IPDSLAM Element Management System Operational Manual

Copyright Notice

Trademark Acknowledgment

Revision Log

Date	Version	Author	Reviewer	Remark
2005/1/20	V1.0.0	James	Jenny	Creation for EMS V1.0.0 RC1
2005/3/28	V1.0.1	James	Jenny	EMS V1.0.0 RC2
2005/5/5	V1.0.2	James	Jenny, Eric	EMS V1.0.0 RC3,RC4
2005/5/15	V1.0.3	James	Jenny, Eric	EMS V1.0.0 RC5
2005/6/2	V1.0.4	Eric	Jenny, Eric	EMS V1.0.0 RC6

Table of Contents

List of Figures

Preface

Target Audience

This guide is intended for users, administrators and technicians responsible for installing, configuring, operating and managing an IPDSLAM device.

Notes, Tips and Warnings

This guide includes various *Notes, Tips*, and *Warnings*, which are highlighted with graphics to indicate important information.

Examples of the standard graphics used to mark this information are as follows:

Notes contain "for your information" text that corresponds to a topic.

Tips offer helpful hints and time-saving suggestions about using features.

Warnings identify essential steps, actions, or system messages that should not be ignored.

Acronyms

Term	Description
ATUC	modem at near (Central) end of line
ATUR	modem at Remote end of line

Chapter 1

IPDSLAM System Description

IPDSLAM Application Description

IP-DSLAM, which is equipped with 24 ADSL ports, is designed for ISP (Internet Service Provider) to implement bandwidth management for multiple subscribers. As IP-DSLAM supports high upstream and downstream bit-rates performance, therefore, IP-DSLAM is being deployed primarily for business customers to replace expensive leased line.

IP-DSLAM is not only equipped with a console port being used for local management, but also provides excellent capabilities of SNMP, Telnet for remote management. In particular, IP-DSLAM can be easily configured by EMS. The EMS system covers topology, configuration, deployment, security, alarm management and backed storage. Moreover, with the solution of port-based and tag-based VLAN, IP-DSLAM can isolate traffic between different users and thus provides improved security.

The compact design of IP-DSLAM is composed of three parts. One is ADSL 24-port with built-in POTS splitters connected to ADSL modems, the second one is Voice module connected to ISP, and the last one is the uplink port module to layer2/3 switch or a broadband router through Ethernet port.
IP-DSLAM provides the feasibility to support multiple applications and is depicted in Figure 1-1.

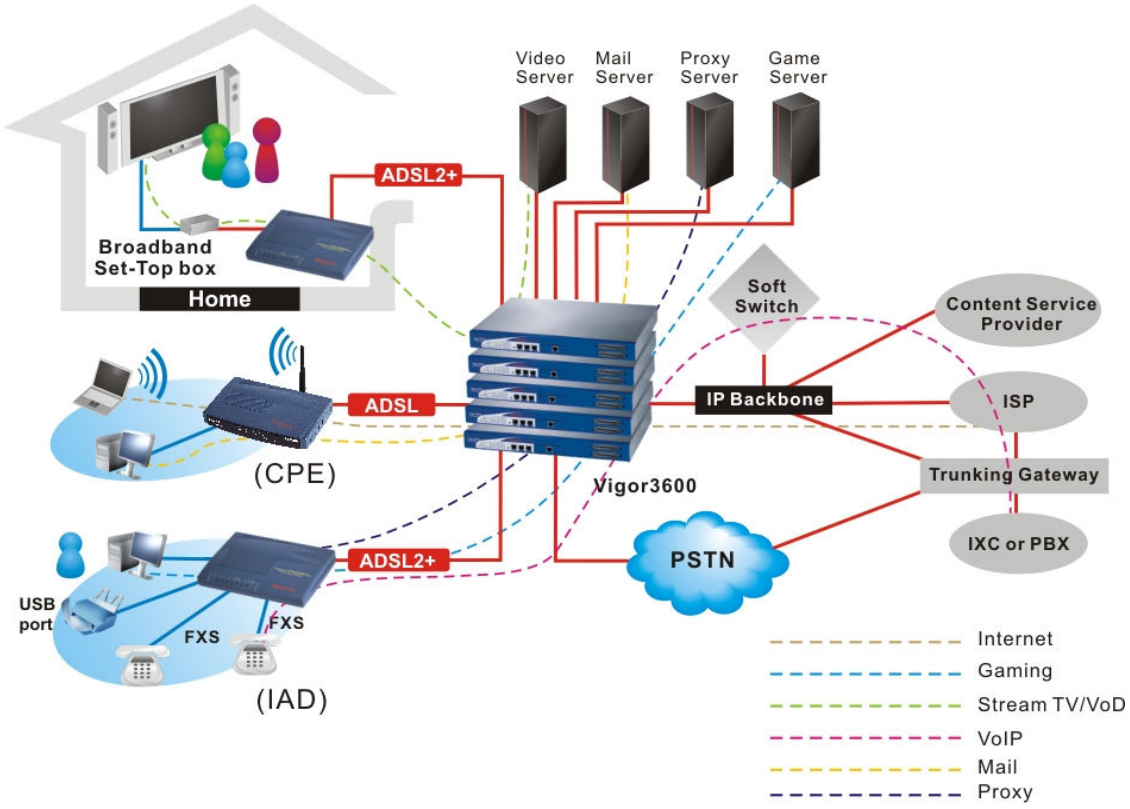


Figure 1-1 Application Scenario of IP-DSLAM for Users

IPDSLAM System Architecture

User can connect the LAN port of IP-DSLAM to an Ethernet WAN switch using a straight-through Category 5 UTP cable with RJ-45 connectors. Then, connect the other end of the cable to an Ethernet switch.
User can stack multiple IP-DSLAM units up to the number of ports available on the Ethernet switch as shown next.

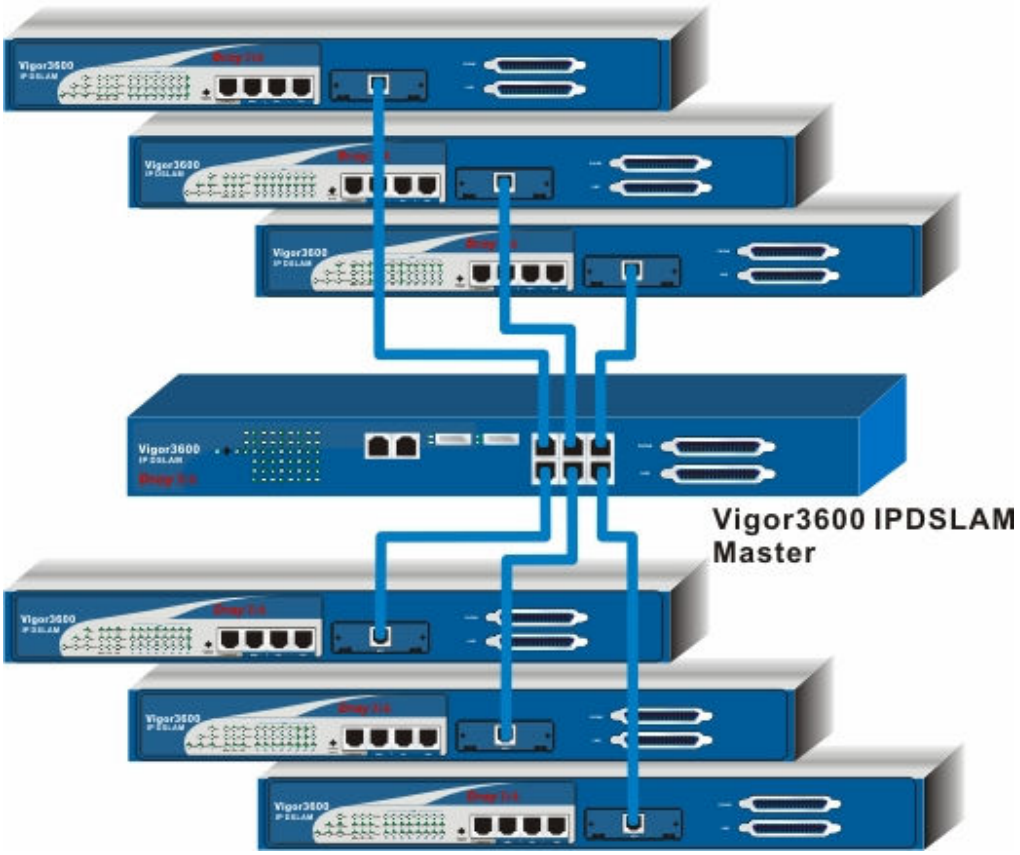


Figure 1-2 IP DSLAM System Architecture

IPDSLAM Master Architecture

The purpose of master unit is as a central unit in DSL application to manage all slave units connected with it. Master unit always collects related information from slave units. Moreover, user can manage slave units through master unit.
The picture of master unit is as below.

Figure 1-3 Master Device Picture

Master unit supports some features as following –
Network Interface - The trunk should be 1000-Based LX, SX or GE Interface.
Cascade Interface - GE interfaces can be cascaded up to six IP-DSLAM slave units.
Capacity – It supports ADSL 2/+ port range from 24 to 168 ports.
Security – It supports Packet filter, and password protection.
Splitter Build in – It supports 24-port xDSL/Splitter included module.
Redundancy - Uplink automatically switch of activity in the event of fiber failure.
Inventory savings - Common equipment across central office and outside plant deployments
Management - Single IP Management
Q.o.S - Packet filter and classification.

IPDSLAM Slave Architecture

The role of slave unit is to provide high-performance, good services DSL features in Internet environment.
The picture of slave unit is as below.

Figure 1-4 Slave Device Picture

Slave unit supports some features as following –
Network Interface - Two 10/100M Fast Ethernet Interfaces or one cascade link is Gigabit Copper interface
Capacity – It supports ADSL 2/+ 24 ports.
Security – It supports Packet filter, and password protection.
Splitter Build in – It supports 24 port xDSL/Splitter included module.
Inventory savings - Common equipment across central office and outside plant deployments
Management – It is managed by IP-DSLAM master unit.
Q.o.S - Packet filter and classification.

Chapter 2

Introduction to Element System Management

Element Management System Server (EMS Server) is a multi-tier architecture, flexible, easy to use for system management. It can manage 1000 to 10000 IPDSLAM devices, depends on the capacity of sever. A step-by-step configuration wizard makes users deploy large numbers of devices to customer sites easily. EMS provides Configuration management, Deployment management, Topology management, Security management, Fault management and backend storage management. Configuration management allows users to remote control the managed devices, or central control by auto provisioning. When Devices are set to “Auto Provisioning” state, the devices will get all settings from the EMS server or the Provisioning server when they are booting up. Another feature in Configuration management is the diagnostic functions used to test the device, make sure that the device is OK. Deployment management is utilized for user to build up some policies for profiles and software upgrade. Administrators can build up some global policies and grant these global policies to some users, then every user can refer these global policies when necessary, or they can build their own policies, and apply these policies to managed devices.

Topology management provides auto discovery for devices and add and delete devices manually. A layer structure is used to show subnet-device relationship. When any fault occurs in some device in a subnet, an alarm warning signal icon is shown in the subnet so that operator can view the status of managed devices immediately. Security management uses a resource-role concept to manage users. For authentication, EMS server has a default mechanism to do that, or an external RADIUS server could be used to provide authentication service. EMS server will maintain an access control list to do authority, grant users with some privilege to resources. Fault management includes alarm collection, status polling, event logging and alert trigger. EMS server monitors all managed devices in a fixed interval, and the device will report alarms when something is wrong in it. EMS server will keep some system event so that trace messages will be stored in the database or files for tracing. Alter trigger provides a notification mechanism to users when any event or alarm received by EMS server. In general, system will send e-mail to users once the condition is fulfilled the filters set by administrator.

The following figure depicts the system overview between IPDSLAM devices and EMS system. The EMS server and IPDSLAM devices use SNMP protocol to communicate with each other.

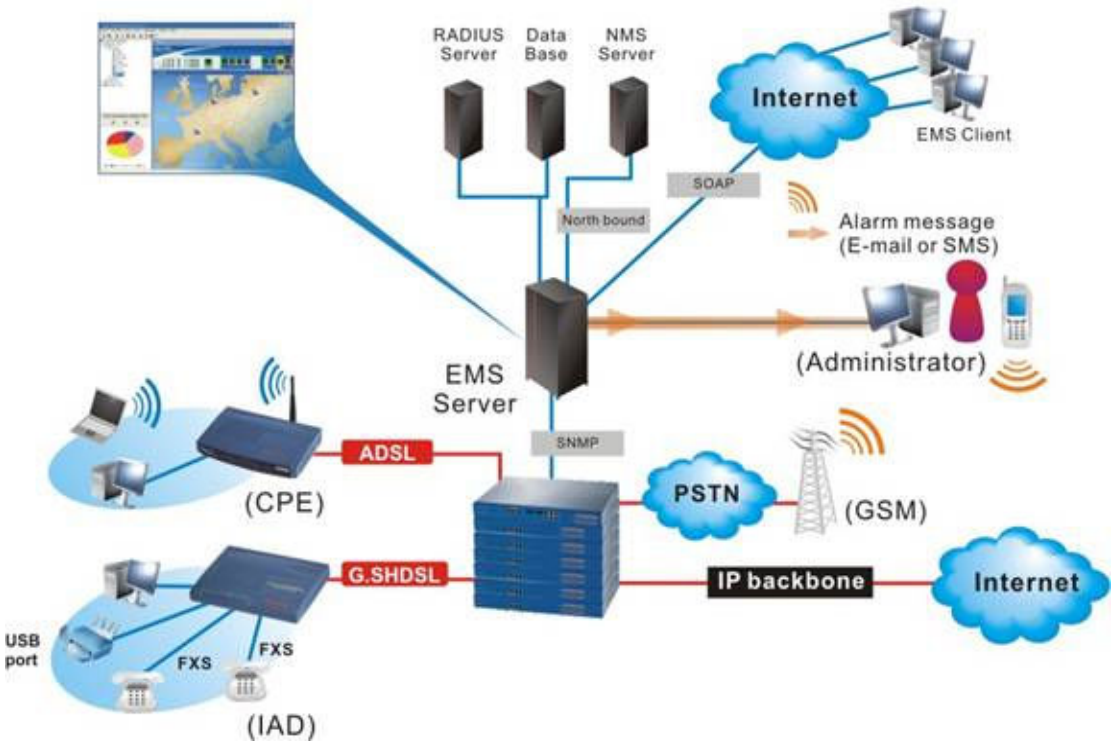


Figure 2-1 IPDSLAM management system overview

For the operation of the whole system, we have to understand the system architecture first. In this Chapter, we first focus on the importance of EMS system overview and technique specifications. We have more detailed function description of the EMS in Chapter 4.

System Description

EMS system is a platform which provides EMS framework for manage SNMP based agents. It includes the following features:

Technical Features

- Allow configuration, diagnostics and view device status
- All management functions are administered in-band through the IP network with standardized protocol (SNMP) between the gateway
- Be able to manage a large number of the IPDSLAM devices
- Support an alarm browser and display alarm details and summary information on GUI
- Support recording and storing of performance statistics for a period.
- All SNMP commands go over SNMP V2C between EMS server and devices
- Support scheduled Software download & upload
- Support Configuration download & upload
- Presents a network map either grouped by IP subnet or as a flat view of the entire network
- Collect alarm and record history event log
- Provide total network view with hierarchy
- User access authentication and security management
- The LED panel for devices is provided for viewing and monitoring
- Auto-polling is provided for monitoring devices in a fixed interval
- A backend database server is used to store log data and management parameters

System Architecture

Software Architecture

EMS is a multi-tiers architecture, including the user interface layer, the presentation layer, the domain and business logic layer and the data store layer. The user interface layer is a graphic user interface that provides an easy to use, easy to operate and no commands to remember for users' interaction with EMS. The presentation layer will transfer the data input via the user interface layer to the business and domain layer and keep the connection session information for users. The business and domain logic layer is an EMS domain tier, including domain dependent tier and domain independent tier. For domain dependent, it means that the functions in this tier are used for managed devices, for example, the configuration management, the monitoring management, and the topology management. For domain independent, the functions are general-purpose functions, for example, the security management, event/log management. The data store tier is a data storage management tire for data manipulation. For example, a backend database server can be used to data manipulation such as insert data, update data, delete data and query data by some conditions. Of course, a backup mechanism is provided for data recovery, and restore.

For platform independent issue, a Java Enterprise Environment (J2EE) platform is used to deploy the EMS server, so it can be run in Linux or Windows™ platform. The backend database server is provided to store user account, topology information, alarm information and event log. For open architecture, the EMS accesses the backend database server by JDBC (Java Database Connectivity), an open database connectivity protocol used to connect to the backend database server. So many JDBC-compliant database servers could be integrated with the EMS server. For example, Microsoft™ SQL server, Oracle™, and MySQL. The default database server used for EMS is MySQL. GUI is either Windows GUI or Java-based GUI, depends on the platform. An instance of the EMS server can manage up to thousands of devices, it means that the number of devices, which are managed by the EMS server, can be scaled to more than 1000 if there are more than one instances in the EMS server. Another issue is the fault tolerant for the EMS

server. EMS server can be run in redundancy mode, which make EMS server more highly availability. When the primary EMS server is started up, a secondary EMS server is in standby mode. Once the primary EMS server is crashed for some reasons, the secondary EMS server is activated immediately.

Configuration Management

EMS provides configuration management for devices management. Operator can remote control devices by invoke the web UI. If there is a provisioning server in the central office, Auto provisioning can make devices to download configuration files once they are started up. The deployment and configuration of large numbers of devices are flexible and easy. For firmware upgrade, administrator can set the schedule for firmware upgrade for individual device or a subnet set in EMS, so firmware upgrade is done by a batch job online or in pre-assigned time.

Security Management

EMS provides a central security management for user account and resource control. For authentication, a default mechanism is provided or an external RADIUS server is used. For resources control, EMS treats functions, managed devices, policies as different resource types, so EMS will grant resources to roles defined by administrator. So the security model for EMS is user-role-resource.
Role:
Default=> Administrator/Operator
Resources:
Functions/Managed Devices/Policies/Map

Monitor Management

Monitor management includes fault management and device polling. Fault management is used to collect all alarms come from managed devices, store the alarm information into backend database and provide query, delete functions for alarm information. EMS also generates analysis report to NMS by northbound interface. Device polling used to monitor the status of devices in a fixed interval and the icon status of the device will be changed if the status of device has been changed. Alarm bubble up is supported while the status of a device in that subnet has been changed. An online trouble-shooting is provided to make operators get solutions for alarms.

EMS provides notifications to operator once it receives alarms. The notification mechanism can be by e-mail or by SMS. Administrator can set the alarm filter and will notify operators once EMS receives these set alarms.

Topology Management

Topology management provides auto discovery and layer structure subnets for managed devices. For auto discovery, we can input a network range and EMS will search the devices located in the network range, and then insert these devices into the Map. Layer structure subnets are a layer structure for subnet and devices, or for subnet and subnet. A device must be belonged to some subnet built in the EMS. The subnet is a logical folder

or group which is used to group devices or another subnet in a folder for manage issue, so at least one subnet in the system, that is, ROOT. So when administrator new a map, a ROOT exists in the top of the layer structure.

Deployment Management

The function of Deployment management is used to deploy predefined profile, we also can set a scheduler for batch deployment, and you also apply a policy to multiple devices on some date/time.

Another type of policy is the firmware upgrade that is used to upgrade software to multiple devices on some date and time. Administrator can build a firmware upgrade policy for batch firmware upgrade. The policy includes the date and time, the version of firmware, the type of firmware.

Log and Event Management

EMS will receive alarms or events and collect them into the backend database, so history data will be kept for a long time. Also, User activities will be kept into the log database for security issue and the administrator can build a log backup by dump database files to some media and clean the history database.

Chapter 3

Installation And Getting started

IPDSLAM EMS is client-server architecture, so the installation procedure should consist of two parts: EMS client installation and EMS server installation. EMS client should be installed in Windows 2000/XP/NT environment and EMS server includes a J2EE server and a backend database server (JDBC-compliant), should be installed in Windows 2000/XP server, LINUX environment and Sun Solaris.

This chapter describes the installation guide for EMS client and EMS server, and how to start EMS program. All functions will be described in chapter4 or later.

Installation

Setup and Install EMS Client Software

The EMS Client installation package comes with a setup program that can help you to easily install the EMS client program with all necessary libraries and DLL files on supported Windows Operation systems (2000, NT, XP).

The EMS client is a graphical user interface tool that retrieves data from EMS server. By the tool, operators can manage devices easily. You can use EMS client tool to perform more network management operations such as

- Graphically represent devices on a network map
- Real time monitor and notify the user about the changed status of the device
- View current event and alarm history
- Security management
- Configuration

Install

For Windows 2000™ Profession or XP home/professional platform

Step1: Setup JAVA VM environment: Run j2re-1_4_2_03-windows-i586-p.exe.
Step2: To Setup EMS Client, run SETUP.EXE in your source disk or CD-ROM that contains EMS Client programs and follow the instructions, step by step, to complete the installation.

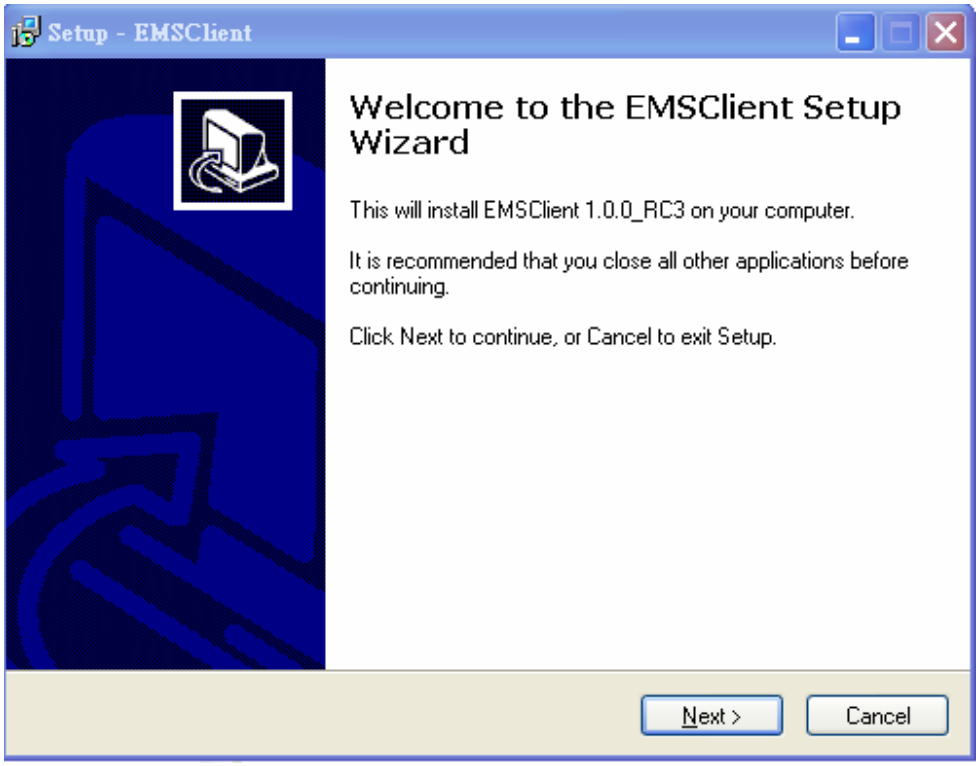


Figure 3-1 EMS Client Setup Program

Uninstall

To uninstall the EMS Client, open the Control Panel, click on the applet "Add/Remove Programs" and choose to Remove EMS Client.

Setup and Install EMS Server Software

The EMS Server installation package comes with some setup packages for different platforms. When you are ready to install EMS server, you should look up the platform folder and then select the platform you wants to install. The server setup packages include application server and backend database server. The platforms could be Windows series or LINUX-like environment.

Install EMS Server

For Windows 2000™ server or XP high end platform

Step1: Setup JAVA VM environment: Run **j2re-1_4_2_03-windows-i586-p.exe**.

Step2: Install MySQL. Run **mysql-4.0.17-win\Setup.exe**.

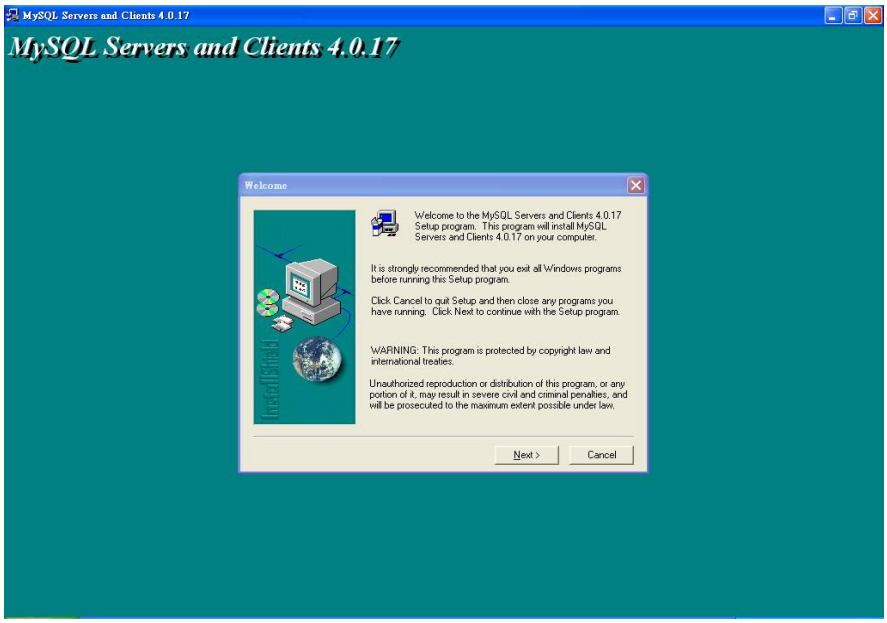


Figure 3-2 Database Server Setup Program

Step3: Execute **setup.exe** to install EMS application server

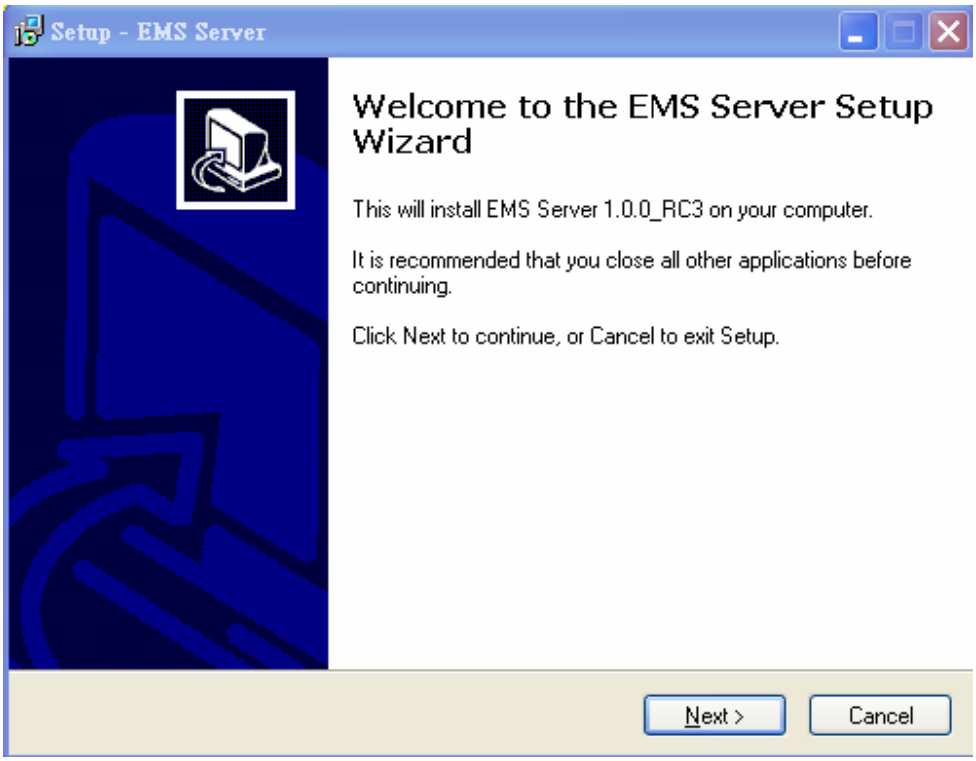


Figure 3-3 EMS Server Setup Program

During setup, the setup wizard will prompt a message to indicate that if you want to rebuild the database, you should select "Yes" if the version of EMS is under V1.0.0 RC4.

For Sun Solaris platform
Step1: Login Solaris with **root** or the root privilege.
Step2: Decompress the setup packages, suggest that make the directory **/usr/local/ems_src** first, then decompress the setup package under this directory:

gzip -cd solaris_ems_server.tar.gz |tar xvf -

Step 3: Change to the directory **/usr/local/ems_src** execute **./install.sh**
Step 4: Before execute ./install.sh , Change the mode of **./install.sh** to 755
chmod 755 install.sh
Step 5: Verify the version of Solaris:
What is the solaris OS version of about your machine (8 or 9)
Input the exact version number of Solaris, 8 or 9.
Step 6: Install the library needed by MySQL database:

1. Install library : libgcc coreutils libiconv ncurses install (installing mysql need)
2. Install mysql
3. Install java
4. Install EMS Server (It will build one mysql database : snmpdb)
5. Install EMS Client
6. Upgrade EMS Server (It will upgrade snmpdb database)
7.Exit

input select num : 1

Select **1** to install the libraries needed by MySQL.

Step 7: Install MySQL database:

1. Install library : libgcc coreutils libiconv ncurses install (installing mysql need)
2. Install mysql
3. Install java
4. Install EMS Server (It will build one mysql database : snmpdb)
5. Install EMS Client
6. Upgrade EMS Server (It will upgrade snmpdb database)
7. Exit

input select num : 2

Select **2** to install the MySQL.

Step 8: Install JAVA environment:

:

1. Install library : libgcc coreutils libiconv ncurses install (installing mysql need)

2. Install mysql
3. Install java
4. Install EMS Server (It will build one mysql database : snmpdb)
5. Install EMS Client
6. Upgrade EMS Server (It will upgrade snmpdb database)
7. Exit

input select num : 3

Select **3** to install the JAVA virtual machine

Step 9: Install EMS application

1. Install library : libgcc coreutils libiconv ncurses install (installing mysql need)
2. Install mysql
3. Install java
4. Install EMS Server (It will build one mysql database : snmpdb)
5. Install EMS Client
6. Upgrade EMS Server (It will upgrade snmpdb database)
7. Exit

input select num : 4

Select **4** to install the EMS application server.

Uninstall EMS Server

For Windows 2000™ server or XP high end platform
To uninstall the EMS Server, open the Control Panel, click on the applet "Add/Remove Programs" and choose to remove **EMS** Server and **MySQL.**

For SUN Solaris platform
To uninstall the EMS server in Solaris, run **./uninstall.sh** under the directory **/usr/local/ems/EMSServer/bin,** then the following menu items are shown:

1. Uninstall library : libgcc coreutils libiconv ncurses install (installing mysql need)
2. Uninstall mysql
3. Uninstall java
4. Uninstall EMS Server
5. Uninstall EMS Client
6. Exit

input select num :

So if any software is needed to removed, select the number of menu items.

Getting Started

After finishing installation for EMS client and server, the next step is to start EMS program. The steps of starting EMS program are described as followings:

Step 1: Start Backend database server

For Windows 2000™ server or XP high end platform

If you use MySQL as the backend database server in Windows™, then MySQL server will be started by system automatically when the server machine is started. A management console will locate in the notification area of the Window environment. Other database server should be reference the user manual.

For SUN Solaris platform

For Solaris environment, run **ems.sh** under the directory **/usr/local/ems/EMSServer/bin,** then select the number of menu items as 1 :

1. start mysql
2. shutdown mysql
3. start ems
4. shutdown ems
5. edit bind ip of EMS Server(please keying ip or servername)
6. set the MAX and MIN memory value of running java (It will valid after restart ing EMS)
7. view the MAX and MIN memory value of running java
8. exit
input select num :1

Then MySQL database server is startup in Solaris, and the message is shown as followings if it is success:
Starting mysqld daemon with databases from/usr/locall/mysql/var

Step 2: Start Application server

For Windows 2000™ server or XP high end platform

If you install Application server in the Windows™ environment, then you can start the EMS server by click **Program->EMS Server->Start EMS Server** to start EMS server. If the server starts at the first time, then a dialog box is shown for input the IP address that EMS server use to bind at the first time:

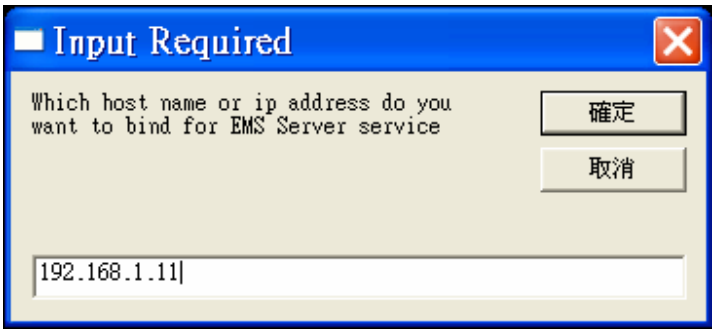


Figure 3-4 Input the IP address EMS Server binds

If EMS server will be started with another IP, go to **Program->EMS Server-> Edit Bind IP of EMSServer** to replace the old IP with the new IP. After change the IP, this file should be saved. **This file can be opened with Notepad.**

For SUN Solaris platform
For Solaris environment, run **ems.sh** under the directory **/usr/local/ems/EMSServer/bin,** then select the number of menu items as 3 :

1. start mysql
2. shutdown mysql
3. start ems
4. shutdown ems
5. edit bind ip of EMS Server(please key in ip or servername)
6. set the MAX and MIN memory value of running java (It will valid after restart ing EMS)
7. view the MAX and MIN memory value of running java
8. exit
input select num :3

When EMS server starts, it binds the IP of one network interface you set. If you want to change this setting, input item 5 for editing the IP:
1. start mysql
2. shutdown mysql
3. start ems
4. shutdown ems
5. edit bind ip of EMS Server(please key in ip or servername)
6. set the MAX and MIN memory value of running java (It will valid after restart ing EMS)
7. view the MAX and MIN memory value of running java
8. exit
input select num :5

When this option is selected, the shell script run **vi** editor to load this configuration file, so change the old IP or name with the new one and save, then restart EMS server will use the new IP as the binding IP.

