

User Manual

IP DSLAM EMS

Version 1.0 June 2006

This user guide is for IP DSLAM EMS
version 3.0 or above.

Table of contents

1	EMS Configuration	3
1.1	EMS Introduction	3
1.2	IP DSLAM EMS Functions	4
1.2.1	Installation	4
1.2.1.1	Hardware and Software Requirements	4
1.2.1.2	Installing EMS	4
1.2.2	Un-install EMS	8
1.2.3	Starting the System	10
1.2.4	Logging into the System	11
1.2.5	Terminating the System	12
1.2.6	Logging out the Current Session	12
1.3	Windows Arrangement	13
1.3.1	Cascade	13
1.3.2	Next Window	13
1.3.3	Previous Window	13
1.3.4	Arrange Icons	13
1.4	Help	15
1.5	Tools Menu Introduction	16
1.5.1	Environmental Options	16
1.5.1.1	SNMP Configuration	16
1.5.1.2	Desktop configuration	16
1.5.1.3	Surveillance configuration	17
1.5.2	Territory manager configuration	18
1.5.2.1	Territory Manager Window	19
1.5.3	Agent Manager Configuration	21
1.5.3.1	Agent Manager Window	21
1.5.3.2	Port DB Manager	23
1.5.3.3	Agent Desktop (Network Monitor)	25
1.5.3.4	Mounted Agent Desktop	27
1.5.4	Telnet	27
1.5.5	Ping	28
1.5.6	User Manager Window	29
1.5.6.1	User Manager Window -- Security	31
2	Manage the IP DSLAM	33
2.1	Activate Function Management Windows	33
2.1.1.1	Function Window:	34
2.1.1.2	Front Panel Window	34

2.2	Default Setting	35
2.3	System Information	36
2.4	Current Event	39
2.4.1	Query	39
2.4.2	Report	40
2.4.3	Refresh	41
2.4.4	Outstanding Event	41
2.4.5	Closed Event	41
2.4.6	Archived	42
2.5	System	43
2.5.1	Commit and Reboot	43
2.6	Configuration	44
2.6.1	VLAN Configuration	44
2.6.1.1	View the VLAN	44
2.6.1.2	Modify the VLAN	44
2.6.1.3	Create a VLAN	45
2.6.2	Ethernet Configuration	47
2.6.2.1	Modify Ethernet	48
2.6.2.2	Create Ethernet	49
2.6.2.3	Delete a Ethernet	50
2.6.3	Static Multicast Configuration	50
2.6.4	IGMP Snooping	51
2.7	DSL	53
2.7.1	Profile Configuration	53
2.7.1.1	Line Profile Configuration	53
2.7.1.2	Alarm Profile Configuration	54
2.7.2	Port Configuration	55
2.7.3	PVC Loopback Testing	56
2.8	DSL Performance Management	58
2.8.1	Physical Layer Info	58
2.8.2	Channel Layer Info	59
2.8.3	Physical Layer PM	59
2.8.4	Channel Layer PM	61
2.9	Get Traffic Information	64

1

EMS Configuration

1.1 EMS Introduction

A Network Management System (NMS), positioning in the highest level of hierarchy, is used to monitor and administer a network.

Under the NMS, an **element management system (EMS)** manages one or more of a specific type of network elements (NEs). An EMS allows the user to manage all the features of each NE individually.

NEs expose one or more management interfaces that the EMS uses to communicate with and to manage them. These management interfaces use a variety of protocols such as SNMP, CLI, XML, and CORBA.

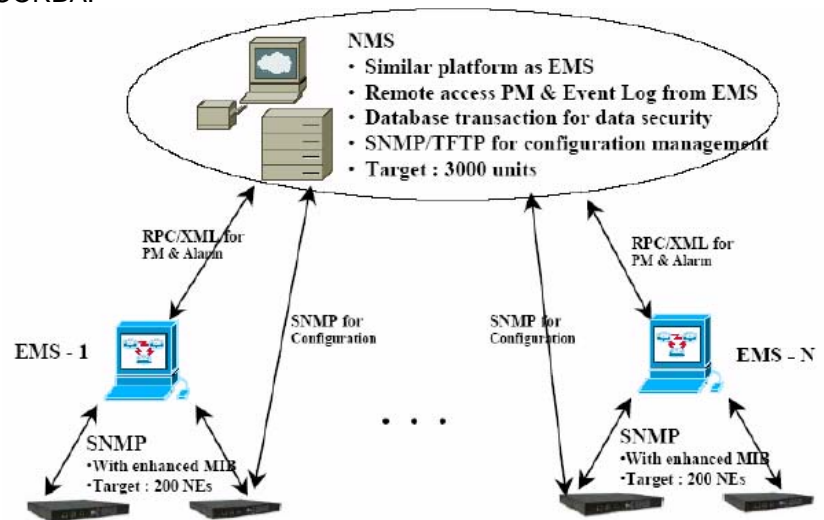


Figure 1-1 Position of EMSs in the Network

1.2

IP DSLAM EMS Functions

IP DSLAM EMS is divided into the task-oriented functional groups as follows, which are further described in subsequent sections.

Session: Allow you to start and to terminate a session as well as to shutdown the system.

- Logout: Allow you to terminate current session without shutting down the system.
- Exit: Allow you to shut down the system.

Tools: Allow you to perform the following tools.

- Environmental options: allow you to define SNMP, Desktop and Surveillance.
- Territory Manager: Used to define the territory.
- Agent Manager: Used to define agent IP addresses.
- Telnet: allow you to login the CID screen of a specific agent IP address.
- Ping: used to check whether a particular IP DSLAM is current connected to the agent or not.
- User manager: Allow you to define a user profile, including login ID and security level.

Windows: allow users to manage daughter windows in the EMS.

- Cascade: allow users to cascade Windows.
- Next Window: allow users to switch to next window.
- Previous Window: allow users to switch to previous window.
- Arrange Icons: those minimized icons will be located in the bottom of EMS.

Help: allow users to view the software version.

- About: software version is displayed.

1.2.1

Installation

1.2.1.1


Hardware and Software Requirements

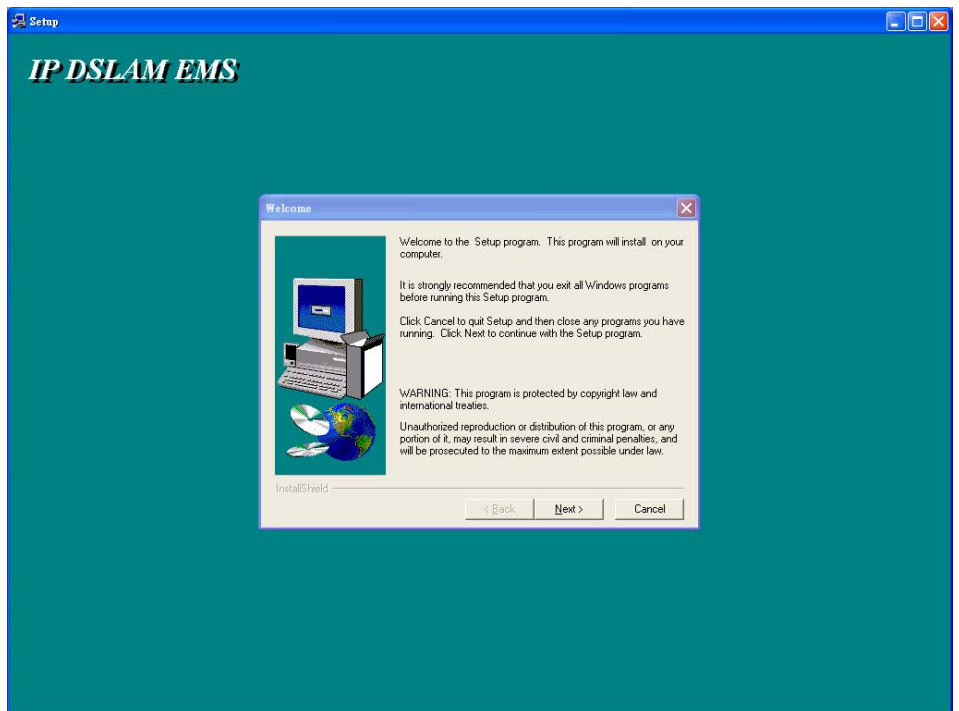
The following checklist provides the minimum hardware and software required to operate EMS.


1. Windows NT/2000/XP
2. Manual CD
3. 2GB Hard disk with a minimum of 650 MB of free space
4. An Ethernet card.
5. Super VGA (800 x 600 resolution) or higher with 256 colors
6. CD-ROM drive

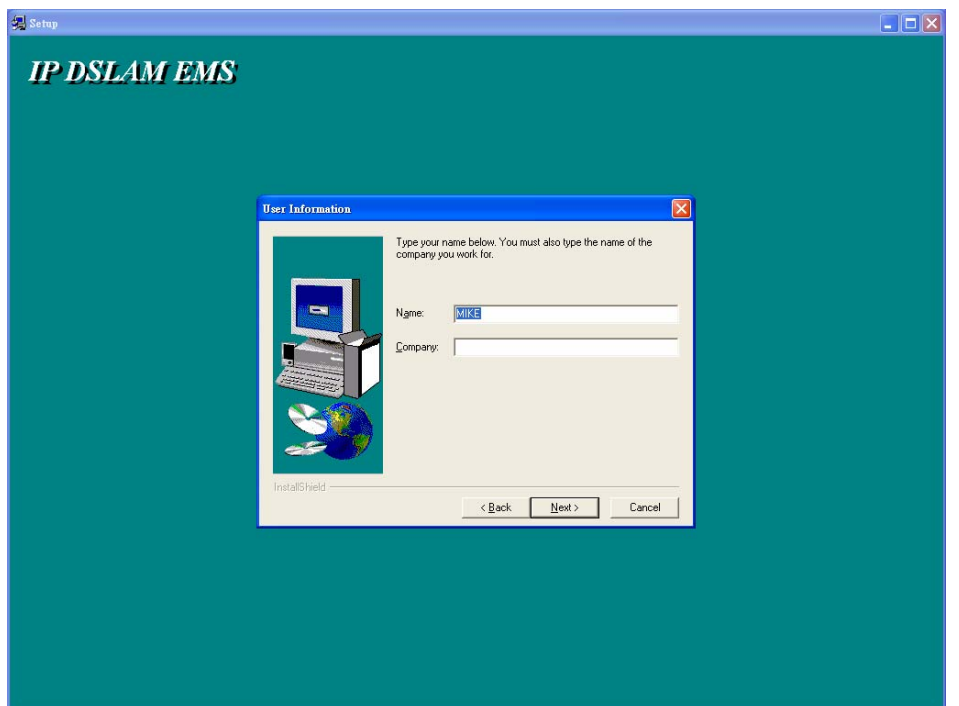
1.2.1.2 Installing EMS

1. Insert Autorun CD into CD –ROM Drive.

2. From the autorun screen, double click the EMS icon to start the installation process.
3. The welcome window of EMS Setup appears. Click on  to continue.




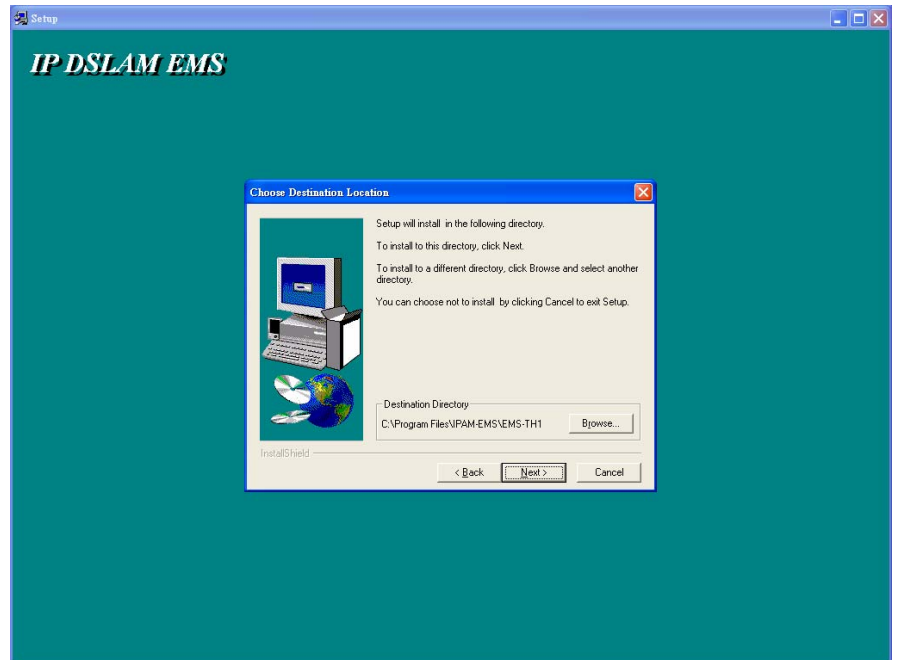
4. When the user information input window appears, enter your name and company name respectively, and then click on  to continue.




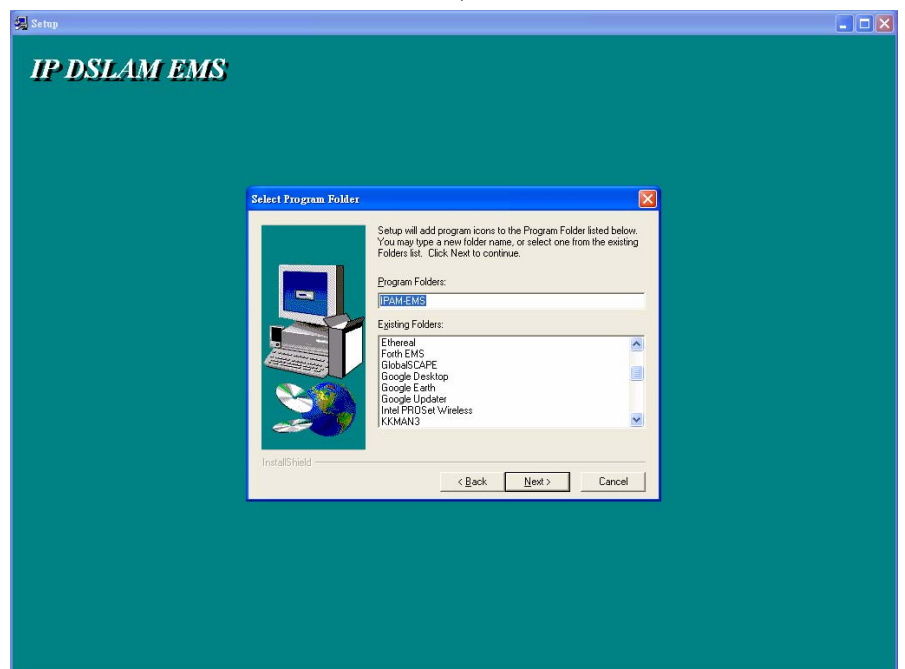
Note: please uninstall previous version of EMS if you want to install a new version.

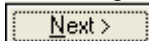
5. When the Destination Location window appears, click the Browse button to change the installation destination directory

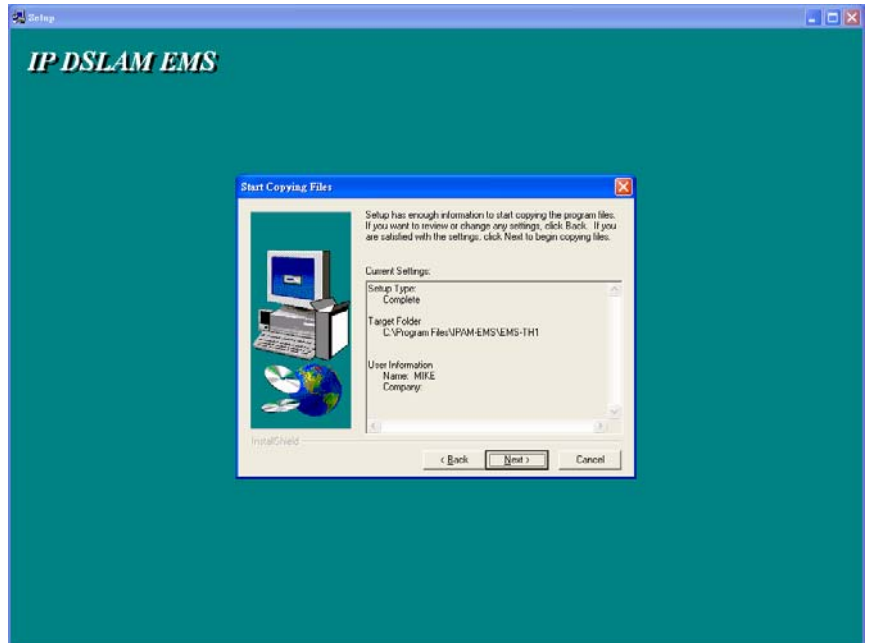
or simply use the default setting “C:\Program Files\EMS\EMS-SD1”. Then, click on  to continue.



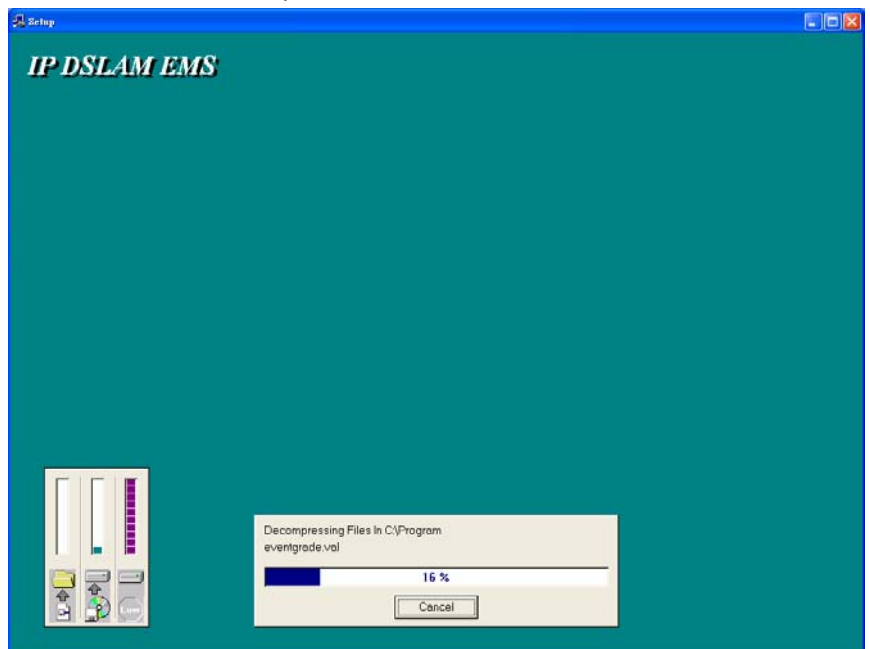
6. When the Select Program Folder window appears, you may either choose the default program folder, “IPAM-EMS\EMS-SD1”, or enter the name you prefer. Then, click on  to continue,




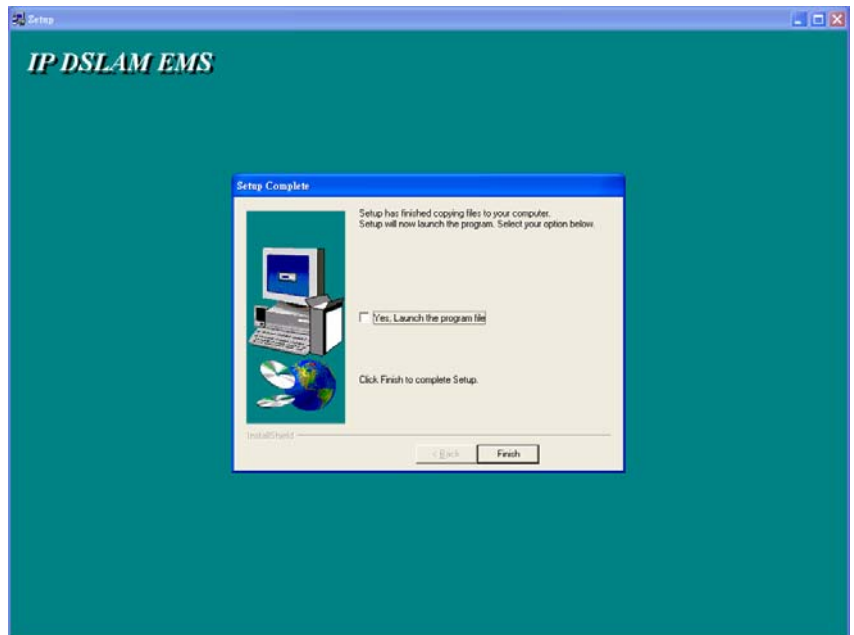
7. When the Start Copying Files window appears, you can confirm your current settings, if you are satisfied with the settings, click on  to start copying files.




