types of packets on which this rule is to be applied. 'Mcast' means this rule is valid for multicast packets, 'Bcast' means this rule is valid for broadcast packets and 'Ucast' means this rule is valid for unicast packets.
Statistics Status	Admin status of rule statistics. Statistics of a rule are collected only when this field is set to 'enable'. This field can be modified only if 'status' has the value 'disable'.
Hit Statistics	The counter time of rule become effective (filter activity).

Figure 3-45 Add Rule Dialog

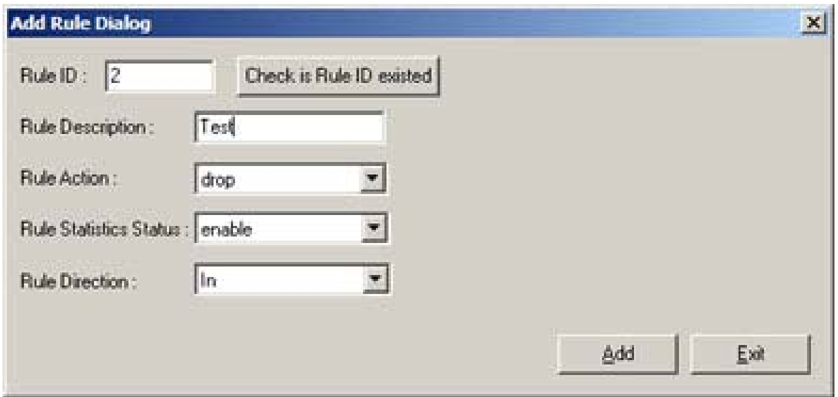


Table 3-35 Creating Filter Rule

Item	Description
Rule ID	Unique identifier of a filter rule. **Valid values:** 2 ~ 300
Rule Description	Description of the application that receives packets matching this rule. This field can be modified only if 'status' has the value 'disable'
Rule Action	Action to be applied for the packets matching this filter rule. This field can be modified only if 'status' has the value 'disable'.
Rule Statistics Status	Admin status of rule statistics. Statistics of a rule are collected only when this field is set to 'enable'. This field can be modified only if 'status' has the value 'disable'.
Rule Direction	Specifies whether the rule will be applied on incoming interfaces (ingress) or outgoing interfaces (egress).

Filter Sub Rule

Figure 3-46 Filter Sub Rule Configuration Dialog

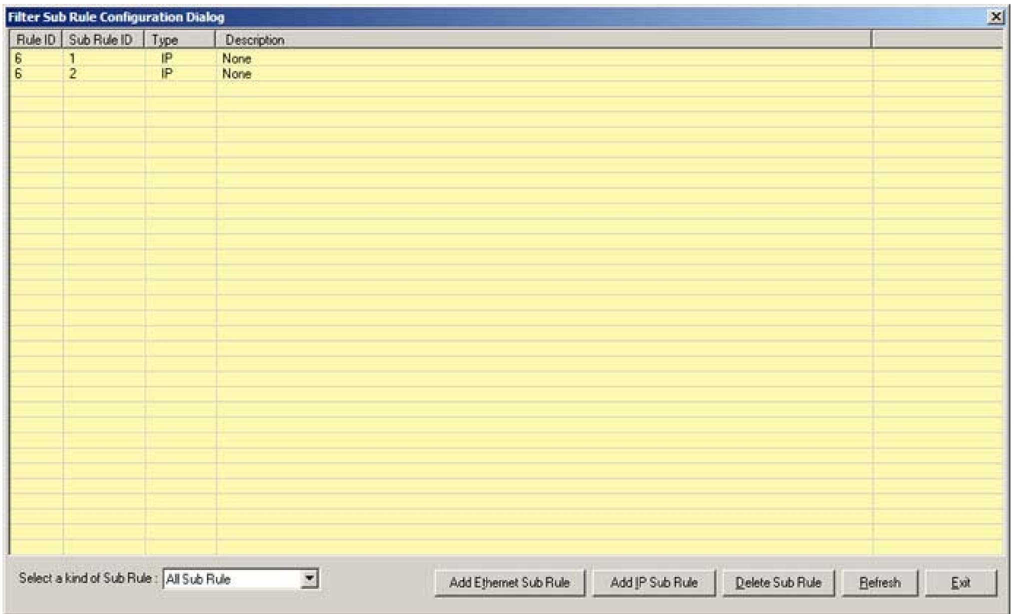


Table 3-36 Management the Filter Sub Rule

Item	Description
Rule ID	Rule Id of the rule in the filter sub rule. **Valid values:** 2 ~ 300
Sub Rule ID	Unique identifier of a filter sub rule **Valid values:** 1 ~ 1000000
Type	This shows the type of sub rule (IP or Ethernet layer)
Description	This shows the sub rule description.

