2011

NMS 3.0.1

Administrator's Handbook

Preface

NMS is a multiplatform and multiprotocol-compatible (such as SNMP, HTTP and CLI) network management system. NMS has various network monitor tools, friendly customized window and simple but versatile network configuration. Hence, the application of NMS can greatly improve the efficiency of network operating. This network management system can realize the real-time monitor of the whole network, making real centralized management of the whole LAN available for the administrator.

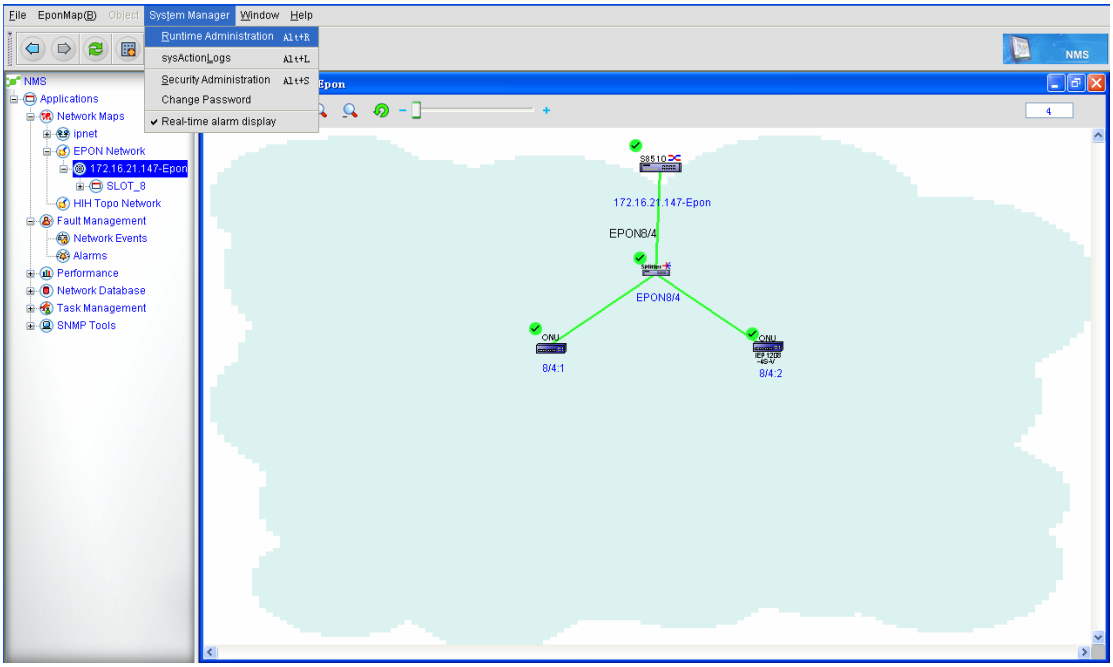
This handbook is edited for the management system and the network administrator can know all management functions and operation methods of this system after reading it.

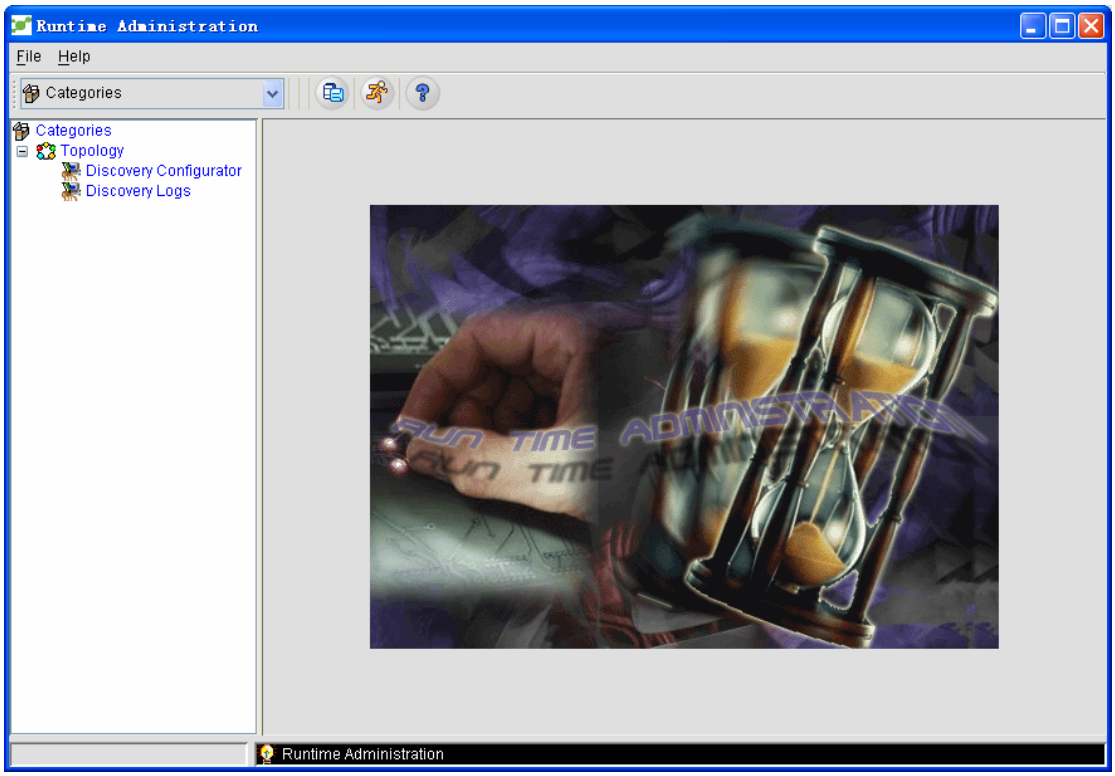
Table of Contents

Discovery Management

Discovery Management provides a platform for device management. All managed devices are logged in from this platform. After login the system will differentiate the devices according to device types and their states and then provide different proper management methods to different devices. The system obtains the basic information of the devices and then stores the information in the database and at last display the information on the corresponding windows according to device types.

The administrator can click **System Management -> Runtime Administration** or use the shortcut key "**ALT+R"** to open the real-time management window, as shown in the following figure:

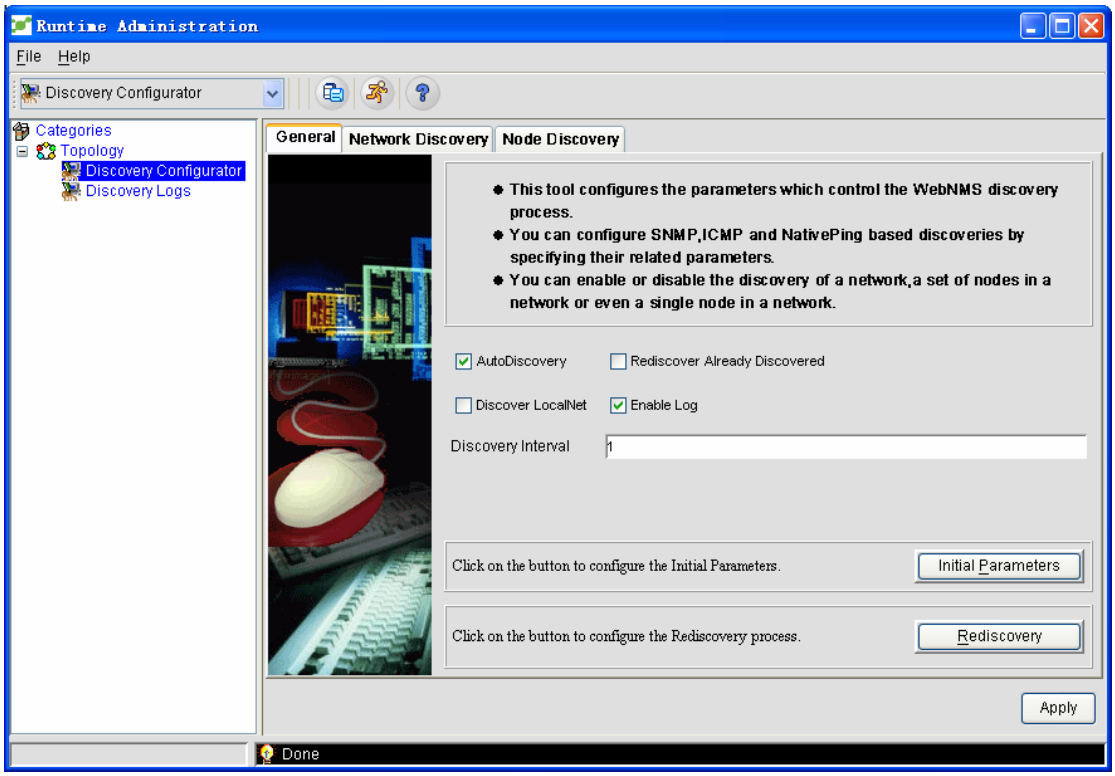




In Runtime Administration tools, the system settings provided by the system makes users configure the network topology flexibly and conveniently. For example, you can configure the protocol and parameters, whether to discover the local network, whether to conduct automatic discovery or whether to discover all nodes in a network for **Discovery Configurator**.

The systematic administrator can perform the following operations to open the **Discovery Configurator** panel.

Click System Management -> Runtime Administration to open the Discovery Configurator page, and then on this page click Topology -> Discovery Configurator. The Discovery Confurator panel is shown in the following figure.

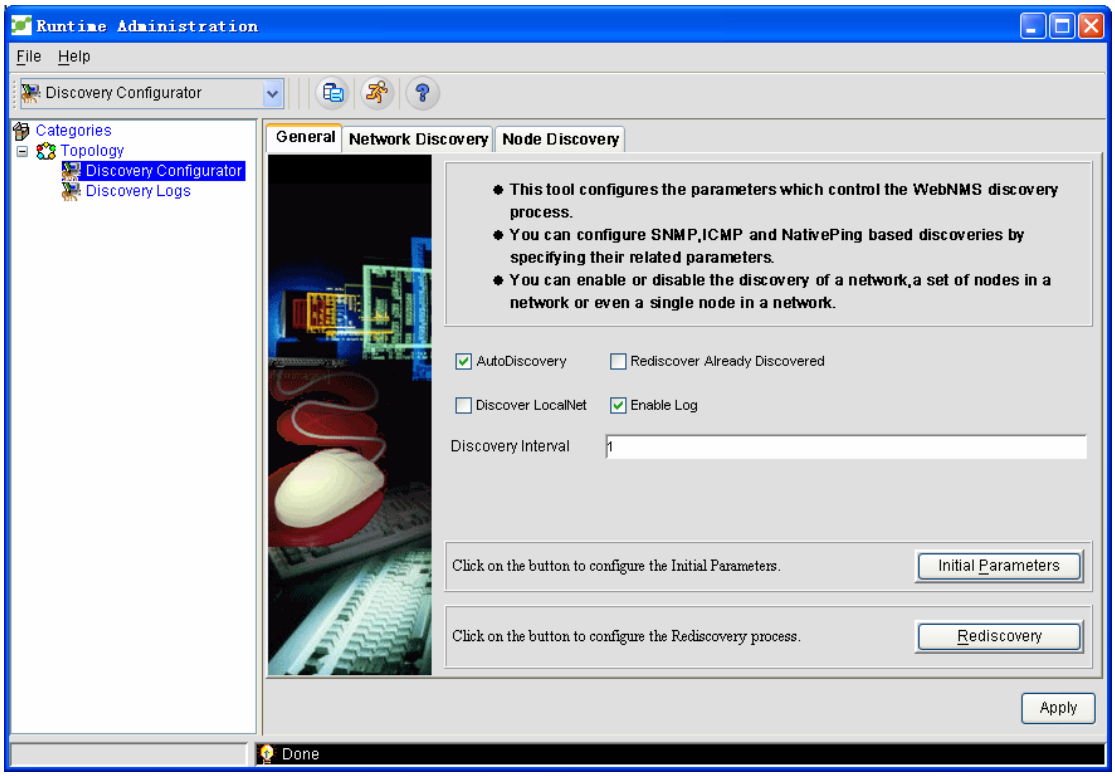


The discovery settings function provided by the system makes the administrator conduct the corresponding settings based on the following three aspects:

- General
- Network discovery
- Node discovery

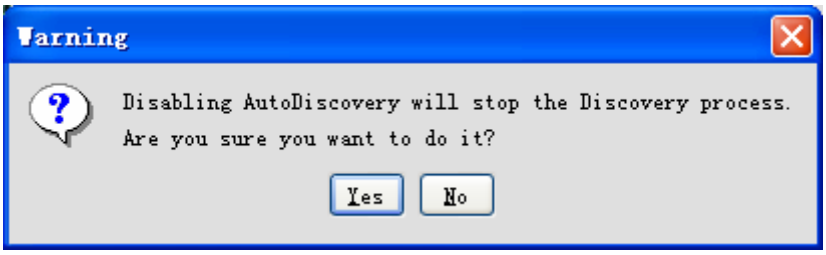
1.1 General

In General you will be presented how to set some common attributes of topology settings. See the following figure.

