

VigorCMS

Operational Manual

Table of Contents

COPYRIGHT	3
CHAPTER 1 IP DSLAM SYSTEM DESCRIPTION.....	5
CHAPTER 2 INTRODUCTION TO CENTRAL MANAGEMENT SYSTEM....	10
CHAPTER 3 INSTALLATION AND GETTING STARTED.....	16
CHAPTER 4 CONFIGURATION MANAGEMENT.....	40
CHAPTER 5 SECURITY MANAGEMENT.....	94
CHAPTER 6 MONITOR MANAGEMENT.....	101
CHAPTER 7 TOPOLOGY MANAGEMENT.....	105
CHAPTER 8 LOG AND EVENT MANAGEMENT	110
CHAPTER 9 PROFILE MANAGEMENT	126
CHAPTER 10 REPORT	142

COPYRIGHT

© Copyright 2005 by Draytek Technologies. All Rights Reserved.

This manual is copyrighted by Draytek Technologies. You may not reproduce, transmit, transcribe, store in a retrieval system, or translate any part of this publication into any language or computer file, in any form or by any means - electronic, mechanical, magnetic, optical, chemical, manual, or otherwise - without expressing written permission from the Draytek Technologies.

Trademark Acknowledgment

All products or service names mentioned in this document may be trademarks of the companies with which they are associated.

Revision History

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




Target Audience

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

Note, Tip and Warnings

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

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

	<i>Note</i> contains “for your information” text that corresponds to a topic.
	<i>Tip</i> offers helpful hints and time-saving suggestions about using features.
	<i>Warnings</i> 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

IP DSLAM System Description

This chapter is divided into the following sections,

- Section 1.1: IP DSLAM Application Description
- Section 1.2: IP DSLAM Slave Architecture

1.1 IP DSLAM Application Description

IP DSLAM, which is equipped with 24 ADSL ports, is designed for ISP (Internet Service Provider) to implement bandwidth management for multiplying 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 remoting management. Particularly, IP DSLAM can be easily configured by CMS. The CMS 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 provides for improving 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 for supporting multiple applications and depicting in Figure 1-1.

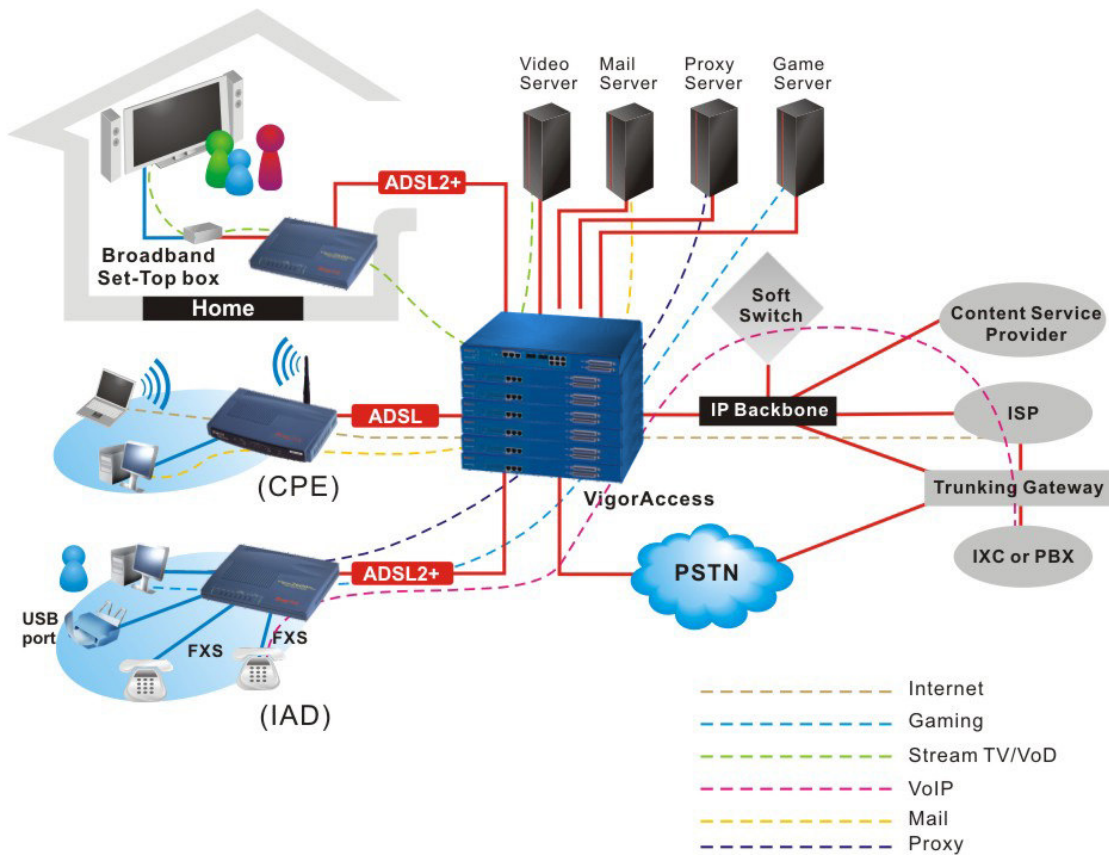


Figure 1-1. Application Scenario of IP DSLAM for users

Users 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.

Users can stack multiple IP DSLAM units up to the number of ports available on the Ethernet switch as shown below Figure 1-2.

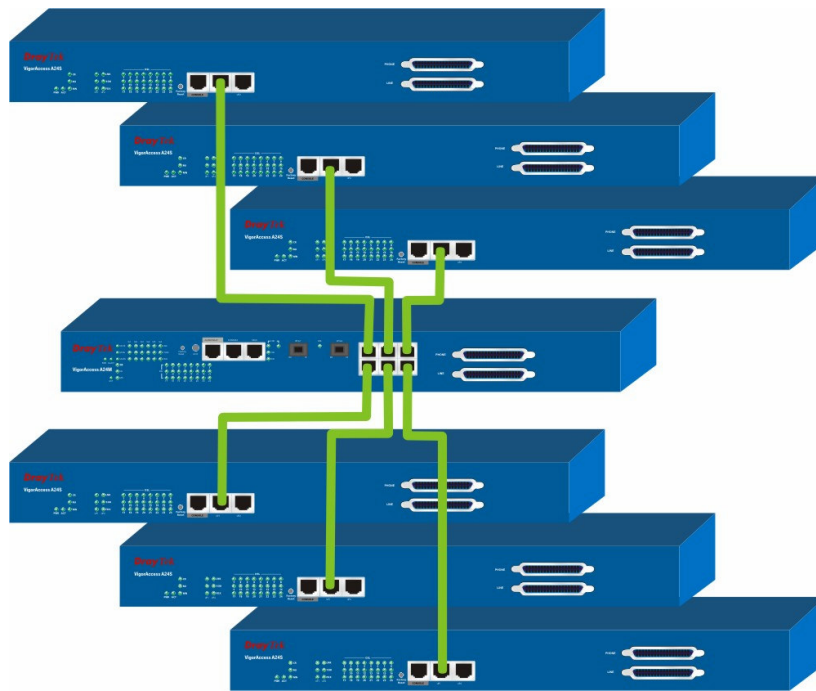


Figure 1-2. IP DSLAM system architecture

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, users can manage slave units through master unit. The picture of master unit is as below Figure 1-3.



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.

1.2 IP DSLAM Slave Architecture

The role of slave unit is to provide high-performance, good services DSL features for Internet environment.

The picture of slave unit is as below Figure 1-4.



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 Central Management System

This chapter is divided into the following sections,

- Section 2.1: System Description
- Section 2.2: System Architecture

Central Management System Server (CMS Server) is a multi-tier architecture, flexible, easy to use for system management. It can manage 1000 to 10000 IP DSLAM devices, depends on the capacity of server. A step-by-step configuration wizard makes users to deploy large numbers of devices to customer sites easily. CMS provides for Configuration management, Deployment management, Fault management, Security management, Topology management, and backend storage management.

Configuration management allows users to remote controlling 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 CMS server or the Provisioning server when they are booting up. Another feature in Configuration management is the diagnostic functions used to test the device, and make sure that the device is OK.

Deployment management is utilized for users 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 build their own policies, and apply these policies for managed devices.

Fault management includes alarm collection, status polling, event logging and alert trigger. CMS server monitors all managed devices in a fixed interval, and the device will report alarms when something is wrong in it. CMS server will keep some system event so that trace messages will be stored in the database or files for tracing. Alert trigger provides a notification mechanism to users when any event or alarm received by CMS server. 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. In general, system will send e-mail to users once the condition is fulfilled the filters set by administrator. Security management uses a resource-role

conception to manage users. For authentication, CMS server has a default mechanism to do that, or an external RADIUS server could be used to provide authentication service. CMS server will maintain an access control list to do authority, grant users with some privilege to resources. Topology management provides auto discovery for devices and add delete devices manually. A layer structure is used to show subnet-device relationship.

The following Figure 2-1 depicts the system overview between IP DSLAM devices and CMS system. The CMS server and IP DSLAM devices use SNMP protocol to communicate with each other.

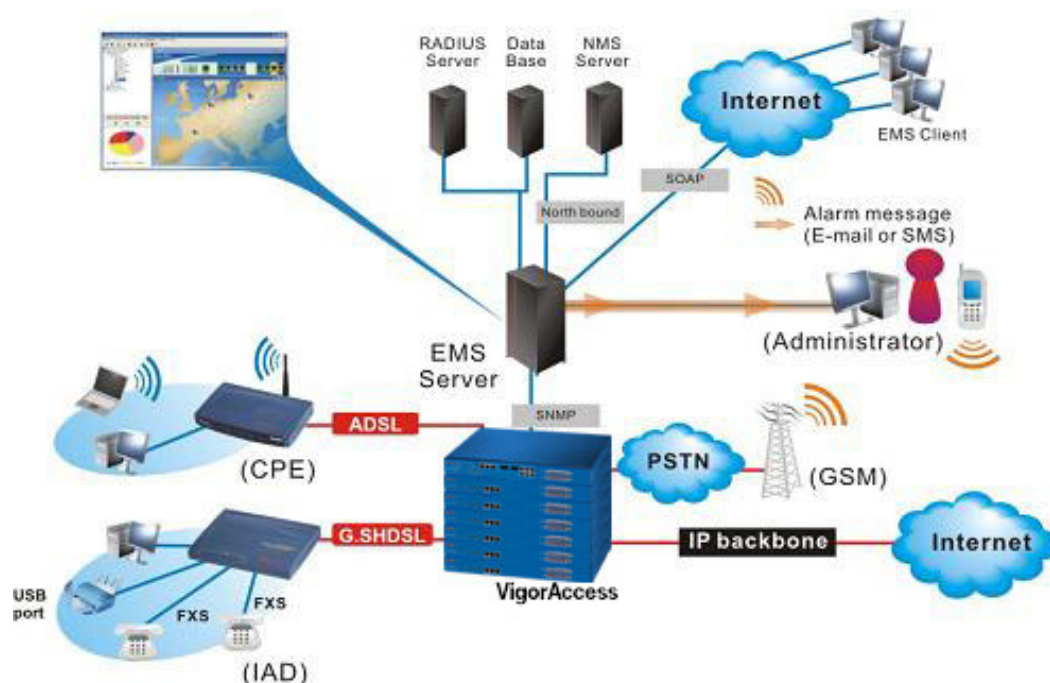


Figure 2-1. IP DSLAM management system overview

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 CMS system overview and technique specifications. We have more detailed function description of the CMS in Chapter 4.

2.1 System Description

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

2.1.1 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 IP DSLAM 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 CMS 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 for total network view with hierarchy.
- Users 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.

2.2 System Architecture

2.2.1 Software Architecture

CMS 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 CMS. The presentation layer will transfer the data input via the user interface layer to the business and domain layer keep the connection session information for users. The business and domain logic layer is an CMS 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 CMS server, so it can be run in Linux or Windows™ platform. The backend database server is provided for storing users' account, topology information, alarm information and event log. For open architecture, the CMS 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 CMS server. For example, Microsoft™ SQL server, Oracle™, and MySQL. The default database server used for CMS is MySQL. GUI is either Windows GUI or Java-based GUI, depends on the platform. An instance of the CMS server can manage up to thousands of devices, it means that the number of devices, which are managed by the CMS server, can be scaled to more than 1000, if there are more than one instance in the CMS server. Another issue is the fault tolerant for the CMS server. CMS server can be run in redundancy mode, which makes CMS server more highly availability. When the primary CMS server is started up, a secondary CMS server is in standby mode. Once the primary CMS server is crashed for some reasons, the secondary CMS server is activated immediately.

2.2.2 Configuration Management

CMS provides configuration management for device management. Operators can remote control devices by invoking 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 CMS, so firmware upgrade is done by a batch job online or in pre-assigned time.

2.2.3 Deployment Management

The function of Deployment management is used to deploy predefined profile, we also can set a scheduler for batching deployment, and you also can 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, and the type of firmware.

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

2.2.5 Security Management

CMS provides a central security management for users account and resource control. For authentication, a default mechanism is provided or an external RADIUS server is used. For resources control, CMS treats functions, managed devices, policies as different resource types, so CMS will grant resources to roles defined by administrator. So the security model for CMS is user-role-resource.

Role:

Default=> Administrator/Operator

Resources:

Functions/Managed Devices/Policies/Map

2.2.6 Topology Management

Topology management provides auto discovery and layer structure subnets for managed devices. For auto discovery, we can input a network range and CMS 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 subnet and subnet. A device must belong to some subnet built in the CMS. 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.

2.2.7 Log and Event Management

CMS will receive alarms or events and collect them into the backend database, so history data will be kept for a long time. Also, users' 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

IP DSLAM CMS is client-server architecture, so the installation procedure should consist of two parts: CMS client installation and CMS server installation. CMS client should be installed in Windows 2000/XP/NT environment and CMS 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 CMS client and CMS server, and how to start CMS program. All functions will be described in Chapter 4 or later.

This chapter is divided into the following sections,

- Section 3.1: Installation
- Section 3.2: Getting Started

3.1 Installation

3.1.1 Setup and Install CMS Client Software

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

The CMS client is a graphical user interface tool that retrieves data from CMS server. By the tool, operators can manage devices easily. You can use CMS 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

3.1.1.1 Install

For Windows 2000™ Profession or XP home/professional platform

Step1: To Setup CMS Client, run SETUP.EXE in your source disk or CD-ROM that contains of CMS Client programs and follow the instructions, step by step, to complete the installation.

The settings will appear on your screen, as shown Figure 3-1. Press Next to continue.

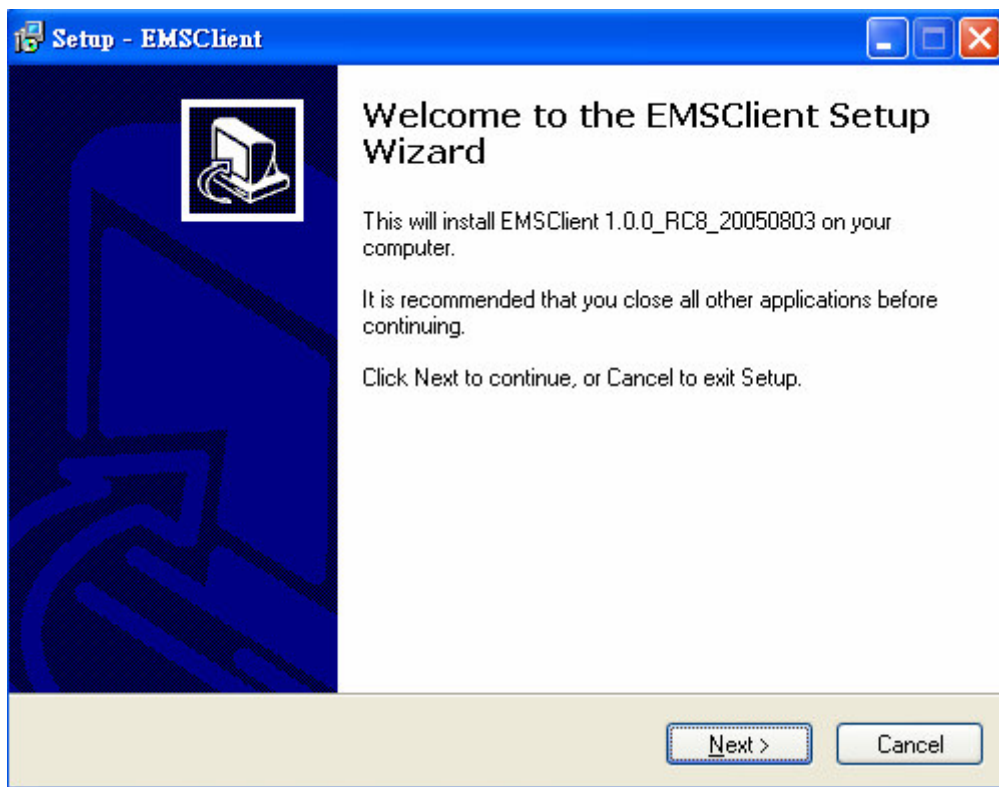


Figure 3-1. CMS client setup program-1

Then select the folder which you want to install as Figure3-2:

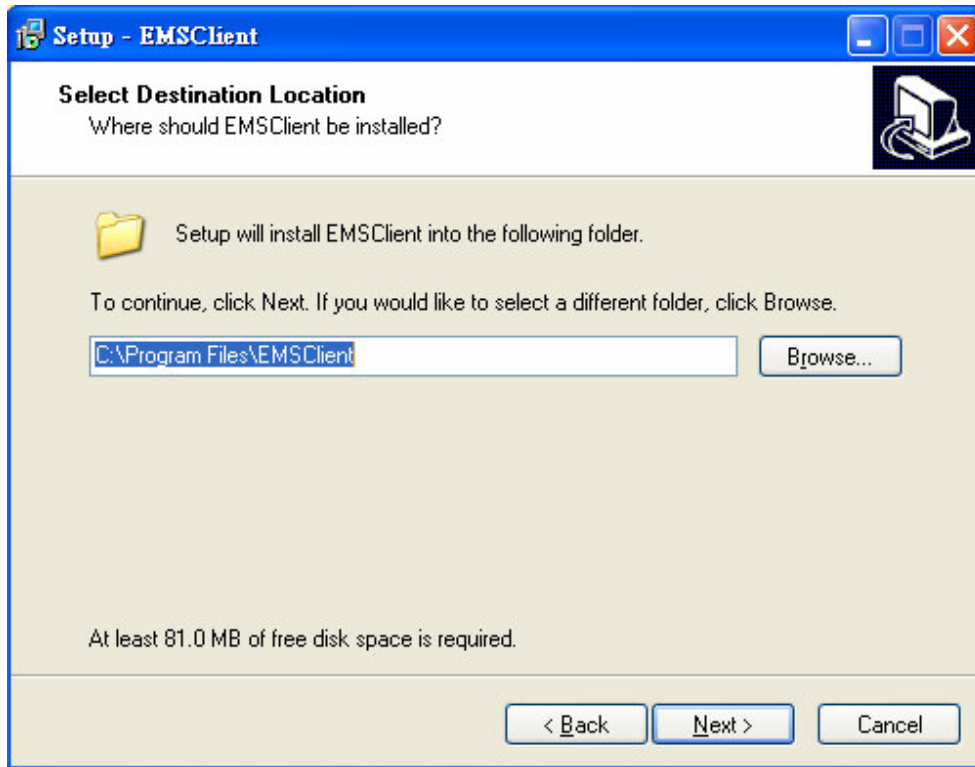


Figure 3-2. CMS client setup program-2

The other setting can use default setting and press Next step by step and the installing process will in progress as Figure3-3.

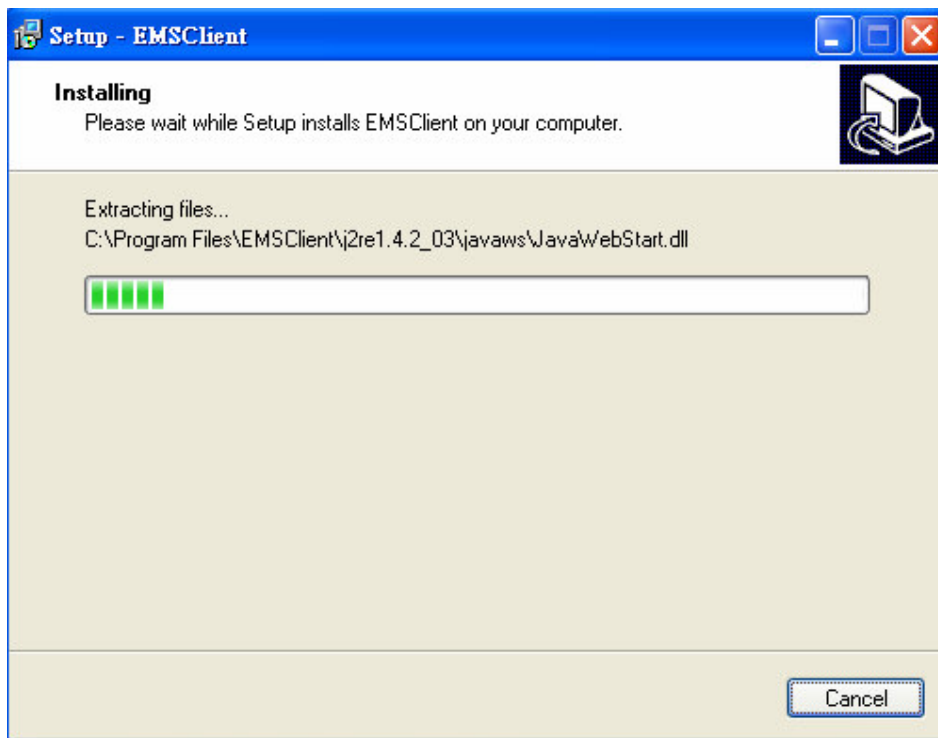


Figure 3-3. CMS client setup program-3

After installing success, it will popup as Figure-3-4. Press Finish button to finish the install CMS Client procedure.

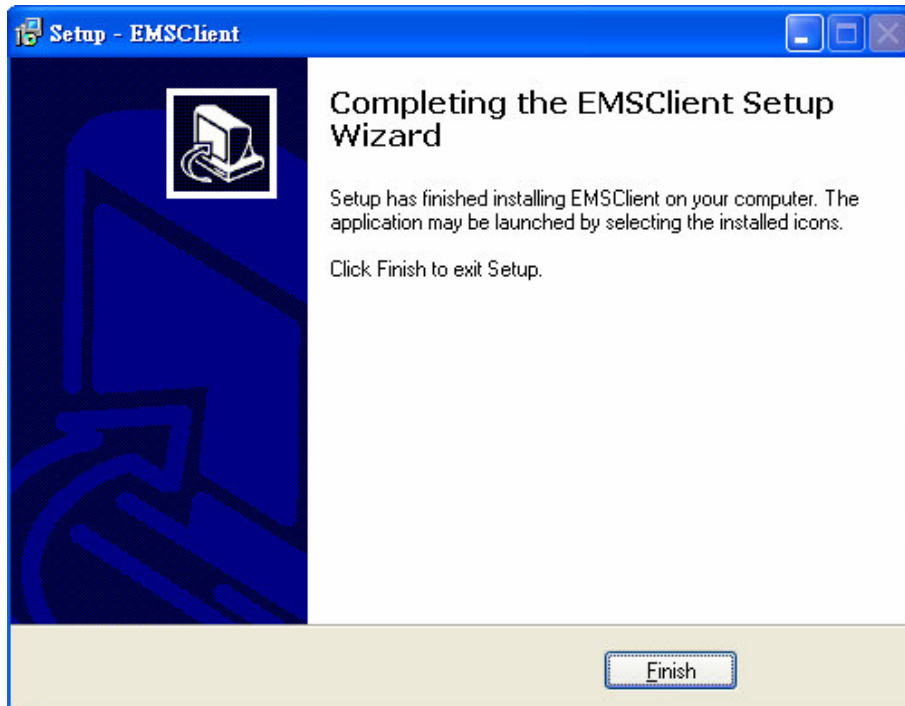


Figure 3-4. CMS client setup program-4

3.1.1.2 Uninstall

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

3.1.2 Setup and Install CMS Server Software

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

3.1.2.1 Install CMS Server

For Windows 2000™ server or XP high end platform

Step1: Setup JAVA VM environment: Run `JDK\Software\j2sdk-1_4_2_03-windows-i586-p.exe.`

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

The settings will appear on your screen, as shown Figure 3-5. Just Press Next Step by Step.

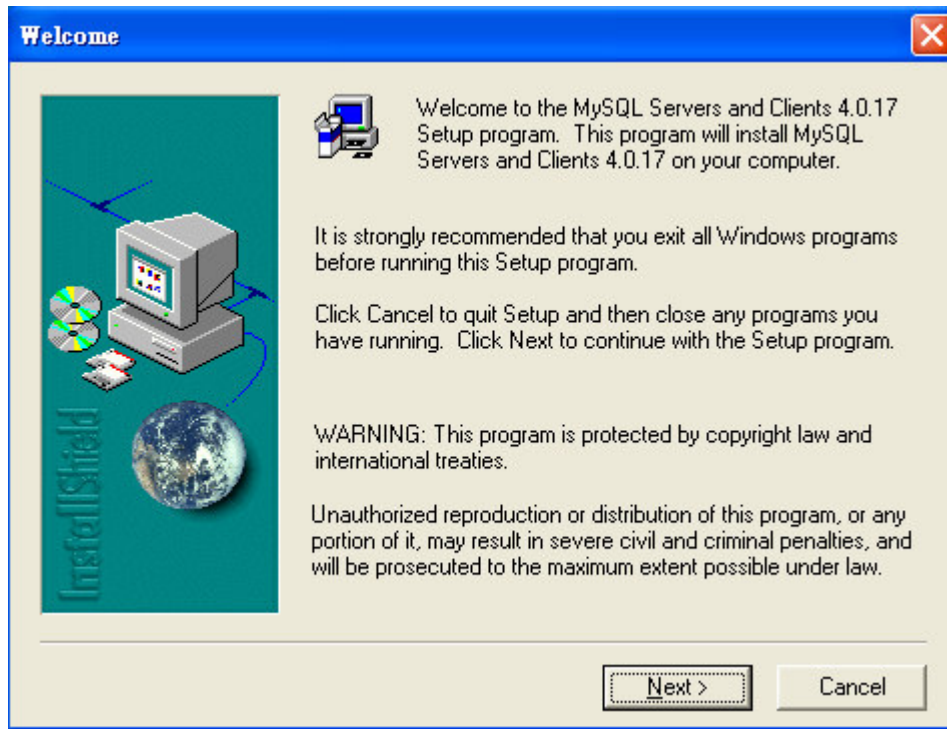


Figure 3-5. Database server setup program-1



The default directory of **mysql** is located at **c:\mysql**.

Please do not change it otherwise you will have some problems on CMS Server installation as Figure 3-6

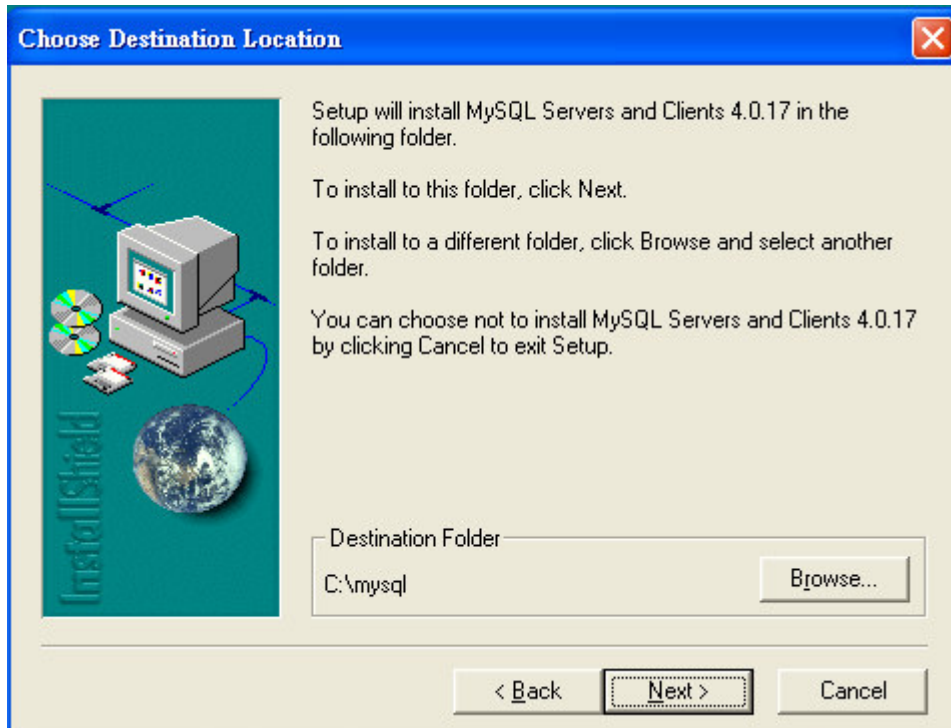


Figure 3-6. Database server setup program-2

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

The settings will appear on your screen, as shown Figure 3-7.