Figure 3-47 Ethernet Sub Rule Dialog

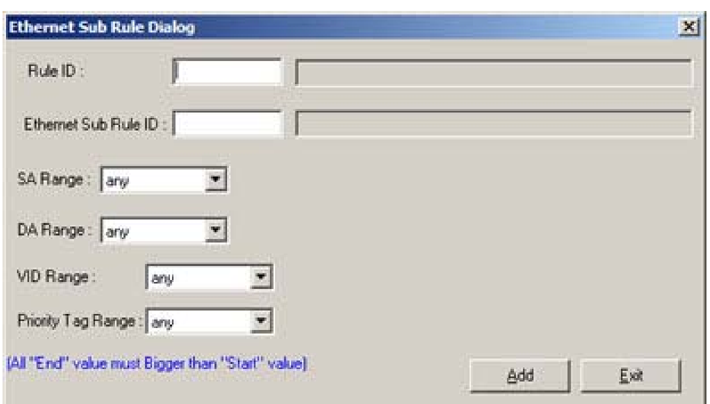


Figure 3-48 IP Sub Rule Dialog

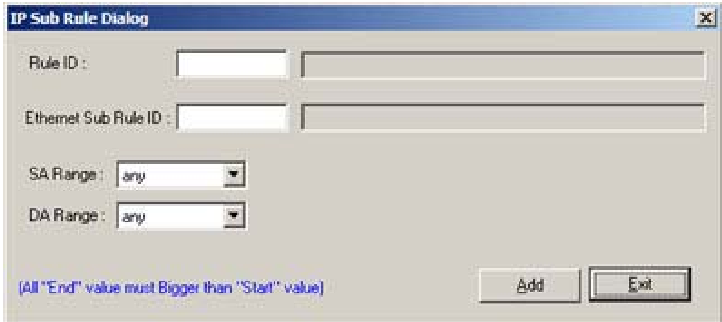


Table 3-37 Configuring IP Sub Rule

Item	Description
Rule ID	Rule Id of the rule in the mapping **Valid values:** 2 ~ 300
Ethernet Sub Rule ID	Unique identifier of a filter sub rule **Valid values:** 1 ~ 1000000
IP Sub Rule ID	Unique identifier of a filter sub rule **Valid values:** 1 ~ 1000000
SA Range	This specific the Source address range.
DA Range	This specific the Destination address range.
VID Range (Ethernet Only)	Start VLAN ID of the range of VLAN IDs. Invalid, if the direction of the rule for which this sub-rule is being created is 'out'.
Priority Tag Range (Ethernet Only)	Start priority tag of the range of priority tags. Invalid, if the direction of the rule for which this sub-rule is being created is 'out'.