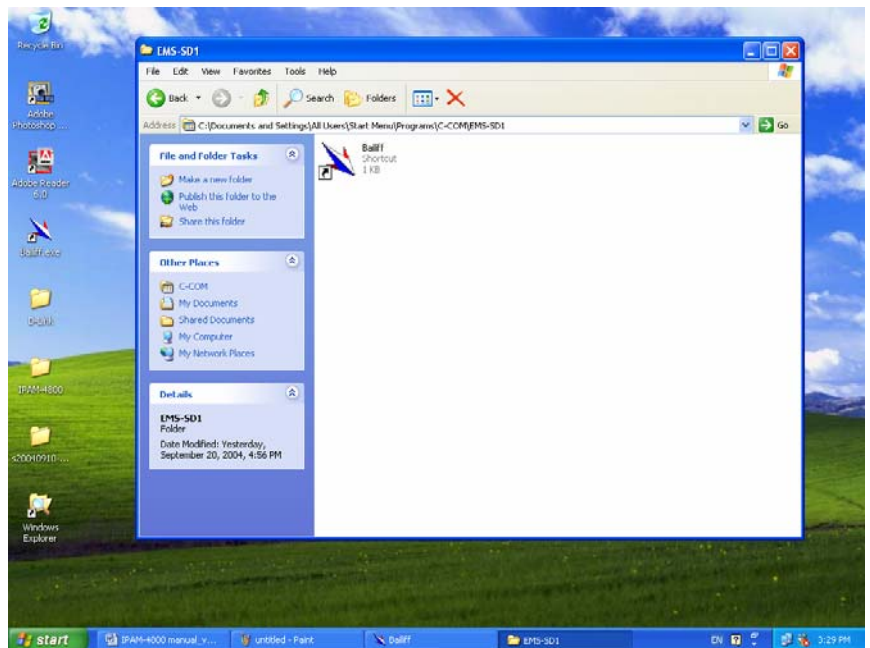
8. When Setup Process Status window appears, the installation process is now in progress. This window displays a bar indicating the percentage of completion for the current installation. In addition, the names of the files being installed appear above the bar until the installation is complete.



9. At the end of the installation process, the following "FINISH" window presents. Simply click on  to complete setup. Now the installation of EMS software is completed.



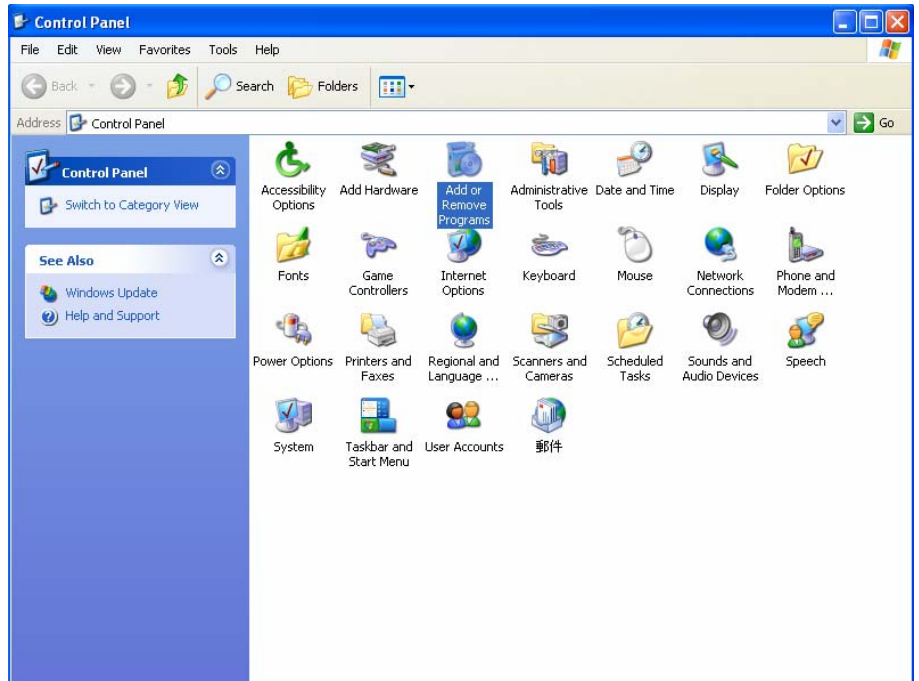
10. After finishing the installation process, a shortcut of EMS is displayed on the desktop. Click on  to activate EMS directly.



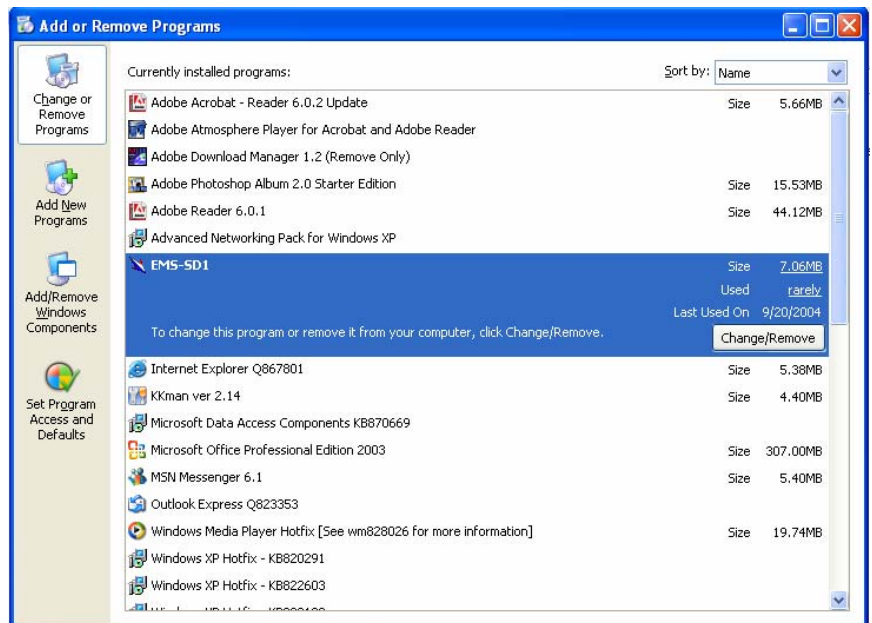
1.2.2

Un-install EMS

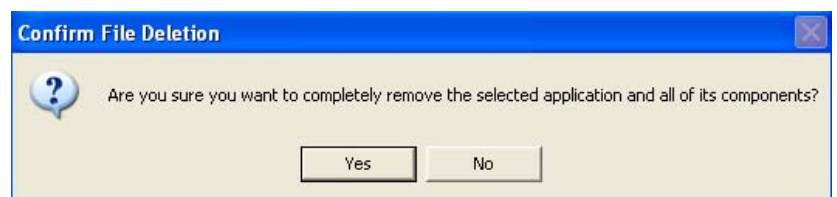
1. Double click the Add/Remove Programs icon in **Control Panel** to run the un-installation procedure.



2. In Add/Remove Programs Properties dialogue box, selecting the “EMS-SD1” folder and then click on **Change/Remove** to remove EMS.



3. After your clicking on **Change/Remove**, the following dialogue box then prompts to you for confirmation. Click on **Yes** to continue the removal process.



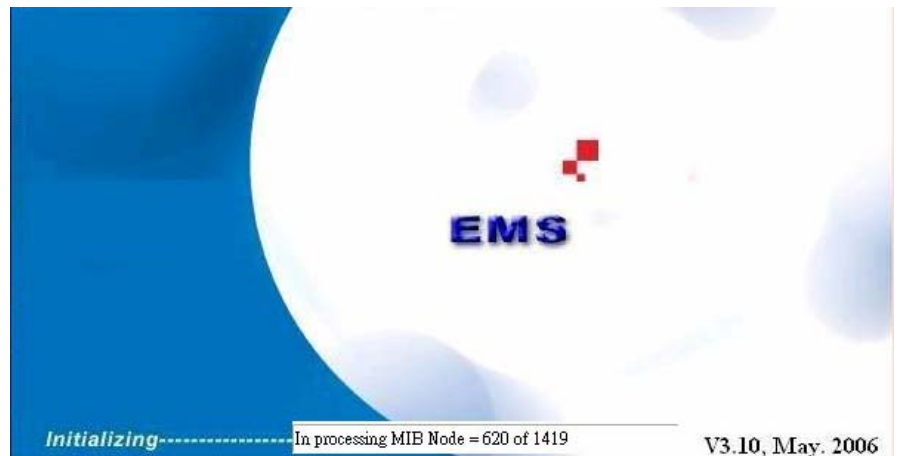
4. The following window, “un-installation completion status” appears. Click to complete the removal process when become enable, indicating that the process is completed.



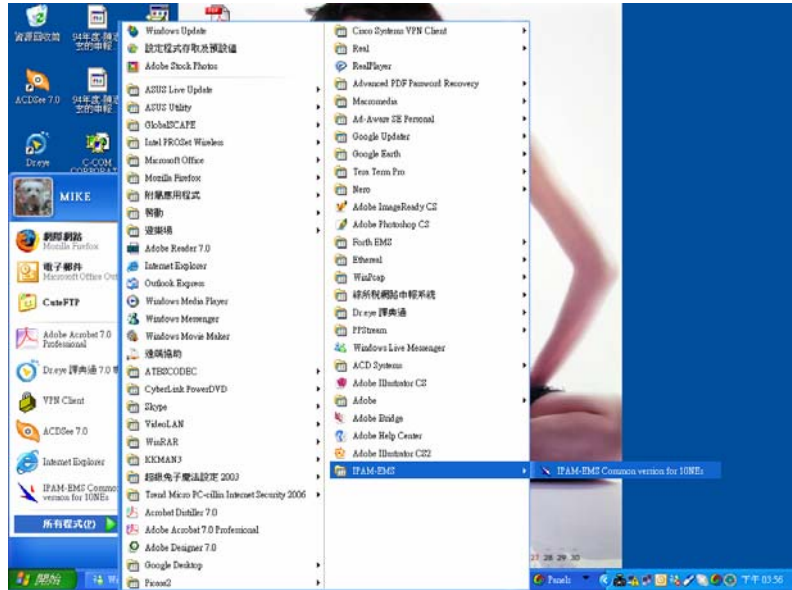
1.2.3

Starting the System

Users can activate the EMS either from Program manger or clicking the shortcut icon on the desktop. From Program Manager, choose the “EMS” program group in the Program Manager window. Then, choose the “EMS-SD1” program item to launch the program. The figure below is the initializing screen.

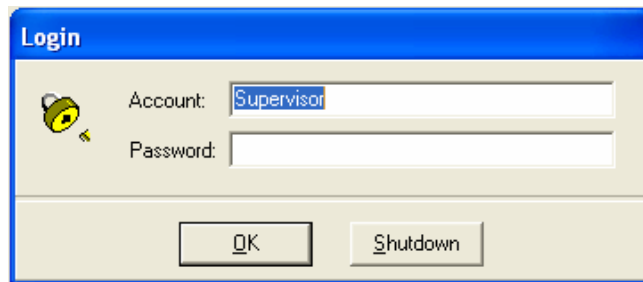


Note: before starting EMS, the SNMP command should be configured as “rw” via CLI so that read-write permissions are given to managers.



1.2.4 Logging into the System

1. Once the system is started, the **Login window** then prompts as follows.



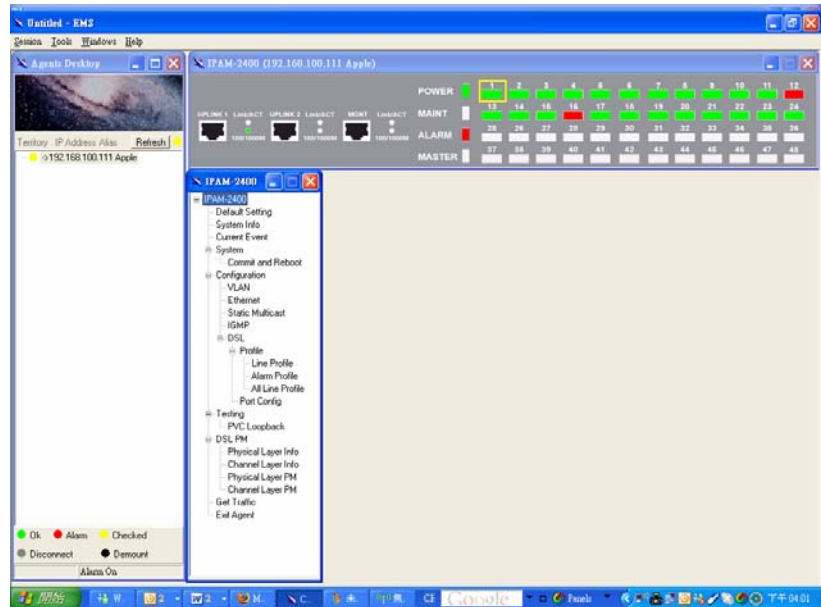
2. Simply enter your user account ID and password respectively, and then click on **OK** to login.

Table 1-1 login default setting

Default Account	Supervisor
Default Password	(blank)

Note: For the security concern, it is very important for you to change your password afterwards. To terminate the login, simply click on **Shutdown**.

3. After launching EMS and logging in with a valid username and password, the main window, EMS then prompts as shown in the following figure.



1.2.5 Terminating the System

To terminate the system at any time, simply choose the **Exit** command from Session Menu.

1.2.6 Logging out the Current Session

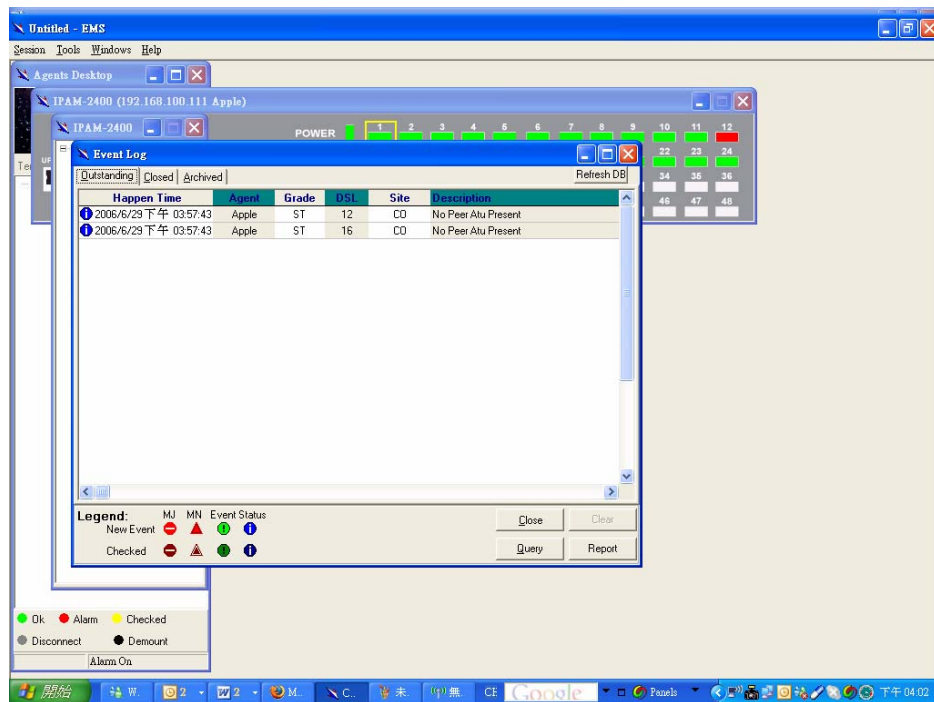
To terminate the current session, choose Logout command from Session Menu. The user account, then, is logged out and Login window prompts for a new login. Normally, this is used when a user wants to re-login in order to gain a higher level of authority for certain operations.

1.3 Windows Arrangement

Users may open many daughter windows in the EMS. To benefit user's viewing every Window, Commands of the Windows Menu is designed to arrange daughter windows. Those commands will be introduced separately.

1.3.1 Cascade

Choose Cascade from Windows menu in the EMS menu bar. The cascade command can cascade those opened windows as follows. User can select a window to perform operations or view status simply by clicking on a specified window.



1.3.2 Next Window

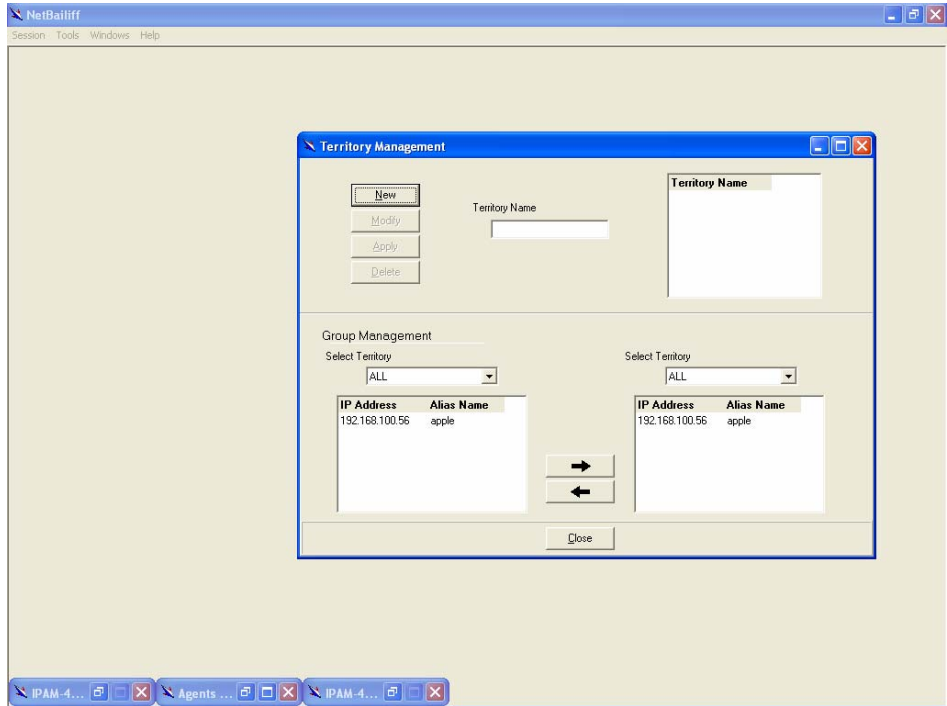
Next Window helps user to view next window so that it will bring the window in the second layer to front.