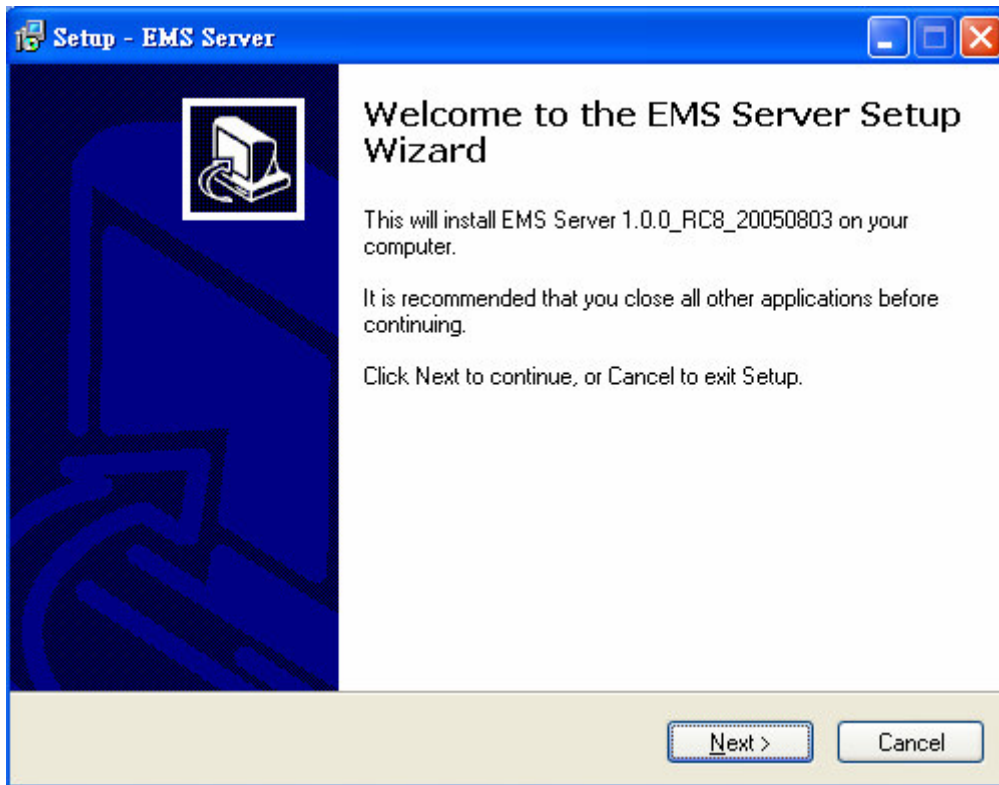


Figure 3-7. CMS server setup program-1

Then choose the location for install CMS Server as following Figure3-8.

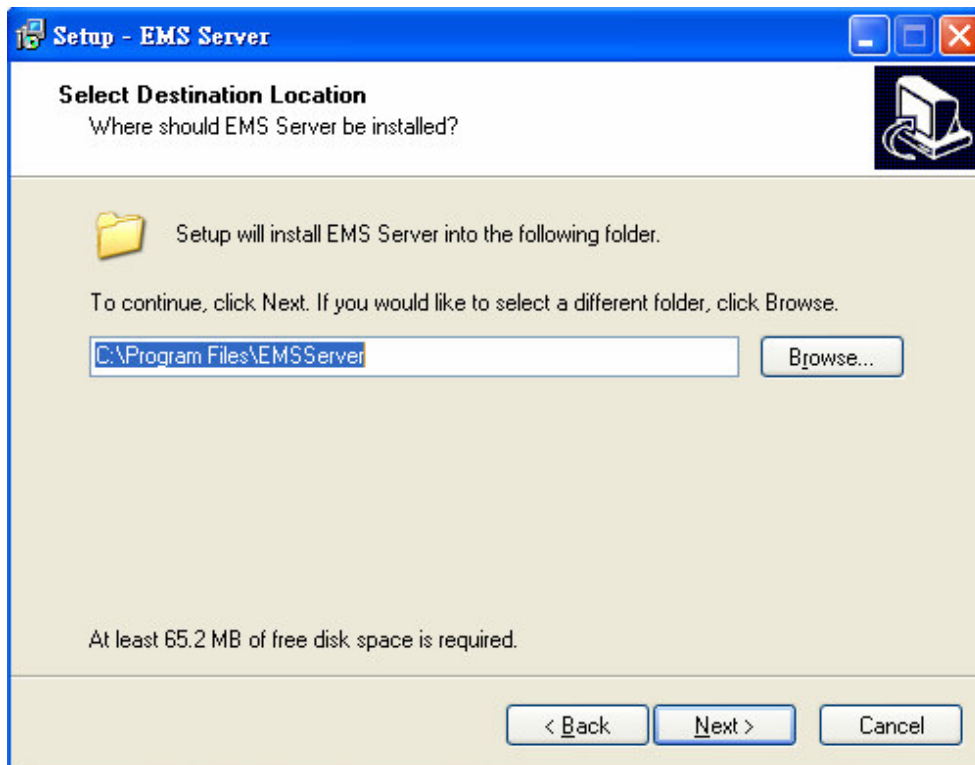


Figure 3-8. CMS server setup program-2

Press Next Step by Step, the CMS Server will install in progress as Figure3-9.

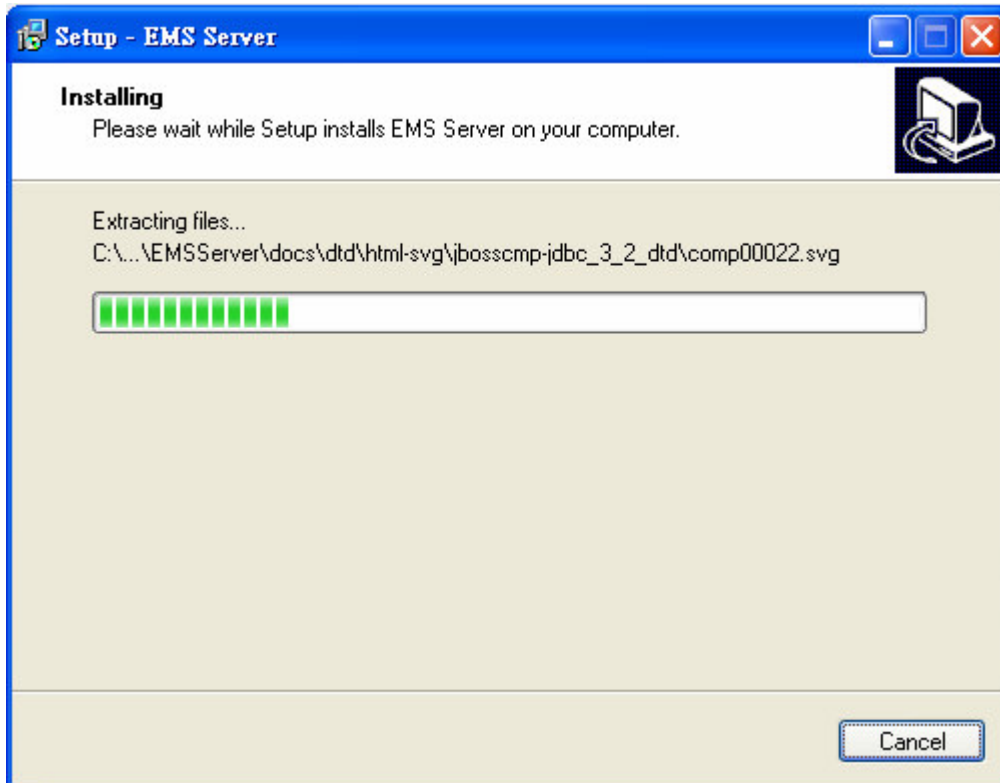


Figure 3-9. CMS server setup program-3



During setup, the setup wizard will prompt a message as Figure3-10 to indicate that if you want to rebuild the database, you should select “Yes” if the version of CMS is under V1.0.0 RC4.

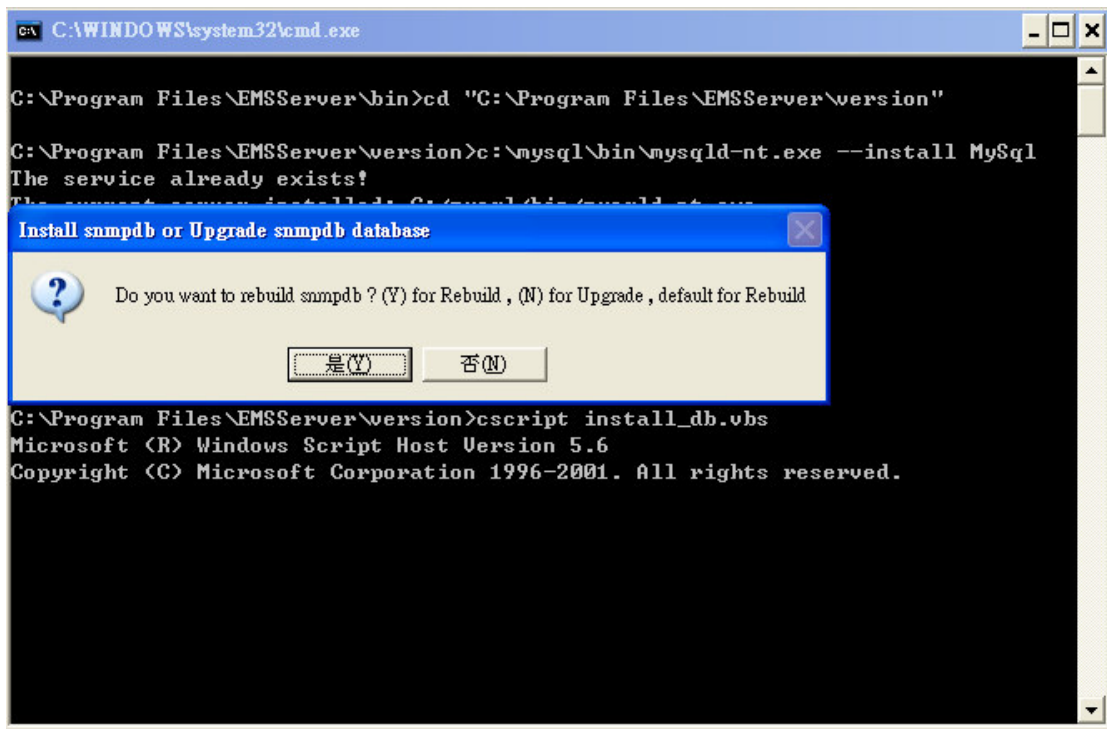


Figure 3-10. CMS server setup program-4

Finally, click Finish button to finish CMS Server installing as Figure 3-11.

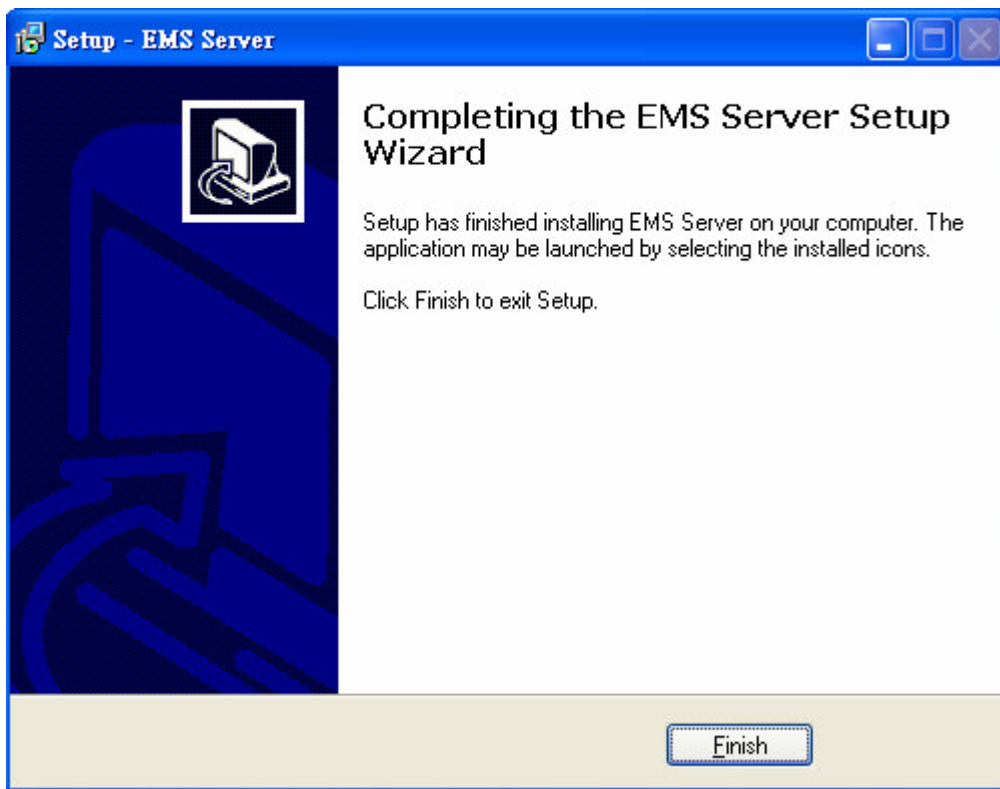


Figure 3-11. CMS server setup program-5

After installing the CMS Server, you must set one environment variable named JAVA_HOME to start the CMS Server. Please follow these steps:

1. Start -> Control Panel as Figure3-12.

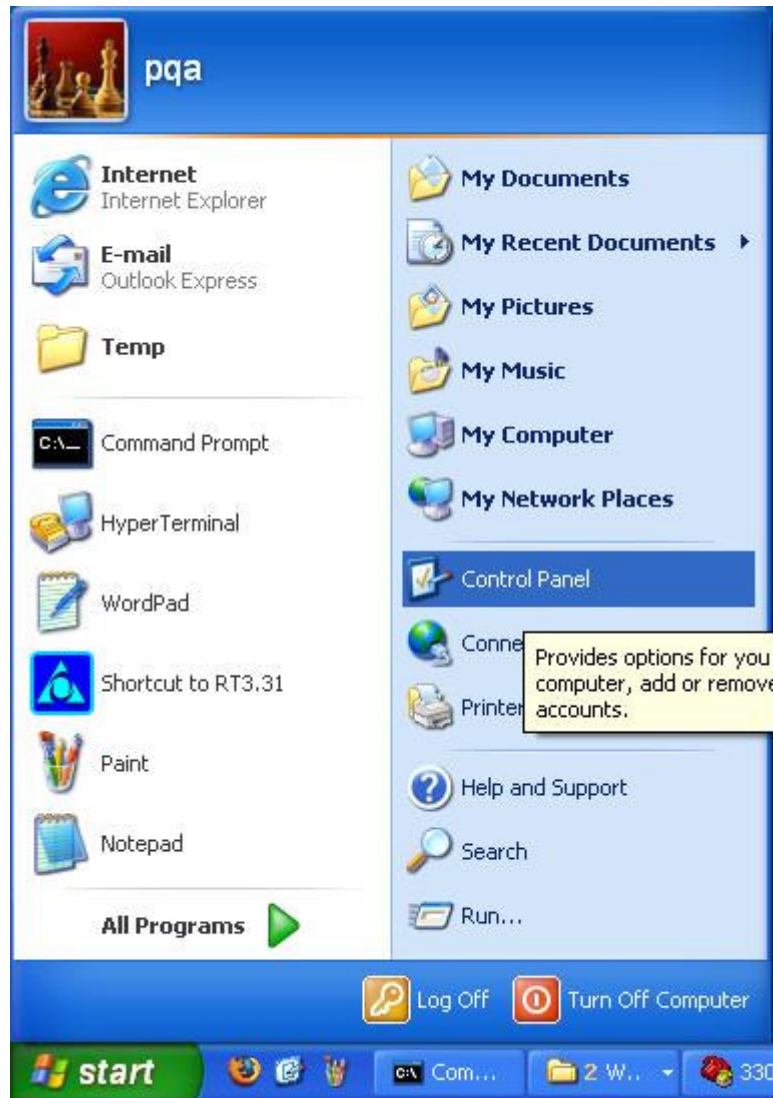


Figure 3-12. CMS server environment-1

Then Press System to start the System Window as Figure3-13.

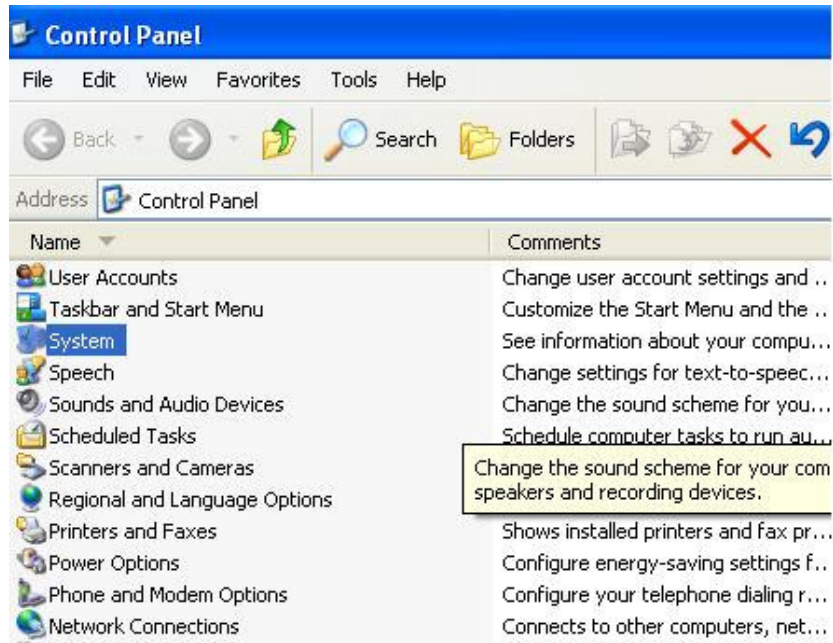


Figure 3-13. CMS server environment-2

2. Find Advanced Tab on System Window.
3. Click Environment Variables button on Advanced Tab to start Environment Variables Dialog as Figure3-14



Figure 3-14. CMS server environment-3

4. Find System Variables on Environment Variables Dialog as Figure 3-15

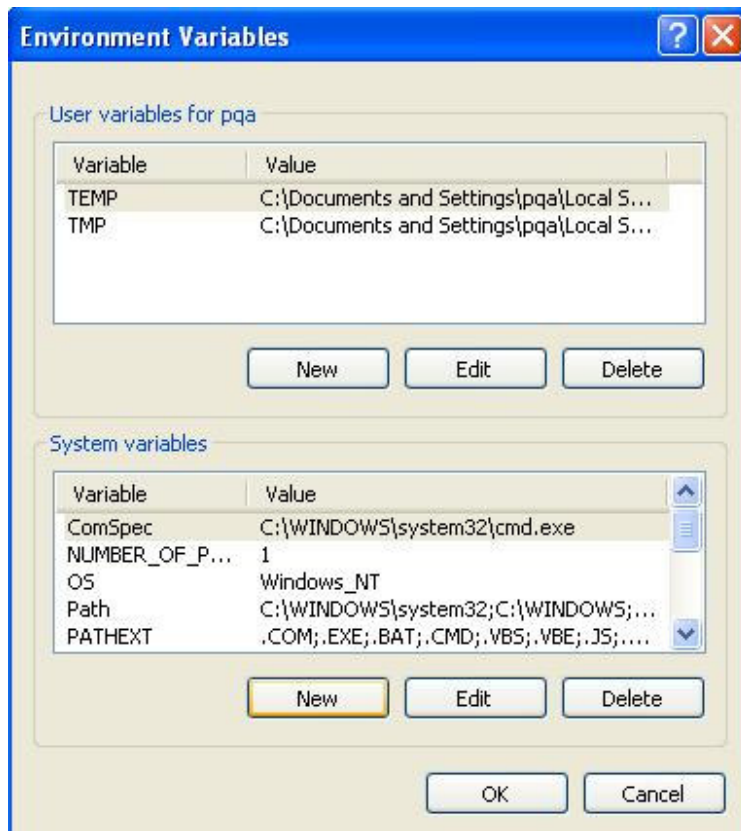


Figure 3-15. CMS server environment-4

5. Click Add button to JAVA_HOME. For instance JAVA_HOME = C:\j2sdk1.4.2_03. as Figure 3-16.

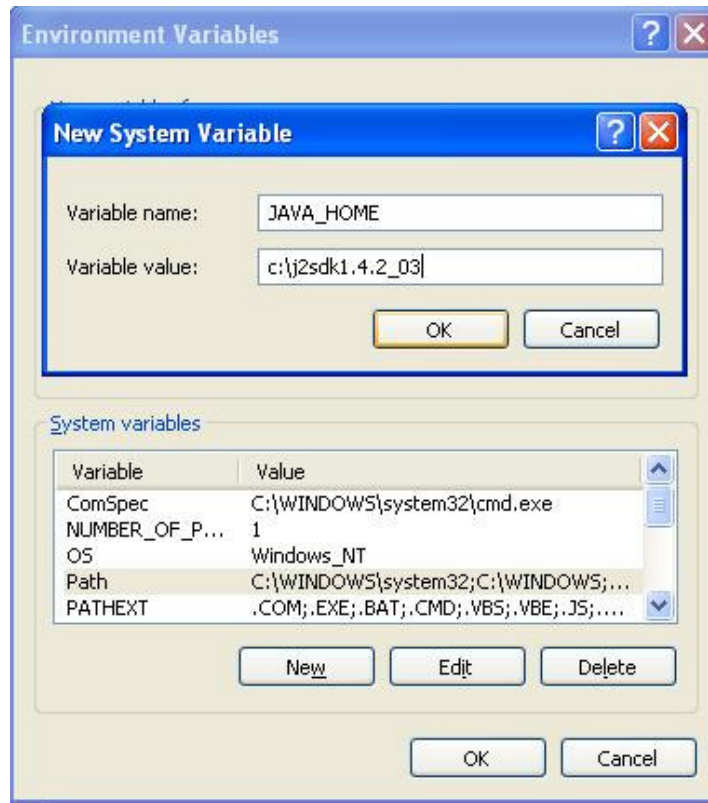


Figure 3-16. CMS server environment-5

Finally the system variable will be like Figure 3-17.

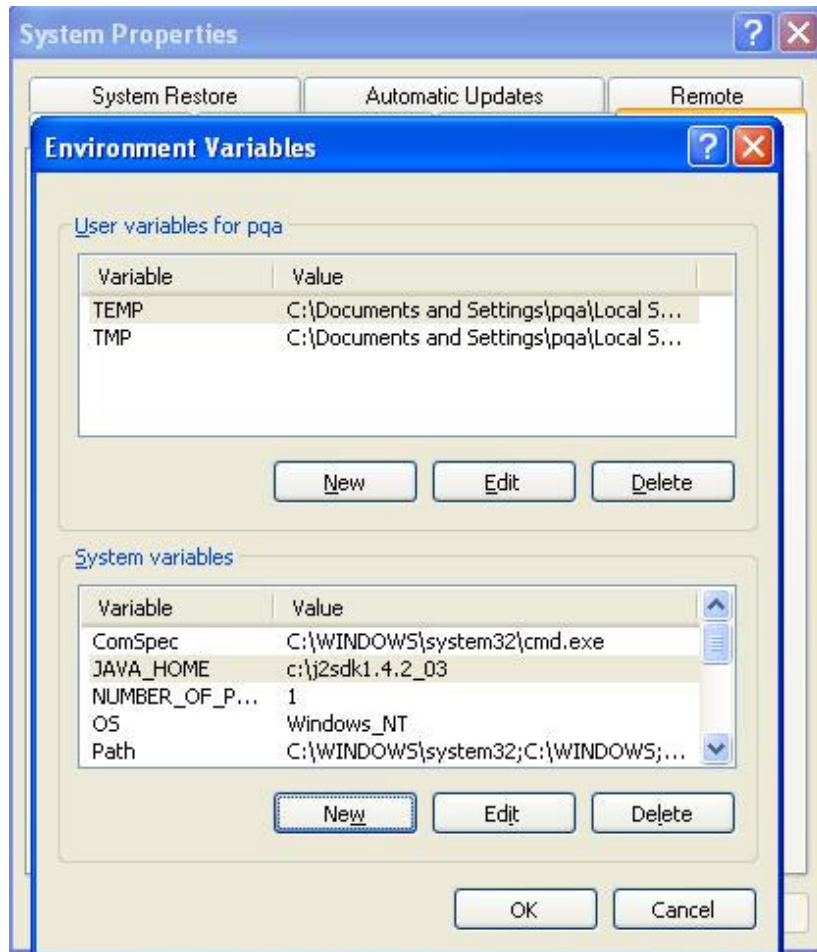


Figure 3-17. CMS server environment-6

For Unix like platform (Solaris and Linux)

Step1: Login Solaris or Linux 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 EMS_Unix_Like_XXX_XXXXXX.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
```

```
chmod 755 uninstall.sh
```

Please make sure you have **/usr/bin/sh** first. If you don't have **/usr/bin/sh**, please do **ln -s /bin/sh /usr/bin/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 CMS Server (It will build one mysql database : snmpdb)*
5. *Install CMS Client*
6. *Upgrade CMS 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 CMS Server (It will build one mysql database : snmpdb)*
5. *Install CMS Client*
6. *Upgrade CMS 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 CMS Server (It will build one mysql database : snmpdb)*
5. *Install CMS Client*
6. *Upgrade CMS Server (It will upgrade snmpdb database)*
7. *Exit*

input select num : 3

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

Step 9: Install CMS application

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

input select num : 4

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

For Linux System

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

input select num :

Because linux os has the library that installing mysql need, it will not appear in menu.

1. Install library : Install the library that installing mysql need. Only display on Solaris System.

2. Install mysql : Install mysql database to save CMS data

3. Install java : Install java software to run CMS

4. Install CMS Server : Install CMS Sever and build snmpdb database that CMS server using.

5. Install CMS Client : Not Available

6. Upgrade CMS Server : If this is not the first time for installing CMS, please select this item to upgrade CMS Server. This will reserve the CMS data you have built.

If your machine do not install any other package, you need to install 1 - 4 step to install CMS Server.

3.1.2.2 Uninstall CMS Server

For Windows 2000™ server or XP high end platform

To uninstall the CMS Server, open the Control Panel, click on the applet "Add/Remove Programs" and choose to remove **CMS Server** and **MySQL**.

For Unix like platform (Solaris and Linux)

To uninstall the CMS server in **Unix like platform (Solaris and Linux)**, run **./uninstall.sh** under the directory **/usr/local/ems/EMSServer/bin**, then the following menu items are shown as below:

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

input select num :

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

3.2 Getting Started

After finishing installation for CMS client and server, the next step is to start CMS program. The steps of starting CMS 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 servers should be refered the user manual.

For Unix like platform (Solaris and Linux)

For Unix like platform (Solaris and Linux) 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 cms*
4. *shutdown cms*
5. *edit bind ip of CMS Server(please keying ip or servername)*
6. *set the MAX and MIN memory value of running java (It will valid after restarting CMS)*
7. *view the MAX and MIN memory value of running java*
8. *exit*

input select num :1



Then MySQL database server is to startup in Unix like platform (Solaris and Linux), and the message is shown as the followings if it is success:

Starting mysqld daemon with databases from/usr/local/mysql/var

Step 2: Start Application server

For Windows 2000TM server or XP high end platform

If you install Application server in the WindowsTM environment, then you can start the CMS server by click **Program->CMS Server->Start CMS Server** to start CMS server. If the server starts at the first time, then a dialog box is shown for inputting the IP address that CMS server using to bind at the first time:Figure 3-18 is shown as an example.



Figure 3-18. Input the IP address CMS server binds



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

For Unix like platform (Solaris and Linux)

For **Unix like platform (Solaris and Linux)** 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 cms
4. shutdown cms
5. edit bind ip of CMS Server(please key in ip or servername)
6. set the MAX and MIN memory value of running java (It will valid after restarting CMS)
7. view the MAX and MIN memory value of running java
8. exit

input select num :3



When CMS 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 cms
4. shutdown cms
5. edit bind ip of CMS Server(please key in ip or servername)
6. set the MAX and MIN memory value of running java (It will valid after restarting CMS)
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 CMS server will use the new IP as the binding IP.



The default size of heaps needed by CMS 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 CMS can be enlarged 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 cms
4. shutdown cms
5. edit bind ip of CMS Server(please key in ip or servername)
6. set the MAX and MIN memory value of running java (It will valid after restarting CMS)
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 CMS Server



If CMS application server is started-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 CMS Client

If you install Application server in the WindowsTM environment, then you can start the CMS client by clicking **Program->CMS Client->Start CMS Client** to start CMS client.

Step 4: Connect to IP DSLAM

The normal procedure to connect to IP DSLAM goes follows:

- I. Setting the IP DSLAM Device.
- II. Add the device to CMS.

Different IP DSLAM device has different way. Please follow the each device guide.

Master Device

1 Setting the IP DSLAM Device.

- I. Login the master by console (9600/8/N/1).
- II. Set the ip address of the outband.

Admin> network outband <Device IP> <Mask>

III. Set trap host

Admin> service snmp -a <HostIP> PS: <HostIP> is CMS Server IP

IV. Change community

Admin> service snmp -c <CommRO> <CommRW> <CommTrap>

PS: Default community is public, private and trap for community of read only, read write, and trap.

The following is an example of the step.

CMS Server IP : 172.16.2.135, Device IP : 172.16.2.151

Admin> network outband 172.16.2.151 255.255.255.0

SUCCESS : Command done.

Admin> service snmp -a 172.16.2.135

SUCCESS : Command done.

Admin> service snmp -c public private trap

SUCCESS : Command done.

2 Add the device to CMS.

- I. The CMS Server must have the ability to connect to the device by device IP. If the CMS Server IP and device IP are on the same domain, you can use a switch to connect CMS Server and device.

For instance, CMS Server IP is 172.16.2.135 and device IP is 172.16.2.151, the connect diagram is following :

CMS Server (172.16.2.135) ----- Switch ----- Device 1 (172.16.2.151)

- II. Please start CMS Client and connect to CMS Server first. Choose Network -> New Device on Main Menu to add the device to CMS Server for management. Input device ip, read community, and write community as you set on the device. Finally select the device type to Master-Slave.

Slave Device

1 Setting the IP DSLAM Device.

- I. Login the slave by console (9600/8/N/1).
- II. Configuration the management ip address for uplink port.
\$aggr intf ifname aggr-0 ip <ip> mask <mask> usedhcp false
- III. Create the SNMP related parameters
\$create snmp comm community <read-community>ro
\$create snmp comm community <write-community>rw
\$create snmp host ip <server ip> community <read-community>
\$create snmp host ip <server ip> community <write-community>
\$create snmp trap host ip <server ip> community <trap-community>
- IV. Save the configuration
\$commit

the following is an example:

```
CMS Server IP : 172.16.2.135, Device IP : 172.16.2.151
$aggr intf ifname aggr-0 ip 172.16.2.151 mask 255.255.255.0 usedhcp false
$create snmp comm community public ro
$create snmp comm community private rw
$create snmp host ip 172.16.2.151 community public
$create snmp host ip 172.16.2.151 community private
$create snmp trap host ip 172.16.2.151 community trap
$commit
```

2 Add the device to CMS.

- I. The CMS Server must have the ability to connect to the device by device IP. If the CMS Server IP and device IP are on the same domain, you can use a switch to connect CMS Server and device. For instance, CMS Server IP is 172.16.2.135 and device IP is 172.16.2.151, the connect diagram is as following:
CMS Server (172.16.2.135) ----- Switch ----- Device 1 (172.16.2.151)
- II. Please start CMS Client and connect to CMS Server first. Choose Network -> New Device on Main Menu to add the device to CMS Server for management. Input device ip, read community, and write community as you set on the device. Finally select the device type to Slave - Standalone.

3.2.1 CMS Window Menu

The CMS client program provides a menu-driven function user interface for operators. The windows menu hierarchy is depicted in the following Figure 3-19:

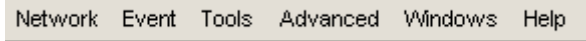


Figure 3-19. CMS window menus

The CMS client program provides a multiple document interface for using one mainframe window with several child windows.

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

3.2.2 CMS Menu Item

The main functions of CMS 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 for 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 CMS 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, CMS provides some utilities for diagnose devices such as ping and trace route.

This chapter describes all configuration functions; includes device management functions, system management functions.

This chapter is divided into the following sections,

- Section 4.1: Device Management
- Section 4.2: DSL Configuration
- Section 4.3: PVC Functions
- Section 4.4: Port Configuration
- Section 4.5: Bridge Configuration
- Section 4.6: ACL Configuration
- Section 4.7: System Management

4.1 Device Management

Device management includes controller configuration and DSL configuration.

4.1.1 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 CMS main window, a device configuration window will be shown as Figure 4-1. The sub functions of device configuration are described as followings:

4.1.2 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 reading operations from CMS to device in SNMP. This value should be set the same as that of the device. If the community set in CMS is not the same as that of the device, this operation will be rejected.

Write Community

The community set for setting operations from CMS to device by SNMP. This value must be set the same as that of the device. If the community set in CMS 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 CMS used to communicate with the device.

The screenshot shows a web-based configuration interface for a network device. At the top, there are three tabs: 'Status', 'Interfaces', and 'ThroughPut'. The 'Status' tab is active. The main content area contains several configuration fields arranged in two columns. The left column includes 'Display Name' (172.16.2.225-Master), 'IP' (172.16.2.225), 'SNMP Version' (V2), and 'Write Community' (private). The right column includes 'Device Type' (V3600M), 'Sys Location' (http://www.lucent.com), 'Read Community' (public), and 'SNMP Port' (161). To the right of these fields are two buttons: 'Refresh' and 'Update'. At the bottom of the interface, there is a row of tabs: 'Controller', 'DSL', 'PVC', 'Port', 'Bridge', and 'ACL'. The 'Controller' tab is currently selected.

Figure 4-1. Device status configurations

4.1.3 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 them from being deliverable to a higher-layer protocol.

OutDiscards

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

InErrors

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

OutErrors

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

Figure 4-2 is shown as an example.

Status		Interfaces		ThroughPut					
	Interfaces	InOctets	OutOctets	InDiscards	OutDiscards	InErrors	OutErrors		
1	G0	73914352	76415325	0	0	0	0	Refresh	
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		

Controller DSL PVC Port Bridge ACL

Figure 4-2. The performance data of network interfaces

4.1.4 Controller/Through Put

The throughput for selecting 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 is shown as an example.

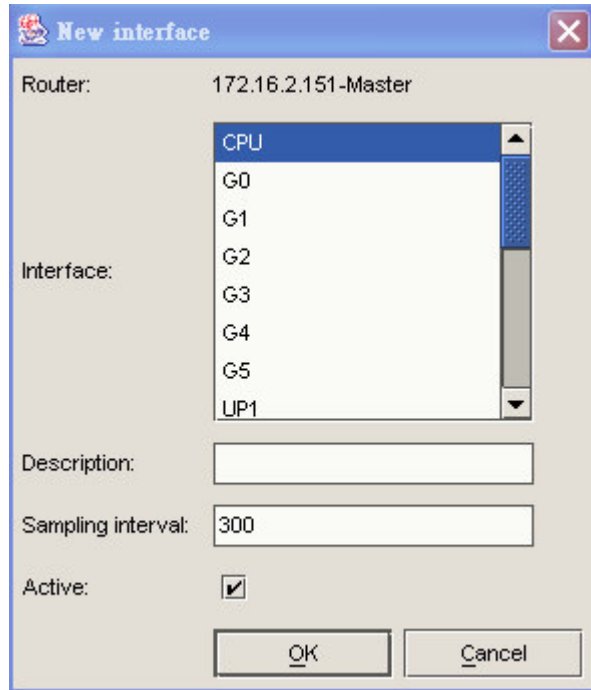


Figure 4-3. The network interfaces selection box

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, or by year. Select a type you can monitor, then the statistic information will be shown for a long time.

Figure 4-4 is shown as an example.

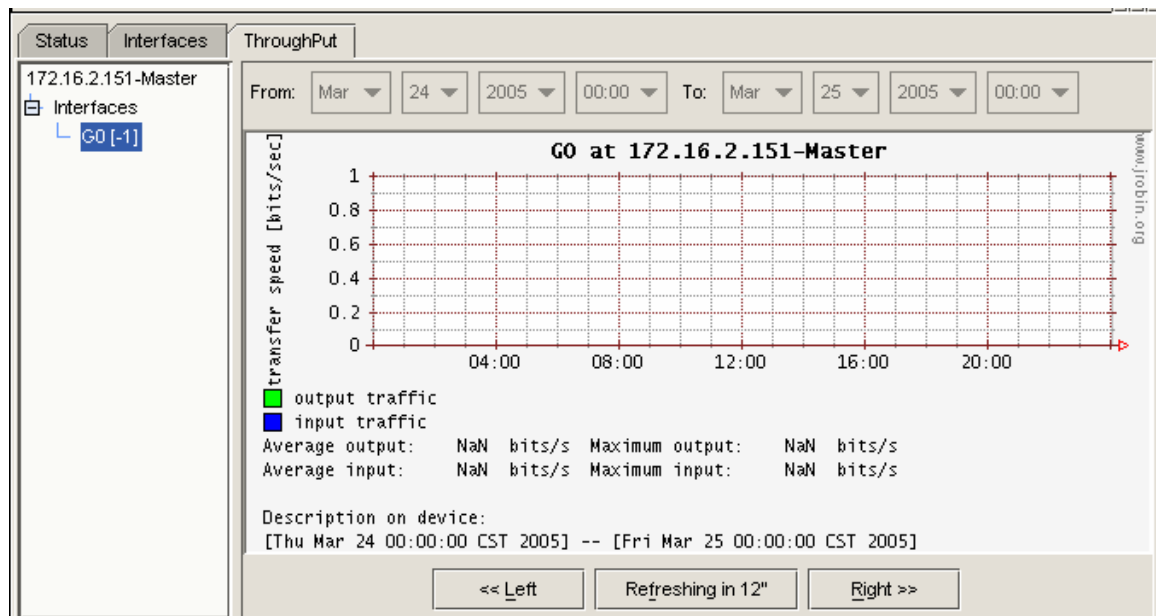


Figure 4-4. The throughput of G0 by hours

4.1.5 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 is shown the location of Reboot function as below.

<Device>	
Controller ▶	Status
DSL ▶	Interfaces
VLAN	Throughput
101th (101)	Commit
102th (102)	Version
103th (103)	Reset
104th (104)	FW Upgrade
Default-Vlan (Backup/Restore
Default-Vlan (

Figure 4-5. Reboot function for controller card

There are options for resetting 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).

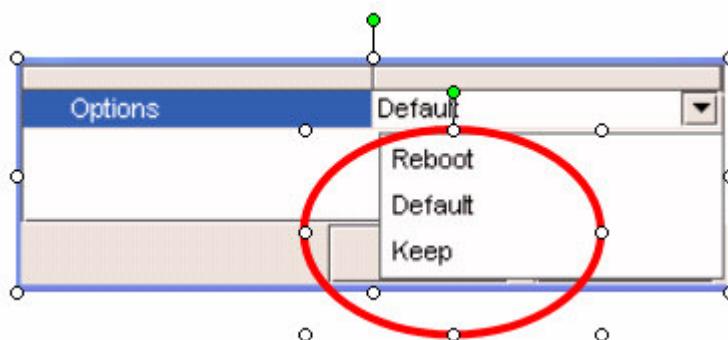


Figure 4-6. The reboot for the controller card: the options for reboot.

4.1.6 Controller/Commit

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

Figure 4-7 is shown the location of Commit function as below.

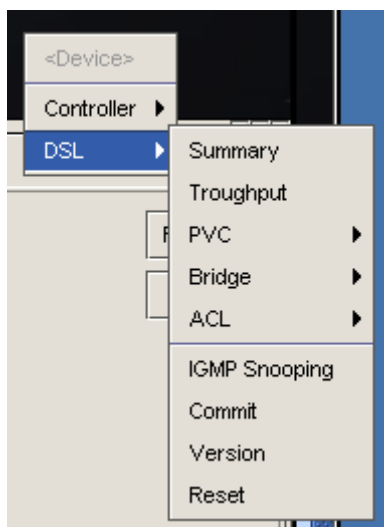


Figure 4-7. Commit function for controller card

4.1.7 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 IP DSLAM device, there are two types for IP DSLAM devices: master and slave.

Software Version of master

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

Hardware Version of master

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

Hardware Version of slave

The version of hardware set for the DSL card is located in the IP DSLAM device.

Control Plane Firmware

The version of software set for the DSL card is located in the IP DSLAM device.

Data Plane Firmware

The version of software set for the DSL card is located in the IP DSLAM device.

Figure 4-8 is shown the version information of the master device as below.

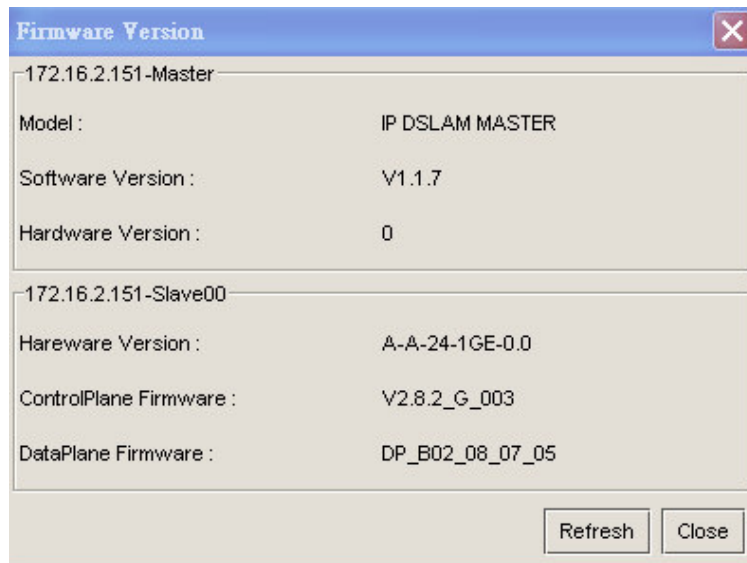


Figure 4-8. The version information of the master device

4.1.8 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 CMS 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.

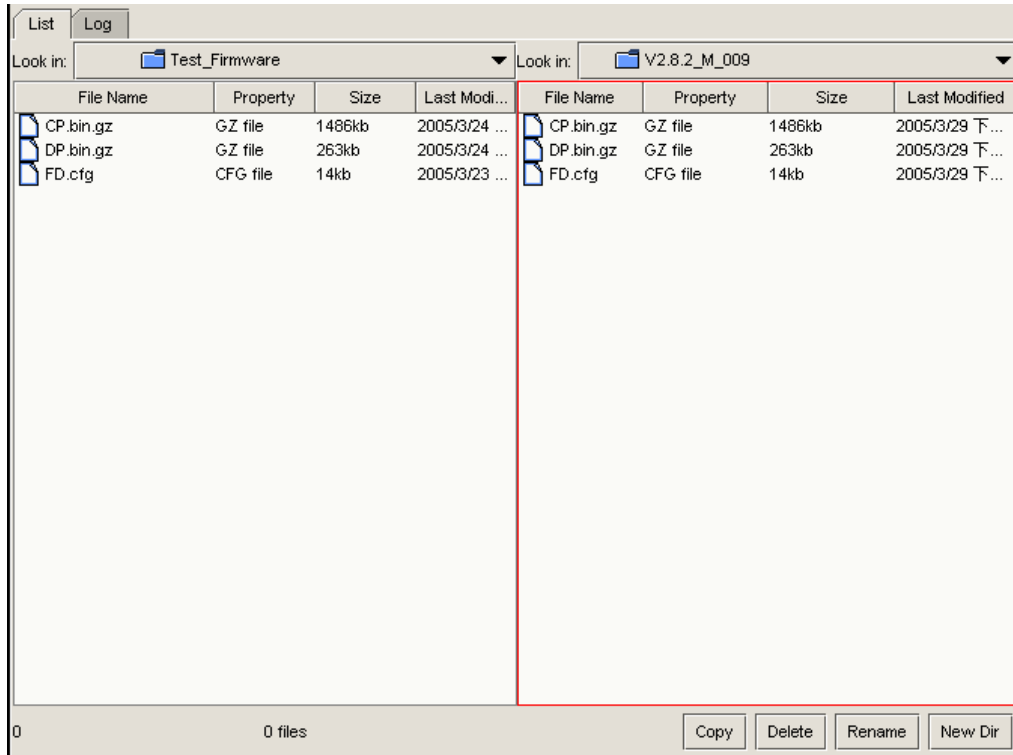


Figure 4-9. File upload window

In this window, the local directory is located in the left panel, and users can select the files that 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 IP DSLAM 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. The page is shown in Figure 4-10.

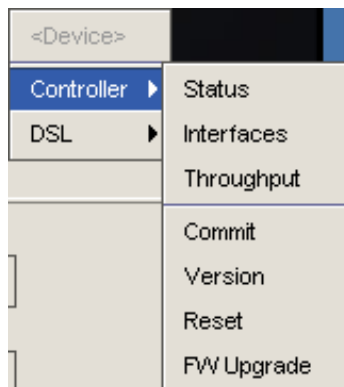


Figure 4-10. The menu function of firmware upgrade for controller

By selecting the firmware ready to upgrade, select “Upgrade” function to upgrade the firmware: Figure 4-11 is shown the version information of the master device.

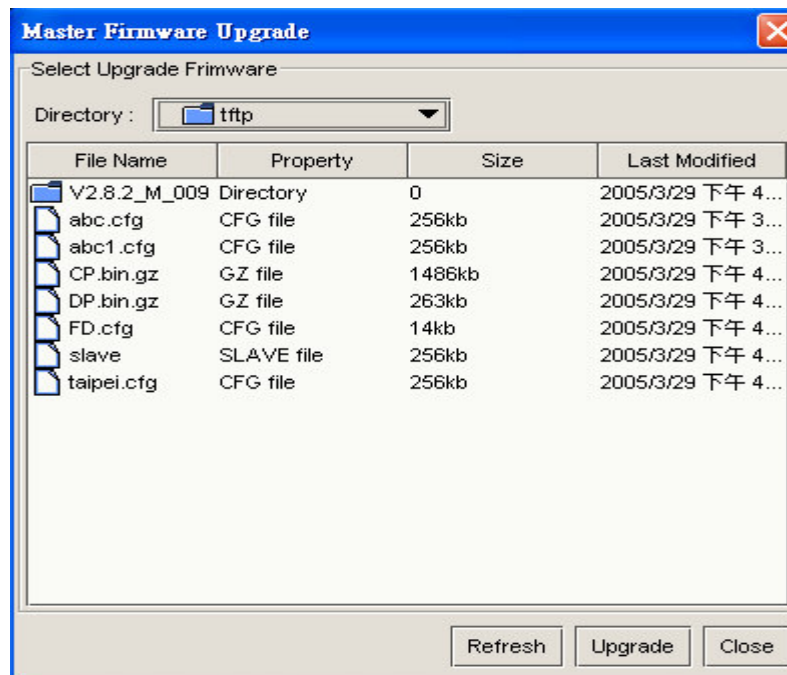


Figure 4-11. The version information of the master device

When you select “upgrade” function, the selected file are upload to the device, the page is shown in Figure 4-12.

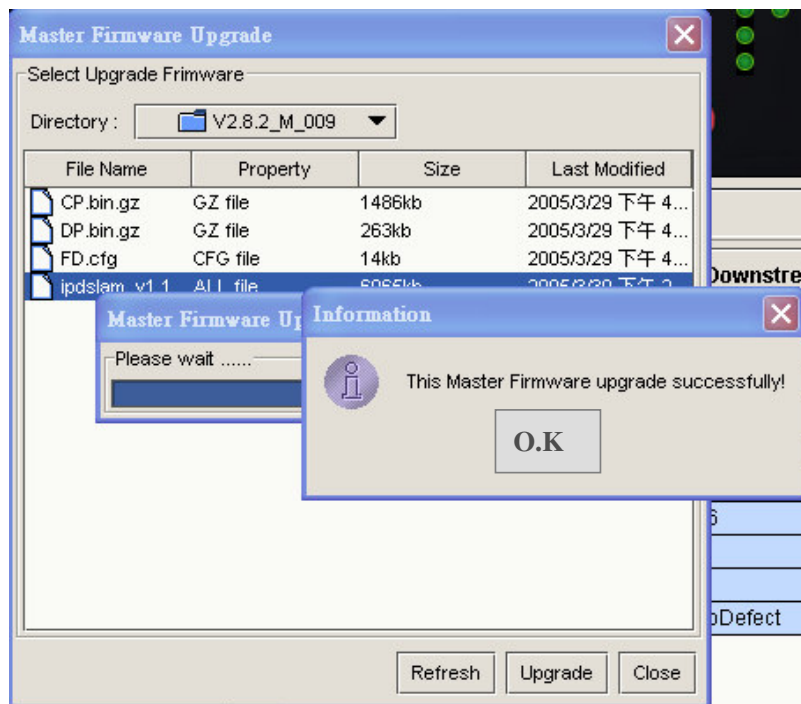


Figure 4-12. Firmware upgrade function for controller card

After finishing the firmware function, you need to reboot the controller card. The page is shown in Figure 4-13.

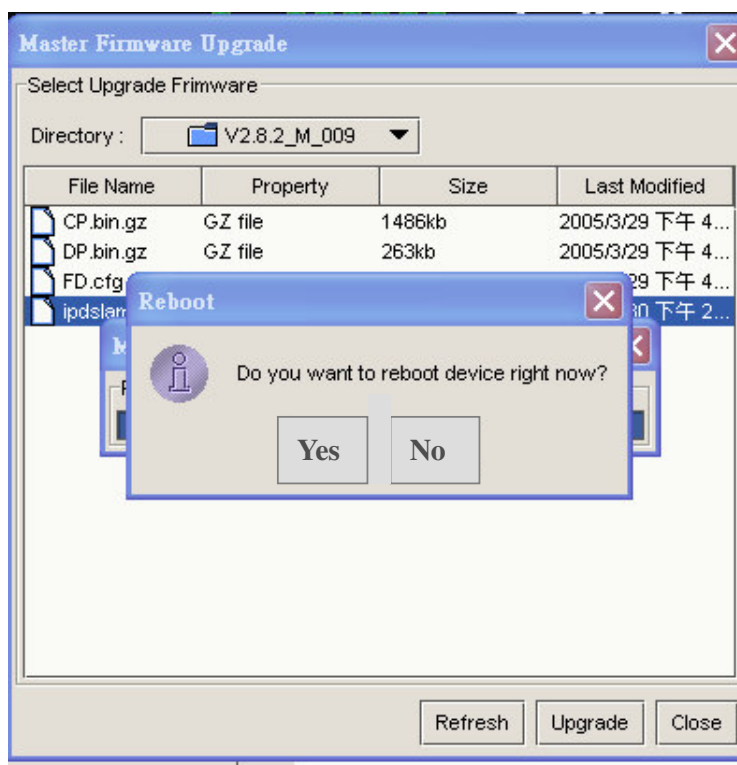


Figure 4-13. The system prompts a “Reboot” message

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. The menu function of firmware upgrade for DSL card is shown in Figure 4-14.

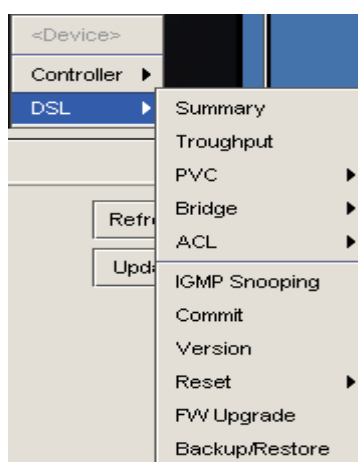


Figure 4-14. The menu function of firmware upgrade for DSL card

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 is shown as below.

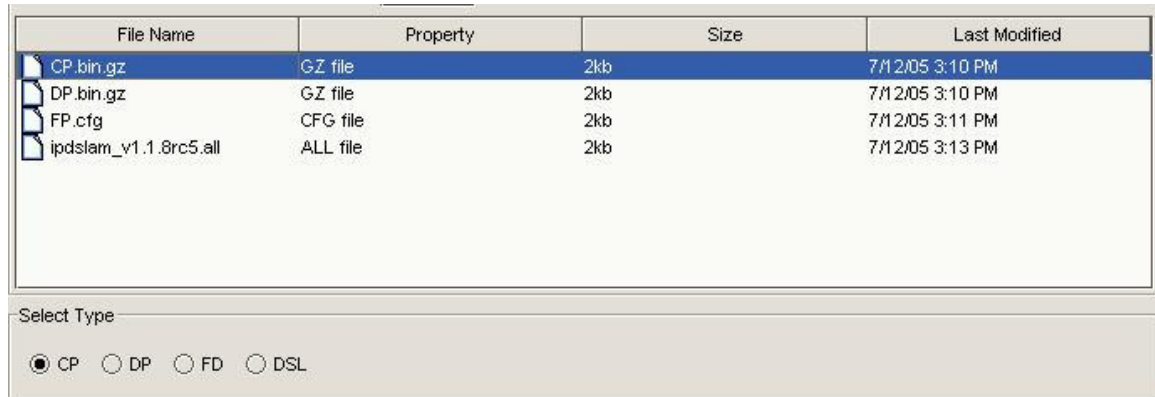


Figure 4-15. The firmware upgrade function for DSL card



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.



Figure 4-16. Reboot the DSL card after firmware upgrade

After all three files are upgrade to the IP DSLAM device, you should reboot DSL card manually. Select “DSL->Reset->Last” to reboot the device. The page is shown in Figure 4-16.

4.1.9 Configuration Backup and Restore

The configuration for DSL cards or controller can be grouped into a file, and can be retrieved by CMS. When downloading to CMS server, the file is transferred by TFTP protocol. This file is stored in the location of TFTP server, provided for restoring to devices if necessary.

To 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.

To 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.

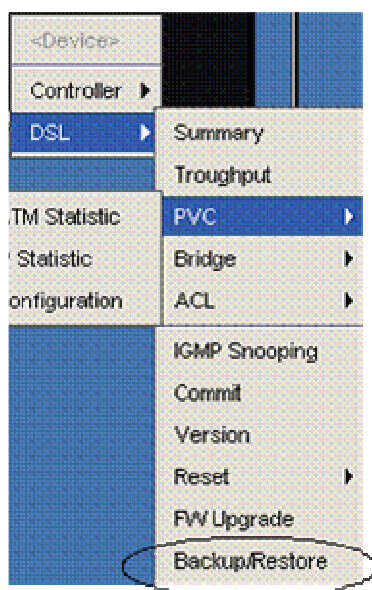


Figure 4-17. Select the backup and restore function

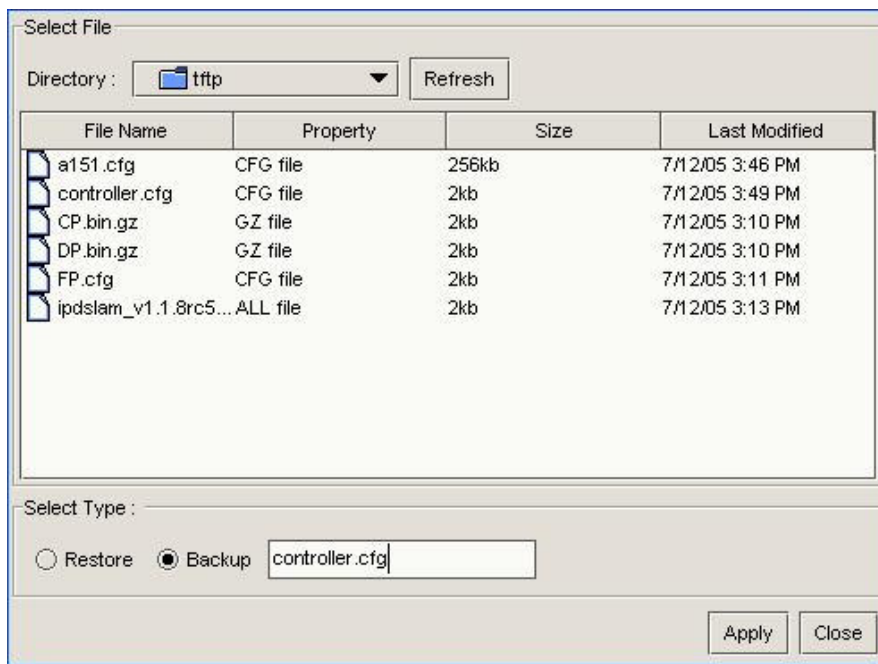


Figure 4-20. Backup the configuration from the device

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 restore function. The page is shown in Figure 4-21.

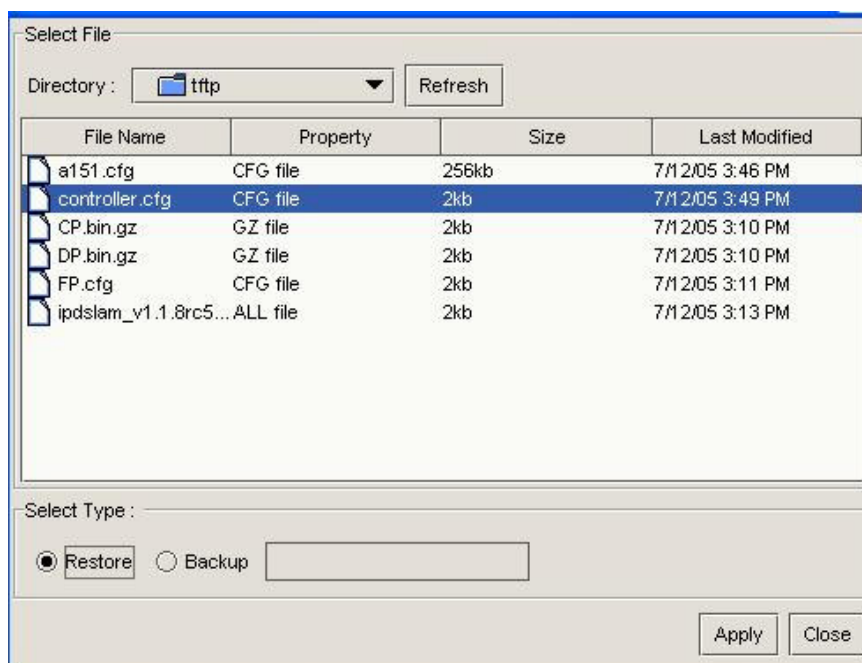


Figure 4-21. Restore the configuration to the device

4.2 DSL Configuration

4.2.1 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 information if **Poll** option is turned on.

Figure 4-22 is shown the Summary Configurations as below:

	Op Status	Standard	SNR DN (1/10dB)	SNR UP (1/10dB)	Intl DN	Intl UP
1	handshake	----	----	----	----	----
2	handshake	----	----	----	----	----
3	handshake	----	----	----	----	----
4	handshake	----	----	----	----	----
5	handshake	----	----	----	----	----
6	handshake	----	----	----	----	----
7	handshake	----	----	----	----	----
8	handshake	----	----	----	----	----
9	handshake	----	----	----	----	----
10	handshake	----	----	----	----	----
11	handshake	----	----	----	----	----
12	handshake	----	----	----	----	----

Finish to retrieve port status

DSL | PVC | Port | Bridge | ACL

Figure 4-22. Summary configurations

4.3 PVC Functions

The function of throughput for DSL card is similar to that for controller. The interfaces for DSL is PVC-based.

4.3.1 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 policy.

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

4.3.2 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”.

Figure 4-23 is shown the IP Statistics of PVC as below.

	Port	PVC	InOctets	OutOctets	InUcastPkts	OutUcastPkts	Int
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

4.3.3 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 Figure 4-24.

ode	Channel	VLAN	IGMP Snoop Leave Mode	802.1P	Traffic Class
1	Interleaved	Default-Vlan(1)	fastNormal	0	Default
2	Interleaved	Default-Vlan(1)	fastNormal	0	Highest
3	Interleaved	Vlan-2(2)	fastNormal	0	Default
4	Interleaved	Vlan-3(3)	fastNormal	0	Default
5	Interleaved	Vlan-4(4)	fastNormal	0	Default
6	Interleaved	Default-Vlan(1)	fastNormal	0	Default
7	Interleaved	Vlan-2(2)	fastNormal	0	Default
8	Interleaved	Vlan-3(3)	fastNormal	0	Default
9	Interleaved	Vlan-4(4)	fastNormal	0	Default
10	Interleaved	Default-Vlan(1)	fastNormal	0	Default
11	Interleaved	Vlan-2(2)	fastNormal	0	Default
12	Interleaved	Vlan-3(3)	fastNormal	0	Default
13	Interleaved	Vlan-4(4)	fastNormal	0	Default
14	Interleaved	Default-Vlan(1)	fastNormal	0	Default
15	Interleaved	Vlan-2(2)	fastNormal	0	Default

Figure 4-24. PVC configurations

Name

The name of this PVC sets in the device.

Port

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

PVC

The identifier of PVC for some port sets 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 sets for this PVC.

VCI

The value of VCI sets for this PVC.

RFC2684 Bridge Mode

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

Channel

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

VLAN

The VLAN ID sets 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 sets in the PVC should be *normal*, *fast* and *fastNormal*.

802.1P

Set the upstream priority on this PVC.

Traffic Class

Set the downstream priority on this PVC. You must define the different traffic class on the Profile manager. Please refer to the Profile Manager chapter.

OAM

This function provides F5 loop-back tests for one port. If the port is not connected, this function would not be performed.

Figure 4-25 is shown the OAM Test Dialog as below.

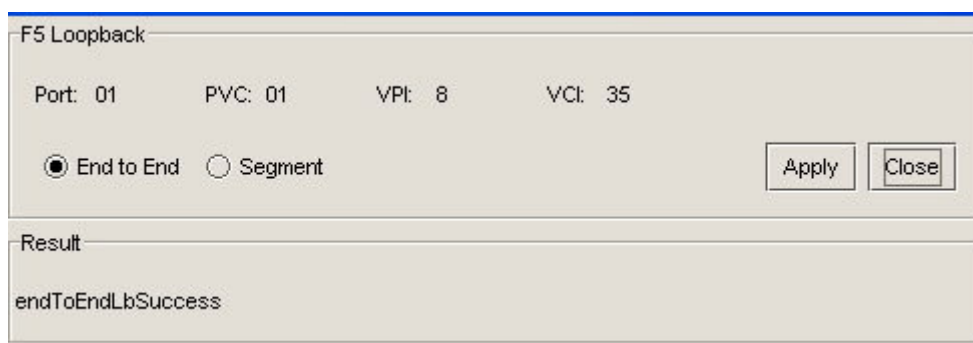


Figure 4-25. OAM test dialog

4.4 Port Configuration

4.4.1 Port/Status

The status for each port set in the device. You can refresh, show bin map, test DELT and enable or disable the port in this window. Figure 4-26 is shown as below.