Filter Mapping

Figure 3-49 Interface Mapping to Rule Dialog

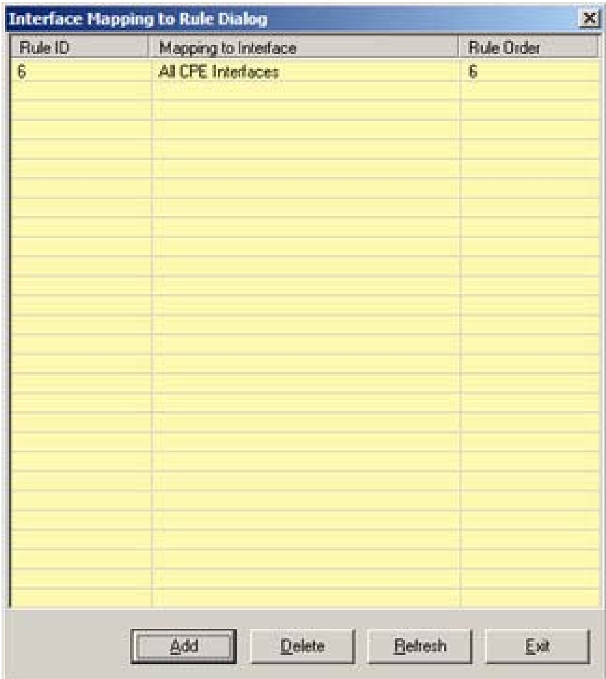


Figure 3-50 Add Mapping Table Dialog

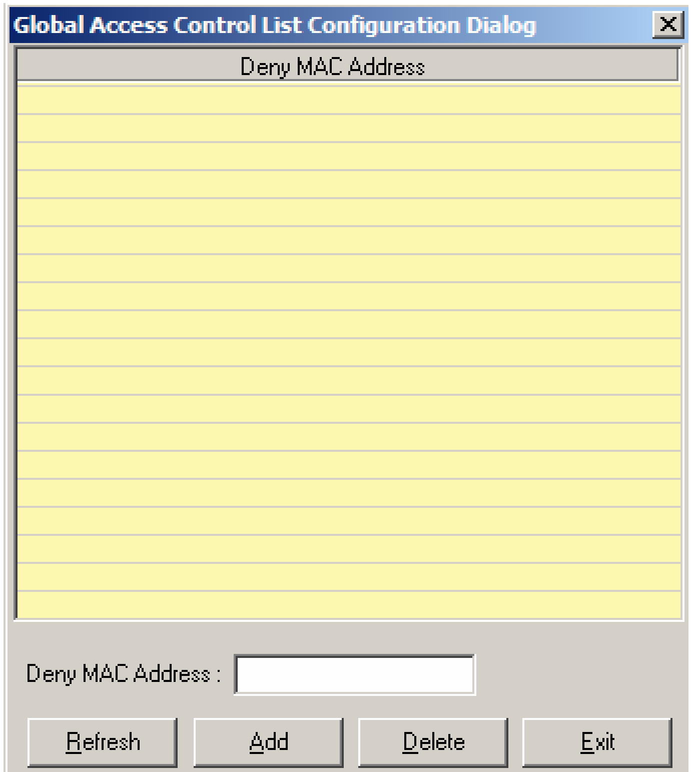
Table 3-38 Creating Mapping Table

Item	Description
Select a Rule	This specifies the mapping rule, the drop-down box contains created rule ID.
Mapping to	Source MAC address comparison type Name of the interface whose mapping is being created. Only EOA, PPPoE, and Ethernet interfaces are allowed. If the value of this field is 'All', it indicates all interfaces. 'All EOA' indicates all 'EOA' interfaces and 'All Ethernet' indicates all 'Ethernet' interfaces. ‘All PPPoE' indicates all 'PPPoE' interfaces and 'All CPE' indicates all EOA and PPPoE interfaces.

Global Access Control List

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

Figure 3-51 Global Access Control List 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.

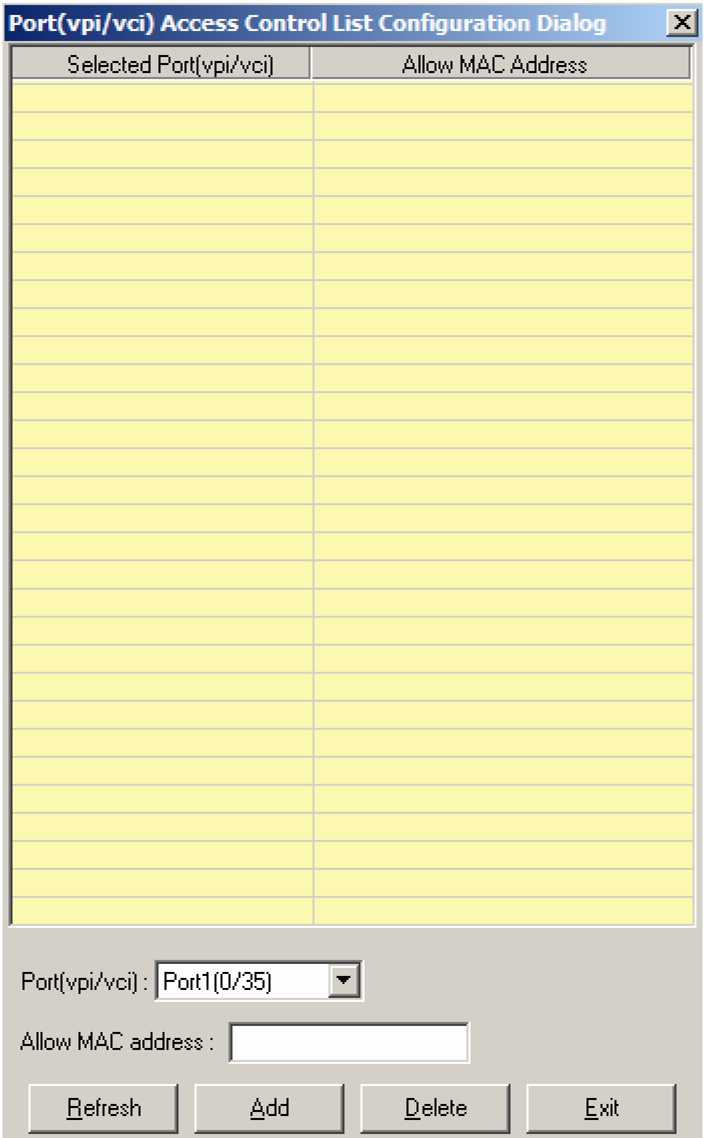
Table 3-39 Configuring Global Access Control List

Item	Description
Deny MAC Address	Source MAC address to be dropped

Port(vpi/vci) Access Control List

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

Figure 3-52 Port/PVC Access Control List 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 3-40 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/vci pair.

Performance Menu

The performance menu contains the ADSL port and Ethernet port interface PM status.

DSL Status

The line status shows the ADSL line information.