1.3.3 Previous Window

Previous Window command can help user to bring the previous window to front.

1.3.4 Arrange Icons

By selecting Arrange Icons of Windows Menu in the manu bar, it will locate those minimized daughter windows in the bottom left of EMS window as the following figure shown. User can select a required icon to perform EMS management.

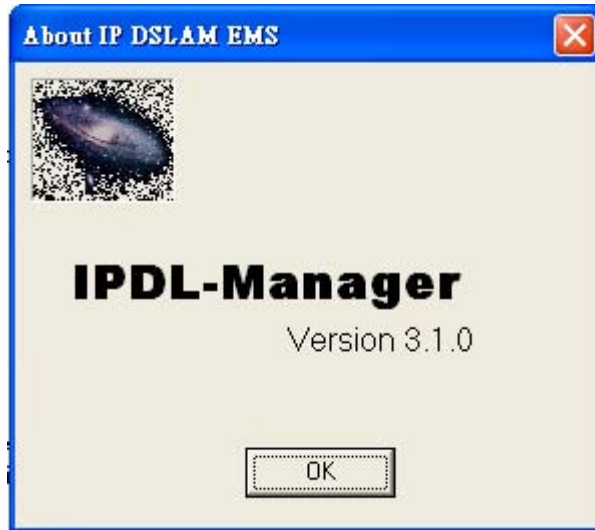


1.4

Help

To view the version of IP DSLAM EMS, choose **About** command via **Help** menu, as shown in the following figure.

Click on to exit the window.



1.5 Tools Menu Introduction



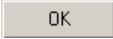
This section describes how to use tools in the EMS, including Environmental options, Territory manager, Agent manager, user managers and Telnet, which are detailed in the following sections.

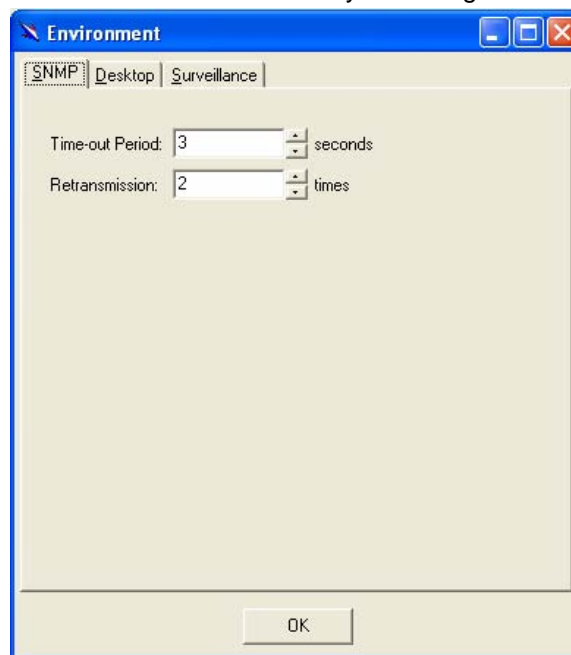
1.5.1 Environmental Options

Choose Environmental Options from Tools Menu, this Environment daughter window then appears. By this function, users can configure SNMP, Desktop and Surveillance respectively.

1.5.1.1 SNMP Configuration

The SNMP Time-out Period and Retransmission times can be configured as shown in the following steps:

1. Click on the TabControl (SNMP/Desktop/Surveillance) of SNMP that will bring SNMP dialogue box to front.
2. Click on  or  to change the Time-out Period seconds and Retransmission times.
3. Click on  to submit your changes.



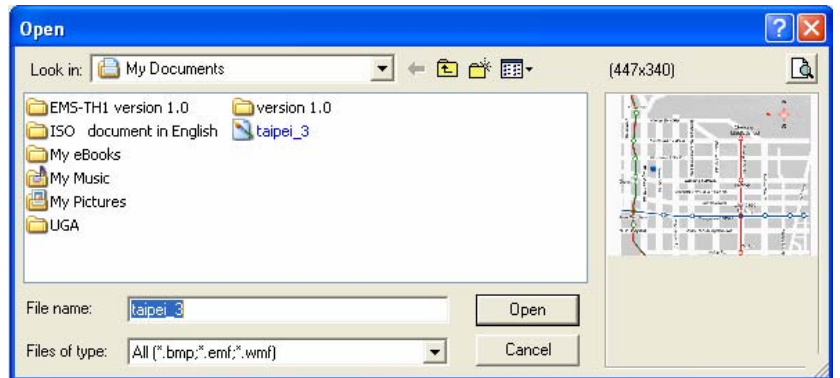
1.5.1.2 Desktop configuration

The desktop is user for setting the map of a required territory.

1. Click on the tab of Desktop that will bring Desktop dialogue box to front, as shown in the following figure.



2. Click on **Territory Manager** to quick start territory manager in which users can define a desired territory. Please refer to page 18 for more details.
3. Click on **Load** to load the map of a territory or click on **Clear** to clear a loaded map. Note: the format of map is limited to *.bmp, *.emf and *.wmf.

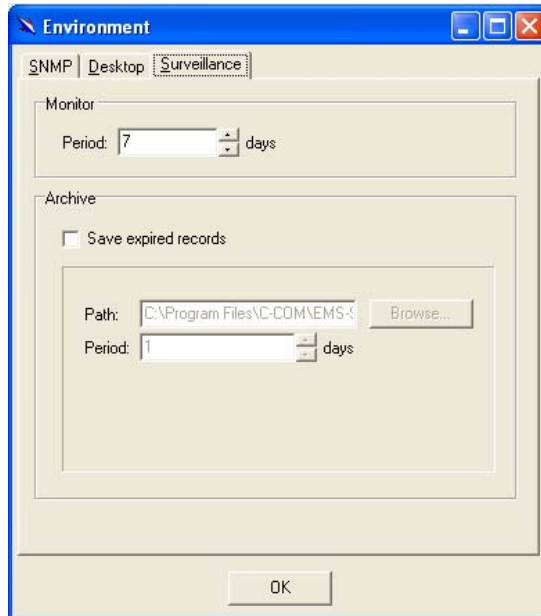




4. Click on **OK** to submit your setting, and then the map will apply to the Mounted Agent.

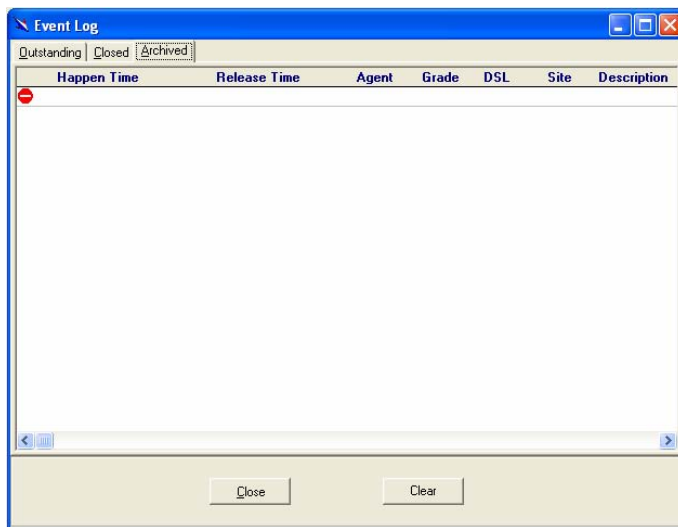
1.5.1.3




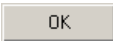
Surveillance configuration

1. Click on the tab of Surveillance that will bring the Surveillance dialogue box to front, as shown in the following figure.



2. Click on  or  to change the monitoring period.
3. Select the checkbox of Save expired records to save surveillance archive, which can be browsed by clicking on the tab of Achieved in the Event Log window as shown in the following figure:



- 4.
5. Clicking on  to choose the directory to record surveillance data and press  or  to define expired period.
6. Click on  to submit your settings.

1.5.2

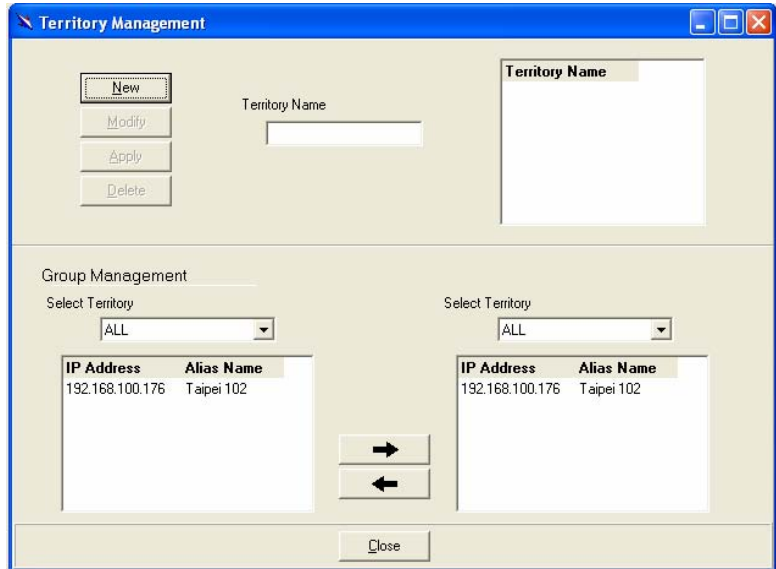
Territory manager configuration

Territory manager help users to build up monitoring territories and agents could be categorized into different territories by users. That benefits users to monitor the status of IP DSLAM systems by territory. Territory manager can be activated either from menu bar or from environmental options.


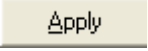
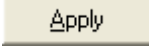
1.5.2.1

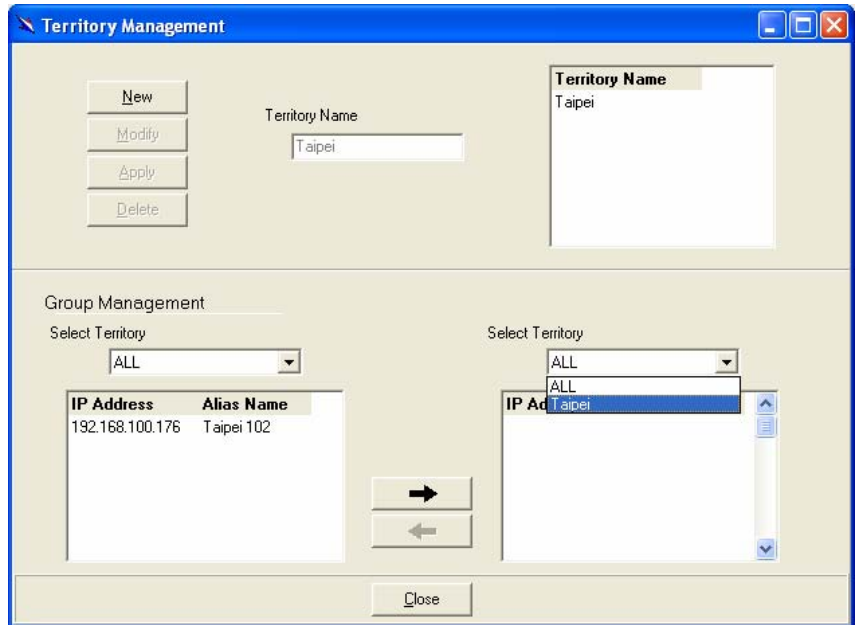
Territory Manager Window


Choose **Territory Manager** via Tools Menu, or Environmental option, and then the Territory Management window appears.

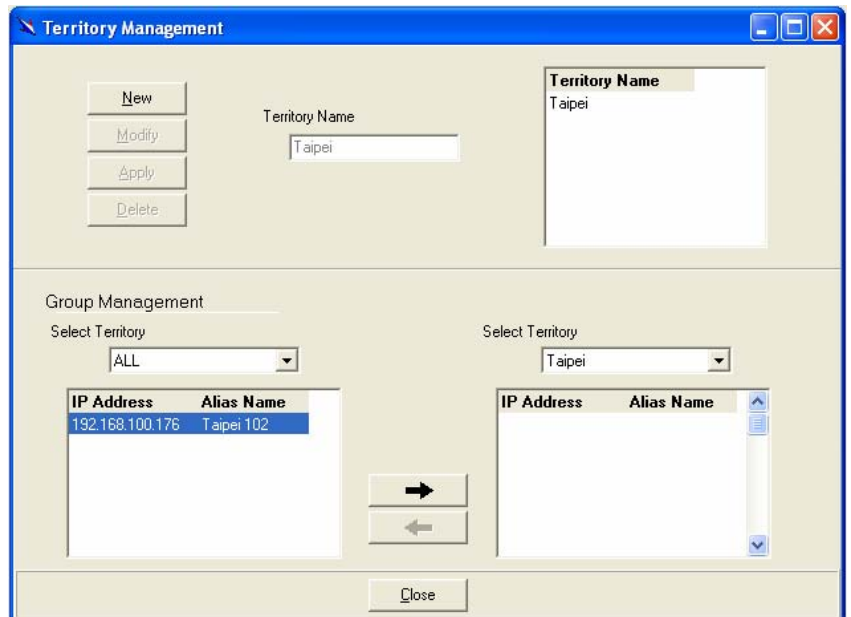


If to add a territory to the system,

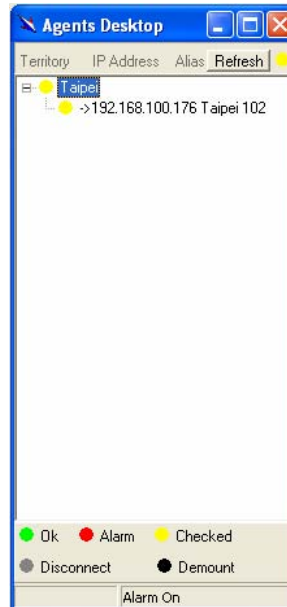
1. Click on , the Territory Name fields then cleared to blank for entering the data.
2. Enter Territory Name and  then become enable.
3. Click on  to apply the territory to the system. After that, you can proceed to group management by Territory Management dialog box.
4. As the following figure shown, the agent, 192.168.100.176 is available in the territory named ALL on the left. Users can shift the monitoring territory from ALL to Taipei simply by selecting Taipei in the Drop-down list on the right.

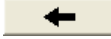
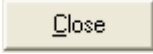


- Choose the agent, 192.168.100.176 on the left and then click on . The agent IP will appear on the right and will be monitored under the territory, Taipei.



- Correspondently, the Agent Desktop displays that Agent IP 192.168.100.176 has been monitored under the territory, Taipei.



7. If users want to move the agent IP from Taipei to other territory, select a desired agent IP and click on  to shift it to the left.
8. Click on  to exit the window or continue to perform other operations in the same window.

1.5.3

Agent Manager Configuration

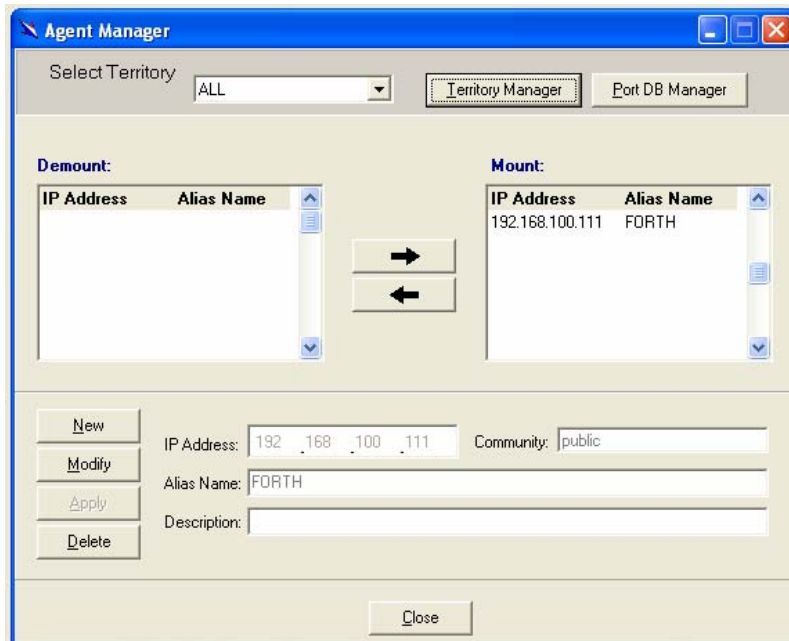
An **agent manager** is a software agent that runs on a managed node (example: a router) and provides an interface to manage it. It can perform operations on managed objects in the node and can also forward notifications to the manager (EMS).

All of the IP DSLAM agents that are to be managed by the EMS must be “registered” to the system. The “registration” process is to make the system aware of agent’s IP address and alias name. Once an agent is registered, it is put into the “demount” agent pool, which is still “inactive” for the network monitor. You then have to activate it if you want it to be monitored. An active agent can also be deactivated from the monitor for certain operational purpose when necessary. Agent Manager is designed for you to perform these operations.

1.5.3.1

Agent Manager Window

Choose Agent Manager from Tools Menu, this window will appear immediately.



As mentioned above, Agent Manager is used to define the IP DSLAM agent's IP address and community string that are to be used in the system, and to activate the system's monitoring of an agent; to deactivate an agent from the system's monitoring.

If to add an agent to the system,


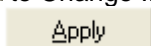
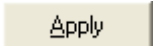
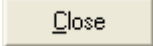
1. Select a territory that a new agent belongs to. Users can click on **Territory Manager** to activate territory manager.
2. Click on **New**, the data fields then cleared to blank for entering the data. Enter values in fields, IP Address, Alias Name and Description. The Apply buttons to the left of these fields then become enable.
3. Click on **Apply** to apply the agent to the system.
4. If to activate (so-called "Mount") the system's monitoring of an agent, click on the required agent entry in the Demount agent list, then click on **→**. The agent will appear on the Mount agent list on the right.
5. Click on **Close** to exit the window or continue to perform other operations in the same window.

If to remove an agent from the system,

1. Click the required agent in the Demount agent list, and then click on **Delete**. The agent will disappear.
2. Click on **Close** to exit the window or continue to perform other operations in the same window.


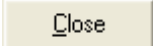
If to change the information of an agent,

1. Select the required agent in the **Demount agent list**. The information of the selected agent will then presented on the data fields.

2. Click on  to Change IP, Alias Name, and Description and then  becomes enable.
3. Click on  to apply the change to the system.
4. Click on  to exit the window.

Note: user can only change alias and description of the agent in the Mount agent list and changing IP is prohibited.

If to activate to monitor an agent,

1. Select the required agent in the Demount agent list, and then click on the Mount button . The agent will appear on the Mount agent list.
2. Click on  to exit the window or continue to perform other operations in the same window.

If to de-activate to monitor an agent,


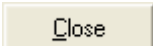
1. Select the required agent in the Mount agent list, and then click on the Demount button . The agent will then disappears from the Mount agent list and appears on the Demount agent list on the left.
2. Click on  to exit the window.


