

Advance Management System
Software Specification and Introduction Guide

Class:	Feature Specification/Product Description
Product:	AMS
Product Version:	Server/Client: v1.0.1
Doc. No.:	BCD3-TM-E-000500
Doc Version:	1.0
Publish Date:	2007/1/20

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

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

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

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

Advance Management System
Software Specification and Introduction Guide
Text Part Number: 0005-0000

Table of Contents

- Chapter 1 Preface..... 1**

 - 1.1 Purpose..... 1
 - 1.2 Organization..... 1
 - 1.3 Conventions 1

- Chapter 2 Advance Management System Overview 3**

 - 2.1 AMS Overview3
 - 2.2 AMS Design Algorithm3
 - 2.3 AMS Feature.....4
 - 2.4 The Architecture of AMS5
 - 2.4.1 AMS Server Software Block Diagram5
 - 2.4.2 AMS Interface Standards Architecture6
 - 2.4.3 AMS Hardware Development Architecture6
 - 2.5 AMS Technical Indices.....7
 - 2.6 System Hardware and Software Requirement7
 - 2.7 Database for AMS Server8
 - 2.8 Backup and Recovery Mechanism8
 - 2.9 AMS O&M Tools.....9

- Chapter 3 Getting Started AMS 11**

 - 3.1 Get the AMS server and client files..... 11
 - 3.2 Starting the AMS Server..... 11
 - 3.3 Starting AMS Client 11
 - 3.4 Navigating the AMS Client12
 - 3.4.1 Keyboard Commands12
 - 3.4.2 Right Mouse Button13
 - 3.4.3 AMS Client Window Overview13

- Chapter 4 DAS3 Series Operation Menus 15**

 - 4.1 Operation Window Overview 15
 - 4.2 System 16
 - 4.2.1 General Information16
 - 4.2.2 Uplink IP Configuration17
 - 4.2.3 Trap Configuration19
 - 4.2.4 SNMP.....20
 - 4.2.5 SNMP Trap Host Configuration.....20
 - 4.2.6 SNMP Host Configuration.....21
 - 4.2.7 SNMP Community Configuration22
 - 4.2.8 Backup & Restore22
 - 4.3 Configuration.....23
 - 4.3.1 VPI/VCI23
 - 4.3.2 Line Profile Configuration.....24
 - 4.3.3 Alarm Profile Configuration27
 - 4.3.4 Power Management.....30
 - 4.3.5 VLAN Management.....31
 - 4.3.6 Limit MAC Number.....37
 - 4.3.7 IGMP Snooping.....38
 - 4.3.8 Spanning Tree Protocol.....40
 - 4.3.9 Bridge Configuration42
 - 4.3.10 DHCP Relay Configuration43
 - 4.4 Fault45
 - 4.4.1 List Events.....45

4.4.2	List Alarms.....	45
4.5	Performance.....	47
4.5.1	ADSL Line Performance	47
4.5.2	Channel Performance	48
4.5.3	Port Performance.....	48
4.5.4	ADSL Line Performance Monitor	49
4.5.5	ADSL Channel Performance Monitor.....	50
4.5.6	Port Performance Monitor.....	50
4.6	Status Management	51
4.6.1	System Statistics	51
4.6.2	System Size Information	52
4.6.3	Port Status.....	53
4.6.4	ADSL Port Status	54
4.6.5	ADSL Line Status.....	55
4.6.6	ADSL Channel Status	56
4.6.7	Current VLAN.....	56
4.7	Utility	57
4.7.1	Ping NE from Client	57
4.7.2	Ping NE from Server	57
4.7.3	Telnet from Client	58
4.7.4	Check SNMP connection from Server	58
4.8	Security	59
4.8.1	User Name and Password	59
4.8.2	Access Control List	60
4.8.3	Filter Configuration.....	61
4.8.4	Filter Wizard.....	66
4.9	Maintenance.....	67
4.9.1	Reboot System	67
4.9.2	Commit.....	68
4.9.3	Restore Factory Configuration.....	69
4.9.4	ATM OAM Test	70
4.9.5	ADSL2 DELT Test	70
4.9.6	SELT Test	72
4.9.7	DSL Bin Information.....	73
Chapter 5 Security Management Functions		75
5.1	Security Management General Functions	75
5.2	Security Management General Features.....	76
5.3	Login and Logout	76
5.4	Viewing System User Online List.....	76
5.5	Operation Privilege.....	77
5.6	Security Level Application	78
Chapter 6 Subscriber and Service Management Functions.....		79
6.1	Service Management General Function	79
6.2	Subscriber Management General Functions	79
6.3	Creating of Subscriber Service Information	80
6.4	Service Management General Function	80
Chapter 7 General System Management Functions		81
7.1	AMS Client Options.....	81
7.2	System Server Management	81
Appendix A Database Dimension and Handle Time		A-1
Appendix B Abbreviations and Acronyms		B-1

List of Figures

Figure 2-1	AMS Server Processes Block Diagram.....	5
Figure 2-2	AMS Interface Standards Diagram.....	6
Figure 2-3	AMS Hardware Development Diagram	7
Figure 2-4	CPU Utilization	9
Figure 2-5	Network Utilization.....	9
Figure 3-1	Started AMS Server Dialog.....	11
Figure 3-2	Login AMS Client.....	12
Figure 3-3	AMS Client Main Window Overview.....	13
Figure 3-4	AMS Client NE Element Display Overview	13
Figure 4-1	AMS Operation Window of DAS3 Series	15
Figure 4-2	System General Information Dialog	16
Figure 4-3	IP Configuration Dialog	17
Figure 4-4	Trap Configuration Dialog.....	19
Figure 4-5	Modify Trap Status Dialog	19
Figure 4-6	Add Trap Host Dialog	21
Figure 4-7	SNMP Host Configuration Dialog.....	21
Figure 4-8	SNMP Community Configuration Dialog	22
Figure 4-9	Backup & Restore Configuration Dialog.....	22
Figure 4-10	VPI/VCI Configuration Dialog.....	24
Figure 4-11	Add VPI/VCI Dialog	24
Figure 4-12	Line Profile Configuration Dialog.....	25
Figure 4-13	ADSL Alarm Profile Dialog.....	28
Figure 4-14	Power Management Dialog	30
Figure 4-15	Static VLAN Dialog	32
Figure 4-16	VLAN Details Dialog.....	32
Figure 4-17	Add VLAN Configuration Dialog	33
Figure 4-18	VLAN Ports Management Dialog	34
Figure 4-19	Modify VLAN Ports Management Dialog.....	35
Figure 4-20	GVRP Ports Management Dialog.....	36
Figure 4-21	Modify GVRP Status Dialog	36
Figure 4-22	Limit MAC Number Dialog.....	37
Figure 4-23	IGMP Snooping Dialog.....	38
Figure 4-24	Modify IGMP Snooping Status Dialog	39
Figure 4-25	Spanning Tree Protocol Dialog.....	40
Figure 4-26	Bridge Configuration Dialog	42
Figure 4-27	DHCP Relay Configuration Dialog	44
Figure 4-28	List Events Dialog.....	45
Figure 4-29	List Alarms Dialog.....	46
Figure 4-30	ADSL Line Performance Dialog	47
Figure 4-31	Channel Performance Dialog	48
Figure 4-32	Port Performance Dialog.....	49
Figure 4-33	ADSL Line Performance Monitor Dialog	49
Figure 4-34	ADSL Channel Performance Monitor Dialog.....	50
Figure 4-35	Port Performance Monitor Dialog.....	50
Figure 4-36	System Statistics Information Dialog.....	51
Figure 4-37	System Size Information Dialog	52
Figure 4-38	Port Status Dialog.....	54
Figure 4-39	ADSL port status Dialog	55
Figure 4-40	ADSL Line Status Dialog	55
Figure 4-41	ADSL Channel Status Dialog	56
Figure 4-42	Current VLAN Dialog.....	56
Figure 4-43	Ping NE from Client Dialog.....	57
Figure 4-44	Ping NE from Server Dialog	57
Figure 4-45	Telnet from client Dialog.....	58

Figure 4-46	Check SNMP Connection from Server Dialog	58
Figure 4-47	User Name and Password Dialog	59
Figure 4-48	Port/PVC Access Control List Dialog	60
Figure 4-49	Global Access Control List Configuration Dialog.....	61
Figure 4-50	Filter Rule Dialog.....	62
Figure 4-51	Add Filter Rule Dialog	63
Figure 4-52	Filter Sub Rule Dialog	64
Figure 4-53	Add Ethernet Sub Rule Dialog	65
Figure 4-54	Add IP Sub Rule Dialog.....	65
Figure 4-55	Filter Wizard Dialog	66
Figure 4-56	Filter Wizard Select Sub Rule Dialog	67
Figure 4-57	System Reboot Dialog.....	67
Figure 4-58	System Commit Dialog.....	68
Figure 4-59	Restore Factory Configuration Dialog	69
Figure 4-60	ATM OAM Test Dialog	70
Figure 4-61	ADSL2 DELT Dialog	71
Figure 4-62	SELT Test Dialog	72
Figure 4-63	DSL Bin Information Dialog	74
Figure 5-1	Login Window	76
Figure 5-2	Operator Access Control List Window.....	77
Figure 5-3	Operator Operation Log List Window	78
Figure 6-1	Subscriber Management List Table	79
Figure 6-2	Subscriber Data Window.....	80
Figure 6-3	Service Management Control Panel	80

List of Tables

Table 4-1	General Information Dialog Description	16
Table 4-2	IP Configuration Dialog Description	17
Table 4-3	Modify Trap Status Dialog Description	20
Table 4-4	Monitoring Line Profile Configuration	26
Table 4-5	ADSL Alarm Profile Dialog Description	29
Table 4-6	ADSL Power Management Dialog Description.....	31
Table 4-7	Static VLAN Dialog Description	32
Table 4-8	VLAN Details Dialog Description.....	33
Table 4-9	Add VLAN Configuration Dialog Description.....	33
Table 4-10	VLAN Ports Management Dialog Description	35
Table 4-11	GVRP Ports Management Dialog.....	36
Table 4-12	Modify GVRP Status Dialog Description	37
Table 4-13	Limit MAC Number Dialog Description.....	37
Table 4-14	IGMP Snooping Dialog Description.....	38
Table 4-15	Spanning Tree Protocol Dialog Description.....	40
Table 4-16	Bridge Configuration Dialog Description	42
Table 4-17	DHCP Relay Configuration Dialog Description	44
Table 4-18	Line Performance Dialog Description.....	47
Table 4-19	Line Performance Dialog Description.....	48
Table 4-20	System Statistics Information Dialog Description.....	52
Table 4-21	System Size Information Dialog Description	53
Table 4-22	Port Status Dialog Description.....	54
Table 4-23	Port/PVC Access Control List Dialog Description	60
Table 4-24	Global Access Control List Configuration Dialog Description	61
Table 4-25	Filter Rule Dialog Description.....	62
Table 4-26	Add Filter Rule Dialog Description	63
Table 4-27	Filter Sub Rule Dialog Description	64
Table 4-28	Ethernet/IP Sub Rule Dialog Description	65

Table 4-29	Filter Wizard Add Rule Dialog Description	66
Table 4-30	DAS3 Series System Factory Default Parameters.....	69
Table 4-31	ATM OAM Test Dialog Description	70
Table 4-32	ADSL 2 DELT Dialog Description	71
Table 4-33	SELT Test Dialog Description	73
Table 4-34	DSL Bin Information Dialog Description	74
Table B-1	Abbreviations and Acronyms Table	B-1

Chapter 1 Preface

This preface discusses the following topic:

- Purpose
- Organization
- Conventions
- Related Documentation

1.1 Purpose

The purpose of this guide is to provide detailed information and description of Advance Management System, which includes both software and hardware architecture and other specific features.

1.2 Organization

This guide contains the following information:

- Preface
- Advance Management System Overview
- Getting Started AMS
- DAS3 Series Operation menus
- Security Management Functions
- Subscriber Management Functions
- General System Management Functions
- Appendix

1.3 Conventions

This section describes the conventions used in this guide.

The DAS Series IP-DSLAM is the Next-Generation xDSL Broadband Access Network comprises a DSLAM and a number of ATU-Rs, STU-Rs, and POTS splitter/Low-pass filter to construct a broadband access network between central office and customer premises. The DAS Series IP-DSLAM uses statistically multiplexing and ATM over xDSL technologies to provide the broadband data communication services, such as high speed Internet access and multimedia services, across existing twisted pair telephone line.

NE/NEs hereinafter referred as DAS Series IP CO-DSLAM, unless specifically indicated.

ADSL mention in this document covers ADSL, ADSL2, and ADSL2+, unless specifically indicated.

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

AMS – A complete centralized SNMP base NMS (Network Management System) provides GUI operation under Client-Server architecture through in-band or out-of-band IP interface to carrying out day of day operation, administration, maintenance, and configuration functions of the NE.

- **AMS Server** – The server station provides multiple NEs management and Database in order to perform reliability, stability, and flexibility to entire network management.

- **AMS Client** – Software system for Network Management System (NMS), it's in Client-Server architecture and has ability to provide controlling and management for the whole network through GUI interface to collocate with AMS Server.



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

Chapter 2 Advance Management System Overview

This chapter provides a general overview of AMS. It contains concepts used in the network and service management for the NEs (IP-DSLAM).

- AMS Overview
- Configuration Management Functions
- Fault Management Functions
- Performance Management Functions
- Security Management Functions

2.1 AMS Overview

The Advance Management System (AMS) enables high-speed data transfer using xDSL technology with the IP-DSLAM. AMS provide the carrier classes' level management of networks. AMS supports various functions and operations for effective management and troubleshooting of faults and the maintenance of the IP-DSLAM. It also supports GUI operations including various testing functions for the IP-DSLAM network elements.

Based on the unified Network Management System (NMS) platform of AMS, it employs the mature and widely-used Client-Server architecture. Therefore, it supports multiple clients and can be used to manage large and complex networks and flexibly extended to satisfy different requirements.

AMS provides a concise and consistent management mode. It provides unified topology management, fault management, performance management, configuration management, and security management. It also provides uniform device panels and operation maintenance interfaces.

2.2 AMS Design Algorithm

AMS is an integrated Service/Network/Element Management System (SMS/NMS/EMS) for the DAS Series equipments. It is designed to provide the operation, administration, maintenance and provisioning (OAM&P) functions of the DSLAM broadband access networks for the Telco operators.

With powerful activities of AMS, the Telco operators can monitor and controlling NEs (IP-DSLAM) equipments from a central Network Operating Center (NOC) and/or multiple geographically separated management site of domains to streamline of their operation needs.

The system supports Fault Management, Configuration Management, Performance Management, and Security Management functions follow by ITU-T TMN recommendations principles as defined in M.3010.

AMS is a centralized system that provides Graphic User Interface (GUI) capabilities for operators to perform OAM functional to the IP-DSLAM network elements (NE) operation of the Network and display the Network topology map. AMS is a total solution for end-to-end management systems.

AMS is developed based on the Client-Server model and follows the concept of Telecommunication Management Network (TMN) defined by ITU-T Rec. M.3000 series and DSL Forum TR-005/TR-066 and TR-030/TR-035 for ADSL Network Element Management and ADSL EMS to NMS, respectively.

AMS is designed based on the following principles:

- Follow the ITU-T TMN standards X.700 series recommendations

- Control, monitor and configure the network in real-time such as diagnostics and status of the NE
- Provide synchronization function to maintain the data consistence between the AMS Server and the NEs
- Centralized management with distributed system
- Client-Server architecture
- High reliability and scalable for future enhancement and upgrade
- Easy to maintain with AMS hardware platform
- Provide southbound and northbound communication interface for NMS
- Provide user-friendly configuration interface
- Provide mass capability to manage xDSL link
- Support workstations working simultaneously
- Support restoration of configuration data in case of system failure
- Keep historic data for each subscriber line
- To enable/disable various alarm severity levels are provided for all possible events/conditions
- Easy to be integrated with the carrier's existing OSSs
- Failure on AMS or loss of communication between AMS and network element will not affect the operation of equipment and network

2.3 AMS Feature

The AMS system supports various functions for the effective operation and maintenance of the xDSL communications network. The system supports topology management, fault management, performance management, configuration management, and security management of the IP-DSLAM.

User Friendly GUI Design for OAM

The AMS provides standard Graphic User Interface (GUI) of AMS Client, it support OAM function operation of the network and display topology map, the command processing functions through graphical menu capabilities to provide convenient operation and maintenance.

Real-time System Status Monitoring

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

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

Administrative

The AMS has ability to displaying the network objects (NEs) graphically to define the topology of the network and configure the network, this feature allow operator be able to built, view and modify the network by placing nodes and subscriber into the network.

The AMS also provides function to equip the node with unit and interface module to adding it on the network.

Administrative function allows operator to planning or supervision their NE on the network.

Error Handling

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

AMS Client support function to depict the failure status of the Location and NE in registered manage network.

Historical Footprint

The AMS is able to maintain an on-line historical log for all received management parameters. The retrieving function with filtering capabilities for management data is provided.

The AMS is able to export and report the log and management information to the specific file format.

2.4 The Architecture of AMS

This section describes the AMS Server architecture and network protocols within used.

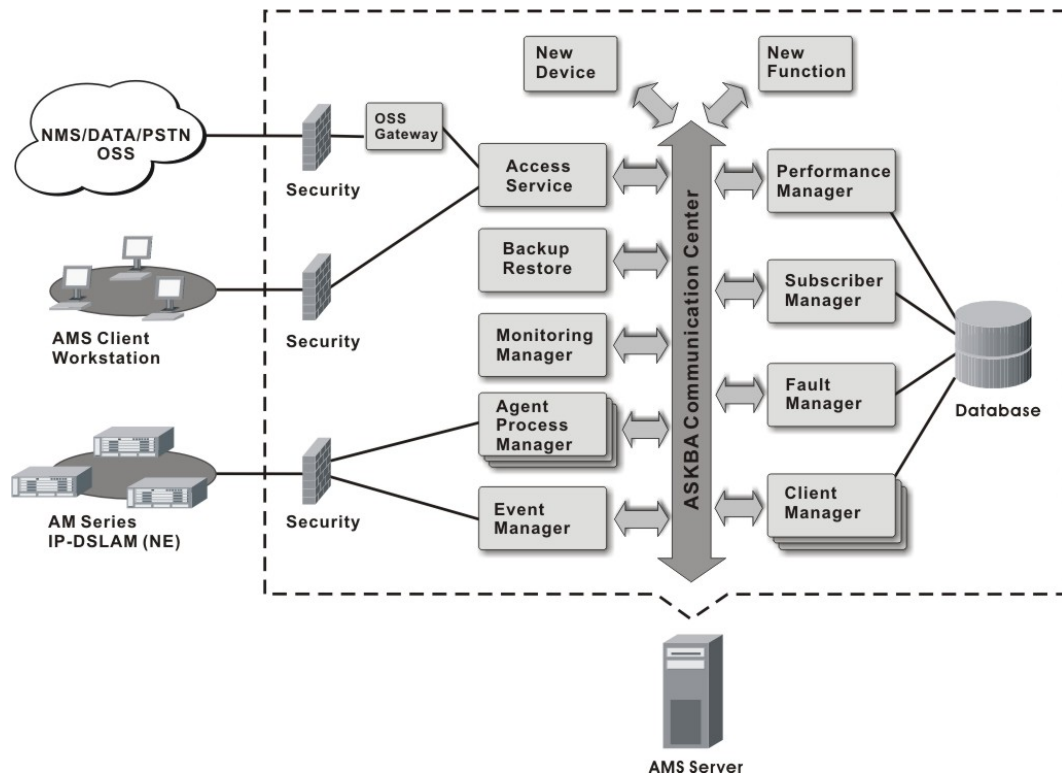
AMS is base on Client-Server architecture with database to store the enormous of NEs (Network Elements) information, includes the fault manager, performance manager, and other facility.