Figure 3-53 DSL Status Dialog

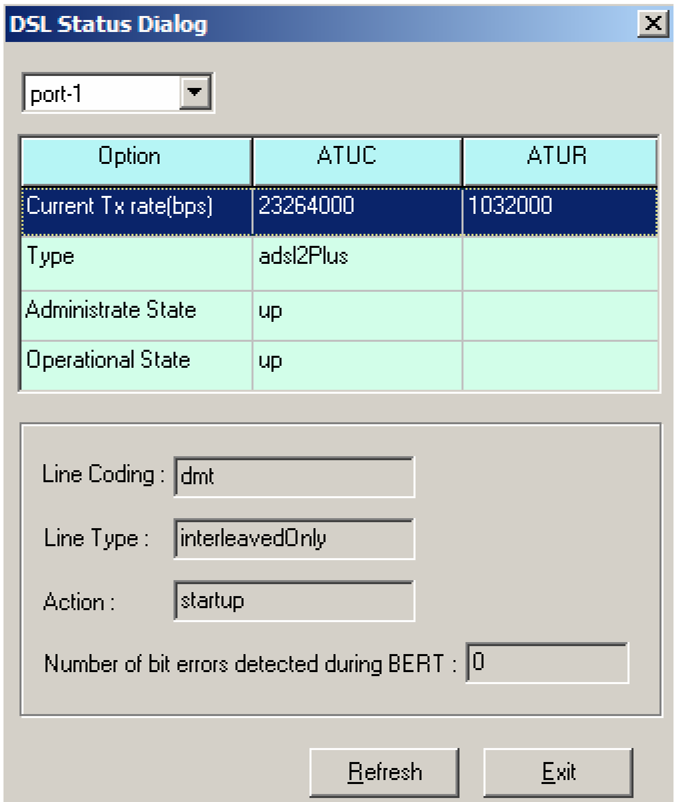


Table 3-41 Line Status Dialog

Item	Description
Port selection menu	Select the ADSL port interface to be display with relative parameters.
Line Coding	ADSL line code type.
Line Type	Line type used by the DSL port.
Action	This object specifies actions that are used to control transceiver operation, including abort, startup and tests.
Number of bit errors detected during BERT	This object provides the count of bit errors since the last time the object was read, as well as the type of synchronization.

Layer Information

The Layer Information will display ATM, Channel, and DSL layer information.