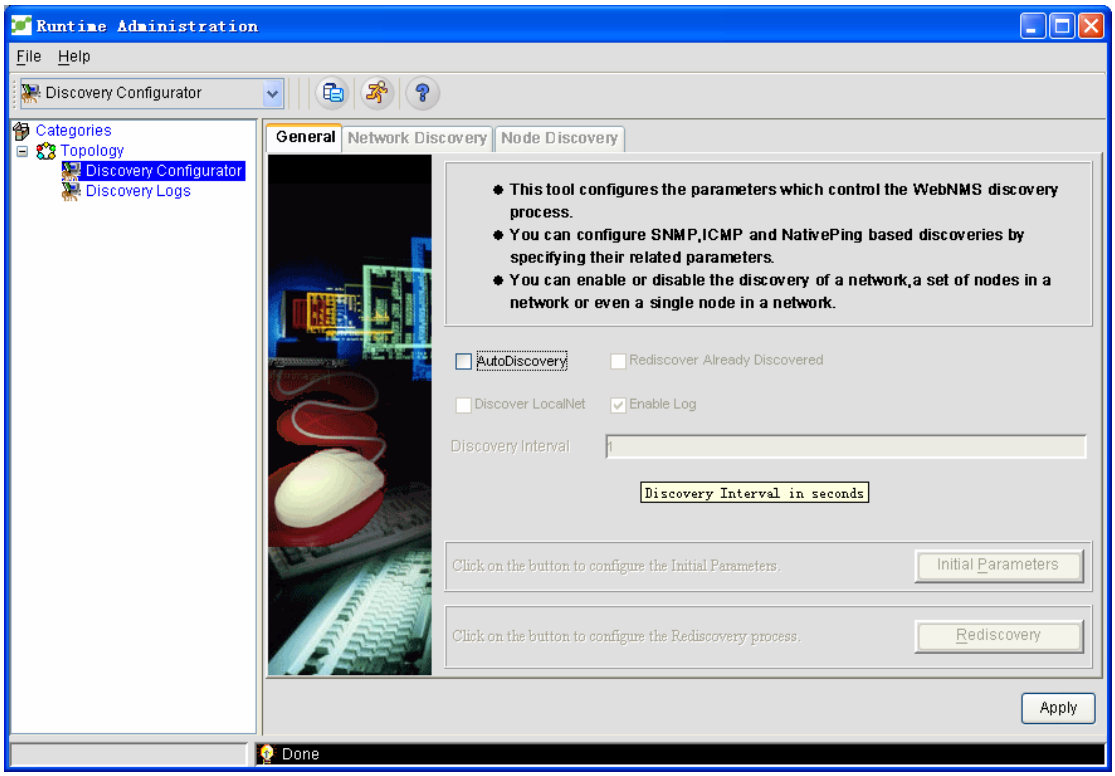


◆ Enable automatic discovery or not

Automatic discovery is enabled by default. If automatic discovery is deselected, the alarm information will be presented, as shown in the following figure:



Note: If the automatic discovery option is canceled, the system will not discover all devices in the networ, and network discovery and node discovery are will be forbidden. See the following figure.



◆ Rediscover the already discovered nodes

The **rediscover the already discovered nodes** option is used to decide whether to rediscover an already discovered network. If this option is selected, rediscovery will be carried on according to the rediscovery interval which is set by users. In defaut settings, this option is deselected.

◆ Discover the local network or not

The **Discover the local network** option is used to permit or forbid to discover the local network where the NMS server is located.

◆ Record the discovery log or not

This option is used to record and discover related information in a single log file. The **Record the log** option is enabled by default. The related logs are saved in a **discoveryLogs.txt** folder.

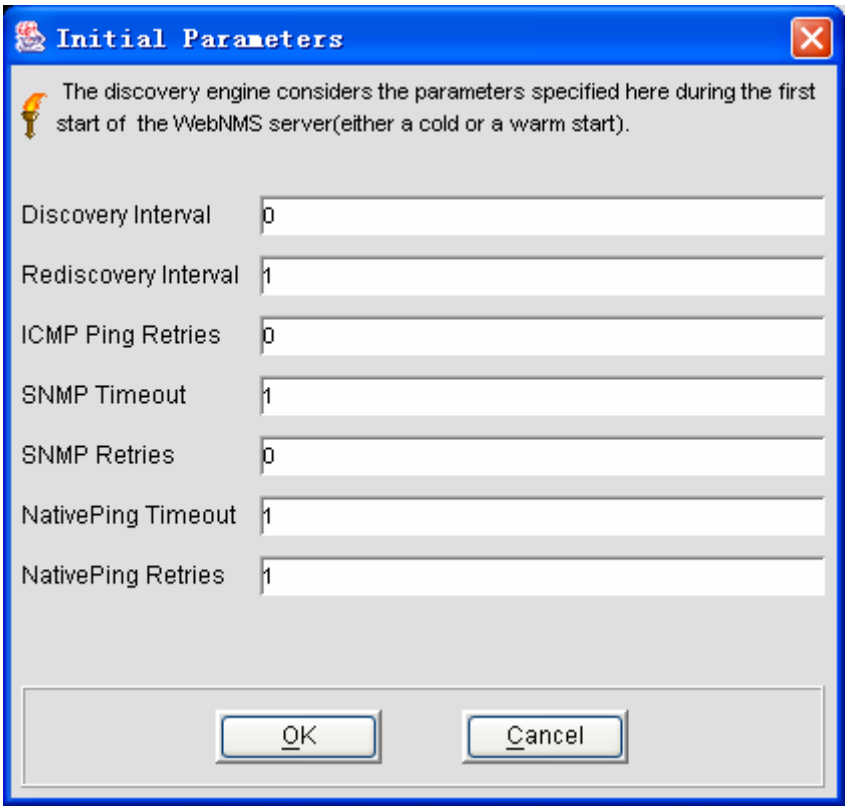
◆ Set the discovery interval

The discovery interval, taking second as its unit, defines the interval between two devices in the discovery network. The default value is 1 second. To find a device, the system will send an SNMP request and an ICMP request to it; if the system receives response, a lot more SNMP requests will be sent to obtain more detailed information about this device. Considering the CPU usage and the network's flux, users have to set a proper discovery interval, whose unit is second.

	Note: If the discovery interval is set to 0, no problem will arise. If you set the discovery interval to **0** in the initial parameter dialog box, the NMS server will read the value of the initial parameter at the first startup; but in the following startups, the NMS server will read the discovery interval value in the regular setup and the values of the corresponding discovery parameters in the local Ping options

◆ Set the initial parameters

The systemati administrator can configure parameters in the **initialized parameter** window to improve the effeciency of the discovery. Click **Discovery Settings -> Regular Settings -> Initialized Parameters**, the **Initialized Parameters** window appears, as shown in the following figure:



The parameters in the **Initialized Parameters** window are described in the following table:

Parameter	Remarks
Discovery interval	Defines the interval between two devices in the discovery network. The default value is 1 second. If this parameter is set to be less than 0 or be some characters, the default discovery interval of the system is 10 seconds.
Rediscovery interval	Defines the interval to carry on complete network discovery (rediscovery of the network), whose unit is hour. The default value is 24 hours. If a minus value (except minus 1) is entered, the system still carry on network rediscovery every 24 hours.
ICMP Ping Retry Times	Sets the retry times of sending the Ping packets. The default value is 0, that is, the Ping packets are only sent once.
SNMP timeout	Sets the timeout time for a device to reply the SNMP packet after this packet is received by the device. (as for not so good network conditions, you can set this parameter to be a bigger value)
SNMP retry times	This parameter is mainly used for topology discovery, status round query and data collection. When the device has no response, the system will resend the SNMP packet. The default value is 0.
Local Ping timeout	Sets the timeout time for a device to reply the local Ping packet after this packet is received by the device. The default value is 1 second.
Local Ping Retry Times	Stands for the times that the system resends the local Ping packet when there is no response from the device, whose default value is 1.

- Set the rediscovery interval

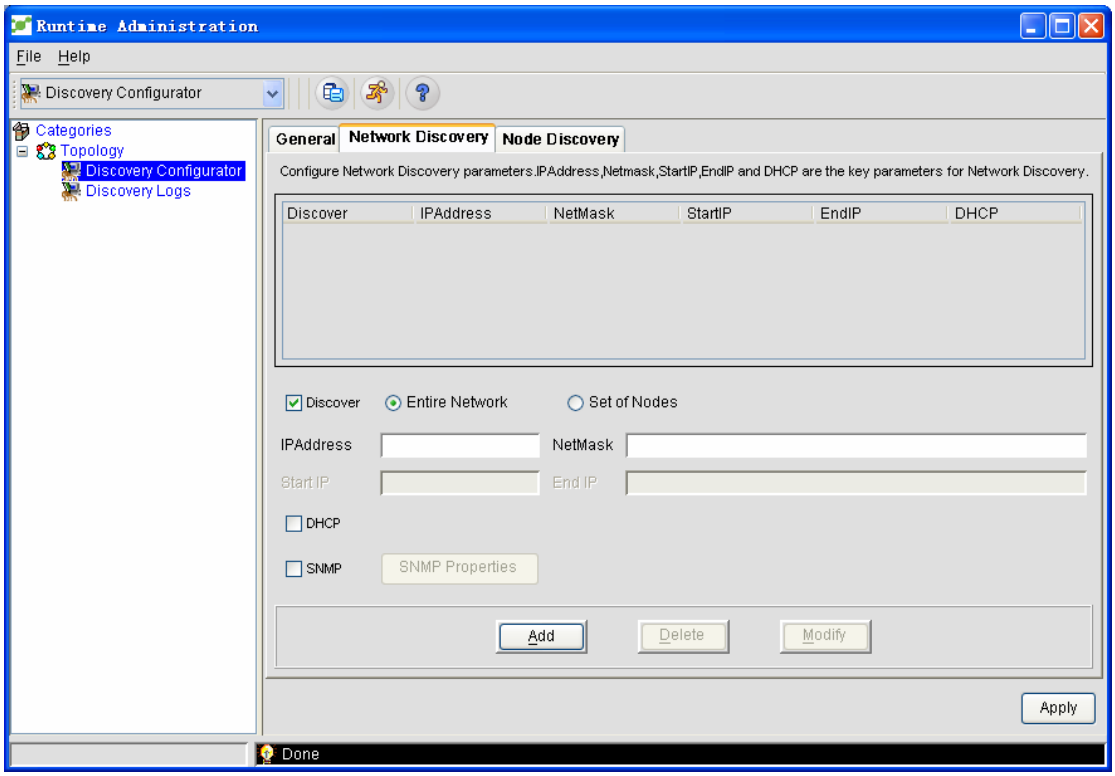
  Users can click **Rediscovery** to set the rediscovery process.