The default size of heaps needed by EMS application server is 128MBytes~196MBytes, while the size of memory is assumed as 512Mbytes. If the size of memory is over 1GMbytes, the size of heaps allocated to EMS can be enlarging to over 256Mbytes. To change the size of heaps, please select item 6 to change the configuration:

1. start mysql
2. shutdown mysql
3. start ems
4. shutdown ems
5. edit bind ip of EMS Server(please key in ip or servername)
6. set the MAX and MIN memory value of running java (It will valid after restart ing EMS)
7. view the MAX and MIN memory value of running java
8. exit
input select num :6
Please input Number or input Enter by using original value.
Maximum memory (Mega)of running java(196):256
Minimum memory (Mega)of running java(128):196
The value will valid after restarting EMS Server

If EMS application server is start-up for all VM environments, and the message is shown as followings if it is success:

INFO [org.jboss.system.server.Server] JBoss (MX MicroKernel) [3.2.3 (build: CVSTag=JBoss_3_2_3 date=200311301445)] Started in 30s:84ms

Step 3: Start EMS Client

If you install Application server in the Windows™ environment, then you can start the EMS client by click **Program->EMS Client->Start EMS Client** to start EMS client.

EMS Window Menu

The EMS client program provides a menu-driven function user interface for operators. The windows menu hierarchy is depicted in the following figure:

Figure 3-5 EMS Window Menus

The EMS client program provides a multiple document interface that uses one mainframe window with several child windows.

All child windows have equal existence rights and exist independently from each other. When close one window shall not cause closing another child window.

EMS Menu Item

The Main functions of EMS are shown as followings:

- Network Add a new sub network or a new device to the current network.
- Event Show the content of alarms and traps.
- Tools Provide ping, trace route and telnet tool to managed devices.
- Advanced Provide system management functions.
- Windows Provide windows functions such as multiple-windows styles.
- Help Provide content-sensitive online help.

Chapter 4

Configuration Management

The functions of Configuration management include device provision, real-time, on-line configuration for IP DSLAM master/slave devices. By EMS client tool, you can add/modify/delete devices as you have these privileges. You also can monitor the status of devices, use mouse to drag and click to invoke any device configuration easily. At the same time, EMS provides some utilities to diagnose devices such as ping and trace route. This chapter describes all configuration functions; include device management functions, system management functions.

Device Management

Device management includes controller configuration and DSL configuration.

Controller Configuration

This Configuration function allows you to configure parameters about devices. When you click the icon of device in the device map in the left panel of EMS main window, a device configuration window will be shown as Fig. The sub functions of device configuration are described as followings:

Controller/status

Display Name

The name of the device we want to connect. This value is set when new a device.

Device Type

The type of the device we want to connect. This value is set when new a device.

Sys Name

The name of the device we want to connect. This value is set when new a device.

Sys location

The location of device we want to connect.

IP

The IP address of the device we want to connect.

Read Community

The community set for read operations from EMS to device in SNMP. This value should be set the same as that of the device. If the community set in EMS is not the same as that of the device, this operation will be rejected.

Write Community

The community set for set operations from EMS to device by SNMP. This value must be set the same as that of the device. If the community set in EMS is not the same as that of the device, this operation will be rejected.

SNMP Port

The port number of SNMP agent is located in the device.

SNMP Version

The version of SNMP set in EMS used to communicate with the device.

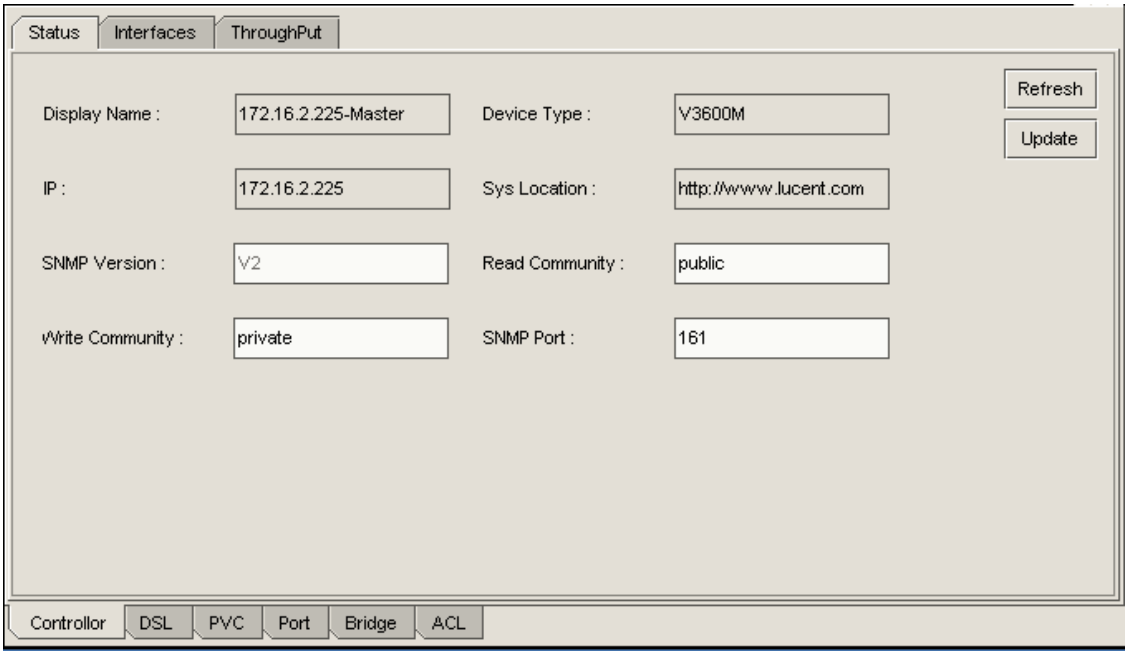


Figure 4-1 Device Status Configurations

Controller/Interfaces

The performance data of network interfaces resided in the controller.

Interfaces

The network interfaces resided in the controller.

InOctets

The total number of octets received on the interface.

OutOctets

The total number of octets transmitted out of the interface.

InDiscards

The number of inbound packets discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.

OutDiscards

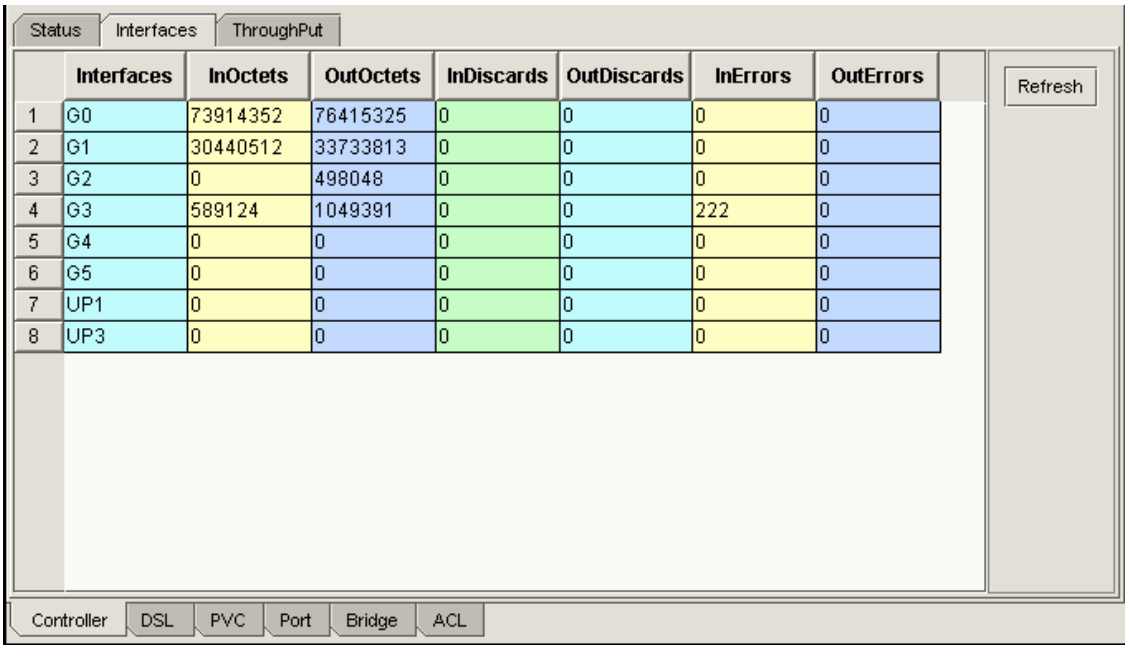
The number of outbound packets discarded even though no errors had been detected to prevent their being transmitted.

InErrors

The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol

OutErrors

The number of outbound packets could not be transmitted because of errors.



	Interfaces	InOctets	OutOctets	InDiscards	OutDiscards	InErrors	OutErrors
1	G0	73914352	76415325	0	0	0	0
2	G1	30440512	33733813	0	0	0	0
3	G2	0	498048	0	0	0	0
4	G3	589124	1049391	0	0	222	0
5	G4	0	0	0	0	0	0
6	G5	0	0	0	0	0	0
7	UP1	0	0	0	0	0	0
8	UP3	0	0	0	0	0	0

Figure 4-2 the performance data of network interfaces

Controller/Through Put

The throughput for selected network interfaces of the controller. When a network Interface is selected; the statistic information can be displayed in graphical style.

Select a network interface

If you want to monitor a network interface, you should click the "Controller->ThroughPut" tab and right-click the "interfaces" function in the three panels, then select "Add Interface(s)" function, and then a dialog box will be displayed for selecting a network interface:

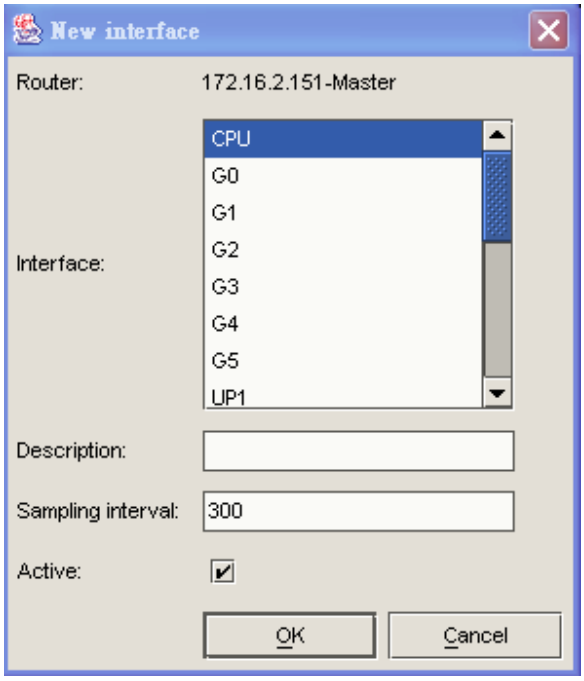


Figure 4-3 the network interfaces selection box

Select a time interval for monitoring

There are some types of time interval can be selected for monitoring: by last 24 hours, by day, by week, by month, by year. Select a type you can monitor, then the statistic information will be shown for a long time.

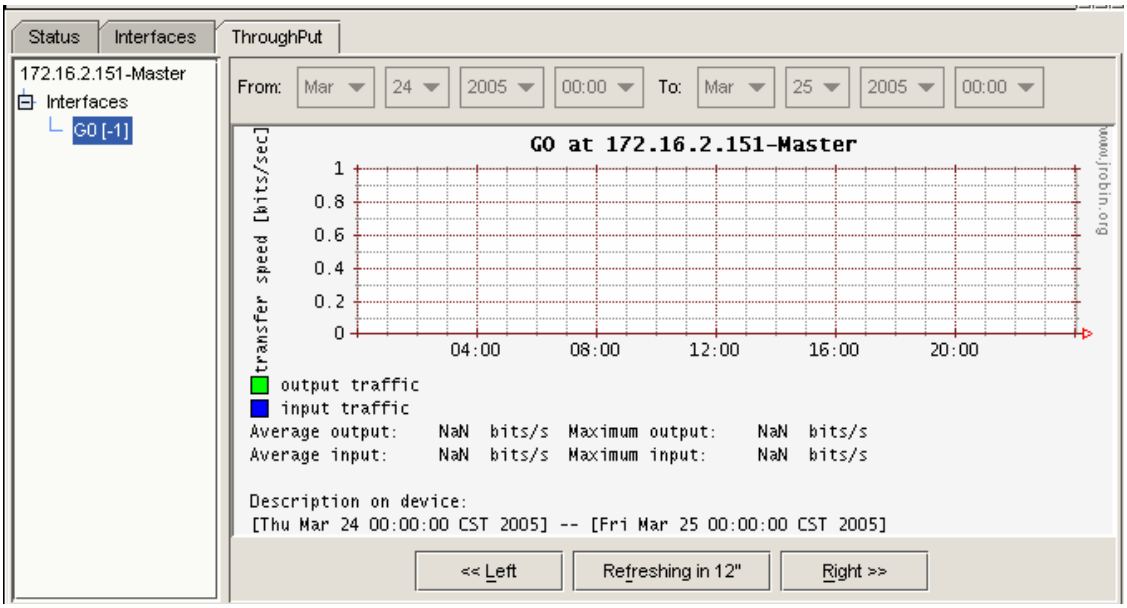


Figure 4-4 the throughput of G0 by hours

Controller/Reset

Reset function will reboot the controller or DSL cards. When reboot the controller, the DSL card is still active and no side effect will occur.

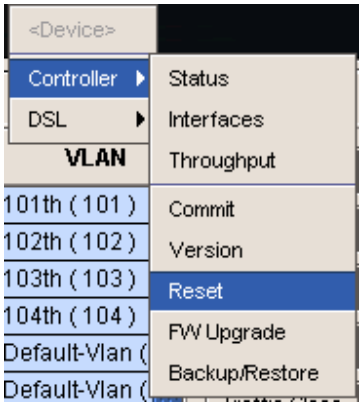


Figure 4-5 Reboot function for controller card

There are options for reset function: *reboot*, *default* and *keep*. Reboot means reboot by the current configuration, default means reboot by the default factory configuration and keep means reboot by the default factory configuration, but keep the network settings(management IP, for example).

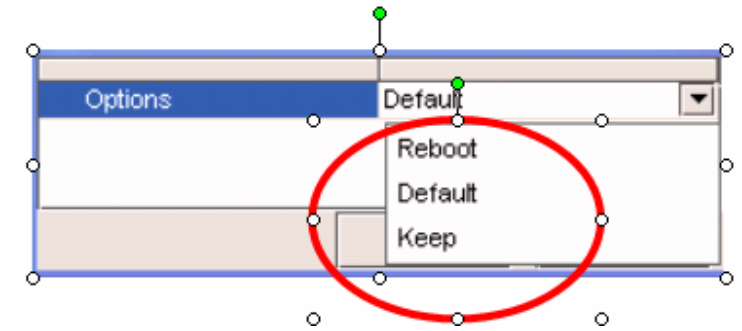


Figure 4-6 The reboot for the controller card: the options for reboot.

Controller/Commit

Commit function is used to confirm all changes for controller / DSL configuration. If this function is selected, all changes to device configuration will be saved to the device. When the device is rebooting or power on again, the new configuration will take effect.

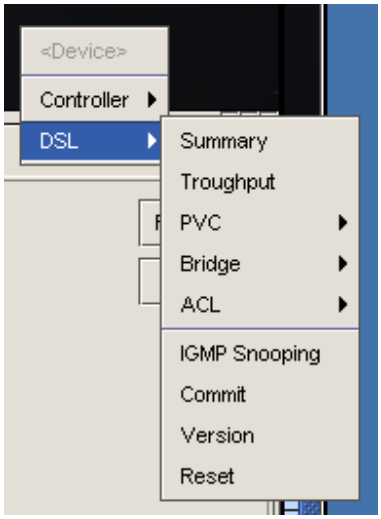


Figure 4-7 Commit function for controller card

Controller/Version

The version information includes controller and DSL card in the master device. The fields are described as following:

Model

The type of the IPDSLAM device, there are two types for IPDSLAM devices: master and slave.

Software Version of master

The version of software for the controller card located in the master device.

Hardware Version of master

The version of hardware for the controller card located in the master device.

Hardware Version of slave

The version of hardware set for the DSL card located in the IPDSLAM device.

ControlPlane Firmware

The version of software set for the DSL card located in the IPDSLAM device.

DataPlane Firmware

The version of software set for the DSL card located in the IPDSLAM device.

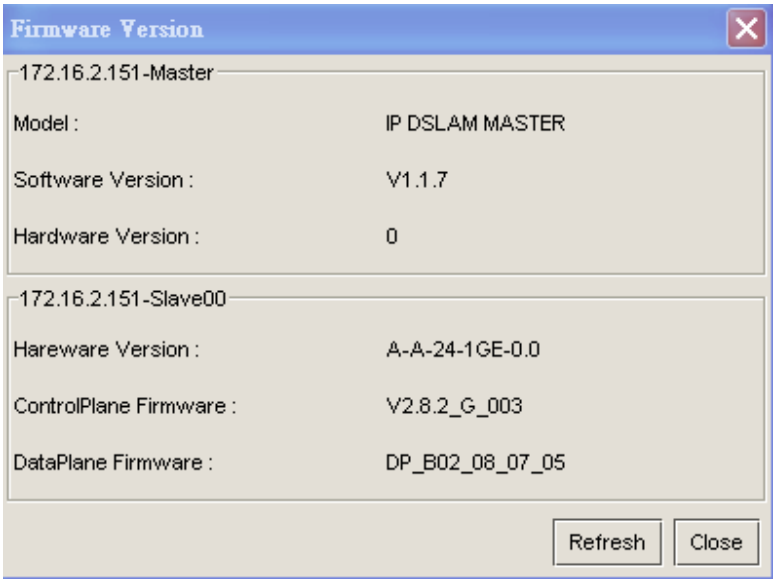


Figure 4-8 the version information of the master device

Software Upgrade

The firmware upgrade function enables operator do software upgrade for controller card in the master device. Before upgrade the new software, the firmware file should be added into the EMS server, and then the file can be selected in the file list window of the firmware upgrade window.

File Upload

Before upgrading new firmware or configuration files, these files should be uploaded into the TFTP server. Select **"Advanced->File Upload"** function and the file upload window will be shown as followings:

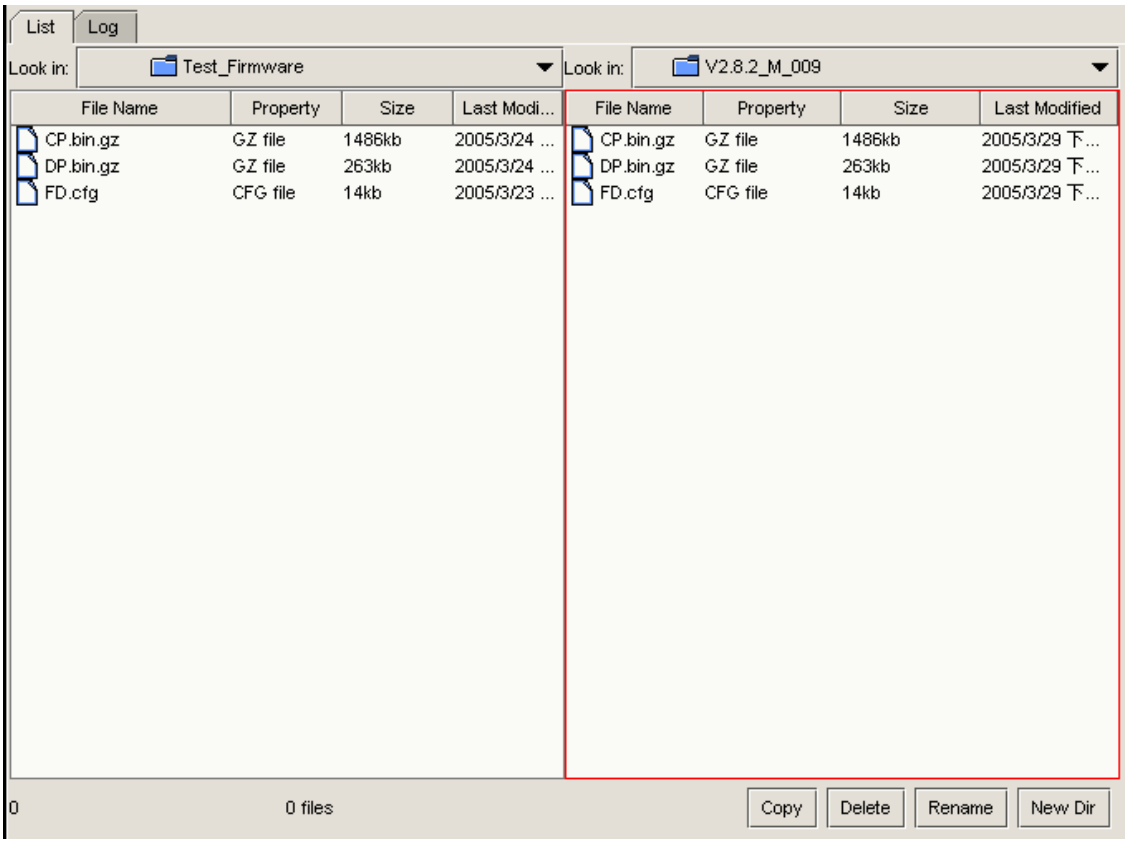


Figure 4-9 File upload window

In this window, the local directory is located in the left panel, and user can select the files you want to upload and click "**Copy**" button, then these files will be copied into the TFTP server.

Firmware upgrade for controller card

There are two types of software for IPDSLAM devices: *controller* and *DSL*. If the firmware is upgraded to the master, you should right-click the LED panel and select "Controller->FW Upgrade" function to upgrade the firmware for controller. As Figure 4-9.

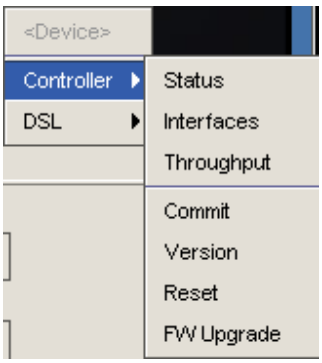


Figure 4-10 the menu function of firmware upgrade for controller

By selecting the firmware ready to upgrade, select "Upgrade" function to upgrade the firmware:

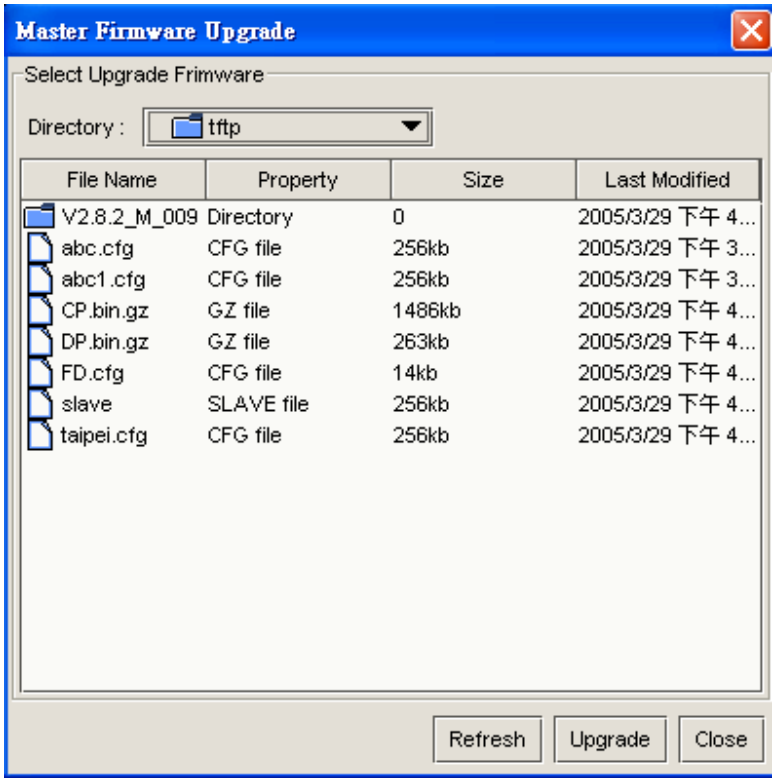


Figure 4-11 the version information of the master device

When you select **"upgrade"** function, the selected file are upload to the device, see the Figure 4-12.

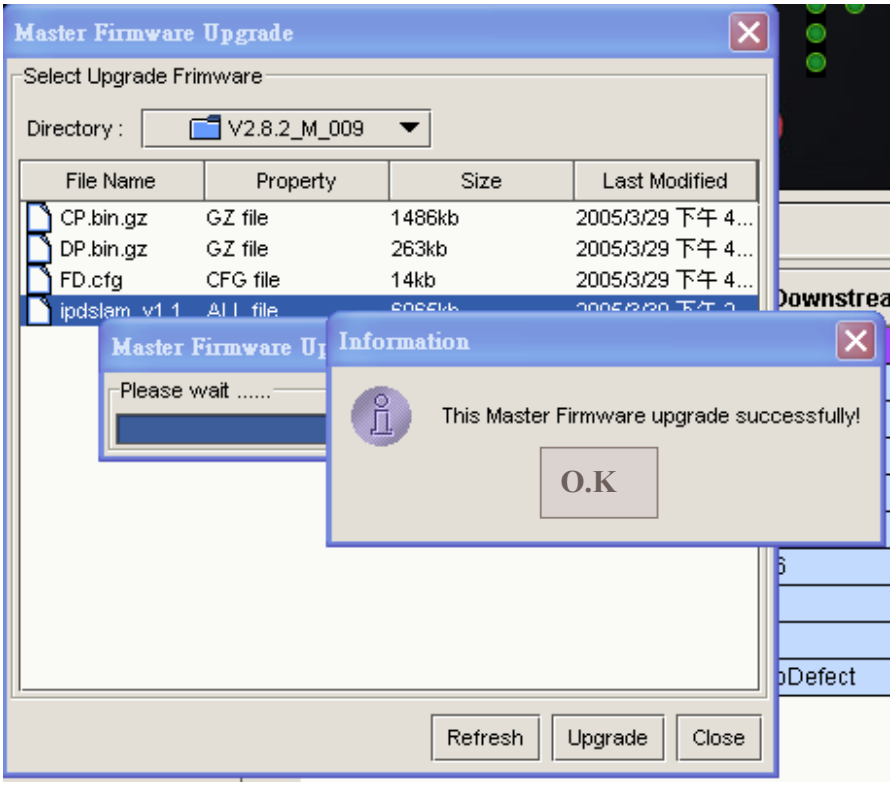


Figure 4-12 Firmware upgrade function for controller card

After finished the firmware function, you need to reboot the controller card.

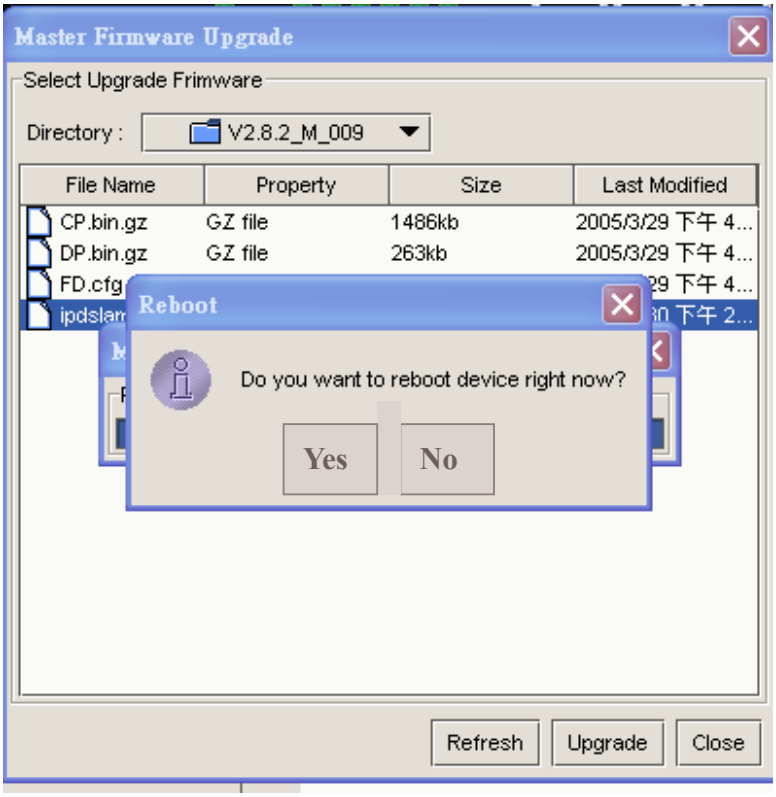


Figure 4-13 the system prompts a "Reboot" message

Firmware upgrade for DSL card

If the type of software is *DSL*, then you should select **"DSL->FW Upgrade"** function to upgrade the new firmware.

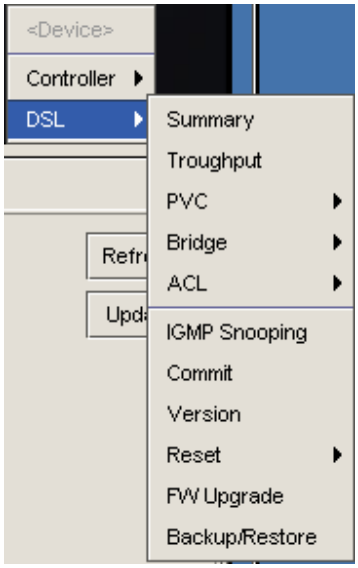


Figure 4-14 the menu function of firmware upgrade for DSL card

For DSL card, there are three firmware files needed to be upgraded together: *CP.bin.gz*, *DP.bin.gz* and *FD.cfg*. Before upgrading these files, you should select the type of these firmware: "CP" for CP.bin.gz, "DP" for DP.bin.gz and "FD" for FD.cfg.

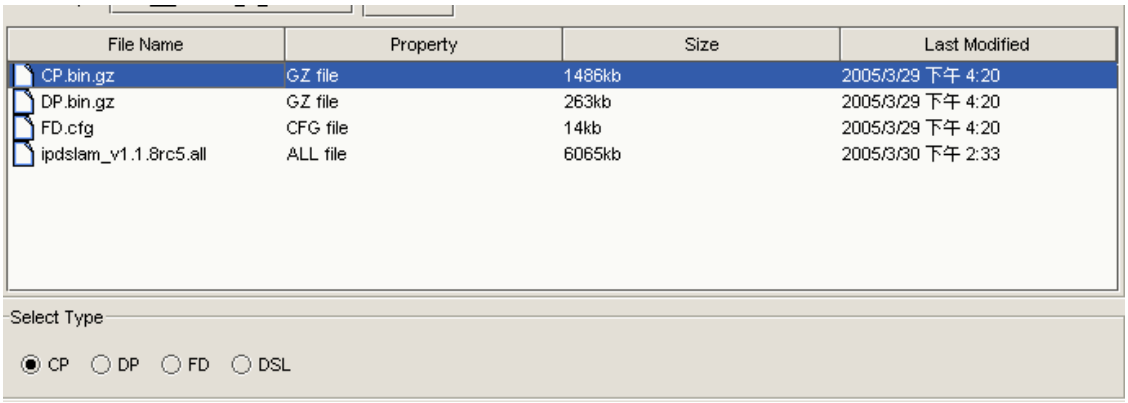


Figure 4-15 the firmware upgrade function for DSL card

Before upgrade the new firmware to TFTP server, you should create a directory named as "V2.8.2_M_009XXX" if the uplink interface is Fast Ethernet and "V2.8.2_G_009XXX" if uplink interface is Giga Ethernet, XXX means any string, then put these files to this directory.