Figure 3-54 Layer Information Dialog

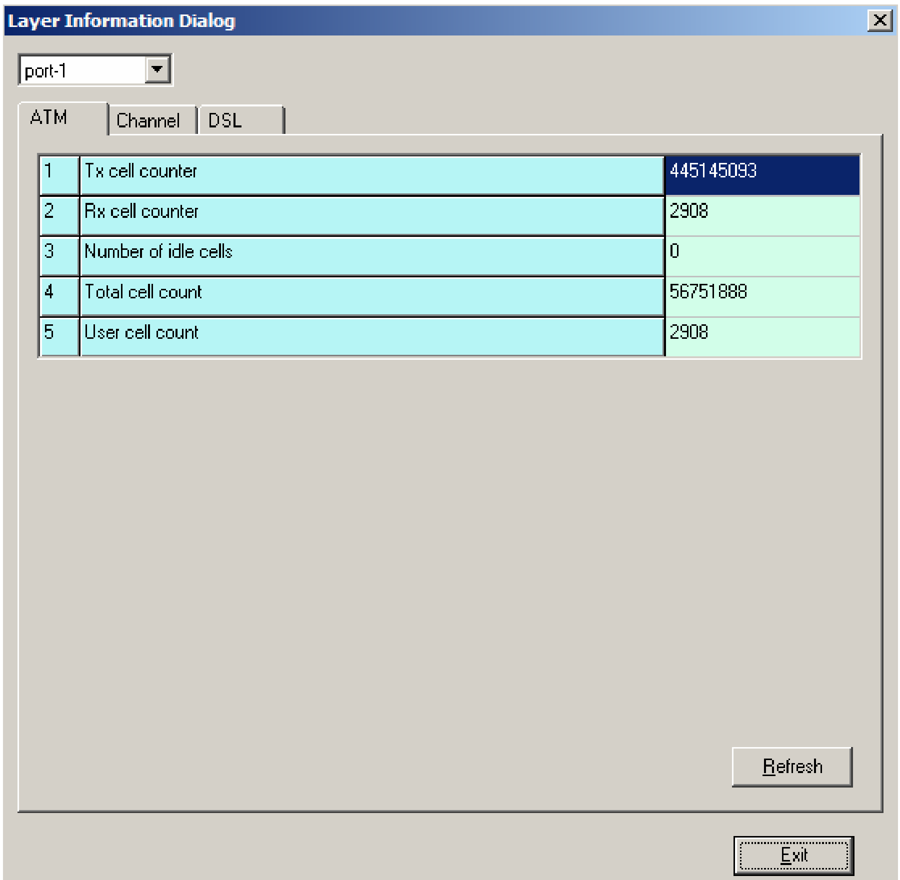


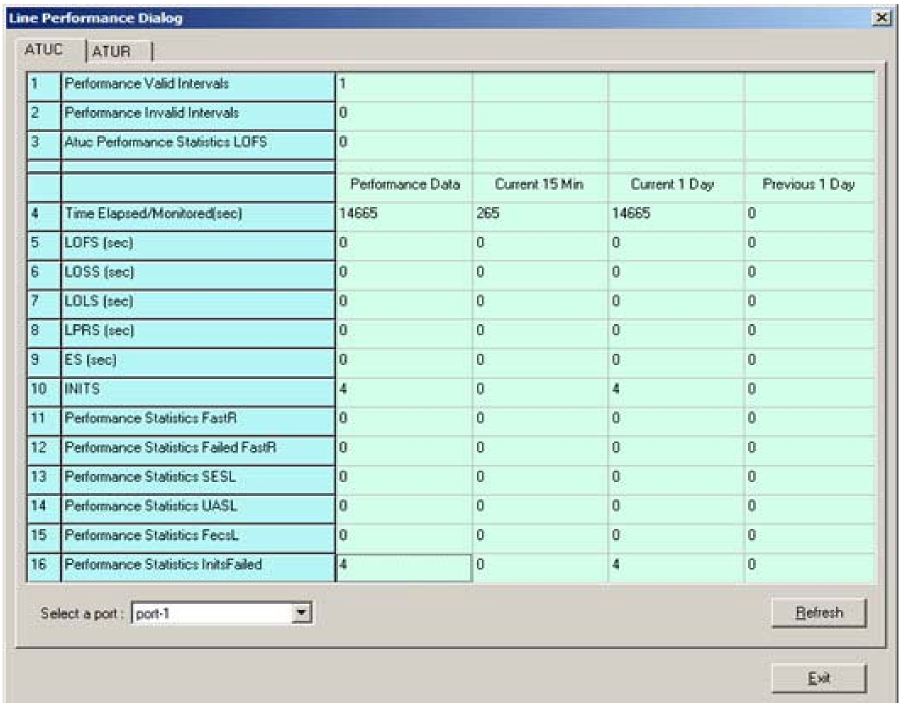
Table 3-42 Layer Information Dialog

Item	Description
Port selection menu	Select the ADSL port interface to be display with relative parameters.
ATM	This page displays cell counter for ATM layer.
Channel	This page displays signal synchronization, data rate, interleave delay, and CRC information.
DSL	This page displays operation state, line standard, management state and power.

Line Performance Data

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

Figure 3-55 Line Performance Dialog

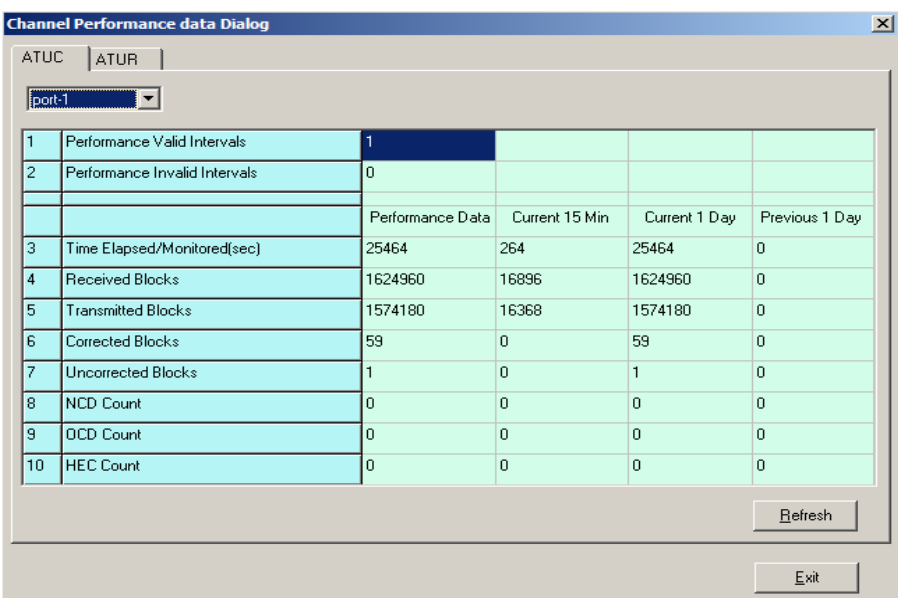


1	Performance Valid Intervals	1			
2	Performance Invalid Intervals	0			
3	Atuc Performance Statistics LOFS	0			
		Performance Data	Current 15 Min	Current 1 Day	Previous 1 Day
4	Time Elapsed/Monitored(sec)	14665	265	14665	0
5	LOFS (sec)	0	0	0	0
6	LOSS (sec)	0	0	0	0
7	LOLS (sec)	0	0	0	0
8	LPRS (sec)	0	0	0	0
9	ES (sec)	0	0	0	0
10	INITS	4	0	4	0
11	Performance Statistics FastR	0	0	0	0
12	Performance Statistics Failed FastR	0	0	0	0
13	Performance Statistics SESL	0	0	0	0
14	Performance Statistics UASL	0	0	0	0
15	Performance Statistics FecsL	0	0	0	0
16	Performance Statistics InitsFailed	4	0	4	0