2.4.1 AMS Server Software Block Diagram

By employing the multi-process, modular architecture, and object-oriented design, with distributed system management supported, AMS provides high scalability, flexibility, and reliability.

The Process Manager (PM) control schedules to the NE daemon in a real-time of unified manner and monitors, all PM use the same ASKBA Communication Center (ACC) to transfer messages in between, thus making the NE daemons highly independent, each PM application can initiate multiple real-time tasks, which can be quickly switched in between.

Figure 2-1 AMS Server Processes Block Diagram



AMS Server provides device-specific component management applications. As one major feature of the NMS, the high scalability shows itself in the modular management to added new functions and easy integrated with other NMS devices.

2.4.2 AMS Interface Standards Architecture

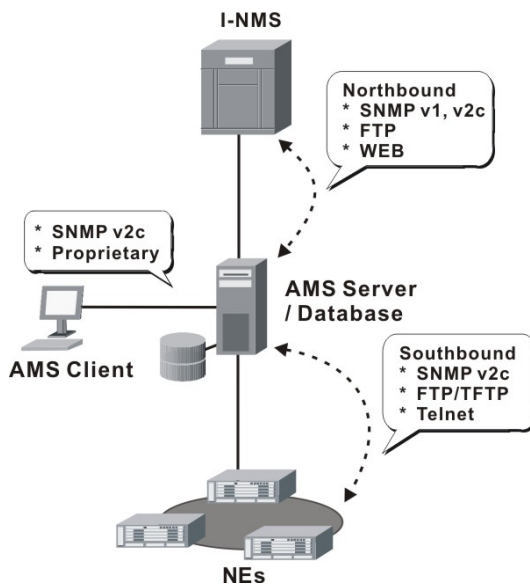
The interface standards use with in AMS Server northbound are support of SNMP v1, SNMP v2c, FTP, and WEB as an open data interface for communication between other OSS (Operation Support Systems), for southbound interface standards use are SNMP v2c and FTP/TFTP. The communication between AMS Client and AMS Server use SNMP and it proprietary protocol.

The interface protocol between AMS Server and NE is SNMP v2c.

The AMS is acts as the manager of management activities to perform monitoring and controlling NEs within its management domain.

The AMS will synchronize the NEs information and its database automatically in real-time for both direction.

Figure 2-2 AMS Interface Standards Diagram



Northbound Interface

- Northbound SNMP (v1, v2c) Interfaces – The integration interfaces of the AMS to other NMS devices.
- Northbound FTP Interface – The management interfaces for report retrieve.
- Northbound WEB Interface – The WEB base monitoring of Configuration, Fault, and Performance management.

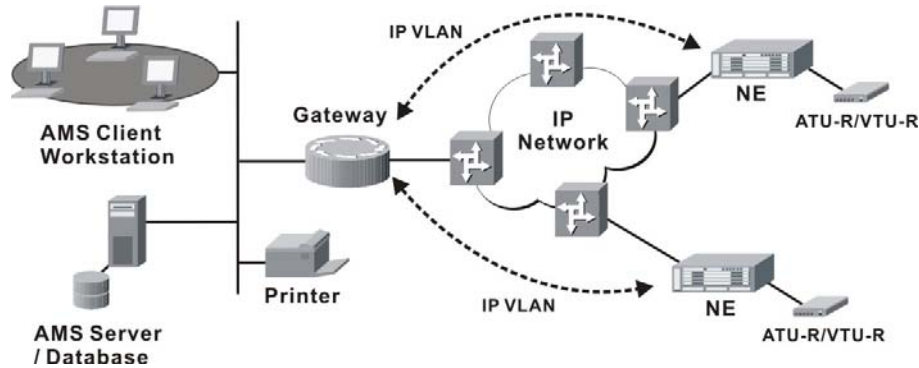
Southbound Interface

- Southbound SNMP v2c Interfaces – The management interfaces of AMS Server to the NE devices.
- Southbound FTP/TFTP Interfaces – The standard FTP/TFTP interfaces used to load, backup, and synchronize the NE devices.
- Southbound Telnet interface – The command line interface (CLI) of the AMS to the NE devices.

2.4.3 AMS Hardware Development Architecture

AMS system has ability to provide the end-to-end connecting via out-of-band IP management Ethernet interface or in-band with VLAN through gateway to reach GE interface of NE, to perform management function either independently or simultaneously.

Figure 2-3 AMS Hardware Development Diagram



AMS consists of a system server (AMS Server), workstations (AMS Client), gateways, switch hubs, and laser printers to manage the NEs, the AMS hardware architecture is shown as Figure 2-3.

The AMS is designed using Client-Server architecture and able to be managed from single software and hardware platform to have centralized network view of NEs.

2.5 AMS Technical Indices

- The AMS supports more than 1,000 NEs and 700,000 xDSL Subscribers in single AMS Server with minimum hardware specification, see this document “Chapter 2.6”.
- AMS Server can support 20 of AMS Client logging simultaneously.
- The current alarm table can store 1,000,000 alarm records at most. The alarm records to be stored in the alarm history table and the event table can be set by the user (the data will be dumped when the alarm history table or the event table is full). A maximum of 1,000,000 history alarms can be stored.
- The log database can save the log information generated during 3 months or more.
- The AMS supports function to maintain the data consistence between the AMS Server and the registered NEs in real-time.
- AMS Server has ability to keep the records of registered NEs parameter status update due to power or equipment failures.

2.6 System Hardware and Software Requirement

AMS has design in high stability and reliability platform, for perform fluent in management, the minimum hardware specification require for handle around 1,000 NEs and 20 concurrent user access from AMS Client are recommend in list below to optimal the performance. System itself have not limitation on the number of elements under it management, the limit has only be restricted by the size of the AMS hardware capabilities.

The recommend hardware & OS for AMS Server:

- Intel® Xeon™ 2.8 GHz or higher
- 1 GB RAM
- 100 GB Hard disk
- RAID 1 support
- SCSI hard disk or SATA-I/II support
- 10/100/1000 Base-T Ethernet network card
- Operating System – MS Windows 2000 Server / Windows 2003 Server

The recommend hardware & OS for AMS Client:

- Pentium 4 2.0 GHz or higher
- 512 MB RAM
- 40 GB Hard disk
- 10/100/1000 Base-T Ethernet network card
- Operating System – MS Windows 2000 Professional

The Software require for AMS System:

- AMS Installation Package
- JDK Runtime (Java)

2.7 Database for AMS Server

The Database use for AMS server is very comprehensive, the current implementing database using with AMS Server is MySQL and operating under same AMS Server OS.

The features of AMS database are lists as follow:

- Accommodate on future enhancement and modification design base
- Stability and flexibility to be able to grow with upgrade hardware
- Easy to migrate and backup
- Portable from one server to another without massive conversion involved
- Support data automated polling to the specify common repository server

2.8 Backup and Recovery Mechanism

With database backup and restore mechanism, AMS provide this mechanism for operator to save and reload the entire network configuration, include, configuration management, fault management, performance management, subscriber management, and security management data, the system data can be stored at the external non-volatile media and can be reloaded on demand to the network. In case if AMS fails due to power or equipment defective, this mechanism can keep the records of network management parameters up-to-date to prevent unnecessary damage.

The NE configuration data are backup in the server in plain text format, server will keep most recent of 30 days NE data, while the restore required; the operator has ability to choose the data from the backup list to retrieve the passed configuration.

Once the backup is in process, none of any user operation and network service will be interrupted, the files will be store in the hard disk of specific backup directory. A display message will inform operator on back and recovery to maintain the data integrity, operator can easy to store backup data to the DAT tape or burning to the recordable CD.

The duration of database backup storage is around 60 seconds with 1500 subscribers in 7 days of performance and fault management relation data files.

The features of AMS database backup and recovery are lists as follow:

- Support both backup and recovery
- Support automation and schedule of backup activity
- Support database backup and recovery on demand
- Support database backup file include the NE's IP address and date-time
- Support NE by NE or entire network backup and recovery

2.9 AMS O&M Tools

The AMS has ability and capabilities to perform the AMS platform of its own self-health check, such as viewing the CPU utilization, Memory, and Network utilization.

Figure 2-4 CPU Utilization

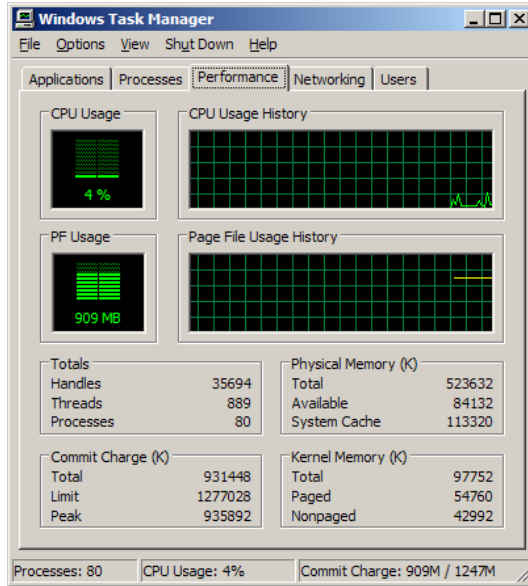
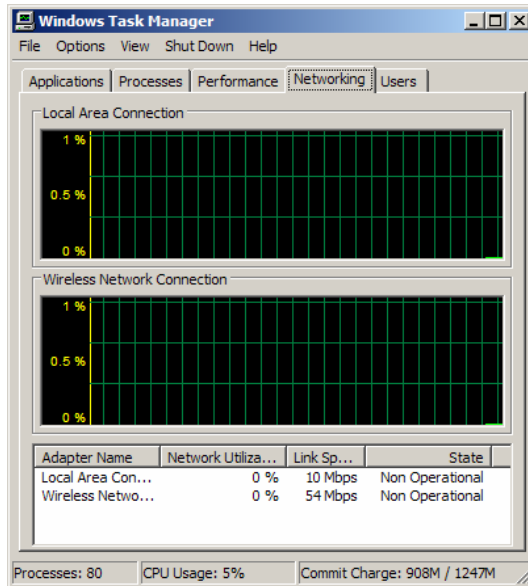


Figure 2-5 Network Utilization



This page is leave in blank for note or memo use

Chapter 3 Getting Started AMS

This chapter provides the detail descriptions to start the AMS in your network.

- Get the AMS server and client files
- Starting the AMS Server
- Starting the AMS Client
- Navigating of AMS Client

3.1 Get the AMS server and client files

AMS software consists of two zip files: AMS_Server_Windows and AMS_Client_Windows. Login and download the files the AMS software from the WEB site <http://tm.askey.com.tw>.

In order to download these files successfully, please contact with the local agent to get your username and password.

3.2 Starting the AMS Server

Unzip the AMS_Server_Windows file to a designated path, for example, C:\AMS_Server_Windows\. Go to the sub-directory under “bin”, for example, C:\AMS_Server_Windows\bin\. Start the AMS Server by executing “startnms.bat” on server PC.

Wait for the message which indicates that AMS server is running, as shown in Figure 3-1.

Figure 3-1 Started AMS Server Dialog

```

C:\WINDOWS\system32\cmd.exe
Process : NmsAuthManager [ Started ]
Process : DBServer [ Started ]
Process : NmsConfigurationServer [ Started ]
Process : NmsSUM [ Started ]
Process : EventMgr [ Started ]
Process : WebNMSAgentApp [ Started ]
Process : ASKEYModuleBE [ Started ]
Process : Collector [ Started ]
Process : MapServerBE [ Started ]
Process : StartProvModule [ Started ]
Process : PolicyFE [ Started ]
Process : MServerFE [ Started ]
Process : NmsSAServerFE [ Started ]
Process : SAServerFE [ Started ]
Process : AuthenticationManagerFE [ Started ]
Process : UserConfigProcessFE [ Started ]
Process : ExampleFE [ Started ]
Process : ProvisioningFE [ Started ]
Process : WebNMSMgmtFEProcess [ Started ]
Process : MapFE [ Started ]
Process : AlertFE [ Started ]
Process : ConfigFE [ Started ]
Process : NmsMainFE [ Started ]
Process : AuthorizationManagerFE [ Started ]
Process : PoLIFE [ Started ]
Process : TopoFE [ Started ]
Process : EventFE [ Started ]

Verifying connection with web server ... verified

Web NMS Server modules started successfully at 一月 02,2007 11:55:52 上午

Please connect your client to the web server on port: 9090
  
```

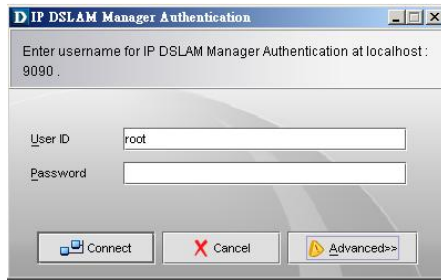
3.3 Starting AMS Client

Unzip the AMS_Client_Windows file to a designated path, for example, C:\AMS_Client_Windows\. Go to the sub-directory under “bin”, for example, C:\AMS_Client_Windows\bin\.

As shown in Figure 3-2, start the AMS Server by executing “startApplicationClient.bat” on the client PC, use User ID/Password = root/public then click “Advanced” button and enter the correct IP address

of AMS server, and press “Connect” button to login.

Figure 3-2 Login AMS Client



Then click “Advanced” button.



Enter the correct IP address of AMS Server.

NOTE The AMS Server and Client can be executed on either the same PC or on different PCs.

3.4 Navigating the AMS Client

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

3.4.1 Keyboard Commands

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

Keyboard Command	Description
Operation	
Tab	Move among the fields in a window/dialog.
Arrow Keys	Scroll through the text in a data entry field or through the values of a list box.

3.4.2 Right Mouse Button

AMS Client software provides right-click mouse functionality. Position the mouse cursor over an NE object which are comprehend of NE entity, Shelf, Slot/Box, or Port display on the Device Tag of each Network element windows, you can click the right mouse button to view the pop-up **Function Menu**, the **Function Menu** options available depends on selected object. You can then use the left or right mouse button to open the accordance function dialog window.

3.4.3 AMS Client Window Overview

The AMS Client element window contains several parts; each part is varying depending on the window in which you are viewing or configuring.

Figure 3-3 AMS Client Main Window Overview

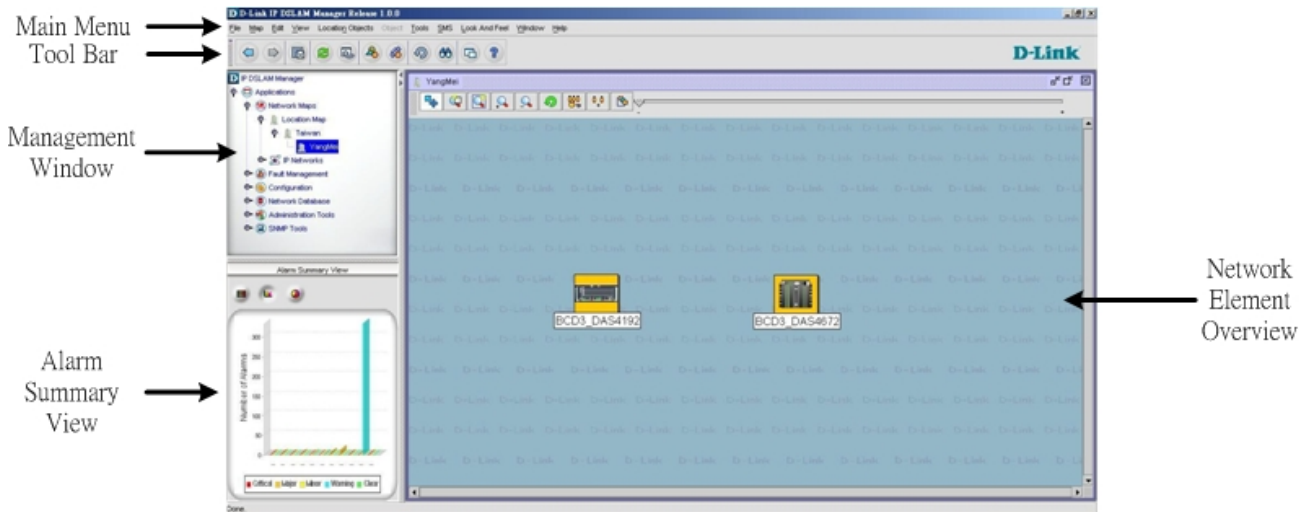
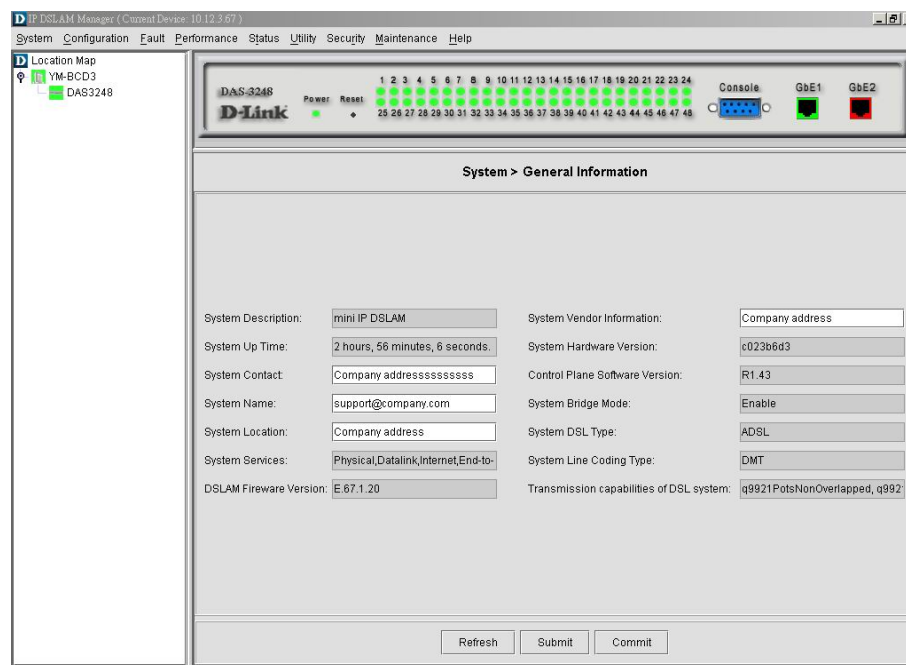


Figure 3-4 AMS Client NE Element Display Overview



This page is leave in blank for note or memo use

Chapter 4 DAS3 Series Operation Menus

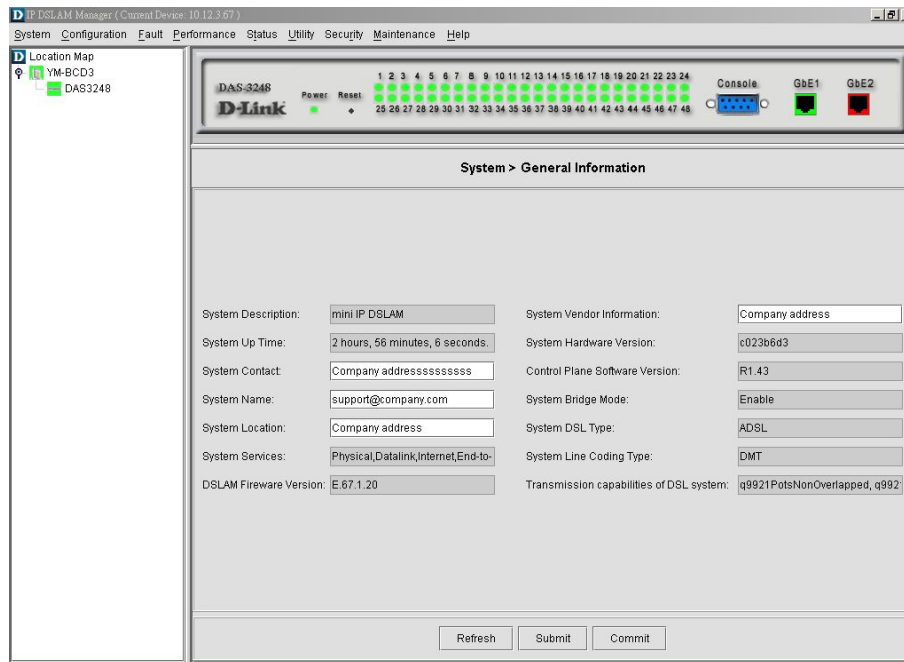
The chapter provides the detail descriptions on software configurations and administrating procedures for DAS AMS. This chapter contains the following sections:

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

4.1 Operation Window Overview

The DAS AMS operation window contains main menu, agent list, alarm and trap information list and real-time LED status panel. AMS will automatically detect model and show the correct LED status panel. Figure 4-1 is the panel for DAS3 Series

Figure 4-1 AMS Operation Window of DAS3 Series



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.