Item	Upstream	Downstream
1 Noise Margin(1/10dB)	85	55
2 Output Power(1/10dB)	5	83
3 Attainable Bitrate(bps)	1320600	28021269
4 Attenuation(1/10dB)	0	132
5 Interleave Current Rate	1088800	22936200
6 Interleave Previous Rate	1088800	24944287
7 Interleave Delay	13	4
8 Fast Current Rate	0	0
9 Fast Previous Rate	0	0
10 Current Status	noDefect	noDefect

Figure 4-26. 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 **adslAtucRateChangevTrap** event for interleave mode. It is also set at initialization to prevent a trap from 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 from 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 startupexchange data.
7 configInitFailure	ATUC is failure during initialization due to peer ATU not be 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.

4.4.2 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 clicking the option for **ATU-C** or **ATU-R**. **Refresh** button is used to retrieve data again.

Figure 4-27 is shown the port performance configuration as below.

	TYPE	PERF	15MIN CURR	1DAY CURR	1DAY PREV	
1	Time Elapsed	-----	808	18808	86400	Port Number : 1 ▾ <input checked="" type="radio"/> ATU-C <input type="radio"/> ATU-R <input type="button" value="Refresh"/>
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 4-27. Port performance configurations

The meanings for these time units are described as followings:

PERF	Description
LOFs	Count of the number of Loss of Framing failures since agent reset.
LOSs	Count of the number of Loss of Signal failures since agent reset.
LOLs	Count of the number of Loss of Link failures since agent reset.
LPRs	Count of the number of Loss of Power failures since agent reset.
ESs	Count of the number of Errored Seconds since agent reset.
Inits	Count of the line initialization attempts since agent reset. Includes both successful and failed attempts.
Interleave RxBLKS	Count of all encoded blocks received on this channel since agent reset in interleaved channel.

Interleave TxBLKs	Count of all encoded blocks transmitted on this channel since agent reset in interleaved channel.
Interleave CoBLKs	Count of all blocks received with errors that were corrected since agent reset in interleaved channel.
Interleave UnCoBLKs	Count of all blocks received with uncorrectable errors since agent reset in interleaved channel.
Fast RxBLKs	Count of all encoded blocks received on this channel since agent reset in fast channel.
Fast TxBLKs	Count of all encoded blocks transmitted on this channel since agent reset in fast channel.
Fast CoBLKs	Count of all blocks received with errors that were corrected since agent reset in fast channel.
Fast UnCoBLKs	Count of all blocks received with uncorrectable errors since agent reset in fast channel.

15MIN CURR, 1DAY CURR, 1DAY PREV	Description
Time Elapsed	Total elapsed seconds in this interval. (current 15-min interval, current 1-day interval, or previous 1-day interval)
LOFs	Count of seconds in the interval when there was Loss of Framing.
LOSs	Count of seconds in the interval when there was Loss of Signal.
LOLs	Count of seconds in the interval when there was Loss of Link.
LPRs	Count of seconds in the interval when there was Loss of Power.
ESs	Count of Errored Seconds in the interval. The errored second parameter is a count of one-second intervals containing one or more crc anomalies, or one or more los or sef defects.
Inits	Count of the line initialization attempts in the interval.
Interleave RxBLKs	Count of all encoded blocks received within the interval in interleaved channel.
Interleave TxBLKs	Count of all encoded blocks transmitted within the interval in interleaved channel.
Interleave CoBLKs	Count of all blocks received with errors that were corrected within the interval in

	interleaved channel.
Interleave UnCoBLKs	Count of all blocks received with uncorrectable errors within the interval in interleaved channel.
Fast RxBLKs	Count of all encoded blocks received within the interval in fast channel.
Fast TxBLKs	Count of all encoded blocks transmitted within the interval in fast channel.
Fast CoBLKs	Count of all blocks received with errors that were corrected within the interval in fast channel.
Fast UnCoBLKs	Count of all blocks received with uncorrectable errors within the interval in fast channel.

4.4.3 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 parameters, you should click the **setting value** field, then input the new value and click **Apply** button. **Reset** button will restore the value. The page is shown in Figure 4-28.

Category	Parameter	Value 1	Value 2
Downstream Rate	Intl Max Tx Rate(bps)	32736000	32736000
	Intl Min Tx Rate(bps)	32000	32000
	Max Intl Delay(ms)	63	63
	Fast Max Tx Rate(bps)	32736000	32736000
	Fast Min Tx Rate(bps)	32000	32000
Upstream Rate	Intl Max Tx Rate(bps)	1088000	1088000
	Intl Min Tx Rate(bps)	32000	32000
	Max Intl Delay(ms)	16	16
	Fast Max Tx Rate(bps)	1088000	1088000
	Fast Min Tx Rate(bps)	32000	32000
Downstream SNR Margin	Target SNR Margin(1/10dB)	60	60
	Max SNR Margin(1/10dB)	310	310
	Min SNR Margin(1/10dB)	0	0

Fast Max Tx Rate(bps)

Figure 4-28. Line profile configurations

4.4.3.1 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

4.4.3.2 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

4.4.3.3 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.

4.4.3.4 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.

4.4.4 Advanced

Atuc Rate mode

Define 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

Define 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 ATR. 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

Select 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.

4.4.5 SRA

Seamless rate adaptation (SRA), a key feature of ADSL2, enables the transceiver to monitor line conditions and dynamically adapt the data rate seamlessly, i.e., without bit errors or requiring a service interruption for retraining.

SRA can be enabled/disabled dynamically while in data mode. SRA is only supported in the downstream direction; upstream SRA is not supported. The receiver initiates SRA, therefore in the downstream direction the CPE is the master and enables SRA.

Downshift SNR Mgn

Set signal/noise margin for rate downshift in the ATUR.

Upshift SNR Mgn

Set signal/noise margin for rate upshift in the ATUR.

MinDownshift Time

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

MinUpshift Time

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

The following Figure 4-29 provides a pictorial view of SRA and how these parameters will be used to manage rate adjustment.

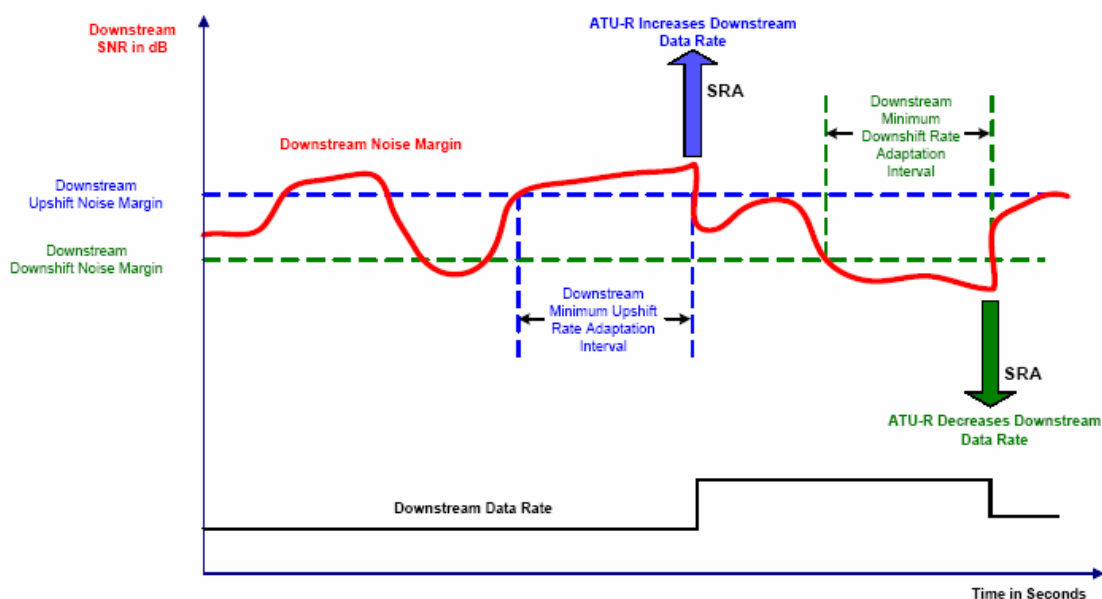


Figure 4-29.

4.4.6 Power Management

With millions of ADSL modems deployed around the world operating at full power 24x7, a significant amount of electricity is consumed. Statistically today, 95% of the time the ADSL modem is idle and not transmitting or receiving any data. A good deal of power can be saved if the modems engage in a standby/sleep mode, similar to computers as defined in the USA by the Energy Star requirements and elsewhere in the world. In addition, this would save power for ADSL transceivers operating in small remote units and digital loop carrier (DLC) cabinets that operate under very strict heat dissipation requirements.

To address these concerns, ITU-T G.992.3 introduces a set of power management states for the ADSL2 link and the use of the overhead messages to coordinate power management between the ATU-C and ATU-R. Power reduction can be achieved by

minimizing the energy transmitted by the ATU as well as by reducing the power consumed by the ATU. As specified in G.992.3, power management is in the downstream direction only.

Power Management allows for changes in the downstream control parameters without a retrain, or errors (i.e., seamless). Power management is similar to Seamless Rate Adaptation in that the signaling mechanism is the same, allowing both features to seamlessly modify downstream configuration. The procedures for power management support:

- Changing parameters to minimize the aggregate transmit power
- Changing parameters to dynamically change the data rate

PM Mode

PM-related parameter used by the ATU-C to set the allowed link states. There are several modes including disable, l3enable, l2enable, l3l2enable.

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 ranged from 900 to 65535.

The following Figure 4-30 provides a pictorial view of Power Management and how these parameters will be used to manage rate adjustment.

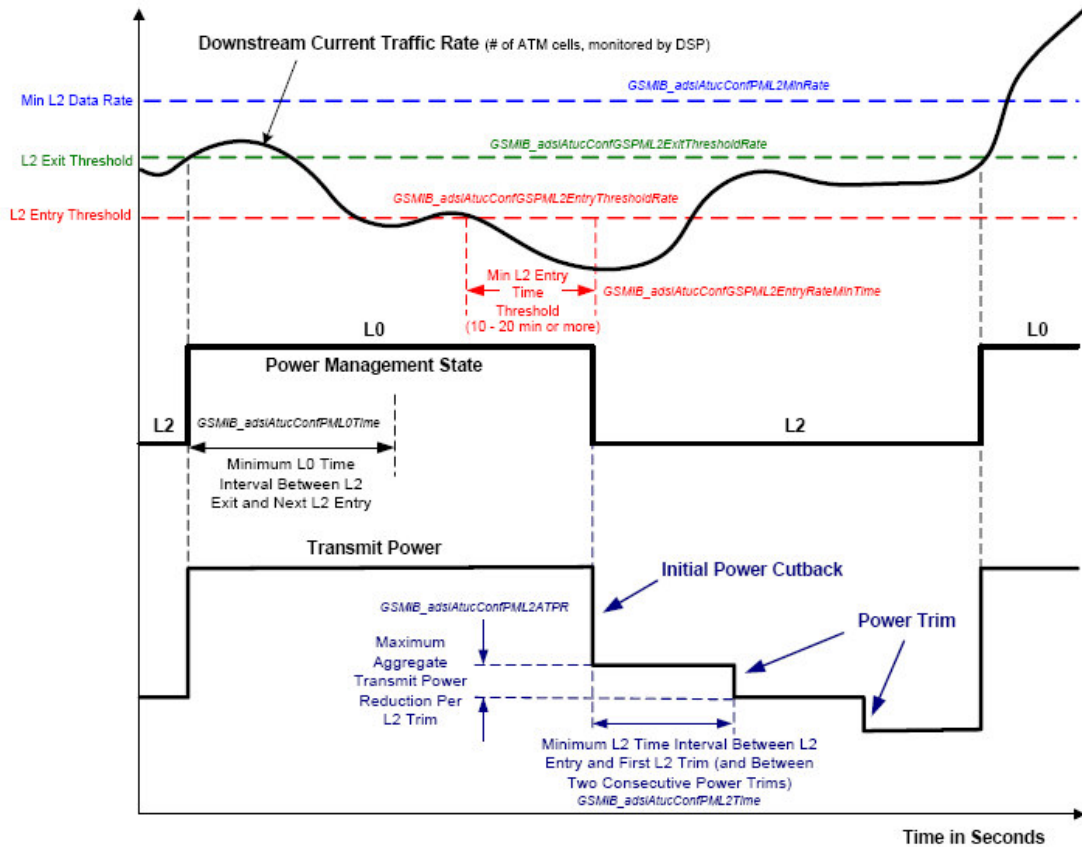


Figure 4-30.

4.4.7 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 4-31 is shown the Alarm profile as below.

Status					Performance					Line Profile					Alarm Profile					PM History				
	Configuration				Current Value				Setting Value				Port Number :											
1	Atuc Thresh 15MinLofs				0				0				1											
2	Atuc Thresh 15MinLoss				0				0				Apply											
3	Atuc Thresh 15MinLols				0				0				Reset											
4	Atuc Thresh 15MinLprs				0				0				Refresh											
5	Atuc Thresh 15MinESs				0				0															
6	Atuc Thresh FastRateUp				4000				4000															
7	Atuc Thresh InterleaveRateUp				4000				4000															
8	Atuc Thresh FastRateDown				4000				4000															
9	Atuc Thresh InterleaveRateDown				4000				4000															
10	Atuc InitFailureTrapEnable				disable				disable															
11	Atur Thresh 15MinLofs				0				0															
12	Atur Thresh 15MinLoss				0				0															
13	Atur Thresh 15MinLols				0				0															
14	Atur Thresh 15MinLprs				0				0															
15	Atur Thresh FastRateUp				0				0															
16	Atur Thresh InterleaveRateUp				0				0															

Figure 4-31. 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 15MinLoss

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 changes 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 changes 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 changes 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 changes 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 changes 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 changes 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 changes 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 changes 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.

4.4.8 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 clicking the option for **ATU-C** or **ATU-R**. **Refresh** button is used to retrieve data again. The page is shown in Figure 4-32.

Status	Performance	Line Profile	Alarm Profile	PM History																																																																																																																																
				<table border="1"> <thead> <tr> <th></th> <th>Time</th> <th>LOFs</th> <th>LOSs</th> <th>LOLs</th> <th>LPRs</th> <th>ESs</th> <th>I</th> </tr> </thead> <tbody> <tr><td>1</td><td>2005-03-23 17:35:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>2</td><td>2005-03-23 17:20:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>3</td><td>2005-03-23 17:05:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>4</td><td>2005-03-23 16:50:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>5</td><td>2005-03-23 16:35:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>6</td><td>2005-03-23 16:20:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>7</td><td>2005-03-23 16:05:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>8</td><td>2005-03-23 15:50:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>9</td><td>2005-03-23 15:35:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>10</td><td>2005-03-23 15:20:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>11</td><td>2005-03-23 15:05:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>12</td><td>2005-03-23 14:50:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>13</td><td>2005-03-23 14:35:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>14</td><td>2005-03-23 14:20:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>15</td><td>2005-03-23 14:05:04</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> </tbody> </table>		Time	LOFs	LOSs	LOLs	LPRs	ESs	I	1	2005-03-23 17:35:04	0	0	0	0	0	0	2	2005-03-23 17:20:04	0	0	0	0	0	0	3	2005-03-23 17:05:04	0	0	0	0	0	0	4	2005-03-23 16:50:04	0	0	0	0	0	0	5	2005-03-23 16:35:04	0	0	0	0	0	0	6	2005-03-23 16:20:04	0	0	0	0	0	0	7	2005-03-23 16:05:04	0	0	0	0	0	0	8	2005-03-23 15:50:04	0	0	0	0	0	0	9	2005-03-23 15:35:04	0	0	0	0	0	0	10	2005-03-23 15:20:04	0	0	0	0	0	0	11	2005-03-23 15:05:04	0	0	0	0	0	0	12	2005-03-23 14:50:04	0	0	0	0	0	0	13	2005-03-23 14:35:04	0	0	0	0	0	0	14	2005-03-23 14:20:04	0	0	0	0	0	0	15	2005-03-23 14:05:04	0	0	0	0	0	0
	Time	LOFs	LOSs	LOLs	LPRs	ESs	I																																																																																																																													