Channel Performance Data

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

Figure 3-56 Channel Performance Dialog

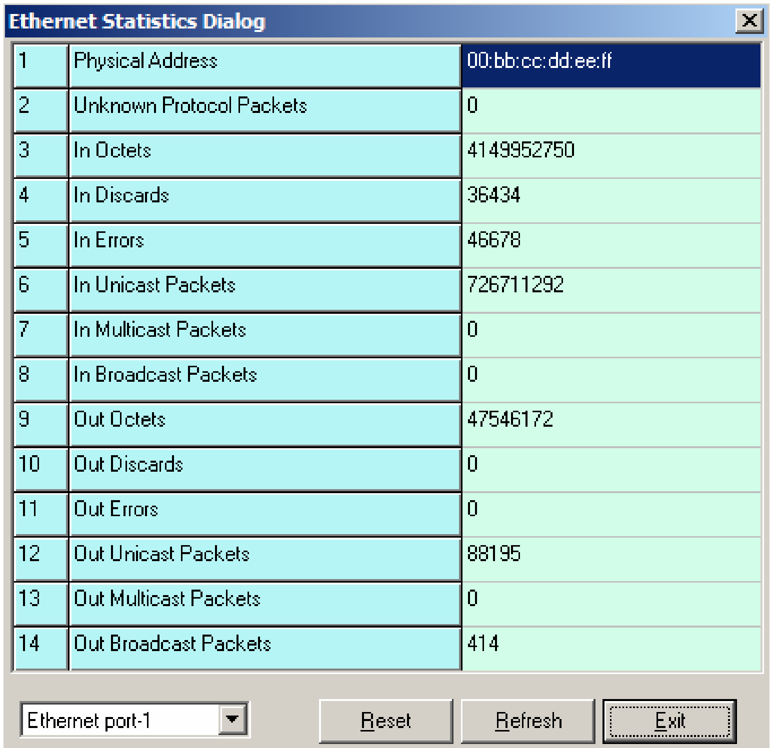


1	Performance Valid Intervals	1			
2	Performance Invalid Intervals	0			
		Performance Data	Current 15 Min	Current 1 Day	Previous 1 Day
3	Time Elapsed/Monitored(sec)	25464	264	25464	0
4	Received Blocks	1624960	16896	1624960	0
5	Transmitted Blocks	1574180	16368	1574180	0
6	Corrected Blocks	59	0	59	0
7	Uncorrected Blocks	1	0	1	0
8	NCD Count	0	0	0	0
9	OCD Count	0	0	0	0
10	HEC Count	0	0	0	0

Ethernet Statistics

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

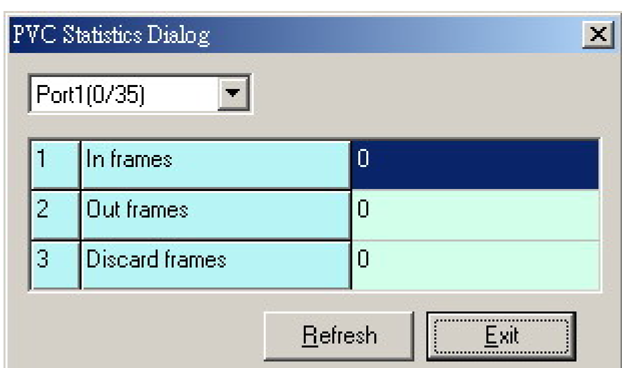
Figure 3-57 Ethernet Statistics Dialog



PVC Statistics

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

Figure 3-58 PVC Statistics Dialog



Diagnostic Menu

The diagnostic menu provides test function from ADSL physical layer to ATM layer.

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 3-59 ADSL2 DELT Run & Report Dialog