Table 1-2 Agent Management Field Definition

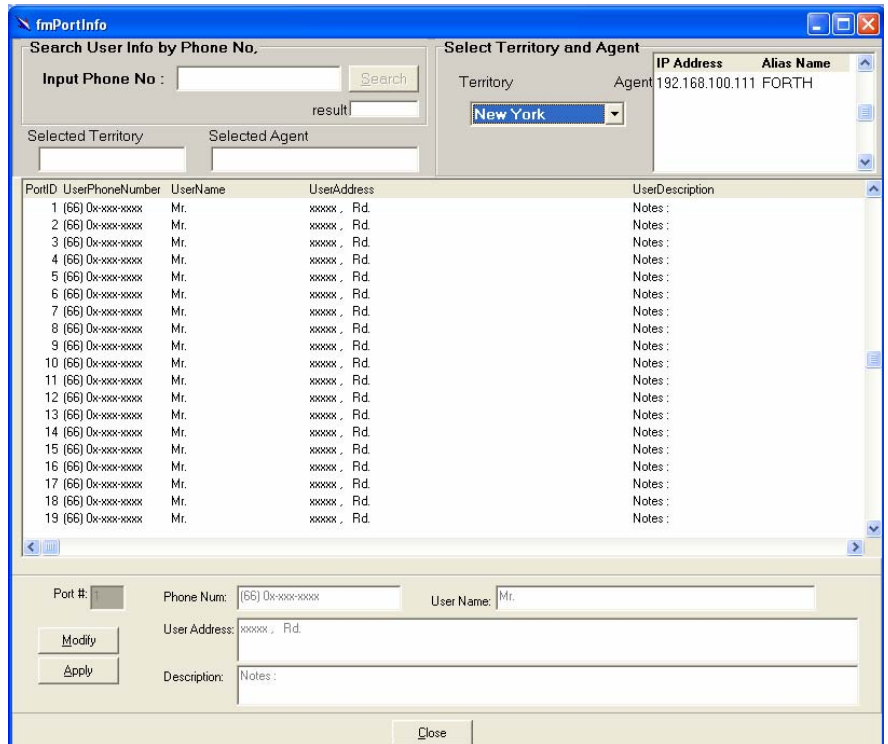
Field	Definition
IP Address	***.***.***.***
Alias name	Name of IP DSLAM
Description	Note

1.5.3.2

Port DB Manager

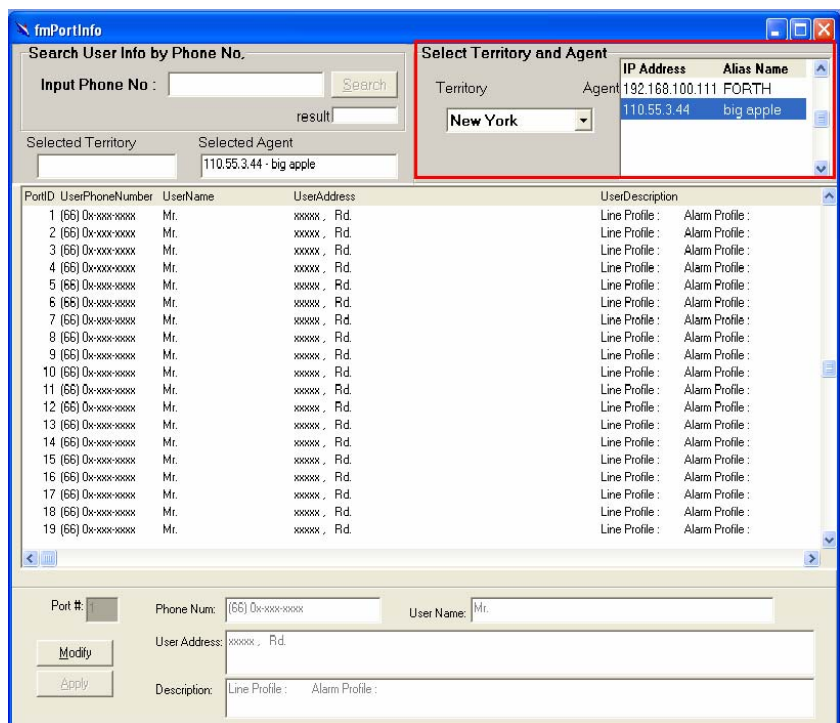
To meet user's requirements on browsing, searching and modifying subscribers' information, the Port DB manager is built-in the agent manager window.

Press  on the agent management window and then the Port DB manager window will prompt immediately, as show in the following figure.



If to browse the information of subscribers,

Users can select the required agent and territory, and the subscribers' information is displayed in real time.



If to modify subscriber information,

1. Select a subscriber to modify by pressing **Modify** to start modification.
2. Change related data of the subscriber.

3. Press to submit your setting.

If to search subscriber information,

1. Input the subscriber's phone number.
2. The will become enable and then press the button.
3. The port DB manager will show the result, found or not found.

PortID	UserPhoneNumber	UserName	UserAddress
1	11111	Mr.	xxxxx, Rd.

4. All of the subscriber's information, including territory and agent, are shown when the result is found.

1.5.3.3

Agent Desktop (Network Monitor)

Agent Desktop (see below) is the main window for the network administrators in performing their day-to-day network monitoring jobs. Like the standard desktop of MS Windows, Agent Desktop appears at all the time when the system is lunched. First appears on the Agent Desktop is the status of agents by an array of colors. By which you may monitor the status of agents, and judge if they are normal or in situations of alarms. You may then double click on the required agent IP to activate the event log window. Similarly, the Mounted Agents Desktop can be started up by double clicking on the icon of territory.

on the Agents Desktop, press to refresh the status of all agents.

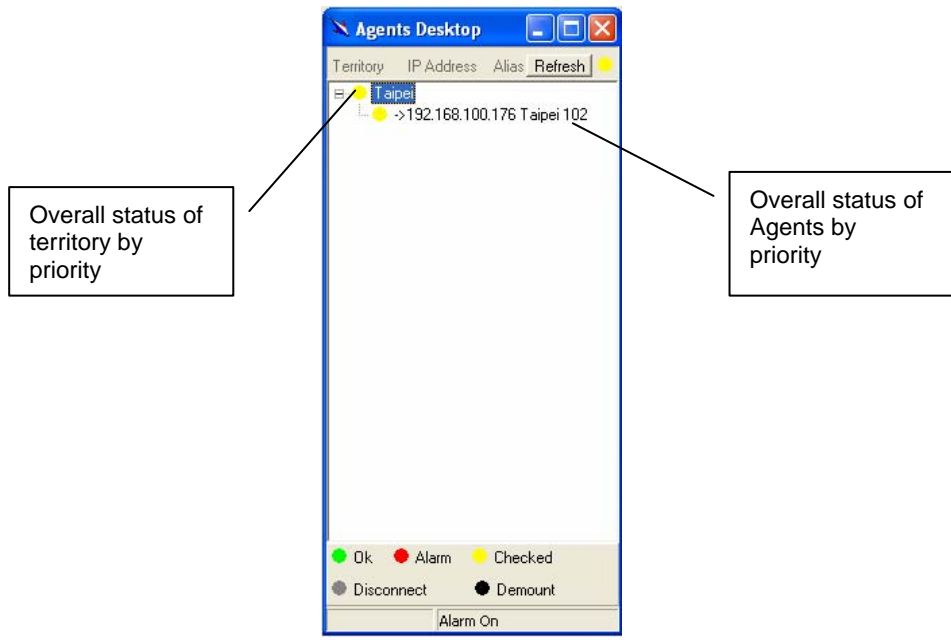


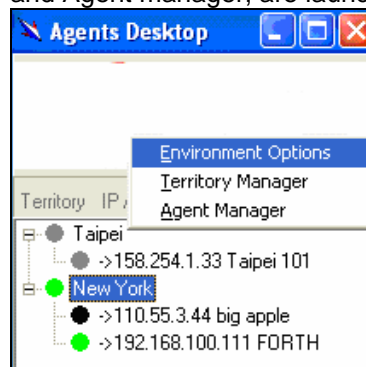
Table 1-3 Legends:

●	Gray icon indicates that the agent is disconnected.
●	Green icon indicates that the agent is in normal condition.
●	Red icon indicates that “Major Alarm” is occurred to the agent and requires network administrator’s attention. Network administrator pays attention to alarms by looking into the alarms using Event Log – Outstanding.
●	The red icon will turn into a yellow icon after the network administrator has looked into the alarms. However, this does not mean the situation is released. If any new alarm happens, yellow will turn red.
●	Black icon indicated that the agent is demounted.

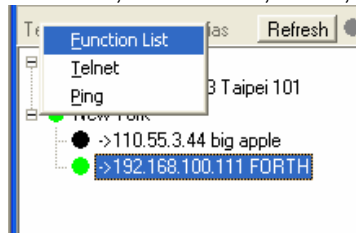
Note: the priority of colors: Gray>red>yellow>green>black

Moreover, related territory and agent functions can be activated from Agent desktop.

- Using right-click menu on a specified territory, environment options, those functions, territory manager, and Agent manager, are launchable.



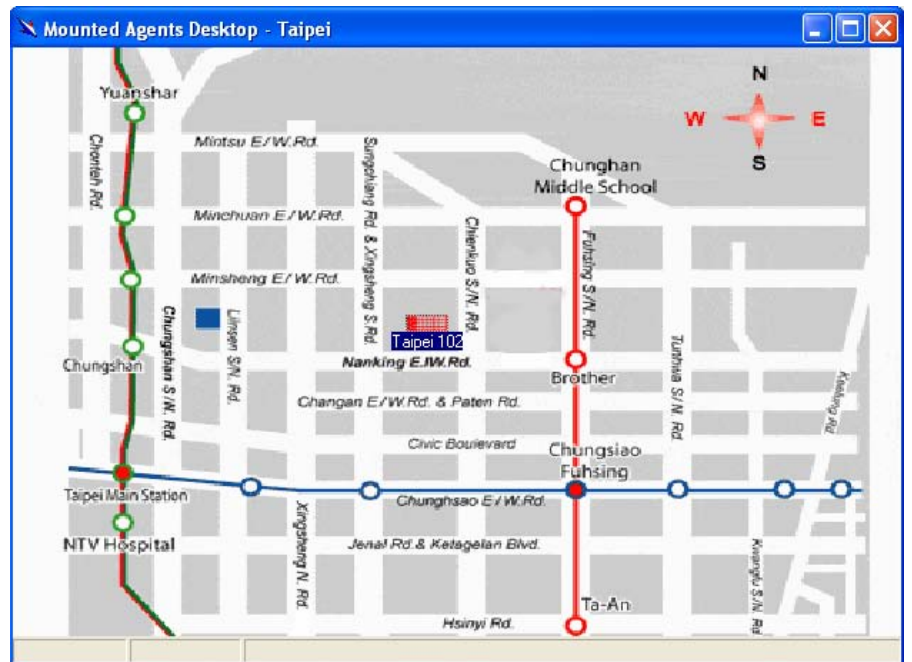
- Using right-click menu on a specified agent, those functions, function list, telnet, and ping, are launchable.



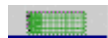
1.5.3.4

Mounted Agent Desktop

Mounted agent desktop's graphical presentation help users to monitor your network easily. Mounted agent desktop can be easily activated by double clicking specified territory icon on the agent desktop. The location of agents and overall network status on a specific territory is clearly displayed.



Legends:

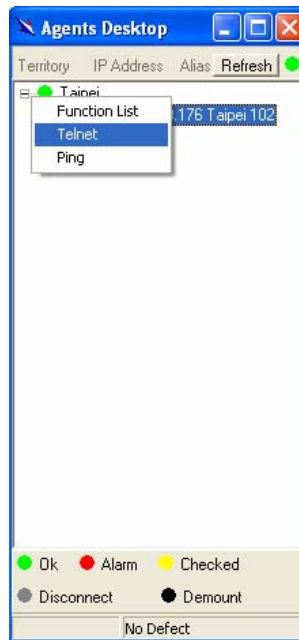


Taipei 102: This icon can be moved to where the agent is located in the map. In addition, its color also changes with the status of the agent. For example, the icon in red means that alarm is occurred to the agent and requires network administrator's attention.

1.5.4

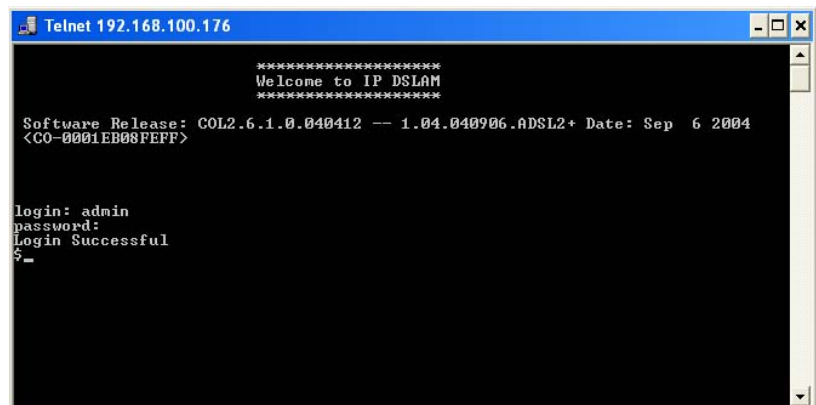
Telnet

Users can use the Telnet to connect to a specific IP DSLAM, and then monitor and interact with the system by CLI.



Launch Telnet procedure:

1. Select an agent IP on the Agent desktop.
2. Click on the right bottom of mouse and then select **Telnet** or choose **Telnet** from tool drop-down menu, and Then Telnet screen will come up immediately.



3. Enter user name and password to access the CID screen.

Note: The default login and password are admin.

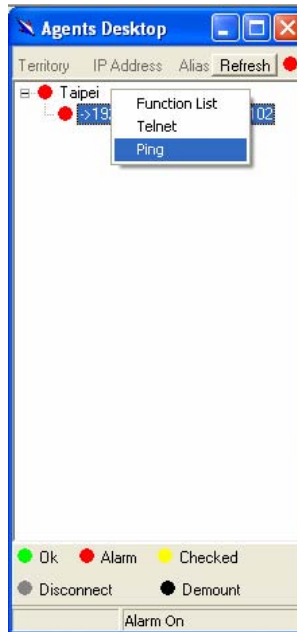
1.5.5

Ping

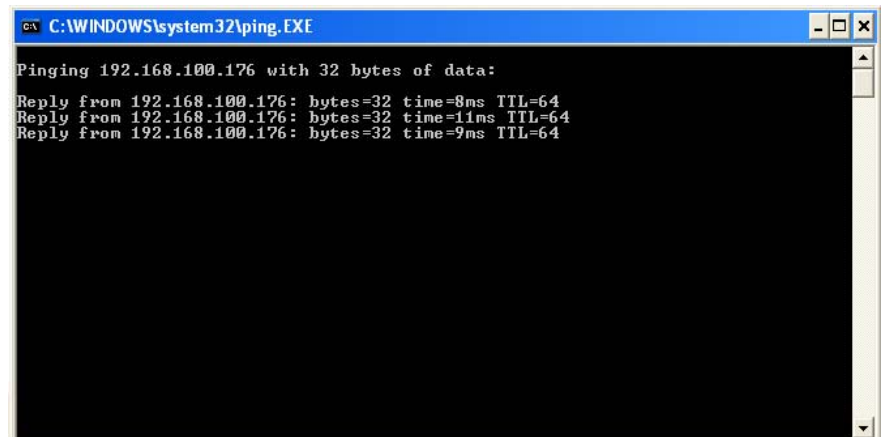
Ping is a command used to determine whether a particular IP DSLAM is currently connected to the agent. It works by sending a packet to the specific IP address and waiting for reply.

Executing Ping command procedure:

1. Select an agent IP on the Agent desktop.



2. Click on the right bottom of mouse and then select **Ping** or choose it from tool drop-down menu. Ping screen will come up immediately and then starts to send packets to check the connection with the IP DSLAM.



3. After showing the connection status, the screen will be closed automatically.

1.5.6

User Manager Window

The EMS uses user accounts, password as well as power level (system privileges) to control access and log in. There are three types of privileges, Supervisor, Constructor and Tester.

Supervisor: The highest level. User with this privilege can access ANY functions and data;

Constructor: User can set and modify the configuration of network equipments.

Tester: user can run maintenance test, such as loop back function.

To perform user manager, proceed as follows,

1. Choose User Manager from Tools Menu to access this window.

Using the **User Manager window**, you can add and remove users as well as change passwords, which are used to control the login.

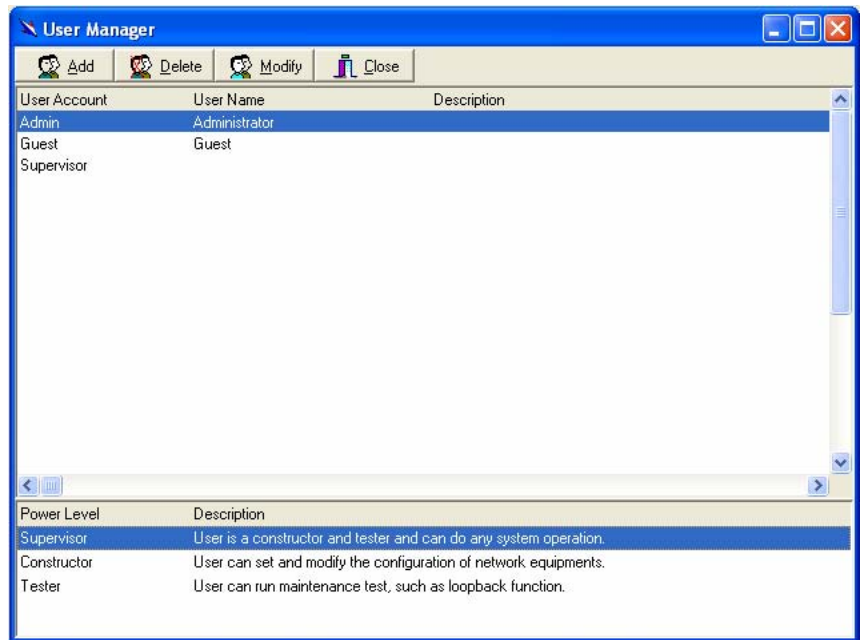

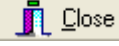


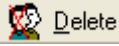
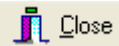
Table 1-4 User Manager Field Definition

Field	Definition
User Account	an ID to be used for login
User Name	The full name of a user
Description	Remarks for note purpose
Power Level	Privileges; Administrator and tester


If to add a user account to the system,

1. Click on  **Add**, the Security window then prompts.
2. Enter the account information as described in Security window below.
3. Click on  **Close** to exit the window or continue to perform other operations in the same window.

If to remove a User Account from the system,

1. Select a user account by clicking on the desired entry in User Account selection list. After selection, the designated one will be highlighted.
2. Click on  **Delete** to delete it.
3. Click on  **Close** to exit the window or continue to perform other operations in the same window.

If to change User Account Information,





1. Select a user account by clicking on the desired entry in User Account selection list. After selection, the designated one will be highlighted.
2. Click on  **Modify** button, the Security window then prompts.