1	2005-03-23 17:35:04	0	0	0	0	0	0																																																																																																																													
2	2005-03-23 17:20:04	0	0	0	0	0	0																																																																																																																													
3	2005-03-23 17:05:04	0	0	0	0	0	0																																																																																																																													
4	2005-03-23 16:50:04	0	0	0	0	0	0																																																																																																																													
5	2005-03-23 16:35:04	0	0	0	0	0	0																																																																																																																													
6	2005-03-23 16:20:04	0	0	0	0	0	0																																																																																																																													
7	2005-03-23 16:05:04	0	0	0	0	0	0																																																																																																																													
8	2005-03-23 15:50:04	0	0	0	0	0	0																																																																																																																													
9	2005-03-23 15:35:04	0	0	0	0	0	0																																																																																																																													
10	2005-03-23 15:20:04	0	0	0	0	0	0																																																																																																																													
11	2005-03-23 15:05:04	0	0	0	0	0	0																																																																																																																													
12	2005-03-23 14:50:04	0	0	0	0	0	0																																																																																																																													
13	2005-03-23 14:35:04	0	0	0	0	0	0																																																																																																																													
14	2005-03-23 14:20:04	0	0	0	0	0	0																																																																																																																													
15	2005-03-23 14:05:04	0	0	0	0	0	0																																																																																																																													
				Port Number : 1 <input checked="" type="radio"/> ATU-C <input type="radio"/> ATU-R <input type="button" value="Refresh"/>																																																																																																																																

Figure 4-32. PM history configuration

4.4.9 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**. The page is shown in Figure 4-33.

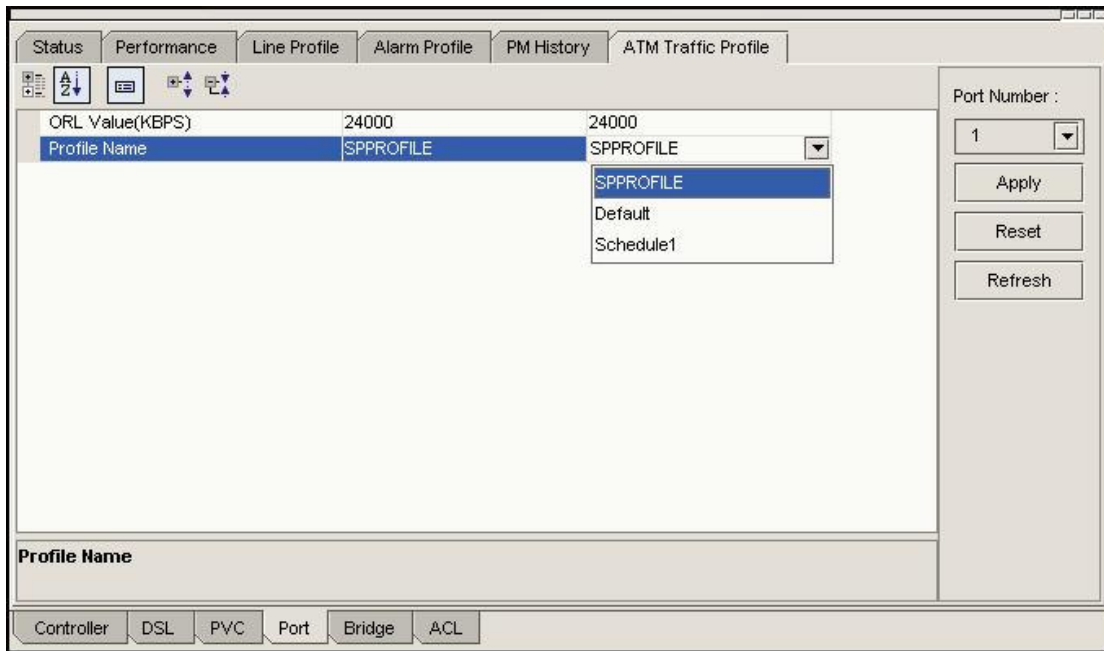


Figure 4-33. The ATM traffic profile

The Profile Name is setting the ATM Scheduling Profile. This Profile must be setting in 4.5.6 first. Otherwise the default Profile Name is SPPROFILE. After changing the value, the success screenshot will show as Figure 4-34.

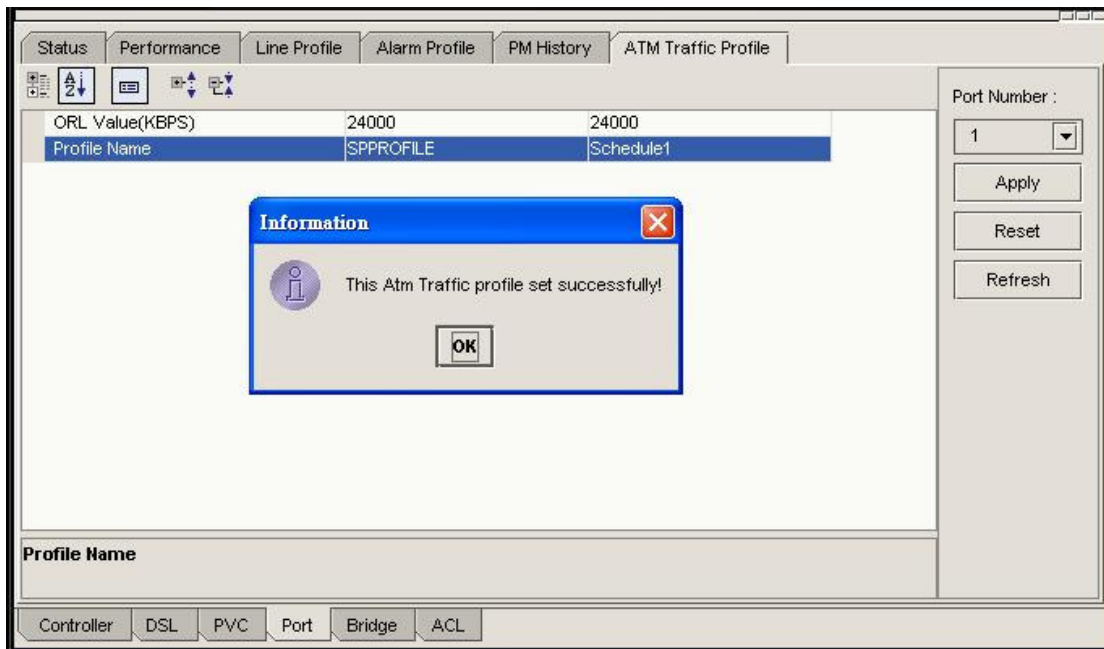
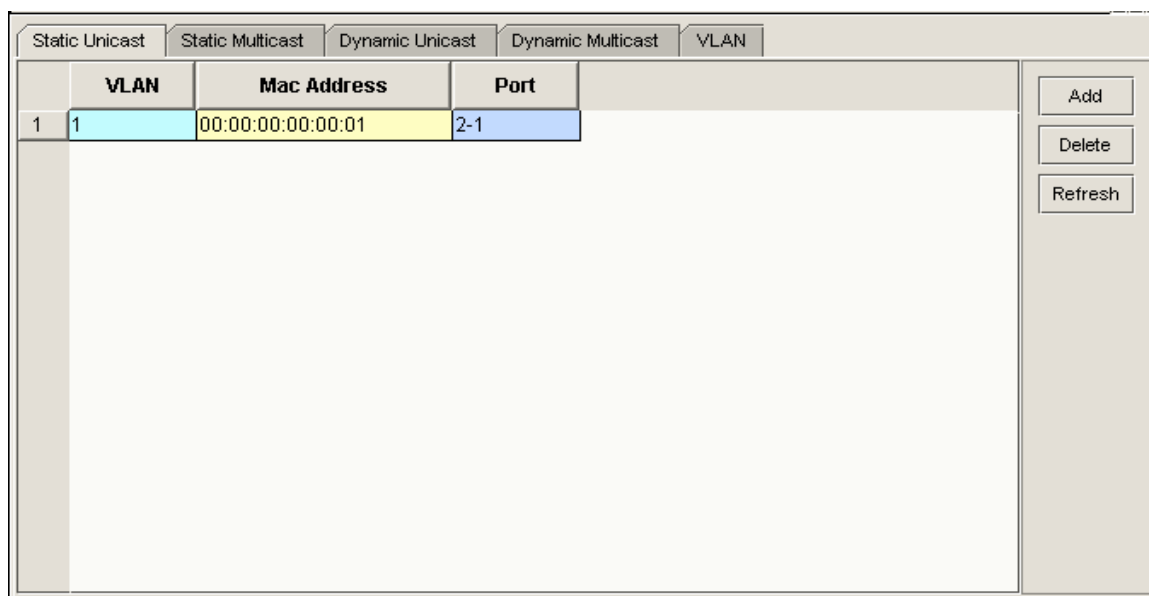


Figure 4-34. Apply ATM traffic profile

4.5 Bridge Configuration

4.5.1 Bridge/Static Unicast

Set the port, which the unicast packets can be sent with the **MAC address**. The page is shown in Figure 4-35.



	VLAN	Mac Address	Port	
1	1	00:00:00:00:00:01	2-1	<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>

Figure 4-35. 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.

4.5.1.1 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 4-35 is shown as below.

The screenshot shows a dialog box for adding a unicast entry. It has three main sections:

- VLAN:** A text input field containing the number 222.
- Mac Address:** A text input field containing the hexadecimal string 00: 00: 00: 00: 00: 00.
- Port:** A list box containing a grid of port identifiers. The first cell '1-1' is highlighted in blue.

The 'Port' list contains the following entries:

1-1	9-1	17-1	1-2
2-1	10-1	18-1	uplink
3-1	11-1	19-1	
4-1	12-1	20-1	
5-1	13-1	21-1	
6-1	14-1	22-1	
7-1	15-1	23-1	
8-1	16-1	24-1	

At the bottom right of the dialog box are two buttons: 'Apply' and 'Cancel'.

Figure 4-35. Add a new unicast entry

4.5.1.2 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 4-36 is shown as below.

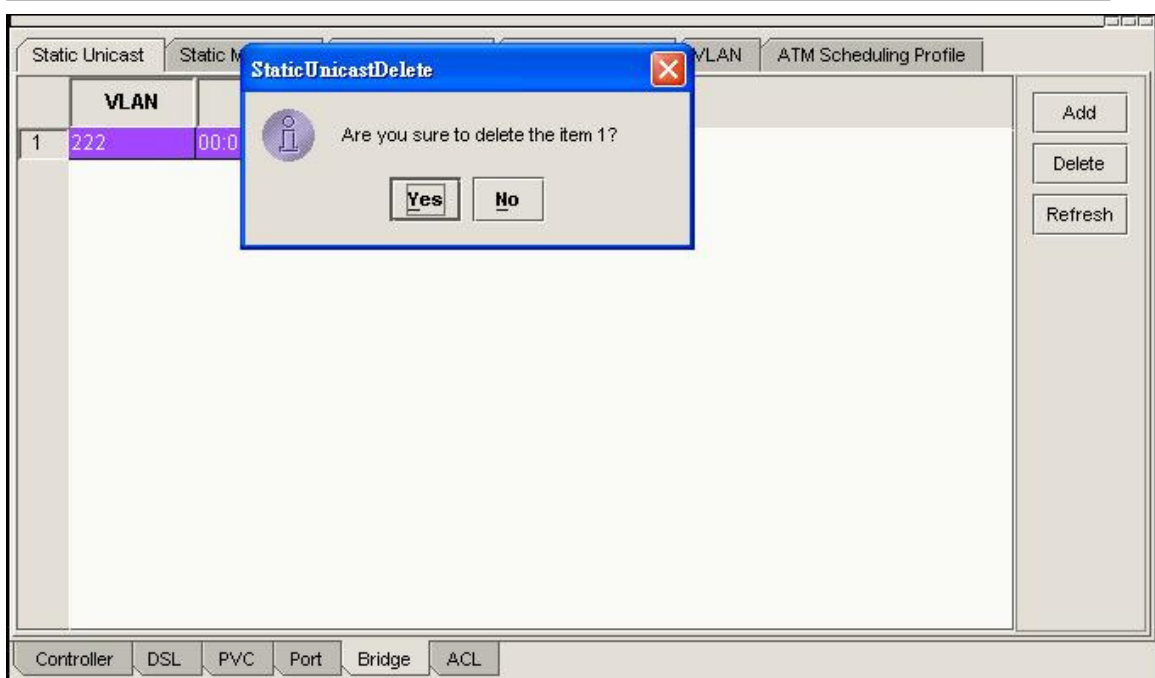


Figure 4-36. Delete a unicast entry

4.5.1.3 Refresh the Unicast Entry

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

4.5.2 Bridge/Static Multicast

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

Figure 4-37 is shown the Static Multicast configuration as below.

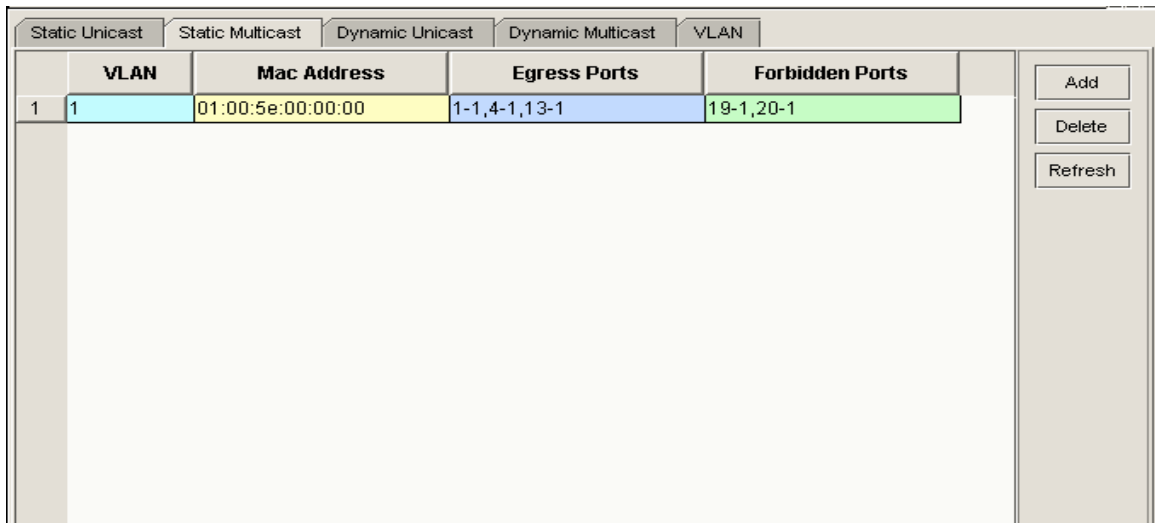


Figure 4-37. Static Multicast configurations

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.

4.5.2.1 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. The page is shown in Figure 4-38.

The screenshot shows a configuration window with the following fields and values:

- VLAN:** 222
- Mac Address:** 01: 00: 5E: 00: 00: 00
- Egress Ports:** A grid of ports with 10-1 and 21-1 selected.
- Forbidden Po...:** A grid of ports with 11-1 and 20-1 selected.

1-1	9-1	17-1	1-2
2-1	10-1	18-1	uplink
3-1	11-1	19-1	
4-1	12-1	20-1	
5-1	13-1	21-1	
6-1	14-1	22-1	
7-1	15-1	23-1	
8-1	16-1	24-1	

1-1	9-1	17-1	1-2
2-1	10-1	18-1	uplink
3-1	11-1	19-1	
4-1	12-1	20-1	
5-1	13-1	21-1	
6-1	14-1	22-1	
7-1	15-1	23-1	
8-1	16-1	24-1	

Buttons: Apply, Cancel

Figure 4-38. Static Multicast configurations

4.5.2.2 Delete a Multicast Entry

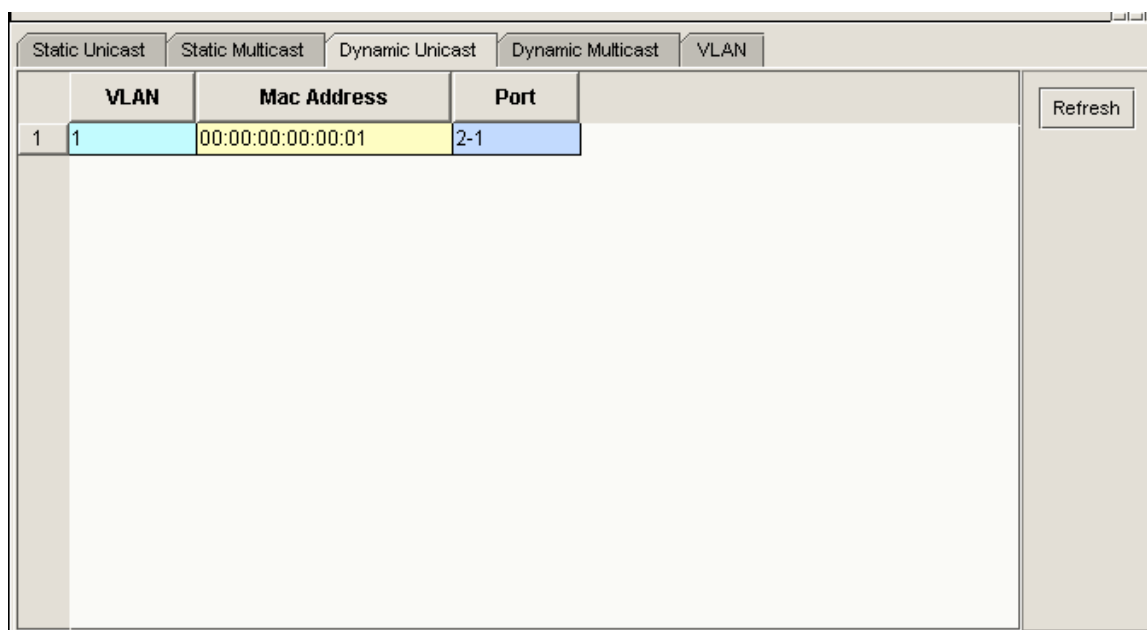
Before deleting a unicast entry, use mouse to click the entry to be deleted, then select **delete** button to delete this entry.

4.5.2.3 Refresh the Multicast Entry

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

4.5.3 Bridge/Dynamic Unicast

Show the map between the port and MAC address now. The page is shown in Figure 4-39.



	VLAN	Mac Address	Port	
1	1	00:00:00:00:00:01	2-1	Refresh

Figure 4-39. Dynamic Unicast configurations

4.5.4 Bridge/Dynamic Multicast

Show the map between the ports and MAC address now. The page is shown in Figure 4-40.

Egress Port

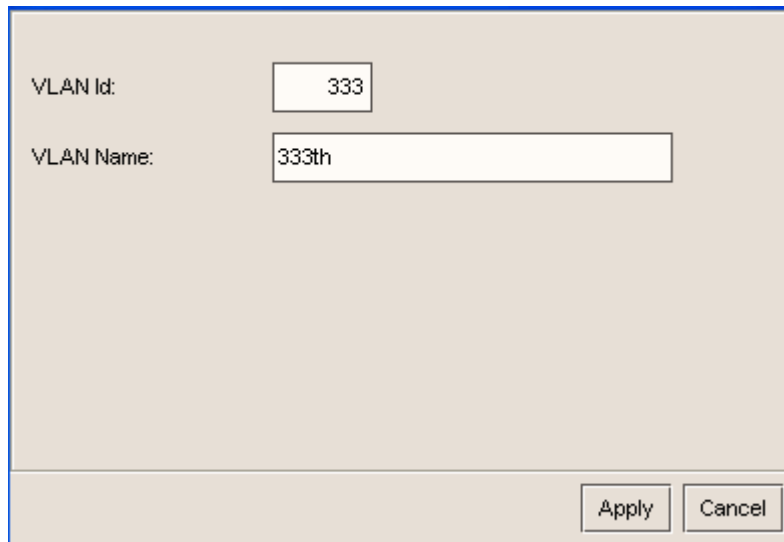
Show the port to which packets with the VLAN ID can be sent.

Untag Port

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

4.5.5.1 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 4-42 is shown as below.



The image shows a dialog box for adding a VLAN entry. It has a light beige background and a blue border. There are two input fields: 'VLAN Id' with the value '333' and 'VLAN Name' with the value '333th'. At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

Figure 4-42. VLAN configurations

4.5.5.2 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.

4.5.5.3 Refresh the VLAN Entry

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

4.5.6 Bridge/ATM Scheduling Profile

Customized Scheduling is a credit-based mechanism for scheduling within queues for an ATM port. When ATM port is scheduled for transmission based on ATM ORL enforcement bandwidth is distributed only among the queues that have some cells. Bandwidth shall be the minimum of the ATM port configured ORL and Line rate on which DSL has trained. It will be divided among the queues, which have frames. If sum of the minimum-Bandwidth exceeds port-Rate then the bandwidth given to each queue is proportional to the minimum bandwidth for that queue. In the section, we could set the value for each parameter.

4.5.6.1 Add a Scheduling Profile

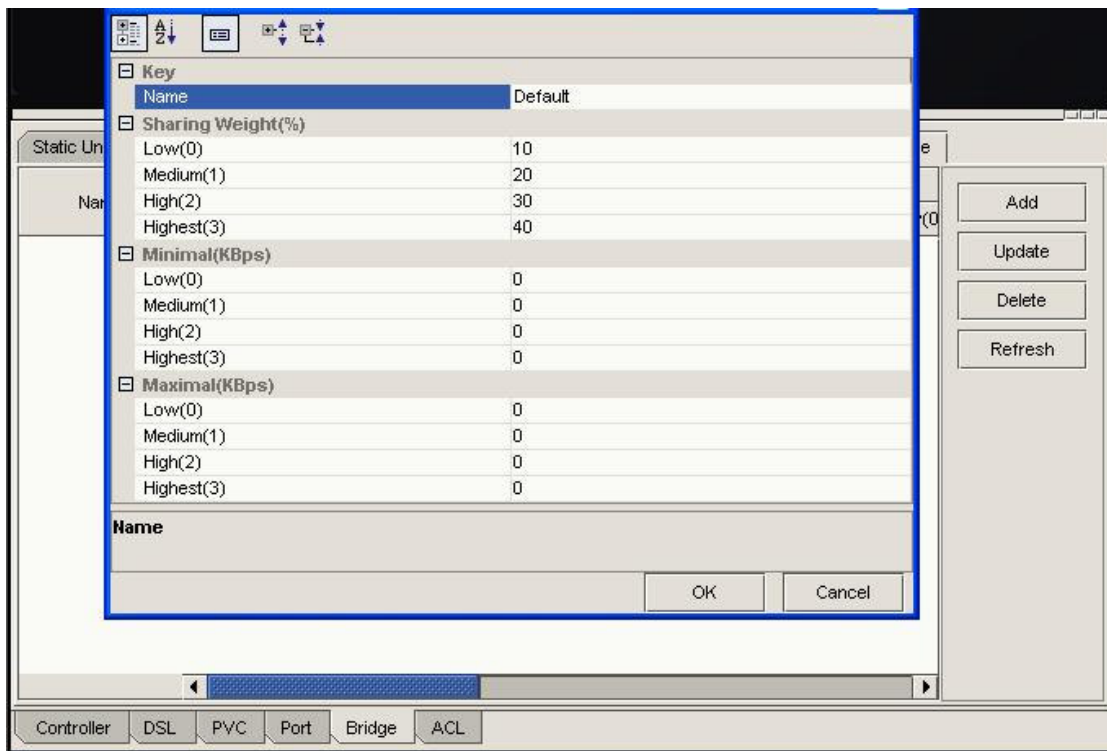


Figure 4-43. Add Scheduling profile

When adding a new Scheduling Profile, the dialog will be shown as Figure 4-43:

- Excess Bandwidth sharing Weight = The proportion of Excess Bandwidth, which this queue wants to share.
- Minimum Bandwidth: giving the minimum bandwidth that this queue requires. Specified in Kbps.
- Maximum Bandwidth: giving the maximum bandwidth that this queue is allowed to use. Specified in Kbps. 0 value implies that there is no maximum bandwidth limit.

After pressing OK, the panel will refresh automatically as follow: The profile should be inserted to the device.

Static Unicast						Static Multicast						Dynamic Unicast						Dynamic Multicast						VLAN						ATM Scheduling Profile					
Name	Sharing Weight					Low(0)																													
	Low(0)	Medium(1)	High(2)	Highest(3)	Low(0)																														
Default	10	20	30	40	0																														
Schedule1	25	25	25	25	0																														

Figure 4-44. Refresh Scheduling profile

4.5.6.2 Update the Scheduling Profile

When updating a selected Scheduling Profile, the dialog will be shown as Figure 4-45:

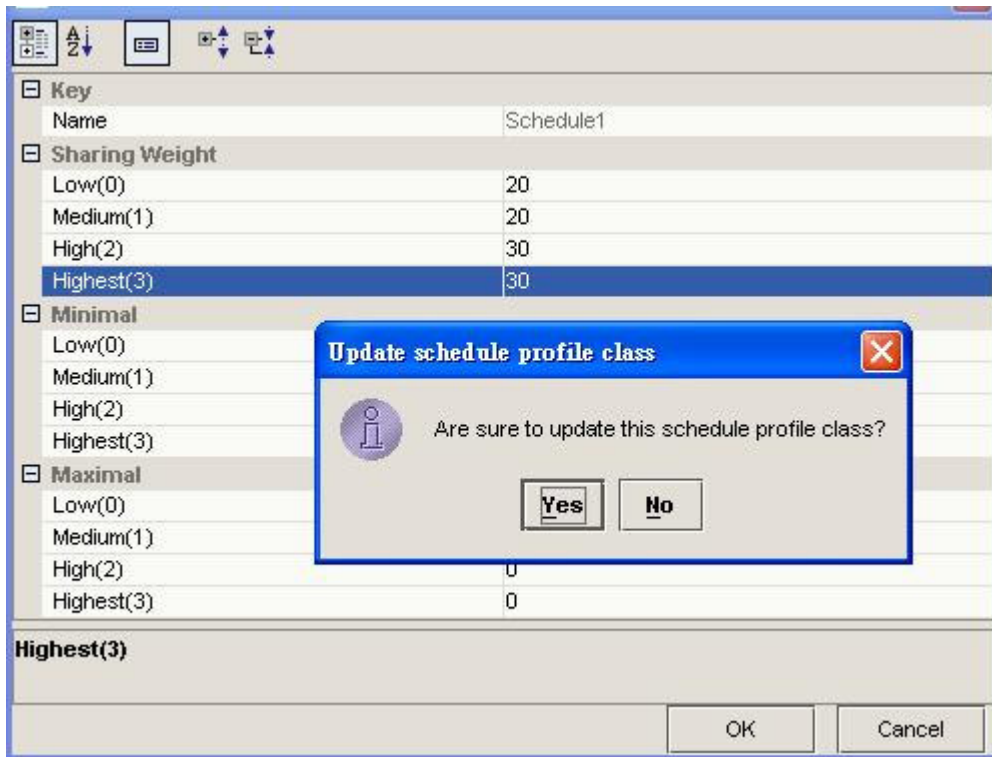


Figure 4-45. Update Scheduling Profile

4.5.6.3 Delete the Scheduling Profile

Use mouse to click a profile, select the delete button, the system will ask if you really want to delete the profile.

4.5.6.4 Refresh the Scheduling Profile

No matter what operation be done, the refresh will reget the profiles from device.

4.6 ACL Configuration

4.6.1 ACL/ Deny

Deny the packets with MAC address from any ports. Figure 4-46 is shown as below.



Figure 4-46. 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 4-47 is shown the MAC entry in the deny configuration as below.

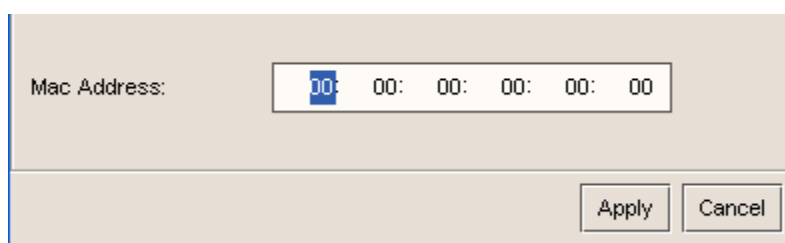


Figure 4-47. Add a MAC entry in the deny configuration

4.6.1.1 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.

4.6.1.2 Delete a MAC Entry

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

4.6.1.3 Refresh the MAC Entry

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

4.6.2 ACL/ Allow

Allow the packets with MAC address from the port. Figure 4-48 is shown the ACL Allow configuration as below.

Deny (Device Based)		Allow (Port Based)	
	Port	Mac Address	
1	3-1	00:00:00:00:00:08	

Buttons: Add, Delete, Refresh

Figure 4-48. 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.

4.6.2.1 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. The page is shown in Figure 4-49.

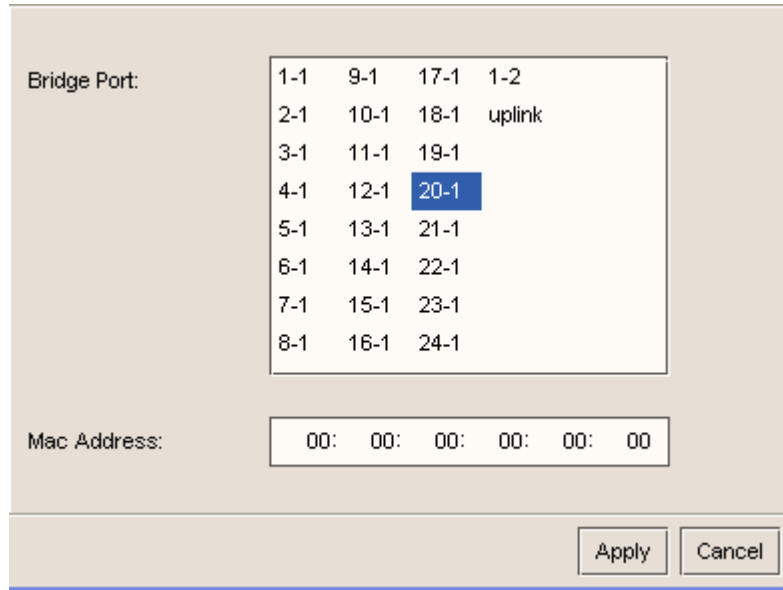


Figure 4-49. ACL allow configuration

4.6.2.2 Delete

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

4.6.2.3 Refresh

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

4.7 System Management

System management includes network utilities used for diagnosing the devices.

4.7.1 Tools Function

4.7.1.1 Tools/ Ping Device

Ping the selected device. Figure 4-50 is shown the Ping Tool as below.



Figure 4-50. Ping tool

4.7.1.2 Tools/ Trace Route

Print the path to the selected device use trace route. Figure 4-51 is shown the Trace Route Tool as below.

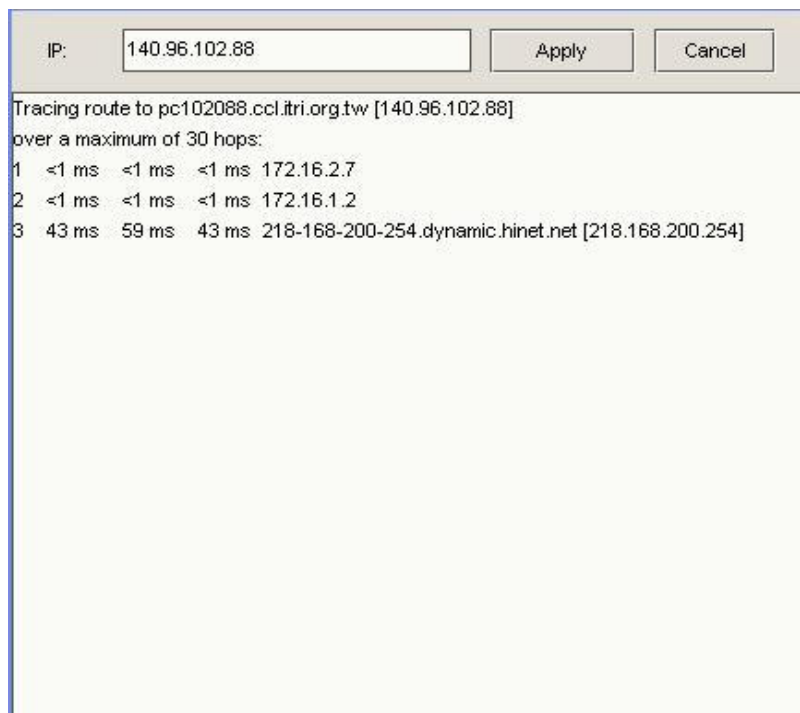


Figure 4-51. Trace route tool

4.7.1.3 Tools/ Telnet Device

Provide a telnet tool to the selected device. The page is shown in Figure 4-52.

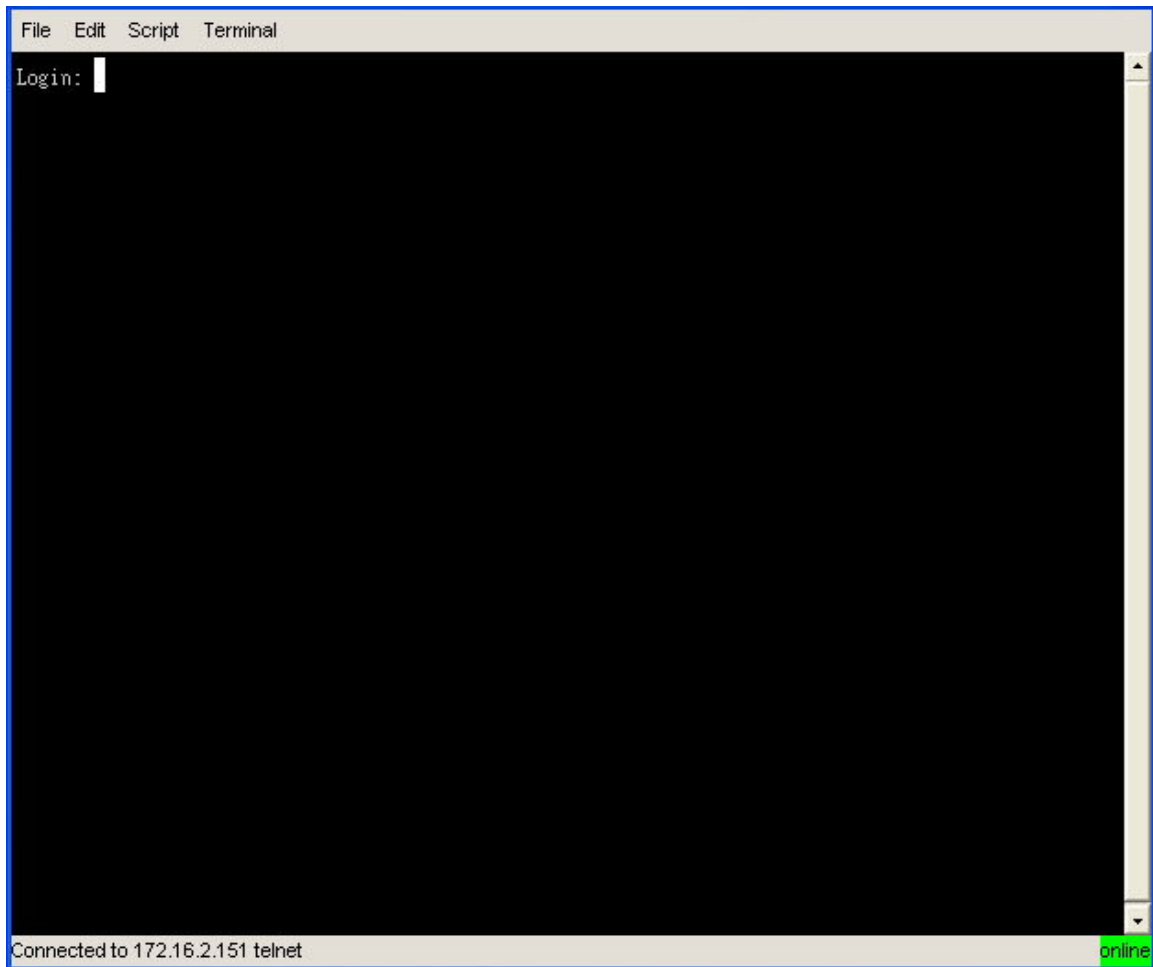


Figure 4-52. Telnet tool

4.7.1.4 Script

The function of Script on Telnet Tool is to provide an interface for operators to run a Telnet script file. Please select **Script->Run** menu item then choose one script file to execute. You can define the telnet command delay by selecting **Script->Set Options**. Figure 4-53,4-54 are shown as below.

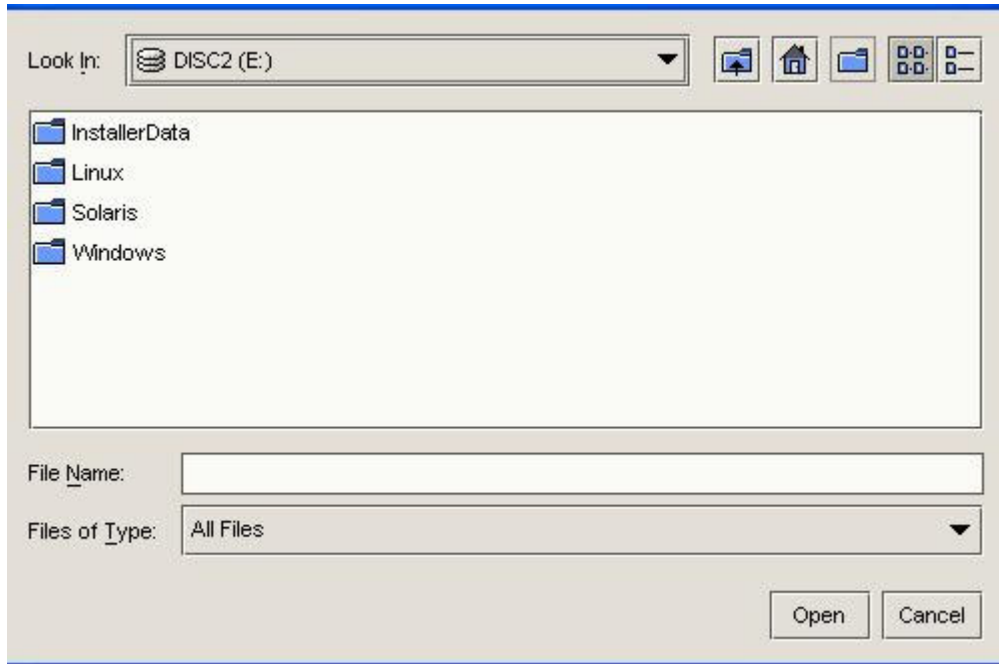


Figure 4-53. Script run



Figure 4-54. Set option

CHAPTER 5

Security Management

Security management for CMS 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 roles are defined in the system. There are 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.

This chapter is divided into the following sections,

- Section 5.1: User Management
- Section 5.2: Group Management
- Section 5.3: Resource Management

5.1 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 Figure 5-1; the functions of user management are described as followings:

5.1.1 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**.

5.1.2 Update user

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

5.1.3 Delete user

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

5.1.4 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 is shown the User Management Setup Window as below.

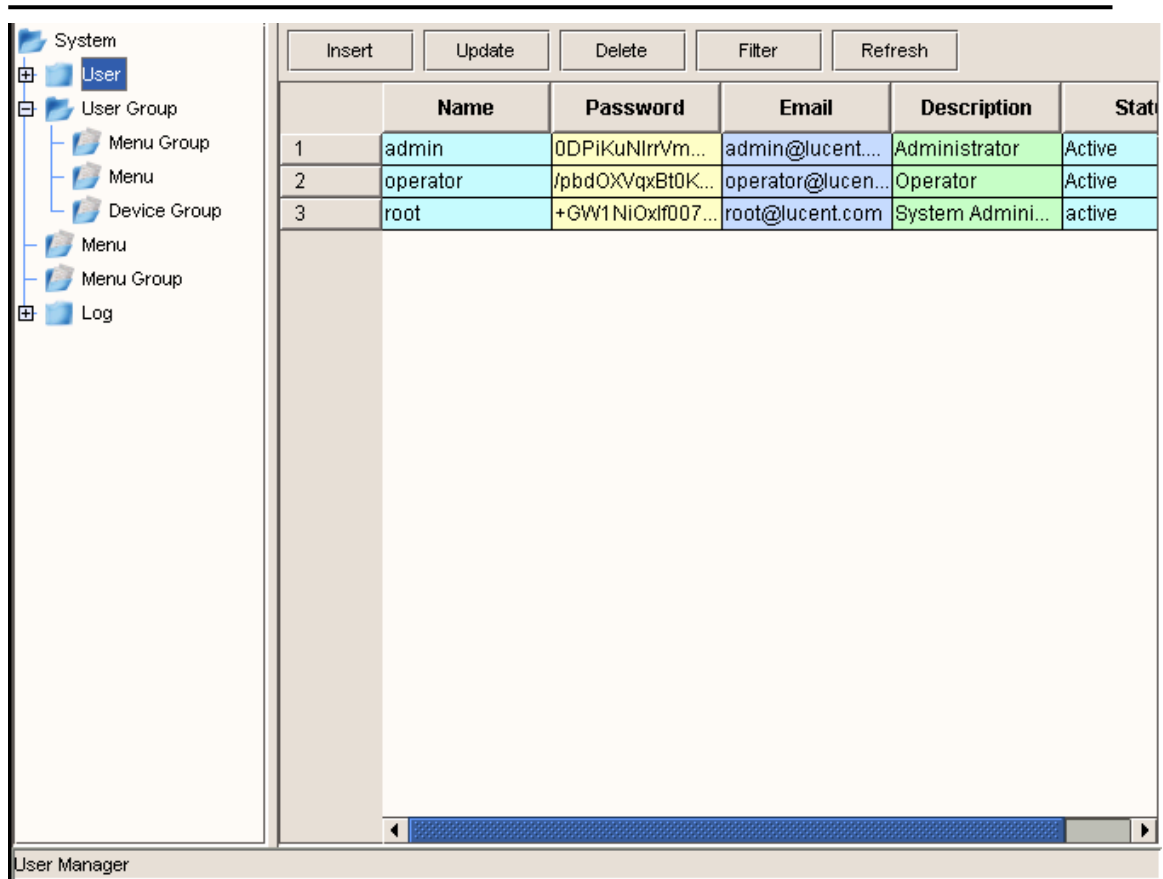


Figure 5-1. User management setup window

5.2 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 CMS, these resources are Application Functions and main menu functions. After creating 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:

5.2.1 Insert group

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

5.2.2 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.

5.2.3 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.