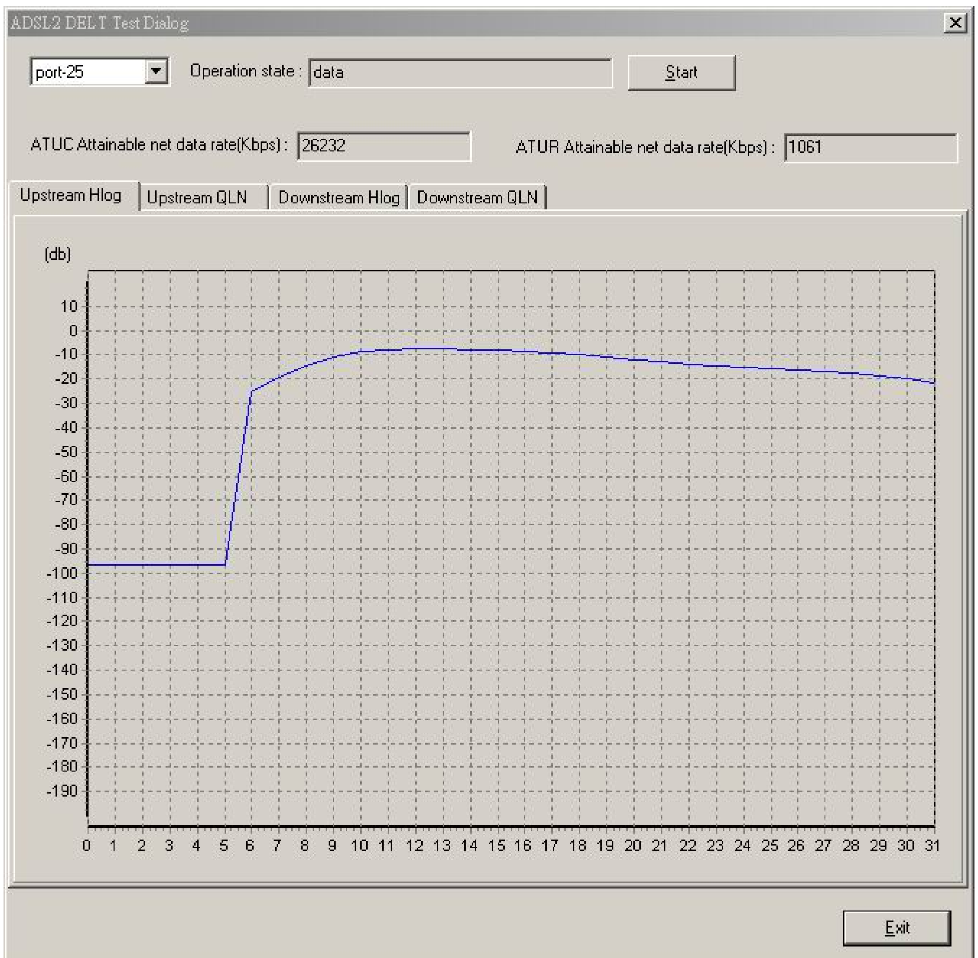


Table 3-43 Monitoring DELT Run & Report

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

Table 3-43 Monitoring DELT Run & Report

Item	Description
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)

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), 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 3-60 ATM OAM Test Dialog

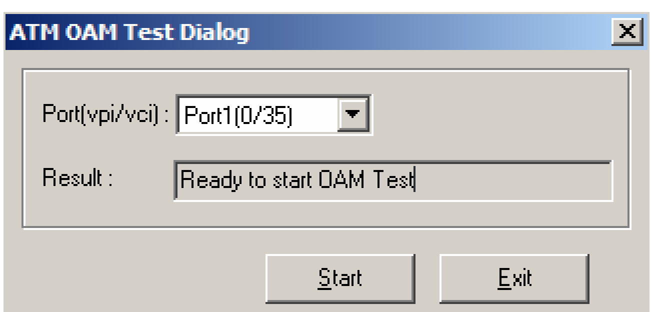


Table 3-44 describes the OAM test field items.

Table 3-44 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

Table 3-44 ATM OAM Test Dialog

Item	Description
	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.

DSL Bin Information

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

Figure 3-61 DSL Bin Information Dialog

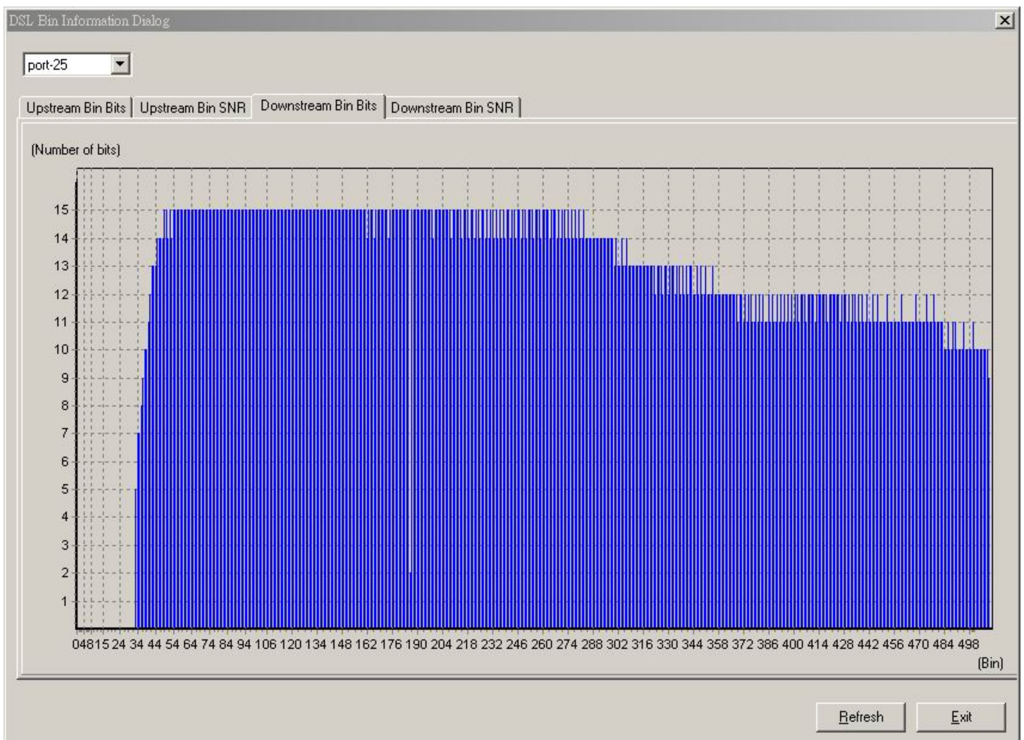


Table 3-45 describes the bin allocation tap items.