  After the **rediscovery** option is selected, the rediscovery interval can then be set; if users select the **rediscovery date** option, the specific date to carry on network rediscovery can be designated.

1.2 Setting Network Discovery

The network discovery settings provided by the system enable an administrator to specify a discovery area or to find a group of nodes in a network. The system supports the DHCP protocol.

Click **Discovery Configurator -> Network Discovery**. The Network Discovery page appears, as shown in the following figure:



1.2.1 Setting Remote Network Discovery

If an administrator wishes to add a remote network and discover this remote network, he can select the "Discovery" option in the **Network Discovery** page to finish this settings.

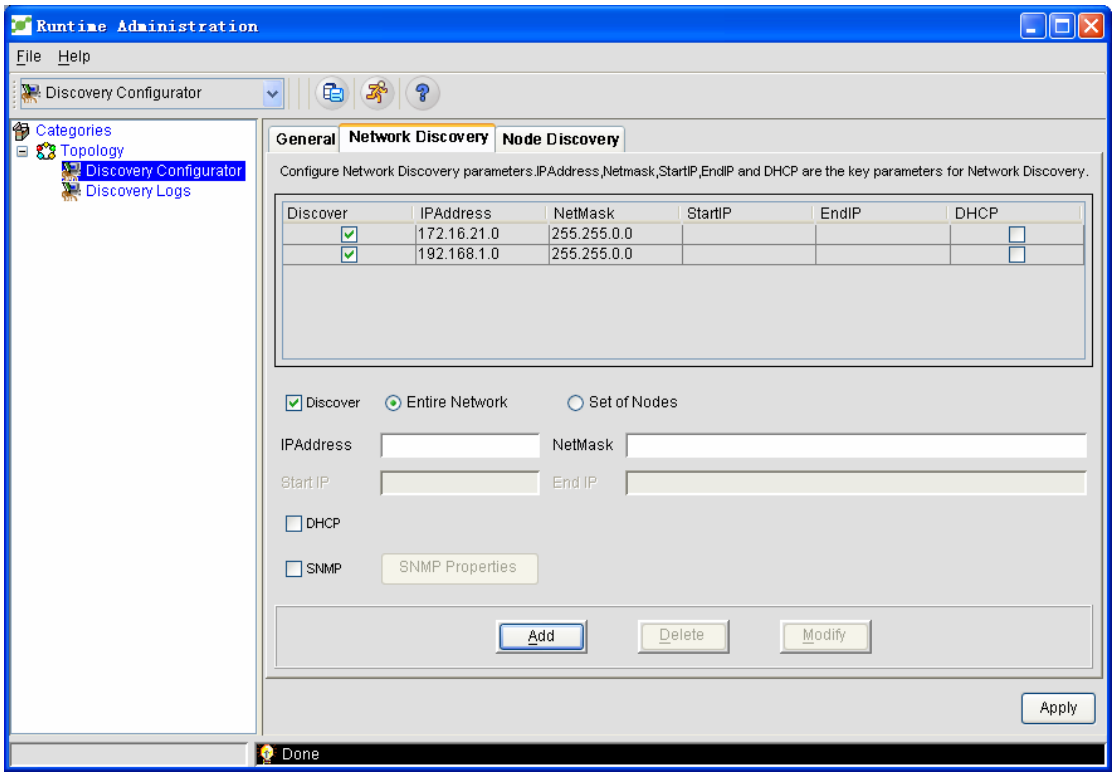
- Select the "Discovery" option on the **Network Discovery** page;
- Enter the IP address and the network mask in the corresponding text box;
- Click **Add**.

After the above-mentioned steps are performed, the IP address and the network mask are added to the discovery list, that is, the system will discover this remote network.

Note: Multiple networks can be discovered if you add multiple IP addresses and network masks.

Example for multiple network settings

As shown in the following figure, two networks are set:



In this example, the system will discover the network whose mask is 225.225.0.0 and whose IP address is 172.16.21.0 and the other network whose mask is same but whose IP address is 198.168.1.0.

1.2.2 Setting Network Discovery in a Designated IP Range

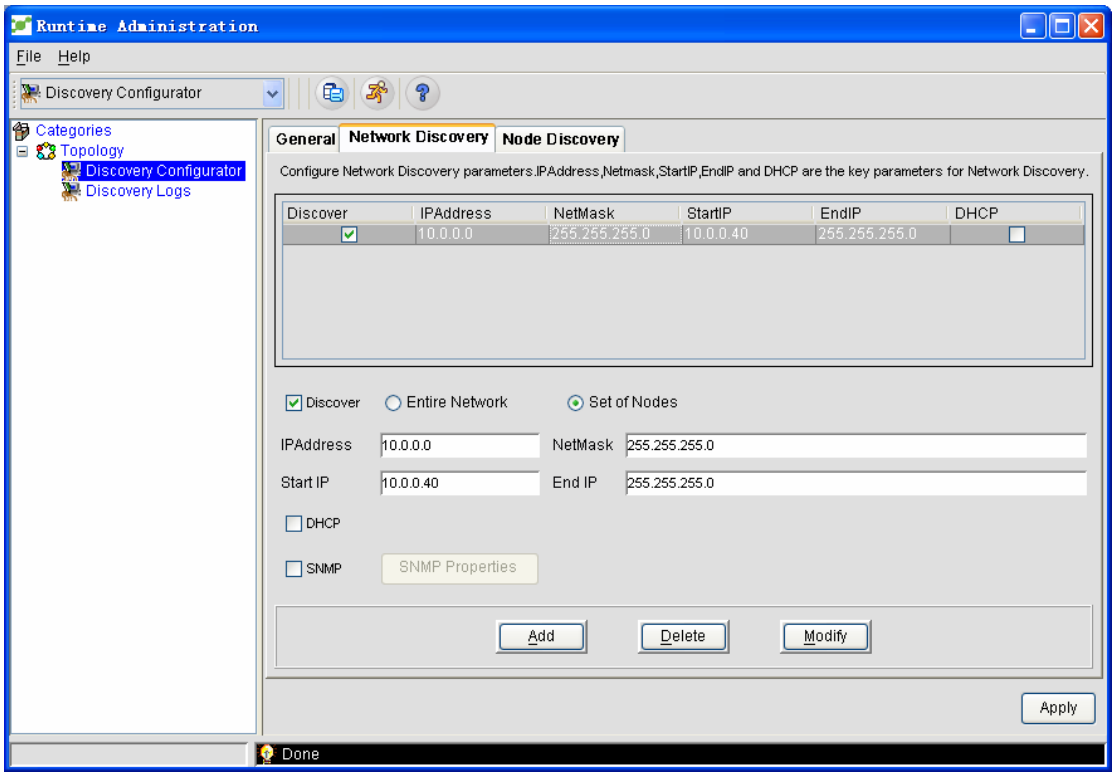
By using the start IP and the end IP, the administrator can designate an IP address range to be discovered. The detailed procedure is shown as follows:

- Select the **Specifying the node** option and activate the start IP or the end IP.
- Enter the IP address, network mask, start IP and end IP.
- Click **Add** to finish the settings.

The administrator can set several IP address ranges in a network.

Example for multiple designated IP address ranges in a network

You can set multiple IP address ranges in a network, as shown in the following figure.



In the above-mentioned example, the system discovers the IP address range from 10.0.0.1 to 10.0.0.40 in network 10.0.0.0 whose mask is 255.255.0.0.

1.2.3 Forbidding Network Discovery

The "discovery" option is selected by default on the **Network Discovery** page. After the "discovery" option is canceled, you can add the IP address and the network mask, or forbid the discovery of the designated network, which further forbids the network to be added to the topology database.

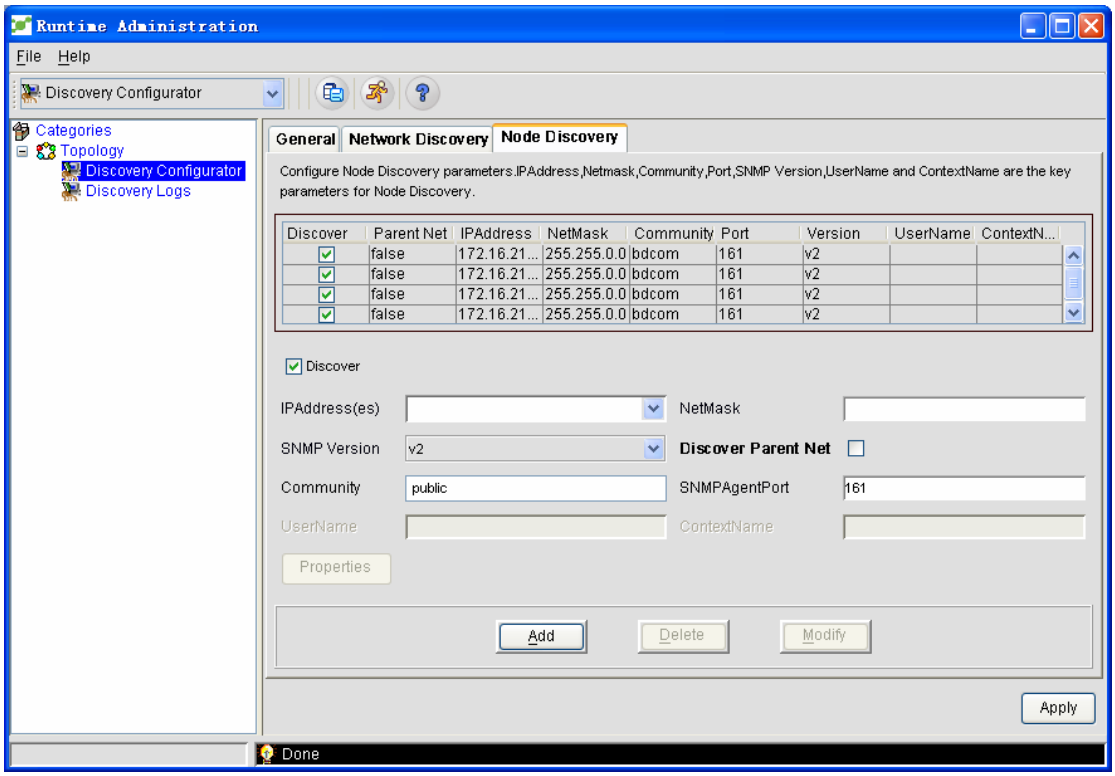
You can click **Edit** to reselect the "discovery" option or modify the IP address.

Multiple networks can be forbidden if you add multiple IP addresses and network masks.

1.3 Setting Node Discovery

The discovery mechanism of NMS can be used to discover the designated devices mandatorily or discover the devices through specific ports or agents when users find any other devices in the discovery network. In this way users can first find and add specific devices and nodes before finding any other nodes in the discovery network.