4.2 System

The section allows you to manage your DAS3 Series IP-DSLAM on the system level. Operator can view System information, modify Uplink IP setting, Trap and SNMP configuration. Backup and restore of system configuration is also covered in this section.

4.2.1 General Information

You can edit the system information in this dialog. Figure 4-2 illustrates the General Information Dialog.

Figure 4-2 System General Information Dialog

Table 4-1 describes the general information dialog field items.

Table 4-1 General Information Dialog Description

Item	Description
System Description	This is a text description of the entity.
System Up Time	This shows the time since the system is up.
System Contact	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 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 ';'.

Table 4-1 General Information Dialog Description

Item	Description
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

4.2.2 Uplink IP Configuration

IP Configuration menu allows operator to modify uplink interface setting. Figure 4-3 illustrates the IP Configuration Dialog.

Figure 4-3 IP Configuration Dialog

Table 4-2 IP Configuration Dialog Description

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

Table 4-2 IP Configuration Dialog Description

Item	Description
Net Mask	This specifies the network mask configured for the interface. Valid values: 255.0.0.0 ~ 255.255.255.255
Use DHCP	This specifies whether current NE uses DHCP.
Interface Type	The type of Ethernet interface, uplink or downlink.
Duplex Mode	The duplex mode use by the Ethernet interface.
Output Rate Limit	This parameter specifies the output rate limiting value to be applied on this interface. The unit is in Mbits/sec. This setting will have effect on receiving data rate of specified port. Valid values: 0 ~ 300 Mbps
Management VLAN ID	VLAN for management traffic on this interface. Nonzero value of this field is valid only if either 'IP Address' field is non-zero or 'Is use DHCP' field is true. If no Management VLAN ID is specified (in the create operation) or it's 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 use DHCP' field is true. Valid values: 0 ~ 7
Current Port Speed	The speed automatically detected or configured by user.
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.

4.2.3 Trap Configuration

Trap Configuration allows operator to enable/disable traps for the NE and system. Figure 4-4 illustrates Trap Configuration Dialog showing the trap status for each port. Figure 4-5 illustrates Modify Trap Status Dialog which allows operator to change system and port trap status.

Figure 4-4 Trap Configuration Dialog

Port ID	Operational State Changed	LinkUp/LinkDown Trap	Initial Failure Trap	Power Management Trap
Port 1	Disable	Enable	Disable	Disable
Port 2	Disable	Enable	Disable	Disable
Port 3	Disable	Enable	Disable	Disable
Port 4	Disable	Enable	Disable	Disable
Port 5	Disable	Enable	Disable	Disable
Port 6	Disable	Enable	Disable	Disable
Port 7	Disable	Enable	Disable	Disable
Port 8	Disable	Enable	Disable	Disable
Port 9	Disable	Enable	Disable	Disable
Port 10	Disable	Enable	Disable	Disable
Port 11	Disable	Enable	Disable	Disable
Port 12	Disable	Enable	Disable	Disable
Port 13	Disable	Enable	Disable	Disable
Port 14	Disable	Enable	Disable	Disable
Port 15	Disable	Enable	Disable	Disable
Port 16	Disable	Enable	Disable	Disable
Port 17	Disable	Enable	Disable	Disable
Port 18	Disable	Enable	Disable	Disable
Port 19	Disable	Enable	Disable	Disable
Port 20	Disable	Enable	Disable	Disable
Port 21	Disable	Enable	Disable	Disable
Port 22	Disable	Enable	Disable	Disable
Port 23	Disable	Enable	Disable	Disable
Port 24	Disable	Enable	Disable	Disable
Port 25	Disable	Enable	Disable	Disable
Port 26	Disable	Enable	Disable	Disable
Port 27	Disable	Enable	Disable	Disable

Figure 4-5 Modify Trap Status Dialog

Table 4-3 describes the fields in Modify Trap Status Dialog.

Table 4-3 Modify Trap Status Dialog Description

Item	Description
System Trap	<p>Authentication Failure Trap : Indicates whether Authentication Failure Trap should be generated for this interface.</p> <p>Binding Status Changed Trap : Indicates whether Binding Status Trap should be generated for this interface.</p>
Interface Trap	<p>Link Up/Link Down : Indicates whether linkUp/linkDown traps should be generated for this interface.</p> <p>Initial Failure : Indicates whether ATUC initialization failure Trap should be generated for this interface.</p> <p>Operate State Change : Indicates whether Operation State Change Trap should be generated for this interface.</p> <p>Power Management : PM state change trap used for ADSL2 / ADSL2plus PM operation. This trap is not valid for ADSL mode.</p>

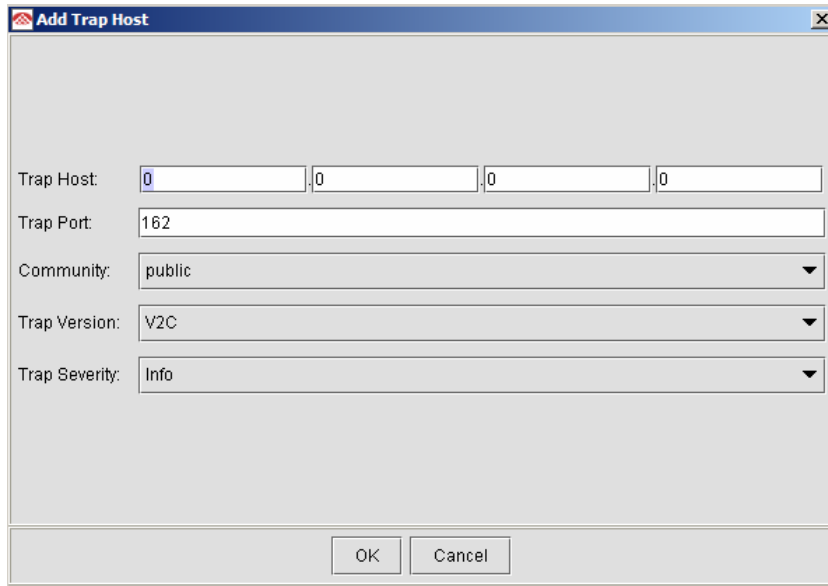
4.2.4 SNMP

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.

4.2.5 SNMP Trap Host Configuration

SNMP Trap Host configuration allows operator to add/remove/modify Trap Host for the network element. Click Add to bring up Figure 4-6 to add additional Trap Host.

Figure 4-6 Add Trap Host Dialog



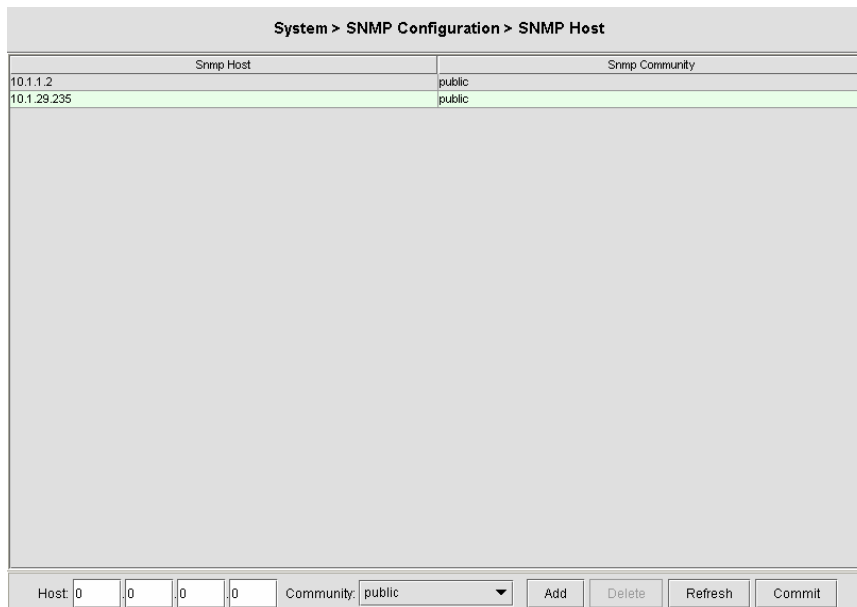
The 'Add Trap Host' dialog box contains the following fields and controls:

- Trap Host: Four input fields, each containing the digit '0'.
- Trap Port: A text input field containing '162'.
- Community: A dropdown menu with 'public' selected.
- Trap Version: A dropdown menu with 'V2C' selected.
- Trap Severity: A dropdown menu with 'Info' selected.
- Buttons: 'OK' and 'Cancel' buttons at the bottom.

4.2.6 SNMP Host Configuration

SNMP Host configuration allows operator to add new host to configure the current network element. Figure 4-7 shows the windows to add new SNMP host. Input new host IP at the bottom of the screen and click Add.

Figure 4-7 SNMP Host Configuration Dialog



The 'SNMP Host Configuration' dialog shows a table of existing hosts and a configuration area at the bottom.

System > SNMP Configuration > SNMP Host	
Snmp Host	Snmp Community
10.1.1.2	public
10.1.29.235	public

At the bottom of the dialog, there is a configuration area with the following elements:

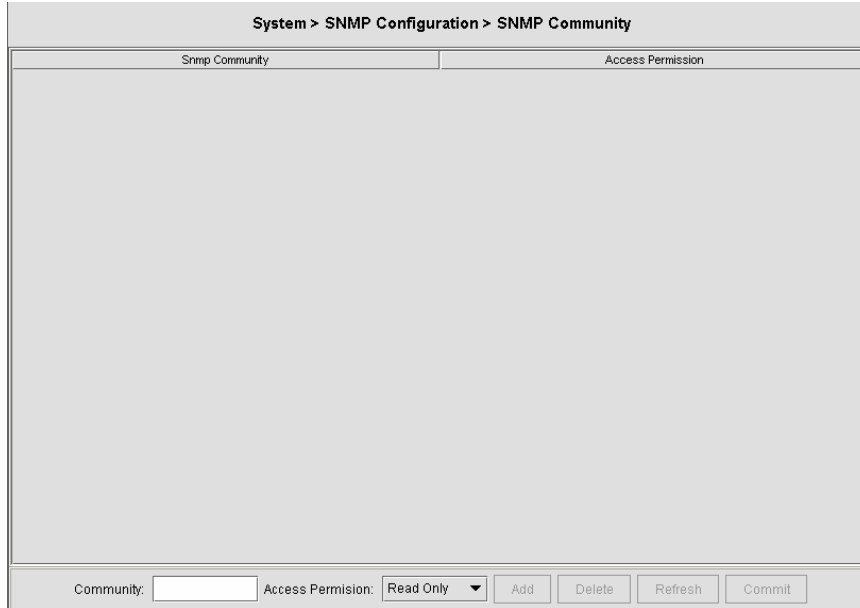
- Host: Four input fields, each containing '0'.
- Community: A dropdown menu with 'public' selected.
- Buttons: 'Add', 'Delete', 'Refresh', and 'Commit' buttons.

4.2.7 SNMP Community Configuration

SNMP Community configuration allows operator to add/remove/modify the SNMP community. The community access has relationship to the mapping Host IP, changed the community access option will change the access privilege of specifics Host IP.

Figure 4-8 illustrates the dialog for the SNMP community configuration.

Figure 4-8 SNMP Community Configuration Dialog



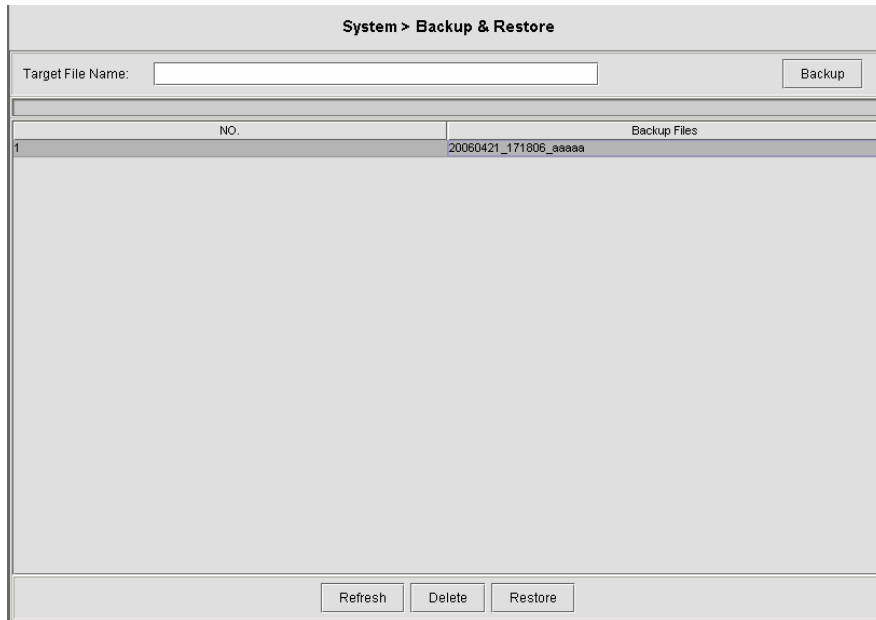
The screenshot shows a web-based configuration dialog titled "System > SNMP Configuration > SNMP Community". It features two tabs: "Snmp Community" and "Access Permission". The main area is currently empty. At the bottom, there are input fields for "Community:" and "Access Permission:" (set to "Read Only"), along with "Add", "Delete", "Refresh", and "Commit" buttons.

4.2.8 Backup & Restore

Backup & Restore function allows operator to save current network element configuration. The file will be saved at the folder containing server component with IP address as sub-folder.

Figure 4-9 illustrates the Backup & Restore Configuration Dialog.

Figure 4-9 Backup & Restore Configuration Dialog



The screenshot shows a web-based configuration dialog titled "System > Backup & Restore". It includes a "Target File Name:" input field and a "Backup" button. Below this is a table with columns "NO." and "Backup Files". One row is visible with "1" in the "NO." column and "20060421_171806_aaaaa" in the "Backup Files" column. At the bottom, there are "Refresh", "Delete", and "Restore" buttons.

NO.	Backup Files
1	20060421_171806_aaaaa

4.3 Configuration

Configuration menu contains setting for VPI/VCI, ADSL Line profile, alarm profile, power management profile, as well as VLAN, MAC, IGMP, Spanning Tree Protocol, Bridge Information, and DHCP configuration.

4.3.1 VPI/VCI

VPI/VCI configuration allows operator to add PVC for the network element. Figure 4-10 shows the window to add VPI/VCI.

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 is 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 4-10 VPI/VCI Configuration Dialog

Configuration Management > VPI/VCI				
Port	VPI	VCI	Status	
Port 1	0	35	Admin Up	
Port 2	0	35	Admin Up	
Port 3	0	35	Admin Up	
Port 4	0	35	Admin Up	
Port 5	0	35	Admin Up	
Port 6	0	35	Admin Up	
Port 7	0	35	Admin Up	
Port 8	0	35	Admin Up	
Port 9	0	35	Admin Up	
Port 10	0	35	Admin Up	
Port 11	0	35	Admin Up	
Port 12	0	35	Admin Up	
Port 13	0	35	Admin Up	
Port 14	0	35	Admin Up	
Port 15	0	35	Admin Up	
Port 16	0	35	Admin Up	
Port 17	0	35	Admin Up	
Port 18	0	35	Admin Up	
Port 19	0	35	Admin Up	
Port 20	0	35	Admin Up	
Port 21	0	35	Admin Up	
Port 22	0	35	Admin Up	
Port 23	0	35	Admin Up	
Port 24	0	35	Admin Up	
Port 25	0	35	Admin Up	
Port 26	0	35	Admin Up	
Port 27	0	35	Admin Up	
Port 28	0	35	Admin Up	
Port 29	0	35	Admin Up	
Port 30	0	35	Admin Up	

Refresh Add Delete Commit

Click “Add” to create additional PVC. Figure 4-11 shows the dialog window for adding VPI/VCI. If click the >>> icon, a new window, which allowing users to add PVC for multiple ports at once, will pop up.

Figure 4-11 Add VPI/VCI Dialog

Add VPI/VCI

Port: PVC Number:

VPI: No Change

VCI: No Change

Encap Type:

Port	VPI	VCI	Encapsulation Type	Status
Port 4	0	35	llcmux	Admin Up
Port 4	0	31	llcmux	Admin Up
Port 4	0	32	llcmux	Admin Up

OK Cancel >>>

4.3.2 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 ‘Submit’ to activate.