After all three files are upgrade to the IPDSLAM device, you should reboot DSL card manually. Select "**DSL->Reset->Last**" to reboot the device

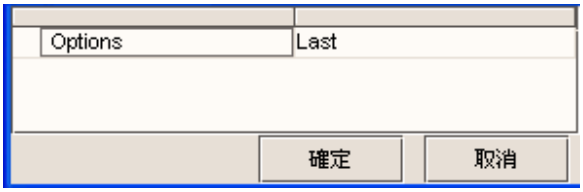


Figure 4-16 reboot the DSL card after firmware upgrade

Configuration Backup and Restore

The configuration for DSL cards or controller can be grouped into a file, and can be

retrieved by EMS. When downloading to EMS server, the file is transferred by TFTP protocol. This file is stored in the location of TFTP server, provided to restore to devices if necessary.

For backup or restore configuration for DSL cards, double-click the device in the left panel, and once the panel for that device, right-click the panel and select **DSL->Backup/Restore** to invoke the Backup/Restore function.

For backup and restore configuration for Controller of the master device, double-click the device in the left panel, and once the panel for that device, right-click the panel and select **Controller->Backup/Restore** to invoke the Backup/Restore function.

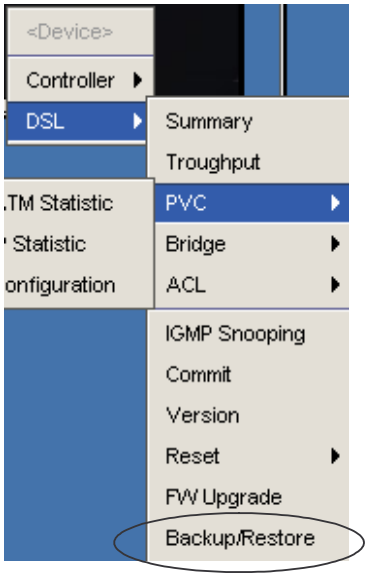


Figure 4-17 select the backup and restore function

Backup Configuration For DSL cards

To backup configuration for DSL cards, input the name of file to be saved under the default directory of TFTP server first, then select "Apply" button to get the configuration information from the selected device.

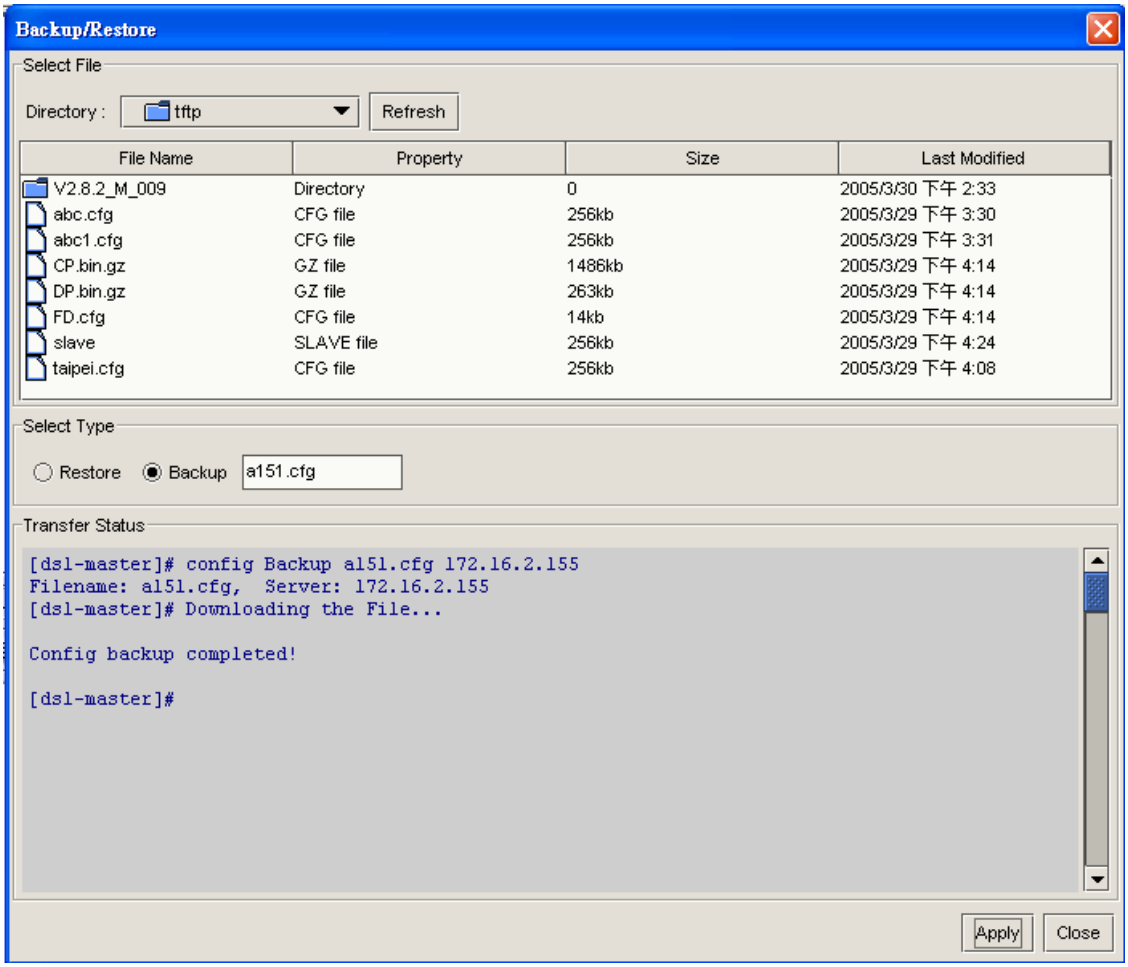


Figure 4-18 Backup the Configuration from the device

Restore Configuration For DSL cards

To restore the configuration file to the selected device, right-click the device panel and select “Backup/Restore” function.

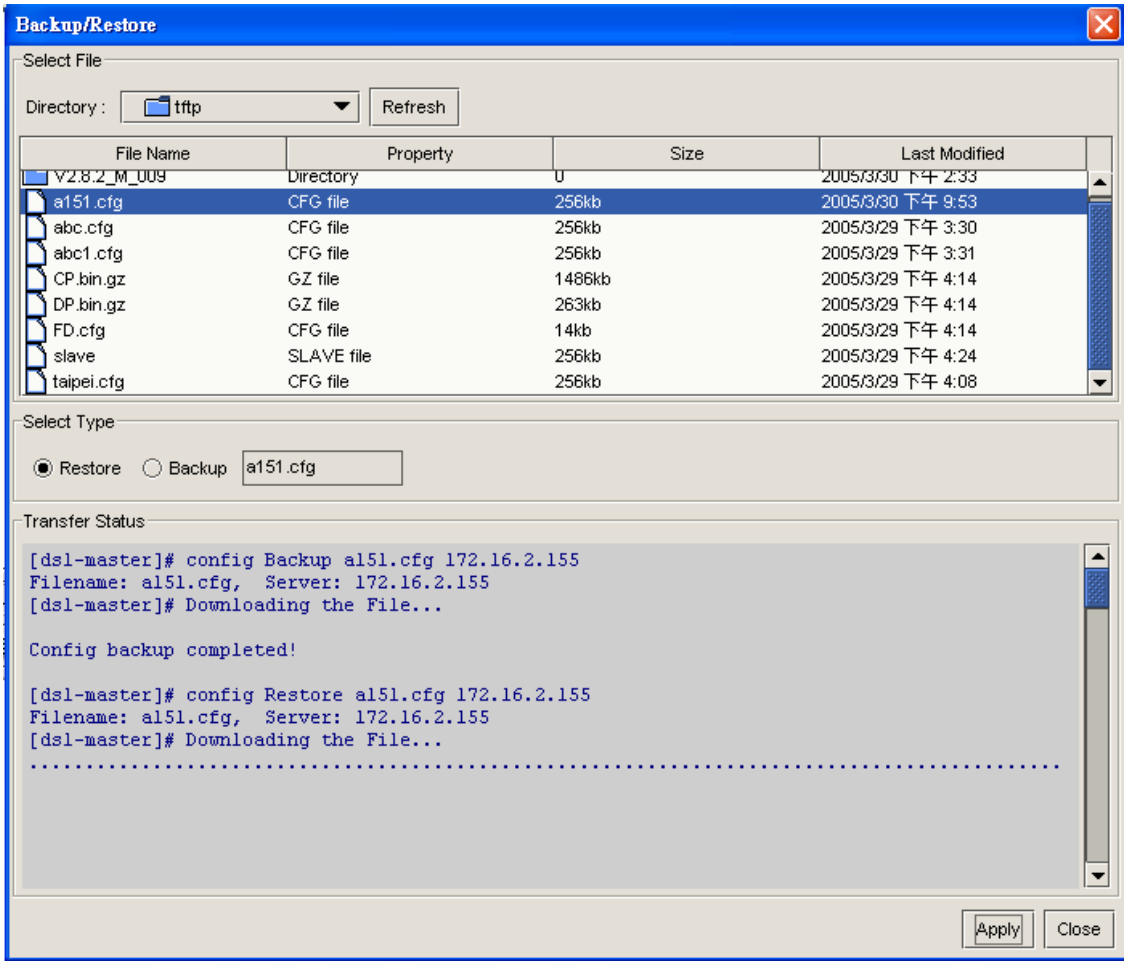


Figure 4-19 restore the configuration to the device

Backup Configuration For Controller

To backup configuration of the controller for the master device, input the name of file to be saved under the default directory of TFTP server first, then select “Apply” button to get the configuration information from the selected device. See figure 4-19.

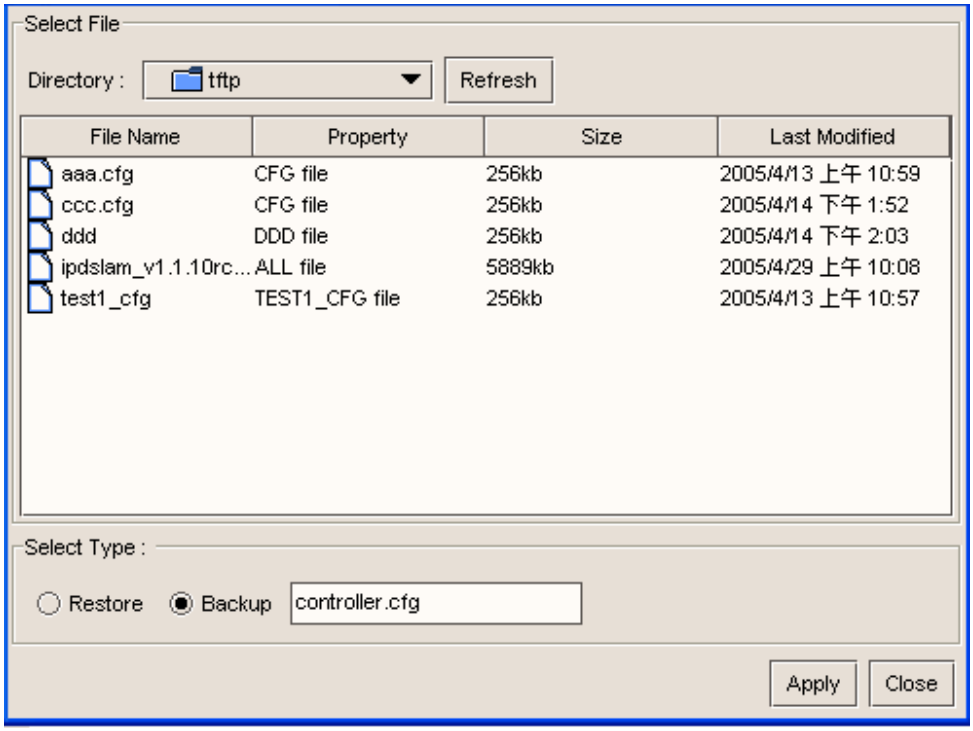


Figure 4-20 Backup the Configuration from the device

Restore Configuration For Controller

To restore the configuration file to the selected master device, select the configuration file from the file list, then select “Restore” option and press “Apply” button to do restore function. See Figure 4-21..

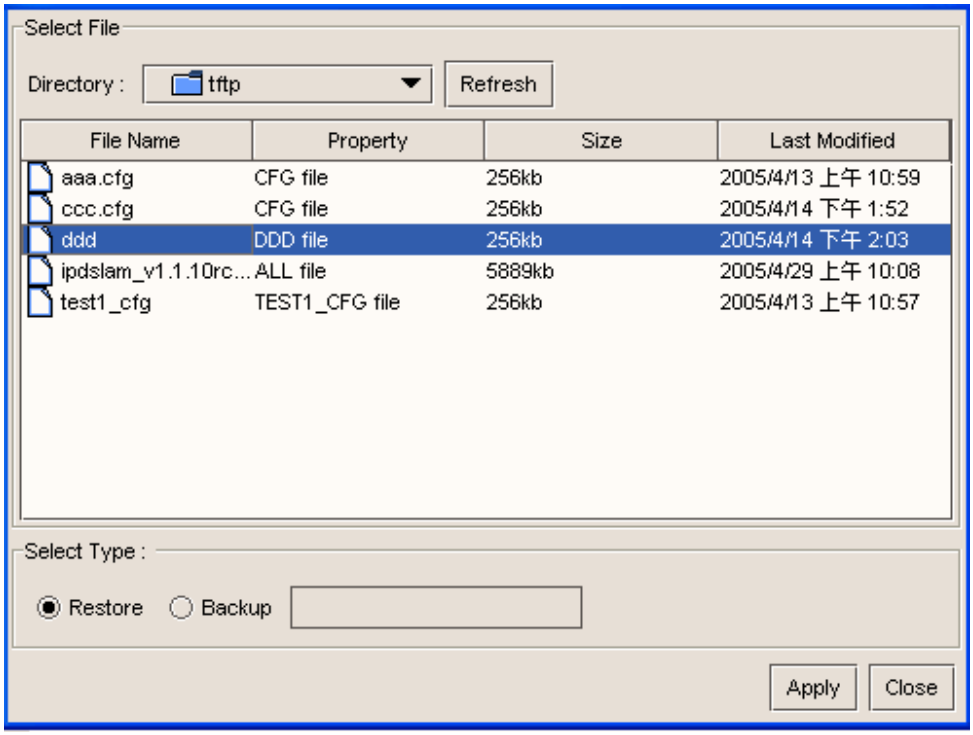


Figure 4-21 restore the configuration to the device

DSL Configuration

DSL/Summary

Display the status for each port in the device. Press the **Start** button to begin to get the information, **Stop** button to stop the retrieve the information if **Poll** option is turned on.

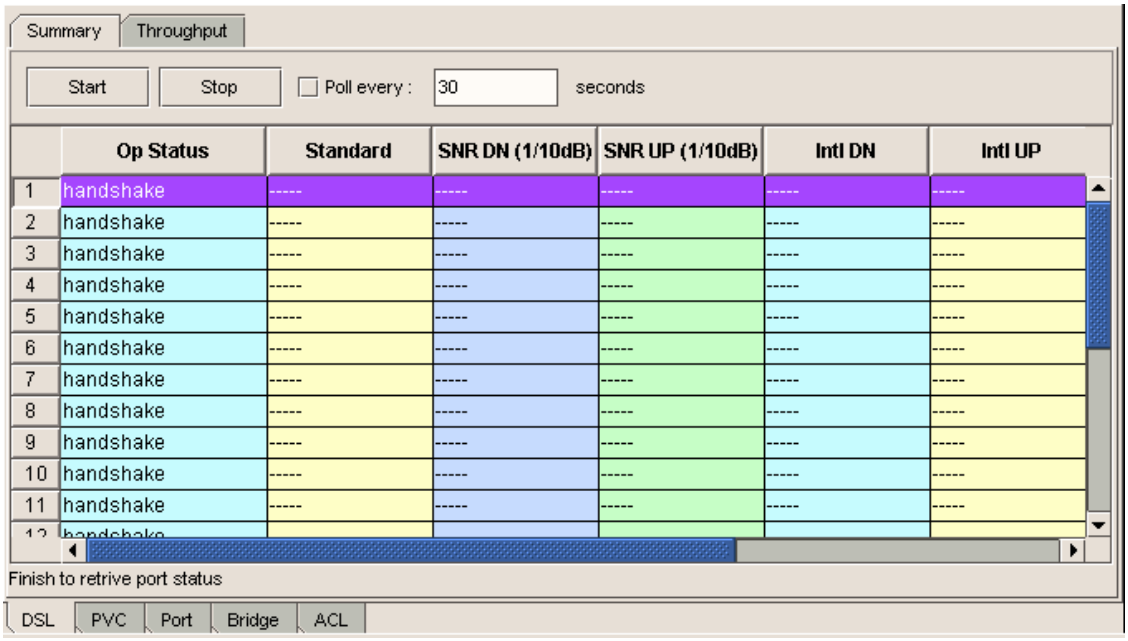


Figure 4-22 Summary Configurations

PVC Functions

PVC/ATM Statistics

Port
The port index of the DSL device

VPI
The VPI value for this port

VCI
The VCI value for this port

RxCells
The amount of cells is received for this PVC.

TxCells
The amount of cells is sent from this PVC.

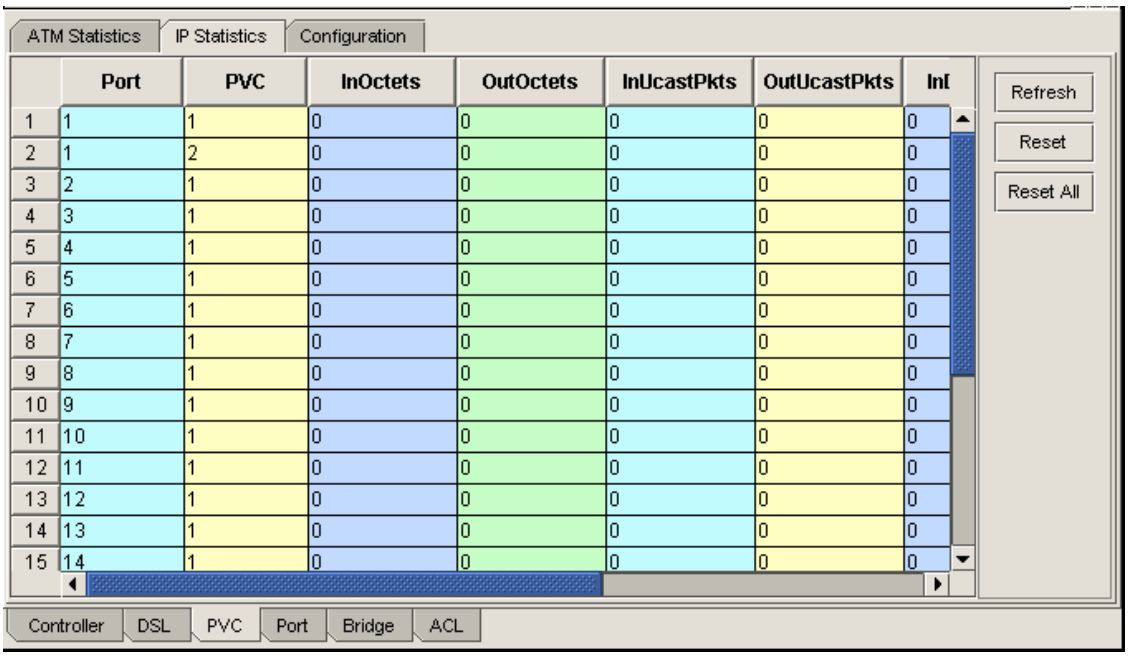
RxCLPO
The number of valid ATM cells received by this VCL with CLP=0. The cells are counted prior to the application of the traffic policing.

Discards
The total number of valid ATM cells discarded by the traffic policing entity. This

includes cells originally received with CLP=0 and CLP=1

PVC/IP Statistic

This function provides the performance information by PVC-based. The meanings of items for this function are the same as that described in the “Controller/Interfaces”.



	Port	PVC	InOctets	OutOctets	InUcastPkts	OutUcastPkts	InU
1	1	1	0	0	0	0	0
2	1	2	0	0	0	0	0
3	2	1	0	0	0	0	0
4	3	1	0	0	0	0	0
5	4	1	0	0	0	0	0
6	5	1	0	0	0	0	0
7	6	1	0	0	0	0	0
8	7	1	0	0	0	0	0
9	8	1	0	0	0	0	0
10	9	1	0	0	0	0	0
11	10	1	0	0	0	0	0
12	11	1	0	0	0	0	0
13	12	1	0	0	0	0	0
14	13	1	0	0	0	0	0
15	14	1	0	0	0	0	0

Figure 4-23 the IP Statistics of PVC

PVC/Configuration

The configurations of PVC for each port set in the device. You can add, update, and delete these PVC settings in this window. The fields for PVC are described as followings:

Name

The name of this PVC.

Port

The identifier of port set in the device. In general, the index of the first port is 1.

PVC

The identifier of PVC for some port set in the device. In general, the index of the first PVC is 1; the number of PVC for one port can be up to eight.

VPI

The value of VPI set for this PVC.

VCI

The value of VCI set for this PVC.

RFC2684 Bridge Mode

This setting could be *LLC* or *VC Multiplexing*.

Channel

The channel mode set for the port, only interleaved or fast mode.

VLAN

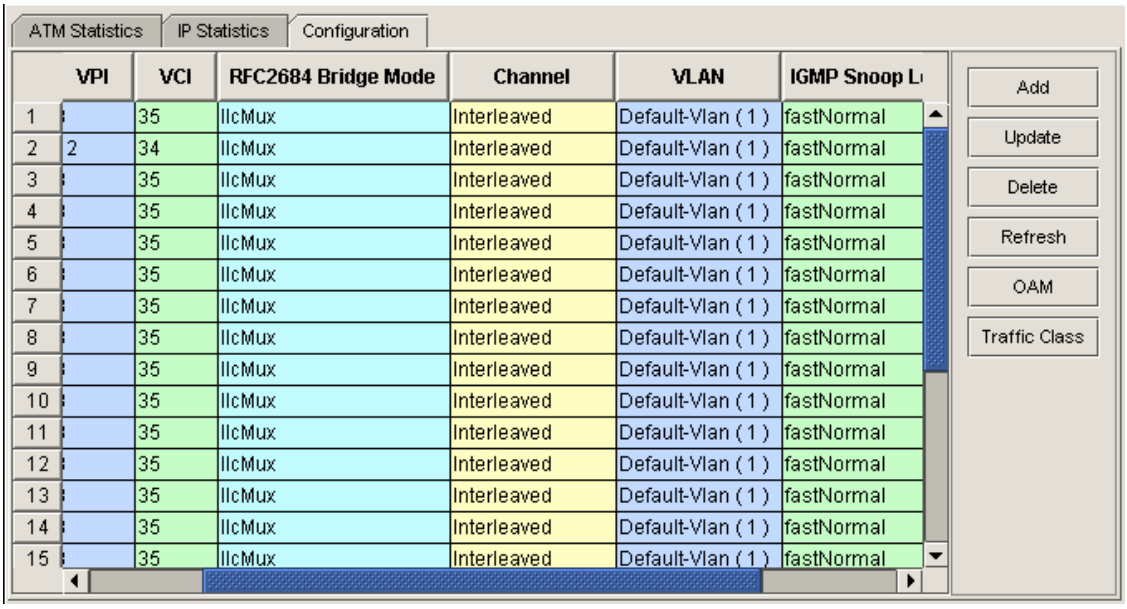
The VLAN ID set for the PVC set in the port. This value should be set in the Bridge configuration.

IGMP Snoop Leave Mode

The mode of IGMP Snoop leave mode set in the PVC should be ***normal***, ***fast*** and ***fastNormal***.

OAM

This function provide F5 loop-back test for one port. If the port is not connected, this function could not be performed.



	VPI	VCI	RFC2684 Bridge Mode	Channel	VLAN	IGMP Snoop L
1		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
2	2	34	llcMux	Interleaved	Default-Vlan (1)	fastNormal
3		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
4		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
5		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
6		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
7		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
8		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
9		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
10		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
11		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
12		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
13		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
14		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal
15		35	llcMux	Interleaved	Default-Vlan (1)	fastNormal

Figure 4-24 PVC Configurations

Port Configuration

Port/Status

The status of the port selected in the **port number** field.

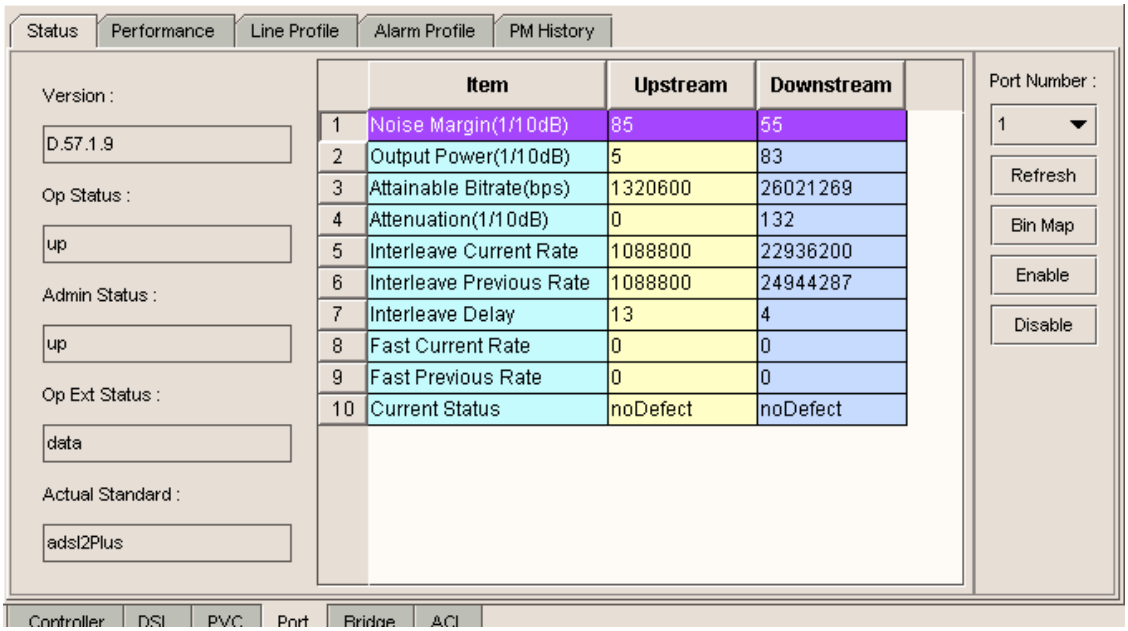


Figure 4-25 Port Status Configurations

Noise Margin(Up Stream/Down Stream)

Noise Margin as seen by this ATU with respect to it received signal. The unit is 1/10 dB.

Output Power(Up Stream/Down Stream)

Measured total output power transmitted by this ATU. This is the measurement that was reported during the last activation sequence.

Attainable Bitrate(Up Stream/Down Stream)

Indicates the maximum currently attainable data rate by the ATU.

Attenuation(Up Stream/Down Stream)

Measured difference in the total power transmitted by the peer ATU and the total power received by this ATU.

Interleave Curent Rate(Up Stream/Down Stream)

Actual transmit rate on this channel for interleave mode

Interleave Previous Rate

The rate at the time of the last **adslAtucRateChangev**Trap event for interleave mode. It is also set at initialization to prevent a trap being sent.

Interleave Delay

Interleave Delay for this channel.

Fast Current Rate

Actual transmit rate on this channel for fast mode

Fast Previous Rate

The rate at the time of the last **adslAtucRateChangeTrap** event for fast mode. It is also set at initialization to prevent a trap being sent.

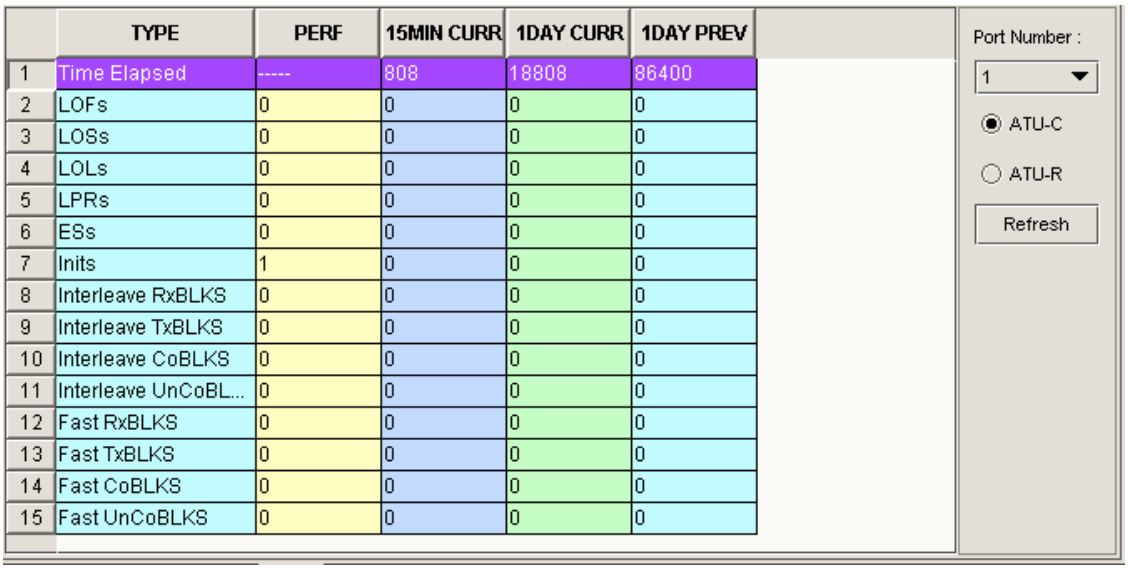
Current Status

Indicates the current status of the ATUC line. The values of status are described as followings:

Status		Meaning
0	**noDefect**	There are no defects on the line
1	**lossOfFraming**	The valid frames are not received in the ATUC
2	**lossOfSignal**	The valid signals are not received in the ATUC
3	**lossOfPower**	ATUC fails due to loss of power
4	**lossOfSignalQuality**	**Loss of Signal Quality** is declared when the Noise Margin falls below the Minimum Noise Margin, or the bit-error-rate exceeds 10^-7.
5	**lossOfLink**	**lossOfLink** is declared when ATUC can not link to ATUR
6	**dataInitFailure**	ATUC is failure during initialization due to bit errors corrupting startup exchange data.
7	**configInitFailure**	ATUC is failure during initialization due to peer ATU not able to support requested configuration
8	**protocolInitFailure**	ATUC is failure during initialization due to incompatible protocol used by the peer ATU.
9	**noPeerAtuPresent**	ATUC is failure during initialization due to no activation sequence detected from peer ATU.

Port/Performance

The performance of the port selected in the **port number** field, you can monitor the value for ATU-C or ATU-R by click the option for **ATU-C** or **ATU-R**. **Refresh** button is used to retrieve data again.



	TYPE	PERF	15MIN CURR	1DAY CURR	1DAY PREV
1	Time Elapsed	-----	808	18808	86400
2	LOFs	0	0	0	0
3	LOSs	0	0	0	0
4	LOLs	0	0	0	0
5	LPRs	0	0	0	0
6	ESs	0	0	0	0
7	Inits	1	0	0	0
8	Interleave RxBLKS	0	0	0	0
9	Interleave TxBLKS	0	0	0	0
10	Interleave CoBLKS	0	0	0	0
11	Interleave UnCoBL...	0	0	0	0
12	Fast RxBLKS	0	0	0	0
13	Fast TxBLKS	0	0	0	0
14	Fast CoBLKS	0	0	0	0
15	Fast UnCoBLKS	0	0	0	0

Figure 4-26 Port Performance Configurations

The time units' count for performance information includes **PERF, 15MIN CURR, 1DAY CURR and 1DAY PREV. The meanings for these time units are described as followings:**

PERF

The Count of the number about the parameters of the performance information is collected since agent reset

15MIN CURR

The Count of the number about the parameters of the performance information is collected during current 15 minutes

1DAY CURR

The Count of the number about the parameters of the performance information is collected during current 24 hours

1DAY PERV

The Count of the number about the parameters of the performance information is collected during previous 24 hours

The parameters of performance information are listed as followings:

Time Elapsed

The number of seconds that have elapsed count since the beginning of the current measurement period.

LOFs

The seconds for Loss of Framing failures count by ATUC .

LOSs

The seconds for Loss of Signal count by ATUC.

LPRs

The seconds for Loss of Power count by ATUC

ESs

The error seconds for CRC, anomalies, or other defects count by ATUC

Inits

The number of the line initialization attempts, including both successful and failed attempts, count by ATUC.

Interleave RxBLKs

The number of encoded blocks are received by ATUC in interleave mode

Interleave TxBLKs

The number of encoded blocks are transmitted by ATUC in interleave mode.

Interleave CoBLKs

The number of error blocks are corrected by ATUC in interleave mode.

Interleave UnCoBLKs

The number of error blocks can not be corrected by ATUC in interleave mode.

Fast RxBLKs

The numbers of encoded blocks are received by ATUC in fast mode

Fast TxBLKs

The numbers of encoded blocks are received by ATUC in fast mode

Fast CoBLKs

The numbers of error blocks are corrected by ATUC in fast mode.

Fast UnCoBLKs

The number of error blocks can not be corrected by ATUC in fast mode.

Port/Line Profile

The line parameters set for one port selected in the port number field, these parameters are defined in RFC 2662, for ADSL MIB. When you want to change the value of some parameter, you should click the **setting value** field, then input the new value and click **Apply** button. **Reset** button will restore the value.