5.2.4 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 group to this group. There are two modes for configuration: “*Device-View*” and “*Device-Modify*”. Assign “*Device-View*” for functions means that all functions can be viewed only, while assigning “*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 is shown as below.

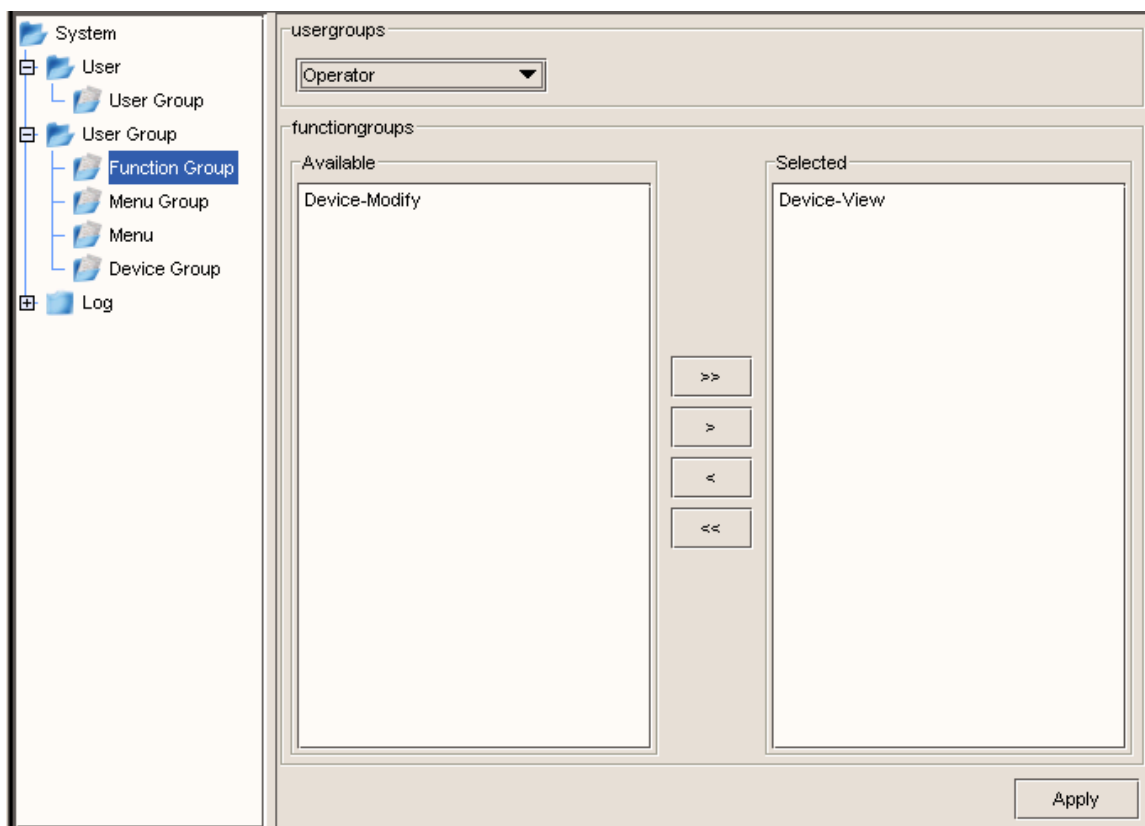


Figure 5-2. Function group assignment

5.2.5 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 5-3 and you select one group from group list box and assign available menu function groups to this group.

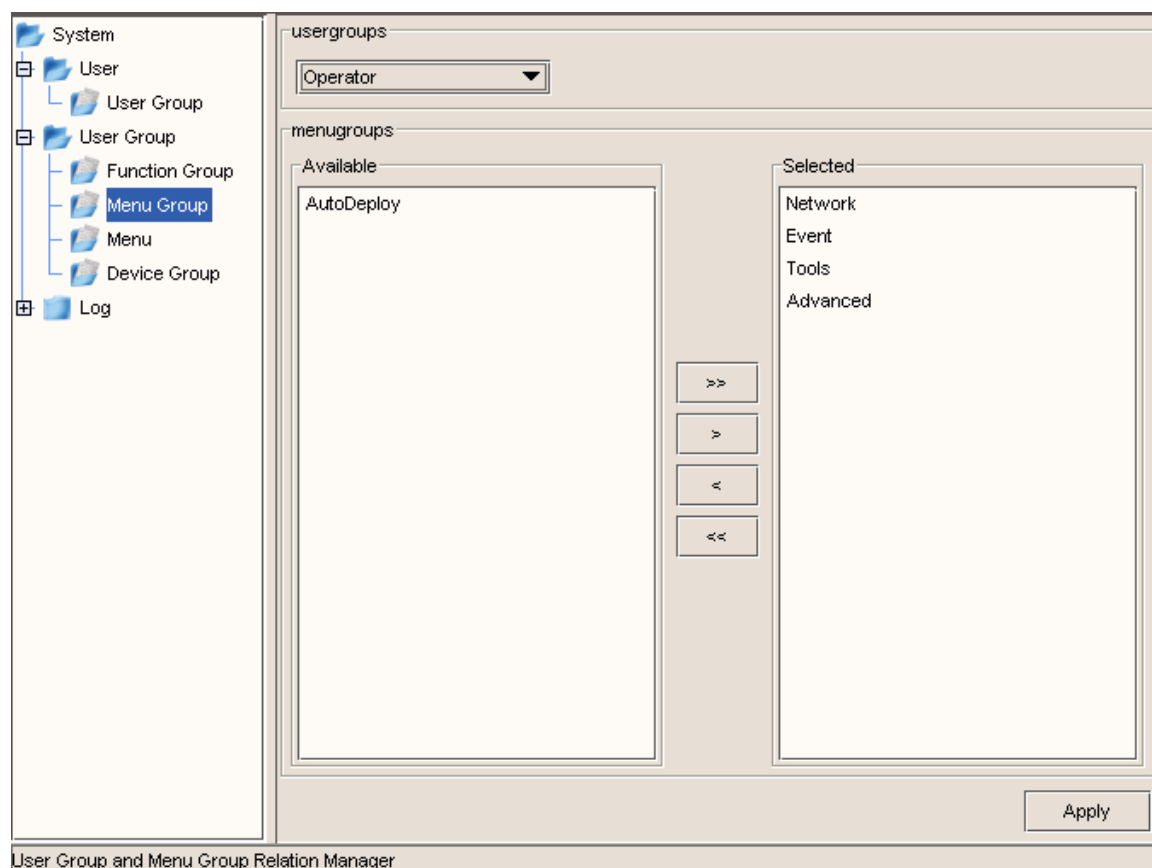


Figure 5-3. Menu assignment

5.2.6 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.

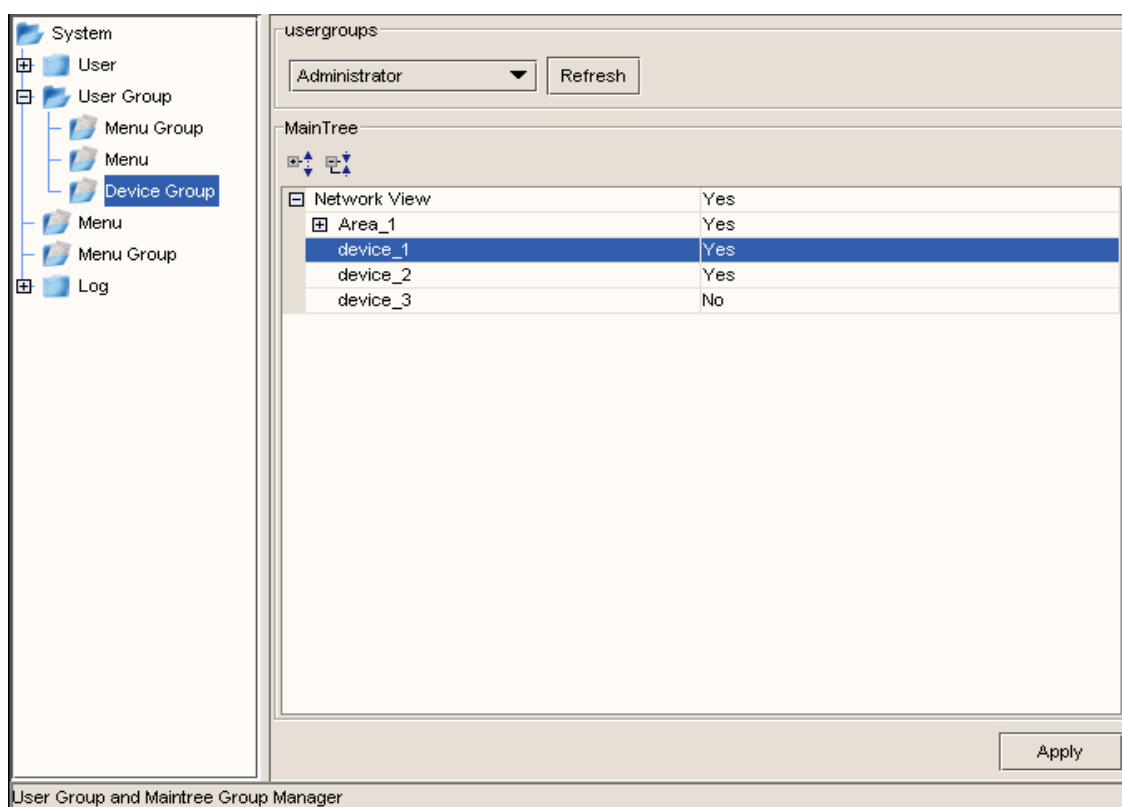


Figure 5-4. Device group setup window

In this case, the device “**device_3**” is set as “**No**”, so the users of **Administrator group** can not manage this device. Furthermore, there are three options for network and device for convenient configurations. A network can set to “**YES**” and all children default empty such that all the children will be managed by the user group. A network or devices can set to empty to follow his parent’s configuration. On the other hand, the network or device can set to “**NO**” to disable the control ability of the usergroup. So the device will be managed or not depended on choosing “**YES**” or “**NO**”. If the device is set to empty, it will follow the configuration of parent node. Figure 5-4 is shown as example, the Network View can set to “**YES**” means if the children set to empty, it is the same as set “**YES**”.

5.3 Resource Management

Resource management provides an interface to add, delete and modify resource information. The resource in the CMS 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:

5.3.1 Insert resource

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

5.3.2 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.

5.3.3 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.

5.3.4 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 Figure 5-5 and you select one group from group list box and assign available menu functions to this group.

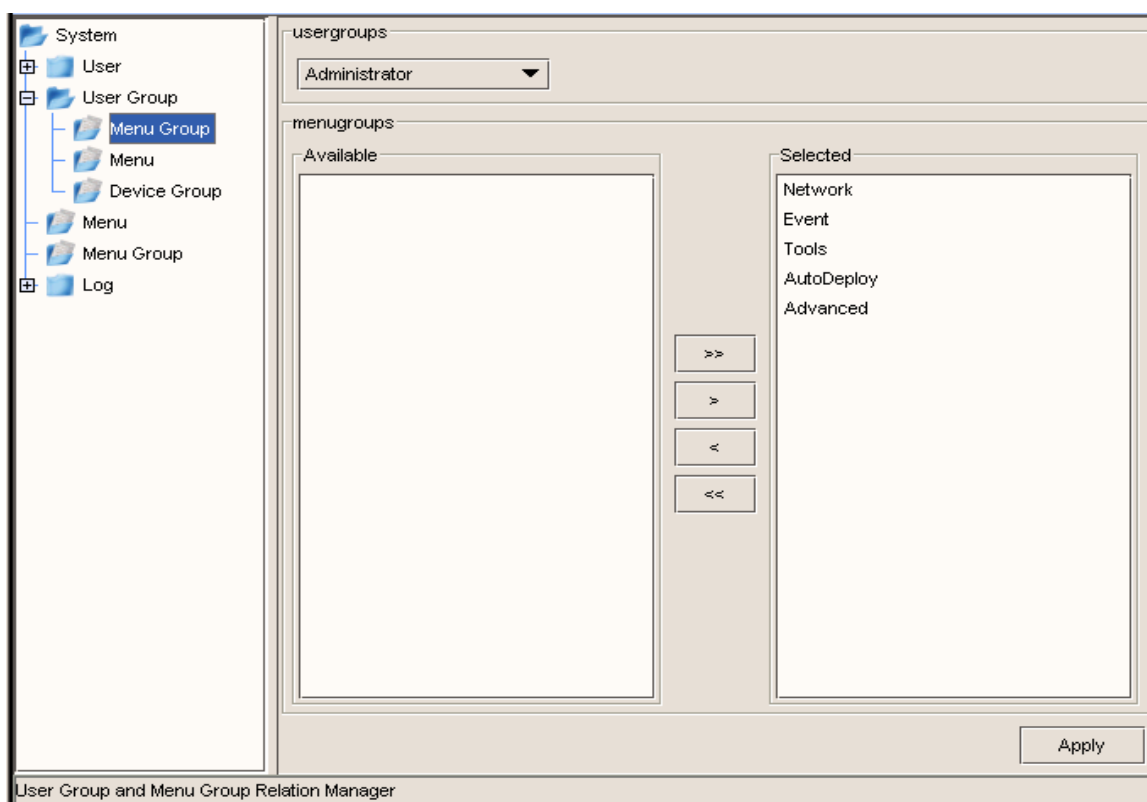


Figure 5-5. Menu group setup window

CHAPTER 6

Monitor Management

Monitor management is a service located in the CMS server; it is responsible for viewing the status of managing 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 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 CMS, including polling function, alarm and trap notification function, and alarm filter for alerting.

This chapter is divided into the following sections,

- Section 6.1: Polling Device
- Section 6.2: Alarm

6.1 Polling Device

CMS 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 CMS client if the status of the device is changed. In the left panel you will see the alarms sent to CMS 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 is shown as below.



Figure 6-1. Device panel

6.2 Alarm

6.2.1 Alarm View

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 is shown the Alarm and Trap Window as below.

The screenshot shows a window titled "Alarm View 1" with a table of alarm data and a control panel on the right. The table has columns for Device Name, Device IP, Alarm Time, Device Type, and Entit. The control panel includes buttons for ACK, Clear, and Clear All, along with dropdown menus for Alarm Type, Severity, Device, Entity, and Port, and a Search button.

	Device Name	Device IP	Alarm Time	Device Type	Entit
1	172.16.2.151	172.16.2.151	2005-07-25 16:...	Master-Slave	port-1,sla
2	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-24,s
3	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-23,s
4	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-22,s
5	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-21,s
6	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-20,s
7	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-19,s
8	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-18,s
9	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-17,s
10	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-16,s
11	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-15,s
12	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-14,s
13	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-13,s
14	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-12,s
15	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-11,s
16	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-10,s
17	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-9,sla
18	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-8,sla
19	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-7,sla
20	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-6,sla
21	172.16.2.151	172.16.2.151	2005-07-25 11:...	Master-Slave	port-5,sla
...					

Figure 6-2. Alarm and trap window

The right part is filtering parameters.

ACK

Select alarms then ack these ack to root.

Clear

Single clear the select alarm.

Clear All

Clean all the alarm in the panel.

Alarm Type

One of the alarm filter rules. There are totally 15 kinds of type. User may choose one of them or select all as filter rules.

Severity

One of the alarm filter rules. There are totally 5 kinds of type. User may choose one of them or select all as filter rules.

Device

One of the alarm filters. User may precisely select the device or a network as filter rules. If the selected device is stand-alone device, the entity will be disabled. The empty device implies all devices as filter rules in Figure 6-3.

Entity

If device is choosed as network or master-slave device, the entity contains 8 types as filter rules. Otherwise choose all to omit entity.

Port

The user may precisely assign the ports which need to be filtered. The empty port implies omitting the ports..

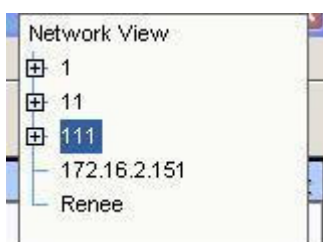


Figure 6-3. Alarm View device



Figure 6-4. Alarm View port

The clear button will delete selected alarm and clear all will clear all the alarm in the panel.

6.2.2 Alarm History View

You can view history alarms when you click the alarm panel in the bottom of the left panel or select the menu **Event->Alarm History View** to see the history alarm received from devices. These history alarms will be stored in backend database for query. Figure 6-5 is shown the Alarm History Window as follow The Start Time, End Time, Alarm Type, Severity, Device, Entity and Port are filter parameters. The empty condition implies all cases. After filling the parameters, the search will get the result sets.

The screenshot shows a window titled "Alarm History View 1" with a table of alarm records and a sidebar with filter options. The table has columns for Device Name, Device IP, Alarm Time, Clear Time, and Device. The sidebar includes filters for Start Time, End Time, Alarm Type, Severity, Device, Entity, and Port, along with a Search button.

	Device Name	Device IP	Alarm Time	Clear Time	Device
1	172.16.2.151	172.16.2.151	2005-07-25 16:...	2005-07-25 16:...	Master-Sl...
2	172.16.2.151	172.16.2.151	2005-07-25 11:...	2005-07-26 15:...	Master-Sl...
3	172.16.2.151	172.16.2.151	2005-07-25 11:...	2005-07-26 15:...	Master-Sl...
4	172.16.2.151	172.16.2.151	2005-07-25 11:...	2005-07-26 15:...	Master-Sl...
5	172.16.2.151	172.16.2.151	2005-07-25 11:...	2005-07-25 11:...	Master-Sl...
6	172.16.2.151	172.16.2.151	2005-07-25 09:...	2005-07-25 16:...	Master-Sl...

Filter sidebar options:

- Start Time: 2005-07-25
- End Time: 2005-07-26
- Alarm Type: All
- Severity: All
- Device: [Empty]
- Entity: ALL
- Port: [Empty]
- Search button

Figure 6-5. History alarm 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 CMS 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 CMS, including network domain creation, device auto discovery.

This chapter is divided into the followings section,

- Section 7.1: Network Map

7.1 Network Map

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

7.1.1 New Network

Create a new network domain for management. It exists a default root domain for using. If you do not want to create another network domain, you can use the root domain for your management domain. The page is shown in Figure 7-1.

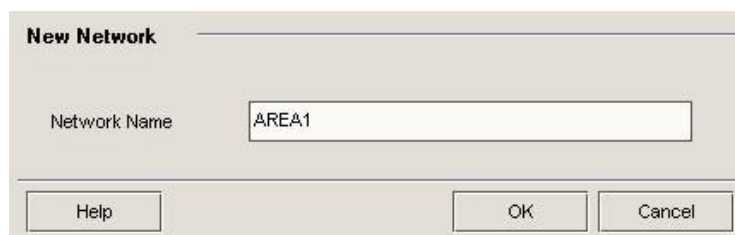


Figure 7-1. New network window

7.1.2 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 reading operations from CMS to device in SNMP. This value should be set the same as that of the device. If the community set in CMS is not the same as that of the device, this operation will be rejected.

Write Community

The community set for write operations from CMS to device in SNMP. This value should be set the same as that of the device. If the community set in CMS 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 CMS 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 is shown the New Device Setup Window as below.

New Device

Display Name

IP

SNMP Port

SNMP Read Community

SNMP Write Community

SNMP Version ▼

Device Type ▼

login user

login password

Figure 7-2. New device setup window

7.1.3 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 discovering. 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. The page is shown in Figure7-3.

	IP	Port	SNMP Read Community	SNMP Write Community	Display Name	SNMP Version	Device Type
1	172.16.2.151	161	public	private	172.16.2.151	V2	Master-Slave
2	172.16.2.152	161	public	private	172.16.2.152	V2	Master-Slave

Figure 7-3. Auto discovery window

7.1.4 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 inspection.

Line

Draw a line for linking to the devices. The page is shown in Figure 7-4.

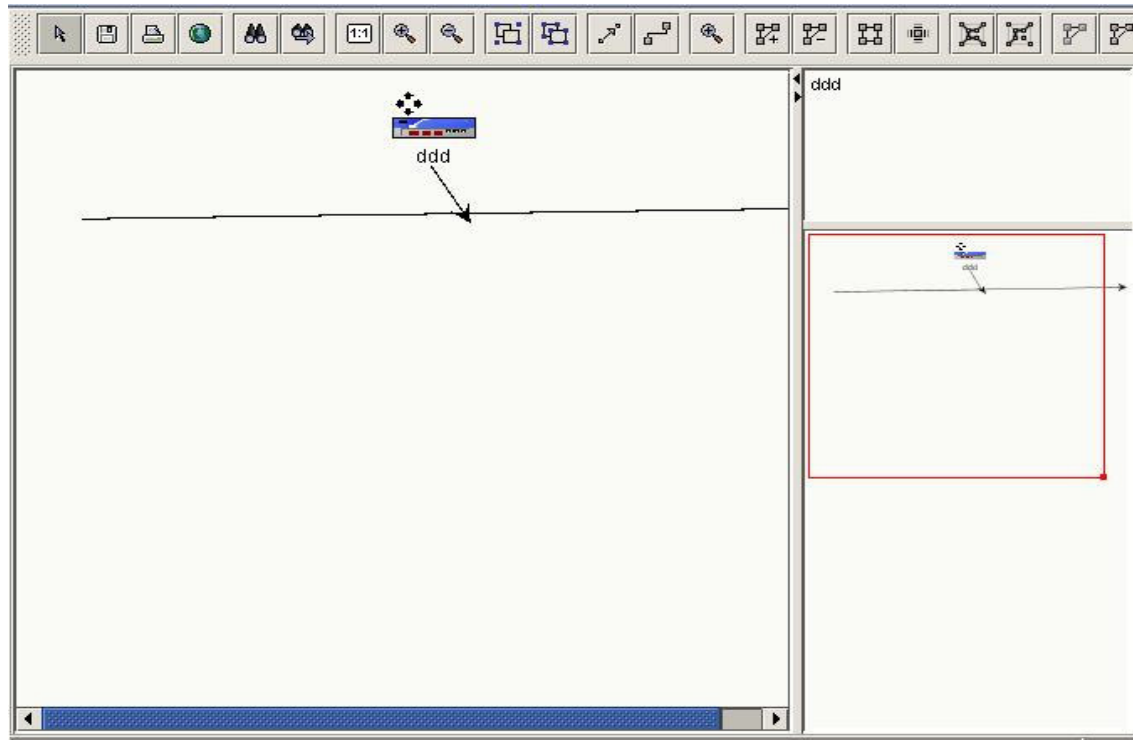


Figure 7-4. Network map editor setup window

CHAPTER 8

Log and Event Management

The function of Log and event management for CMS 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. CMS client provides a GUI for operators to input the filter conditions for query.

This chapter is divided into the following sections,

- Section 8-1: Event management
- Section 8-2: Log management

8.1 Event management

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

8.1.1 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.

To see the active or history alarm, you have to choose **Event->Alarm View** or **Event->Alarm History View**. Alarm View is to display active alarm and Alarm History View is a interface to query the history alarm.

8.1.2 Current Alarm

The current alarms are new raised events from the managed devices. Figure 8-1 is the current alarms from devices.

	Device Name	Device IP	Alarm Time	Device Type	Entities
1	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	slave-1
2	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-24,slav
3	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-23,slav
4	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-22,slav
5	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-19,slav
6	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-18,slav
7	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-17,slav
8	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-16,slav
9	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-14,slav
10	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-13,slav
11	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-12,slav
12	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-11,slav
13	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-10,slav
14	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-9,slav
15	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-8,slav
16	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-7,slav
17	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-6,slav
18	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-5,slav
19	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-4,slav
20	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-3,slav
21	172.16.2.151	172.16.2.151	2005-06-23 09:...	Master-Slave	port-2,slav

Figure 8-1. Current alarm window

Currently, CMS provides the multi Alarm View. You can add a new Alarm View by choosing the **Event->Alarm View** again or you can click pie chart of alarm summary panel. Each Alarm View is independent. You can change the condition on different Alarm View.

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 CMS 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 CMS.

DSLFail: The DSL card of device can not be accessed by CMS.

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 users.

Ack User

Show the users who acknowledged this current alarm.

Ack Time

Show the date time that this alarm is acknowledged.

8.1.3 Alarm filter

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

8.1.4 History Alarm

History alarms are collected by CMS 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.