Click **Discovery Configurator -> Network Discovery**. The **Network Discovery** page appears, as shown in the following figure:



1.3.1 Discovering a Node with Designated IP

If the administrator wants to find the designated node before any other nodes are found in the discovery network, he can use the "discovery" option to conduct this operation. The detailed procedure is shown as follows:

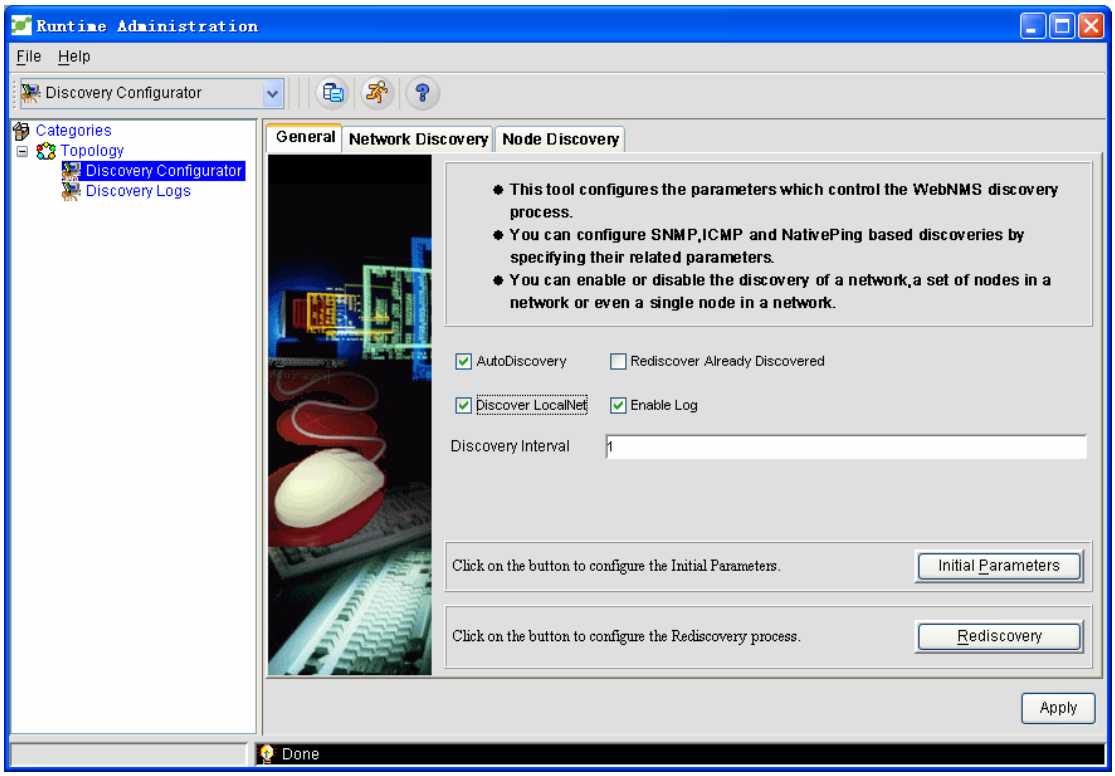
- Select the "discovery" option on the **node discovery** page and then enter the IP address and the network mask in the corresponding text box. Note: The IP address and the network mask is necessary.
- Click **Add**. After the IP addresses and the network masks are added to the discovery list, the system will perform the discovery of these nodes.

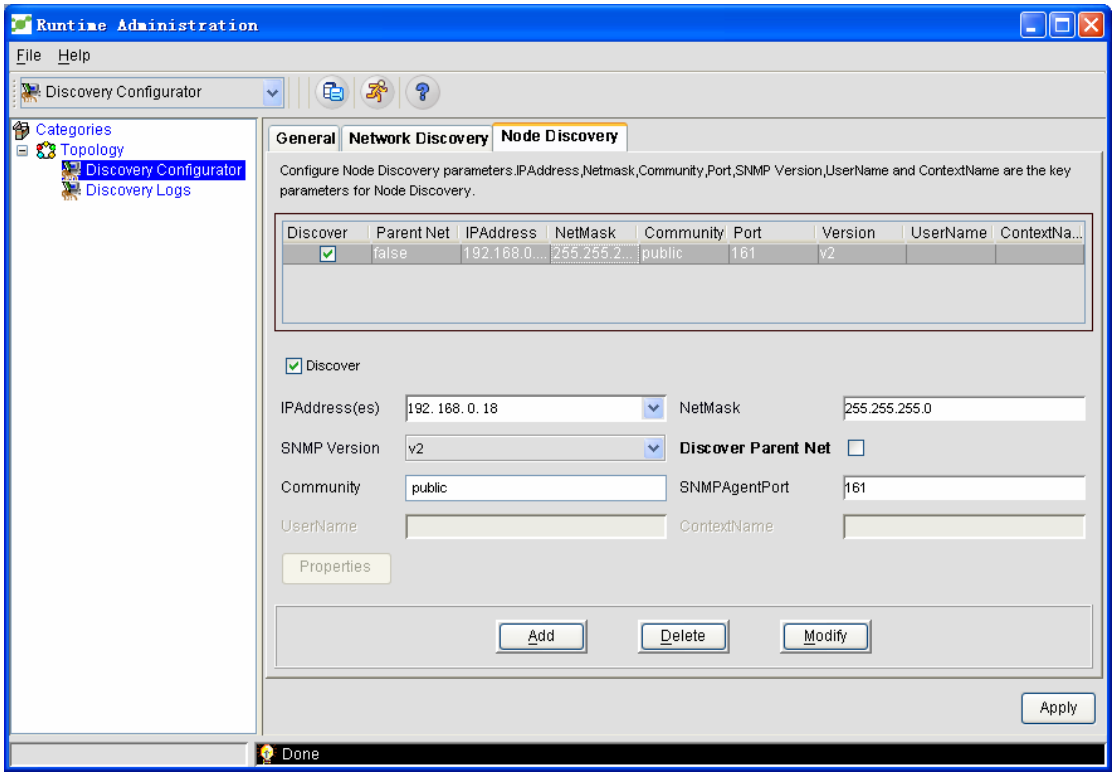
You can use the "Add" option to add or set more IP addresses.

1.3.2 Forbidding Node Discovery in the Local Network

For how to discover the nodes in a forbidden local network, see **Forbidding the discovery of the local network** in the regular parameter settings.

See the following figure to forbid the discovery of the local network and set the node discovery in this network.





Conduct the above-mentioned settings and you can find and add the node whose IP address is 192.168.0.18 (If you want to finde the whole network where this node is located, select the "Discover the father network" option).

1.3.3 Setting Parent Network Discovery for a Node

The "Discover the father network" option is enabled by default. This option can be used to enable the discovery of the father network of the selected node, that is, it is to enable the discovery of the other nodes of this father network. Users can cancel this option to forbid the discovery of the father network of this selected node. By default, only when this "Discovery" option is selected can this network be found.

1.3.4 Setting SNMP Device Discovery Based on the Community and the Agent Port

By default, when NMS finds the SNMP device, NMS finds that the community's character string used by the engine is **public** and the agent port is **161**. However, some devices in the network may use different ports and communities. In order to find these devices, the administrator can set the SNMP device discovery based on the community and the agent port through the following options.

- SNMP version: select the corresponding SNMP version from the dropdown box of the SNMP version (v1/v2/v3).
- Community: designate the community of nodes. The default community is **public**.
- SNMP agent port: designate the SNMP agent port of the node. The default agent port is port 161.

1.3.5 Setting SNMPv3 Device Discovery

To find the SNMPv3 device, you can follow the steps below:

- Select v3 in the **SNMP version** dropdown box. The **username** text box and the **context name** text box will be activated.
- Enter the username.
- Enter the context name.

Please refer to the SNMP settings to obtain more information about SNMPv3 device discovery.

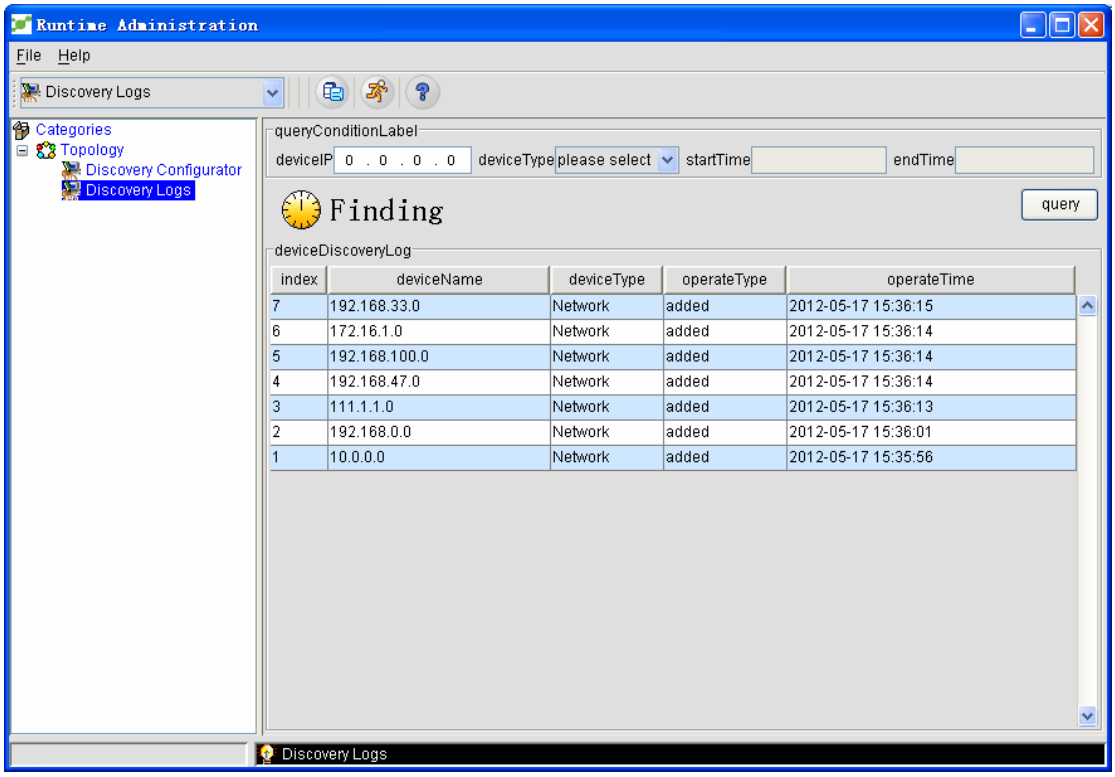
1.3.6 Forbidding the Discovery of a Node with a Designated IP

On the "node discovery" page, the "discovery" option is selected by default. To forbid the discovery of the designated node, you can cancel the "discovery" option and add the corresponding IP address and network mask. In this way these nodes will be forbidden to be found and added to the topology database.