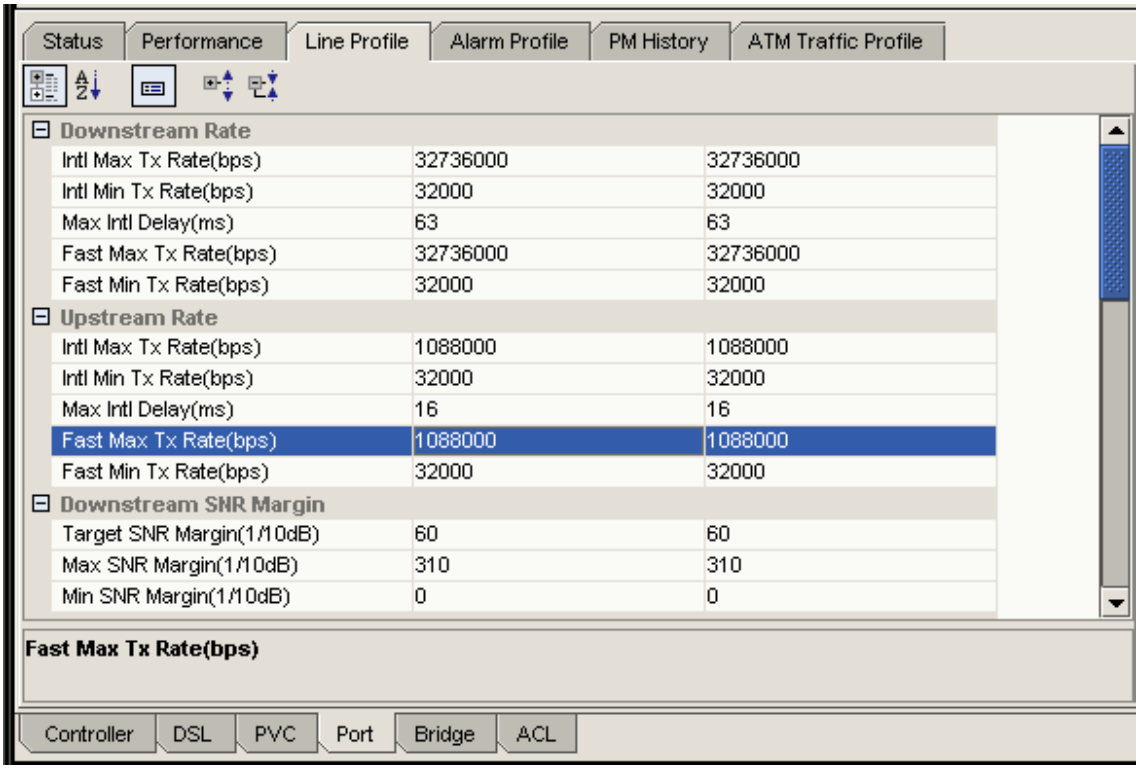


Figure 4-27 Line Profile Configurations

Downstream rate

Intl Max Tx Rate(bps)

Set maximum Transmit rate for Interleave channels in bps in the ATUC.

Intl Min Tx Rate(bps)

Set minimum Transmit rate for Interleave channels in bps in the ATUC.

Max Intl Delay(ms)

Set maximum Interleave delay for this channel in the ATUC

.

Fast Max Tx Rate(bps)

Set maximum Transmit rate for fast channels in bps in the ATUC.

Fast Min Tx Rate(bps)

Set minimum Transmit rate for fast channels in bps in the ATUC

Upstream rate

Intl Max Tx Rate(bps)

Set maximum Transmit rate for Interleave channels in bps in the ATUR.

Intl Min Tx Rate(bps)

Set minimum Transmit rate for Interleave channels in bps in the ATUR.

Max Intl Delay(ms)

Set maximum Interleave delay for this channel in the ATUR

.

Fast Max Tx Rate(bps)

Set maximum Transmit rate for fast channels in bps in the ATUR.

Fast Min Tx Rate(bps)

Set minimum Transmit rate for fast channels in bps in the ATUR

Downstream SNR Margin

Target SNR Margin(1/10 dB)

Set target signal/noise Margin in the ATUR

Max SNR Margin(1/10 dB)

Set maximum acceptable signal/noise Margin. If the Noise Margin is above this the modem should attempt to reduce its power output to optimize its operation in the ATUR.

Min SNR Margin(1/10 dB)

Set minimum acceptable signal/noise Margin. If the Noise Margin falls the level, the modem should attempt to increase its power output to optimize its operation in the ATUR.

Upstream SNR Margin

Target SNR Margin(1/10 dB)

Set target signal/noise Margin in the ATUC

Max SNR Margin(1/10 dB)

Set maximum acceptable signal/noise Margin. If the Noise Margin is above this the modem should attempt to reduce its power output to optimize its operation in the ATUC.

Min SNR Margin(1/10 dB)

Set minimum acceptable signal/noise Margin. If the Noise Margin falls the level, the modem should attempt to increase its power output to optimize its operation in the ATUC.

Advanced

Atuc Rate mode

Defines what form of transmit rate adaptation is configured on the ATUC. There are three modes defined as followings:
fixed (1): no rate adaptation

adaptAtStartup (2): perform rate adaptation only at initialization
adaptAtRuntime (3): perform rate adaptation at any time

Type

Defines the type of ADSL physical line entity, by defining whether and how the line is channel zed. The definitions for the type are:
noChannel (1): no channels exist
fastOnly (2): fast channel exists only
interleavedOnly (3): interleaved channel exists only
fastOrInterleaved (4): either fast or interleaved channels can exist, but only one at any time
fastAndInterleaved (5): either fast or interleaved channels exist

Annex

Set the annex type of ADSL line. The annex type includes **annexA(0),annexB (1),highSpeed (2),gspanPlus (3),v1010 (4) and adsl2(5**)

Standard

Provides actual standard used for the connection with AUTR. The definitions for the standard are as followings:
t1413(0)
gLite(1)
gDmt(2)
alctl14(3)
multimode(4)
adi(5)
alctl(6)
t1413auto(9)
adslPlus(48)
gspanPlus(64)
adsl2(26)
adsl2Plus(27)
readsl2(28)
adsl2Auto(29)
adsl2PlusAuto(30)

Trellis

Enable or disable the trellis coding.

EcFdmMode

Set if there is overlap or no overlap of bins. There are two modes for this parameter: **fdmMode and ecMode**.

PsdMaskType

Selects the PSD mask option to be used. This parameter is used only for G.Span/ ADSL+ and G.Span Plus. There are several modes including adsl, hsadslM1, hsadslM2, msk2Rfi, flatMskRfi, cabMsk2Rfi, coMsk2Rfi0, adsl2NonovlpM1, adsl2NonovlpM2, adsl2NonovlpFlat

UpStartBin

Lowest bin number allowed for Rx signal.

UpEndBin
Highest bin number allowed for Rx signal.

DownStartBin
Highest bin number allowed for Tx signal.

DownEndBin
Lowest bin number allowed for Tx signal.

SRA

Downshift SNR Mgn
Set signal/noise margin for rate downshift in the ATUC.

Upshift SNR Mgn
Set signal/noise margin for rate upshift in the ATUC.

MinDownshift Time
Set minimum time that the current margin is below **DownshiftSnrMgn** before a downshift occurs in the ATUC.

MinUpshift Time
Set minimum time that the current margin is above **UpshiftSnrMgn** before an upshift occurs in the ATUC.

Power Management

PM Mode
PM-related parameter used by the ATU-C to set the allowed link states. There are several modes including disable, l3enable, l2enable, l3|l2enable.

L0 Time(sec)
PM configuration parameter, related to the L2 low power state. This parameter represents the minimum time (in seconds) between an exit from the L2 state and the next entry into the L2 state.

L2 Time(sec)
PM configuration parameter, related to the L2 low power state. This parameter represents the minimum time (in seconds) between an Entry into the L2 state and the first Power Trim in the L2 state and between two consecutive Power Trims in the L2 State.

L2 ATPR(1/10dB)
PM configuration parameter, related to the L2 low power state. This parameter represents the maximum aggregate transmit power reduction (in dB) that can be performed through a single Power Trim in the L2 state.

L2 Min Rate(bps)
PM configuration parameter, related to the L2 low power state. This parameter specifies

the minimum net data rate during the low power state (L2). The data rate is coded in bit/s.

L2 Entry ThresholdRate(bps)

PM configuration parameter, related to the L2 low power state. This parameter specifies the downstream data rate threshold that triggers autonomous entry into low power state (L2). Supported for ADSL2/ADSL2plus ONLY.

L2 Exit ThresholdRate(bps)

PM configuration parameter, related to the L2 low power state. This parameter specifies the downstream data rate threshold that triggers autonomous exit from low power state (L2).

L2 Entry Rate MinTime(sec)

PM configuration parameter, related to the L2 low power state. This parameter specifies the minimum interval of time that the net data rate for the bearer channel should stay below Entry Threshold Rate before autonomous entry into low power state (L2). The minimum entry rate time is coded in seconds, and can range from 900 to 65535.

Port/Alarm Profile

The alarm parameters set for one port selected in the port number field, these parameters are defined in RFC 2662, for ADSL MIB. When you want to change the value of some parameter, you should click the **setting value** field, then input the new value and click **Apply** button. **Reset** button will restore the value.

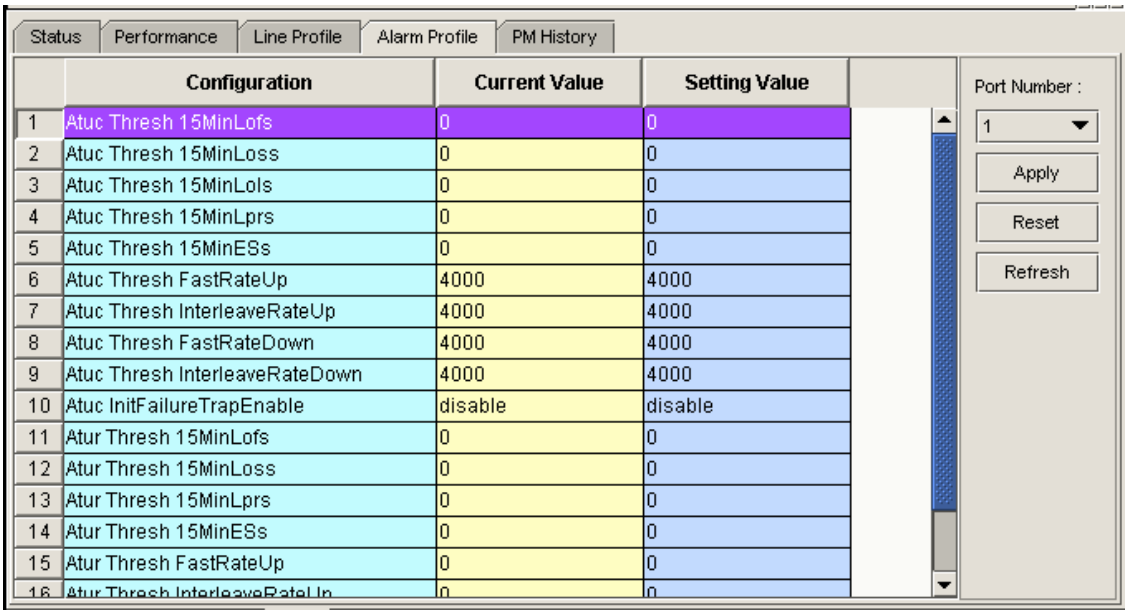


Figure 4-28 Alarm profile Configuration

Atuc Thresh 15MinLofs

The number of Loss of Frame Seconds encountered by an ADSL interface within any given 15 minutes performance data collection period, which causes the SNMP agent to

send an **adslAtucPerfLofsThreshTrap** in the ATUC.

Atuc Thresh 15MinLofss

The number of Loss of Signal Seconds encountered by an ADSL interface within any given 15 minutes performance data collection period, which causes the SNMP agent to send an **adslAtucPerfLossThreshTrap** in the ATUC.

Atuc Thresh 15MinLols

The number of Loss of Link Seconds encountered by an ADSL interface within any given 15 minutes performance data collection period, which causes the SNMP agent to send an **adslAtucPerfLolsThreshTrap** in the ATUC.

Atuc Thresh 15MinLors

The number of Loss of Power Seconds encountered by an ADSL interface within any given 15 minutes performance data collection period, which causes the SNMP agent to send an **adslAtucPerfLprsThreshTrap** in the ATUC.

Atuc Thresh 15MinLoESs

The number of Errored Seconds encountered by an ADSL interface within any given 15 minutes performance data collection period, which causes the SNMP agent to send an **adslAtucPerfESsThreshTrap** in the ATUC..

Atuc Thresh FastRateUp

Configure change in rate causing an **adslAtucRateChangeTrap** in the **Fast Mode**, this trap will be generated when the current channel transmit rate is greater than the previous channel transmit rate plus this parameter in the ATUC.

Atuc Thresh InterleaveRateUp

Configure change in rate causing an **adslAtucRateChangeTrap** in the **Interleave Mode**. this trap will be generated when the current channel transmit rate is greater than the previous channel transmit rate plus this parameter in the ATUC...

Atuc Thresh FastRateDown

Configure change in rate causing an **adslAtucRateChangeTrap** in the **Fast Mode**, this trap will be generated when the current channel transmit rate is less than or equal to the previous channel transmit rate minus this parameter in the ATUC.

Atuc Thresh InterleaveRateDown

Configure change in rate causing an **adslAtucRateChangeTrap** in the **Interleave Mode**, this trap will be generated when the current channel transmit rate is less than or equal to the previous channel transmit rate minus this parameter in the ATUC..

Autc InitFailureTrapEnable

Enables and disables the **InitFailureTrap** in the ATUC.

Atur Thresh 15MinLofs

The number of Loss of Frame Seconds encountered by an ADSL interface within any given 15 minutes performance data collection period, which causes the SNMP agent to send an **adslAturPerfLofsThreshTrap** in the ATUR.

Atur Thresh 15MinLofss

The number of Loss of Signal Seconds encountered by an ADSL interface within any given 15 minutes performance data collection period, which causes the SNMP agent to send an **adslAturPerfLossThreshTrap** in the ATUR..

Atur Thresh 15MinLols

The number of Loss of Link Seconds encountered by an ADSL interface within any given 15 minutes performance data collection period, which causes the SNMP agent to send an **adslAturPerfLolsThreshTrap** in the ATUR..

Atur Thresh 15MinLors

The number of Loss of Power Seconds encountered by an ADSL interface within any given 15 minutes performance data collection period, which causes the SNMP agent to send an **adslAturPerfLprsThreshTrap** in the ATUR.

Atur Thresh 15MinLoESs

The number of Errored Seconds encountered by an ADSL interface within any given 15 minutes performance data collection period, which causes the SNMP agent to send an **adslAturPerfESsThreshTrap** in the ATUR.

Atur Thresh FastRateUp

Configure change in rate causing an **adslAturRateChangeTrap** in the **Fast Mode**, this trap will be generated when the current channel transmit rate is greater than the previous channel transmit rate plus this parameter in the ATUR.

Atur Thresh InterleaveRateUp

Configure change in rate causing an **adslAturRateChangeTrap** in the **Interleave Mode**. This trap will be generated when the current channel transmit rate is greater than the previous channel transmit rate plus this parameter in the ATUR...

Atur Thresh FastRateDown

Configure change in rate causing an **adslAturRateChangeTrap** in the **Fast Mode**, this trap will be generated when the current channel transmit rate is less than or equal to the previous channel transmit rate minus this parameter in the ATUC.

Atur Thresh InterleaveRateDown

Configure change in rate causing an **adslAturRateChangeTrap** in the **Interleave Mode**, this trap will be generated when the current channel transmit rate is less than or equal to the previous channel transmit rate minus this parameter in the ATUC..

Port/PM History

The history performance of the port selected in the **port number** field, you can monitor the value for ATU-C or ATU-R by click the option for **ATU-C** or **ATU-R**. **Refresh** button is used to retrieve data again.

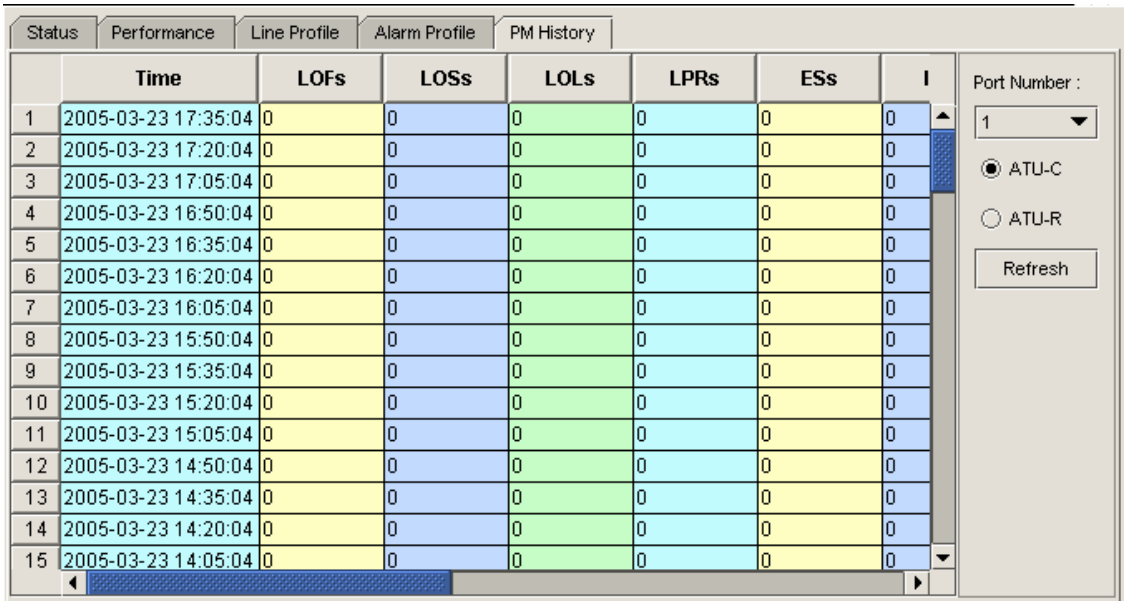


Figure 4-29 PM history Configuration

Port/ATM Traffic Profile

Select the “Port->ATM Traffic Profile” function enable the rate limitation for the ADSL line. This value should be less than the maximum value of **Atuc Fast Max Tx Rate** and **Atuc Intl Max Tx Rat.**

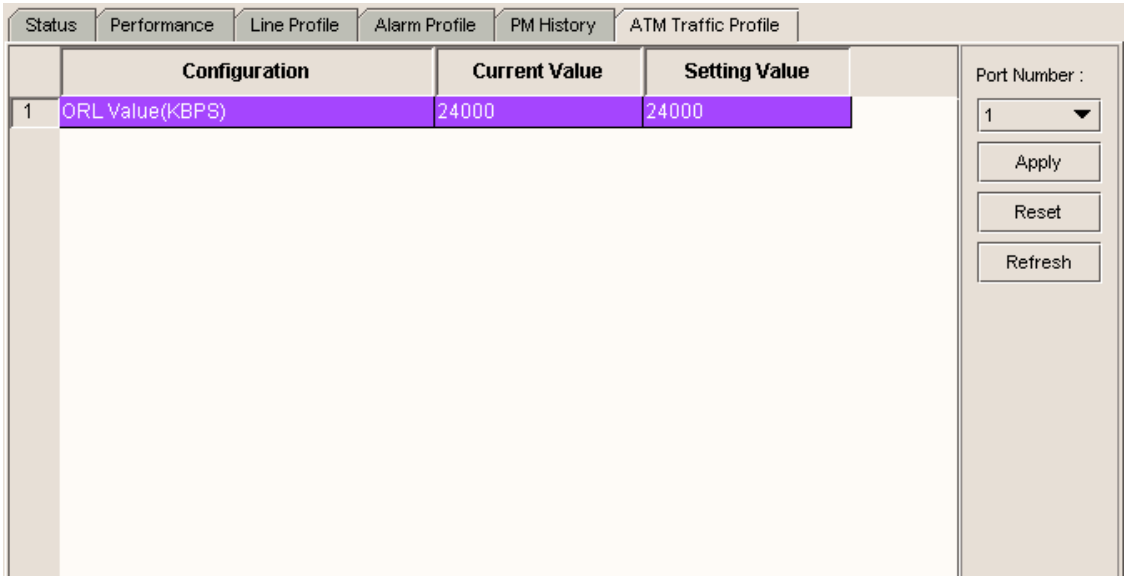


Figure 4-30 The ATM Traffic Profile

Bridge Configuration

Bridge/Static Unicast

Set the port, which the unicast packets can be sent with the **MAC address**.

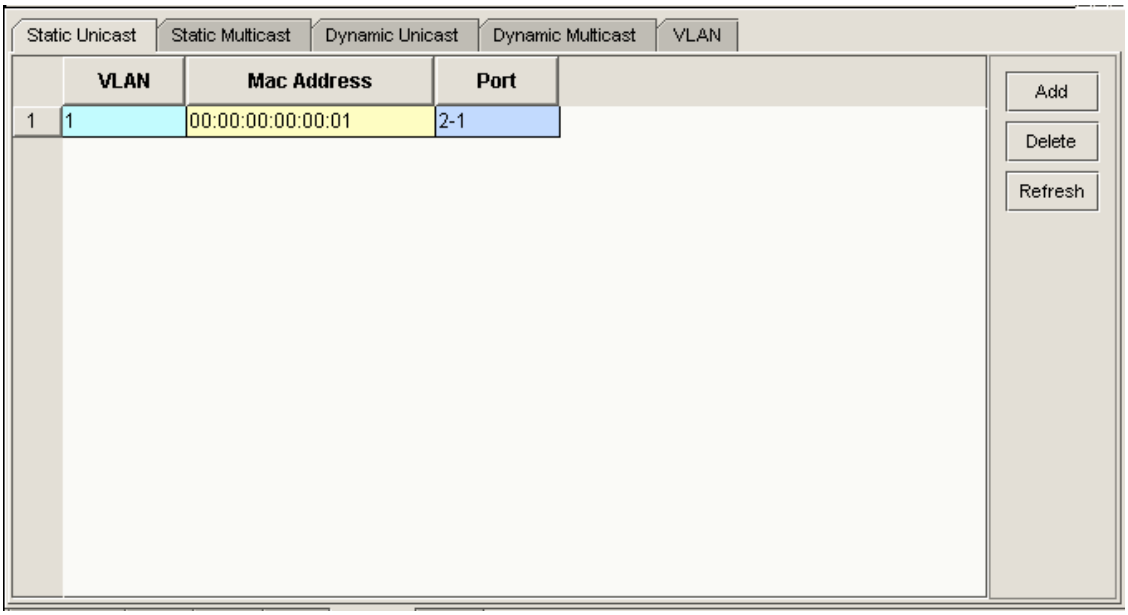


Figure 4-31 Static Unicast Configurations

VLAN

The VLAN ID associated with the unicast entry.

MAC Address

The MAC address associated with the unicast entry.

Port

The bridge port (PVC) associated with the unicast entry. The format is **portid-pvcindex,** the **portid** is the index of DSL port, and **pvcindex** is the index of PVC associated with this DSL port.

Add a Unicast Entry

When adding a new unicast entry, select **bridge->unicast** function first, then select **Add** button to input the VLAN, MAC and Port.

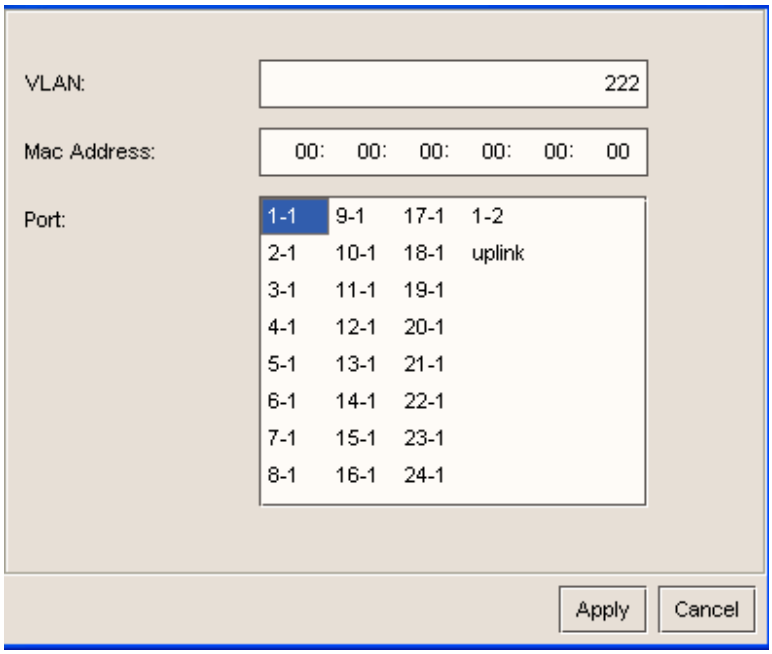


Figure 4-32 add a new unicast entry

Delete a Unicast Entry

Before deleting a unicast entry, use mouse to click the entry to be deleted, then select **delete** button to delete this entry.

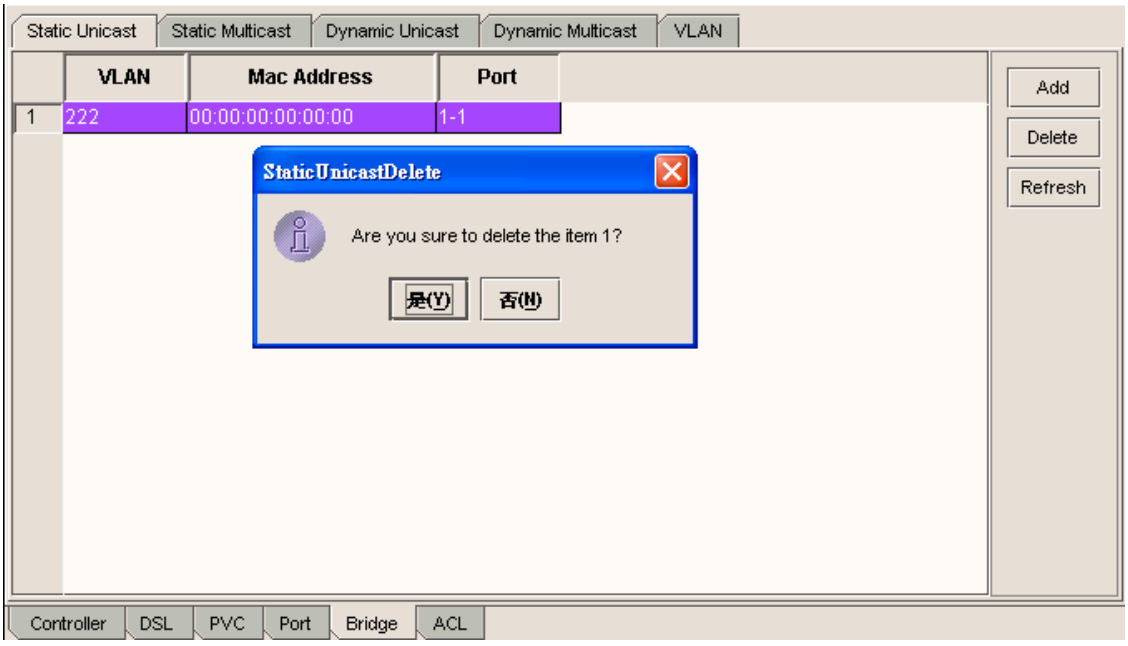


Figure 4-33 delete a unicast entry

Refresh the Unicast Entry

Select **Refresh** button to retrieve unicast entries from the device again.

Bridge/Static Multicast

Set the egress ports, which the multicast packets can be sent with the **MAC address**.

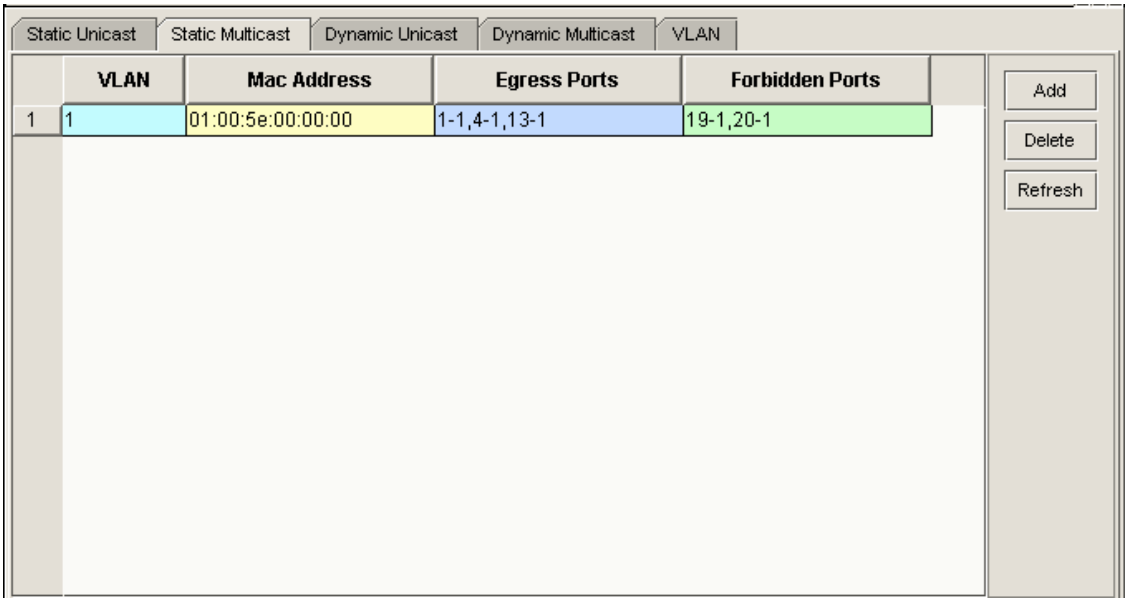


Figure 4-34 Static Multicast Configurations

VLAN

The VLAN ID associated with the multicast entry.

MAC Address

The MAC address associated with the multicast entry.

Egress Ports

Set the ports to which multicast packets can be sent.

Forbidden Ports

Set the ports that multicast packets can not be sent or received.

Add a Multicast Entry

When adding a new unicast entry, select **bridge->multicast** function first, then select **Add** button to input the VLAN, MAC, Egress Ports and Forbidden ports. The Egress ports and Forbidden ports can be multiple selections, using mouse and CTRL key to

select the ports.

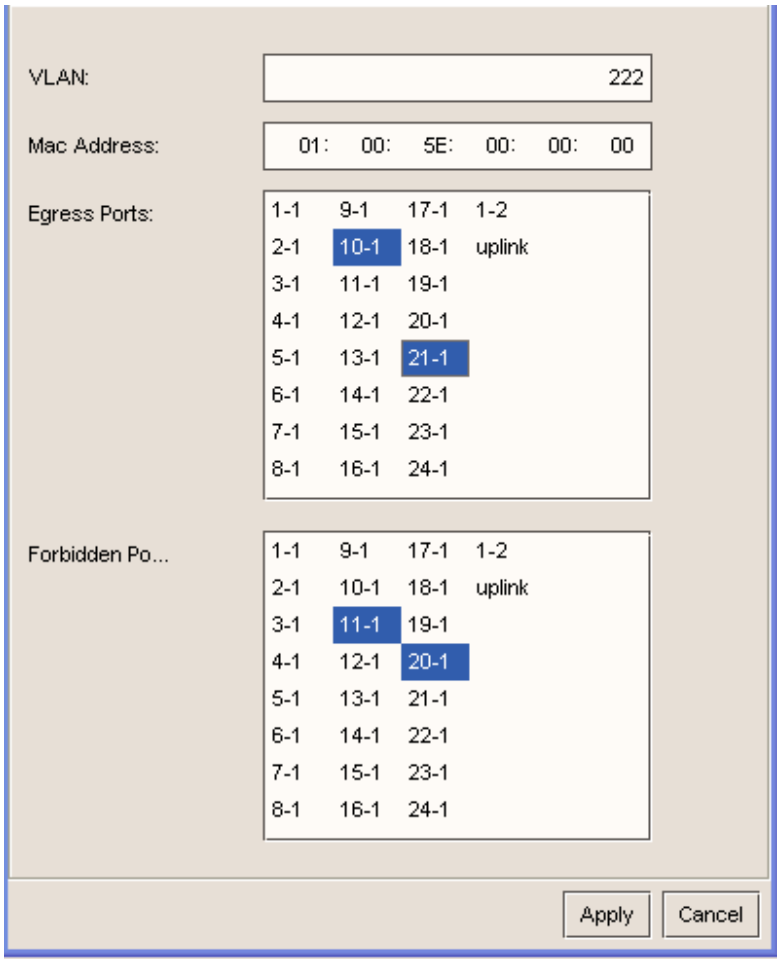


Figure 4-35 Static Multicast Configurations

Delete a Multiicast Entry

Before deleting a unicast entry, use mouse to click the entry to be deleted, then select **delete** button to delete this entry.

Refresh the Multiicast Entry

Select **Refresh** button to retrieve unicast entries from the device again.

Bridge/Dynamic Unicast

Show the map between the port and MAC address now.