Figure 4-12 Line Profile Configuration Dialog

Configuration Management > ADSL Line Profiles

Port: Port Status:

Line Interface
 Standard: Psd Mask Type: Line Type:

ATUC
 Rate Mode: DMT Configure Mode: DMT Trellis Operation:

-SNR Margin(dB/10)		-Min Time(sec)		-TX Rate(Kbps) and Delay(ms)	
Target SNR Margin:	<input type="text" value="60"/>	UpShift Time:	<input type="text" value="0"/>	Min TX Rate:	<input type="text" value="32"/>
Max SNR Margin:	<input type="text" value="310"/>	DnShift Time:	<input type="text" value="0"/>	Max TX Rate:	<input type="text" value="28,000"/>
Min SNR Margin:	<input type="text" value="0"/>			Max Interleave Delay:	<input type="text" value="16"/>
UpShift SNR Margin:	<input type="text" value="120"/>				
DnShift SNR Margin:	<input type="text" value="0"/>				

-SNR Margin(dB/10)		-Min Time(sec)		-TX Rate(Kbps) and Delay(ms)	
Target SNR Margin:	<input type="text" value="60"/>	UpShift Time:	<input type="text" value="30"/>	Min TX Rate:	<input type="text" value="32"/>
Max SNR Margin:	<input type="text" value="310"/>	DnShift Time:	<input type="text" value="30"/>	Max TX Rate:	<input type="text" value="1,088"/>
Min SNR Margin:	<input type="text" value="310"/>			Max Interleave Delay:	<input type="text" value="16"/>
UpShift SNR Margin:	<input type="text" value="90"/>				
DnShift SNR Margin:	<input type="text" value="30"/>				

Table 4-4 describes the full ADSL connection parameters.

Table 4-4 Monitoring Line Profile Configuration

Item	Description
Select a port	Select the ADSL port interface to be display with relative parameters.
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)

Table 4-4 Monitoring Line Profile Configuration

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)
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)
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 interleaver input and their placement in the bit stream at the interleaver 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)

4.3.3 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 4-13 ADSL Alarm Profile Dialog

The screenshot shows a web-based configuration interface titled "Configuration Management > ADSL Alarm Profiles". At the top, there is a "Port:" dropdown menu set to "Port 1". Below this, the interface is divided into two main sections: "ATUC" and "ATUR". Each section contains two columns of input fields. The left column in each section is labeled "-15 min (sec)" and the right column is labeled "1 day (sec)". Each column lists various alarm types with their corresponding values, all of which are currently set to "0".

Profile	Time Period	LOFs	LOSs	LOLs	LOPs	ESs	Fail FastR	SESL	UASL	FECsL
ATUC	-15 min (sec)	0	0	0	0	0	0	0	0	0
	1 day (sec)	0	0	0	0	0	0	0	0	0
ATUR	-15 min (sec)	0	0	0	0	0	0	0	0	0
	1 day (sec)	0	0	0	0	0	0	0	0	0

At the bottom of the dialog, there are three buttons: "Refresh", "Submit", and "Commit".

Table 4-5 describes the alarm profile dialog option items.

Table 4-5 ADSL Alarm Profile Dialog Description

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

4.3.4 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 to re-initialize and to enter into steady-state communication mode.

Figure 4-14 Power Management Dialog

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

Table 4-6 ADSL Power Management Dialog Description

Item	Description
Port selection pull down menu	Select the ADSL port interface to be display with relative parameters.
Power Management State Now	The Line Power Management status, not available for ADSL connection. Status: Data Operation, Idle Operation, L2 Operation
Power Management State Be Configured To:	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 Min 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 Entry Threshold Rate	PM configuration parameter. L2 state entry data rate. Valid values: 0 ~ 30000
Power Management Mode L2 Exit Threshold Rate	PM configuration parameter. L2 state exit 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
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.

4.3.5 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 DAS3 Series 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 4-15 Static VLAN Dialog

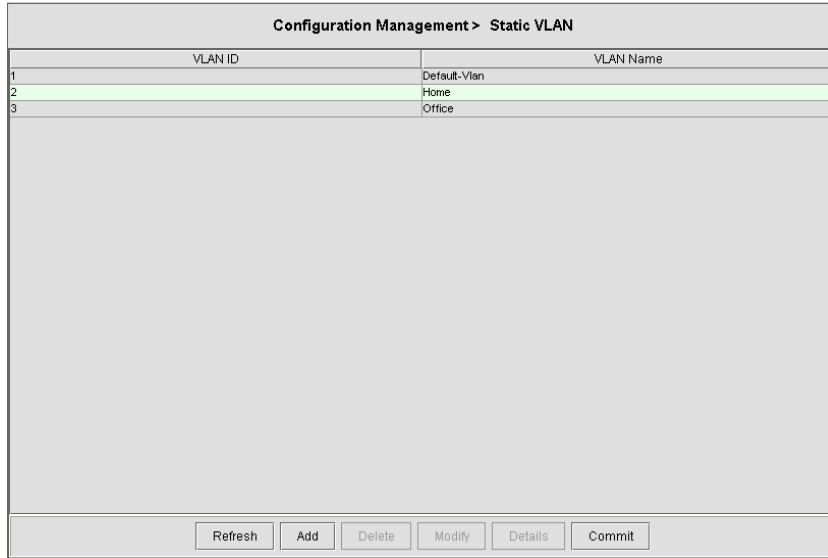


Table 4-7 Static VLAN Dialog Description

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

Click 'Detail' button to monitoring the selected VLAN information.

Figure 4-16 VLAN Details Dialog

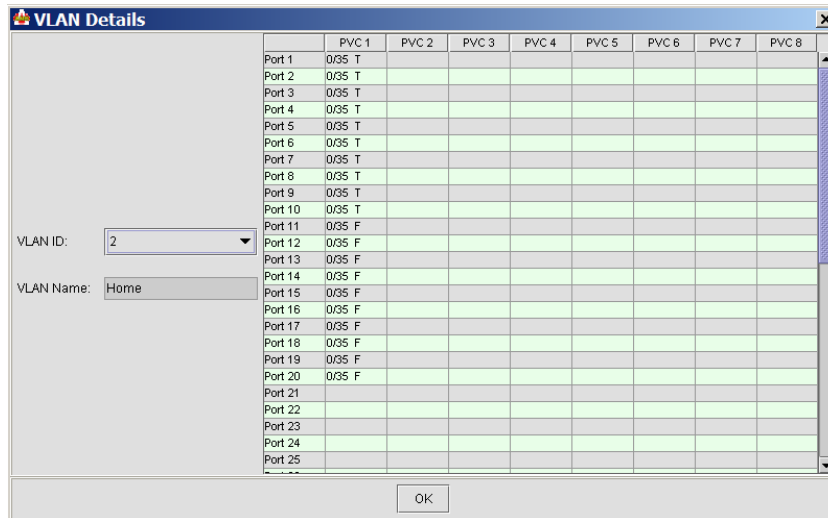


Table 4-8 VLAN Details Dialog Description

Item	Description
VLAN Index	Select desired VLAN to show VLAN configuration
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
PVC	For each port, display the path, circuit identifier number.
T/U	This setting determines a specific port to receive tagged (T) or untagged (U) frame.

Click 'Add' button to add the new VLAN with associate port interface.

Figure 4-17 Add VLAN Configuration Dialog

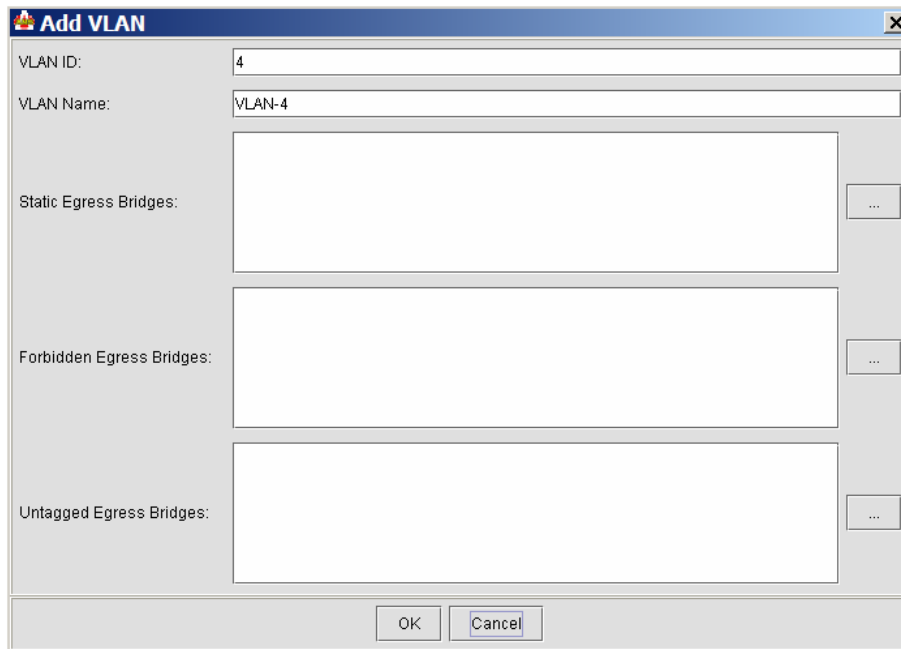



Table 4-9 Add VLAN Configuration Dialog Description

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

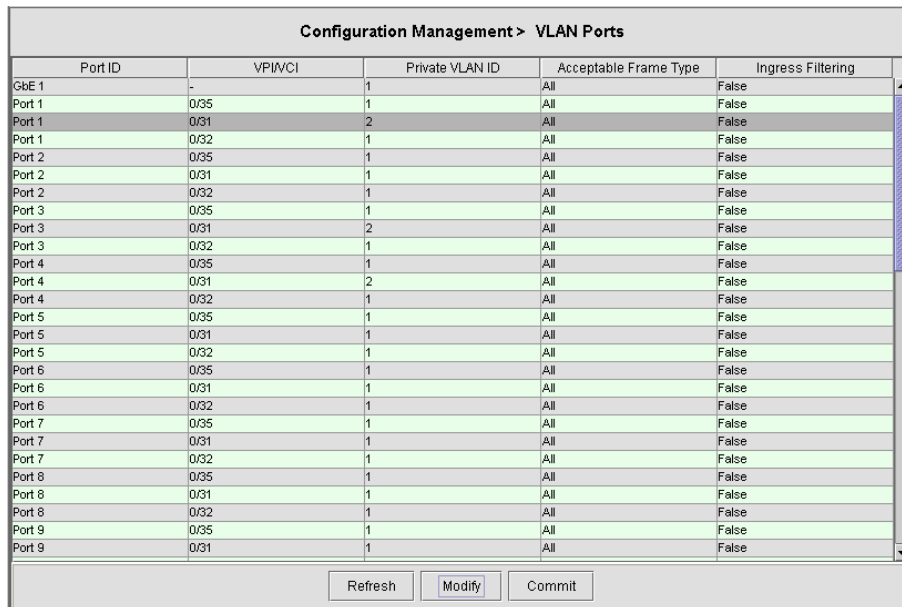
Table 4-9 Add VLAN Configuration Dialog Description

Item	Description
Static Egress Bridges	This specifies the bridge ports to be included in the VLAN. Within a port, different PVCs can be assigned to different VLAN.
Forbidden Egress Bridges	This specifies the bridge ports to be excluded in the VLAN. If a port is selected for this option, it will not be selectable for “ Static Egress Bridges ”
Untagged Egress Bridges	This specifies whether the bridge ports will be tagged or untagged. Tagged means the frame will carry its original tag or the Port VLAN ID. Untagged means the frame will not carry any tag while leaving the VLAN.
	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 4-18 VLAN Ports Management Dialog



Port ID	VPI/VCI	Private VLAN ID	Acceptable Frame Type	Ingress Filtering
GbE 1	-	1	All	False
Port 1	0/35	1	All	False
Port 1	0/31	2	All	False
Port 1	0/32	1	All	False
Port 2	0/35	1	All	False
Port 2	0/31	1	All	False
Port 2	0/32	1	All	False
Port 3	0/35	1	All	False
Port 3	0/31	2	All	False
Port 3	0/32	1	All	False
Port 4	0/35	1	All	False
Port 4	0/31	2	All	False
Port 4	0/32	1	All	False
Port 5	0/35	1	All	False
Port 5	0/31	1	All	False
Port 5	0/32	1	All	False
Port 6	0/35	1	All	False
Port 6	0/31	1	All	False
Port 6	0/32	1	All	False
Port 7	0/35	1	All	False
Port 7	0/31	1	All	False
Port 7	0/32	1	All	False
Port 8	0/35	1	All	False
Port 8	0/31	1	All	False
Port 8	0/32	1	All	False
Port 9	0/35	1	All	False
Port 9	0/31	1	All	False

Click “Modify” to modify the setting.

Figure 4-19 Modify VLAN Ports Management Dialog

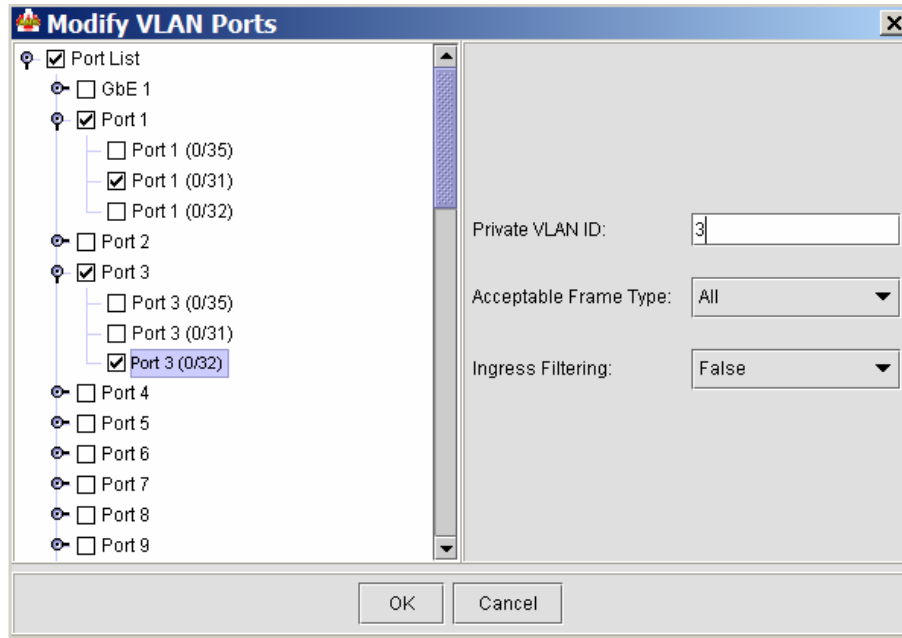


Table 4-10 VLAN Ports Management Dialog Description

Item	Description
Private VLAN ID	The VLAN ID to be assigned if untagged frames is accepted.
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.
	Press the 'OK' button to confirm the setting.

GVRP Ports Management

The GVRP (GARP (Generic Attribute Registration Protocol)VLAN Registration Protocol) 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 Layer 2 switches 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 4-20 GVRP Ports Management Dialog

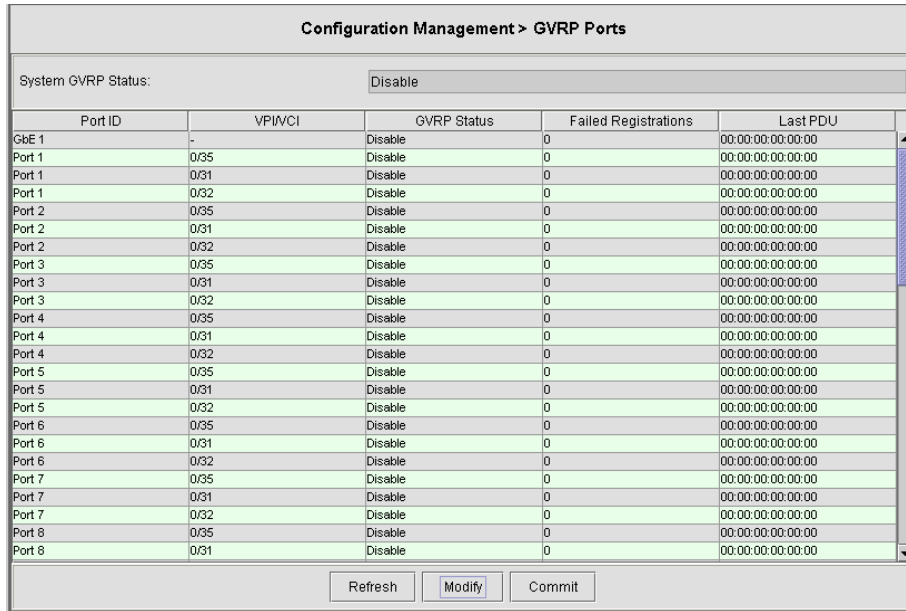


Table 4-11 GVRP Ports Management Dialog

Item	Description
System GVRP status	The administrative status to be set by operator for GVRP on the DSLAM
VPI/VCI	This specifies the ADSL or network Ethernet interface.
Bridge GVRP Status	The administrative status requested by management for GVRP on each port
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.

Click 'Modify' to modify the configuration.

Figure 4-21 Modify GVRP Status Dialog

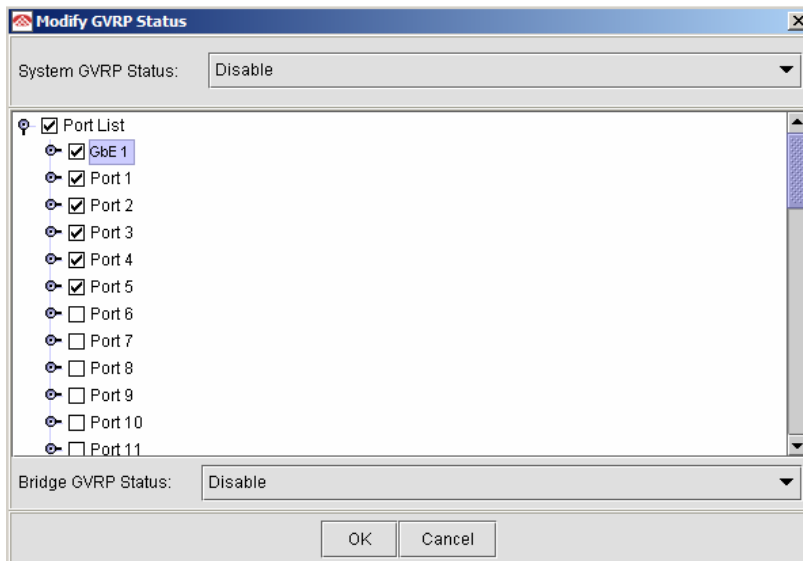


Table 4-12 Modify GVRP Status Dialog Description

Item	Description
System GVRP status	The administrative status to be set by operator for GVRP
Bridge GVRP Status	The administrative status requested by management for GVRP.
	Press the 'OK' button to confirm the setting.