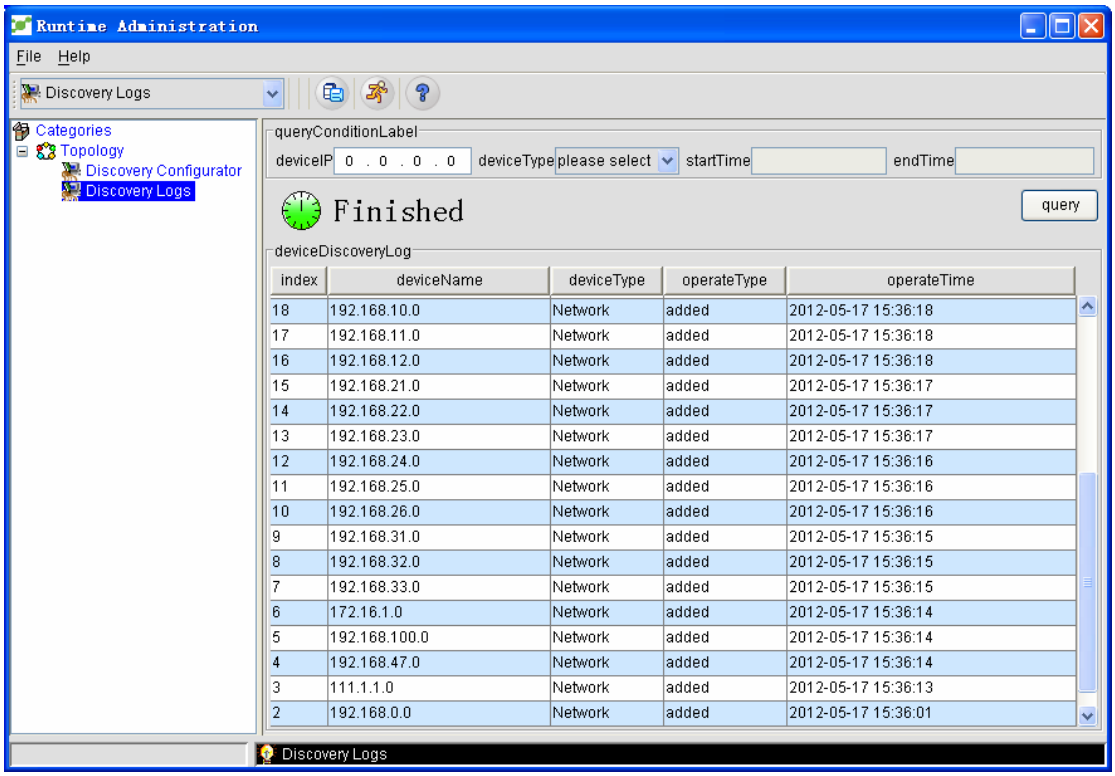
1.4 Discovery Log

1.4.1 Network Discovery Status

After configuring **Node Discovery**, please click **Apply** to automatically transfer to the **Discovery log** page. The detected network and equipment will appear in the log. If there is network discovery, the log page makes the being-detected status available, as shown in the following figure.

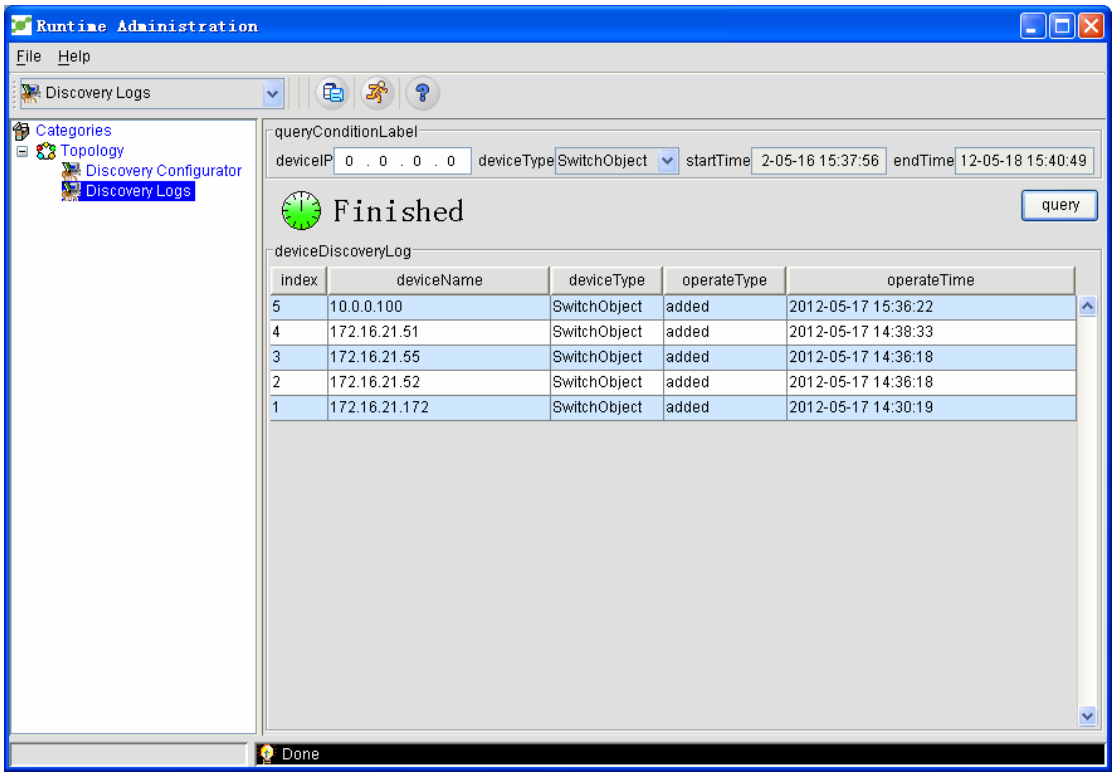


When all network discoveries are done, the log window makes available the **Discovery Done** status. See the following figure.



1.4.2 Discovery Log Query

If you want to query the device discovery and delete the logs, you can query them through this function. You can query the required logs according to your condition. If you has not set your condition, all logs will be queried.



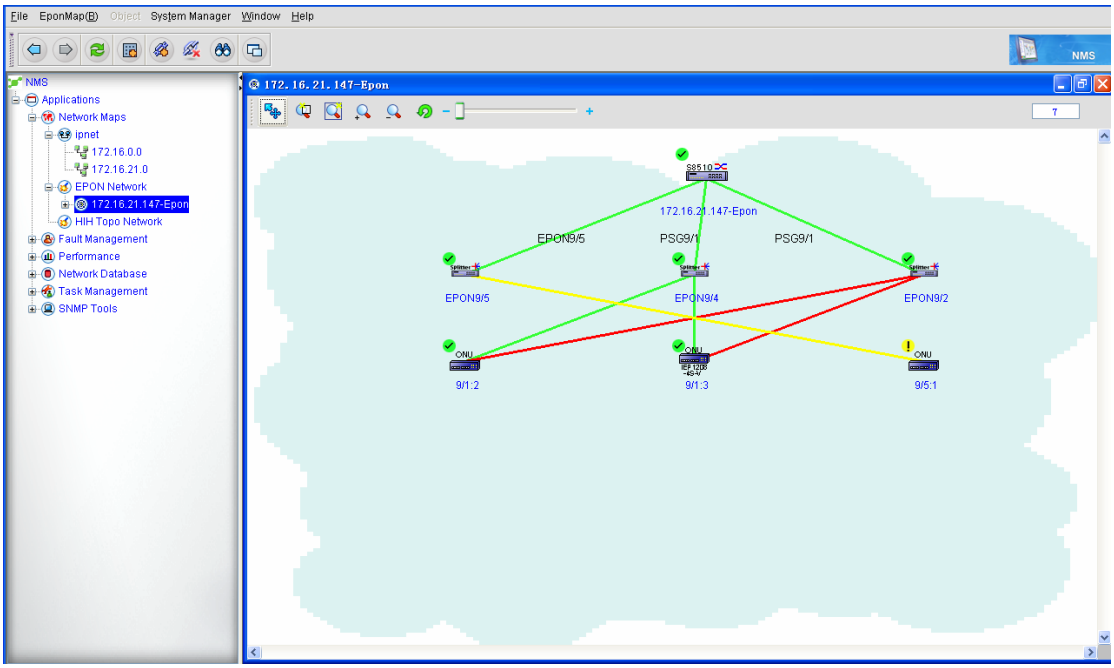
1.5 Precautions

Sometimes, a device is already in the IP network or the EPON network but cannot be rediscovered or discovered during the discovery operation.

In this case, the deletion of a device in the IP network would not lead to the deletion of the device's node in the EPON network. On the contrary, the deletion of a device in the EPON network would lead to the deletion of the device’s node in the IP network.

2. Map Management

Map management is also called as topology management, including IP topology management, EPON topology management, and hand-in-hand topology management. See the following figure:



The shortcut menus are listed below:

 Back: Click it to go back to the previous page.

 Next: Click it to go to the next page.

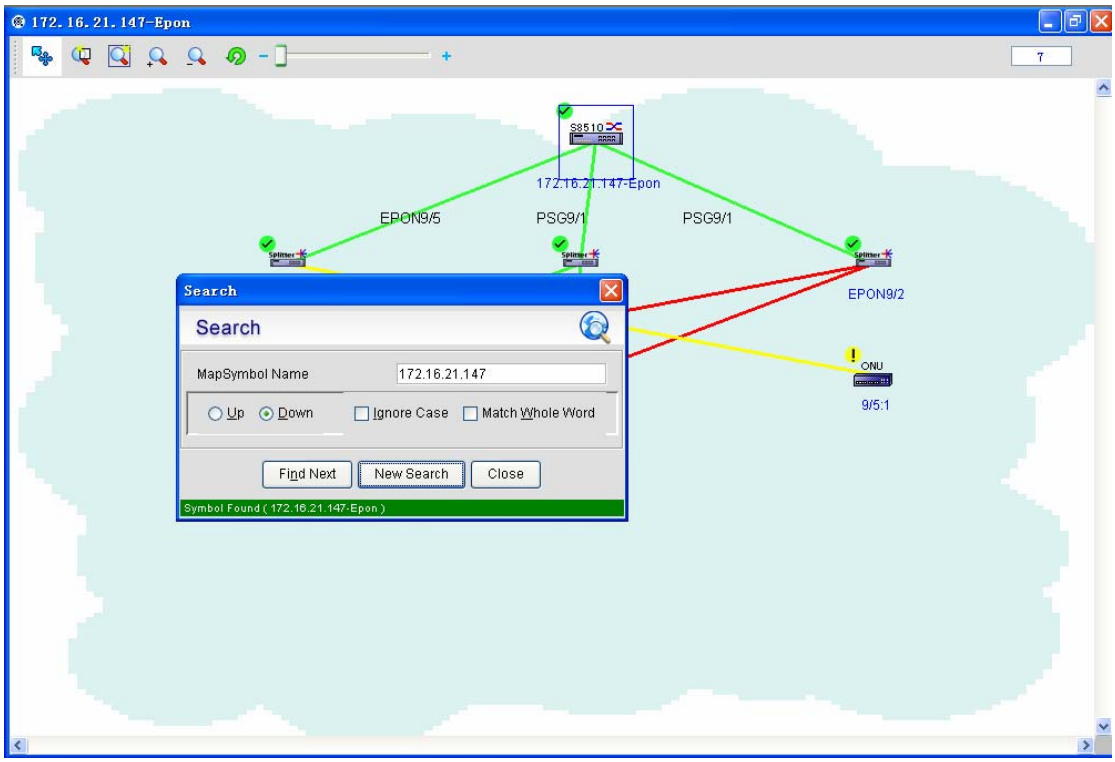
 Refresh: Click it to reread and display the topology in the database.

 Add: This symbol will be explained later.

 Add a link: This symbol will be explained later.