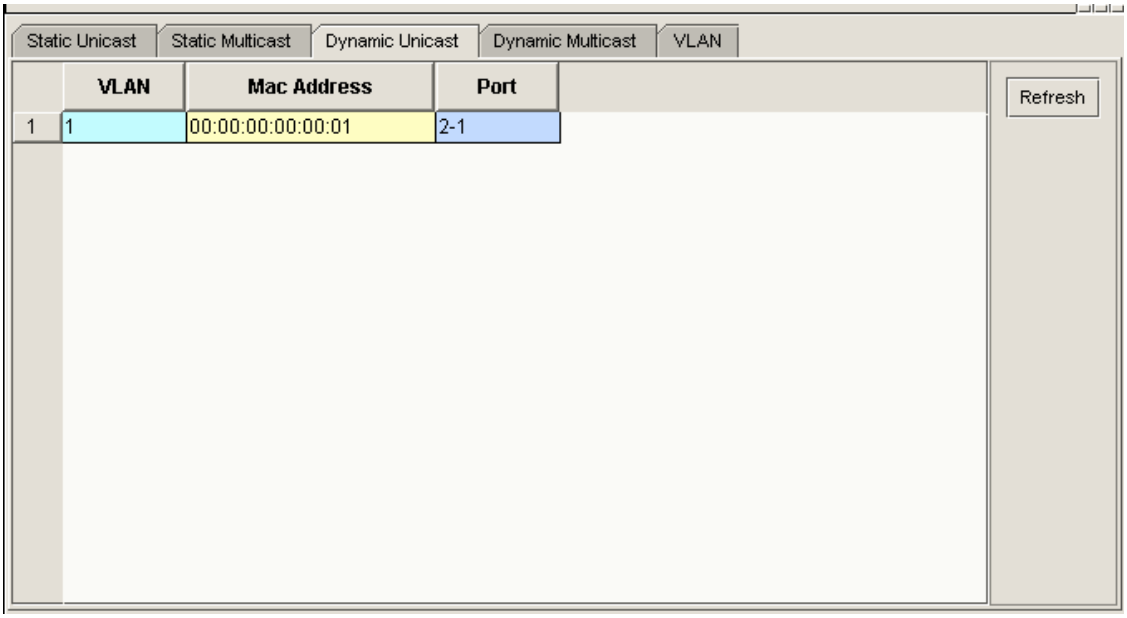


Figure 4-36 Dynamic Unicast Configurations

Bridge/Dynamic Multicast

Show the map between the ports and MAC address now.

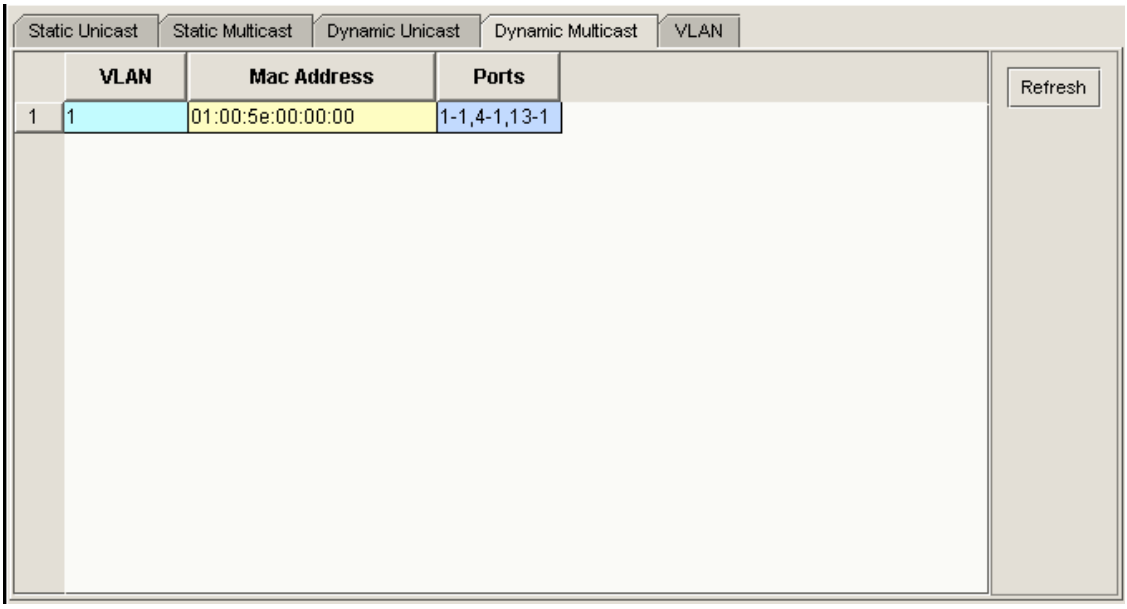


Figure 4-37 Dynamic Multicast Configurations

Bridge/VLAN

Set the VLAN ID list.

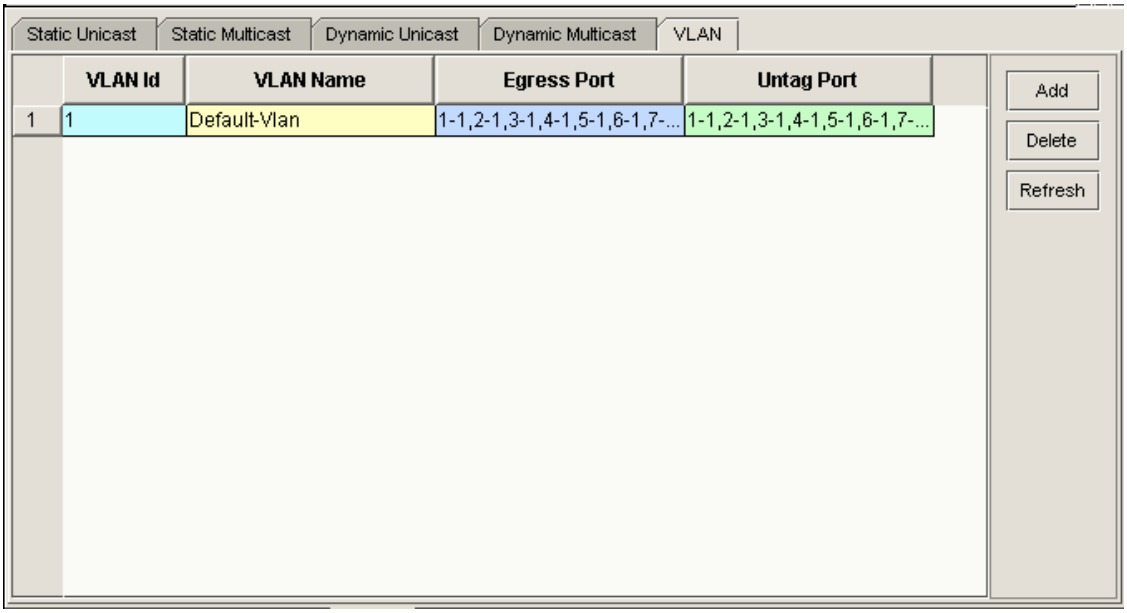


Figure 4-38 VLAN Configurations

VLAN

The VLAN ID associated with the VLAN entry.

VLAN Name

The name of VLAN associated with the VLAN entry.

Egress Port

Show the port to which packets with the VLAN ID can be sent.

Untag Port

Show the port to which packets with the VLAN ID can be sent and remove the VLAN tag.

Add a VLAN Entry

When adding a new VLAN entry, select **bridge->VLAN** function first, then select **Add** button to input the VLAN ID and the name of the VLAN entry.

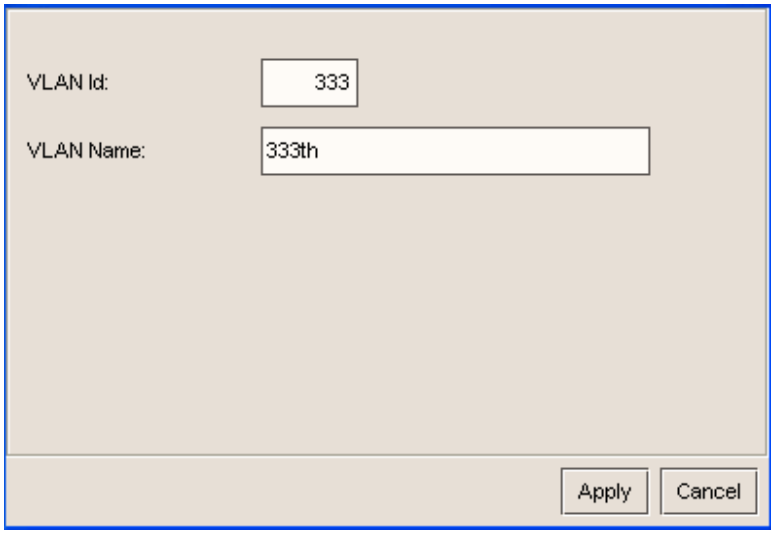


Figure 4-39 VLAN Configurations

Delete a VLAN Entry

Before deleting a VLAN entry, use mouse to click the entry to be deleted, then select **delete** button to delete this entry.

Refresh the VLAN Entry

Select **Refresh** button to retrieve VLAN entries from the device again.

ACL Configuration

ACL/ Deny

Deny the packets with MAC address from any ports.

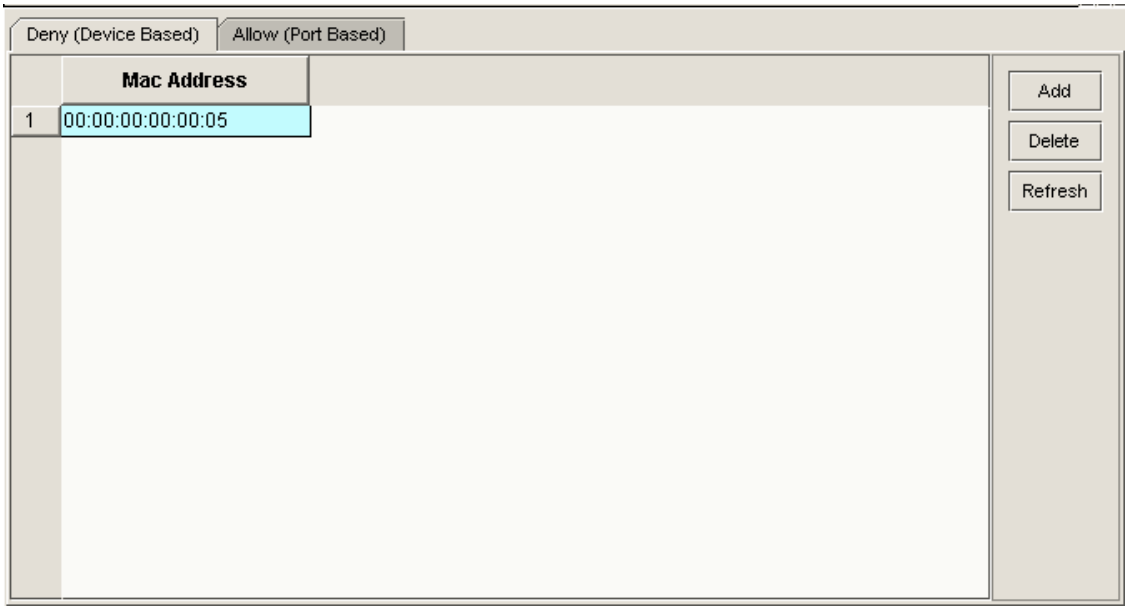


Figure 4-40 ACL Deny Configuration

MAC Address

If the source address of some packets with this MAC address, the packets will not be permitted to send or receive from any port of DSLAM.

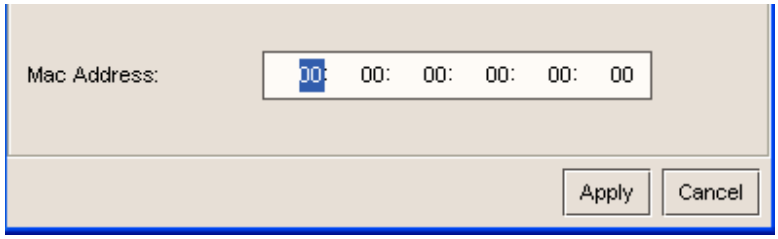


Figure 4-41 Add a MAC entry in the deny configuration

Add a MAC Entry

When adding a new VLAN entry, select **ACL->Deny (Device based)** function first, then select **Add** button to input the MAC address.

Delete a MAC Entry

Before deleting a MAC entry for deny, use mouse to click the entry to be deleted, then select **delete** button to delete this entry.

Refresh the MAC Entry

Select **Refresh** button to retrieve MAC entries from the device again.

ACL/ Allow

Allow the packets with MAC address from the port

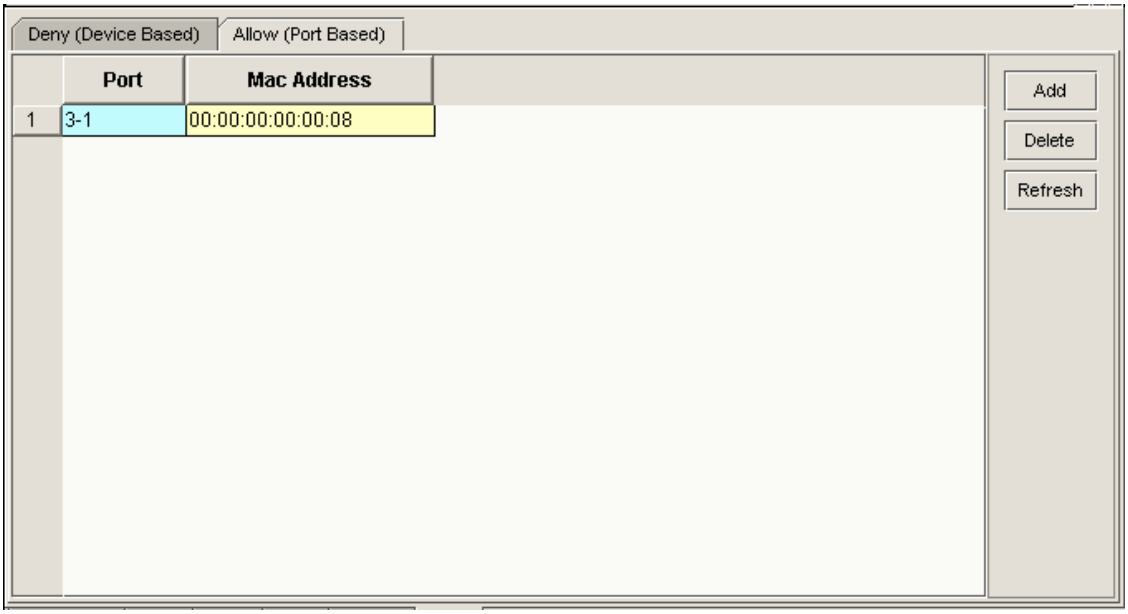


Figure 4-42 ACL Allow Configuration

Port

Set the DSL port to which packets can be permitted sent with the MAC address.

MAC Address

Set the MAC address with which packets are allowed to send to some port of DSLAM

Add

When adding a new MAC entry, select **ACL->Allow (Port based)** function first, then select **Add** button to input the MAC address and port.

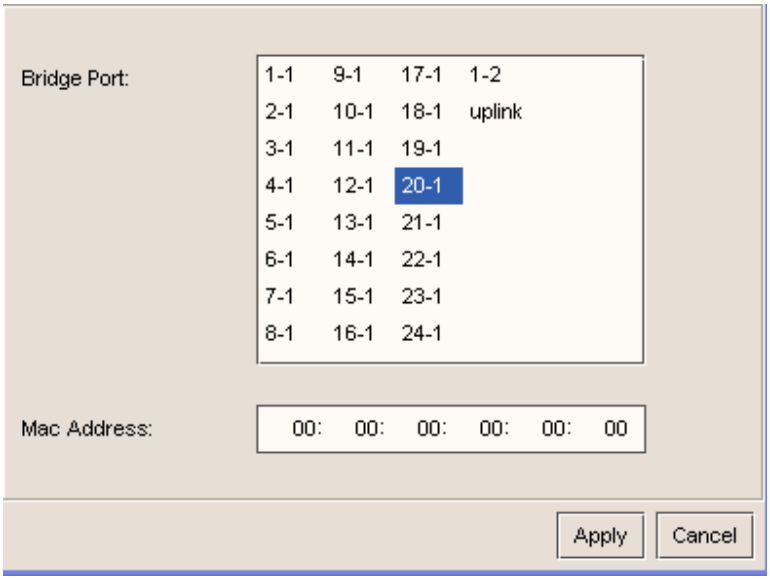


Figure 4-43 ACL Allow Configuration

Delete

Before deleting an allowed MAC entry, use mouse to click the entry to be deleted, then select **delete** button to delete this entry.

Refresh

Select **Refresh** button to retrieve allowed MAC entries from the device again.

System Management

System management includes network utilities used for diagnose the devices.

Tools Function

Tools/ Ping Device

Ping the selected device.

Figure 4-44 Ping Tool

Tools/ Trace Route

Print the path to the selected device use trace route.

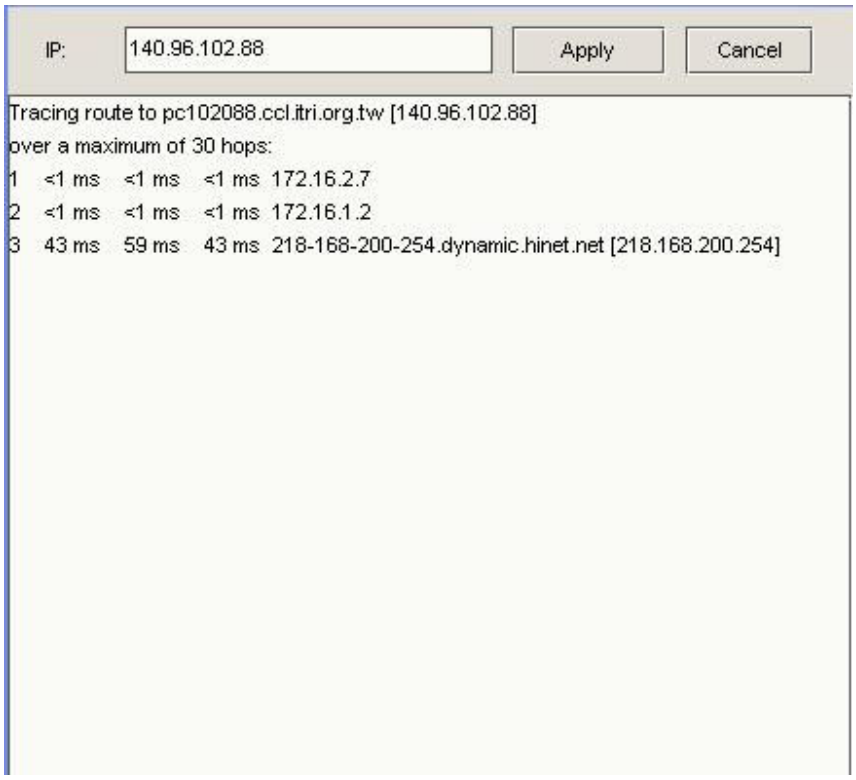


Figure 4-45 Trace Route Tool

Tools/ Telnet Device

Provide a telnet tool to the selected device.

Figure 4-46 Telnet Tool

Chapter 5

Security Management

Security management for EMS provides the authentication and authority for operators. The mechanism is role-based policy; it means that there are some roles built in advance. When creating a new role, we can assign some privileges to the role, so there are roles defined in the system. There is two default roles defined in the system: administrator and user. These roles are used when adding a user, that is, this user must be assigned to some role, and so he or she can execute some functions permitted by the role.
This chapter describes all security management functions; these functions are used only for administrator.

User Management

User management includes add, delete update and query users. When you click the main menu item **Advance->System manager,** you will see the function list under the tree folder in the left panel of the system manager window. Click the **System->User** under the tree will present a user list dialog box as Fig 5-1; the functions of user management are described as followings:

Insert user

Add a new user to the system, includes the fields: user name, password, e-mail, description and status. The type of all fields is **Text.**

Update user

Before selecting update operation, you should select one user you want to change in the user list, then press **Update** button in the top panel.

Delete user

Before selecting update operation, you should select one user you want to change in the user list, then press **Delete** button in the top panel.

User group assignment

When a new user is created, administrator could assign the user to a predefined group (role). Click the **System->User->User Group** under the tree will present a user list dialog box as figure 5-11 and you select one user from user list box and select available roles to the user. The default roles are **Administrator**, **operator** and **System administrator**.

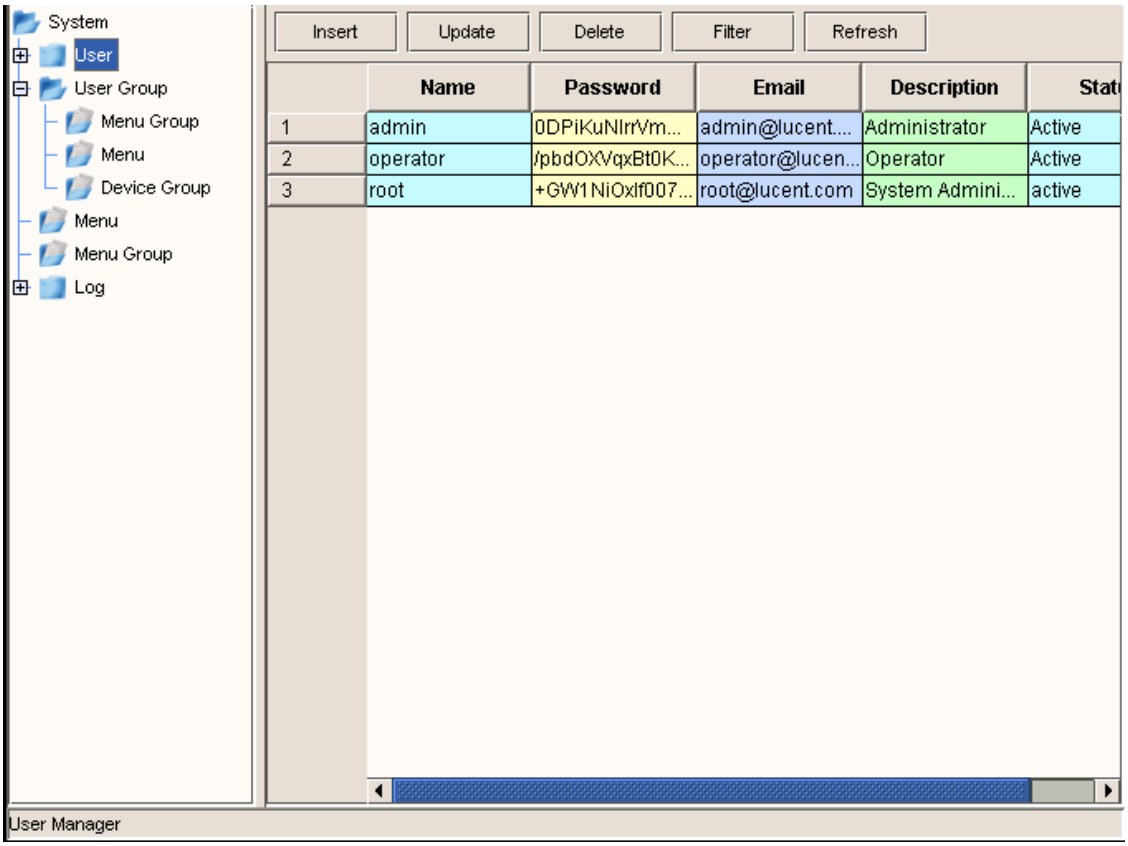


Figure 5-1 User Management Setup Window

Group Management

Group manage provide an interface to add, delete, modify group information. By the concept of group, we can create some resources used for groups. In this version of EMS, these resources are Application Functions and main menu functions. After create a group, some functions can be assigned to the group, so the user of this group can use these functions granted this group. The function for group and resource are described as followings:

Insert group

Add a new group to the system, includes the fields: group name.

Update group

Before selecting update operation, you should select one group you want to change in the user list, then press **Update** button in the top panel.

Delete group

Before selecting delete operation, you should select one user you want to change in the group list, then press **Delete** button in the top panel.

Function group assignment

When a new group is created, administrator could assign predefined function groups to this group. Click the **System->User Group->Function Group** under the tree will present a user list dialog box as figure 5-2 and you select one group from group list box and assign available function groups to this group. There are two modes for configuration: "*Device-View"* and "*Device-Modify"*. Assign "*Device-View"* for functions means that all functions can only be viewed only, while assign ""*Device-Modify"* means that all functions can be modified and viewed. The default user group *"Operator"* is set as *"Device-View",* So all users with *"Operator"* only can view the configuration.

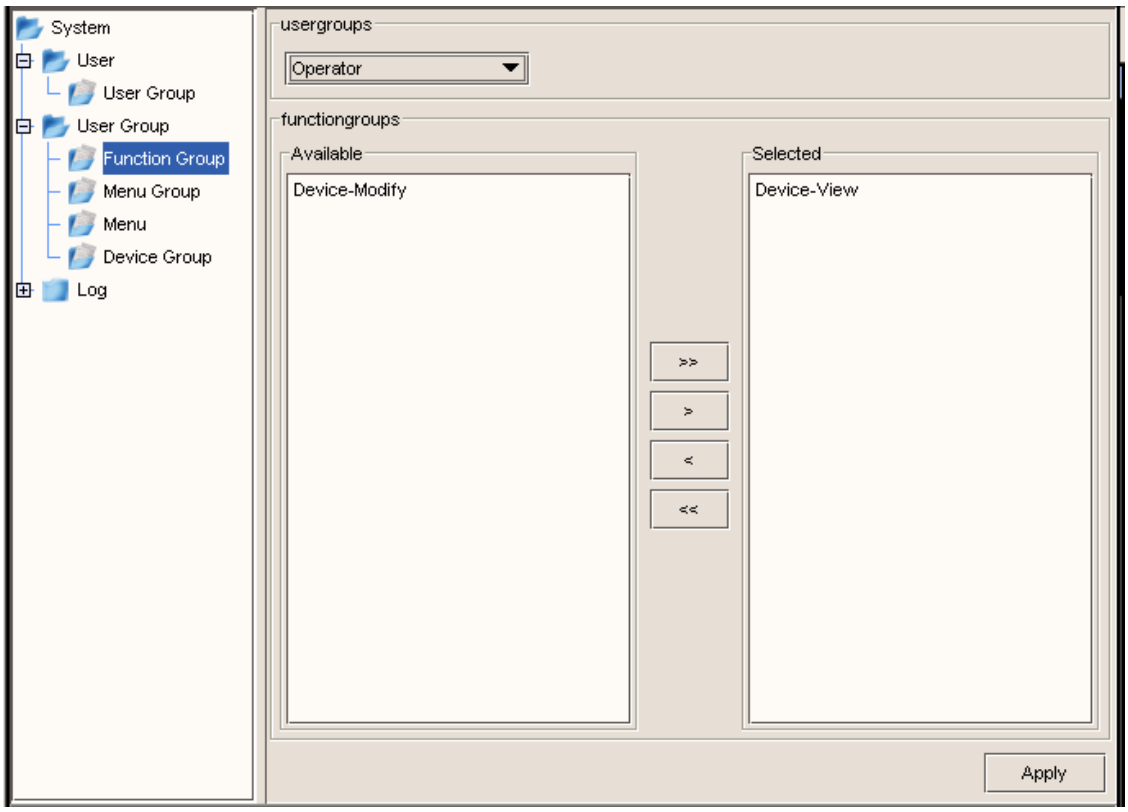


Figure 5-2 Function Group Assignment

Menu group assignment

When a new group is created, administrator could assign predefined menu groups to this group. Click the **System->User Group->Menu Group** under the tree will present a user list dialog box as figure 5-1 and you select one group from group list box and assign available menu function groups to this group.

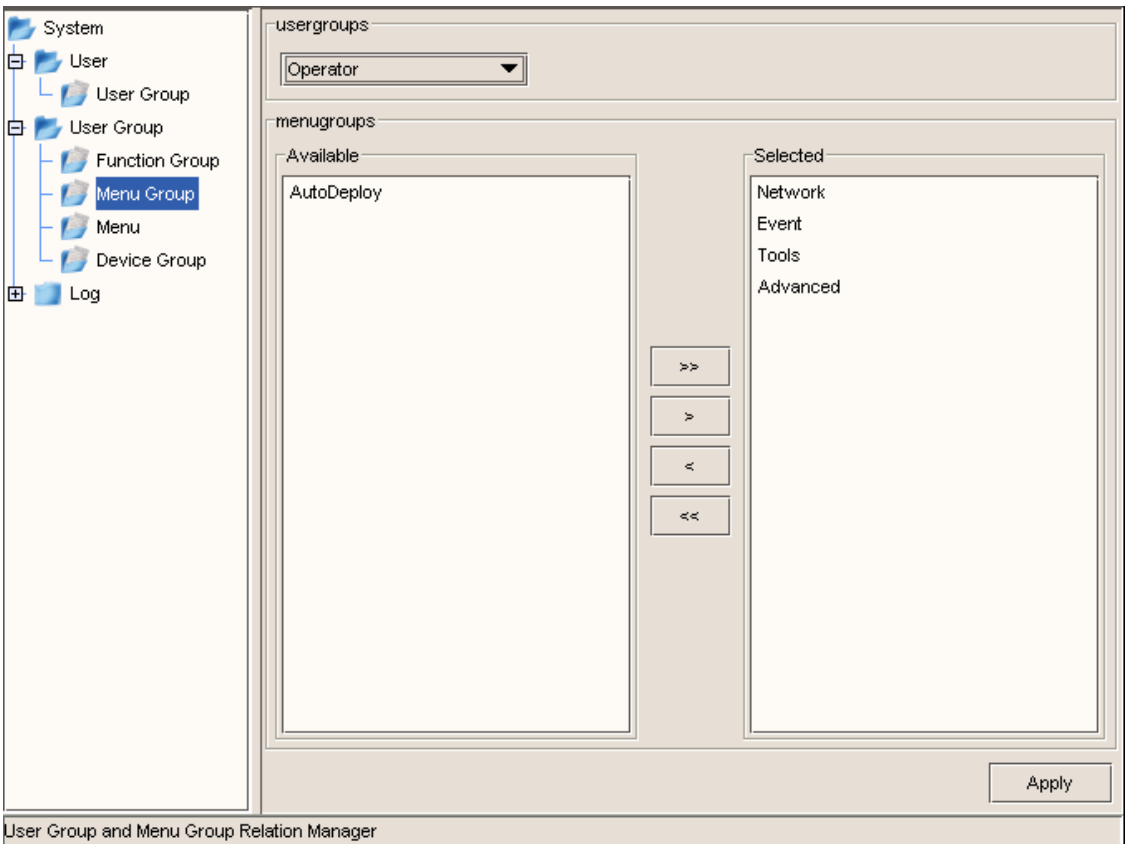


Figure 5-3 Menu Assignment

Device group assignment

The administrator can assign devices to some predefined user groups. Click the **System->User Group->Device Group** under the tree will present a user list dialog box as figure 5-1 and you select one group from group list box and assign available devices to this group.

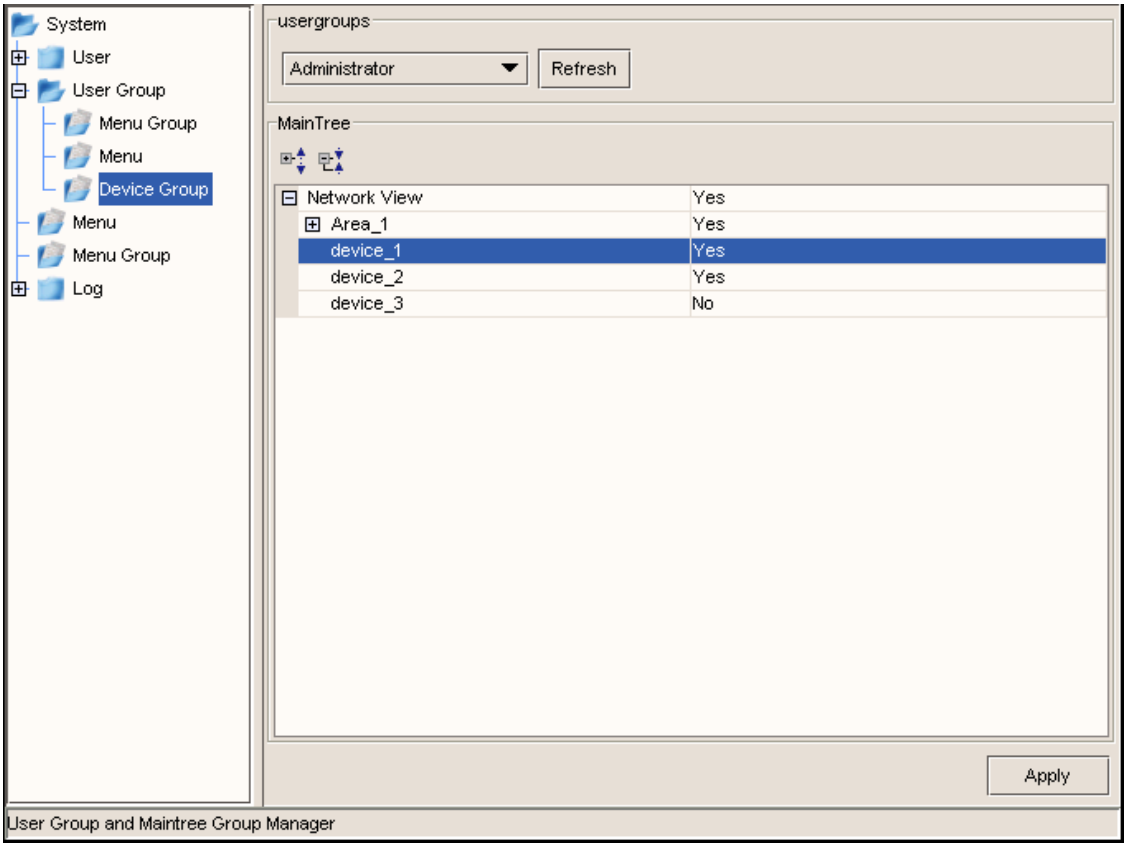


Figure 5-4 Device Group Setup Window

In this case, the device "**device_3**" is set as "**No**", so the users of **Administrator group** can not manage this device**.**

Resource Management

Resource management provides an interface to add, delete and modify resource information. The resource in the EMS includes Function Group and Menu Group. Click System->Function Group or System->Menu Group in the left panel will present the input dialog box. The functions for resource management are described as followings:

Insert resource

Add a new function group or menu group to the system includes the fields: function group name or menu group name.