4.3.6 Limit MAC Number

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

Figure 4-22 Limit MAC Number Dialog

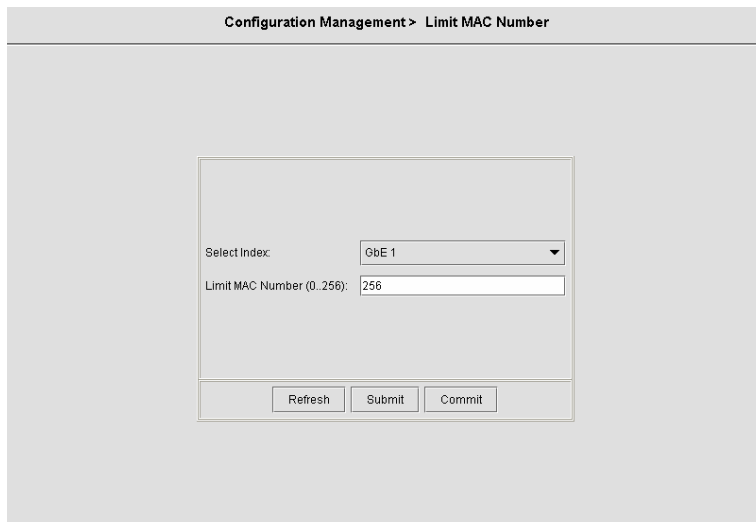


Table 4-13 shows the limit MAC number field items.

Table 4-13 Limit MAC Number Dialog Description

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.

4.3.7 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 4-23 IGMP Snooping Dialog

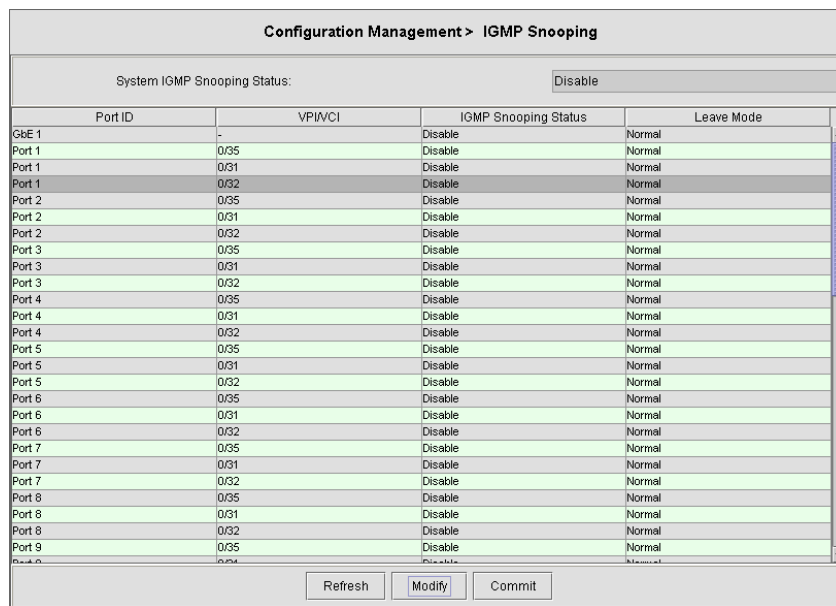


Table 4-14 IGMP Snooping Dialog Description

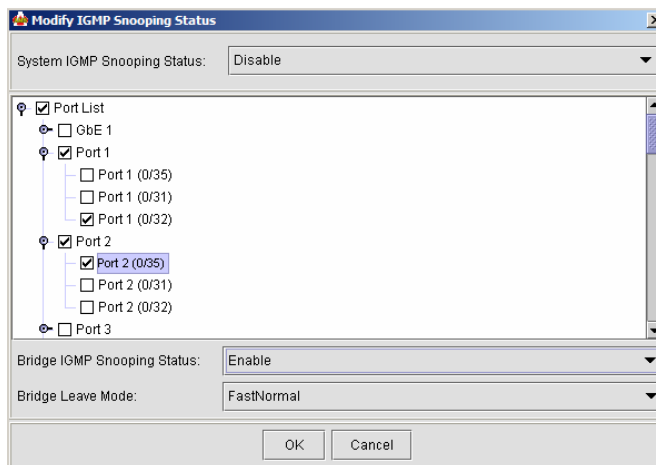
Item	Description
System IGMP Snooping Status	Specified whether or not IGMP Snooping is to be enabled in the system.
Port ID	This specifies the network port interface.
VPI/VCI	This specifies the virtual path, circuit identification for the PVC in the port.
IGMP Snooping Status	A Bridge Port, for which IGMP Snooping needs to be enabled or disabled.

Table 4-14 IGMP Snooping Dialog Description

Item	Description
Leave Mode	<p>IGMP Snooping Leave message processing mode for the port.</p> <p>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.</p> <p>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.</p> <p>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.</p>
	Press the ' Commit ' button to confirm the setting.
	Press the ' Modify ' button to change the setting.

Click '**Modify**' to change the setting of IGMP Snooping for the whole system and individual port. Figure 4-23 shows the dialog to enable/disable IGMP Snooping feature.

Figure 4-24 Modify IGMP Snooping Status Dialog



4.3.8 Spanning Tree Protocol

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

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

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

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

Figure 4-25 Spanning Tree Protocol Dialog

Table 4-15 describes the spanning tree parameters field items.

Table 4-15 Spanning Tree Protocol Dialog Description

Item	Description
System STP status	Spanning Tree Protocol to be enabled on the Bridge or not.
GbE Port STP status	This specifies the STP status of Gigabit Ethernet interface.

Table 4-15 Spanning Tree Protocol Dialog Description

Item	Description
	Press the ‘ Submit ’ button to confirm the setting.
Set Spanning Tree Protocol Status	
STP Priority	This value can determine if the IP-DSLAM will be root switch among all known switches. The switch with the highest priority (lowest numeric value) becomes the Spanning Tree root switch. MAC address (the lowest numeric value) is used to decide root switch if priority is the same. Valid values: 0 ~ 61440 in steps of 4096
Time Since Top Changed	The time elapsed since the root node of the Spanning Tree has changed. The change of the root node will cause the Spanning Tree to reconfigure.
Top Changed	The count which the root node has changed in the existing Spanning Tree.
Designated Root	The root of current Spanning Tree indicating by its MAC address.
Root Cost	The cost configured in the DSLAM contributing to the path cost leading to the root
Root Port	The port number of the port which offers the lowest cost path from this bridge to the root bridge.
Max Age	The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of seconds, when this bridge is the root of the spanning tree.
Hello Time	The value that all bridges use for HelloTime when this bridge is acting as the root.
Forward Delay	The value that all bridges use for Forward Delay when this bridge is acting as the root.
Hold Time	This time value determines the interval length during which no more than two Configuration bridge PDUs shall be transmitted by this node, in units of seconds.
Bridge Max Age	The maximum age time of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of seconds. Valid values: 6 ~ 40 (Seconds)
Bridge Hello Time	The amount of time between the transmission of Configuration BPDU (Bridge Protocol Data Units) by this node on any port when it is the root of the spanning tree or trying to become so, in units of second. Valid values: 1 ~ 30 (Seconds)
Bridge Forward Delay	This value, measured in units of seconds, controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used, when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database. Valid values: 4 ~ 30 (Seconds)
	Press the ‘ Submit ’ button to confirm the setting.

4.3.9 Bridge Configuration

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

Figure 4-26 Bridge Configuration Dialog

Table 4-16 Bridge Configuration Dialog Description

Item	Description
Aging Time	The timeout period, in seconds, for aging out dynamically learned forwarding information from CPEs. The value 0 can be configured when aging is to be stopped. Valid values: 10 ~ 1,000,000
Uplink Aging Time	The timeout period, in seconds, for aging out dynamically learned forwarding information from uplink side port. This is used only for full bridge configuration. The value 0 can be configured when aging is to be stopped. Default is set to 600 sec. Valid values: 10 ~ 1,000,000
Dnlink (Slave) Aging Time	The timeout period, in seconds, for aging out dynamically learned forwarding information learned from the downlink device. The value 0 can be configured when aging is to be stopped. Default is set to 600 sec. Valid values: 10 ~ 1,000,000
Flood Support	This is used to specify whether the unknown unicast packets are to be flooded or not. The value for this is used along with per vlan configuration for flood support to determine if flooding has to be done for unknown unicast packet.
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.

Table 4-16 Bridge Configuration Dialog Description

Item	Description
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.
Status of full Bridging Status	<p>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.</p> <ul style="list-style-type: none"> * Residential bridging, all packets from a CPE side port are sent to Net side port without doing a lookup in the forwarding table. * Restricted bridging, there is a lookup and a packet coming from a CPE port destined for another CPE port is dropped. Hence, CPE-CPE switching is not permitted. * Unrestricted bridging, all traffic is forwarded based on lookup.

4.3.10 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 4-27 DHCP Relay Configuration Dialog

Table 4-17 DHCP Relay Configuration Dialog Description

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 ‘ Submit ’ 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.
	Press the ‘ Submit ’ button to confirm the setting.

4.4 Fault

The Fault Management pages will list the events and alarms generate by the currently configuring network element.

4.4.1 List Events

The List Events submenu will list all of the events and operator can sort the events according to status, source, and date. The Events are categorized into Critical, Major, Minor, Information, Unknown.

Figure 4-28 List Events Dialog

Status	Source	Date	Message
Unknown	10.1.29.236	Mon Apr 24 11:38:41 CST 2006	Node failure. This probably means one or more interfaces
Clear	IF-10.1.29.236	Mon Apr 24 11:38:41 CST 2006	Interface clear.
Major	10.1.29.236	Mon Apr 24 11:33:42 CST 2006	Node failure. This probably means one or more interfaces
Major	IF-10.1.29.236	Mon Apr 24 11:33:41 CST 2006	Interface failure. Status poll failed.
Unknown	10.1.29.236	Mon Apr 24 10:43:32 CST 2006	Node failure. This probably means one or more interfaces
Information	10.1.29.236_EthernetPort2	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort48	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_EthernetPort1	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort46	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort47	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort45	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort44	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort43	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort42	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort41	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort40	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort39	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort38	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort37	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort36	Mon Apr 24 10:43:32 CST 2006	Object Added to Database
Information	10.1.29.236_AdslPort34	Mon Apr 24 10:43:32 CST 2006	Object Added to Database

4.4.2 List Alarms

The List Alarms submenu will list the unsolved events generated by the current network element. The operator can manually clear the events.

Figure 4-29 List Alarms Dialog

Fault Management > List Alarms

Node Alarms Total 2 From 1 To 2 Page Length 25

Status	Failure Object	Group	Owner	Date	Message
Clear	IF-10.1.29.236	10.1.29.236		Mon Apr 24 11:38:41 CST 2006	Interface clear.
Major	10.1.29.236	10.1.29.236		Mon Apr 24 11:33:42 CST 2006	Node failure. This probably mes

4.5 Performance

In the Performance menu, operator can view the ADSL line performance parameters as well as the ADSL channel performance parameters.

4.5.1 ADSL Line Performance

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

Figure 4-30 ADSL Line Performance Dialog

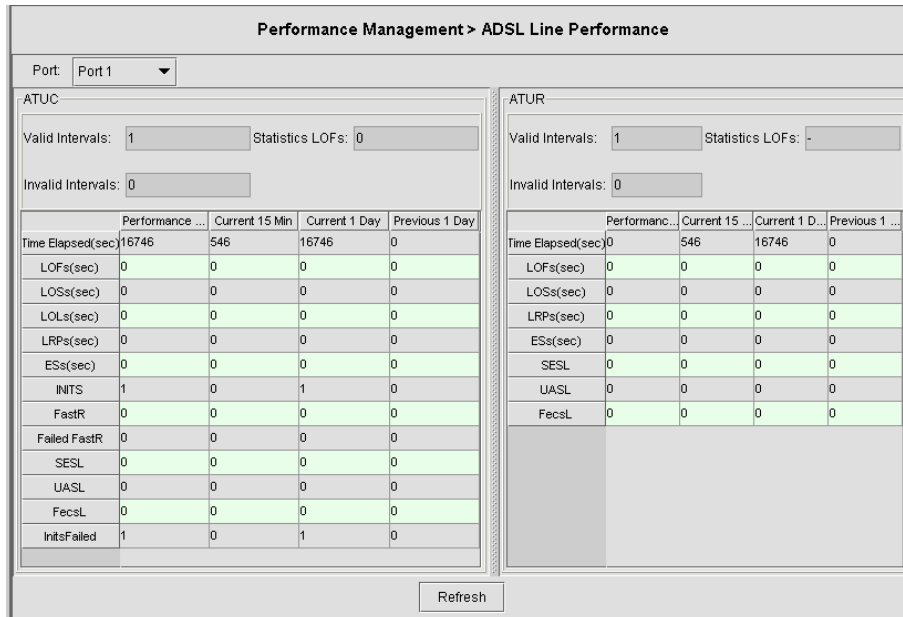


Table 4-18 Line Performance Dialog Description

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

Table 4-18 Line Performance Dialog Description

Item	Description
UAS	Unavailable Second. This specifies the second which the link is abnormal for 10 seconds.

4.5.2 Channel Performance

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

Figure 4-31 Channel Performance Dialog

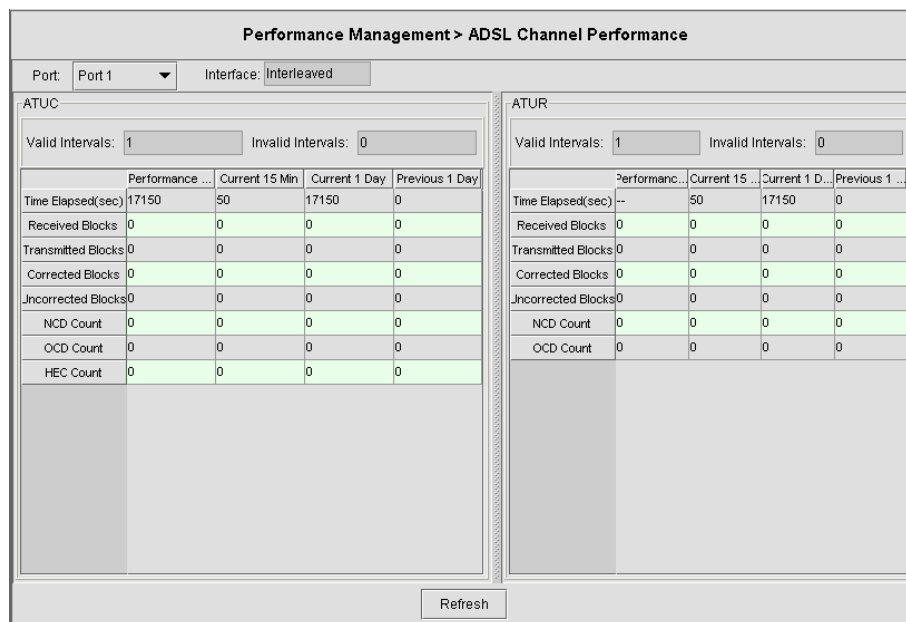


Table 4-19 Line Performance Dialog Description

Item	Description
Port selection menu	Select the ADSL port interface to be display with relative parameters.
Received Blocks	The block counts which are received.
Transmitted Blocks	The block counts which are transmitted.
Corrected Blocks	The block counts which are corrected via CRC bit.
Uncorrected Blocks	The block counts which are not recoverable.

4.5.3 Port Performance

The port performance can provide statistic on the packets counts on Unicast, Multicast, Broadcast packets as well as the total traffic volume on the ports.

Figure 4-32 Port Performance Dialog

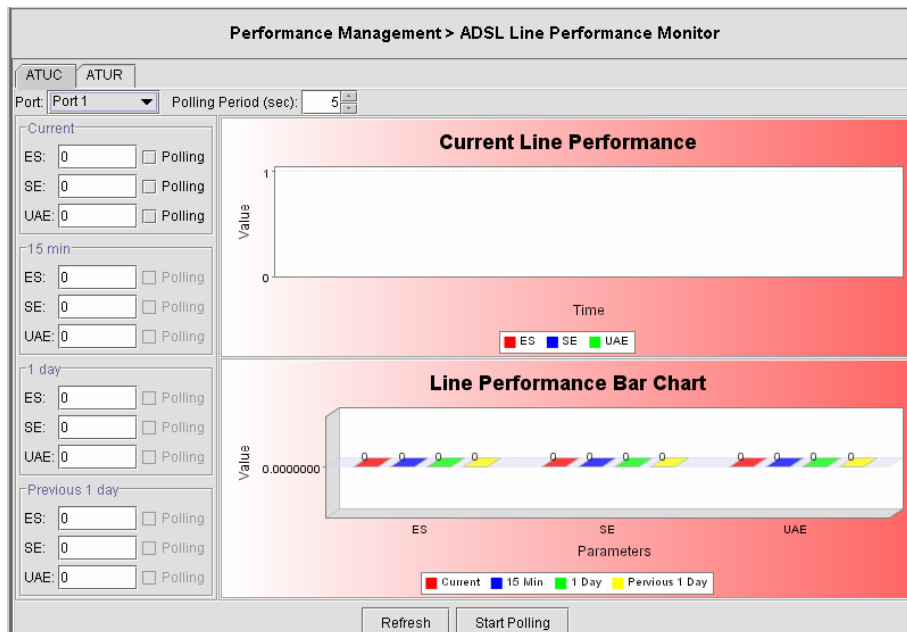
Performance Management > Port Performance										
Ethernet Port	IN					OUT				
	Octets (byte)	Unicast Pa...	Multicast Pa...	Broadcast ...	Discarded ...	Octets (byte)	Unicast Pa...	Multicast P...	Broadcast ...	Discarded ...
GbE 1	441304	230	508	2975	0	71594	199	0	1	0
Port 1	0	0	0	0	0	0	0	0	0	0
Port 2	0	0	0	0	0	0	0	0	0	0
Port 3	0	0	0	0	0	0	0	0	0	0
Port 4	0	0	0	0	0	0	0	0	0	0
Port 5	0	0	0	0	0	0	0	0	0	0
Port 6	0	0	0	0	0	0	0	0	0	0
Port 7	0	0	0	0	0	0	0	0	0	0
Port 8	0	0	0	0	0	0	0	0	0	0
Port 9	0	0	0	0	0	0	0	0	0	0
Port 10	0	0	0	0	0	0	0	0	0	0
Port 11	0	0	0	0	0	0	0	0	0	0
Port 12	0	0	0	0	0	0	0	0	0	0
Port 13	0	0	0	0	0	0	0	0	0	0
Port 14	0	0	0	0	0	0	0	0	0	0
Port 15	0	0	0	0	0	0	0	0	0	0
Port 16	0	0	0	0	0	0	0	0	0	0
Port 17	0	0	0	0	0	0	0	0	0	0
Port 18	0	0	0	0	0	0	0	0	0	0
Port 19	0	0	0	0	0	0	0	0	0	0
Port 20	0	0	0	0	0	0	0	0	0	0
Port 21	0	0	0	0	0	0	0	0	0	0
Port 22	0	0	0	0	0	0	0	0	0	0
Port 23	0	0	0	0	0	0	0	0	0	0
Port 24	0	0	0	0	0	0	0	0	0	0
Port 25	0	0	0	0	0	0	0	0	0	0

Refresh Reset

4.5.4 ADSL Line Performance Monitor

Through ADSL Line Performance Monitor, Operator can view the ES (Error Second), SE (Sever Error), and UAE (Unavailable Error) statistic on different gathering period.