3. Change the account information as described in Security window below.
4. Click on Close button to exit the window or continue to perform other operations in the same window. 2. Click on Add button, the Security window then prompts.

1.5.6.1

User Manager Window -- Security

This window is a daughter window of User Manager Window, and is used when adding a user account or changing account information.

1. Either  or  is selected, this window appears.
2. Enter data in the fields, User Account, User Name, Description, Password as required. Re-enter the password in field, Verify Password, for purpose of verification.
3. If to force the user to change their password at the next login, click on the checkbox to the left of the field, To Change Password When Login Next Time.
4. If to suspend a user account, click on the checkbox to the left of the field, Account Suspended.
5. If to assign a new Power Level to the user, click on the desired entry in the Demount list, then click on the Mount button, . The selected Power Level entry will then be added to the Mount list on the right.
6. If to remove a Power Level from the user, click on the desired entry in the Mount list on the right, then click on the Demount button, . The selected Power Level entry will then be removed.

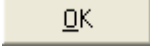
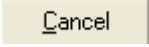
7. Click on  to complete the operation or  to abort the change. Either one is selected; the window is exited to User Manager Window.

Table 1-5 Register-Security Field Definition

Field	Definition
User Account	An ID to be used for login
User Name	The full name of a user
Description	Remark for note purpose
Password	Any character string, including blank
Verify Password	Re-enter the password as a confirmation
To change password when next login	If this is checked, the associated user needs to change their password at the next login.
Account Suspended	Suspend the account.
Power Level	Privileges; Administrator and tester

2

Manage the IP DSLAM

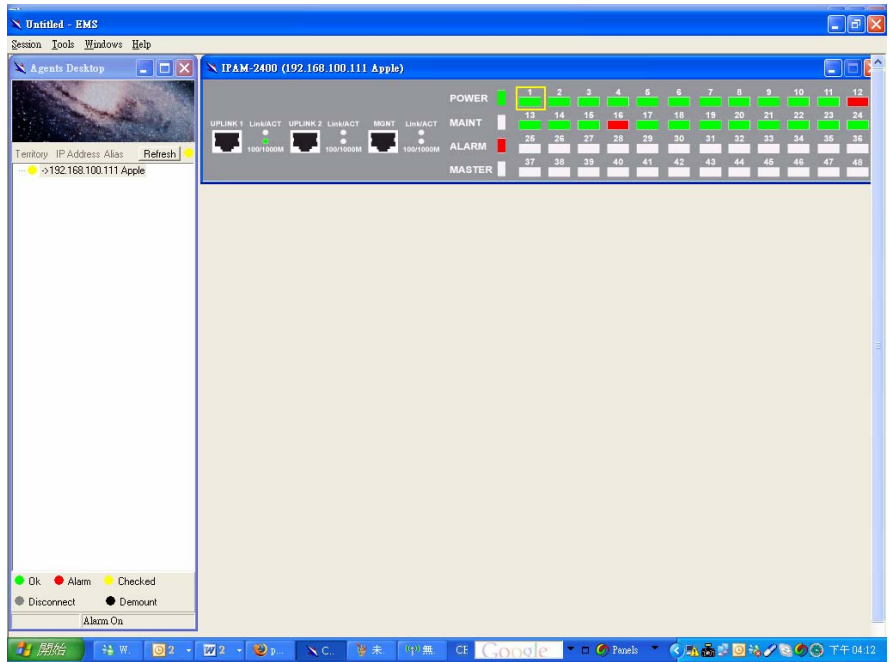
After successfully setting up the environment of EMS, you can manage different IP DSLAM via your EMS remotely. This chapter will tell you how to interact with a specified IP DSLAM.

2.1 Activate Function Management Windows

Via EMS, users can remotely monitor the current status of a specified IP DSLAM, and then proceed the configuration. To activate the function management windows, choose a specified agent that you want to manage, and then double click the agent, or click the right button of the mouse to select Function List, as shown in the following figure.

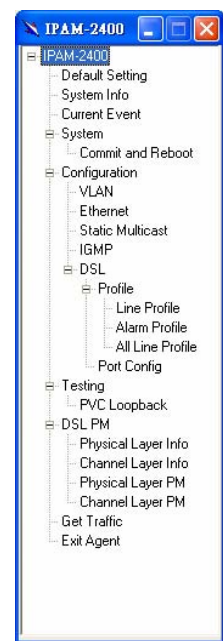


After that, the function management windows, including Function window and Front panel window, will prompt immediately as shown in the following figure.



2.1.1.1 Function Window:

Via the Function window, users can activate specified function immediately by double clicking on a specified function.



a

2.1.1.2 Front Panel Window

The Front Panel Window displays the current status of the IP DSLAM. Users can select a required DSL port to do further configuration or status monitoring.

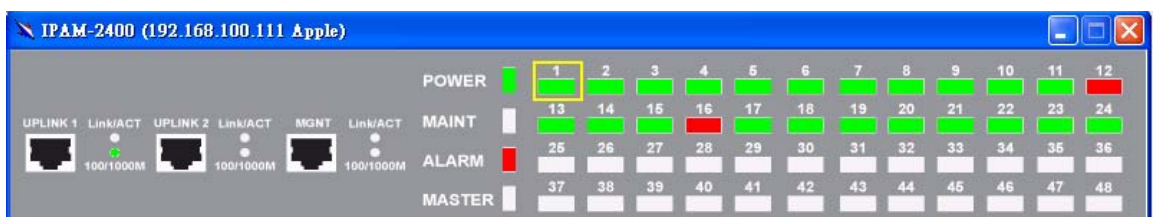


Table 2-1 is the LED description, by which users can check the IP DSLAM's status directly.

Table 2-1 LED Description

<LED ID>	Color	Description
POWER	Green	Lit when power on.
MAINT	Yellow	Lit when maintenance commands were issued.
ALARM	Red	Lit when MJ/MN events happen.
MASTER	Green	Lit when system was acted as management master for stacking application (future feature).
100/1000M	Green	data is transmitted through 100/1000Mbps Ethernet interface.
Link/ACT	Green	Giga uplink is activated.
ADSL1 – ADSL48	Green/ No Light Red	Lit Solid Green when ADSL link is in active state; LED off when ADSL link is not in service Lit Red when loss of signal occurs.

Moreover, move your cursor on a specified port, and then use right-click menu to execute the required function, reset, refresh, Admin Up and Admin down.

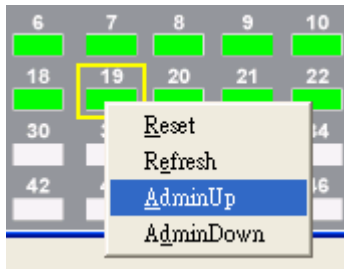


Table 2-2 Port right-click menu Description

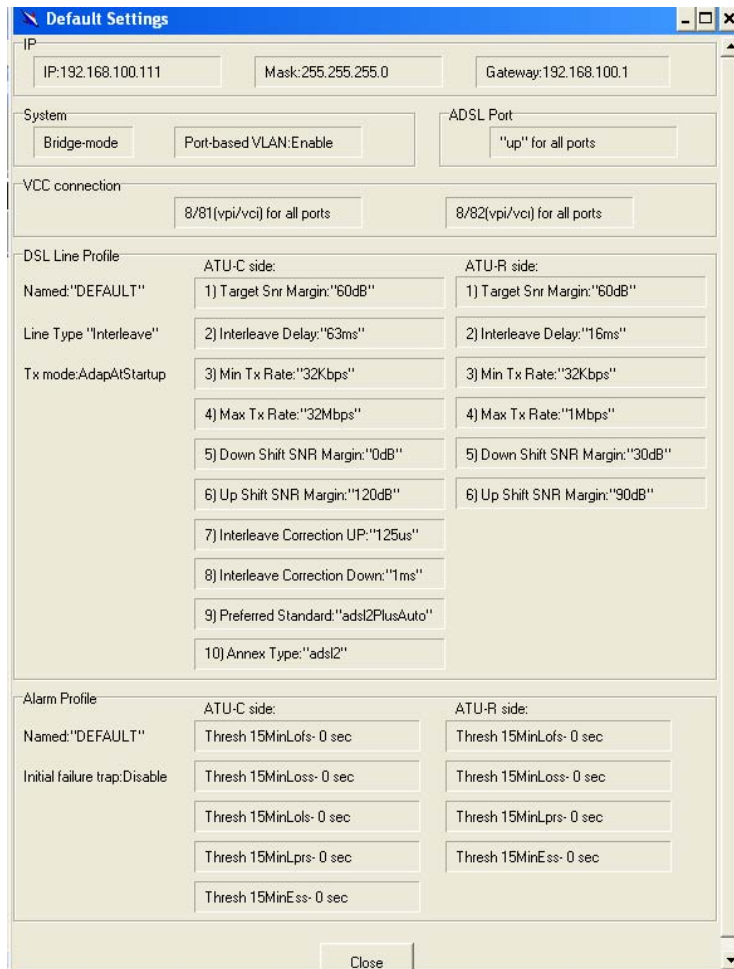
Name	description
Reset	Restart a specified port
Refresh	Refresh LED status
AdminUp	Set the port's admin status enable
AdminDown	Set the port's admin status disable

2.2 Default Setting

This section describes how to get the information of the default setting of the IP DSLAM.

1. Click on “**Default Setting**” from the Function window.

The Default Setting window appears as follows:



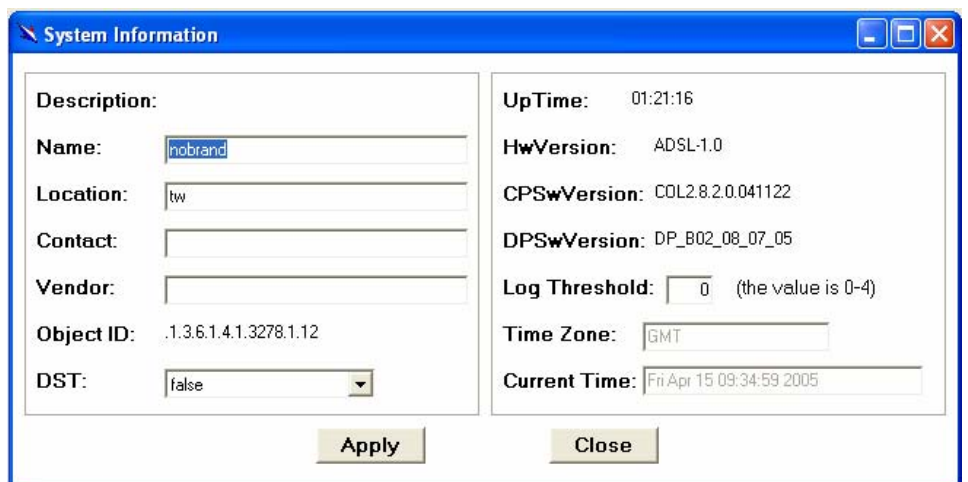
In the default setting window, the status of, IP, System, VCC connection, DSL line profile and Alarm profile are displayed clearly. How to modify them will be introduced in the following sections.

2.3 System Information

This section describes how to get and input the information of the IP DSLAM.

1. Double Click on "System Information" from the Function window.

The **System Information** window appears as follows:



Input necessary information on those fields.

Table 2-3 Sysinfo field definition

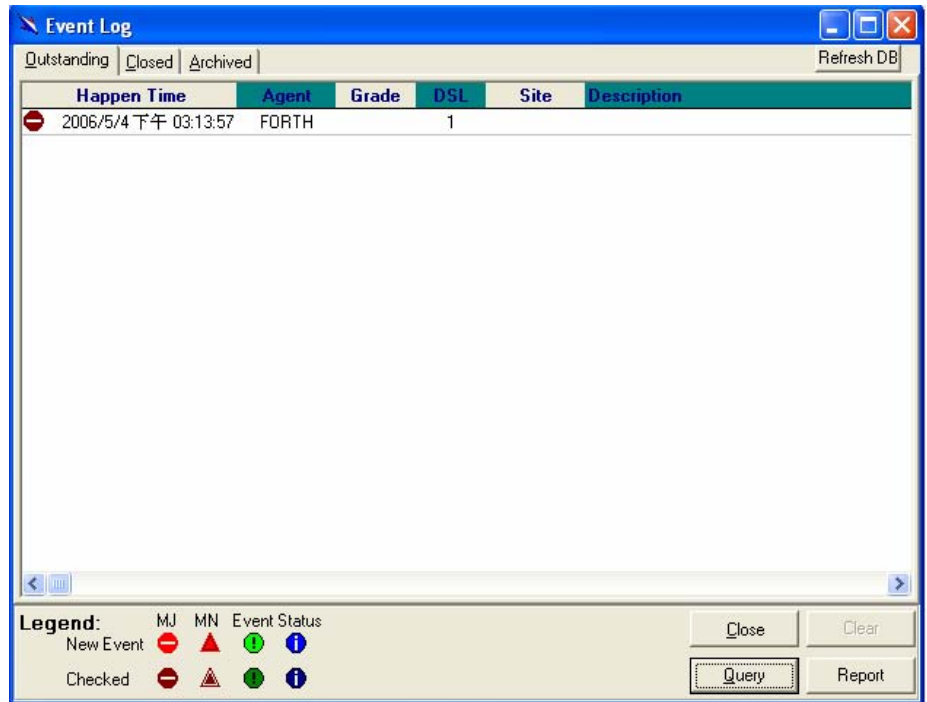
Field	Definition
Name	Alias name of the IP DSLAM
Location	Location of the IP DSLAM
Contact	The contact person of the IP DSLAM
Vendor	The vendor of the IP DSLAM
Object ID	Vendor ID
DST	This specifies if the Daylight Savings Time has been enabled or not. True: on False: off
UpTime	System up time
HwVersion	Hardware version of the IP DSLAM.
CPSwVersion	Control plant version
Log Threshold	This specifies the severity level of the trap equal to or lowers than that shall be logged. 0 represents log threshold is disable. 1 is the lowest and represents critical traps. Valid values: 0-4
Time Zone	Time zone Valid values: Given below, are the valid values, followed by their descriptions. IDLW - International Date Line West NT - Nome HST - Hawaii Standard CAT - Central Alaska AHST- Alaska-Hawaii Standard YST - Yukon Standard PST- US Pacific Standard MST- US Mountain Standard CST- US Central Standard EST- US Eastern Standard AST- Atlantic Standard NFST- Newfoundland Standard NFT- Newfoundland BRST-Brazil Standard AT- Azores WAT - West Africa GMT - Greenwich Mean UTC - Universal (Coordinated) WET - Western European CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter EET - Eastern Europe, Russia Zone 1 IST - Israeli Standard BT - Baghdad, Russia Zone 2 IT - Iran ZP4 - "Russia Zone 3" ZP5 - "Russia Zone 4" INST - "Indian Standard" ZP6 - "Russia Zone 5" NST - "North Sumatra" WAST - West Australian Standard SSMT - South Sumatra, Russia Zone 6

	JT- Java CCT - China Coast, Russia Zone 7 ROK - Korean Standard KST - Korean Standard JST - Japan Standard, Russia Zone 8 CAST - Central Australian Standard EAST - Eastern Australian Standard GST - Guam Standard, Russia Zone 9 IDLE - International Date Line East NZST - New Zealand Standard NZT - New Zealand Example: IDLW , that stands for International Date Line West
Current Time	This indicates the current time.

2. Click on **Apply** to submit your settings or **Close** to close the window.

2.4 Current Event

EMS receives the event trap from the IP DSLAMs and also polls the IP DSLAMs periodically to monitor the current status of Current Event window can be activated from Function window.



On the event log window, administrator can switch different tabs to check the system's status:

1. **Outstanding:** Allow you to view the outstanding events or status and system information.
2. **Closed:** Allow you to trace events or status that are already closed and are still within the surveillance period.
3. **Archived:** Allow you to browse the expired records.

EMS also divided the events into 4 levels (major/minor/event/status change), and displayed different colors in the event log.

Table 2-4 Legends


Icons	The grade of alarm indicated	Abbreviation	The Icon has been checked.
	Major Alarm	MJ	
	Minor Alarm	MN	
	Event		
	Status		

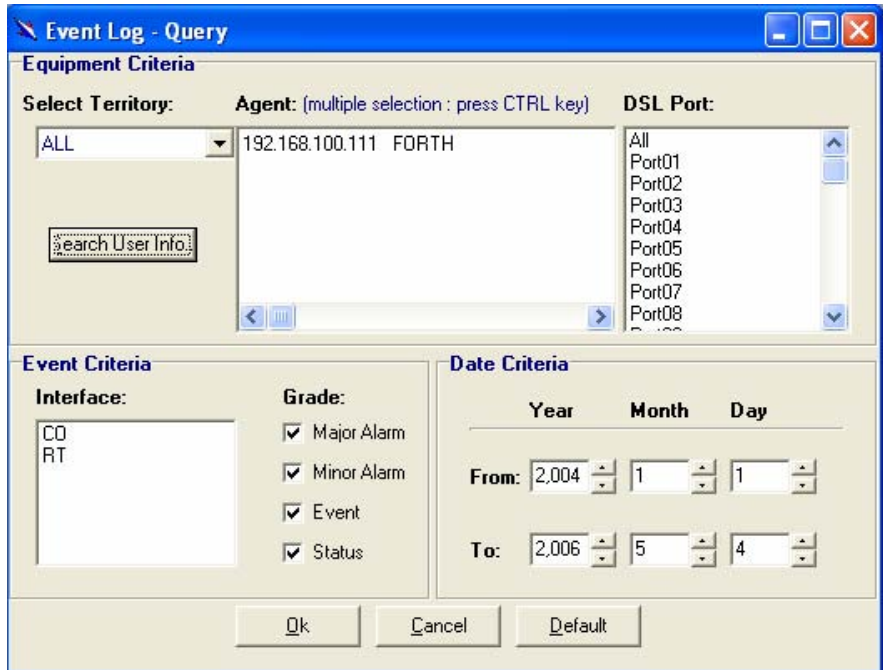
Besides, the EMS was powered with query function so that the administrator can set criteria to see the filtered events.

Finally, administrator can run report on different event log.

2.4.1

Query

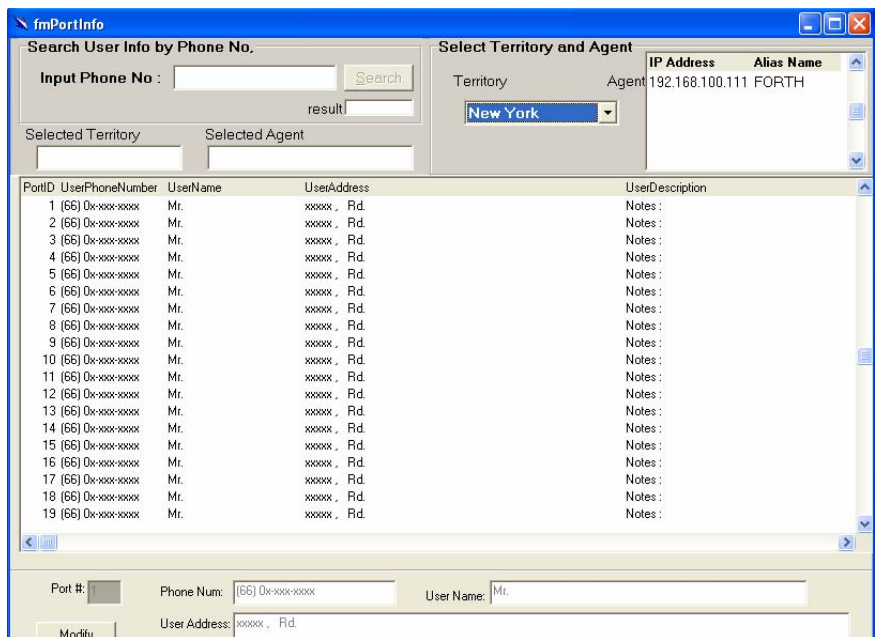
The query function can be activated by pressing  and the query window is displayed as follow.