Update resource

Before selecting update operation, you should select one group you want to change in the user list, then press **Update** button in the top panel.

Delete resource

Before selecting delete operation, you should select one user you want to change in the group list, then press **Delete** button in the top panel.

Menu assignment

When a new group is created, administrator could assign predefined menu groups to this group. Click the **System->User Group->Menu Group** under the tree will present a user list dialog box as figure5-3 and you select one group from group list box and assign available menu functions to this group.

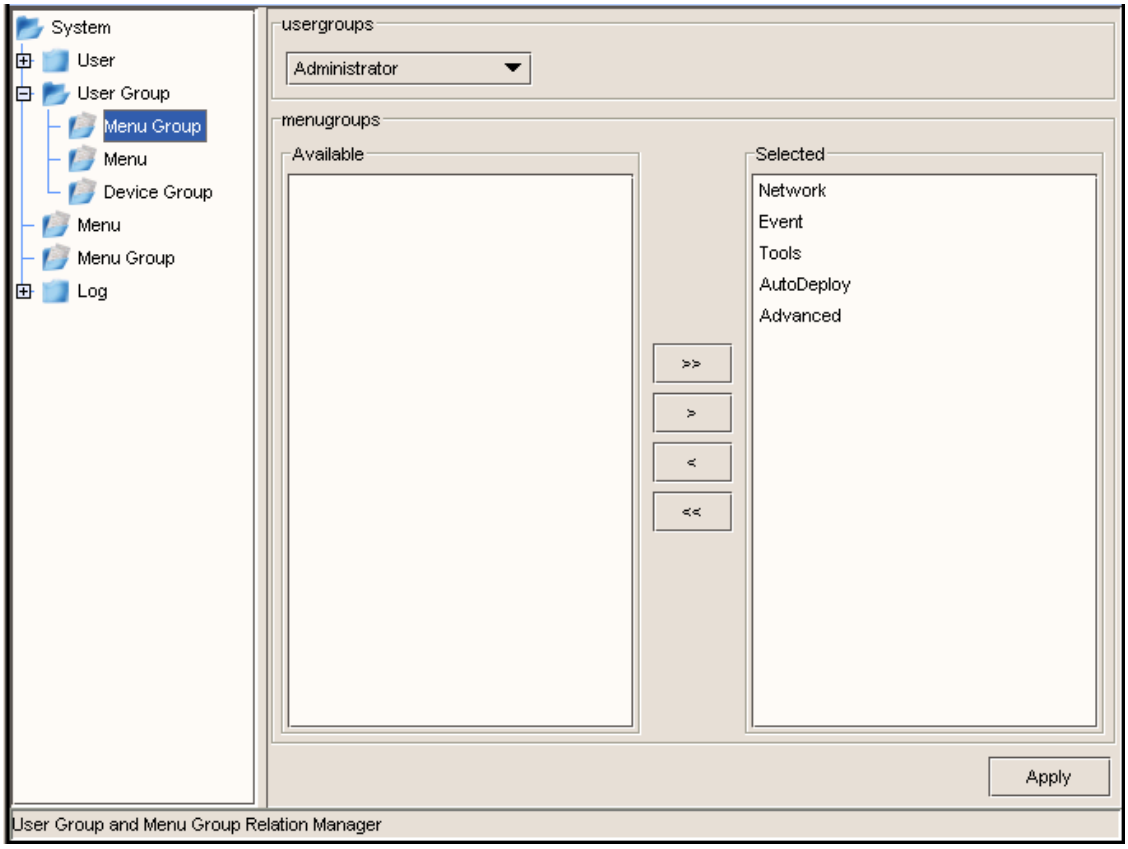


Figure 5-5 Menu Group Setup Window

Chapter 6

Monitor Management

Monitor management is a service located in the EMS server; it is responsible for viewing the status of managed devices and storing this information into the backend database, provides an interface to query. The information includes alarms, traps and the status. Monitor module will collect the information from devices and dispatch them to other modules such as alert system or northbound interface according to the property of the information.
This chapter describes the monitor system in the EMS, including polling function, alarm and trap notification function, and alarm filter for alerting.

Polling Device

EMS server sends some SNMP OIDs to the managed device to check if the device is failure or not in 5-minutes interval and sends notification the EMS client if the status of the device is changed. In the left panel you will see the alarms sent to EMS when polling service get the information. Another function is the LED panel when you select a device located in the tree. When you open a device box, you will see the LED changed in general.

Figure 6-1 Device Panel

Alarm

You can view alarms when you click the alarm panel in the bottom of the left panel or select the menu Event->Alarm View to see the traps received from devices. These alarms will be stored in backend database for query.

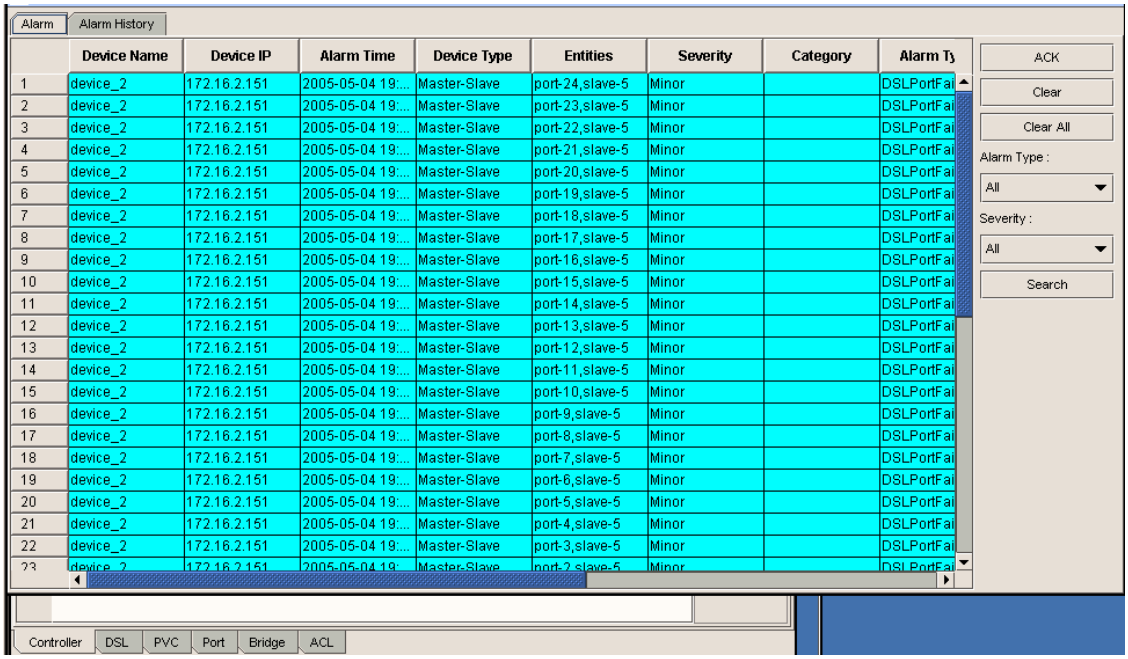


Figure 6-2 Alarm and Trap Window

Chapter 7

Topology Management

Topology management is the network map built in the system, when create management architecture for devices, sometimes some networks domain could be built for different zones. By the topology function, operator can manage devices easily. In the EMS client, administrator can edit the network map using the editor toolbox to build the link state, and some alarm icons located in the map so that operator can view the state of all devices located in the network domain. The topology is built only for administrator.
This chapter describes the topology functions in the EMS, including network domain creation, device auto discovery.

Network Map

Network map is the topology which illustrates the network architecture that EMS will manage. You can create this topology for manage issue for one zone or one area, and then use the editor toolbox to edit the map. The functions for network map are described as followings:

New Network

Create a new network domain for management. There exists a default root domain for use. If you do not want to create another network domain, you can use the root domain for your management domain.

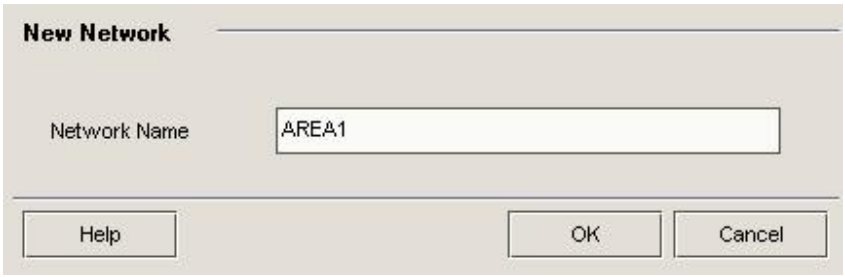


Figure 7-1 New Network Window

New Device

Create a new device under some network domain. The fields in the new device window are described as followings:

Display Name

The name of the device we want to connect. This value is set when new a device.

Device Type

The type of the device we want to connect. This value is set when new a device.

Sys Name

The name of the device we want to connect. This value is set when new a device.

IP

The IP address of the device we want to connect.

Read Community

The community set for read operations from EMS to device in SNMP. This value should be set the same as that of the device. If the community set in EMS is not the same as that of the device, this operation will be rejected.

Write Community

The community set for write operations from EMS to device in SNMP. This value should be set the same as that of the device. If the community set in EMS is not the same as that of the device, this operation will be rejected.

SNMP Port

The listening port of SNMP agent located in the device.

SNMP Version

The version of SNMP set in EMS used to communicate with the device.

Login user

The login user name used to login to the device.

Login password

The login password used to login to the device.

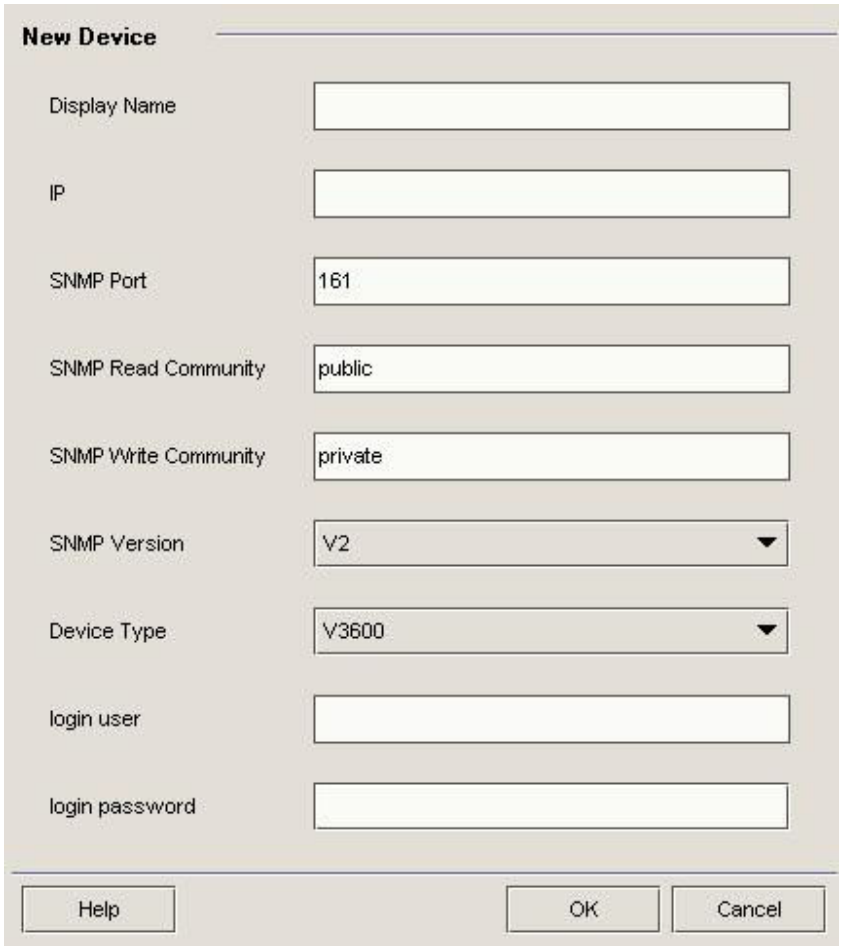


Figure 7-2 New device Setup Window

PVC Lookup

When you create a network domain, a network domain window will be presented if you click the network domain in the left panel of the main window. When you new devices under this map, you will see a new icon presented in the map. You can move the devices and draw lines to all devices intent for connection. The functions for this editor are described as followings:

Search

Search if there exist any PVC with the key word input in the database.

Find

Find the device in the network map and open the device panel.

Close

Close the PVC Lookup dialog.

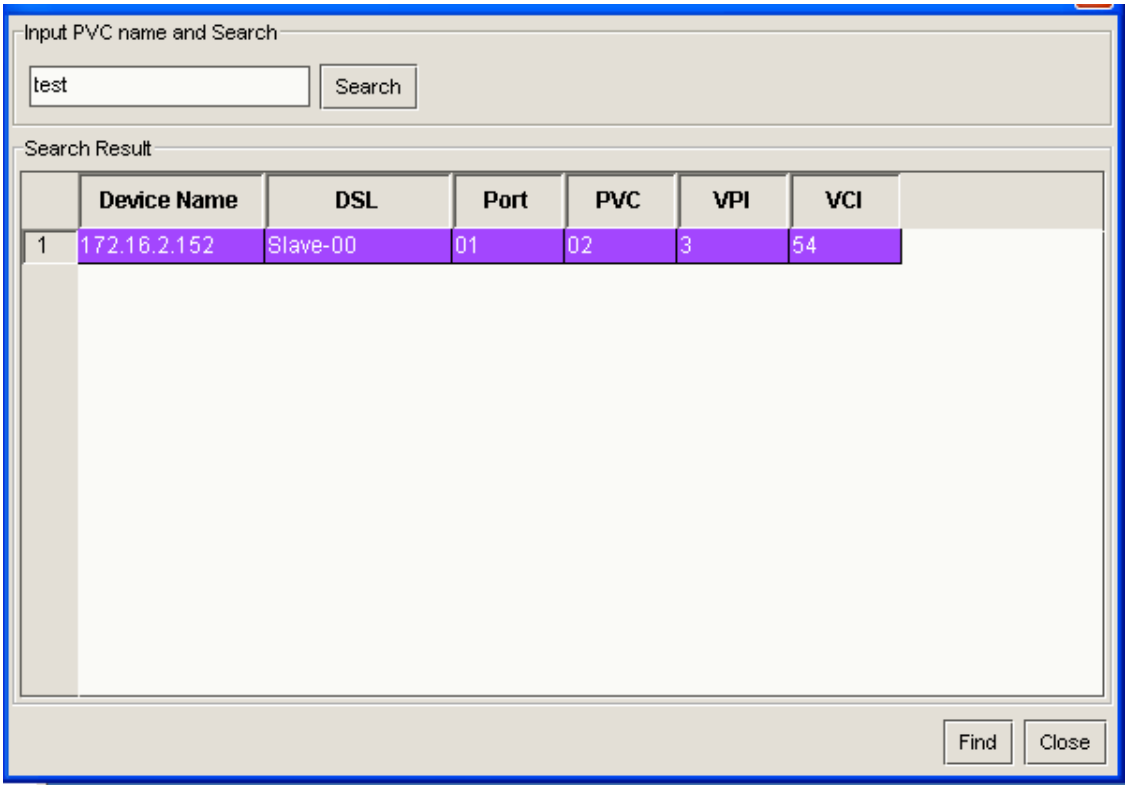


Figure 7-3 PVC Lookup window

Auto Discovery

When you want to know how many devices in the network or want to add them in the network. The auto discovery will let you see the list. The user may modify the default value of these values to add the selected devices to the network.

IP Address

Give an IP address for the engine to discover.

Subnet Mask

This is the subnet mask work with IP address. In Class C, you may type 255.255.255.0. You can specify the precise subnet mask such as 255.255.255.252 or 255.255.255.240.

Community

The read community for discover. The default value is public.

Auto Discovery

According to the ip address and subnet mask, start discovering.

Add

When there are result list in the table or key in by user. Add these devices to the

network if these devices have not be added in the network.

Cancel

Cancel the discovering action.

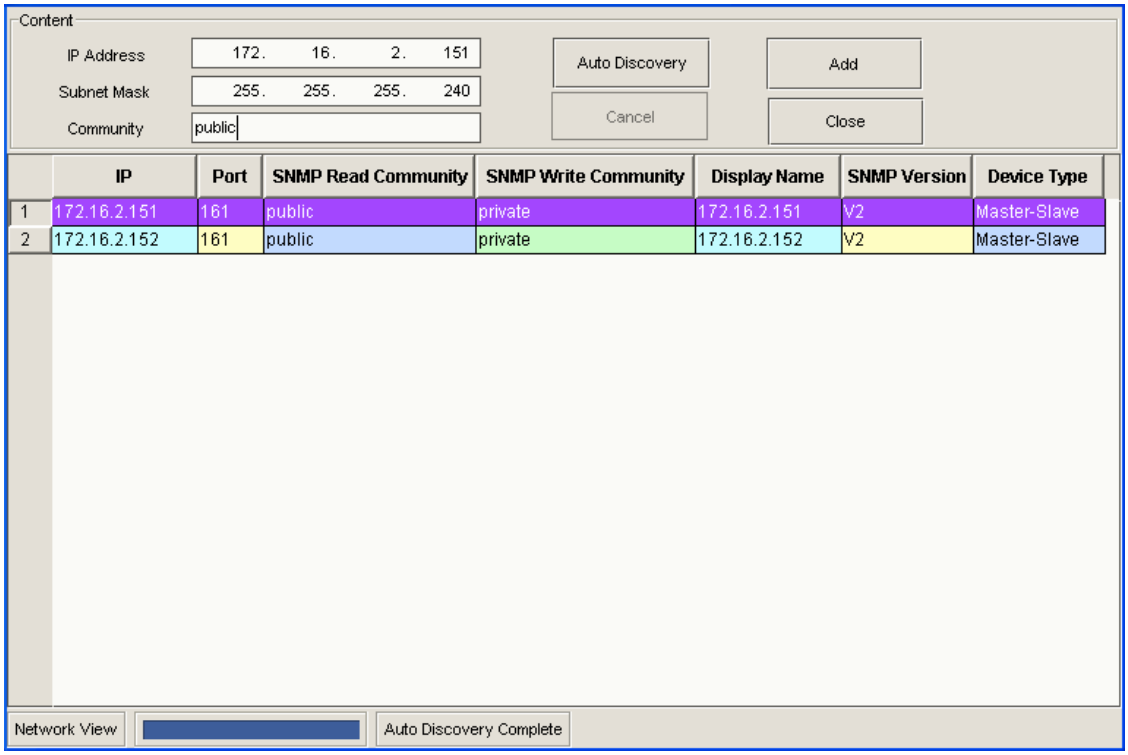


Figure 7-5 Auto Discovery Window

Network Map Editor

When you create a network domain, a network domain window will be presented if you click the network domain in the left panel of the main window. When you new devices under this map, you will see a new icon presented in the map. You can move the devices and draw lines to all devices intent for connection. The functions for this editor are described as followings:

Save

Save the network map to the backend server if you change anything for it.

Find

Find the devices in the network map.

Zoom In/Zoom Out

Zoom in or zoom out the map for inspect.

Line

Draw a line for link to the devices

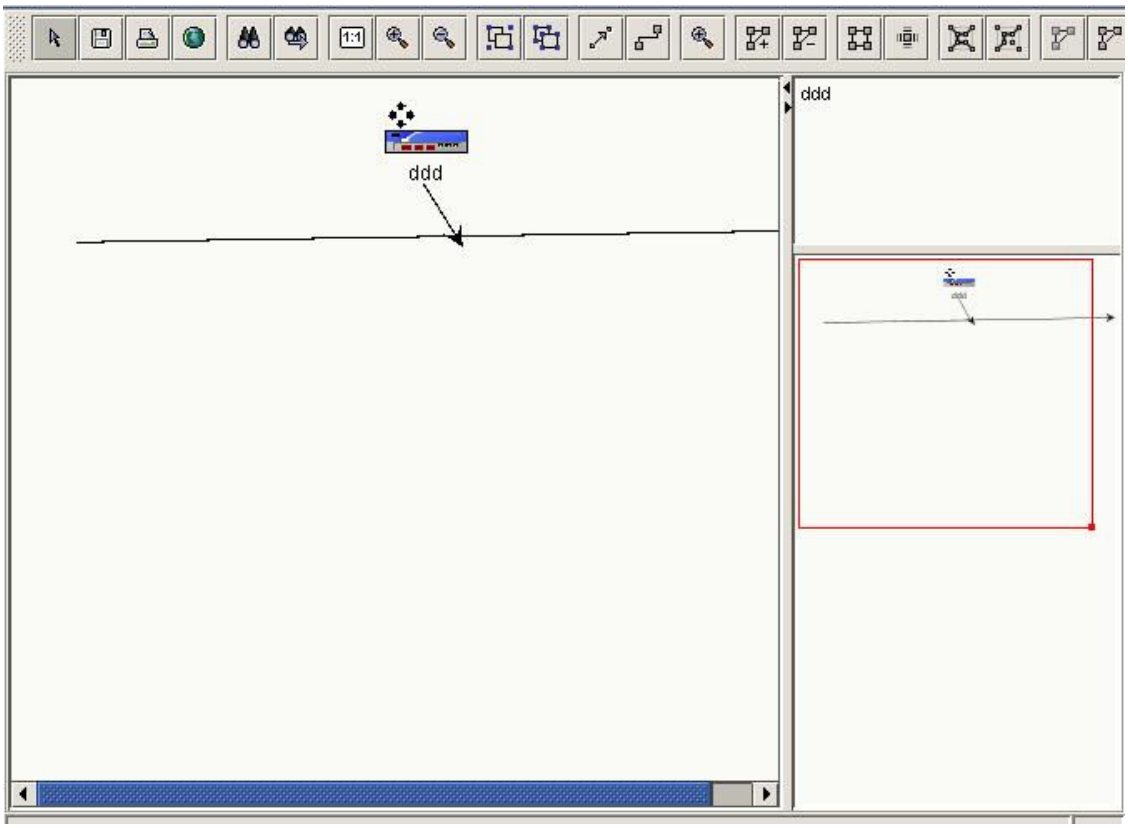


Figure 7-6 Network Map Editor Setup Window

Start Time

The time the job will be started.

Loop Count

The count for the scheduled job will be executed during the scheduling time.

Loop Interval

The interval for the scheduled job will be executed during the scheduling time.

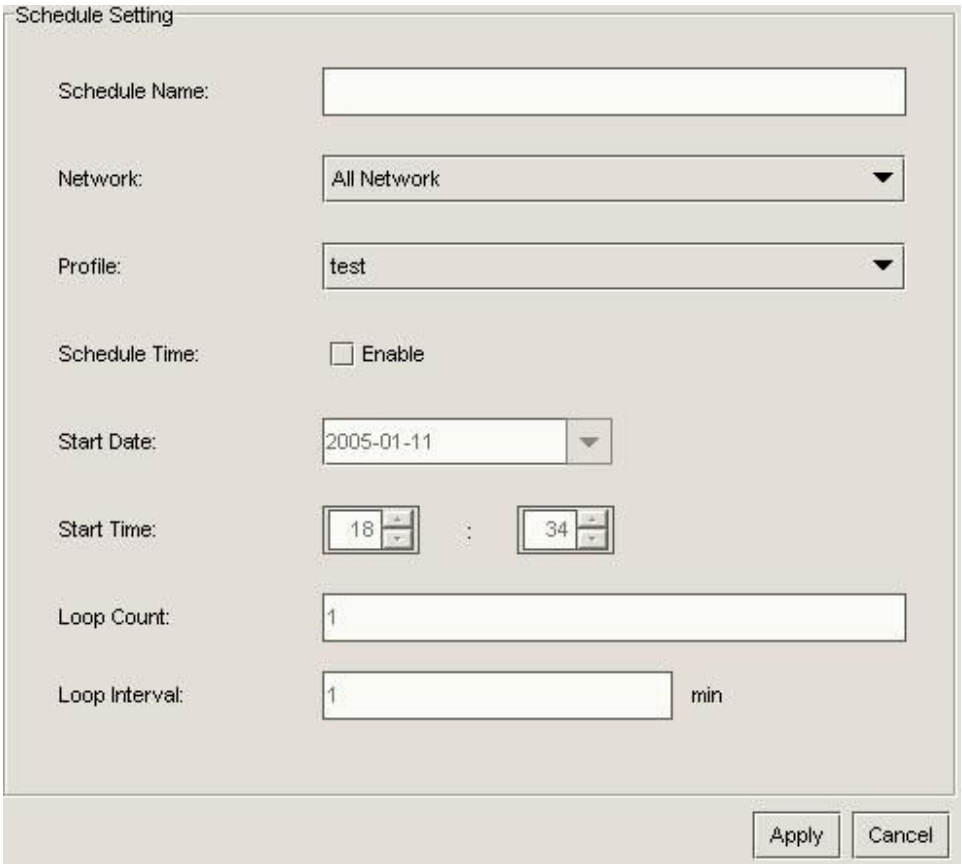


Figure 7-7 Scheduler Setup Window

Log for deployment

For auto deployment, there are some failures for some reasons. EMS server will keep the error logs if any unexpected exception occurs in some phase. EMS provides a query interface for operators to query the error logs if necessary.

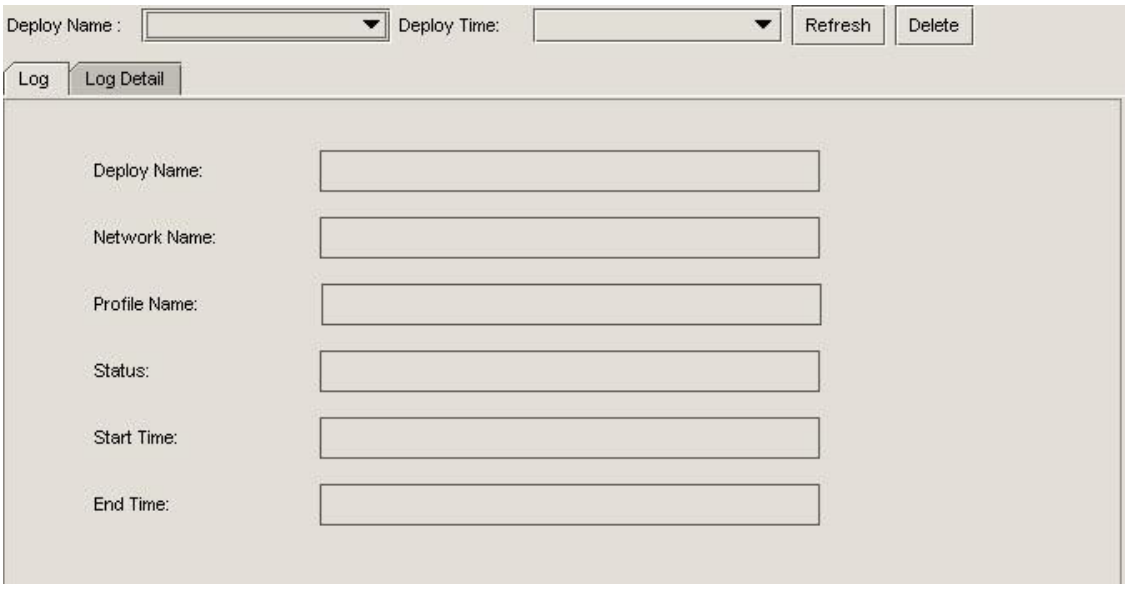


Figure 7-8 Log for deployment Window

Chapter 8

Log and Event Management

The function of Log and event management for EMS is to provide an interface for operators to query history events or user logs stored in the backend database. The events include history alarms and traps, while the content of user logs is the behaviour of login user. By the log, administrator can audit the behaviours of all users for some purposes. This chapter describes how to query history alarms, history traps and user logs.
EMS client provide a GUI for operators to input the filter conditions for query.

Event management

Event management includes the history alarms and history traps, stored in the backend database. EMS provides a query interface for operators to query history alarm and traps.

Alarm management

Alarm management provides the query interface for active alarm and history alarm. Active alarms exist if the status of device has not been changed. If any clear alarm is received, then the active alarm will be removed from the active alarm list. All alarms will be kept in the database as history alarms. Click the alarm panel of bottom in left panel will present the alarm dialog box. The fields about alarm are described as followings:

Current Alarm

The current alarms are new raised events from the managed devices. Figure 6-2 is the current alarms from devices. The information about the current alarm is described as followings:

Device Name

Show the name of some device that raises this alarm.

Device IP

Show the IP of some device that raises this alarm.

Alarm Time

Show the time of this current alarm

Device Type

Show the type of some device that raises this alarm.

Entities

Show the objects that raises this alarm. The entities include the index of DSL port and the index of the slave device.

Severity

Show the level of the current alarm. The levels of severity defined in EMS are **warning, minor, major and critical.**

Alarm Type

Show the type of the current alarm. The types of alarm are:
DeviceFail: The device can not be accessed by EMS.
DSLFail: The DSL card of device can not be accessed by EMS.
DSLPortFail: The port of DSL card is failure for some reasons.
AtucLossTCA: Lost of signal occurs in the ATUC.
AtucLofsTCA: Lost of frame occurs in the ATUC.
AtucRateChange: The channel rate of ATUC is changed for some reasons.
AturRateChange: The channel rate of ATUR is changed for some reasons.
AtucLprsTCA: Lost of power occurs in the ATUC
AtucESsTCA: The error seconds count by the ATUC for some errors.
AturLossTCA: Lost of signal occurs in the ATUR.
AturLprsTCA: Lost of power occurs in the ATUR
AturESsTCA: The error seconds count by the ATUR for some errors.
Fanfail: The fan of device is failure for some reasons.
Fanstuck: The fan of device is failure for some reasons.

Description

Show the detail of the current alarm.

Problem Cause

Show the reason what raise this alarm.

Ack Status

Show if this alarm is acknowledgement or not by some user.

Ack User

Show the user who acknowledged this current alarm.

Ack Time

Show the date time that this alarm is acknowledged.

Alarm filter

EMS provides the alarm filter function to view the current alarms for convenient ion. The factors for filter are **alarm severity** and **alarm type**. By filter, you can only view the current alarms match these filters.

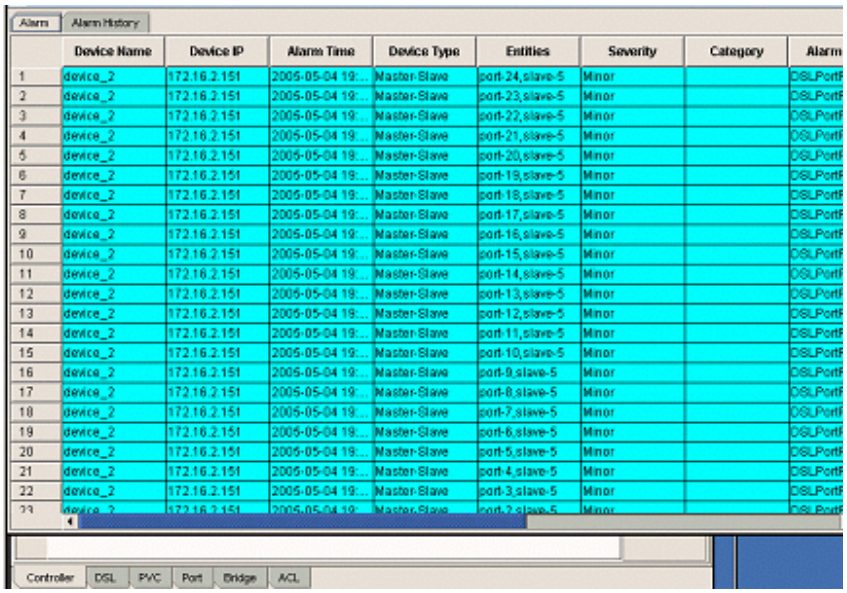


Figure 8-1 Current Alarm Window

History Alarm

History alarms are collected by EMS server for a long time and keep the information to the backend database. If one current alarm has been cleaned or regards as a history alarm for some reasons, then it is marked as “history” and keeps them into the backend database.