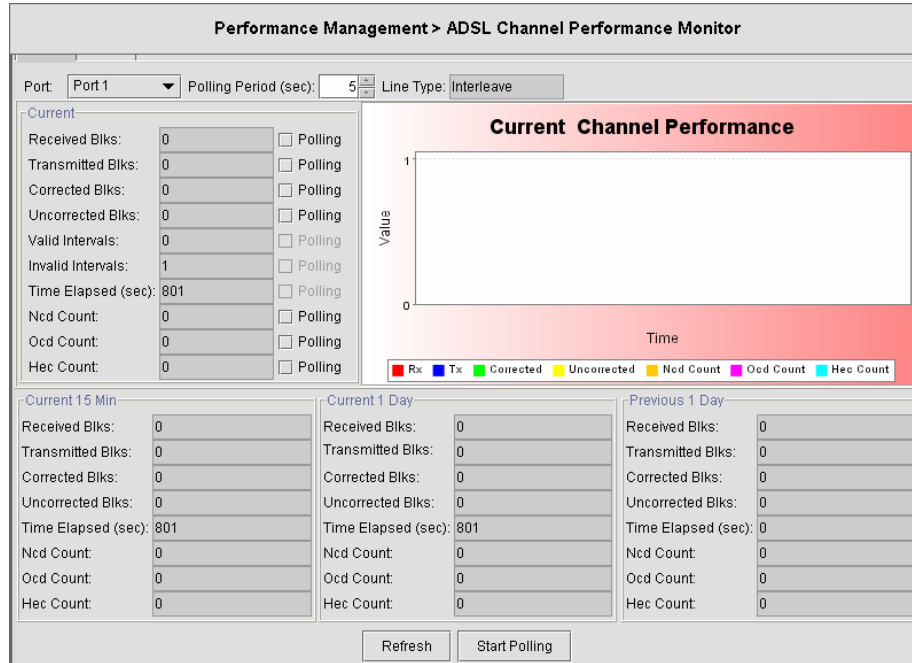
Figure 4-33 ADSL Line Performance Monitor Dialog



4.5.5 ADSL Channel Performance Monitor

Through Channel Performance Monitor option, operator can view traffic statistic on the data channel level.

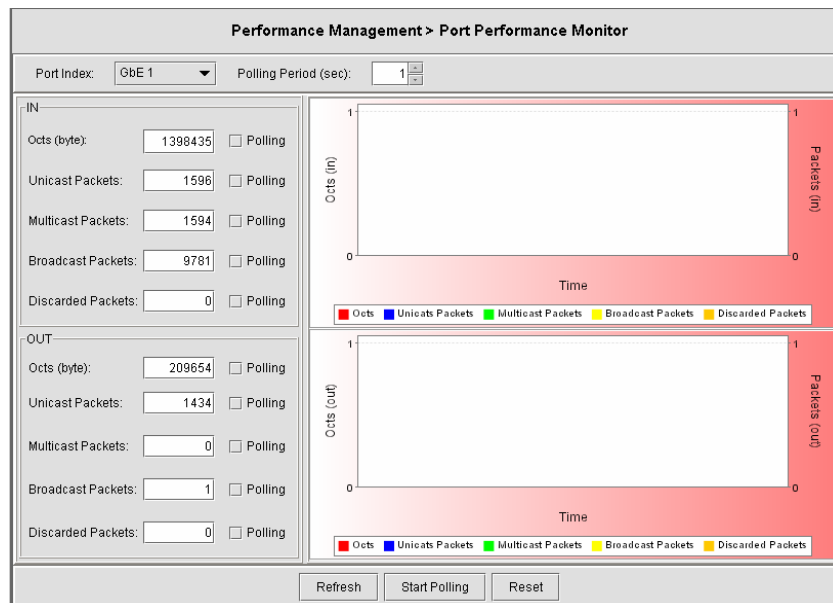
Figure 4-34 ADSL Channel Performance Monitor Dialog



4.5.6 Port Performance Monitor

The port performance can provide statistic on the packets counts on Unicast, Multicast, Broadcast packets as well as the total traffic volume on the ports.

Figure 4-35 Port Performance Monitor Dialog



4.6 Status Management

4.6.1 System Statistics

The statistics information dialog monitors current system network status. Table 4-20 describes the system statistics information field items.

Figure 4-36 System Statistics Information Dialog

The screenshot shows a web-based interface titled "Status Management > System Statistics". It contains a grid of statistics, each with a label and a text input field. At the bottom, there is an "Auto refresh count down" field and two buttons: "Refresh" and "Reset".

Statistic Label	Value
CPE unicast address count	0
Downlink unicast address count	0
Net unicast address count	256
CPE learn entry discards	0
Downlink learn entry discards	0
Net learn entry discards	13822
Learnt address conflicted with static address (times)	0
Dynamic address moved (times)	0
Unicast address lookup failed (times)	1422
Multicast address lookup failed (times)	0
Control module packets sent	43888
Control module packets received	253804
Control module packets discarded	0
PPPOE Session Look up failures	0

Auto refresh count down: 6

Refresh Reset

Table 4-20 System Statistics Information Dialog Description

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.
Packets sent to the control module count	Number of times Packets are sent to control plane
Packets received by the control module count	Number of times Packets are received sent to control plane

4.6.2 System Size Information

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

Figure 4-37 System Size Information Dialog

Status Management > System Size Information

Max ATM Port Number:	48	Max VLAN Number:	512
Max VC Number:	384	Max VLAN ID Value:	4095
Max VC Number per ATM Port:	8	Max Static UCast Entry Number:	512
Max OAM Activity Number:	10	Max Generic Filter Ingress Rule Number:	275
Max RMON Probe Number	20	Max Generic Filter Egress Rule Number:	25
Max Priority Queue Number per Ethernet port:	8	Max High Priority Generic Filter Ingress Subrules:	75
Max Priority Queue Number per EOA Interface:	4	Max High Priority Generic Filter Egress Subrules:	25
Max Multicast Group Number:	256	Max Low Priority Generic Filter Ingress Subrules:	425
Max Learned MAC Adresse Number:	4000	Max Low Priority Generic Filter Egress Subrules:	175
			Device Q-Bridge Capabilities: i/capable, c/gpvidtagging

Table 4-21 describes the system size information field items.

Table 4-21 System Size Information Dialog Description

Item	Description
Max ATM Ports	Maximum number of ATM ports
Max VCs	Maximum number of VCs possible in the system.
Max VC per Port	Maximum number of VCs possible per ATM port
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 Priority queues Number per Ethernet port	This specifies the max number of priority queues that can be configured on a bridge port created over an Ethernet interface.
Max Priority queues Number per EOA Interface	This specifies the max number of priority queues that can be configured on a bridge port created on EOA interface.
Max Multicast groups Number	Maximum number of multicast groups that are configured in the system.
Max Learned MAC addresses Number	Maximum number of MAC addresses that are learned by the system.
Max VLAN Number	Maximum number of VLANs supported.
Max VLAN ID Value	Maximum values of VLAN ID that the bridge can support.
Max static Unicast entries	Maximum number of static unicast entries.
Max generic filter ingress rules	Maximum number of generic filter ingress rules that can be created.
Max generic 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 egress subrules of high access priority	Maximum number of generic filter egress 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 low access priority	Maximum number of generic filter egress sub rules of low access priority that can be created.
Device Q-Bridge Capabilities	Device capabilities of the bridge.

4.6.3 Port Status

The port status submenu will display ATM, Channel, and DSL layer information.

Figure 4-38 Port Status Dialog

Status Management > Port Status

Port: Port 1 ▾

Interface

Type	Speed (bps)	Desired State	Operational State	Up Time
ADSL	0	Up	Down	0 hours, 0 minutes, 26 seconds.
Interleave	0	Down	Down	0 hours, 0 minutes, 0 seconds.
Fast	0	Down	Down	0 hours, 0 minutes, 0 seconds.
ATM	0	Up	Down	0 hours, 0 minutes, 26 seconds.

AAL5

AAL5 Port	Speed (bps)	Desired State	Operational State	Up Time
1	0	Up	Down	0 hours, 0 minutes, 26 seconds.

EOA

EOA Port	Speed (bps)	Desired State	Operational State	Up Time
1	0	Up	Down	0 hours, 0 minutes, 0 seconds.

Table 4-22 Port Status Dialog Description

Item	Description
Port selection menu	Select the ADSL port interface to be display with relative parameters.
Interface	These fields specify the data rate, operation state, and up time for ADSL, and ATM layer.
AAL5	These fields specify the data rate, operation state, and up time for AAL5 layer.
EOA	These fields specify the data rate, operation state, and up time for EOA layer.

4.6.4 ADSL Port Status

ADSL port status allows operator to view the port status including the operational state, cell count, transmission rate for both ATUC and ATUR, and many other variables related to the port condition.

Figure 4-39 ADSL port status Dialog

Status Management > ADSL Port Status							
Port ID	Admin State	Operational State	ATUC: Actual Transmit Rate		ATUR: Actual Transmit Rate		Actual Standard
			Interleave	Fast	Interleave	Fast	
Port 1	Up	Down	0	0	0	0	T1413
Port 2	Up	Down	0	0	0	0	T1413
Port 3	Up	Down	0	0	0	0	T1413
Port 4	Up	Down	0	0	0	0	T1413
Port 5	Up	Down	0	0	0	0	T1413
Port 6	Up	Down	0	0	0	0	T1413
Port 7	Up	Down	0	0	0	0	T1413
Port 8	Up	Down	0	0	0	0	T1413
Port 9	Up	Down	0	0	0	0	T1413
Port 10	Up	Down	0	0	0	0	T1413
Port 11	Up	Down	0	0	0	0	T1413
Port 12	Up	Down	0	0	0	0	T1413
Port 13	Up	Down	0	0	0	0	T1413
Port 14	Up	Down	0	0	0	0	T1413
Port 15	Up	Down	0	0	0	0	T1413
Port 16	Up	Down	0	0	0	0	T1413
Port 17	Up	Down	0	0	0	0	T1413
Port 18	Up	Down	0	0	0	0	T1413
Port 19	Up	Down	0	0	0	0	T1413
Port 20	Up	Down	0	0	0	0	T1413
Port 21	Up	Down	0	0	0	0	T1413
Port 22	Up	Down	0	0	0	0	T1413
Port 23	Up	Down	0	0	0	0	T1413
Port 24	Up	Down	0	0	0	0	T1413
Port 25	Up	Down	0	0	0	0	T1413
Port 26	Up	Down	0	0	0	0	T1413
Port 27	Up	Down	0	0	0	0	T1413
Port 28	Up	Down	0	0	0	0	T1413

Refresh

4.6.5 ADSL Line Status

ADSL line status allows operator to view the line status including the noise margin, status, cell count, and many other variables related to the port condition.

Figure 4-40 ADSL Line Status Dialog

Status Management > ADSL Line Status

Port: Port 1

Operational state of the ATUC: Hand Shake

Actual standard used for the connection: T1413

Number of bit errors detected during BERT: 0

Number of bit errors: 0

Line Power Management State: Idle Operation

Whether an extended or the standard upstream PSD is used: Standard

-ATUC (dB/10)

Current SNR Margin: 0

Current attenuation: 0

Current state: Loss Of Framing

Current output power: 0

-ATUR (dB/10)

Current SNR Margin: 0

Current attenuation: 0

Current state: Loss Of Framing

Current output power: 0

Refresh

4.6.6 ADSL Channel Status

The ADSL Channel status can provide information on Channel related variable. The operator can quickly review the redundancy, delay, transmission rate and block length in term of byte on the channel level.

Figure 4-41 ADSL Channel Status Dialog

Status Management > ADSL Channel Status

Port ID	ATM Status	RS Symbols	RS Redundancy	Interleave Delay (ms)	Current Tx Rate (bps)	Previous Tx Rate (bps)	CRC Block Length (byte)
Port 1	No ATM De...	0	0	0	0	0	0
Port 2	No ATM De...	0	0	0	0	0	0
Port 3	No ATM De...	0	0	0	0	0	0
Port 4	No ATM De...	0	0	0	0	0	0
Port 5	No ATM De...	0	0	0	0	0	0
Port 6	No ATM De...	0	0	0	0	0	0
Port 7	No ATM De...	0	0	0	0	0	0
Port 8	No ATM De...	0	0	0	0	0	0
Port 9	No ATM De...	0	0	0	0	0	0
Port 10	No ATM De...	0	0	0	0	0	0
Port 11	No ATM De...	0	0	0	0	0	0
Port 12	No ATM De...	0	0	0	0	0	0
Port 13	No ATM De...	0	0	0	0	0	0
Port 14	No ATM De...	0	0	0	0	0	0
Port 15	No ATM De...	0	0	0	0	0	0
Port 16	No ATM De...	0	0	0	0	0	0
Port 17	No ATM De...	0	0	0	0	0	0
Port 18	No ATM De...	0	0	0	0	0	0
Port 19	No ATM De...	0	0	0	0	0	0
Port 20	No ATM De...	0	0	0	0	0	0
Port 21	No ATM De...	0	0	0	0	0	0
Port 22	No ATM De...	0	0	0	0	0	0
Port 23	No ATM De...	0	0	0	0	0	0
Port 24	No ATM De...	0	0	0	0	0	0
Port 25	No ATM De...	0	0	0	0	0	0

Refresh

4.6.7 Current VLAN

The Current VLAN submenu displays the VLAN information on the system.

Figure 4-42 Current VLAN Dialog

Status Management > Current VLAN

VLAN ID	Status
1	Other
2	Permanent
3	Permanent

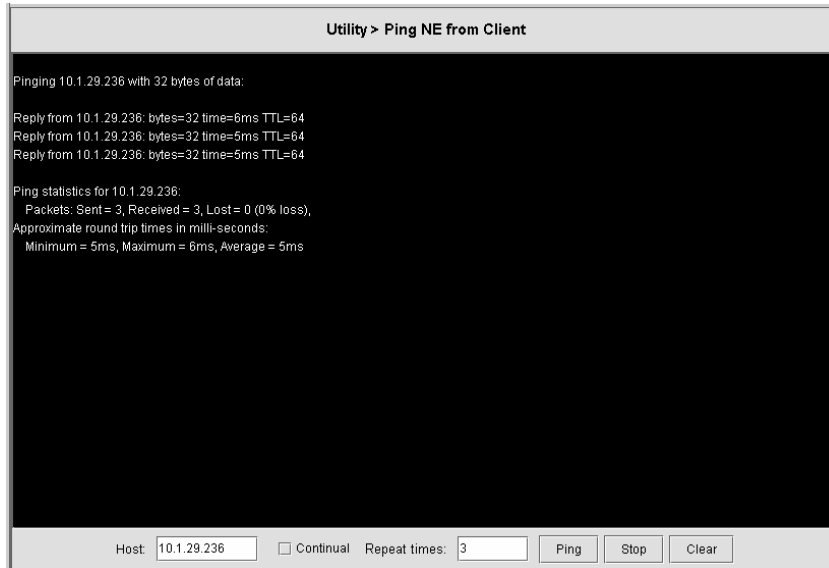
Refresh View Details

4.7 Utility

4.7.1 Ping NE from Client

The Ping command can be used to verify the link availability between NE and the AMS client.

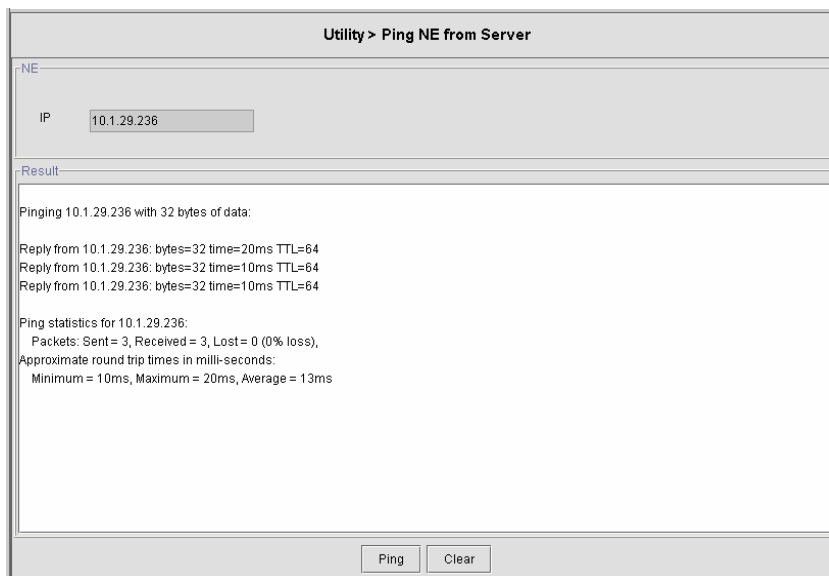
Figure 4-43 Ping NE from Client Dialog



4.7.2 Ping NE from Server

The Ping command can be used to verify the link availability between NE and the AMS server.

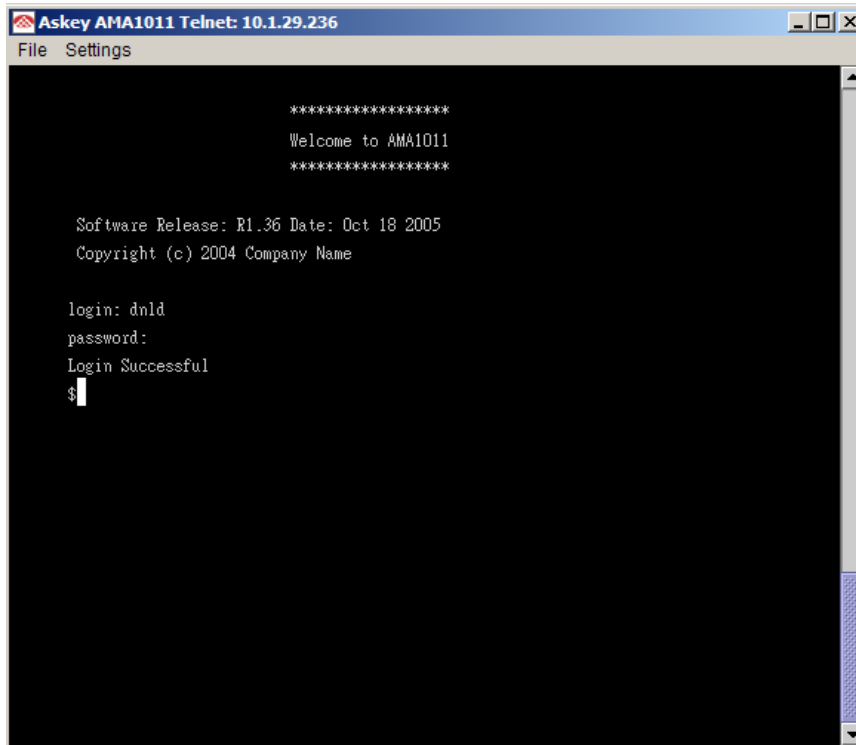
Figure 4-44 Ping NE from Server Dialog



4.7.3 Telnet from Client

Telnet to the NE from Client will start a CLI environment to configure the NE.