As shown in above figure, users can set different criteria, including equipment, event and date criteria to filter events.

After setting the criteria, users can choose **Ok** to run query, **Cancel** to exit or **Default** to return to default values.

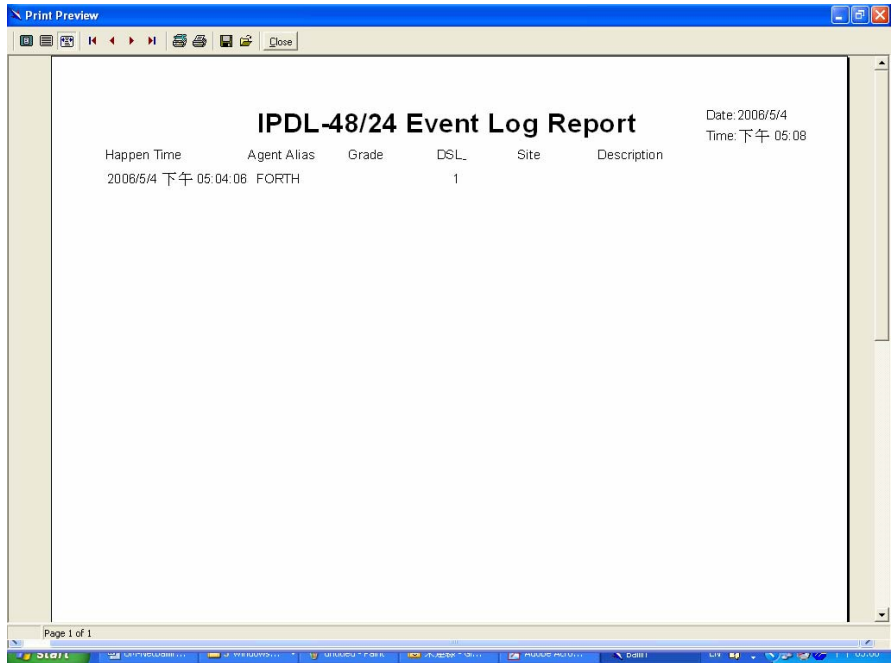
In addition, users can press **Search User Info.** to search user information.



2.4.2

Report

Users can run report on outstanding, closed or archived events. Press **Report** to generate a report.



The report can (1) print (2) save (3) load from disk.

Note: different with outstanding event report, system adds close time field on closed and archived event report.

2.4.3 Refresh

To get the latest data from database, users can press the **Refresh DB**.

2.4.4 Outstanding Event

This tab allows you to view the outstanding events of specific agents.

If to view the event log of a specific agent,

1. Click "**Current Event**" from Function window. The Event Log window appears as follow:

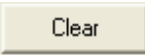
Table 2-5 Outstanding Event Window Field Definitions

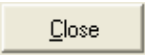
Field	Description
Happen time	The date/time when the event is occurred.
Agent	The IP address of the agent associated
Grade	Severity level of event or status.
DSL	DSL Port
Site	Down stream or upstream
Description	The description of the event or status.

2.4.5 Closed Event

This window allows you to browse the closed alarms and events of specified agents.

1. Click on the tab of **Closed** that will bring the **Closed** screen to front, as the following figure shown:

2. Click on  to clear all records.

3. Click on  to exit the window.

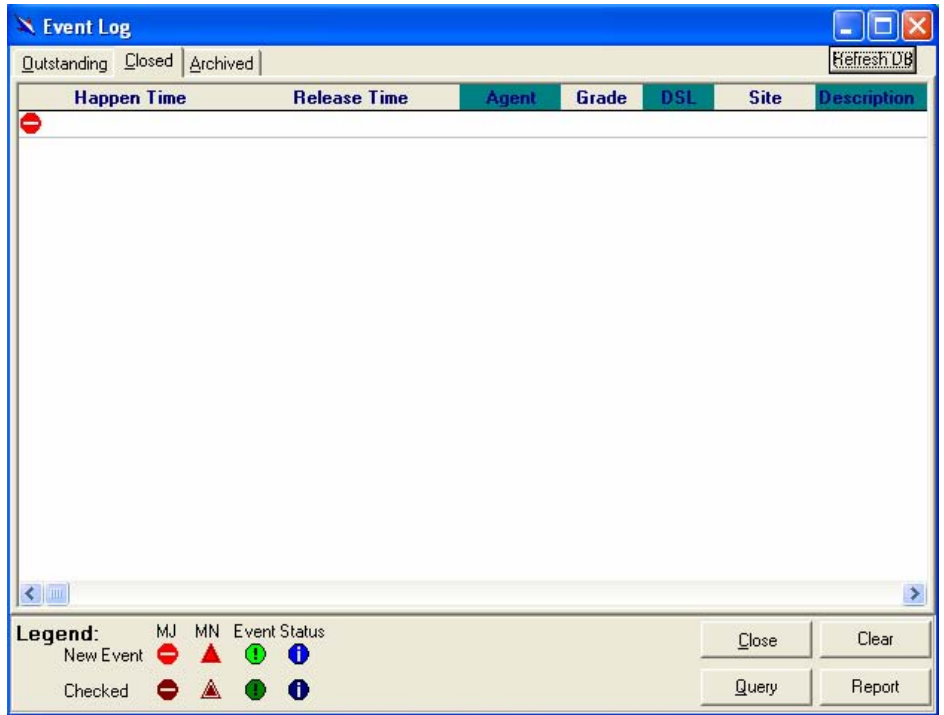


Table 2-6 Closed Event Window Field Definition

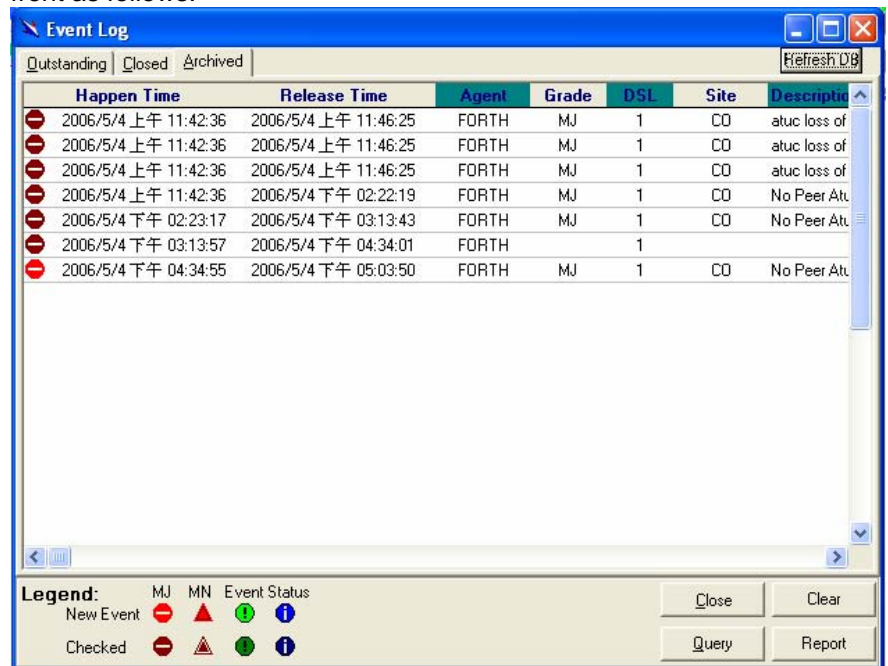
Field	Description
Release Time	The date/time when the event is closed.
Others	Rest of the fields is as same as described in "Outstanding Events".

2.4.6

Archived

This window allows you to browse the expired records, which can be configured in the Environment window.

1. Click on the tab of **Archived** that will bring the **Archived** screen to front as follows:



2. Click on to clear all records.
3. Click on to exit the window.

2.5

System

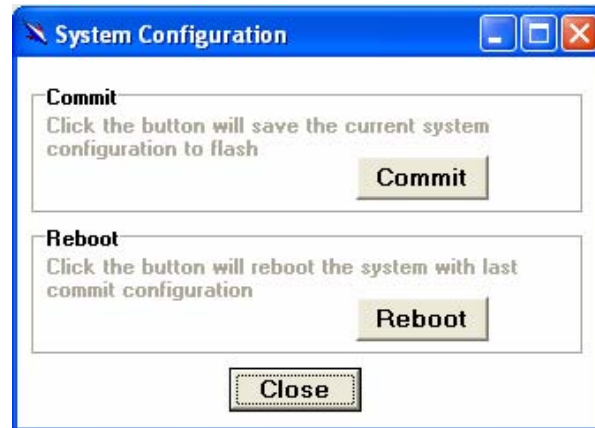
2.5.1

Commit and Reboot

This section describes how to save the current configuration to flash or reboot the IP DSLAM.

1. Double Click on “Commit and Reboot” from the Function window.

The System Information screen appears as follows:



2. If to commit the active configuration to the flash, click on **Commit**.
3. If to reboot the system and to set the boot configuration, click on **Reboot**.
4. Click on **Close** to close the System Configuration window.

2.6 Configuration

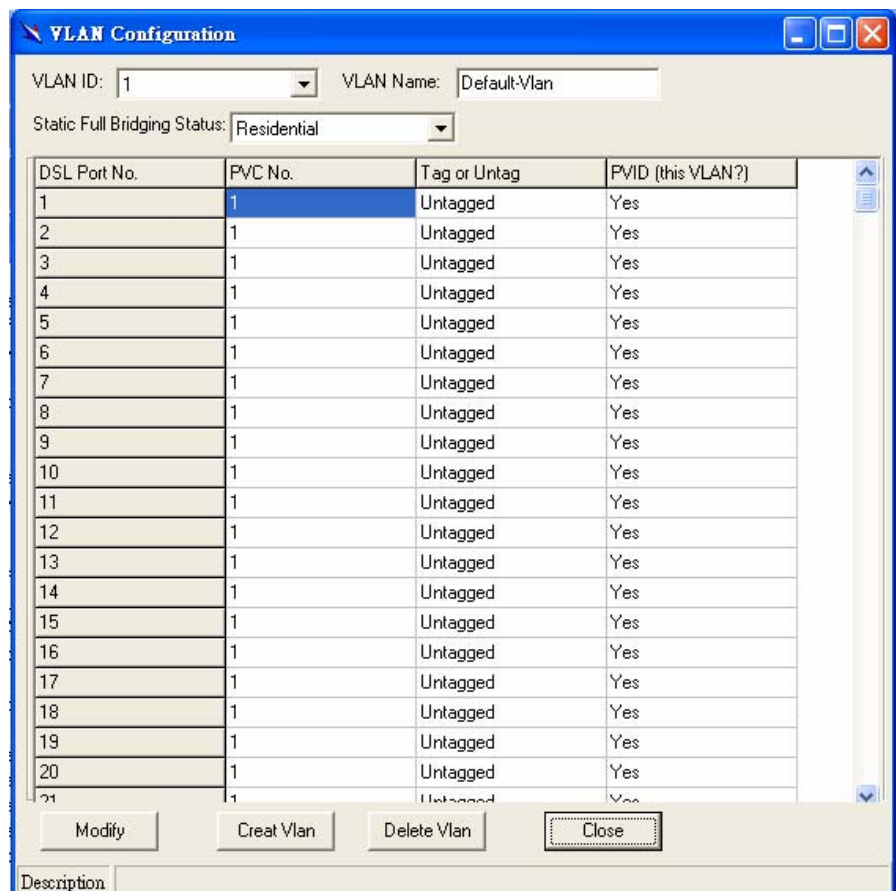
This section describes how to configure the IP DSLAM by selecting **Configuration** from Function window. This section will cover those functions:

2.6.1 VLAN Configuration

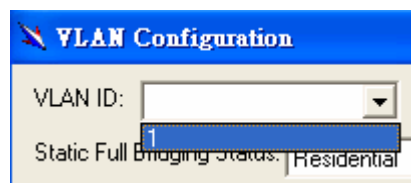
Allow user to view, create and modify VLAN configuration. To configure VLAN, proceed as follows:

2.6.1.1 View the VLAN

1. Double Click on “VLAN configuration” from the Function window. The VLAN configuration window appears as follow:

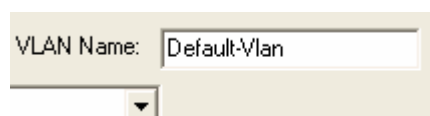


2. Select the required VLAN by using the VLAN ID drop-down list.



2.6.1.2 Modify the VLAN

1. Change the VLAN's name in the VLAN Name field.



2. Set the static full bridge status as restricted, unrestricted or residential.

Static Full Bridging Status:	Residential
DSL Port No.	1
	Restricted Unrestricted Residential

- Set the port's PVC no. from disable to 8.



DSL Port No.	PVC No.
1	1
2	Disable
3	1
4	3
5	4
6	5
7	6
	7

- Set the port tagged or untagged.

DSL Port No.	PVC No.	Tag or Untag
1	1	Untagged
2	1	Tagged
3	1	Untagged


- Set the Port's PVID.

DSL Port No.	PVC No.	Tag or Untag	PVID (this VLAN?)
1	1	Untagged	1
2	1	Untagged	No(PVID=100)
3	1	Untagged	Yes
4	1	Untagged	
5	1	Untagged	1

- Click on  to submit your settings or click on  to close the VLAN Configuration window.

2.6.1.3

Create a VLAN

- Click  to activate a new VLAN configuration window where new VLAN's values are configurable.

VLAN Configuration

VLAN ID: 100 VLAN Name:

Static Full Bridging Status:

DSL Port No.	PVC No.	Tag or Untag	PVID (this VLAN?)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			

Return Create Vlan Apply Close

Description: Select Tagged to tag this VLAN ID when it send out the packet vis this port

- Input VLAN ID, VLAN name, PVC No., Tag or Untag and PVID on each port respectively.
- click **Apply** to submit your setting and press
- Click **Return** to return to previous configuration window.

VLAN Configuration

VLAN ID: 400 VLAN Name: ffg

Static Full Bridging Status: Restricted

DSL Port No.	PVC No.	Tag or Untag	PVID (this VLAN?)
1	1	Tagged	No(PVID=300)
2	1	Untagged	No(PVID=100)
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			

Modify Create Vlan Delete Vlan Close

Description

Table 2-7 VLAN Configuration Field Definitions

Field	Definition
-------	------------

VLAN ID	The VLAN id for this VLAN. In devices supporting "Shared Vlan for multicast" capability, the information for a multicast mac addr is shared across vlans hence vlan id is an optional parameter. In devices supporting "Independent Vlan for multicast" capability each vlan can have its own information for a multicast mac addr hence vlandid is a mandatory parameter in all the commands other than - get. For No Vlan case vlan id is not required.
VLAN Name	Name of the VLAN
static full bridge status	This specifies the state of full bridging for the VLAN. There can be three values associated with this, based on global fullBridgingStatus. These values can be restricted bridging, unrestricted full bridging and residential bridging. If the user does not specify the bridging mode at the time of VLAN creation the VLAN inherits the globally set bridging mode. The user can modify bridging mode for a created VLAN. If the dynamic entry for the VLAN to be created already exists, the user can only specify globally set bridging mode for this VLAN. The bridging modes are defined as Restricted, Unrestricted, and Residential. The default residential VLAN, like any other residential VLAN allows only one net side bridge port as its member. This port shall be added automatically to the default VLAN if it is the only net side bridge port being added to the VLAN. Subsequently, the user can add another net side port to the egressportslist and untaggedportslist only after removing the previously added net side bridge port. Unrestricted bridging is not applicable for bridge ports created over the PPPoE interface even though the VLAN may be unrestricted. Default value: residential
PVC No.	The set of ports, which are permanently assigned to the egress list for this VLAN by management.
Tag or Untag	The set of ports, which are transmitting traffic for this VLAN, as either tagged or untagged frames.
PVID	Port VID

2.6.2

Ethernet Configuration

Allow user to view and modify **Ethernet** configuration. To view or configure Ethernet, proceed as follows:

1. Double Click on "**Ethernet configuration**" from the Function window. The Ethernet Configuration window appears.

2. Ethernet configuration window displays Ethernet and Gateway setting in the mean time.
3. To view the Ethernet Configuration of UPLINK1, UPLINK2, or UPLINK3 by using the Ethernet drop-down list.

2.6.2.1

Modify Ethernet

1. If to modify the Ethernet Configuration, select which Ethernet uplink first and then press **Modify** to execute your configuration.

The screenshot shows the 'Ethernet Configuration' window. At the top, there is a 'Select Ethernet' dropdown menu with 'UPLINK1' selected. Below this are several configuration options, each with radio buttons for 'Enabled' and 'Disabled':

- DHCP: Enabled (selected)
- Type: Uplink (selected)
- Admin Status: Enabled (selected)
- Operation Status: Enabled (selected)

On the right side, there are input fields for:

- IP Address: 192 . 168 . 100 . 111
- Mask: 255 . 255 . 255 . 0
- Mgmt Vlan Index: 0

Below these settings are five buttons: **Modify**, **Apply**, **Create**, **Delete**, and **Close**.

The 'Gateway Setting' section contains three input fields for Destination, Network Mask, and Gateway, all currently empty.

The 'Routing Table' section features a table with the following data:

Destination	Mask	Gateway
192.168.100.0	255.255.255.0	192.168.100.111

Below the routing table are 'Add' and 'Delete' buttons. At the bottom of the window, there is a 'Description' field.

2. The figure below shows Admin Status, IP address, mask and Mgmt VLAN index are configurable.

Ethernet Configuration

Select Ethernet: UPLINK1

DHCP: Enabled Disabled IP Address: 192.168.100.111

Type: Uplink Downlink Mask: 255.255.255.0

Admin Status: Enabled Disabled Mgmt Vlan Index: 0

Operation Status: Enabled Disabled

Modify Apply Create Delete Close

Gateway Setting

Destination	Network Mask	Gateway

Routing Table

Destination	Mask	Gateway
192.168.100.0	255.255.255.0	192.168.100.111

Add Delete

Description

- Submit your setting by pressing **Apply** and exit by pressing **Close**.

2.6.2.2

Create Ethernet

- If to create a new uplink or management interfaces, click on **Create** and then select a new Ethernet configuration from Select Ethernet drop-down menu. After that, users can set related parameters.

Ethernet Configuration

Select Ethernet: UPLINK2

DHCP: Enabled Disabled IP Address: . . .

Type: Uplink Downlink Mask: . . .

Admin Status: Enabled Disabled Gateway: . . .

Operation Status: Enabled Disabled Mgmt Vlan Index: . . .

Modify Apply Create Delete Close

- Click on **Apply** to submit your settings or click on **Close** to close the Ethernet Configuration window.
- Once you create a new Ethernet interface, the system will generate a routing IP on the routing table automatically.