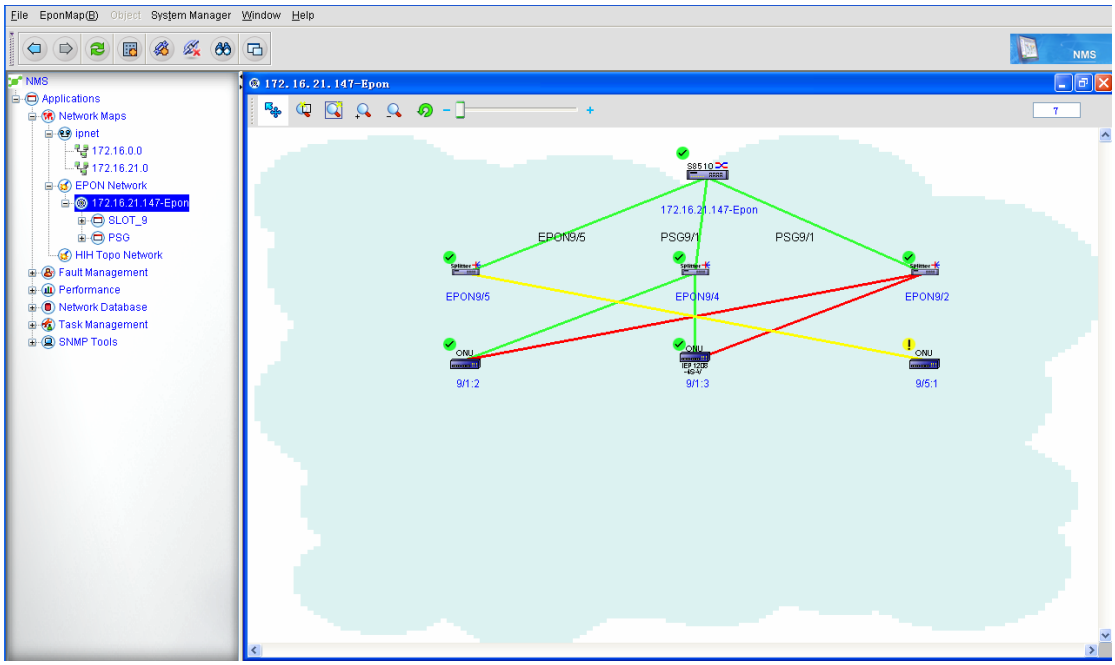
 Delete a link: This symbol will be explained later.

 Device detection: For example, you can click it to look for the icon of "172.16.21.147", as shown in the following figure:

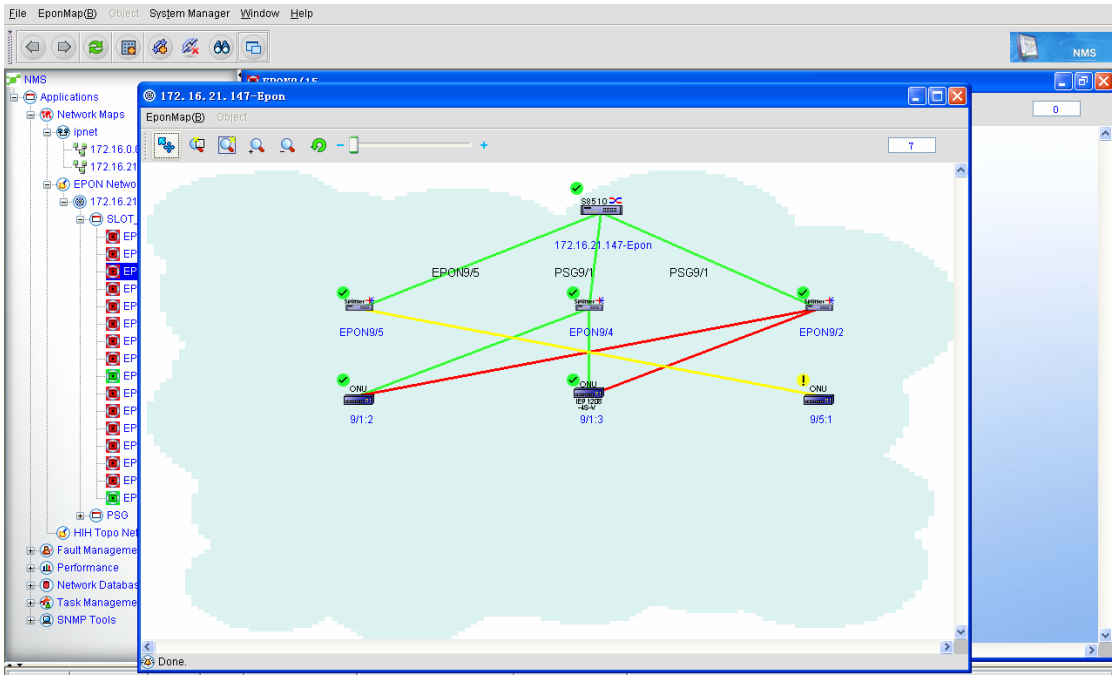



Segment the current window: The result of clicking it is shown below:

Before the window is segmented:

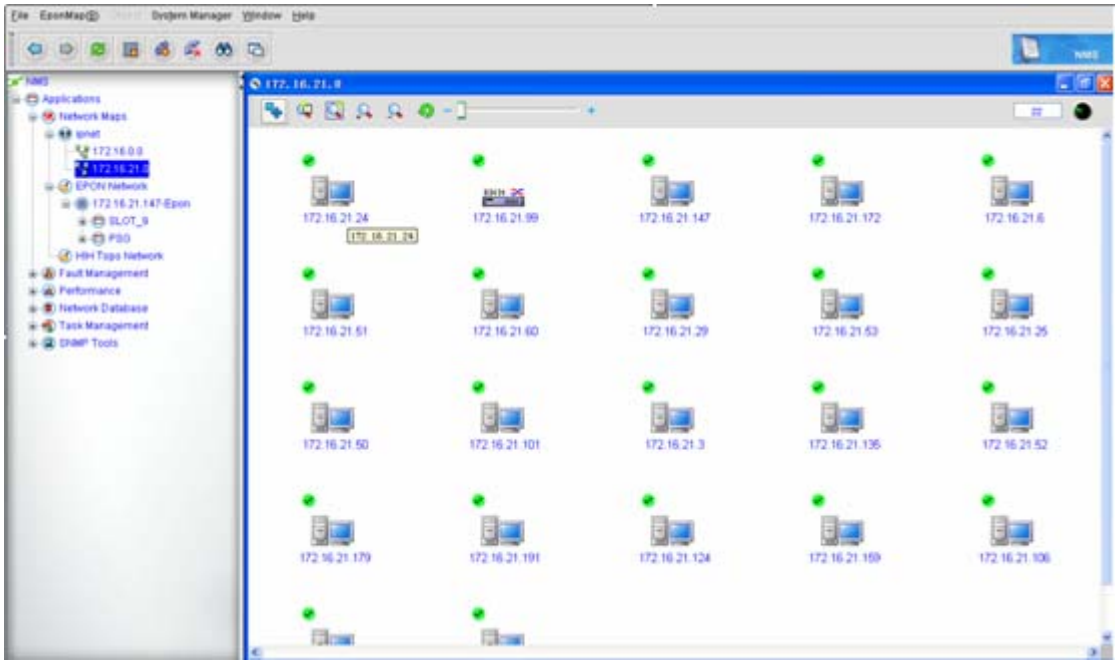


After the window is segmented:



2.1 IP Topology Management

Unfold the **IP Network** node to open the IP topology management page. See the following figure:



The IP network topology consists of the following parts:

- Title bar

The title bar shows the current network, such as 172.16.21.0.

- Tool bar

The tool bar shows in the following figure:

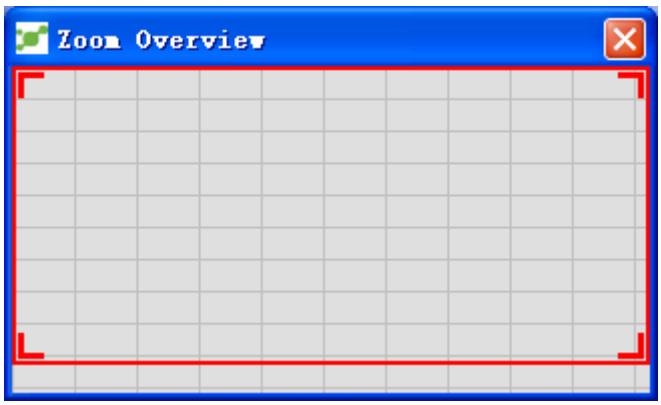
 Select mode: There are two modes available for choice: the anchor mode and the non-anchor mode.

The anchor mode: the detected device icons are forbidden to move in this mode.

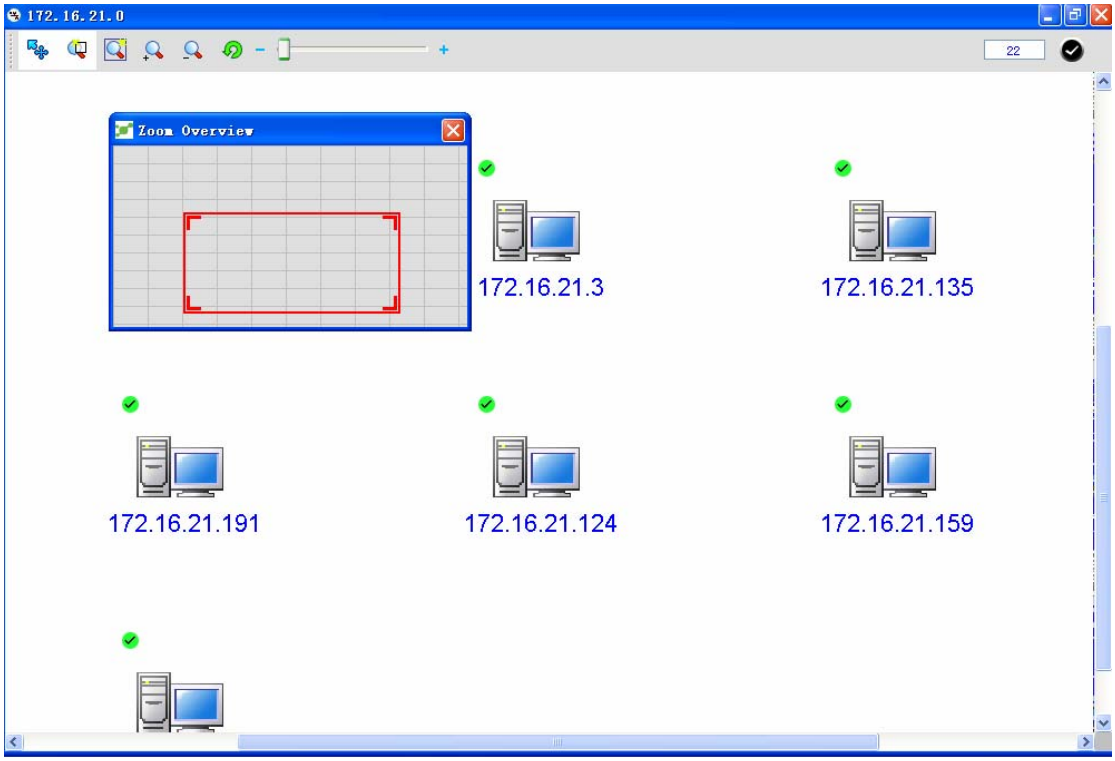
The anchor mode: the detected device icons are allowed to move in this mode.

If you click the "Select mode" shortcut button in non-anchor mode, the non-anchor mode changes to the anchor mode. So it is with the anchor mode.