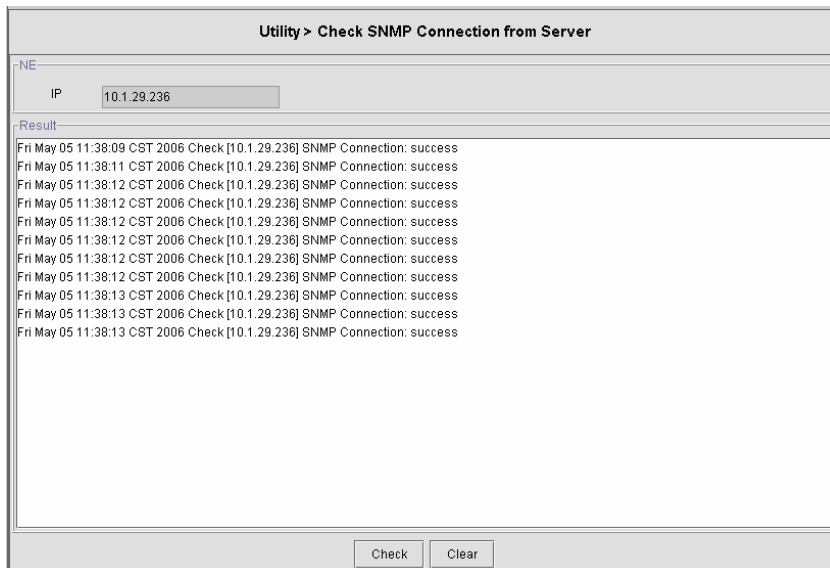
Figure 4-45 Telnet from client Dialog



4.7.4 Check SNMP connection from Server

This function can allow the AMS server to check the SNMP connection.

Figure 4-46 Check SNMP Connection from Server Dialog



4.8 Security

4.8.1 User Name and Password

To allow more operators to administrate the IP-DSLAM, additional user account can be added. Two privilege levels can be chosen: Super User and User. Super User has the privilege to modify system configuration but User can only view system status and configuration without alteration. Figure 4-47 shows the user name and password dialog.

Figure 4-47 User Name and Password Dialog

Security > User Name & Password		
User Name	Password	Privilege
dntd	*****	Super User

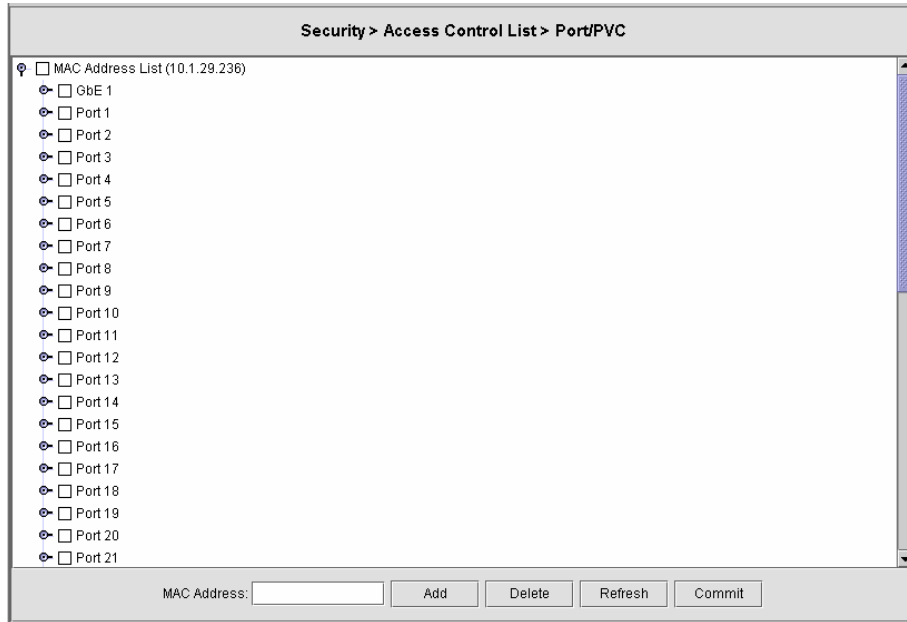
Refresh Add Delete Commit

4.8.2 Access Control List

Port/PVC

The per port access control list allow the MAC addresses to entry the system. Figure 4-48 shows the Access Control List for Port/PVC.

Figure 4-48 Port/PVC Access Control List 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 4-23 Port/PVC Access Control List Dialog Description

Item	Description
Port	Select the ADSL port interface to be display with relative parameters.
MAC Address	This specifies MAC address to be allowed for the port, pvi, pci pair.

Global

The global access control list denies the MAC addresses pass-through the system at all port interface. Figure 4-49 shows the Global Access Control List.

Figure 4-49 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 4-24 Global Access Control List Configuration Dialog Description

Item	Description
MAC Address	Source MAC address to be dropped

4.8.3 Filter Configuration

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

Filter Rule

Filter Rule Dialog shows the created filter rules and allows operator to create new rules. Figure 4-50 shows the Filter Rule Dialog.

Figure 4-50 Filter Rule Dialog

Security > Filter Rule								
Rule ID	Description	Action	Set Priority	Status	Direction	Packet Type	Statistics Status	Hit Statistics
2	no illegal	drop	--	disable	in	UniCast	enable	--
3	legal	allow	--	disable	in	UniCast	enable	--

Refresh Add Delete Detail

Table 4-25 Filter Rule Dialog Description

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).

Click 'Add' to add new Filter Rule. Figure 4-51 shows the dialog of adding Filter Rule.

Figure 4-51 Add Filter Rule Dialog

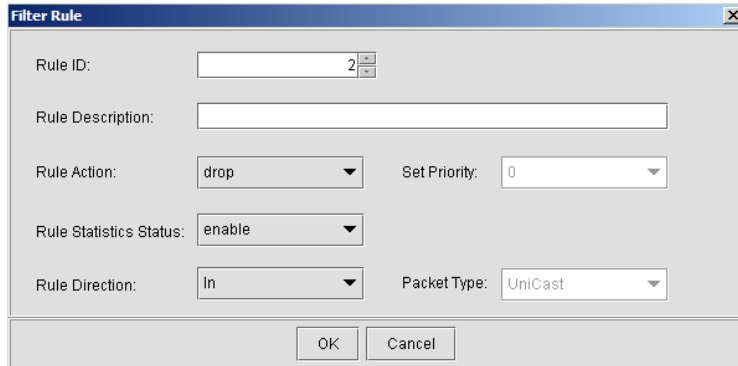


Table 4-26 Add Filter Rule Dialog Description

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

Filter Sub Rule allows operator to add Ethernet and IP sub rules as a subsidiary rule or Filter Rule. Figure 4-52 shows the dialog of adding Filter Sub Rule.

Figure 4-52 Filter Sub Rule Dialog

Rule ID	Sub Rule ID	Type	Description
2	1	Ethernet	SA any , DA any , VLAN ID equal: 2 , P...
2	4	IP	SA equal: 2.3.4.5 , DA in range 3.4.5.6 ...

Table 4-27 Filter Sub Rule Dialog Description

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 4-53 and Figure 4-54 show the dialogs to add Ethernet and IP sub rule.

Figure 4-53 Add Ethernet Sub Rule Dialog

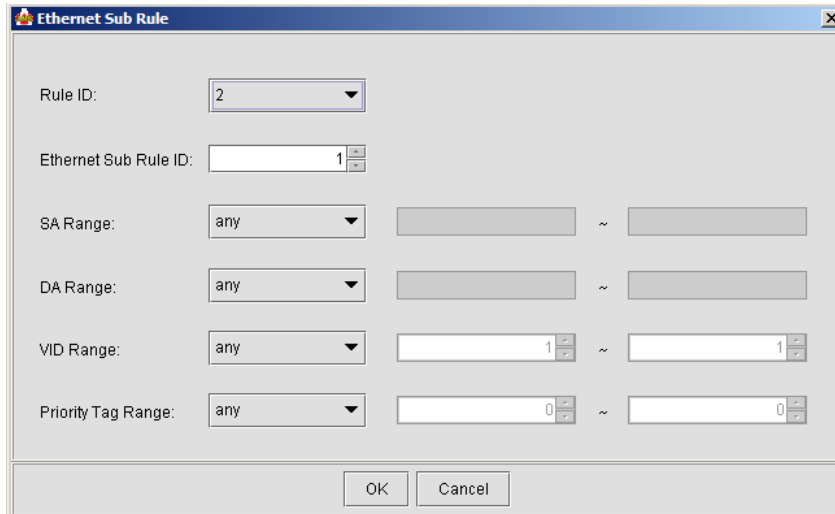


Figure 4-54 Add IP Sub Rule Dialog

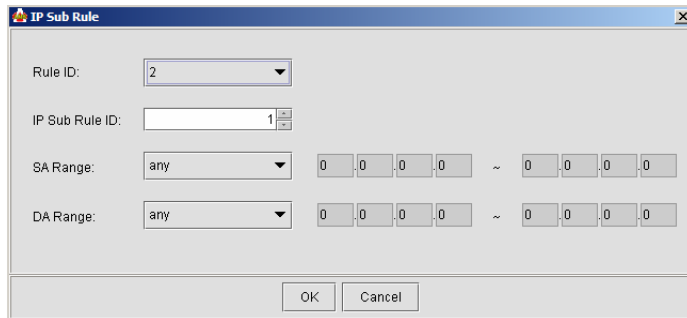


Table 4-28 Ethernet/IP Sub Rule Dialog Description

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'.

4.8.4 Filter Wizard

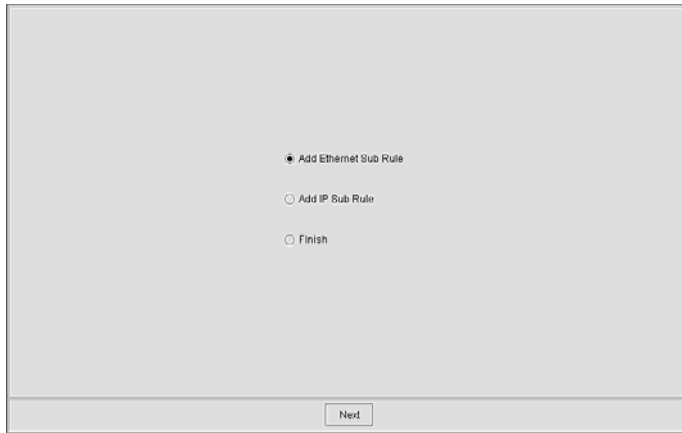
Filter Wizard can guide administrator to set up rules and sub rule for the filter.

Figure 4-55 Filter Wizard Dialog

Table 4-29 Filter Wizard Add Rule Dialog Description

Item	Description
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]
Priority	Only Applicable when setting priority is involved.
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).
Packet Type	Only Applicable when Rule Direction is Out
Next	Click ' Next ' to advance to ' Add Rule ' step

Figure 4-56 Filter Wizard Select Sub Rule Dialog



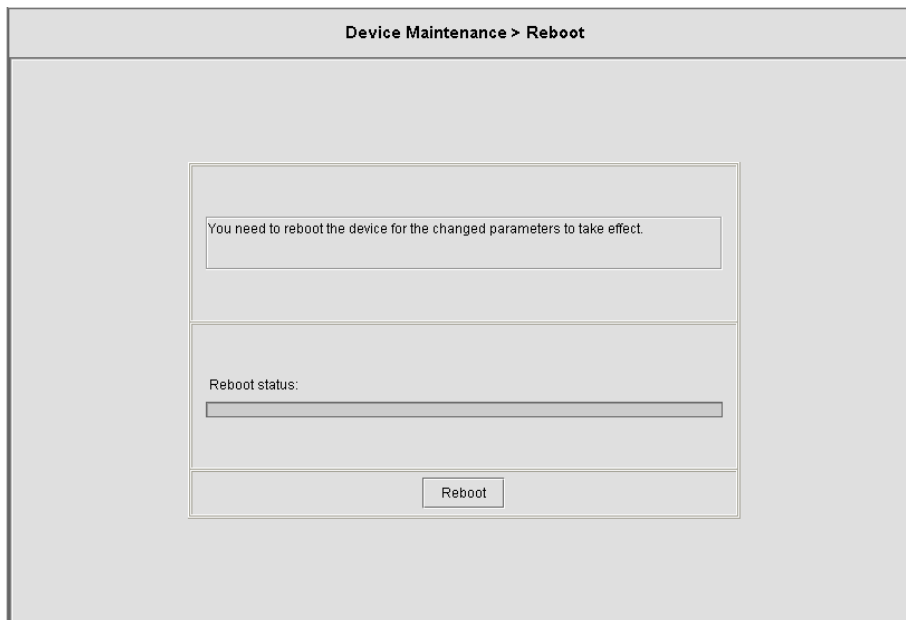
Select ‘Add Ethernet Sub Rule’, ‘Add IP Sub Rule’, or “Finish” to configure the subsequent sub rule for Ethernet or IP interface. Figure 4-53 and Figure 4-54 show the dialogs for add Ethernet and IP sub rule.

4.9 Maintenance

4.9.1 Reboot System

Reboot system (restart) takes around 90 seconds to accomplish. Figure 4-57 shows the System Reboot Dialog.

Figure 4-57 System Reboot Dialog



4.9.2 Commit

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 4-58 shows the System Commit Dialog.

Figure 4-58 System Commit Dialog



Commit action takes around 20 seconds to accomplish.

4.9.3 Restore Factory Configuration

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

Figure 4-59 Restore Factory Configuration Dialog



The restore factory default parameters are list in Table 4-30.

Table 4-30 DAS3 Series System Factory Default Parameters

Item	Description
ADSL Layer	
VPCI (VPI/VCI)	0/35 for each ADSL port interface.
Encapsulation	LLCMUX
Standard	ADSL2+
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	None IP, Downlink
Management	
SNMP community	public (re-write privilege)
SNMP host ip	192.168.1.2
Telnet Username / Password	dnld / dnld

4.9.4 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 4-60 shows the ATM OAM Test Dialog.

Figure 4-60 ATM OAM Test Dialog

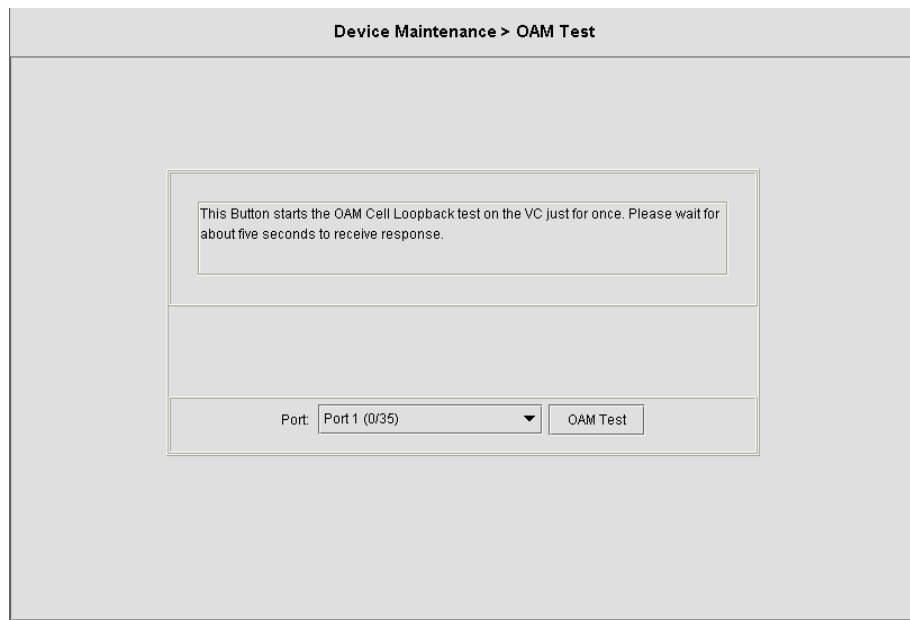


Table 4-31 describes the OAM test field items.

Table 4-31 ATM OAM Test Dialog Description

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

4.9.5 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).