	Device Name	Device IP	Alarm Time	Clear Time	Device
1	172.16.2.151	172.16.2.151	2005-06-23 10:...	2005-06-23 10:...	Master
2	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
3	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
4	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
5	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
6	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
7	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
8	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
9	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
10	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
11	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
12	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
13	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
14	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
15	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
16	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
17	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
18	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
19	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
20	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
21	172.16.2.151	172.16.2.151	2005-06-23 09:...	2005-06-23 09:...	Master
--					

Start Time: 2005-06-22

End Time: 2005-06-23

Alarm Type: All

Severity: All

Search

Figure 8-2. History alarm window

Like Alarm View, CMS also provides the multi Alarm History View. You can add a new Alarm History View by choosing the **Event->Alarm History View** again. Each Alarm History View is independent. You can change the condition on different Alarm History View.

8.1.5 Alarm Audio

Alarm audio provides unacknowledged alarm for sending alarm prompt sound at intervals. Alarm promptly can be distinguished by various sound according to alarm level.

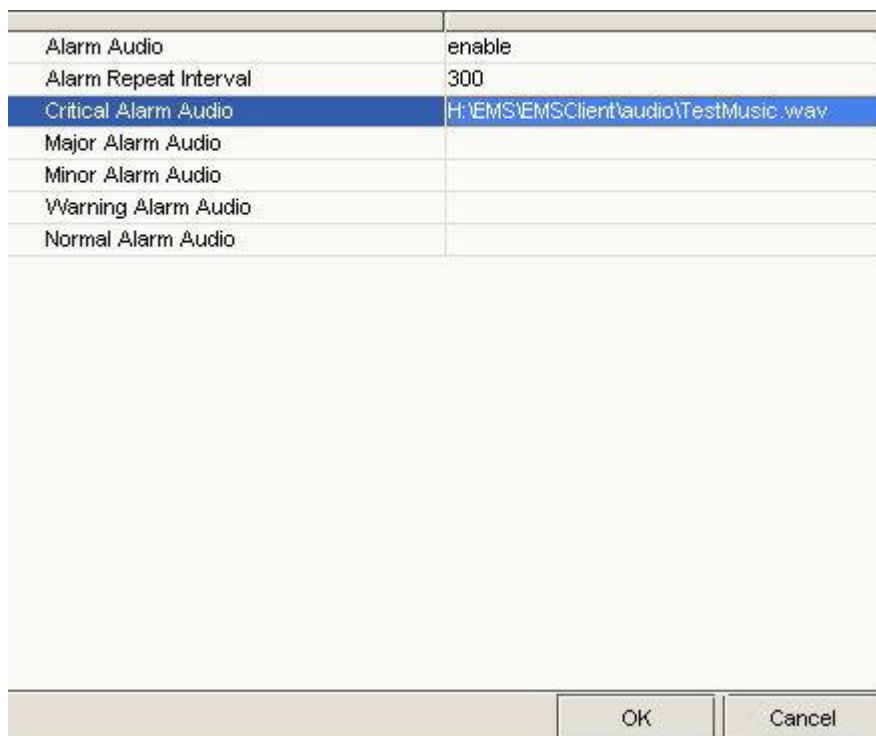


Figure 8-3. Preference dialog

To acting the alarm audio, you have to enable alarm audio, set the intervals, and define sound file for different alarm level. You set these parameters on Preference Dialog. To active the Preference Dialog, please select **Advanced**->Preference on Main Menu. The Preference is as bellow Figure 8-3:

8.1.6 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**. Figure 8-4 is shown as below.

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 CMS.

Sys Uptime

The system uptime of the device raised this trap.

The screenshot shows a web interface for trap management. At the top, there are two tabs: 'Trap View' and 'Trap History View'. Below the tabs is a table with the following columns: 'Trap Time', 'Device Name', 'Device Type', 'Device IP', and 'Trap Name'. The table contains 15 rows of data, all with the same values: '2005-01-07' for time, 'V3600' for device name and type, and '140.96.102...' for device IP. The trap name is truncated as 'adslAtucRateChange...'. To the right of the table is a search panel with 'Start Time' and 'End Time' dropdown menus (set to '2005-01-07' and '2005-01-10' respectively) and a 'Search' button. Below the table is a large empty white box.

	Trap Time	Device Name	Device Type	Device IP	Trap Name
1	2005-01-07 00:33:06	V3600	V3600	140.96.102....	adslAtucRateChange...
2	2005-01-07 00:33:51	V3600	V3600	140.96.102....	adslAtucRateChange...
3	2005-01-07 00:34:35	V3600	V3600	140.96.102....	adslAtucRateChange...
4	2005-01-07 00:35:58	V3600	V3600	140.96.102....	adslAtucRateChange...
5	2005-01-07 00:36:53	V3600	V3600	140.96.102....	adslAtucRateChange...
6	2005-01-07 00:38:16	V3600	V3600	140.96.102....	adslAtucRateChange...
7	2005-01-07 00:40:34	V3600	V3600	140.96.102....	adslAtucRateChange...
8	2005-01-07 00:40:34	V3600	V3600	140.96.102....	adslAtucRateChange...
9	2005-01-07 00:41:18	V3600	V3600	140.96.102....	adslAtucRateChange...
10	2005-01-07 01:53:30	V3600	V3600	140.96.102....	adslAtucRateChange...
11	2005-01-07 01:54:25	V3600	V3600	140.96.102....	adslAtucRateChange...
12	2005-01-07 01:55:08	V3600	V3600	140.96.102....	adslAtucRateChange...
13	2005-01-07 01:55:53	V3600	V3600	140.96.102....	adslAtucRateChange...
14	2005-01-07 01:56:36	V3600	V3600	140.96.102....	adslAtucRateChange...
15	2005-01-07 01:57:21	V3600	V3600	140.96.102....	adslAtucRateChange...

Figure 8-4. 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 CMS server can capture are listed as followings:

Trap Name	Trap description
ColdStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
WarmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.
LinkDown	A linkDown trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the if OperStatus object for one of its communication links is about to transit into the down state.
LinkUp	A linkUp trap signifies that the SNMPv2 entity, acting in an agent role, has detected that the if OperStatus object for one of its communication links has transitted out of the down state.
AuthenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
EgpNeighborLoss	An egpNeighborLoss trap signifies that an EGP neighbor has been marked down and the EGP peer relationship no longer obtains.
GsvAdslAtucOpstateChangeTrap	This trap indicates the change in the operational status of the port.
GsvPortBindingInFdbChangedTrap	This trap indicates that the port on which the mac address has been learned has changed.
GsvPortMacAddrChangeTrackTrap	This trap indicates that the port on which the tracked MAC address is being received has changed.
GsvPortMacAddrFirstTrackTrap	This trap indicates that the particular mac address has been received for the first time. This trap will also be received if the tracked MAC address is received from an existing port and the port from which it was earlier received has been deleted by now.
GsvIpaddrGetFailTrap	This trap indicates that DHCP client could not get an ip address from DHCP server.
GsvControlQueueCongestionStartTrap	For ethernet or atm interface, this trap indicates that the interface is in congestion.

GsvControlQueueCongestionStopTrap	For ethernet or atm interface, this trap indicates that the congestion on this interface has eased.
GsvInterfaceStatsResetTrap	This trap indicates that interface status has been reset for an interface.
GsvAdslChipLockUpDetectedTrap	This trap indicates that all the Xcvrs in the chip have locked up.
GsvAdslChipLockUpRecoveryTrap	This trap indicates that the chip has successfully recovered from the lock up condition.
GsvAdslChipLockUpRecoveryFailedTrap	This trap indicates that the recovery from lockup condition of the chip has failed.
GsvAdslChipPreInitChkSumFailedTrap	This trap indicates that the pre-init checksum calculation for the chip failed.
GsvAdslXcvrLockUpDetectedTrap	This trap indicates that an Xcvr lockup has been detected.
GsvAdslXcvrLockUpRecoveryTrap	This trap indicates successful recovery of an Xcvr from the lockup condition.
GsvAdslXcvrLockUpRecoveryFailedTrap	This trap indicates the failure of Xcvr's recovery from lockup.
GsvAdslAtucPerfLofsThresh1DayTrap	This trap indicates that Loss of Framing 1-Day interval threshold for ATUC has reached.
GsvAdslAtucPerfLossThresh1DayTrap	This trap indicates that Loss of Signal 1-Day interval threshold for ATUC has reached.
GsvAdslAtucPerfLolsThresh1DayTrap	This trap indicates that Loss of Link 1-Day interval threshold for ATUC has reached.
GsvAdslAtucPerfLprsThresh1DayTrap	This trap indicates that Loss of Power 1-Day interval threshold for ATUC has reached.
GsvAdslAtucPerfESsThresh1DayTrap	This trap indicates that Errored Second 1-Day interval threshold for ATUC has reached.
GsvAdslAtucPerfSesLThresh1DayTrap	This trap indicates that Severely Errored Seconds-line 1-Day threshold for ATUC has reached.
GsvAdslAtucPerfUasLThresh1DayTrap	This trap indicates that Unavailable Seconds-line 1-Day threshold for ATUC has reached.
GsvAdslAturPerfLofsThresh1DayTrap	This trap indicates that Loss of Framing 1-Day interval threshold for ATUR has reached.
GsvAdslAturPerfLossThresh1DayTrap	This trap indicates that Loss of Signal 1-Day interval threshold for ATUR has reached.

GsvAdslAturPerfLprsThresh1DayTrap	This trap indicates that Loss of Power 1-Day interval threshold for ATUR has reached.
GsvAdslAturPerfESsThresh1DayTrap	This trap indicates that Errored Second 1-Day interval threshold for ATUR has reached.
GsvAdslAturPerfSesLThresh1DayTrap	This trap indicates that Severely Errored Seconds-line 1-Day threshold for ATUR has reached.
GsvAdslAturPerfUasLThresh1DayTrap	This trap indicates that Unavailable Seconds-line 1-Day threshold for ATUR has reached.
GsvPppoeMaxDiscDoneTrap	This trap indicates that the maximum retries in discovery stage have exceeded for a PPPoE interface.
GsvAdslAtucPerfFecsLThreshTrap	This trap indicates that Forward error correction seconds 15-Min threshold for ATUR has reached.
GsvAdslAtucPerfFecsLThresh1DayTrap	This trap indicates that Forward error correction seconds 15-Min threshold for ATUC has reached.
GsvAdslAturPerfFecsLThreshTrap	This trap indicates that Forward error correction seconds 15-Min threshold for ATUR has reached.
GsvAdslAturPerfFecsLThresh1DayTrap	This trap indicates that Forward error correction seconds 1-Day threshold for ATUR has reached.
GsvHdsl2ShdslFramerOHAndDefects	This trap indicates the Framer Overhead and Defects
GsvShdslOpStateChangePortId	This trap indicates the change in the operational status of the port.
GsvShdslRmtAtmCellStatusTrap	This trap indicates the SHDSL Remote ATM Cell Status Response.
GsvShdslConfReqUtcTrap	This trap indicates the SHDSL UTC recieved in response of STU-R Config Request.
GsvShdslRmtEOCUtcTrap	This trap indicates the SHDSL UTC Recieved in response of Remoting EOC request.
GsvShdslGenericFailureTrap	This trap indicates the SHDSL Generic Failure Trap.
GsvAtmPortUnderDeficitTrap	This trap indicates that the atm port is under deficit as per rate required by its classes based on the scheduling profile applied to the ATM port.
GsvAtmPortOutOfDeficitTrap	This trap indicates that the atm port has come out of deficit.

GsvAsaAtmVcEncapTypeChangedTrap	This trap indicates that Autosensing agent has changed the ATM VC AAL5 Encapsulation Type.
GsvAdslAtucPmStateChangeTrap	This trap indicates that Auto Sensing Agent is unable to Tear Down the current stack due to configuration change.
GsvDslChipLbusAccessFailedTrap	This trap indicates that Auto Sensing Agent is unable to Tear Down the current stack due to configuration change.
GsvFanUpTrap	This trap indicates the FAN Up Trap.
GsvFanDownTrap	This trap indicates the FAN Down Trap.
GsvFanRecoverTrap	This trap indicates the FAN Recover Trap.
GsvFanStuckTrap	This trap indicates the FAN Stuck Trap.

8.2 Log management

Log management includes the user login/logout history, action history, and device set history stored in the backend database. CMS provides a query interface for operators to query these history logs.

8.2.1 User Login/Logout log

User Login/Logout logs record the information of the user login or logout CMS system. You can select the User login/out log to active the user log GUI interface on the System Manager.

Gentime	User Name	Client Address	Start Time	End Time
2005-08-08 19:16:45	root	172.16.2.166	2005-08-08 19:16:45	2005-08-08 19:19:19
2005-08-08 19:19:19	root	172.16.2.166	2005-08-08 19:19:19	2005-08-08 19:19:19
2005-08-08 19:23:23	root	172.16.2.166	2005-08-08 19:23:23	2005-08-08 19:23:23

Figure 8-5. User Login/out Log window

The fields of this function are described as followings:

Gen Time

The timestamp of the user log is generated.

User Name

Display the name of the login user.

Client Address

Display the ip address of the login user computer.

Start Time

Display the login time.

End Time

Display the logout time.

8.2.2 Device Set log

Device Set logs record the information of the users' setting device likes provision, line profile and alarm profile. You can select the Device Set log to active the device set log GUI interface on the System Manager. The page is shown in Figure 8-6.

Gentime	User Name	Client Address	Device IP	Community
2005-08-01 17:51...	root	172.16.2.166	172.16.2.151	private_00
2005-08-01 17:54...	root	172.16.2.166	172.16.2.151	private_00
2005-08-01 17:55...	root	172.16.2.166	172.16.2.151	private_00
2005-08-02 18:28...	root	172.16.2.166	172.16.2.151	private_00
2005-08-02 18:28...	root	172.16.2.166	172.16.2.151	private_00
2005-08-02 18:28...	root	172.16.2.166	172.16.2.151	private_00
2005-08-02 18:28...	root	172.16.2.166	172.16.2.151	private_00
2005-08-02 18:37...	root	172.16.2.166	172.16.2.151	private_00
2005-08-02 18:39...	root	172.16.2.166	172.16.2.151	private_00