Table 3-45 DSL Bin Information Dialog

Item	Description
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)

Table 3-45 DSL Bin Information Dialog

Item	Description
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)

SELT Test

SELT (Single End Loop Test) is single-ended test, meaning that a copper loop is tested from the DSLAM only, without the need for any external test equipment in either the CO or at the remote end of the loop. SELT is primarily used for PROACTIVE loop pre-qualification. By knowing in advance if a loop is capable of supporting ADSL2+. By determining distance, wire gauge and noise, loop conditions can be fixed prior to rolling a truck to the customer premise. This not only saves time and money, but also improves customer satisfaction by avoiding “false start” installations.

Figure 3-62 SELT Test Dialog

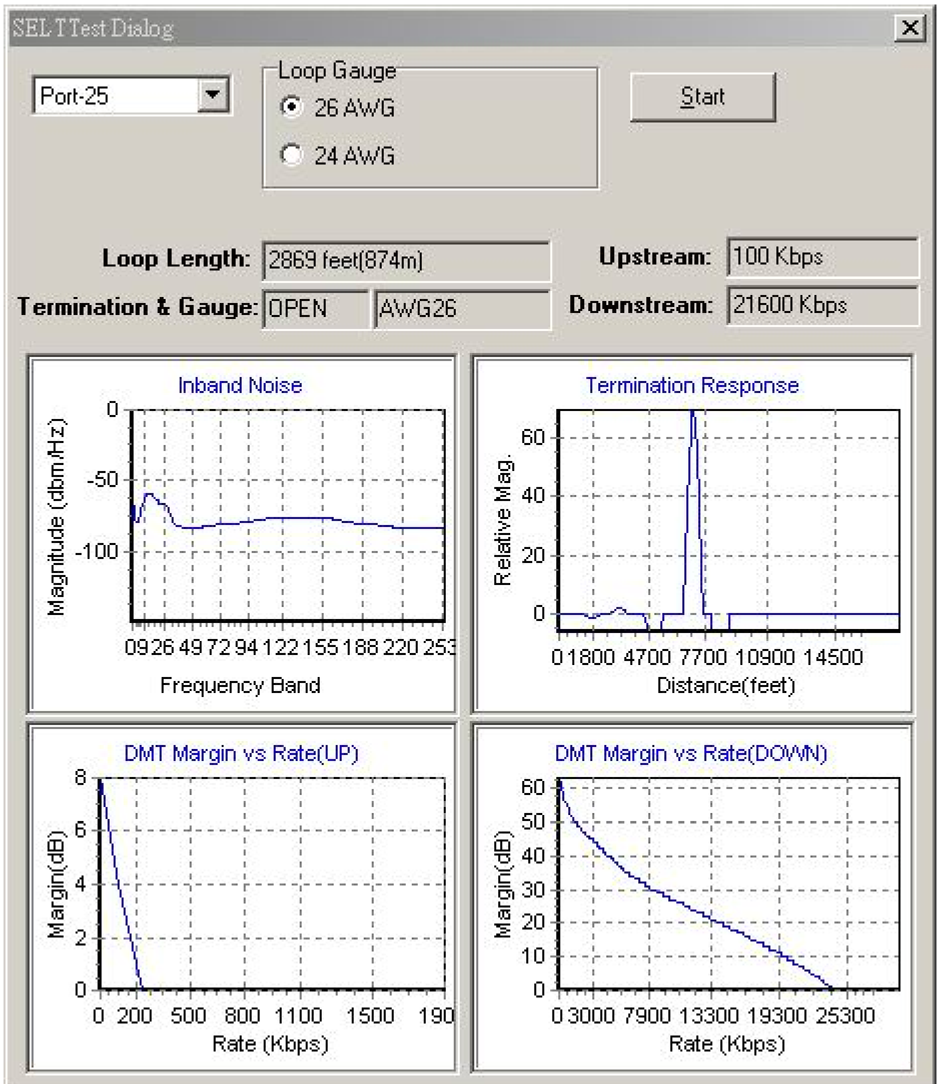


Table 3-46 SELT Testing Dialog

Item	Description
Port selection menu	Please select port from pull down menu
Value	Display various field obtains during SELT test.

Appendix A Abbreviations and Acronyms

The abbreviations and acronyms used in this document.

Table A-1 Abbreviations and Acronyms Table

Abbreviations	Full Name
AAL	ATM Adaptation Layer
ADSL	Asymmetric Digital Subscriber line
AIS	Alarm Indication Signal
ATM	Asynchronous Transfer Mode
ATU-C	ADSL Transceiver Unit at the central office end
ATU-R	ADSL Transceiver Unit at the remote end
CBR	Constant Bit Rate
CV	Coding Violation
DSLAM	Digital Subscriber line Access Multiplexer
ES	Error Seconds
EOA	Ethernet over ATM
GE	Gigabit Ethernet
IP	Internet Protocol
LAN	Local Area Network
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
VCL	Virtual Channel Link
VDSL	Very high-speed Digital Subscriber line
VLAN	Virtual Local Area Network
VP	Virtual Path
VPI	Virtual Path Identifier
VTU-O	VDSL Transmission Unit at the Optical network interface
VTU-R	VDSL Transmission Unit at the remote end
WAN	Wide Area Network
xDSL	ADSL/VDSL

Index