Gateway Setting

Destination	Network Mask	Gateway
<input type="text"/>	<input type="text"/>	<input type="text"/>

Routing Table

Destination	Mask	Gateway
192.168.100.0	255.255.255.0	192.168.100.111

4. Press to delete a routing IP.

2.6.2.3

Delete a Ethernet

1. Choose an Ethernet interface and press .
2. Then delete success message prompts.

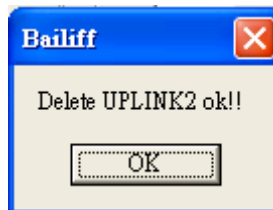


Table2-8 Ethernet Configuration Field Definitions

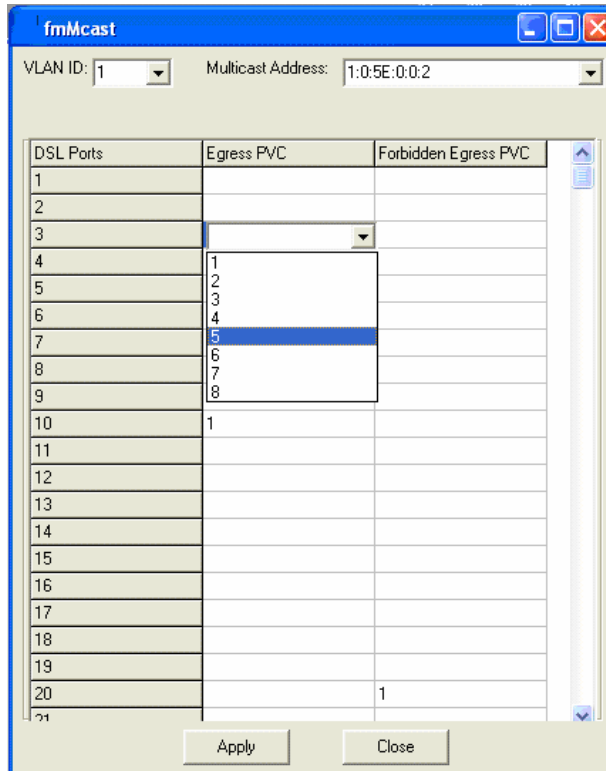
Field	Definition
DHCP	DHCP client enabled or disabled
Type	Upstream or downstream
Admin Status	The desired state of UPLINK (enable/disable)
Operation Status	System is enabled or not.
IP address	IP address of the UPLINK
Mask	This specifies the network mask configured for the UPLINK.
Gateway	Gateway IP
Mgmt Vlan Index	VLAN for management traffic on this interface. Nonzero value of this field is valid only if either 'ip' field is non-zero or 'usedhcp' field is true. If no Management Vlanid is specified (in the create operation) or its value is set to zero (either in create or modify operation) then the system shall use the value of 'portvlanid' associated with the bridge port created on this interface as the Management Vlan Index. In case the management vlan (i.e. 'mgmtvlanid' or the associated 'portvlanid', if 'mgmtvlanid' is zero) doesn't exist on the system then management shall not happen on this interface till the corresponding VLAN is created with the Net side port as its member.

2.6.3

Static Multicast Configuration

Allow user to view and modify Static Multicast configuration. To view or modify Static Multicast configuration, proceed as follows:

1. Double Click on “**Ethernet configuration**” from the Function window. The Static Multicast Configuration window appears.





2. Select the VLAN ID to view or modify by using the VLAN ID drop-down list.
3. Use Egress PVC and Forbidden Egress PVC drop-down list to set the specified DSL port's Egress PVC and Forbidden Egress PVC.
4. Click on  to submit your settings or click on  to close the VLAN Configuration window.

Table 2-9 VLAN Configuration Field Definitions

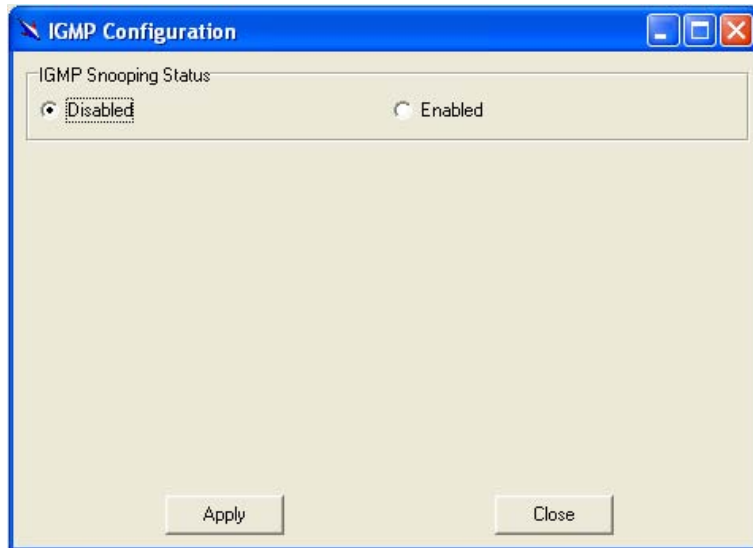
Field	Definition
VLAN ID	The VLAN id for this VLAN. In devices supporting "Shared Vlan for multicast" capability, the information for a multicast mac addr is shared across vlans hence vlan id is an optional parameter. In devices supporting "Independent Vlan for multicast" capability each vlan can have its own information for a multicast mac addr hence vlanid is a mandatory parameter in all the commands other than - get. For No Vlan case vlan id is not required.
Multicast address	A multicast address is an address that designates a group of entities within a domain.
Egress PVC	The set of ports, which are permanently assigned to the egress list for this VLAN by management.
Forbidden Egress PVC	The set of ports, which should transmit egress packets for this VLAN, as untagged.

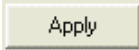
2.6.4

IGMP Snooping

IGMP snooping, as implied by the name, is a feature that allows an IP DSLAM to "listen in" on the IGMP conversation between hosts and routers. To set IGMP Snooping status as Disabled or Enable, the procedure is as follows:

1. Choose a specified port to execute IGMP snooping function.
2. Double click on IGMP Configuration via Function window. Then the IGMP Configuration window appears as follows:



3. Select Disabled or Enabled, and then click  to submit your setting.

This section describes how to configure DSL settings by selecting **DSL** from Function window. This section will cover those functions:

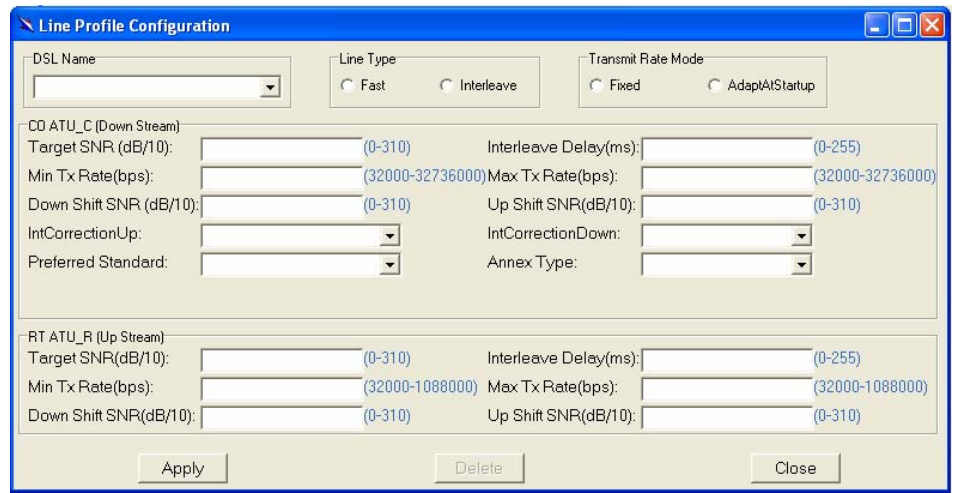
2.7.1 Profile Configuration

Allow users to configure Line Profile and alarm profile.

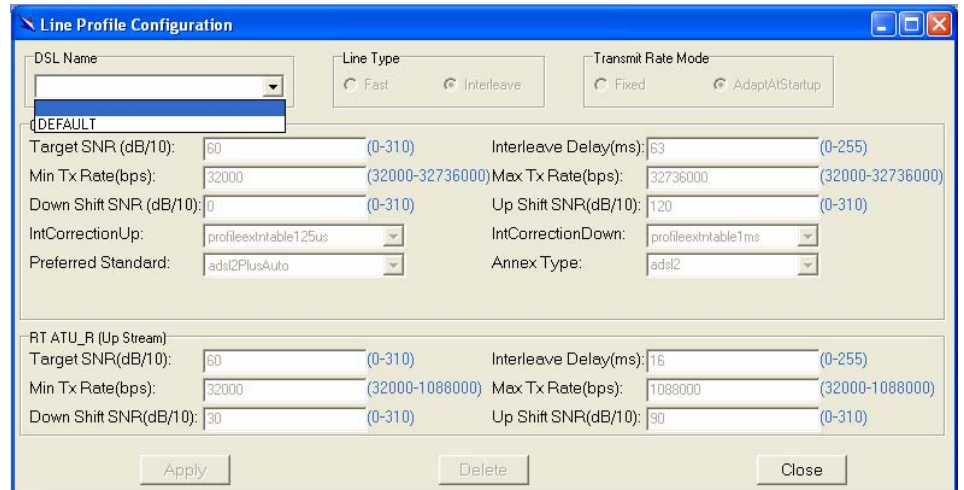
2.7.1.1 Line Profile Configuration

If to configure Line Profile, proceed as follows.

1. Double Click on “Line Profile configuration” from the Function window. The Line Profile configuration window appears.



2. To create a new line profile, click the DSL Name drop-down list and then select the blank.



3. After that, the fields become enable. Input the values in those fields and then name the new line profile.
4. Click on **Apply** to submit your setting or click on **Delete** to delete a line profile.

Table 2-10 Line Profile Field Definitions

Field	Definition
Line Type	The ADSL line type, Fast or Interleaved
Transmit Rate Adaption	Defines what form of transmitting rate to be adaptated, fixed or adaptAtStartup
Target SNR (dB/10)	Target Signal / Noise Margin.(0-310)

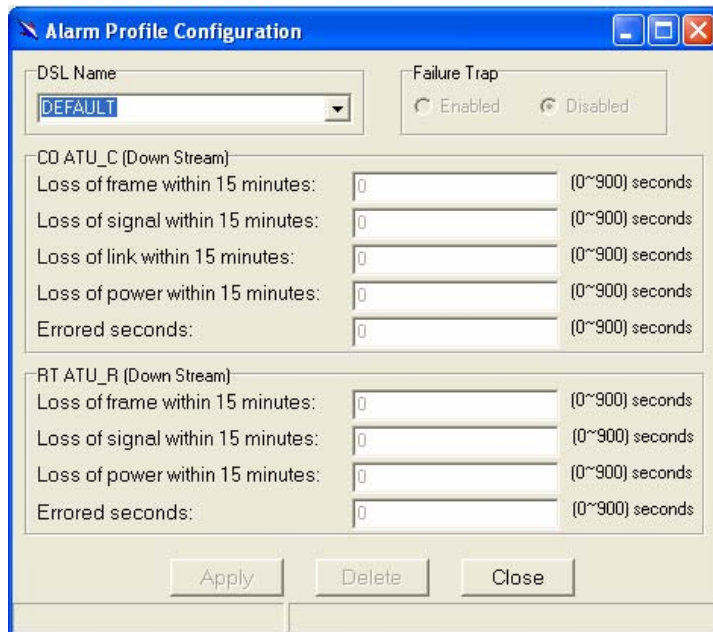
Min Tx Rate(bps)	The minimum transmitting rate of ATU-C side or ATU-R side.
Down Shift SNR (dB/10)	Configured Signal/ Noise Margin for rate downshift. If the noise margin falls below this level, the modem should attempt to decrease its transmit rate. In the case that RADSL mode is not present, the value will be 0.
IntCorrectionUP	Sets the correction time for the upstream interleaved buffer. RS can also be disabled. Value: 125us 250us 500us 1ms 2ms 4ms disable
Preferred Standard	Preferred standard compliance. Outcome is dependent upon standard support of the remote unit.GlobespanVirata High Speed ADSL DMT (ADSL+) applications only Value: t1413 gLite gDmt alctl14 multimode adi alctl t1413Auto adslPlus GspanPlus
Maximum Transmit Rate	The maximum transmitting rate of ATU-C side or ATU-R side.
Interleave Delay (ms)	The value of Interleave Delay for this channel.
UP Shift SNR (dB/10)	Configured Signal/ Noise Margin for rate upshift. If the noise margin rises above this level, the modem should attempt to increase its transmit rate. In the case that RADSL is not present, the value will be 0.
IntCorrectionDown	This parameter sets the correction time for the downstream interleaved buffer. RS can also be disabled.
Annex Type	This parameter is set as per Annex compliance of the code release. GlobespanVirata High Speed ADSL DMT (ADSL+) applications only.

2.7.1.2

Alarm Profile Configuration

If to configure Alarm Profile, proceed as follows.

1. Double Click on “**Alarm Profile Configuration**” from the Function window. The Alarm Profile Configuration window appears.



2. To create a new alarm profile, click the DSL Name drop-down list and then select the blank.
3. After that, the fields become enable. Input the values in those fields and then name the new alarm profile.

- Click on to submit your setting or click on to delete a alarm profile.

Table 2-11 Alarm Profile Field Definitions

Field	Definition
Loss of frame within 15 minutes	The threshold of the number of “Loss of Frame Seconds” within 15 minutes performance data collection period.
Loss of signal within 15 minutes	The threshold of the number of “Loss of Signal Seconds” within 15 minutes performance data collection period.
Loss of link within 15 minutes	The threshold of the number of “Loss of Link Seconds” within 15 minutes performance data collection period. (But only ATU-C side)
Loss of power within 15 minutes	The threshold of the number of “Loss of Power Seconds” within 15 minutes performance data collection period.
Errored seconds	The threshold of the number of “Errored Seconds” within 15 minutes performance data collection period.

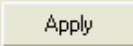
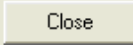
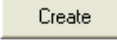
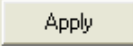
2.7.2

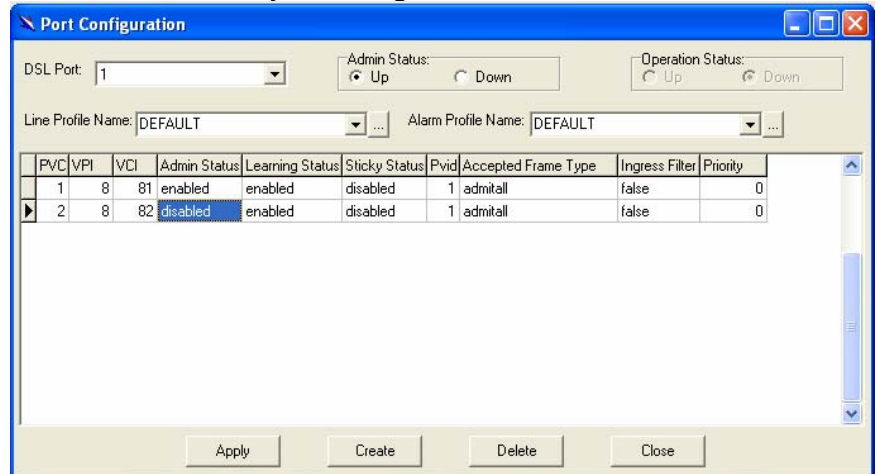
Port Configuration

Allow users to proceed port configuration. The procedures are as follows:

- Double Click on “**Port Configuration**” from the Function window. The Port Configuration window appears.

- Choose the port to configure from the DSL Port drop-down list.
- Configure the Administration status as “Up” or “Down”.
- Modify user’s information on phone number, user name, user address and description fields respectively.
- Choose a Line Profile from the Line Profile Name drop-down list. If to configure a Line Profile, Click on to activate the Line Profile Configuration window.
- Choose an Alarm Profile from the Alarm Profile Name drop-down list. If to configure an Alarm Profile, Click on to activate the Alarm Profile Configuration window. If necessary, modify values of specified PVC, including VPI, VCI, Admin Status, Learning Status, Sticky Status, Pvid, Accepted Frame Type and Ingress Filter, and priority.

7. Click on  to submit your settings or click on  to close the port configuration window.
8. If to create new PVC, click on  and then PVC2 appears and where users can set parameters. After that, click on  to submit your setting.



Note: one DSL port supports max. 8 PVCs.

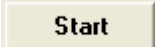
Table 2-12 Port Configuration Field Definitions

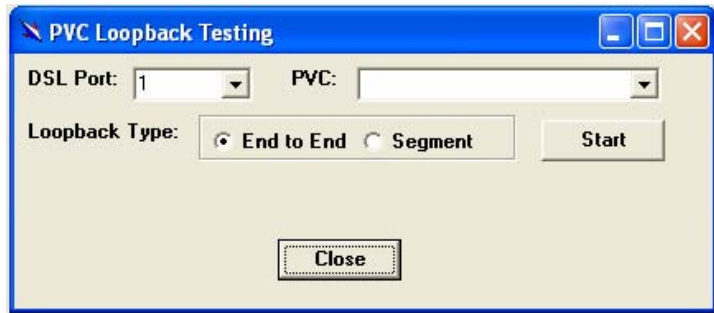
Field	Definition
DSL Port	Port No. of the IP DSLAM
VPI	Virtual Path Identifier
VCI	Virtual Channel Identifier
Learning Status	The state of learning on this bridge port. The value enable (1) indicates that unicast Mac address learning is enabled and the value disable indicates that unicast Mac address learning is disabled on this bridge port.
Sticky Status	Indicates if the port has been set as sticky. The value enable (1) indicates that the entries learned on this port will not be aged out. It also indicates that the entries learned on this port shall not be learned on any other port. The entries learned on this port can only be removed by management action or by making the value as disable (2) , so that the entries can be aged out.
Pvid	Port VID
Accepted Frame Type	Used to up/down connection.
Ingress Filter	When this is true , the device will discard incoming frames for VLANs, which do not include this Port in its Member set. When false , the port will accept all incoming frames.
Priority	Optional Connection priority. No VLAN tag, no priority.

2.7.3

PVC Loopback Testing

This section describes how to start or stop OAM loopback.

1. Double Click on “**Port Loopback testing**” from the Function window.
2. Select the DSL port and PVC.
3. Select the loopback type and then click on  to execute loopback test.