2005-08-02 19:25...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 09:27...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 09:44...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 09:44...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 09:46...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 09:46...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 09:46...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 09:50...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 09:52...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 10:10...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 10:10...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 10:13...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 10:13...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 13:41...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 13:41...	root	172.16.2.166	172.16.2.151	private_00
2005-08-03 13:41...	root	172.16.2.166	172.16.2.151	private_00

Figure 8-6. Device set log window

The fields of this function are described as followings:

Gen Time

The timestamp of the user log is generated.

User Name

Display the name of the login user.

Client Address

Display the ip address of the login user computer.

Device IP

Display the ip address of the setting device.

Community

Display the snmp write community of the setting device.

Action Name

Describe the action of the setting.

Error Status

Describe the setting is successful or not.

Error Index

Describe the error index on setting content if error status is greater than 0.

Error Text

Describe the error on setting content if error status is greater than 0.

Content

Set content.

8.2.3 Action log

Action logs record the information of any requests from users to CMS System. For instance, if you want to see the port status, you can active the port status panel and select one port to get port status. At this time, CMSClient will request CMSServer to get the port information from device and return, then CMSClient displays it on the port status panel. We call this is a action. As a result, action logs record very detail information for any users' requests. You can select the Action log to active the action log GUI interface on the System Manager. Figure 8-7 is shown as below.

Action Class	User Name	Client Address	Server Address	Action Time	Client
EntityQryAction	root	172.16.2.166	172.16.2.166	2005-08-08 19:16...	2005-08-
AutoDeployLogsQ...	root	172.16.2.166	172.16.2.166	2005-08-08 19:17...	2005-08-
TrapHistoryDetail...	root	172.16.2.166	172.16.2.166	2005-08-08 19:17...	2005-08-
DataMaintainAction	root	172.16.2.166	172.16.2.166	2005-08-08 19:17...	2005-08-

Figure 8-7. Action log window

The fields of this function are described as followings:

Action Class

Describe the action of the request.

User Name

Display the name of the login user.

Client Address

Display the ip address of the login user computer.

Server Address

Display the ip address of the CMS Server.

Action Time

The timestamp of the action is generated.

Client Time

The timestamp of the action is requested by users.

Process Time

The timestamp of the action is starting to process by server .

Server Time

The timestamp of the action is responding to client.

Request Content

Display the parameter of the request.

Response Content

Display the parameter of the response.

CHAPTER 9

Profile Management

The function of profile management for CMS 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.

This chapter is divided into the following sections,

- Section 9.1: Line Profile Management
- Section 9.2: Alarm Profile Management
- Section 9.3: ATM Traffic Profile Management
- Section 9.4: TrafficClass Profile Management
- Section 9.5: PVC Profile Management

9.1 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 Figure 9-1; the functions of line profile management are described as followings:

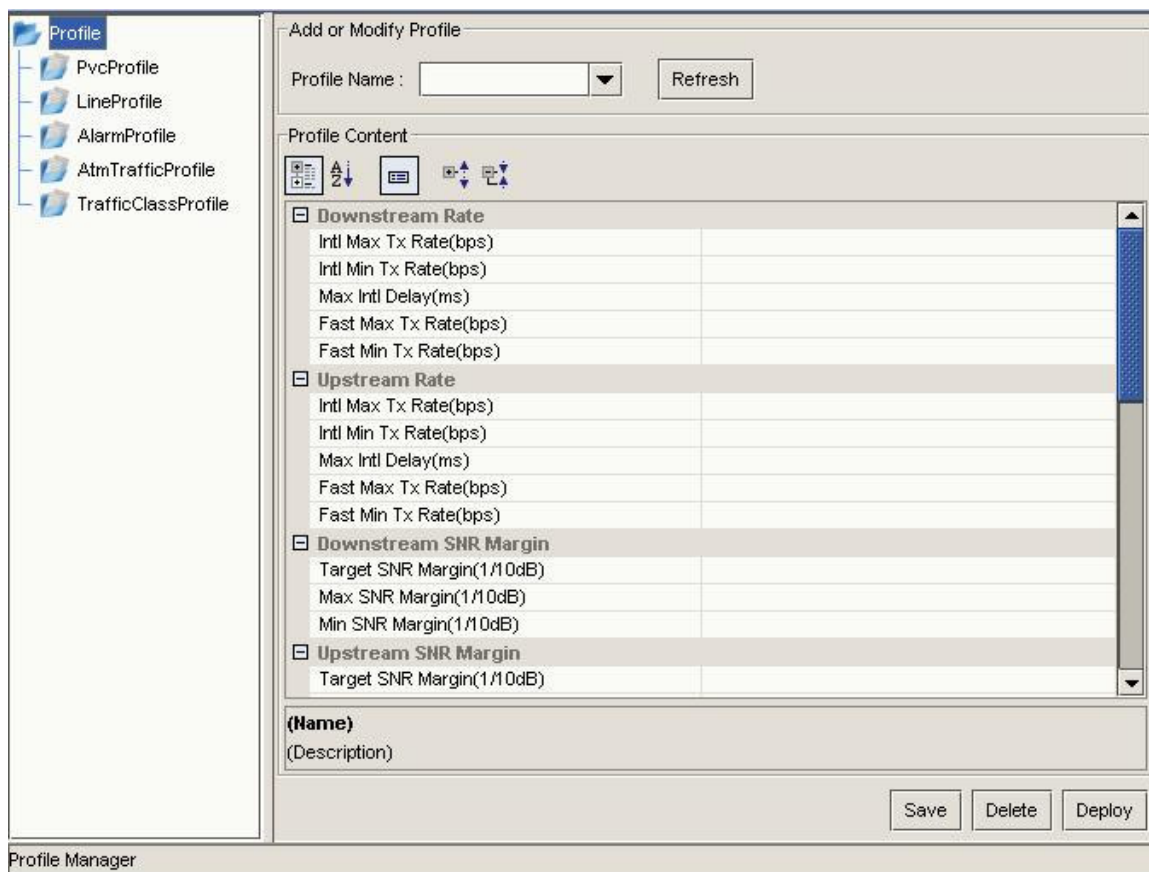


Figure 9-1. Line profile management window

9.1.1 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 selecting 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.

9.1.2 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.

9.1.3 Delete Line Profile

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

9.1.4 Select Line Profile

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

Step1 : After pushing the Select button, the system will display a dialog to choose devices and port as below Figure 9-2:

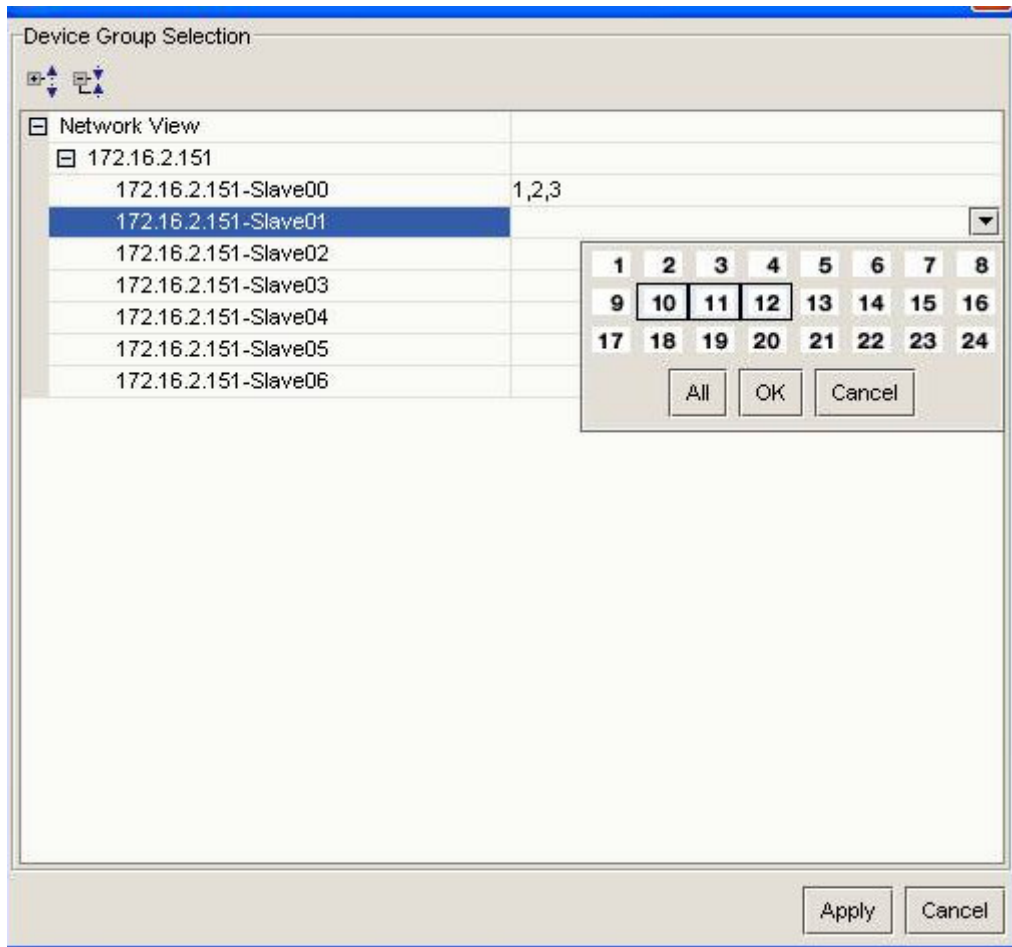


Figure 9-2. Device group selection dialog

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 below Figure9-3:

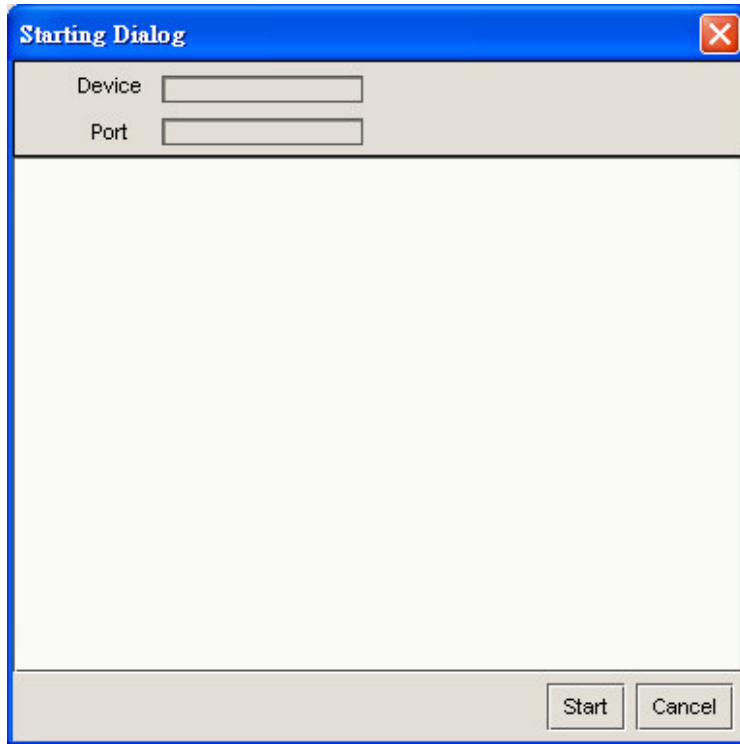


Figure 9-3. Deploy progress dialog

Step3 : Push the start button to start the deploy the line profile, the result will display on the center of the dialog as below Figure 9-4 :

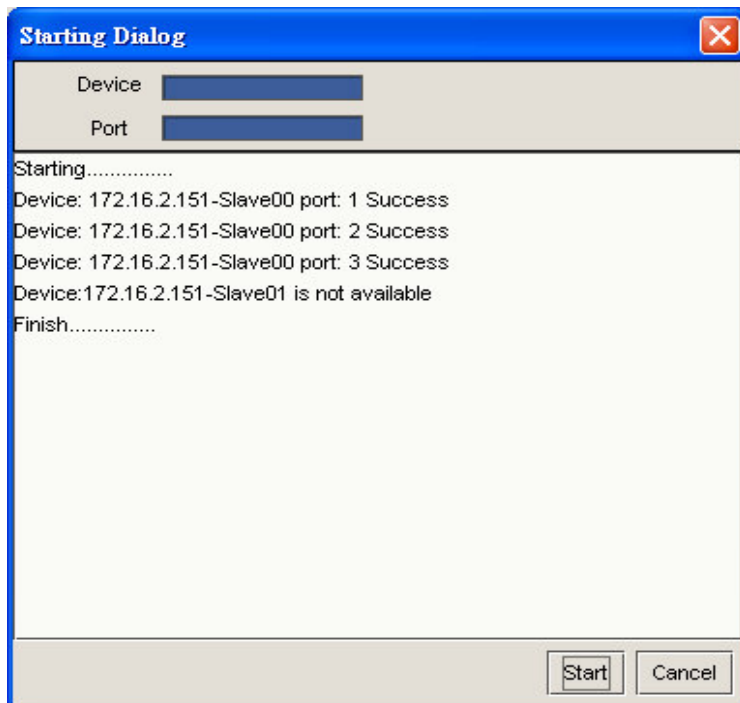


Figure 9-4. Deploy progress dialog

9.2 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 Figure 9-5; the functions of alarm profile management are described as followings:

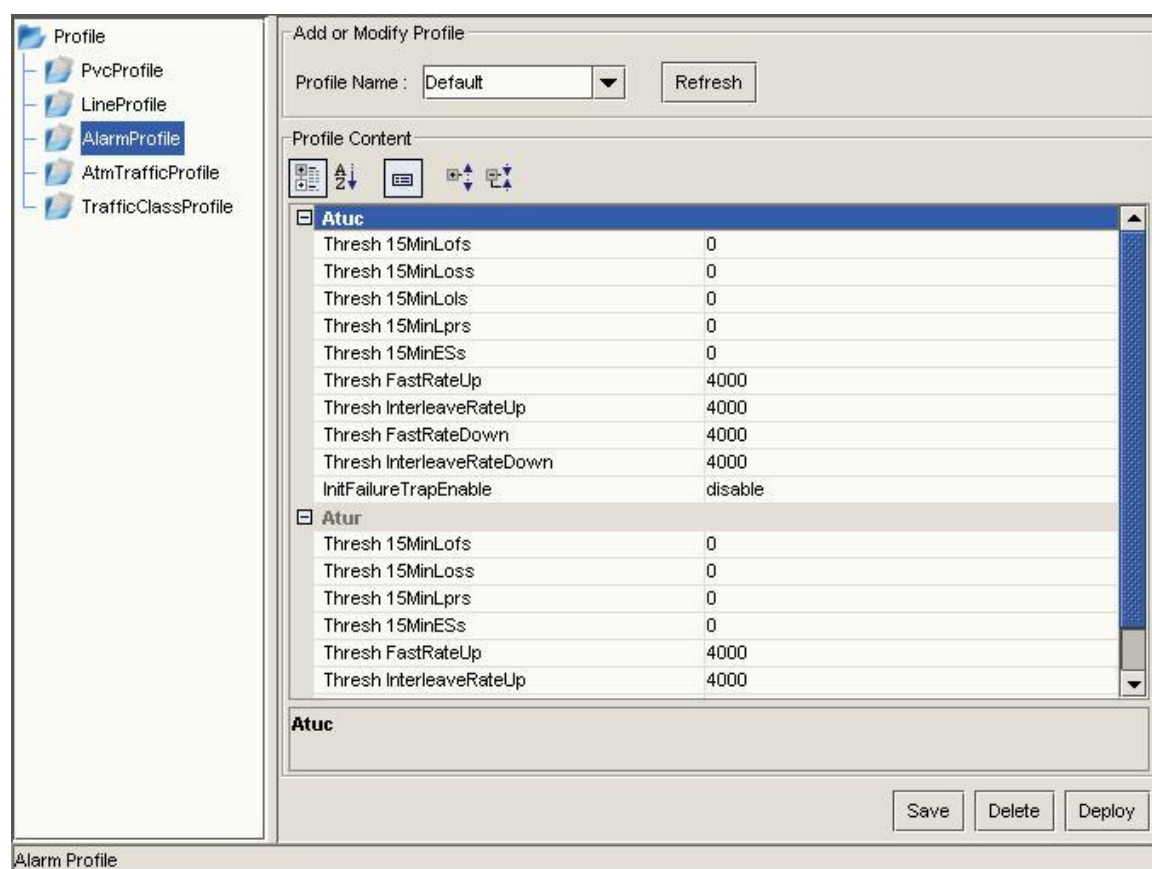


Figure 9-5. Alarm profile management window

9.2.1 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 choose any profiles by selecting 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.

9.2.2 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.

9.2.3 Delete Alarm Profile

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

9.2.4 Select Alarm Profile

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

Step1 : After pushing the Select button, the system will display a dialog to choose devices and port as below Figure 9-6:

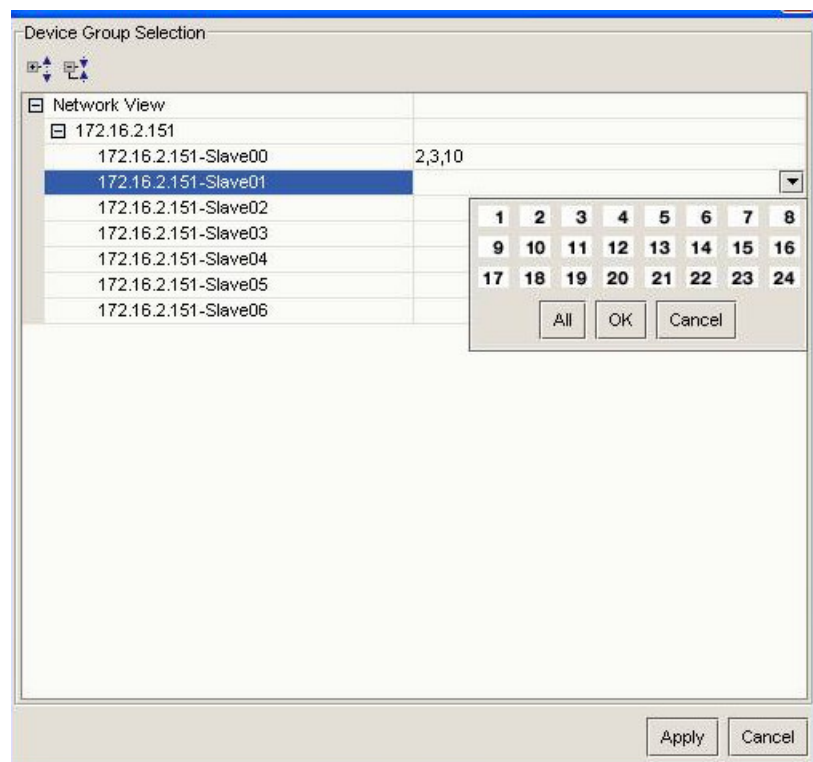


Figure 9-6. Device group selection dialog

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 below Figure 9-7:

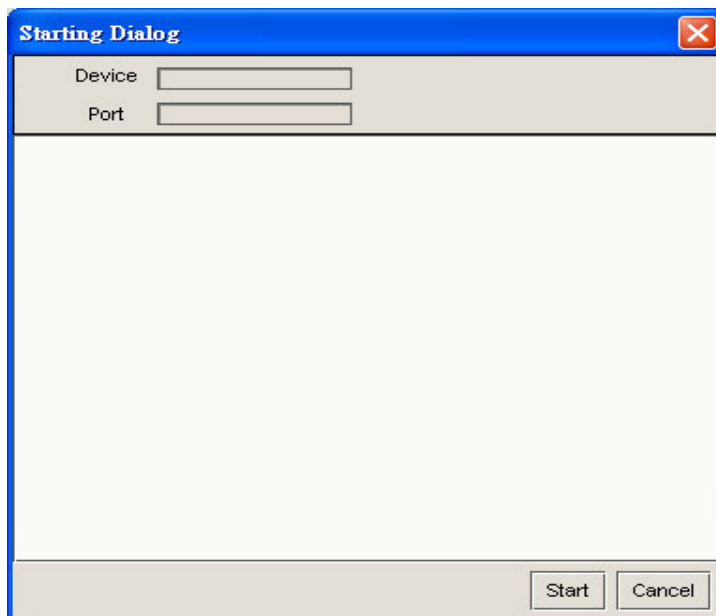


Figure 9-7. Deploy progress dialog

Step3 : Push the start button to start the deploy the alarm profile, the result will display on the center of the dialog as below Figure 9-8:

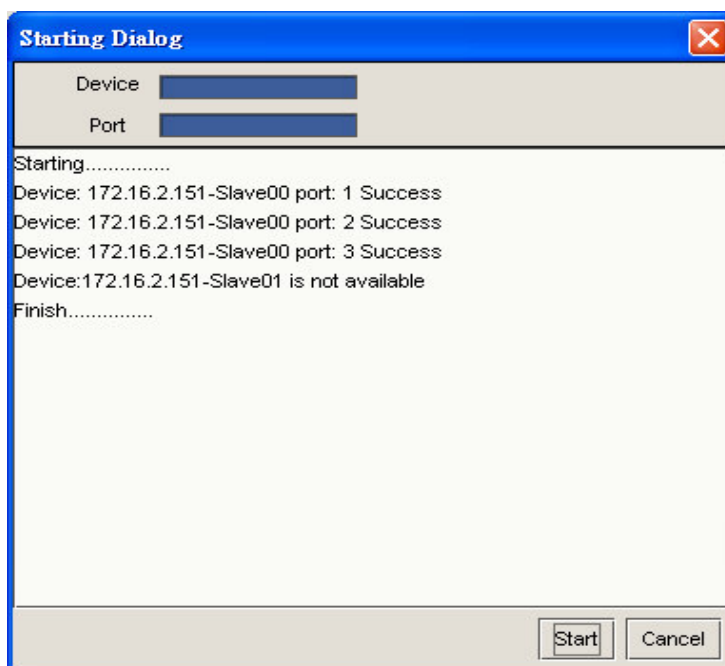


Figure 9-8. Deploy progress dialog

9.3 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 Figure 9-9; the functions of Atm traffic profile management are described as followings:

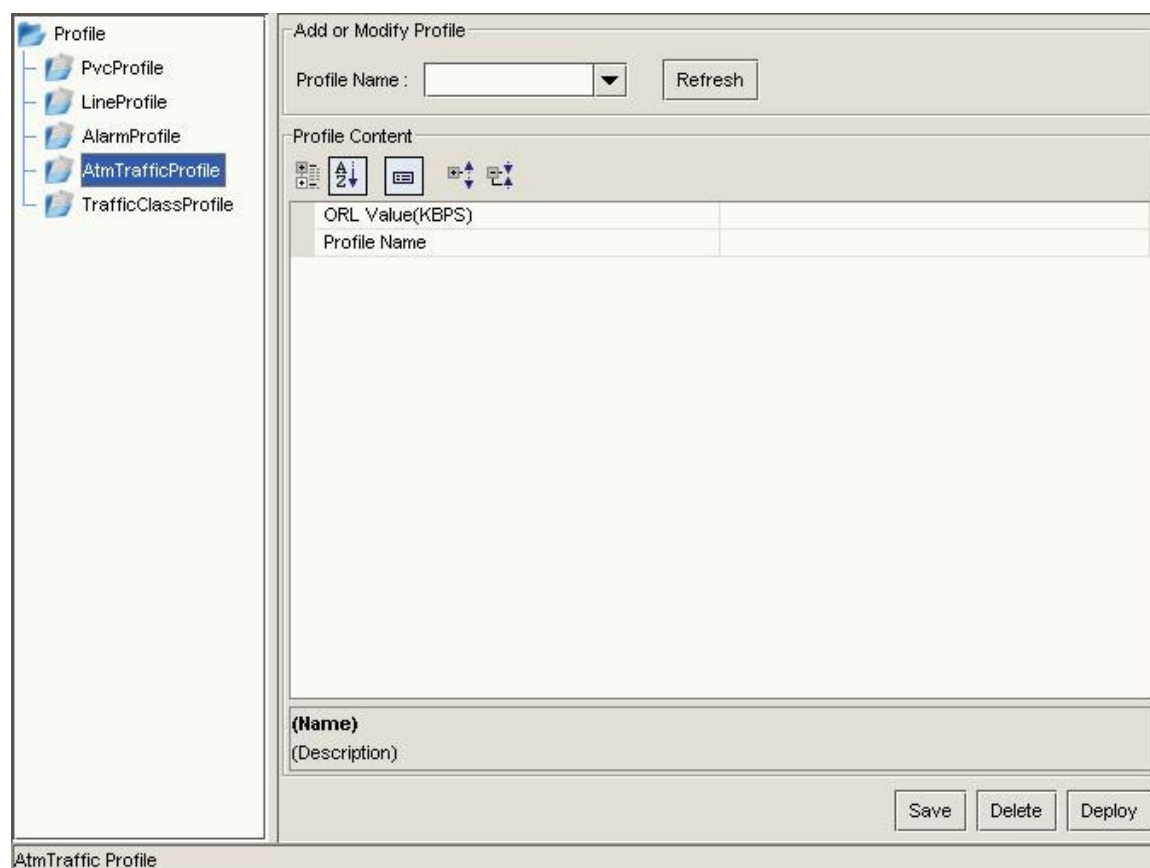


Figure 9-9. Atm Traffic profile management window

9.3.1 Refresh Atm Traffic Profile

After starting the Atm traffic profile window, the system will query the all Atm traffic profiles which store on the backend database. You can choose any profiles by selecting an Atm 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.

9.3.2 Save Atm Traffic Profile

After changing the profile content, you can use the save button to save the Atm 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.

9.3.3 Delete Atm Traffic Profile

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

9.3.4 Select Atm Traffic Profile

Select button let you to deploy the Atm traffic profile to the device. The steps go as follows:

Step1 : After pushing the Select button, the system will display a dialog to choose devices and port as below Figure 9-10:

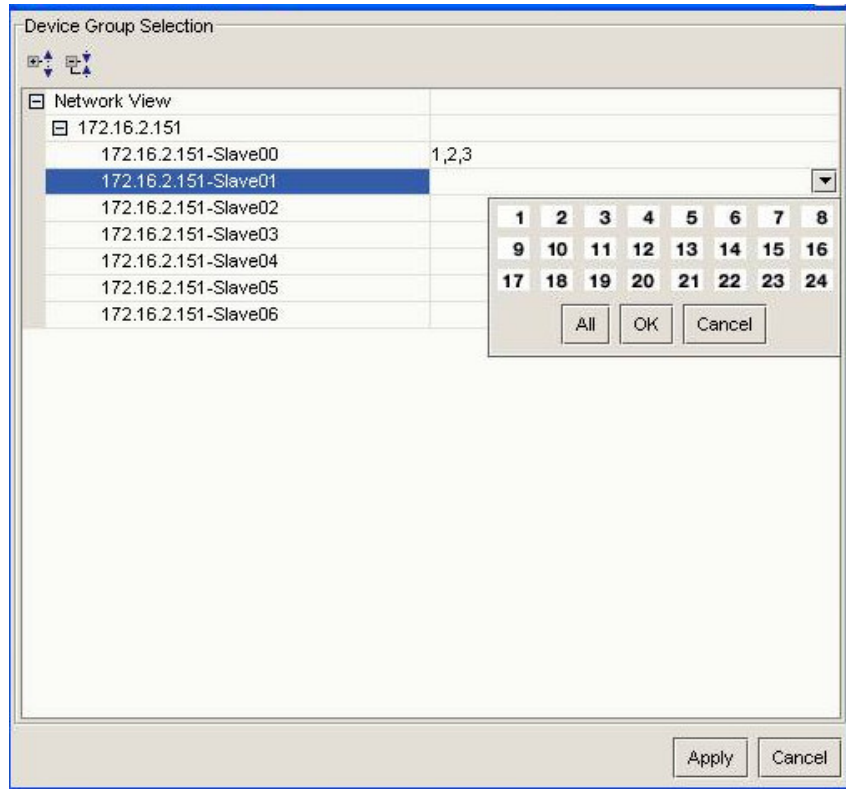


Figure 9-10. Device group selection dialog

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 below Figure 9-11:

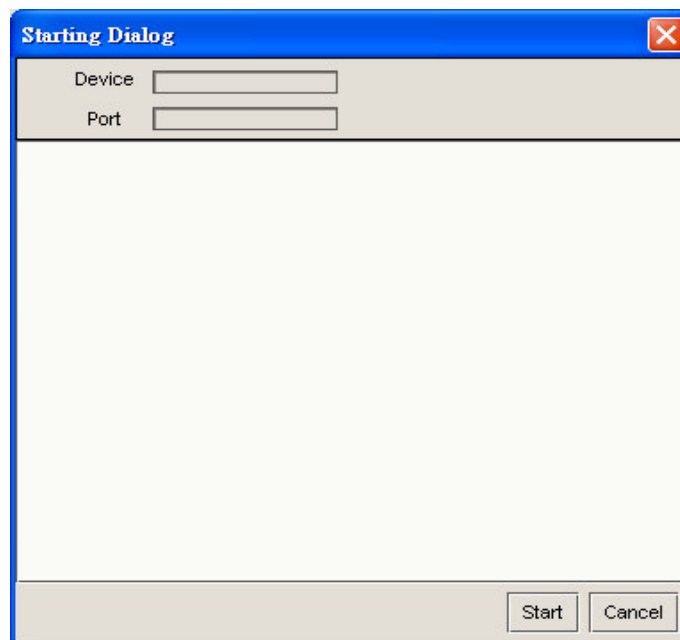


Figure 9-11. Deploy progress dialog

Step 3 : Push the start button to start the deploy the Atm traffic profile, the result will display on the center of the dialog as below Figure 9-12:

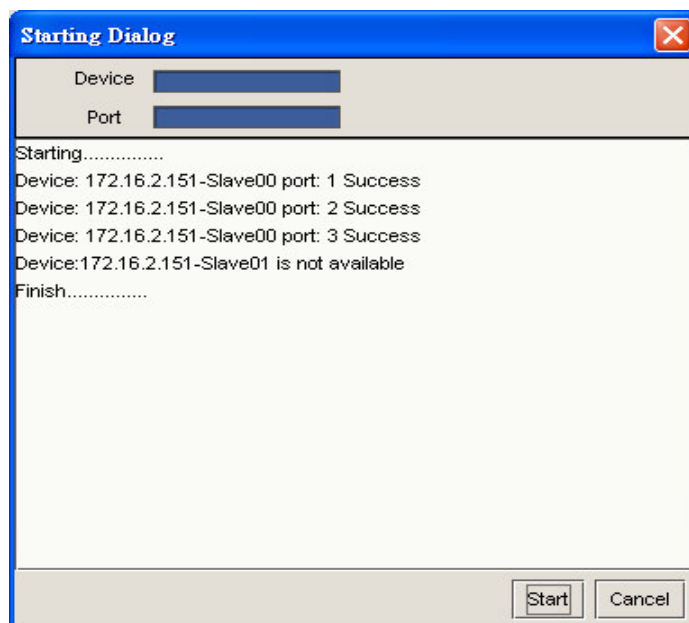


Figure 9-12. Deploy progress dialog

9.4 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 Figure 9-13; 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 :

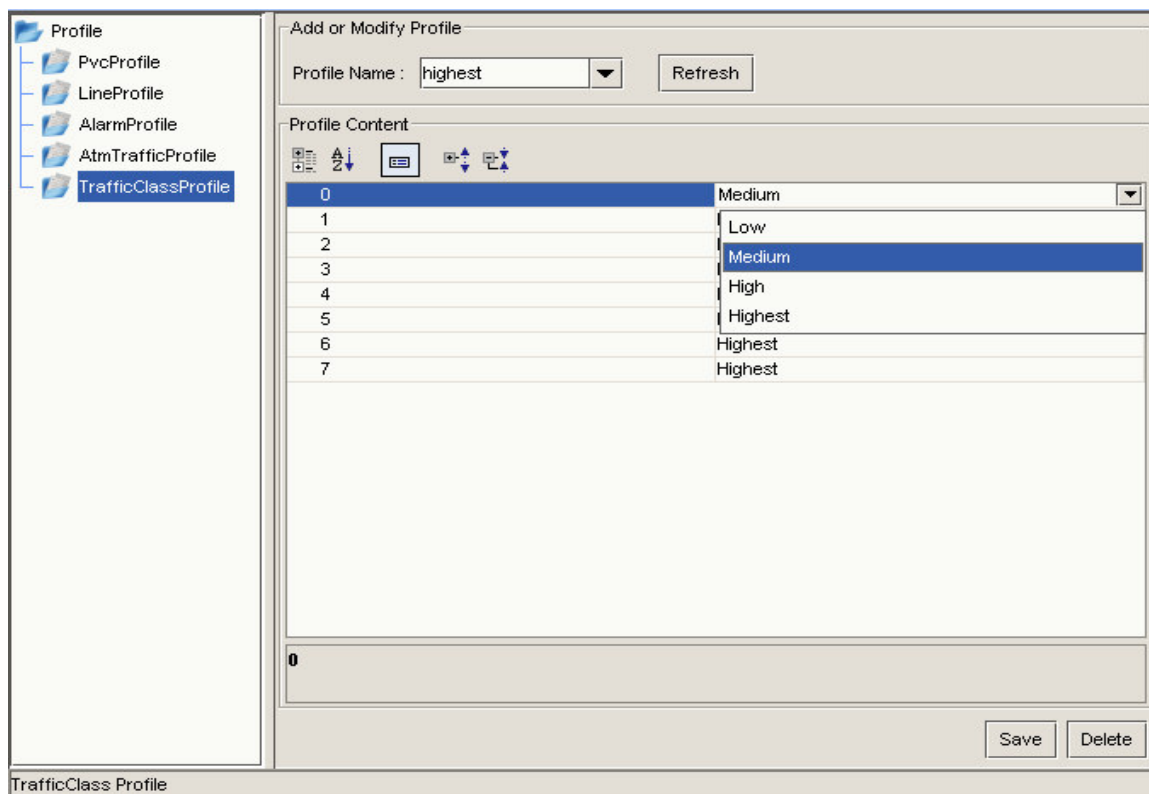


Figure 9-13. Traffic class window

9.4.1 Refresh Traffic Class Profile

After starting the TrafficClass profile window, the system will query the all TrafficClass profiles which store on the backend database. You can choose any profiles by selecting 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.

9.4.2 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.

9.4.3 Delete TrafficClass Profile

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

9.5 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 Figure 9-14; before setting the PVC Profile, the Traffic Class profile should be setup first. The functions of PVC profile management are described as followings: Basically, users may select profile from database or add it manually.

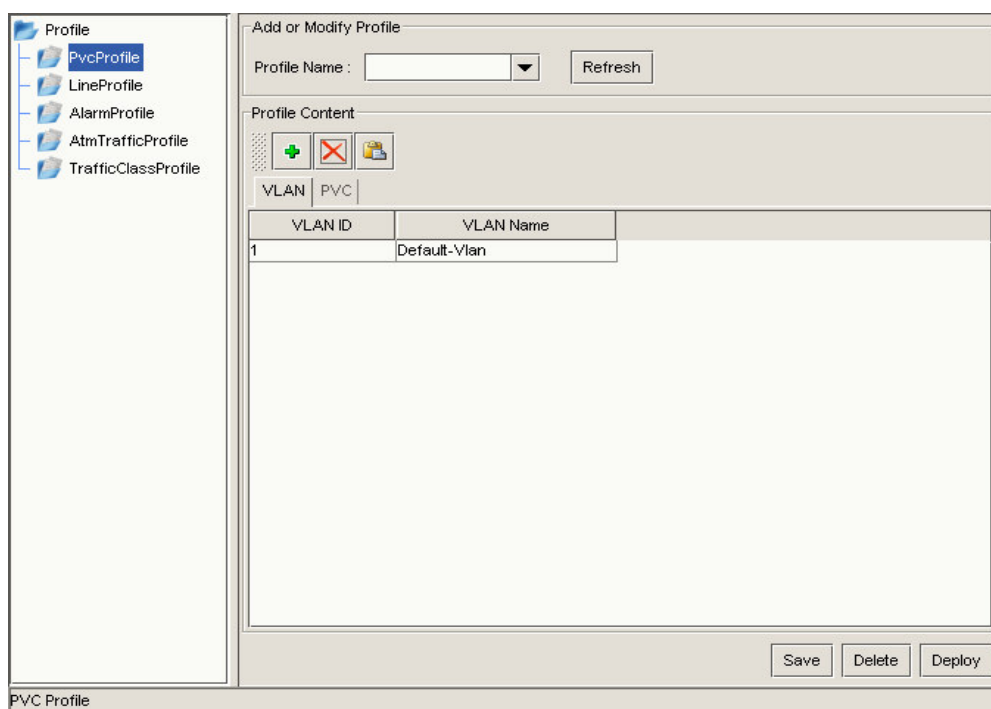


Figure 9-14. PVC profiles VLAN window

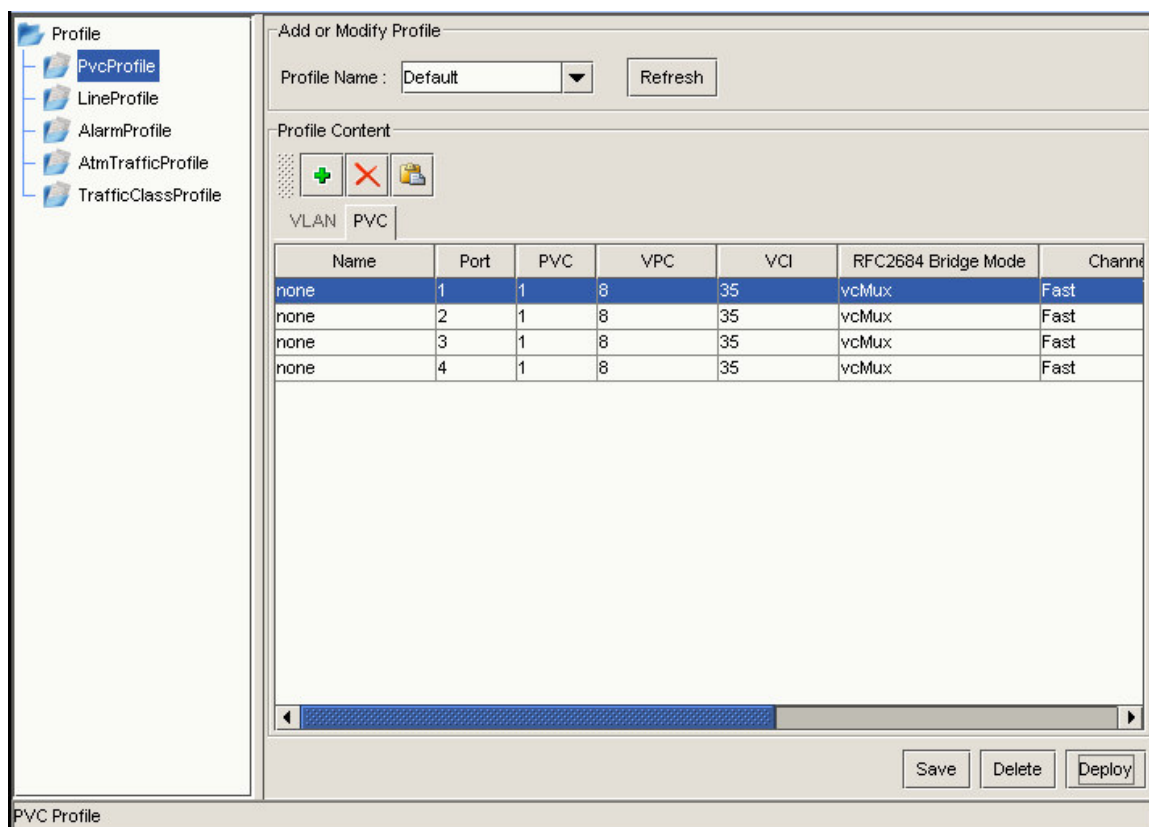


Figure 9-15. PVC profiles PVC window

9.5.1 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 choose any profiles by selecting 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.

9.5.2 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.

9.5.3 Delete PVC Profile

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



The first icon will add a new empty entry to the table. Then users 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 users quickly filled out the table.

9.5.4 Deploy PVC Traffic Profile

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

Step 1 : After pushing the Deploy button, the system will display a dialog to choose devices as below Figure 9-16: the device will be deployed on the value set to “YES”.

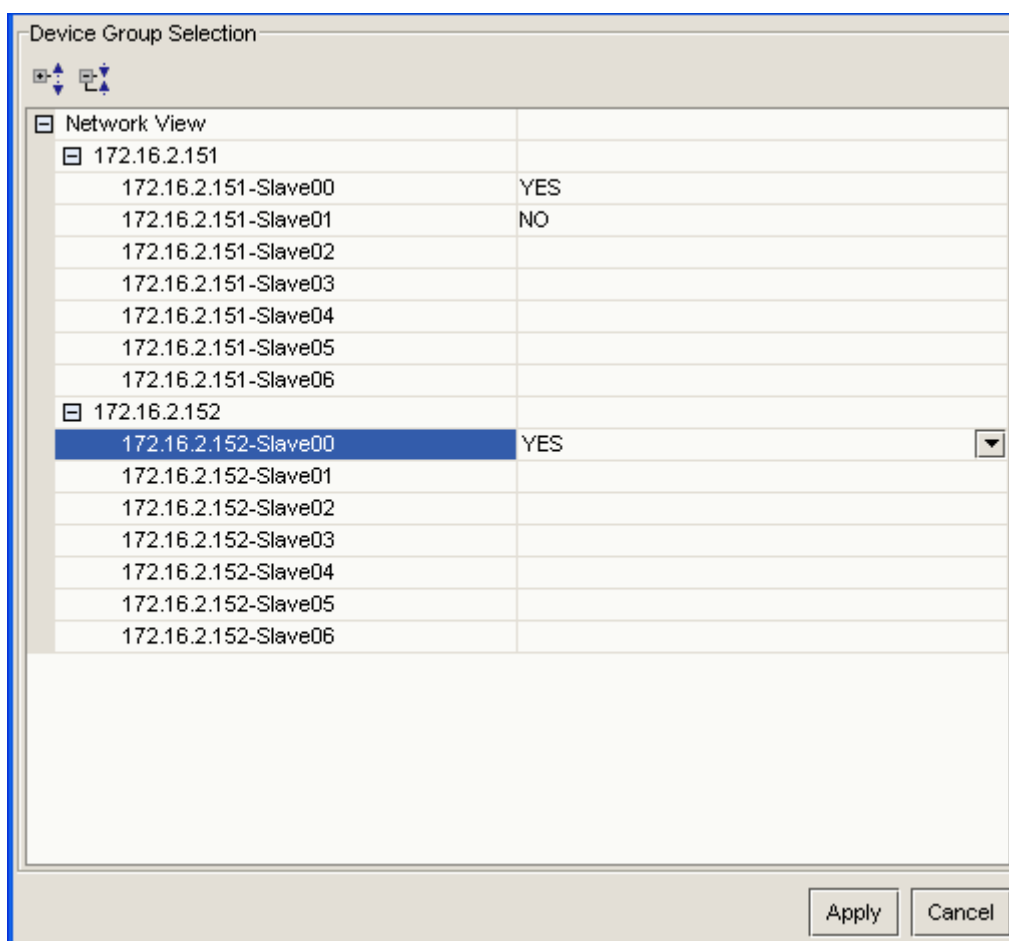


Figure 9-16. Device group selection dialog

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 below Figure 9-17 :

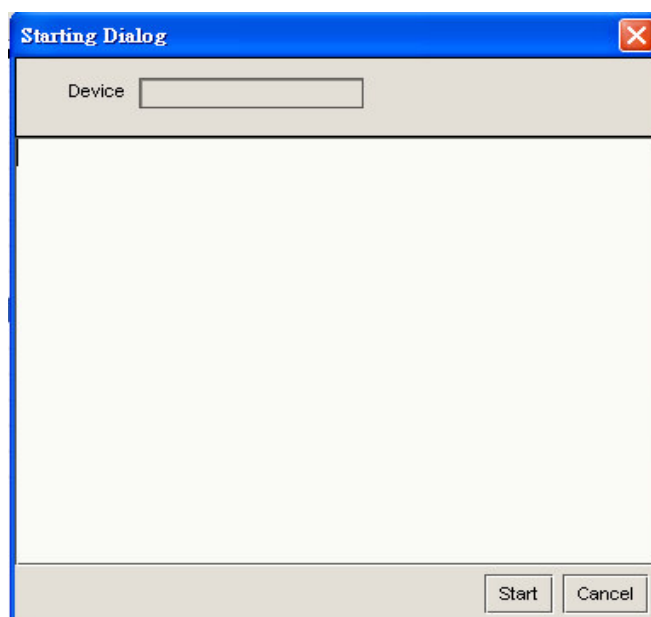


Figure 9-17. Deploy initial progress dialog

Step 3 : Push the start button to start the deploy the PVC profile, the result will display on the center of the dialog as below Figure 9-18: From the result: users 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.

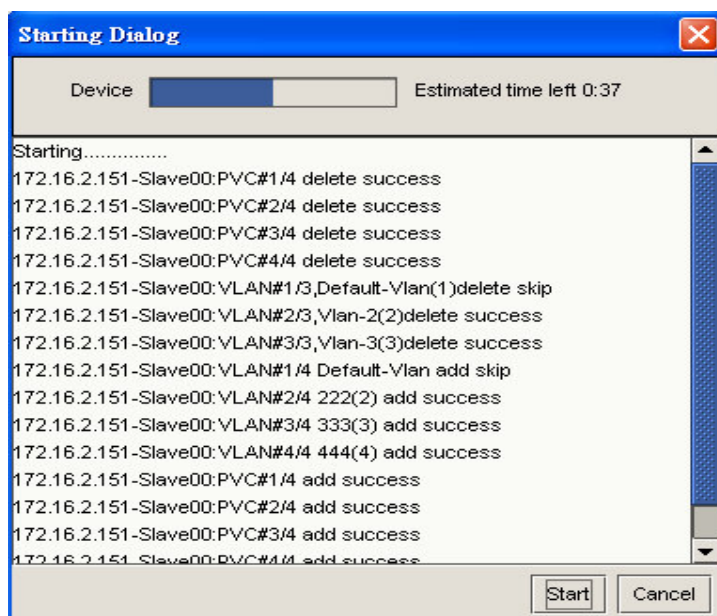


Figure 9-18. Deploy progress dialog

CHAPTER 10

Report

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

This chapter describes how to create alarm history and Long Term PM report. This chapter is divided into the following sections,

- Section 10.1: Report Dialog
- Section 10.2: Alarm History Report
- Section 10.3: Long Term PM Report

10.1 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:

Input Parameter	
Start Date	2005-06-02 00:00:00
End Date	2005-06-02 23:59:59
Severity	All
Alarm Type	All

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.

10.2 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 is shown as below.

Device Name	Device IP	Alarm Time	Device Type	Status	Severity	Alarm Type	Description	Protocol Code	Ack Status	Ack User	Ack Time
172.16.2.131	172.16.2.131	2009/02-17 12:25:52	Master Slave	master-0	Critical	DeviceFail	Link Down	Status = down	1		null
172.16.2.131	172.16.2.131	2009/02-17 12:26:00	Master Slave	master-0	Critical	DeviceFail	Link Down	Status = down	1		null
172.16.2.131	172.16.2.131	2009/02-17 01:14:51	Master Slave	slave-0	Critical	DSL LossConnection	Link Down	Status = down	1		null
172.16.2.131	172.16.2.131	2009/02-17 01:14:51	Master Slave	slave-6	Critical	DSL LossConnection	Link Down	Status = down	1		null
172.16.2.131	172.16.2.131	2009/02-17 01:13:09	Master Slave	slave-0	Critical	DSL LossConnection	Link Down	Status = down	1		null
172.16.2.131	172.16.2.131	2009/02-17 01:15:08	Master Slave	port-3 slave-0	Warning	DSU Port LossConnection	Link Down	Status = down	1		null
172.16.2.131	172.16.2.131	2009/02-17 02:28:07	Master Slave	port-1 slave-0	Warning	DSU Port LossConnection	Link Down	Status = down	1		null

Figure 10-2. Alarm history report

10.3 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 is shown as below.

Queue	Area	CPU	I/O	Mem	LPA	PPA	PPA	PPA	PPA	PPA	PPA	PPA	PPA	PPA	PPA	PPA
2005-06-02 07:15:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 07:30:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 07:45:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 08:00:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 08:15:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 08:30:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 08:45:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 09:00:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 09:15:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 09:30:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 09:45:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 10:00:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 10:15:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 10:30:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 10:45:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 11:00:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 11:15:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 11:30:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005-06-02 11:45:00	Alive	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 10-3. Long Term PM report