There are two formulas provided to illustrate the communication quality. **QLN(f)** can be used for analyzing crosstalk or RF interference, e.g., spikes in a plot of this data would indicate interferers. **H(f)** is the frequency response of the channel, i.e., amplitude magnification and phase shift at each frequency point, which can be used for analyzing the physical copper loop condition, e.g., determining line quality and presence of bridge taps. Two formats for the channel characteristics are defined:

- **Hlin(f)**: a format providing complex values in linear scale
- **Hlog(f)**: a format providing magnitude values in a logarithmic scale

Figure 4-61 ADSL2 DELT Dialog

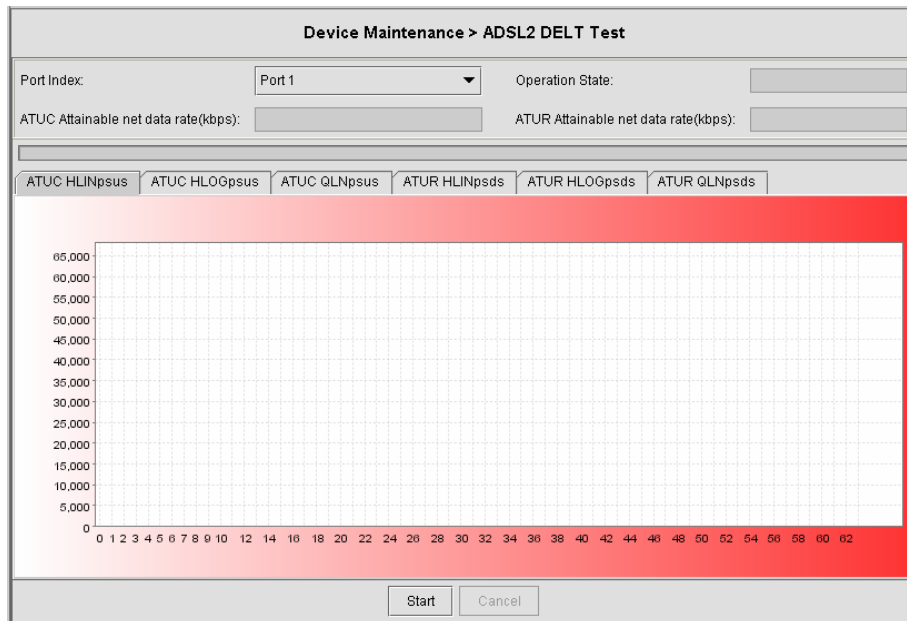


Table 4-32 ADSL 2 DELT Dialog Description

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). Then, in the background ATU will be trained to data mode. Here is the state flow: delt → handshake → discovery → Training → data
ATUC Attainable net data rate	Indicates the maximum currently attainable data rate by the ATU. This value will be equal to, or greater than the current line rate. (Downstream)
ATUR Attainable net data rate	Indicates the maximum currently attainable data rate by the ATU. This value will be equal to, or greater than the current line rate. (upstream)
Upstream HLIN	The DELT-related parameter that provides an array of complex downstream Hlin (f) values in linear scale. (Not available for ADSL and ADSL2plus)

Table 4-32 ADSL 2 DELT Dialog Description

Item	Description
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)

4.9.6 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 4-62 SELT Test Dialog

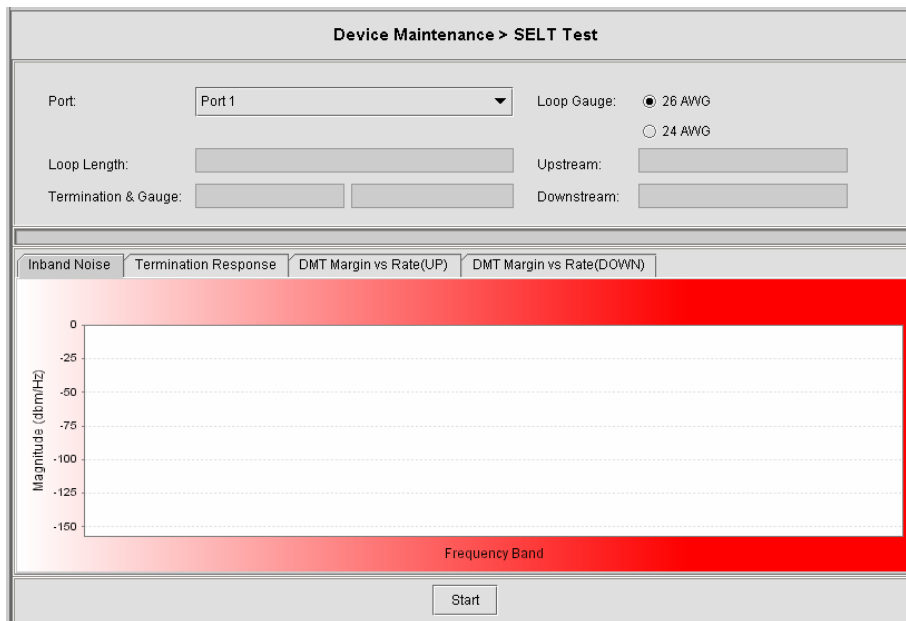


Table 4-33 SELT Test Dialog Description

Item	Description
Port selection menu	Please select port from pull down menu
Value	Display various field obtains during SELT test.
Loop Gauge	Allow the SELT to be performed on different Gauge of Loop.
Loop Length	<p>The Length of the loop from IP-DSLAM to the user end of Loop. The loop length parameter provides the length, measured in feet, of the loop.</p> <p>SELT can reliably estimate loop lengths up to 10 kft, without the presence of bridged taps. If the analysis engine determines that the loop length exceeds 10 kft, an estimation of 0 ft will be returned, indicating the result as invalid.</p> <p>In the presence of bridged taps, the loop estimation results, and subsequent rate estimations, are not reliable.</p>
Termination & Gauge	<p>This parameter indicates whether the loop is an open or short circuit.</p> <p>Note that for the Loop Termination test, single ended loop testing will only gives accurate information if the remote side is un-terminated (open or short). If the loop is off hook, terminated with a DSL modem or if there are microfilters or inline splitters present, the results will be invalid. Therefore, the Loop Termination test may be considered only a pre-deployment test.</p>
Upstream / Downstream	This field indicates the Upstream/Downstream capability.
Inband Noise Diagram	This diagram indicates the noise level at the frequency spectrum.
Termination Response Diagram	This parameter provides 180 values that indicate signal termination response magnitude from 0 to 18 kft in 100 ft increments. The absolute maximum or peak in this graph corresponds to loop length or the location of the first open/short. Local maxima may correspond to other open/shorts or discontinuities in the loop.
DMT Margin vs. Rate	Rate vs. margin, which is also referred to as SNR, specifies the sum of the coding gain plus operation margin.
Special Note	<ol style="list-style-type: none"> 1. When applying SELT test, please do not connect the modem to the CPE end of the wire. 2. When the loop is longer than 10kft, the result will be 0 ft. 3. When the loop is connecting to a telephone, the loop termination is shown as open, and loop length estimate will be correct.

4.9.7 DSL Bin Information

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

Figure 4-63 DSL Bin Information Dialog

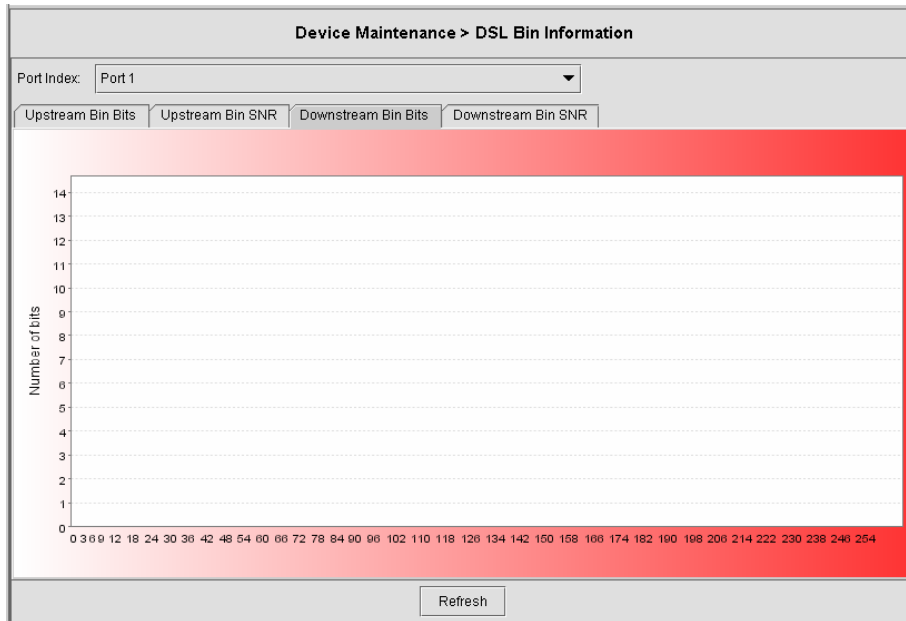


Table 4-34 describes the bin allocation tap items.

Table 4-34 DSL Bin Information Dialog Description

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 31 st element, which contains the number bits for bin 31. (upstream)
Upstream Bin SNR	The DELT-related parameter that provides an array of real downstream SNR (f) values in dB (Not available for ADSL and ADSL2plus)
Downstream Bin Bits	Number of upstream bits/ bin for the bin indexed by this element of the string. The 0th element contains the number of bits per bin for 0, through the 31 st 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)

Chapter 5 Security Management Functions

This chapter provides a general security management overview and features of AMS. It contains concepts used in the network and service management for the AMS Client.

5.1 Security Management General Functions

Security management is used to provide security mechanisms to make sure secure access to the AMS and the Network, it protects resources and controlling the authorization within the AMS. To provide the system from:

- Unauthorized access to any internal information
- Modification of information
- Disturbance of the functionality

Security feature of AMS assured in every management facility (by the type of implementation), that the security in given on application level, it does not provide globe access in any kind to bypass on operation system.

The security management of AMS configures the operator's managing operations into Network Administrator, Network Manager, or Operator to assure the system security. According to each operating class, the menus provide administrator to re-designed and set the security class flexibly base upon operating environment. All operator password management and operating history, and access history are managed to provide function for searching at corresponding history when required.

Registration and Management Function of Operator

Provides function for registering the actual AMS user with log-in and password (password change allow only for administrator group user to do so) facilities, and assigning the operating class for ensuring appropriate authority to multiple users.

It allow only System Administrator to assign new category (group) of user define as well as create, delete, and modify the users.

Menu Access Authority Setup Function

The menu access authority function allow access in each menu according to their operating class on each of the AMS account user, The AMS manages this by dividing into several operating classes, such as Administrator, Manager, and User. Menu setup can be performed according to each operating class.

User Operation Log Management Function

The operation logging and storing of all security-relevant activities refers to the administrator that allow to tracing every used functions list of corresponding user.

Connection Status Search Function

Displays the status of the account user currently connected to the AMS Server. The AMS Server enables multi Client connection.

Connection Release Function

This function provide administrator to forcefully release the connection of the currently on-line user. After the force connection release, the corresponding operator with AMS connection session will be terminating.

Multiple Level Securities

AMS provides security management function of account user in multiple security levels, operator with different identify provide it own access right, access right are configurable by Administrator class level.

Hierarchic Level Securities

AMS has ability to perform securities of account user in hierarchic level base up on there own location; this provides access right that has to be configurable about topological and function restrictions.

5.2 Security Management General Features

Security management of AMS is architecture and design proposed with incorporate feature to ensure and procure the security of the AMS.

The AMS can create user account with proper privilege, this is the most important task of the system administration, without a valid account, authorization control and hacker attacks will post a big threat of the network security.

The features of performance management functions include the following:

- Support AMS Client, AMS Server, and database security by login username and password
- Without any delay and effect other working process of AMS when it login to server
- Support multiple account user working simultaneously
- Support different categories (groups) of user accounts
- Allowed administrator to add, remove, and modify user authority.
- Support user profile
- Support access right for all user categories
- Support audit trail on all user categories

5.3 Login and Logout

AMS Client provides on-line multiple-user security login to prevent unauthorized account to access AMS network.

Figure 5-1 Login Window



The AMS follow the operator's attribute to given their right privileges while login.

5.4 Viewing System User Online List

AMS provide observing and search function of online account operators.

AMS system has ability to display all operator access to the AMS Server. Security management also allow operator to add, remove, and modify operator account.

The user description can also be memo in the comment column, which can be the, full name, telephone number, division, address, NE function menu controlled, and NE location controlled.

AMS has design in Location topological of layer structure; the upper layer location is able to perform all the functions available to the lower layer.

5.5 Operation Privilege

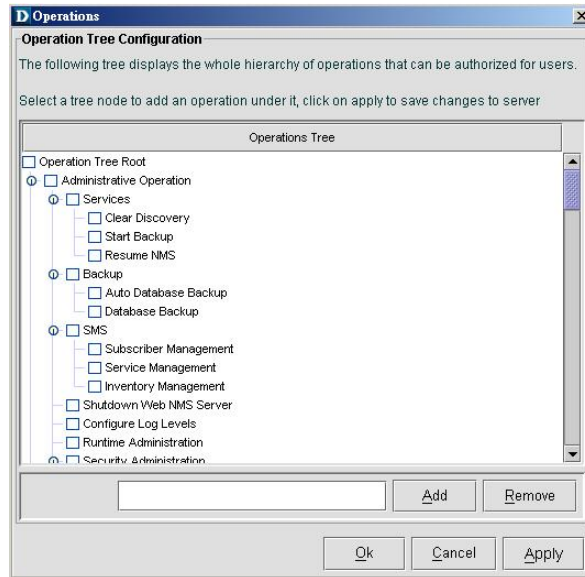
AMS provide function to ensure that only authorized operator are allowed to access all or certain part of management system, several level of access right are provide that ensure that authorized operators are given access to the facilities relevant to there job function.

AMS system has ability to assign the operator in different categories (group), the default known as “Admin” and “User”, the privilege of each group can be manually defined.

- There is no limit to the number of AMS operator account that may be registered
- There is no limit to the number of AMS operator group that may be created
- The uppermost class is the Administrator, who can access all the menus of AMS in default

AMS provides access right of an individual by an Administrator who ahs only right to given the appropriate authorization.

Figure 5-2 Operator Access Control List Window



Access Control authority only be allowed by the Administrator privileges

5.6 Security Level Application

The AMS system will automatically log the operator behavior. This will allowed operator to trace the major activities of the specify user.

After the query request, the system will list in chronological order all user records that will display the user login location, operation and operation elapsed time as shown in Figure 5-3 below.

Figure 5-3 Operator Operation Log List Window

User Name	Operation Name	Audit Time	Status	Category	Audited Object
root	Authentication : 10.12.1.56	2007-01-03 17:31:44.984	SUCCESS	Authentication	
root	Execute Task	2007-01-03 17:48:08.781	SUCCESS	Configuration	10.12.3.97
root	Get Alert Details	2007-01-03 18:14:34.265	SUCCESS	Fault	rootlocation
root	Get Alert Annotation	2007-01-03 18:14:34.625	SUCCESS	Fault	rootlocation
root	Get Event Filters	2007-01-03 18:16:01.453	SUCCESS	DEFAULT	
root	Get Event Filters	2007-01-03 18:16:01.546	SUCCESS	DEFAULT	
root	Set Event Filters	2007-01-03 18:16:22.218	SUCCESS	DEFAULT	
root	Set Event Filters	2007-01-03 18:16:22.421	SUCCESS	DEFAULT	
root	Execute Task	2007-01-03 18:23:51.265	SUCCESS	Configuration	10.12.3.97
root	Execute Task	2007-01-03 18:23:51.656	SUCCESS	Configuration	10.12.3.97

The AMS security management trail function include following item:

- Date and Time
- Operation activities
- NE related to the activity
- Operator Name
- Operation category
- Operation audited object

Chapter 6 Subscriber and Service Management Functions

The subscriber management is used to manage subscriber information that uses the xDSL service. Operators can manage it in per port base, all information were stored in AMS Server database and provided in a table form. Export in text format is support.

6.1 Service Management General Function

General functions of service management are described as following:

Subscriber Registration and Management Function

Provides function for registering the subscriber information of subscriber port interface.

Service Ordering and Provisioning

AMS provide service ordering and provisioning in service level, this will allow operator to manage their service to the subscriber under port base.

Service Administration and Assurance

Administration allow operator to activate or de-activation the afford service to subscriber under port base.

6.2 Subscriber Management General Functions

General functions of subscriber management are described as following:

Subscriber Search Function

Search function for operator to find out the subscriber locating, it provide single NE search or entire system search base on subscriber ID or subscriber name, the sub-string search is support.

The list table allow to exporting to ASCII format as well as MS Word.

Figure 6-1 Subscriber Management List Table

The screenshot shows a web-based interface for managing subscribers. The search criteria are as follows:

- ID: (empty text box)
- Name: (empty text box)
- Tel: (empty text box)
- Location: rootlocation_Taiwan_YangMei (dropdown)
- NE: DAS4192 (dropdown)
- Shelf: 1 (dropdown)
- Slot: 1 (dropdown)
- Port: 1 (dropdown)
- Subscriber:
- Ordering:

The table below the search form has the following columns:

ID	Name	Telephone	Location	NE	NE IP Addr...	Shelf	Slot	Port	Service Type	Admin Status	Link Status

At the bottom of the window, there are buttons for: Add, Modify, Delete, Query, Service, Export, and Close.

Cross Reference of xDSL Setting Inquiry

The xDSL setting information can be easy to figure out with subscriber management function, to enhance the operator configuring and troubleshooting.

6.3 Creating of Subscriber Service Information

The subscriber data can be store and retrieve from the database of AMS, it allow operator to add / modify / delete the service type and general subscriber information in order to trace in the future.

Figure 6-2 Subscriber Data Window

6.4 Service Management General Function

The service management provides a “Provision”, “Administrative”, and “Assurance” function control over xDSL port base, the service management control panel helps operator to quickly handle the subscriber port interface and it’s relative service information.

Figure 6-3 Service Management Control Panel

Chapter 7 General System Management Functions

This chapter provides a general system management overview and features of AMS. It contains concepts used in the network and system management for the AMS Client and AMS Server.

The AMS performs management function of server registration; this includes the SNMP polling period, topology appearance setting, database log management, auto backup period, and NE auto discovery.

7.1 AMS Client Options

Client options covers the communication interval between AMS Server and AMS Client, it allowed operator to manage the reacting time and topology functions.

The Alarm Warning feature assist operator in vision and hearing from AMS when alarm arise, the AMS is support to indicated with colors for different status by GUI interface, any addition and deletion of element or plug-in unit of NE will be automatically detected and reflected in GUI interface.

The Map function provides property of Topology Map boundary and pattern of different Locations.

7.2 System Server Management

AMS server periodically checks the status of all NEs that are registered. This continuously monitors the connection status with NE, and depicts any failure state of the node in the displayed managed Network immediately, and for auto backup, inquires deal from the NE to store in the database, to provide functions for information synchronization with NE and for backup when fault occurs.

This function provides the SNMP polling option, alarm and PM log file size, periodical auto backup feature, Alarm notification setting, and Northbound connection property.

This page is leave in blank for note or memo use

Appendix A Database Dimension and Handle Time

AMS database has handled four categories of NE's information, Configuration, fault, performance, and security, the dimension of each category is describing as follow.

The below example is taken approximate 300 K subscribers in single database, calculation within 30 days of alarm history, 7 days of performance monitor information, and 20 concurrent operator's log file for 2 months.

Configuration Management / Subscriber Service Management

Dimension of PVC to VLAN mapping is 100 bytes, 300 K subscribers is around 30 MB in total.
Dimension of xDSL profile record is 100 bytes, 300 K subscribers is around 30 MB in total.

Other data regarding to configuration management and subscriber service management is around 20 MB.

Total HD space required of CM is taken about 80 MB.

The response times taken for retrieve CM information are around 10 sec. under above condition.

Fault Management

Assume NE generates one alarm from xDSL interface per day, the dimension of single alarm is 180 bytes, and for 300 K subscribers is around 54 MB in total.

Alarm generate up to one month takes around 54 MB times 30 day, the outcome is 1.62 GB in total.

The response time for retrieve history alarm is less then 10 sec.

The response time for retrieve current alarm is less then 3 sec.

Performance Management

Assume only 10% of PM information been visited by server and keep in 7 days, each PM is in 60 bytes, for 300 K subscribers is taken around 1.3 GB (300 K x 10% x 60 x 7 x 96)

The response time for retrieve PM table is less then 15 sec.

Security Management

Dimension of one record is 120 bytes, assume 3000 records generate per days, the total add up dimension for 20 user in 2 month is approximate 140 MB.

Total database HD space required for the above circumstance is approximate 3 GB.

The response time for add NE/Operator is less then 5 sec.

This page is leave in blank for note or memo use

Appendix B Abbreviations and Acronyms

The abbreviations and acronyms used in this document.

Table B-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
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
xDSL	ADSL/VDSL