History alarms can be queried by the date/time, severity and type.

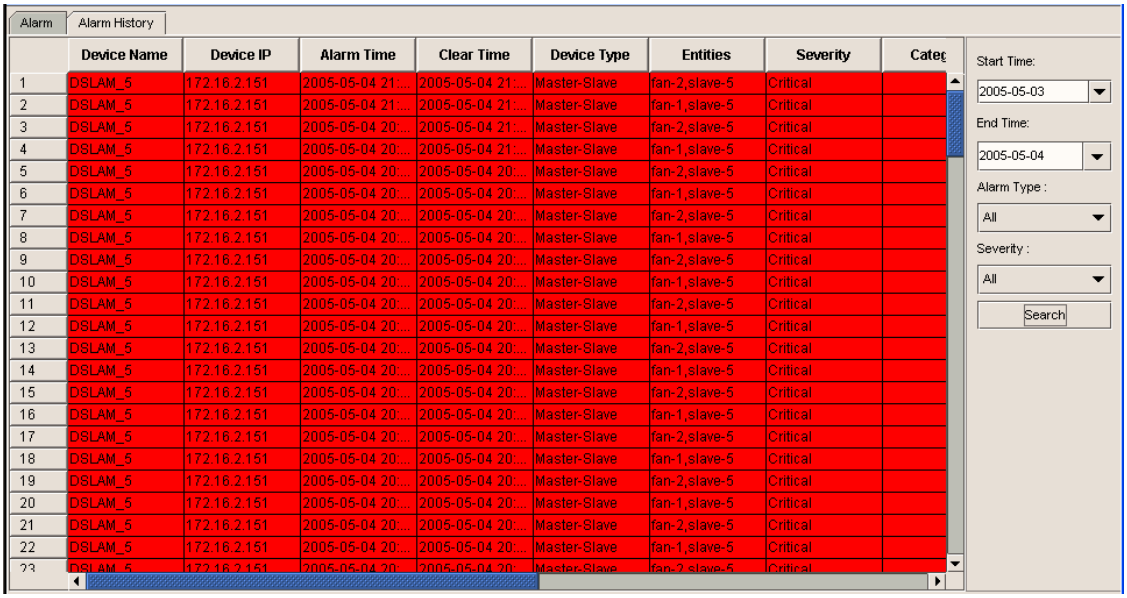


Figure 8-2 History Alarm Window

Trap management

The trap management includes trap view and query history traps. When you select Event->Trap View, a dialog box will be shown and list the current traps. The history traps are shown in the **Trap History View**.

The fields of this function are described as followings:

Trap Time

The timestamp of the trap is received.

Device Name

The name of the device raised this trap.

Device Type

The type of the device raised this trap.

Device IP

The IP of the device raised this trap.

Trap Name

The name of Trap is received by EMS.

Sys Uptime

The system uptime of the device raised this trap.

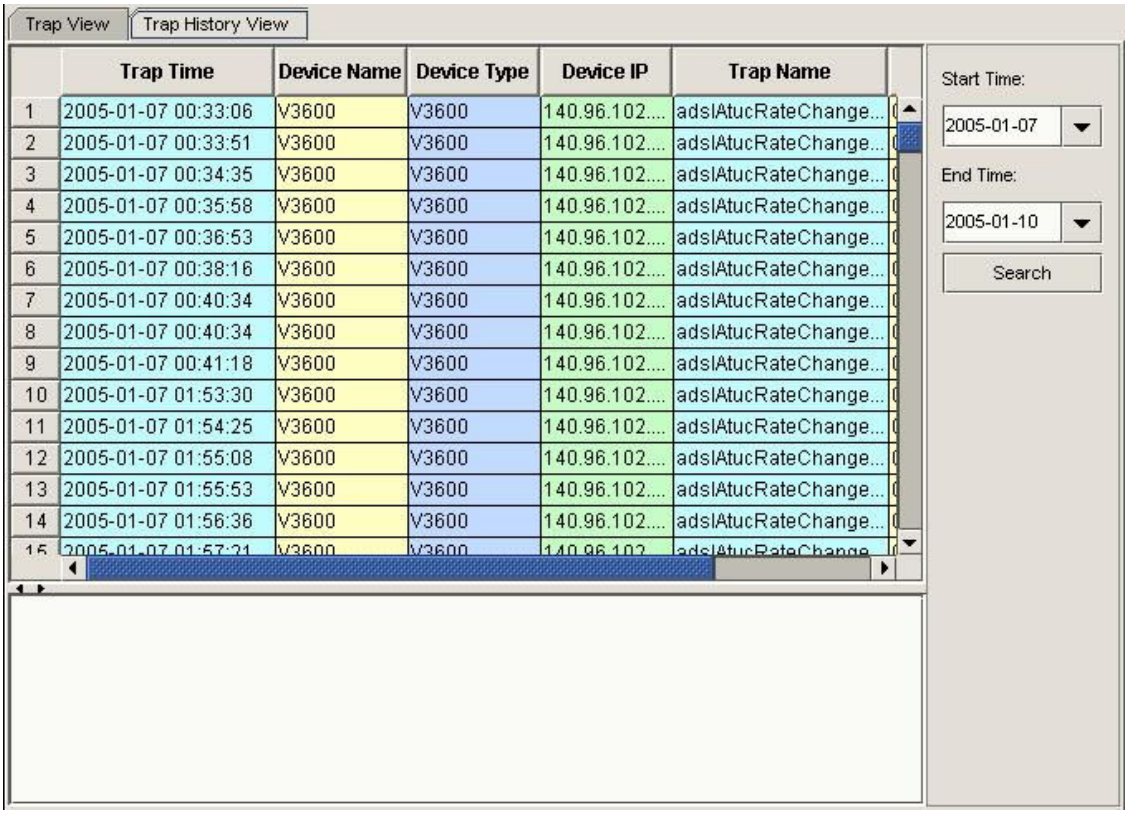


Figure 8-3 Trap query window

Trap Description

To view the detail of received traps, select the trap then the detail information about this trap is shown in the bottom area of trap window, as shown in the figure 8-4. The information including the object that raise this trap, and variable binding if attached. The traps EMS server can capture are listed as followings:

Chapter 9

Profile Management

The function of profile management for EMS is to provide an interface for operators to do the configuration management more quickly. It can do the configuration to many devices and ports at the same time by using the given profile. Currently, we provide line profile, alarm profile, and ATM traffic profile.
This chapter describes how to create, save, delete, and deploy profiles.

Line Profile Management

Line profile management includes refresh, save, delete and deploy. When you click the main menu item **Advance->Profile manager,** you will see the function list under the tree folder in the left panel of the profile manager window. Click the **Profile->LineProfile** under the tree will present a line profile management window as Fig 9-1; the functions of line profile management are described as followings:

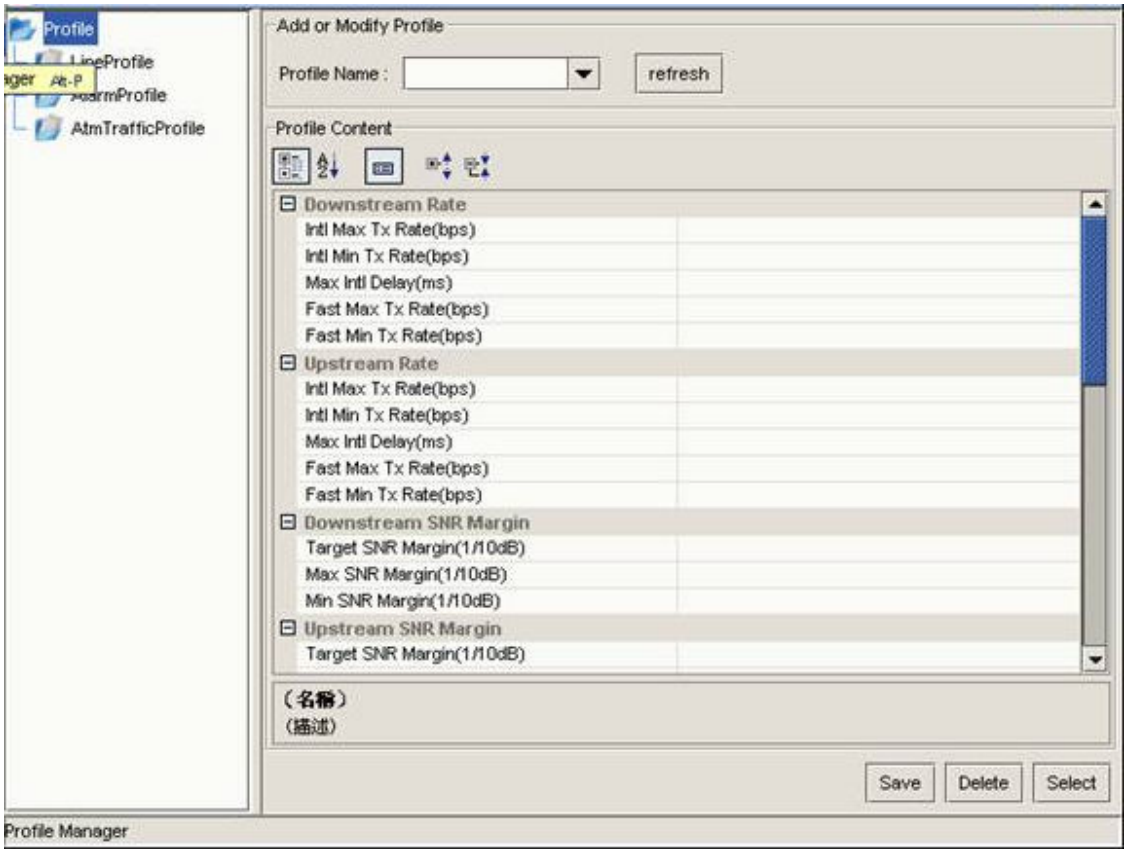


Figure 9-1 Line profile management window

Refresh Line Profile

After starting the line profile window, the system will query the all line profiles which store on the backend database. You can choice any profile by select a line profile name. Once selecting a profile, all the profile data will display all profile parameters on the profile content panel.
You can use the refresh button to requery the all profiles.

Save Line Profile

After changing the profile content, you can use the save button to save the line profile. If the profile name exists on the database, the system will update the profile. Otherwise it will create this profile by using the profile name.

Delete Line Profile

You can push the Delete button to delete the profile by using the profile name.

Select Line Profile

Select button let you to deploy the line profile to the device. The steps goes follows:

Step1 : After push the Select button, the system will display a dialog to choice devices and port as bellow:

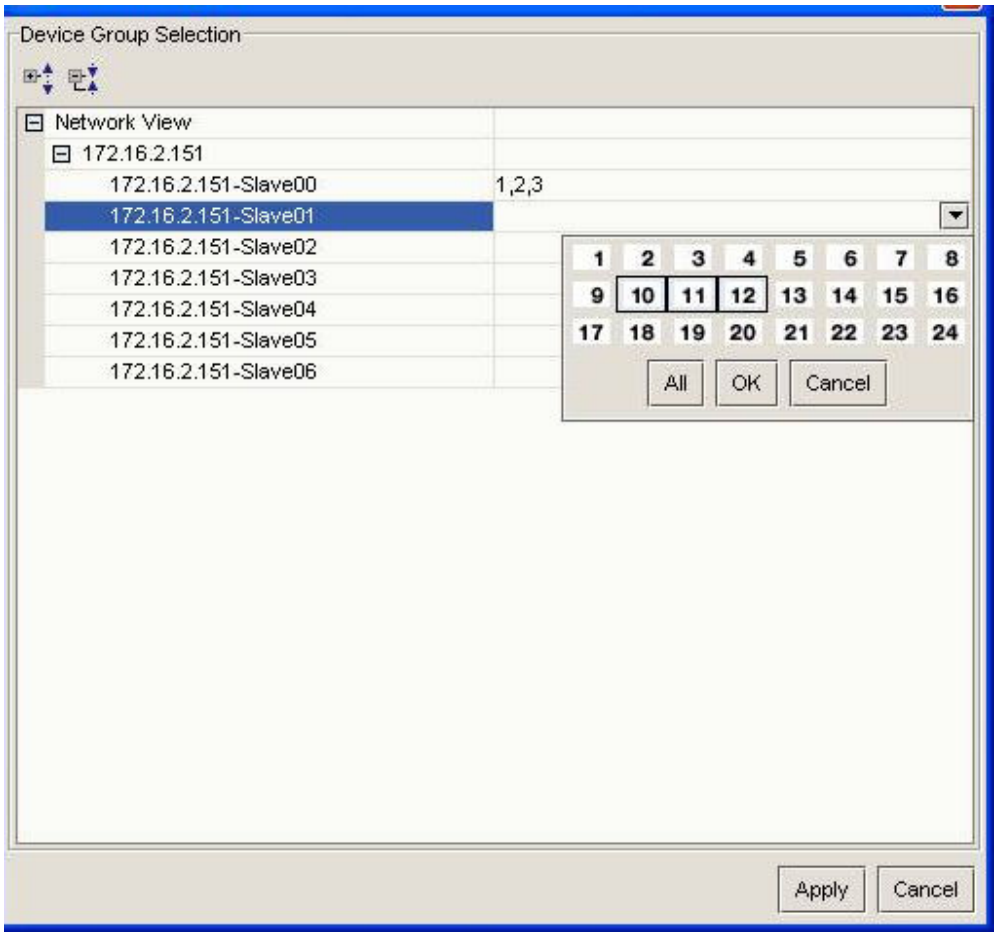


Figure 9-2 device group selection dialog

Step 2 : Push the apply button to apply this line profile to selected profiles. The system will display the deploying dialog to show the display result as bellow:

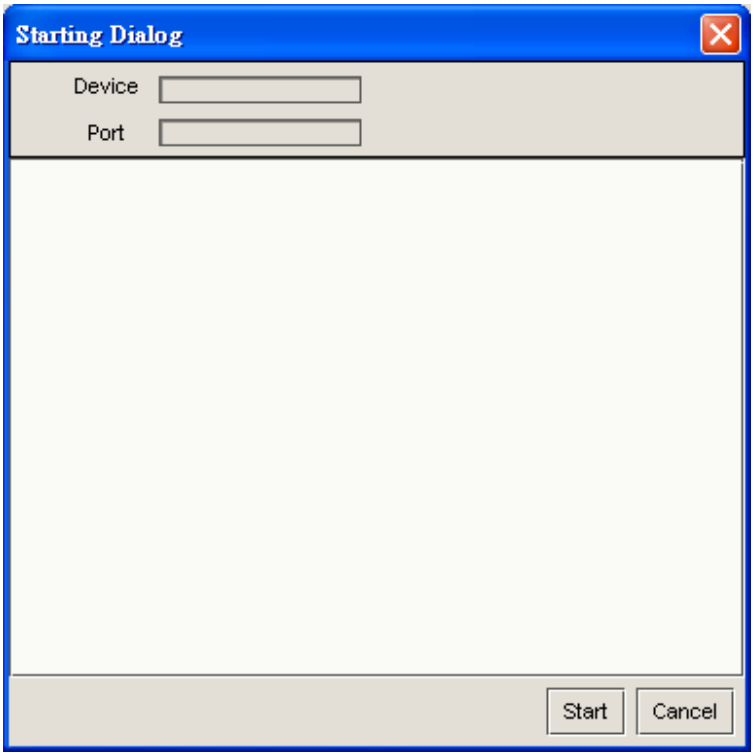


Figure 9-3 Deploy progress dialog

Step3 : Push the start button to start the deploy the line profile, the result will display on the center of the dialog as bellow:

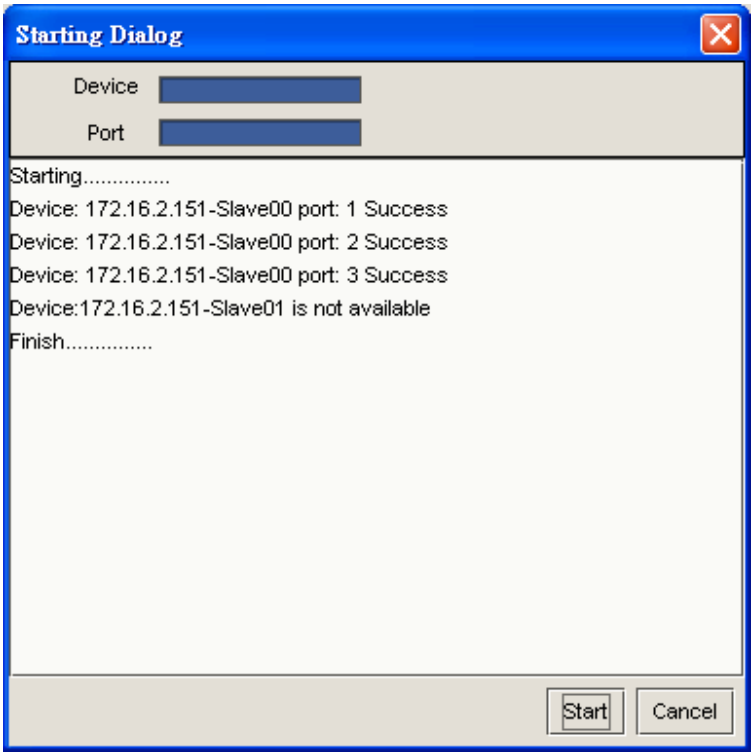


Figure 9-4 Deploy progress dialog

Alarm Profile Management

Alarm profile management includes refresh, save, delete and deploy. When you click the main menu item **Advance->Profile manager,** you will see the function list under the tree folder in the left panel of the profile manager window. Click the **Profile->AlarmProfile** under the tree will present a alarm profile management window as Fig 9-5; the functions of alarm profile management are described as followings:

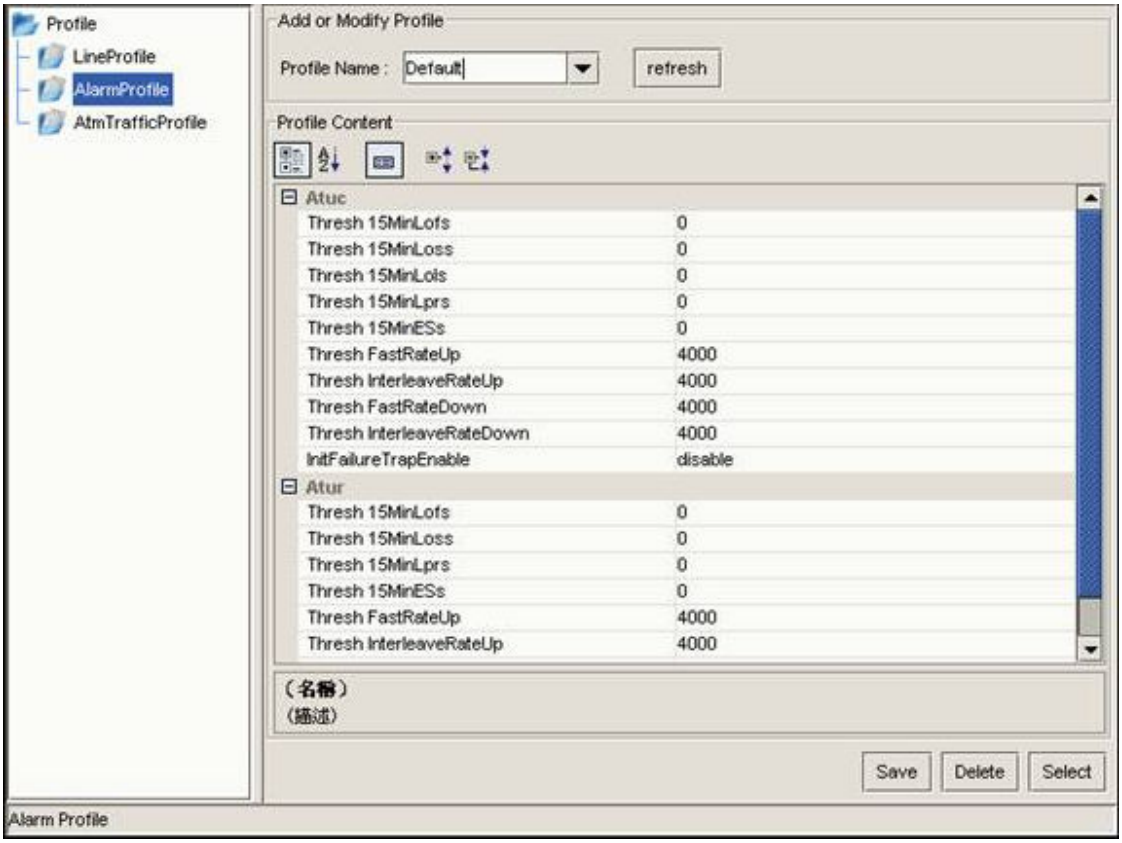


Figure 9-5 Alarm profile management window

Refresh Alarm Profile

After starting the alarm profile window, the system will query the all alarm profiles which store on the backend database. You can choice any profile by select an alarm profile name. Once selecting a profile, all the profile data will display all profile parameters on the profile content panel.
You can use the refresh button to requery the all profiles.

Save Alarm Profile

After changing the profile content, you can use the save button to save the alarm profile. If the profile name exists on the database, the system will update the profile. Otherwise it will create this profile by using the profile name.

Delete Alarm Profile

You can push the Delete button to delete the profile by using the profile name.

Select Alarm Profile

Select button let you to deploy the alarm profile to the device. The steps goes follows:

Step1 : After push the Select button, the system will display a dialog to choice devices and port as bellow:

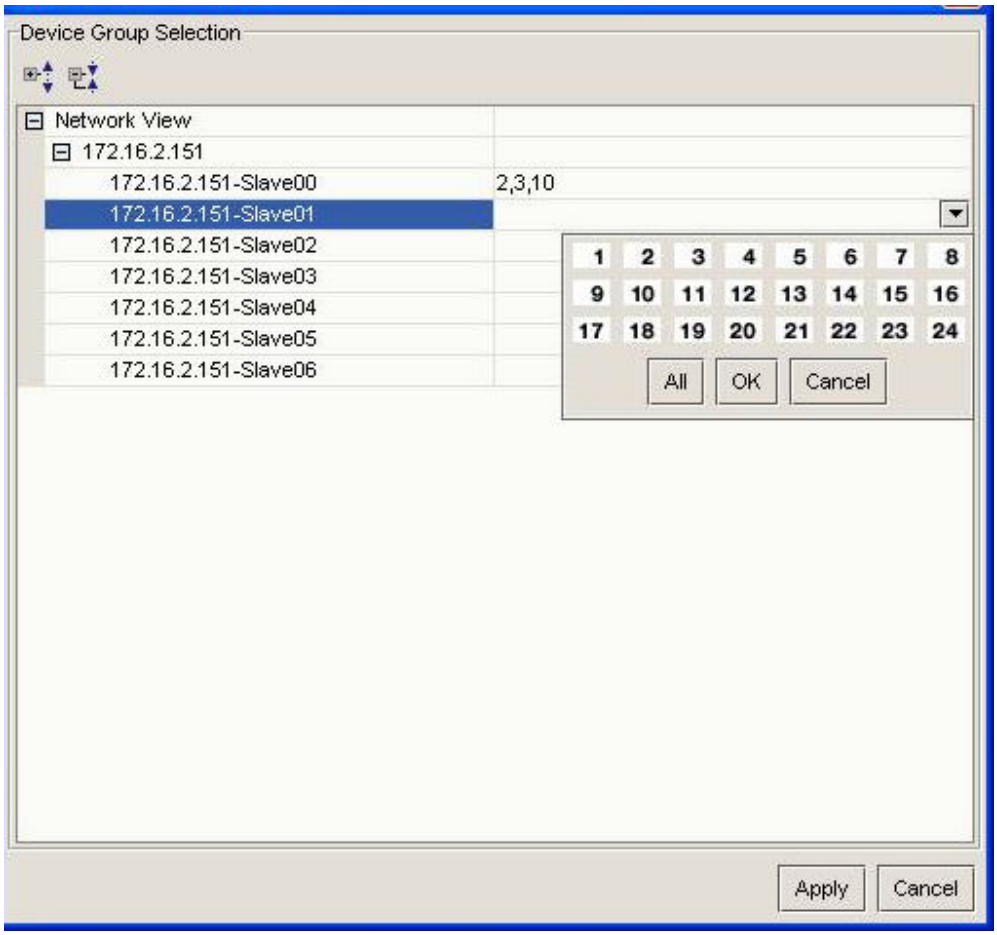


Figure 9-6 device group selection dialog

Step 2 : Push the apply button to apply this alarm profile to selected profiles. The system will display the deploying dialog to show the display result as bellow:

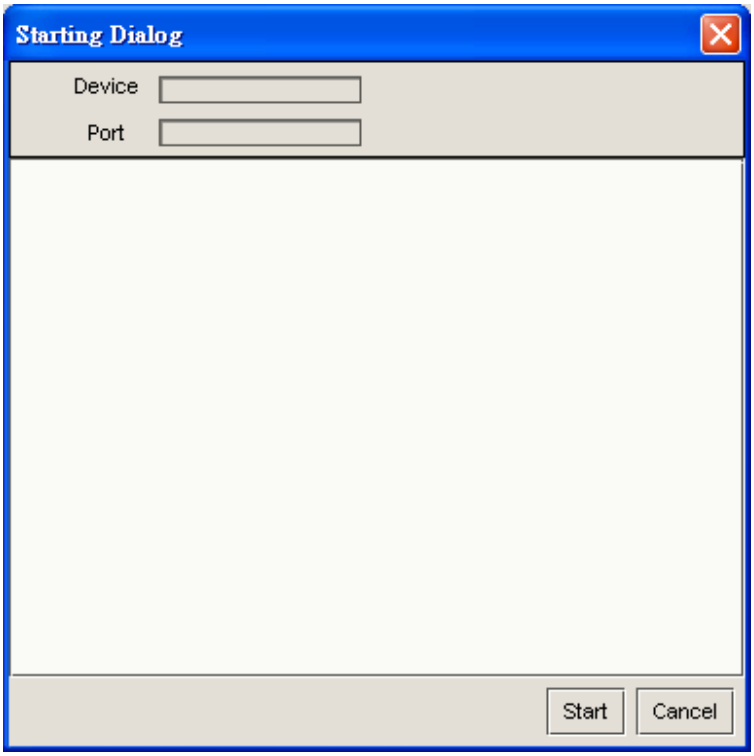


Figure 9-8 Deploy progress dialog

Step3 : Push the start button to start the deploy the alarm profile, the result will display on the center of the dialog as bellow:

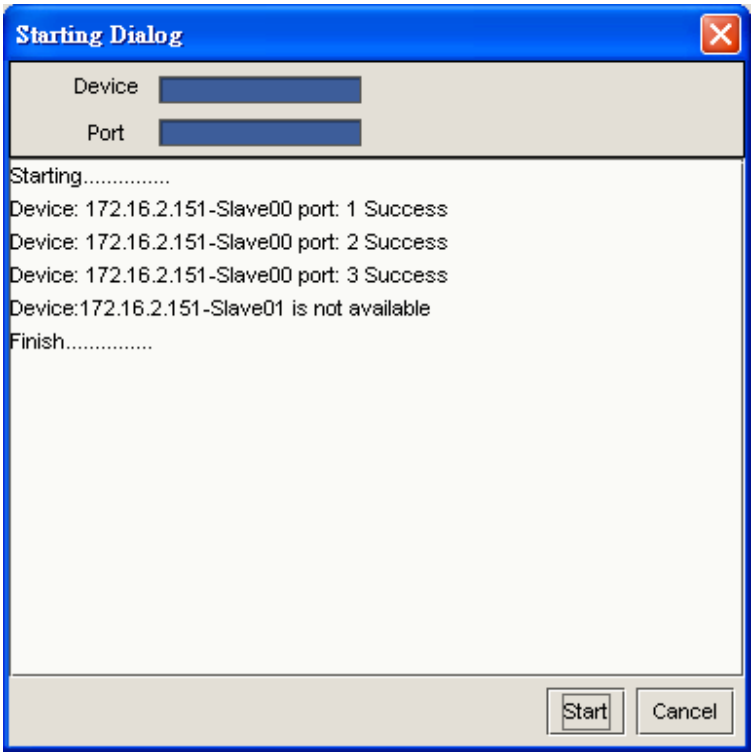


Figure 9-9 Deploy progress dialog

ATM Traffic Profile Management

ATM traffic profile management includes refresh, save, delete and deploy. When you click the main menu item **Advance->Profile manager,** you will see the function list under the tree folder in the left panel of the profile manager window. Click the **Profile->AtmTrafficProfile** under the tree will present a Atm traffic profile management window as Fig 9-10; the functions of Atm traffic profile management are described as followings:

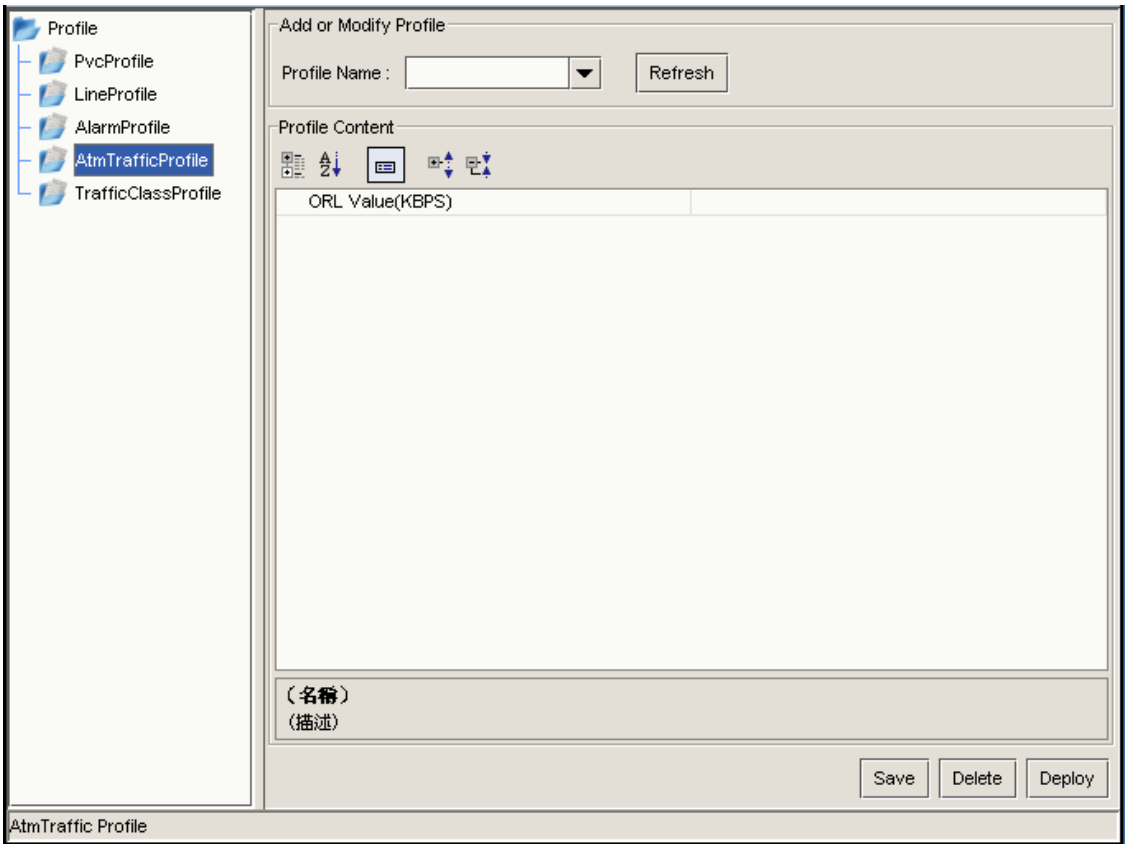


Figure 9-10 Atm Traffic profile management window

Refresh Atm Traffic Profile

After starting the Atrm traffic profile window, the system will query the all Atrm traffic profiles which store on the backend database. You can choice any profile by select an Atrm traffic profile name. Once selecting a profile, all the profile data will display all profile parameters on the profile content panel.
You can use the refresh button to requery the all profiles.

Save Atm Traffic Profile

After changing the profile content, you can use the save button to save the Atrm traffic profile. If the profile name exists on the database, the system will update the profile. Otherwise it will create this profile by using the profile name.

Delete Atm Traffic Profile

You can push the Delete button to delete the profile by using the profile name.