2.8

DSL Performance Management

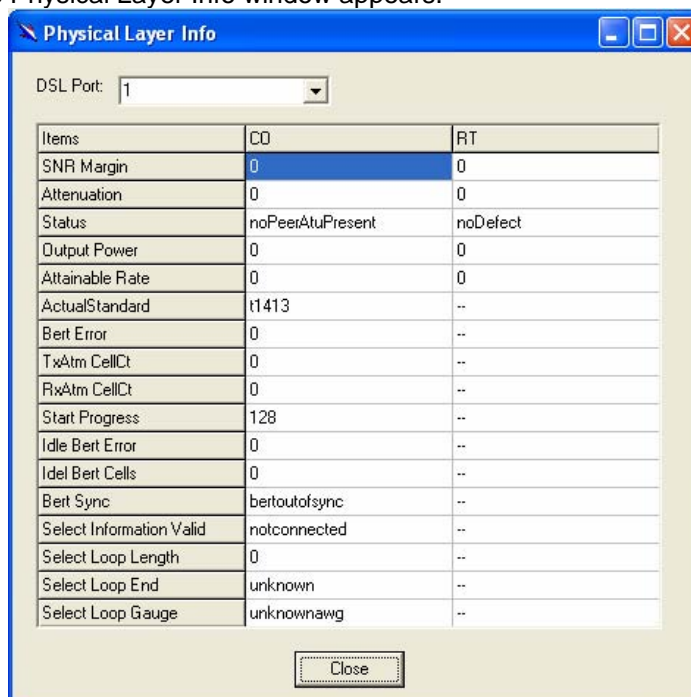
This section describes how to utilize DSL Performance Management by selecting **DSL Performance Management** from Function window. This section will cover those functions:

2.8.1

Physical Layer Info

Allow users to view the physical layer information of a specified DSL port from the IP DSLAM. The procedures are as follows:

1. Double Click on **“Physical Layer Info”** from the Function window. The Physical Layer Info window appears.



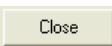
2. Select the port ID from the DSL Port drop-down list to view a specified DSL's physical Layer Info.
3. Click on  to close the window.

Table 2-13 Physical Layer Info Field Definitions

Field	Definition
SNR margin	Noise margin value. (dB)
Attenuation	Difference in the total power transmitted and the total power received by the peer atu. (db)
Status	Current status of the ATU line. The possible values displayed are as follows: No defect: there are no defect on the line los: atu-r failure due to not receiving signal lpr: atu-r failure due to loss of signal
output power	Total output power transmitted by atu. (dBm)
attainable rate	The maximum currently attainable data rate by the atu. (kbps)
ActualStandard	Actual standard used for connection, based on the outcome of the negotiation with the Remote Unit.
Bert Error	Provides the number of bit errors detected during BERT.
TxAtm CellCt	Provides Tx ATM cell counter.
RxAtm CellCt	Provides Rx ATM cell counter.
Start Progress	Defines the current detailed start up state of Xcvr. 0x0 – startup not in progress; 0x0 – 0x0FFF

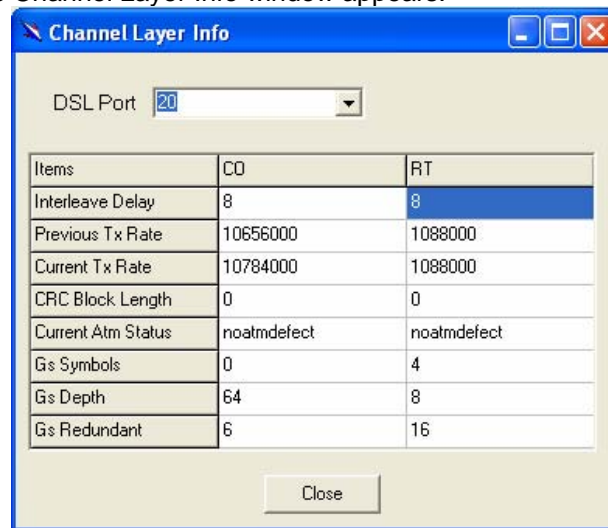
	Handshake/Training/ Profile Management/ Fast Retrain in progress; 0x8000 – 0x8FFF DSP firmware Down- Load in progress; 0xF000 – 0xFFFF illegal Parameter
Idle Bert Error	Number of bit errors.
Idle Bert Cells	Number of idle cells.
Bert Sync	Indicates whether the Signal is in Sync or not.
Select Information Valid	Indicates the information validity for the SELT operation conducted on the Xcvr.
Select Loop Length	Indicates the LOOP Length in Feet once when the SELT information is valid on the Xcvr.
Select Loop End	Indicates whether the loop is short or open once when the SELT information is valid on the Xcvr.
Select Loop Gauge	Indicates the LOOP wire gauge information once, when the SELT information is valid on the Xcvr.

2.8.2

Channel Layer Info

Allow users to view the Channel layer information of a specified DSL port from the IP DSLAM. The procedures are as follows:

1. Double Click on “**Channel Layer Info**” from the Function window. The Channel Layer Info window appears.



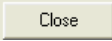
2. Select the port ID from the DSL Port drop-down list to view a specified DSL’s channel Layer Info.
3. Click on  to close the window.

Table 2-14 Channel Layer Information Field Definitions

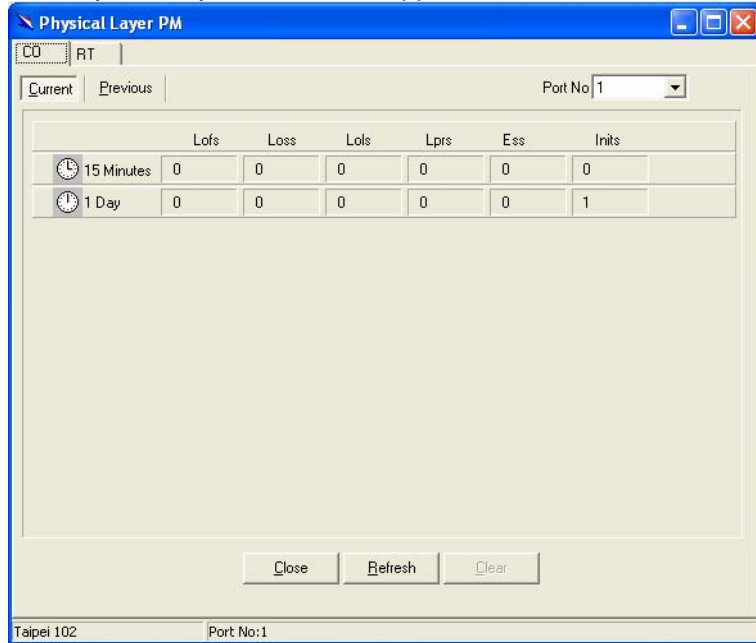
Field	Definition
Interleave delay	Interleave delay for this channel. (milli-seconds)
Previous TX rate	Previous actual transmit rate on this channel if ADSL loop retain. (kbps)
Current TX rate	Actual transmit rate on this channel. (kbps)
CRC block length	The length of the channel data-block on which the CRC operates.
Current Atm Status	Indicates the current ATM Status.
Rs Symbols	Indicates the number of DMT symbols per Reed-Solomon code word (S), in the downstream direction.
Rs Depth	Indicates interleaving depth (D), in the downstream direction.
Rs Redundancy	Indicates the number of redundant bytes (R), per Reed-Solomon code in the downstream direction

2.8.3

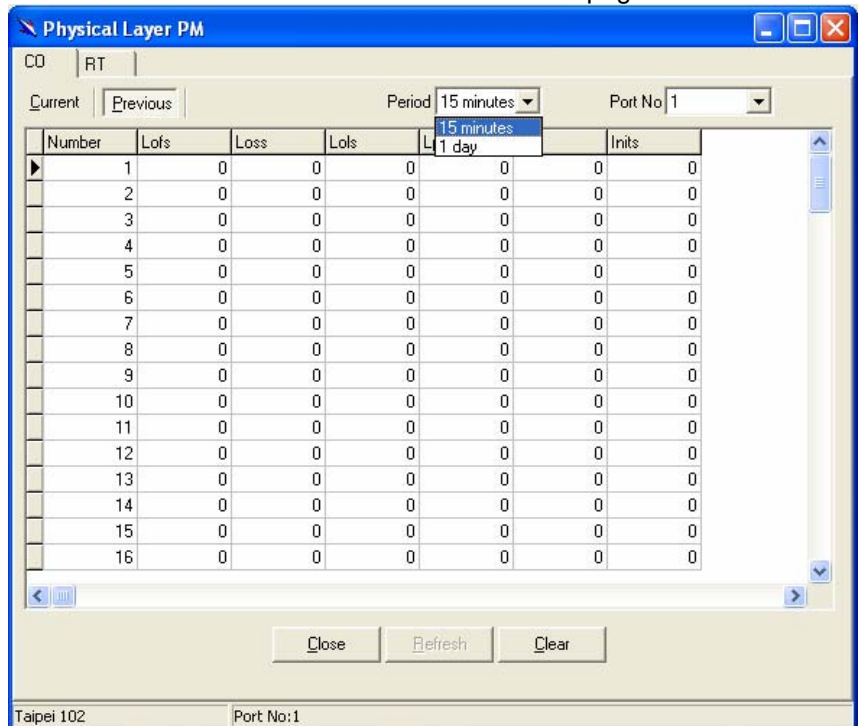
Physical Layer PM

Allow users to view the Physical layer performance of a specified DSL port from the IP DSLAM. The procedures are as follows:

1. Double Click on “**Physical Layer PM**” from the Function window. The Physical Layer PM window appears.



2. Press Co or RT tab to view the Physical Layer Performance data at down stream or up stream.
3. Click on **Current** to activated Current page in which users can select Port No. to view 15 minutes and 1 Day ES, SES and UAS record. If to retrieve the latest data, press **Refresh**.
4. Click on **Previous** to activate previous 15 minutes and 1 day performance data page in which Period and Port No. are selectable. **Note:** refresh button is disable in this page.



5. Click on **Clear** to clear the physical layer data.
6. Click on **Close** to close the window.

Table 2-15 Current Phy-Layer PM Information Field Definitions

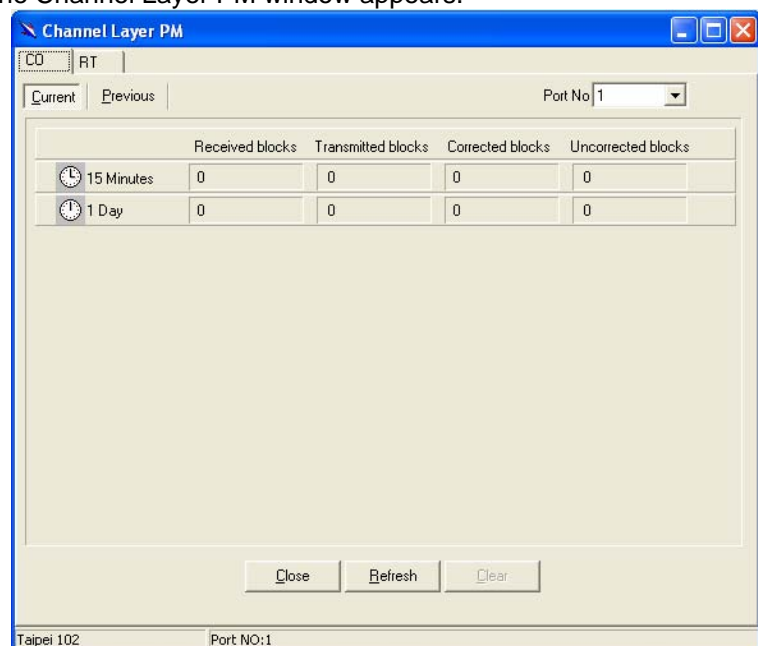
Field	Definition
CO	down stream
RT	up stream
Lofs	Number of lof failures since reset.
Loss	Number of los failures since reset.
Lols	Number of lol failures since reset.
Lprs	Number of lpr failures since reset.
Ess	Number of error seconds since reset.
Inits	Number of initialization attempts since reset. It includes both successful and failed attempts.
Current 15-min lofs	Number of seconds in the current 15-minute interval during which lof was detected.
Current 15-min loss	Number of seconds in the current 15-minute interval during which los was detected.
Current 15-min lols	Number of seconds in the current 15-minute interval during which lol was detected.
Current 15-min lprs	Number of seconds in the current 15-minute interval during which lpr was detected.
Current 15-min ess	Number of error seconds in the current 15-minute interval.
Current 15-min inits	Number of inits in the current 15-minute interval. It includes both successful and failed attempts.
Current 1-day time elapsed	Number of seconds that have elapsed since the beginning of the current 1-day interval.
Current 1-day lofs	Number of seconds in the current 1 day interval during which lof was detected.
Current 1-day loss	Number of seconds in the current 1 day interval during which los was detected.
Current 1-day lols	Number of seconds in the current 1 day interval during which lol was detected.
Current 1-day lprs	Number of seconds in the current 1 day interval during which lpr was detected.
Current 1-day ess	Number of error seconds in the current 1 day interval.

2.8.4

Channel Layer PM

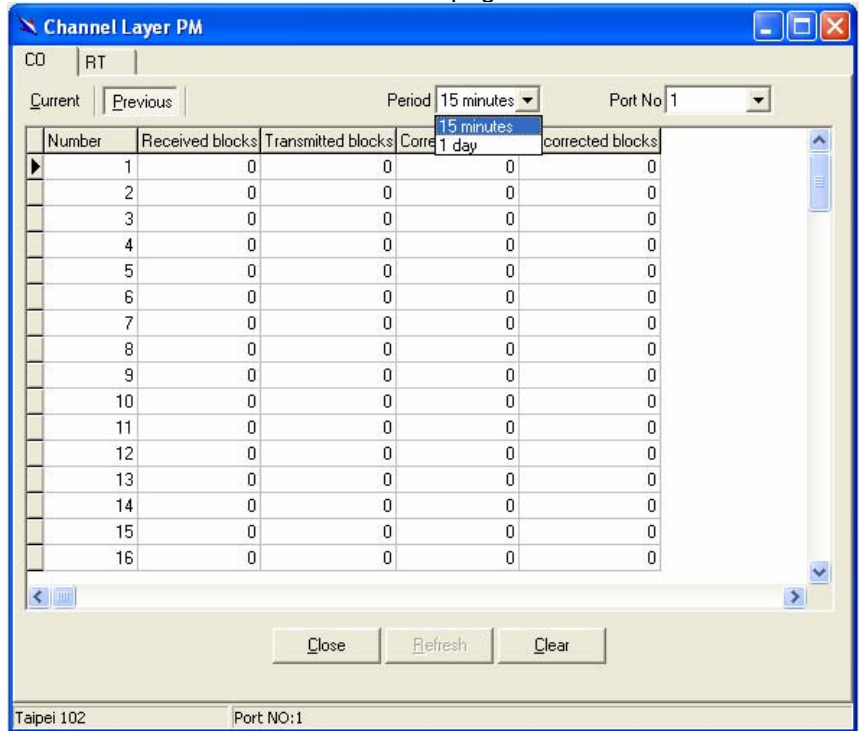
Allow users to view the Channel layer performance of a specified DSL port from the IP DSLAM. The procedures are as follows:

1. Double Click on “**Channel Layer PM**” from the Function window. The Channel Layer PM window appears.



2. Press Co or RT tab to view the Channel Layer Performance data at down stream or up stream.
3. Click on **Current** to activated Current page in which users can select Port No. to view 15 minutes and 1 Day ES, SES and UAS record. If to retrieve the latest data, press **Refresh**.
4. Click on **Previous** to activate previous 15 minutes and 1 day performance data page in which Period and Port No. are selectable.

Note: refresh button is disable in this page.



5. Click on **Clear** to clear the channel layer data.
6. Click on **Close** to close the window.

Table 2-16 Current Channel-Layer PM Information Field Definitions

Field	Definition
CO	down stream
RT	up stream
Received blocks	The total number of blocks of data received since the last agent reset.
Transmitted blocks	The total number of blocks of data transmitted since the last agent reset.
Corrected blocks	Number of corrected blocks of data transmitted since the last agent reset.
Uncorrected blocks	Number of uncorrected blocks of data transmitted since the last agent reset.
Current 15-min received blocks	Number of blocks of data received during the current 15-minute interval.
Current 15-min Transmitted blocks	Number of blocks of data transmitted during the current 15-minute interval.
Current 15-min corrected blocks	Number of corrected blocks of data transmitted during the current 15-minute interval.
Current 15-min Uncorrected blocks	Number of uncorrected blocks of data transmitted during the current 15-minute interval.
current 1-day time elapsed	Number of seconds that have elapsed since the start of the current day interval.
Current 1-day received blocks	Number of blocks of data received during the current day interval.

Field	Definition
Current 1-day transmitted blocks	Number of blocks of data transmitted during the current day interval.
Current 1-day corrected blocks	Number of corrected blocks of data transmitted during the current day interval.
Current 1-day uncorrected blocks	Number of uncorrected blocks of data transmitted during the current day interval.

2.9

Get Traffic Information

Allow users to view the managed IP DSLAM's traffic in real time, including Ethernet uplink Tx/Rx data and ADSL Tx/Rx data. To display the traffic information, double click on the “**Get Traffic**” from the Function window and then the traffic information window prompts.

The screenshot shows a window titled "Traffic Information" with a table containing traffic data for 48 ports. The table has three columns: "Port No", "Total Bytes (Tx/Rx)", and "KBytes/s (Tx/Rx)".

Port No	Total Bytes (Tx/Rx)	KBytes/s (Tx/Rx)	Port No	Total Bytes (Tx/Rx)	KBytes/s (Tx/Rx)
Port 1	0 / 0	0.000 / 0.000	Port 25	Null / Null	Null / Null
Port 2	Null / Null	Null / Null	Port 26	Null / Null	Null / Null
Port 3	8832 / 0	0.000 / 0.000	Port 27	Null / Null	Null / Null
Port 4	7968 / 0	0.000 / 0.000	Port 28	Null / Null	Null / Null
Port 5	7968 / 0	0.000 / 0.000	Port 29	Null / Null	Null / Null
Port 6	7536 / 0	0.000 / 0.000	Port 30	Null / Null	Null / Null
Port 7	7824 / 0	0.000 / 0.000	Port 31	Null / Null	Null / Null
Port 8	8928 / 0	0.000 / 0.000	Port 32	Null / Null	Null / Null
Port 9	8400 / 0	0.000 / 0.000	Port 33	Null / Null	Null / Null
Port 10	7968 / 0	0.000 / 0.000	Port 34	Null / Null	Null / Null
Port 11	8544 / 0	0.000 / 0.000	Port 35	Null / Null	Null / Null
Port 12	7968 / 0	0.000 / 0.000	Port 36	Null / Null	Null / Null
Port 13	8112 / 0	0.000 / 0.000	Port 37	Null / Null	Null / Null
Port 14	7296 / 0	0.000 / 0.000	Port 38	Null / Null	Null / Null
Port 15	7536 / 0	0.000 / 0.000	Port 39	Null / Null	Null / Null
Port 16	8400 / 0	0.000 / 0.000	Port 40	Null / Null	Null / Null
Port 17	8400 / 0	0.000 / 0.000	Port 41	Null / Null	Null / Null
Port 18	7968 / 0	0.000 / 0.000	Port 42	Null / Null	Null / Null
Port 19	7680 / 0	0.000 / 0.000	Port 43	Null / Null	Null / Null
Port 20	8400 / 0	0.000 / 0.000	Port 44	Null / Null	Null / Null
Port 21	8544 / 0	0.000 / 0.000	Port 45	Null / Null	Null / Null
Port 22	8400 / 0	0.000 / 0.000	Port 46	Null / Null	Null / Null
Port 23	8400 / 0	0.000 / 0.000	Port 47	Null / Null	Null / Null
Port 24	8256 / 0	0.000 / 0.000	Port 48	Null / Null	Null / Null

Table 2-17 Get traffic Field Definitions

Field	Definition
Port No.	Port number
Total Bytes (Tx/Rx)	Total transmission/Receiving bytes Null: not connected with CPE
Kbytes/s (Tx/Rx)	Transmission/Receiving Kbytes per seconds