 Zoom: Click it, and the zoom preview is shown in the following figure:



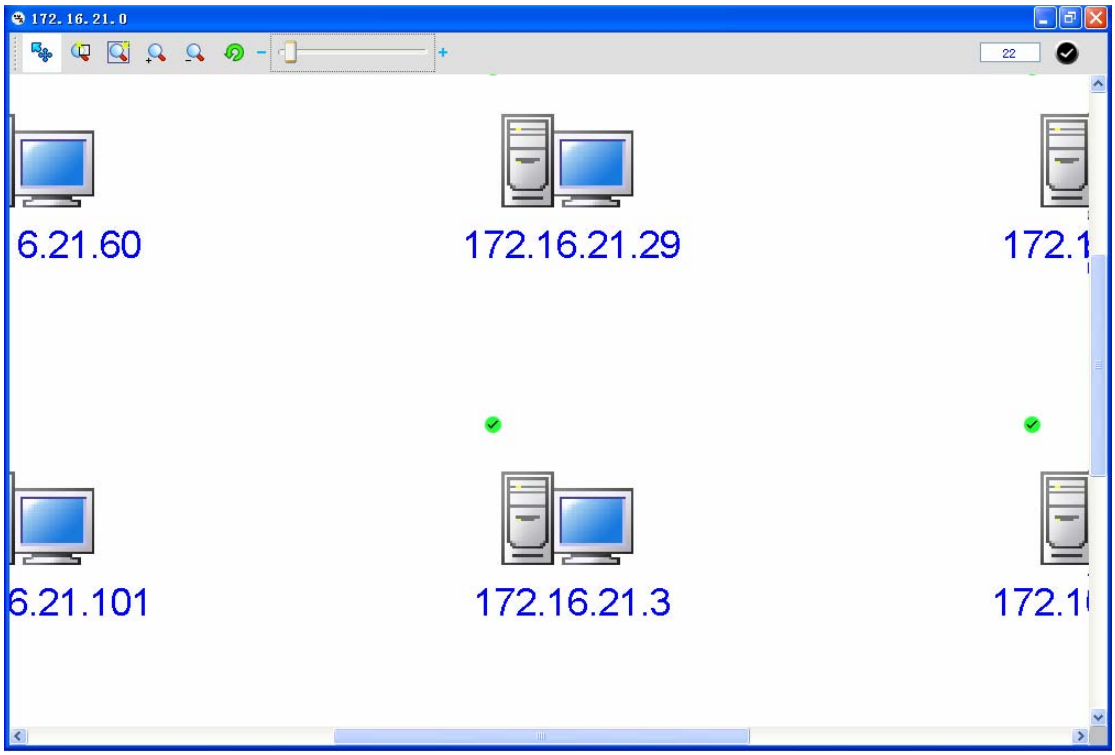
Put the cursor on the foursquare of the **Zoom** button and you can change the size of the zoom window. See the following figure:



Zoom mode: Click it and then you cannot choose a device icon and the device icon can only be zoomed out. You can click to select the zoom mode. Zoom out: Click it to enlarge a device icon.

Zoom in: Click it to reduce a device icon.

Icon zoom rate: When you move the slide, you can enlarge or reduce the size of a chosen device icon. See the following figure:



Resume: A device icon can be removed to another place, but it can go back to its original place if you click the **Resume** button.

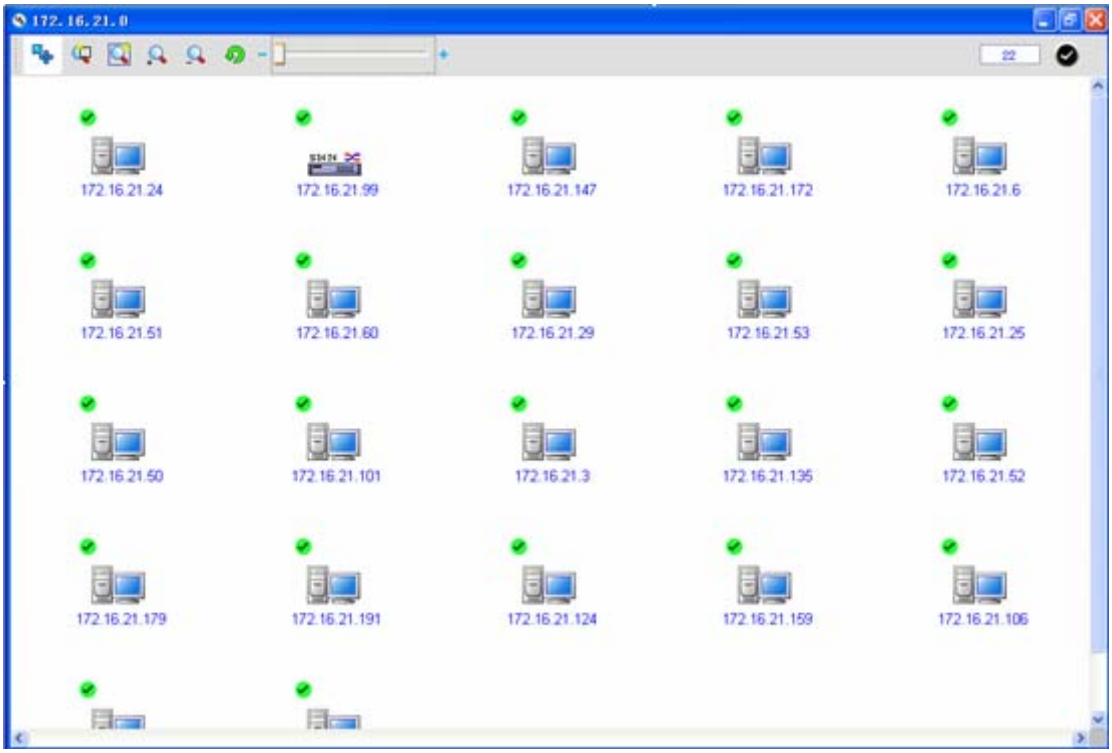
◆ Search state:

The search state tells users the number of currently searched devices and the state of the radar detector. The following figure shows that 14 devices are currently being found and the search is still going on.

The following figure shows that the search is already done and 17 devices are found.

◆ Search display zone:

The search display zone presents the currently detected IP topology. See the following figure:



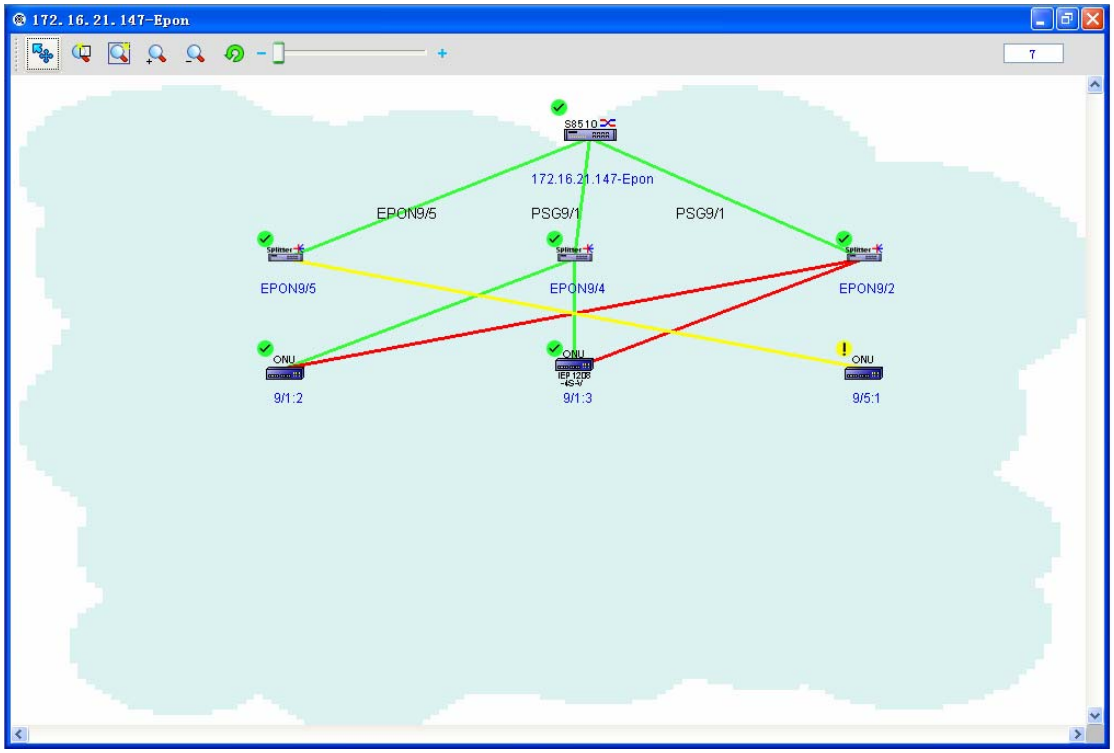
Means the device is currently working normally.

Means the device is not under work.

After you choose a detected device icon, you can manage this device.

2.2 EPON Topology Management

Unfold the **EPON Network** node to open the EPON topology management page. See the following figure:



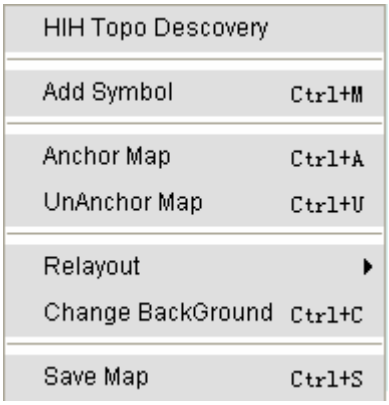
When the EPON topology is opened, you may find it is similar to the IP topology. Here gives a detailed description of the EPON topology and its operations.

In the EPON topology, you can find two links between OLT and optical splitter, one being green and the other red. They relate with PSG and CSG (for details, please refer to related documents).

PSG is adopted between OLT and optical splitter. When the main link (represented by the green line) cannot work normally due to troubles, the standby link (represented by the red line) will turn to work immediately.

CSG is adopted between optical splitter and ONU. It also adopts link redundancy, that is to say, the standby optical splitter will turn to work in time if one optical splitter has trouble.

If you right click the EPON network icon, the operation menu will pop up, as shown in the following figure:



The specific operations will be described below:

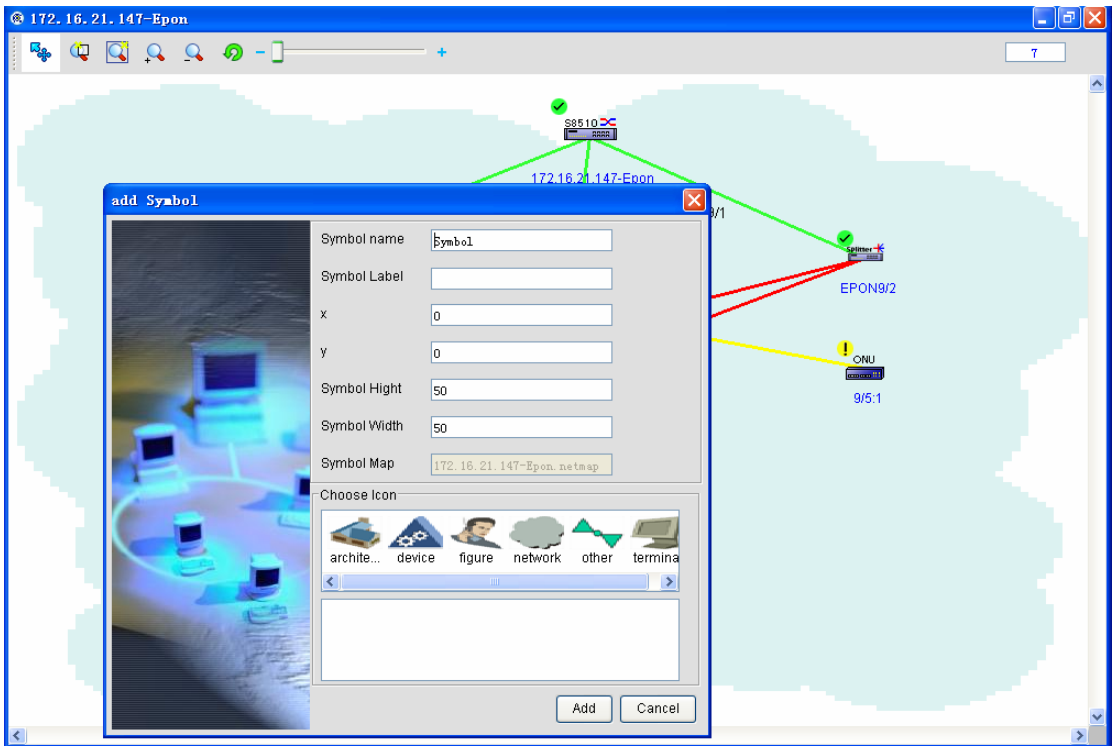
◆ Hand-in-hand discovery

For details, see section "Hand-in-Hand Topology."