Select Atm Traffic Profile

Select button let you to deploy the Atrm traffic profile to the device. The steps goes follows:

Step1 : After push the Select button, the system will display a dialog to choice devices and port as bellow:

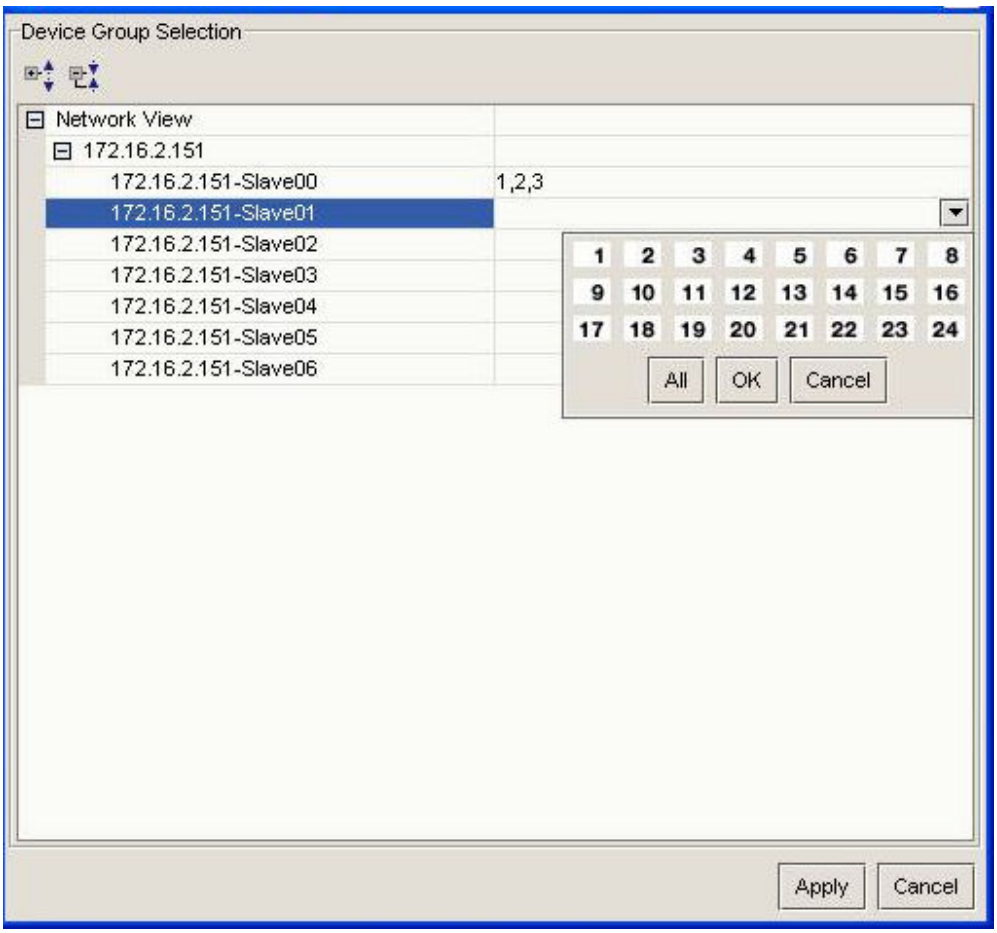


Figure 9-11 device group selection dialog

Step 2 : Push the apply button to apply this Atm traffic profile to selected profiles. The system will display the deploying dialog to show the display result as bellow:

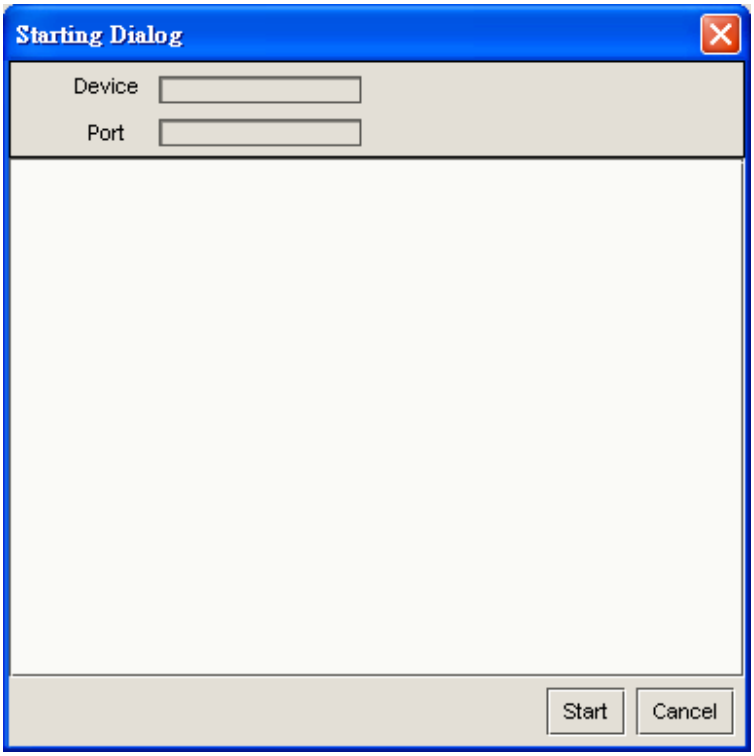


Figure 9-12 Deploy progress dialog

Step3 : Push the start button to start the deploy the Atm traffic profile, the result will display on the center of the dialog as bellow:

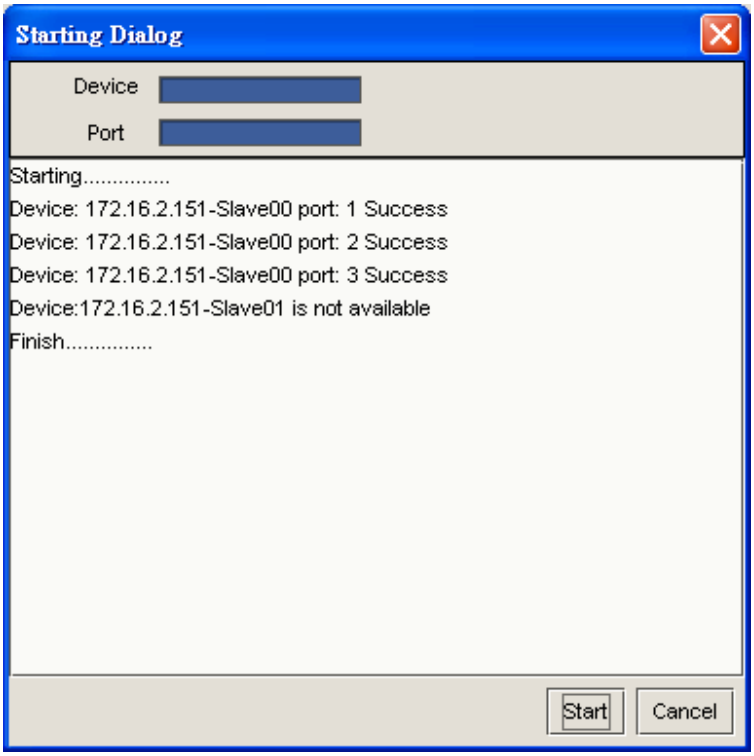


Figure 9-14 Deploy progress dialog

TrafficClass Profile Management

TrafficClass profile management includes refresh, save, and delete. When you click the main menu item **Advance->Profile manager,** you will see the function list under the tree folder in the left panel of the profile manager window. Click the **Profile->TrafficClass Profile** under the tree will present a TrafficClass profile management window as Fig 9-15; This profile do not have deploy function, it is used for PVC Profile. So before filling the PVC Profile, the Traffic Class profile should be setup first. The functions of TrafficClass profile management are described as followings:

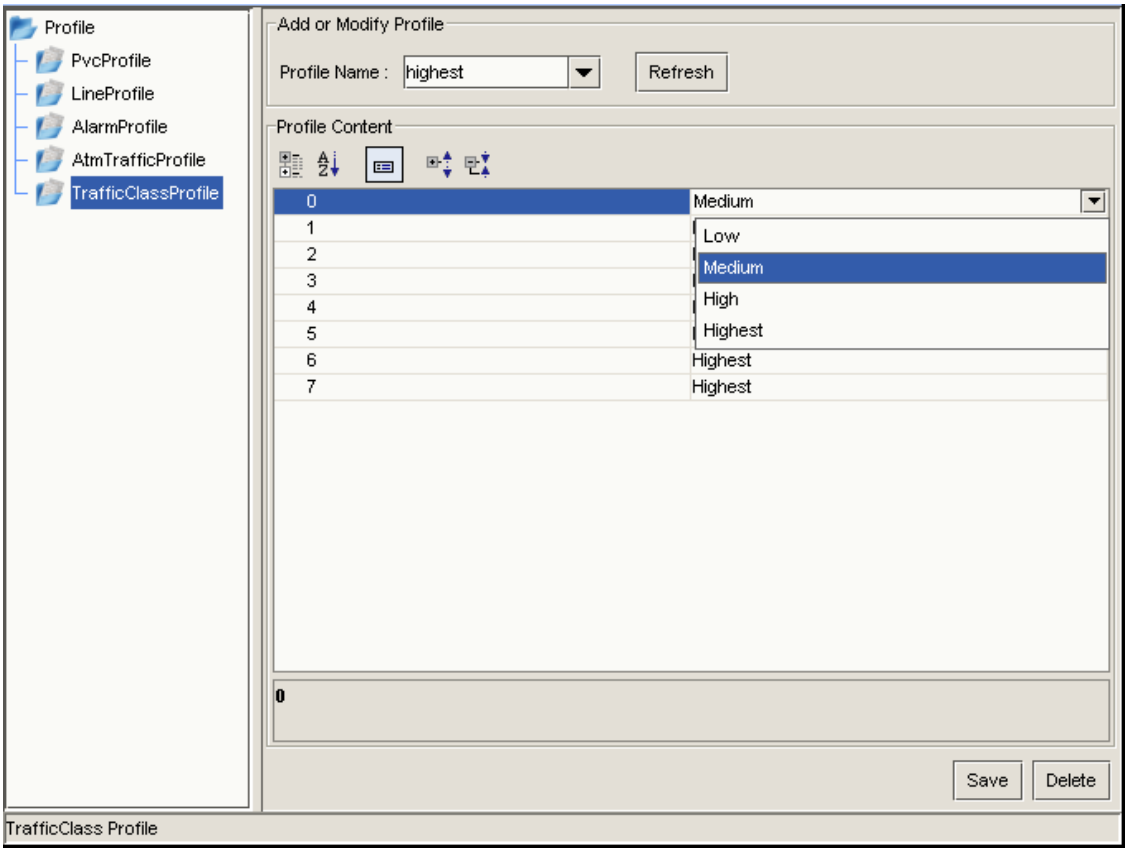


Figure 9-15 Traffic Class window

Refresh TrafficClass Profile

After starting the TrafficClass profile window, the system will query the all TrafficClass profiles which store on the backend database. You can choice any profile by select a TrafficClass profile name. Once selecting a profile, all the profile data will display all profile parameters on the profile content panel.
You can use the refresh button to requery the all profiles.

Save TrafficClass Profile

After changing the profile content, you can use the save button to save the TrafficClass profile. If the profile name exists on the database, the system will update the profile. Otherwise it will create this profile by using the profile name.

Delete TrafficClass Profile

You can push the Delete button to delete the profile by using the profile name. Otherwise the table will be clear.

PVC Profile Management

PVC profile management includes refresh, save, delete and deploy. When you click the main menu item **Advance->Profile manager,** you will see the function list under the tree folder in the left panel of the profile manager window. Click the **Profile->PVC Profile** under the tree will present a PVC profile management window as Fig 9-16; before setting the PVC Profile, the Traffic Class profile should be setup first. The functions of PVC profile management are described as followings: Basically, user may select profile from database or add it manually.

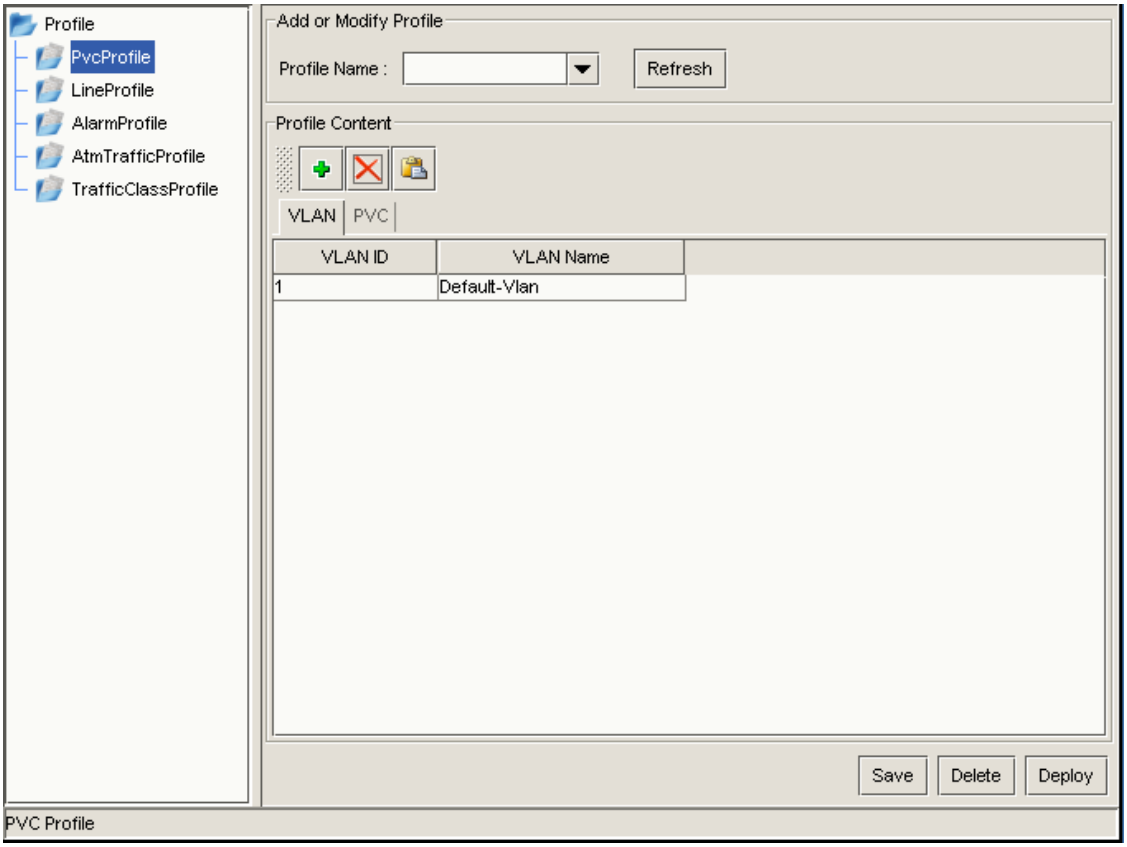


Figure 9-16 PVC Profiles VLAN window

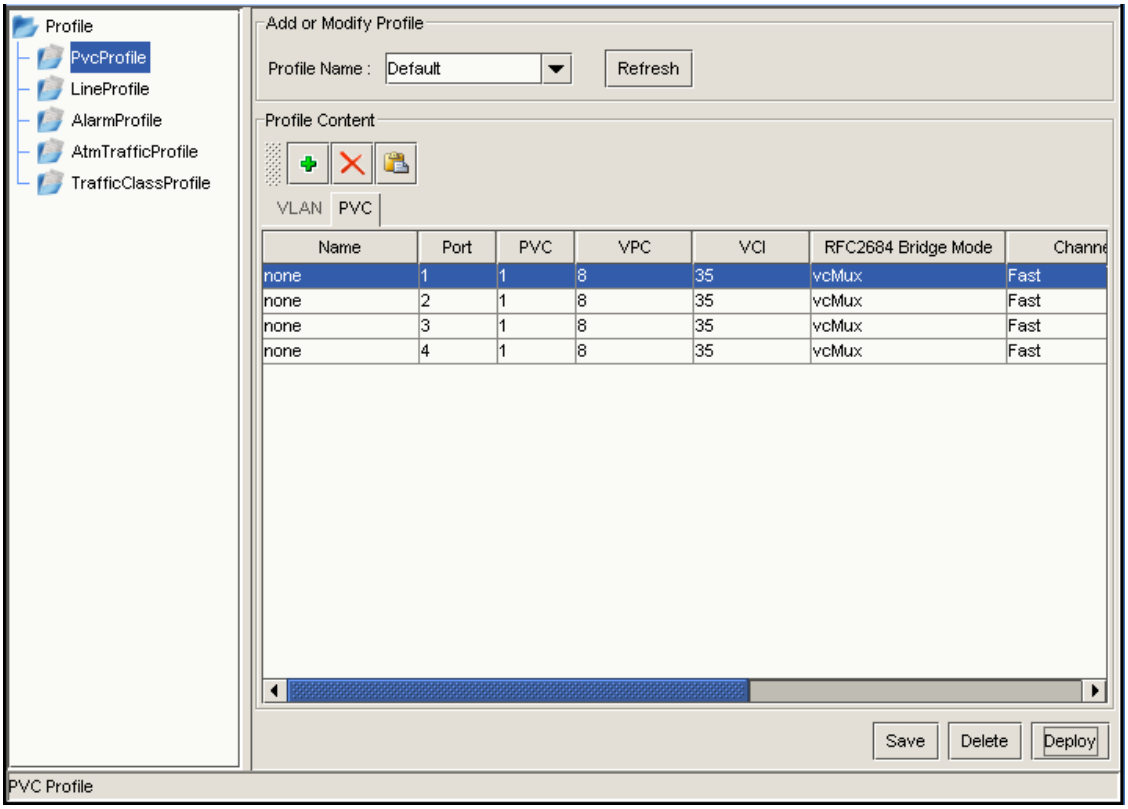


Figure 9-17 PVC Profiles PVC window

Refresh PVC Profile

After starting the PVC profile window, the system will query the all PVC profiles which store on the backend database. You can choice any profile by select a TrafficClass profile name. Once selecting a profile, all the profile data will display all profile parameters on the profile content panel.
You can use the refresh button to requery the all profiles.

Save PVC Profile

After changing the profile content, you can use the save button to save the PVC profile. If the profile name exists on the database, the system will update the profile. Otherwise it will create this profile by using the profile name.

Delete PVC Profile

You can push the Delete button to delete the profile by using the profile name. Otherwise the table will be clear.

The first icon will add a new empty entry to the table. Then user must fill related data on

the table.
The second icon will delete the selected rows data on the table.
The last icon will paste the selected rows on the table, it will help user quickly filled out the table.

Deploy PVC Traffic Profile

Deploy button let you to deploy the PVC profile to the device. The steps go as follows:

Step1 : After push the Deploy button, the system will display a dialog to choice devices as bellow: the device will be deploy on the value set to “YES”.

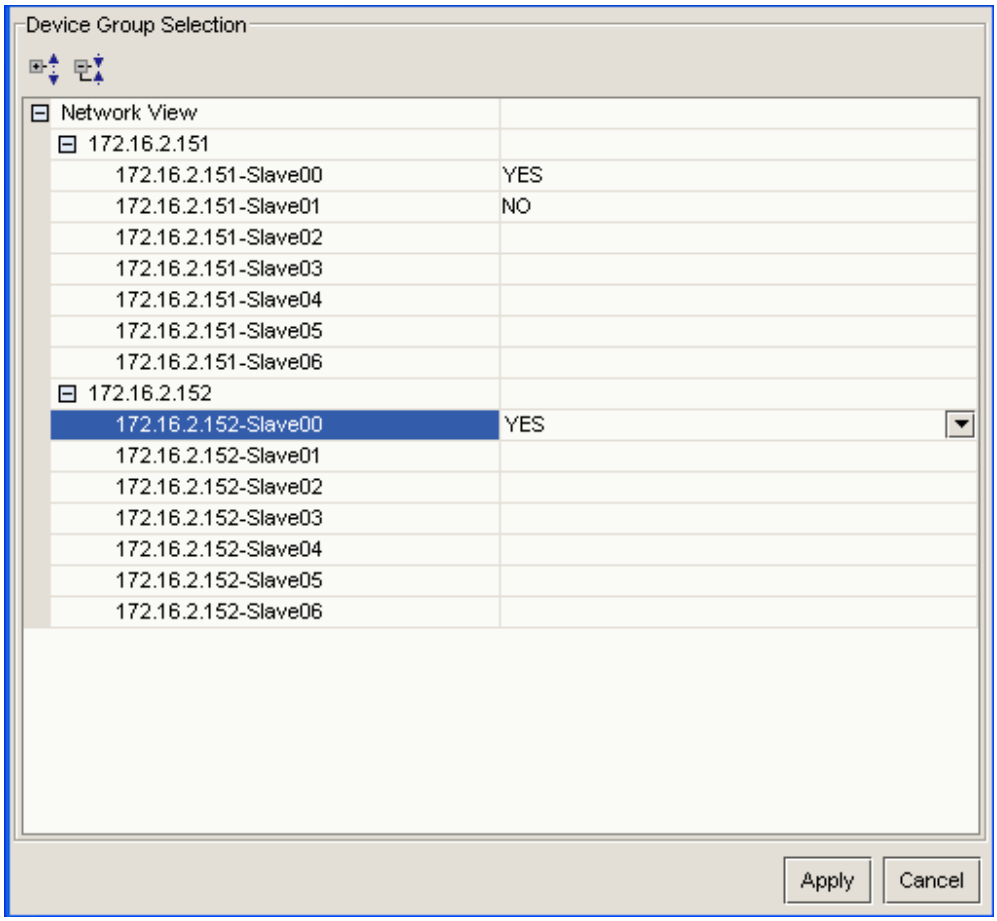


Figure 9-18 device group selection dialog

Step 2 : Push the apply button to apply this PVC profile to selected profiles. The system will display the deploying dialog to show the display result as bellow:

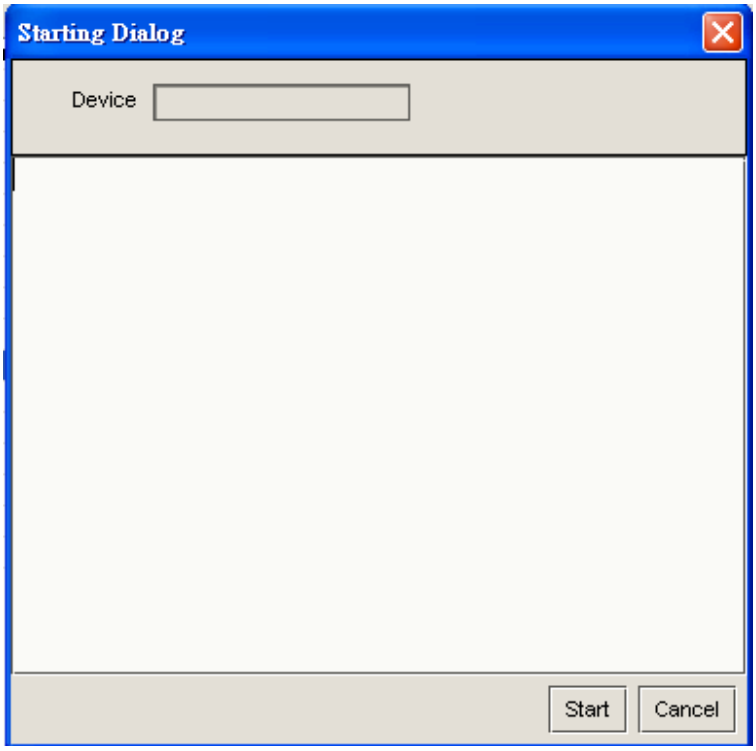


Figure 9-19 Deploy initial progress dialog

Step3 : Push the start button to start the deploy the PVC profile, the result will display on the center of the dialog as bellow: From the result: user may see the whole action log. If the device is not available, the device will skip. On the other hand, if the value of profile is not valid, the procedure will stop.

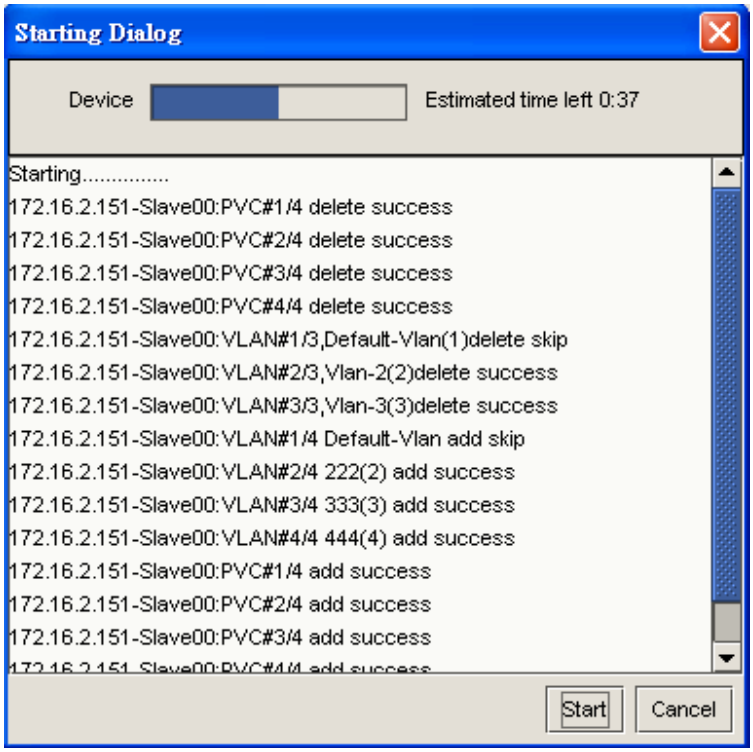


Figure 9-20 Deploy progress dialog

Capter 10

Report

The function of report for EMS is to provide an interface for operators to export, save and print some statistic data of EMS database. Currently, we provide alarm history, and Long Term PM report.
This chapter describes how to create alarm history and Long Term PM report.

Report Dialog

All reports are generated through Report Dialog. You need to click the main menu item **Advance->Report** to open the Report Dialog as followings:

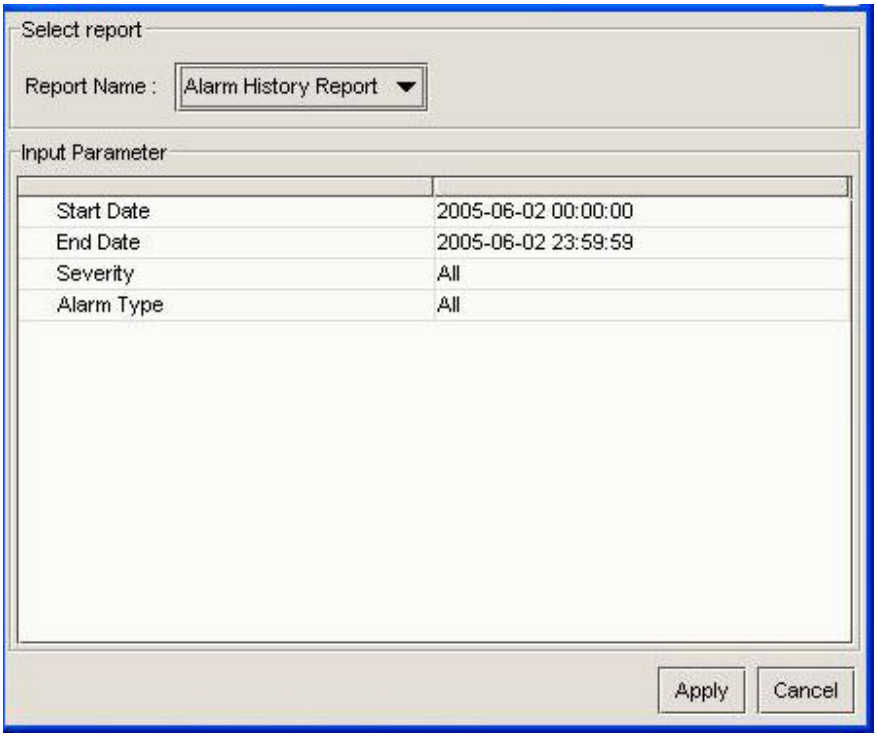


Figure 10-1 Report dialog

Report Name

You can select different report name to generate different report.

Parameters

Different reports can input different parameters. After changing report by selecting the report name, the input parameters panel will display the parameters that you can input for this report. Please change the parameters for each report.

Alarm History Report

Alarm history report is exactly the same as alarm history panel on alarm window. But you can save, print with a well defined format.

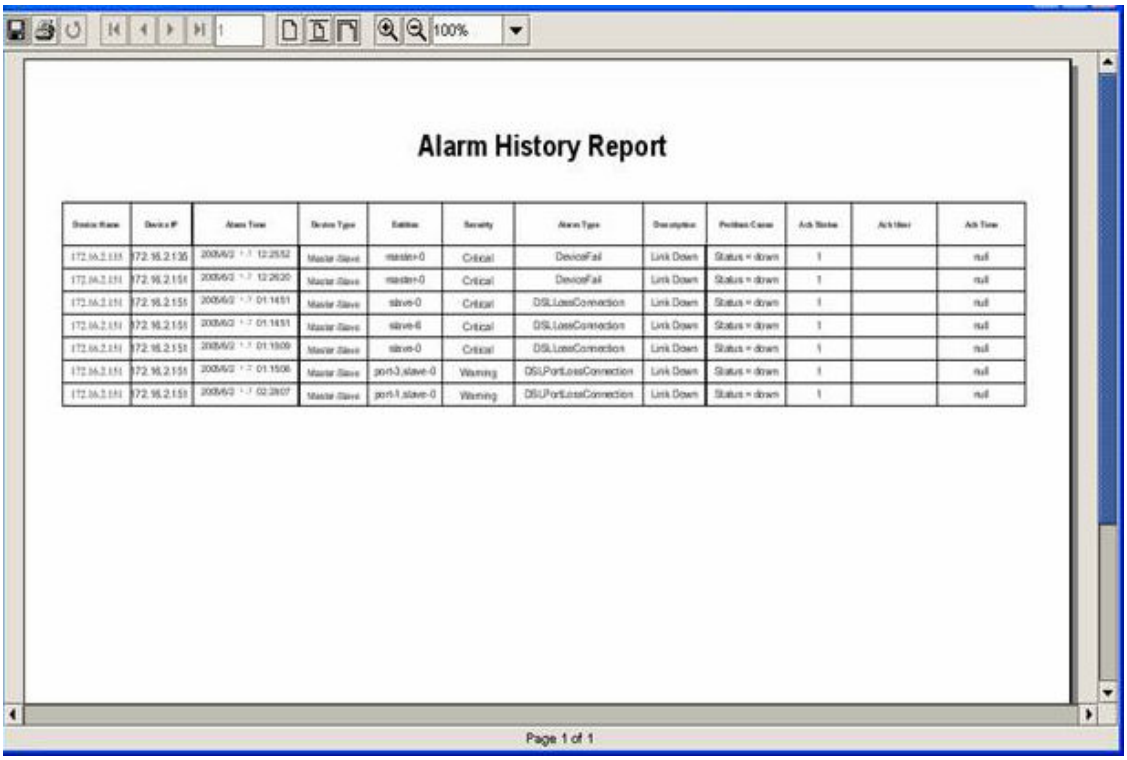


Figure 10-2 Alarm History Report

Long Term PM Report

Long Term PM report is exactly the same as Long Term PM data panel on Long Term PM window. But you can save, print with a well defined format.

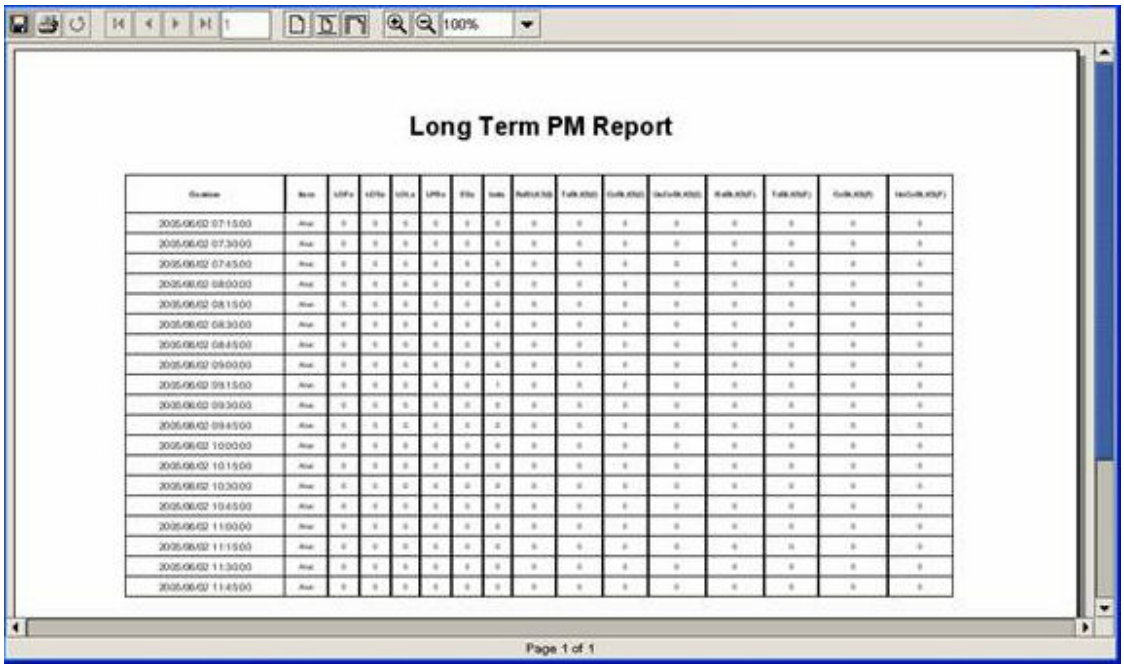


Figure 10-3 Long Term PM Report