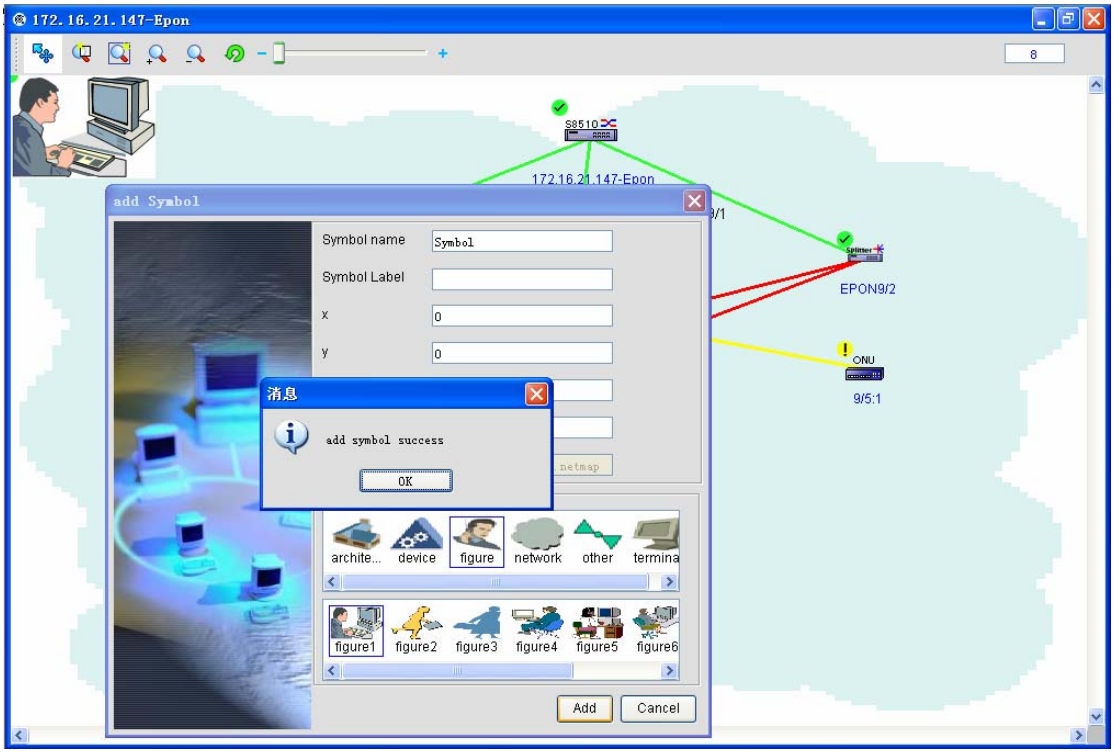
◆ Add an icon:

To add an icon to the topology, do as follows:

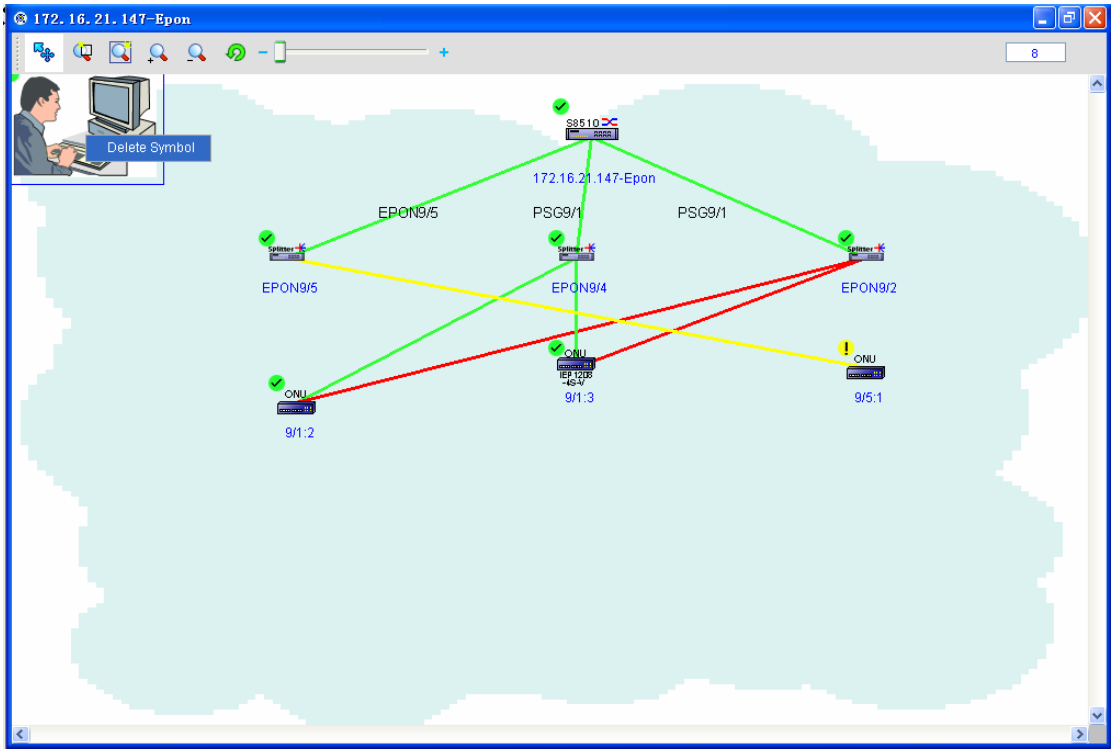
If you click **Add an icon** or the shortcut button  , the following page appears:



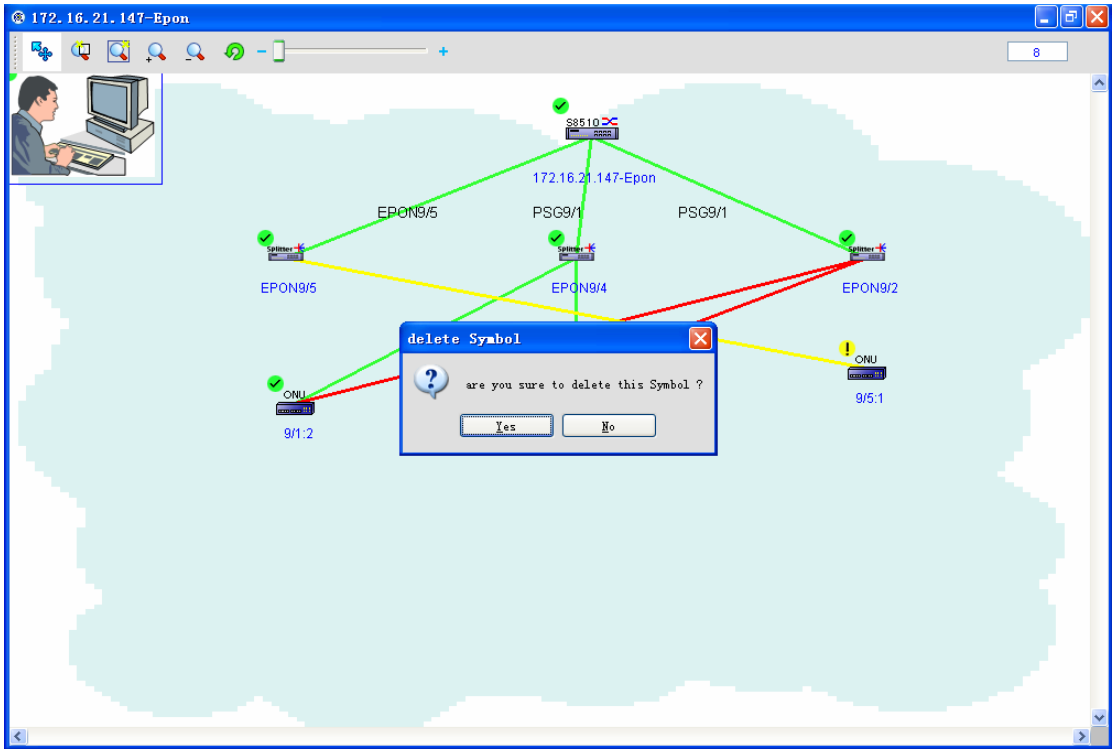
Then you can choose a proper icon and click the **Add** button. The chosen icon is added to the topology. See the following figure:

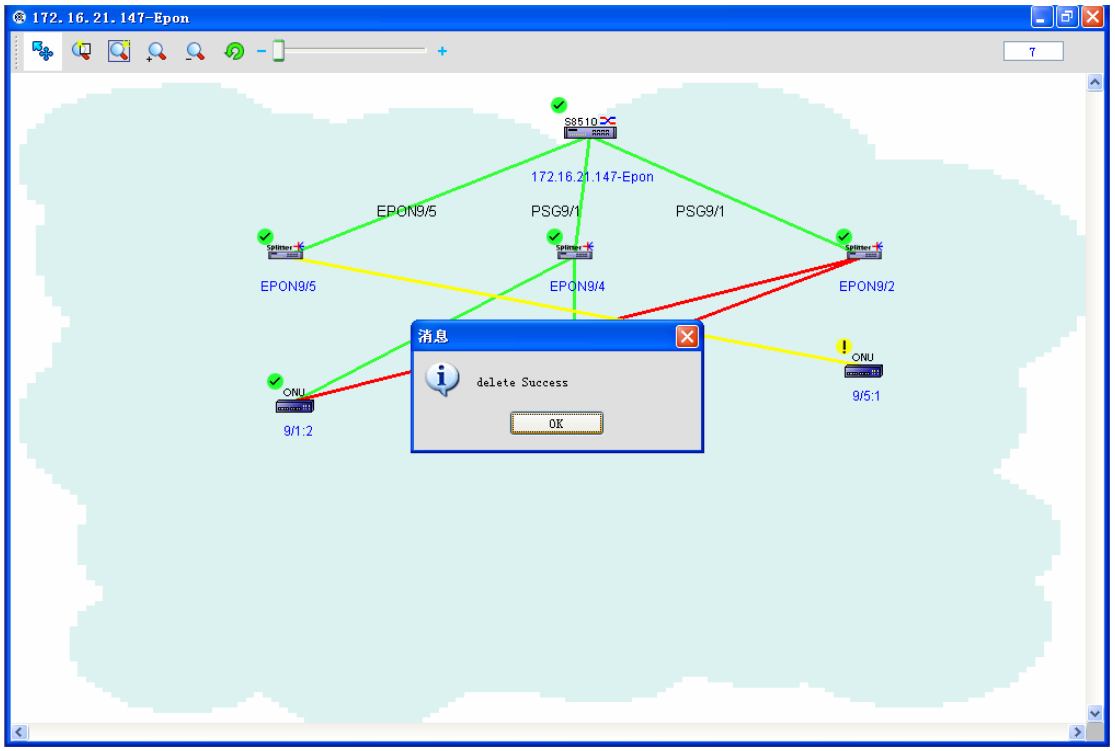


When you want to delete an icon, first choose an icon and right click it, as shown in the following figure:



And then select **Yes** in the dropdown box. Finally the icon is deleted. See the following figure:

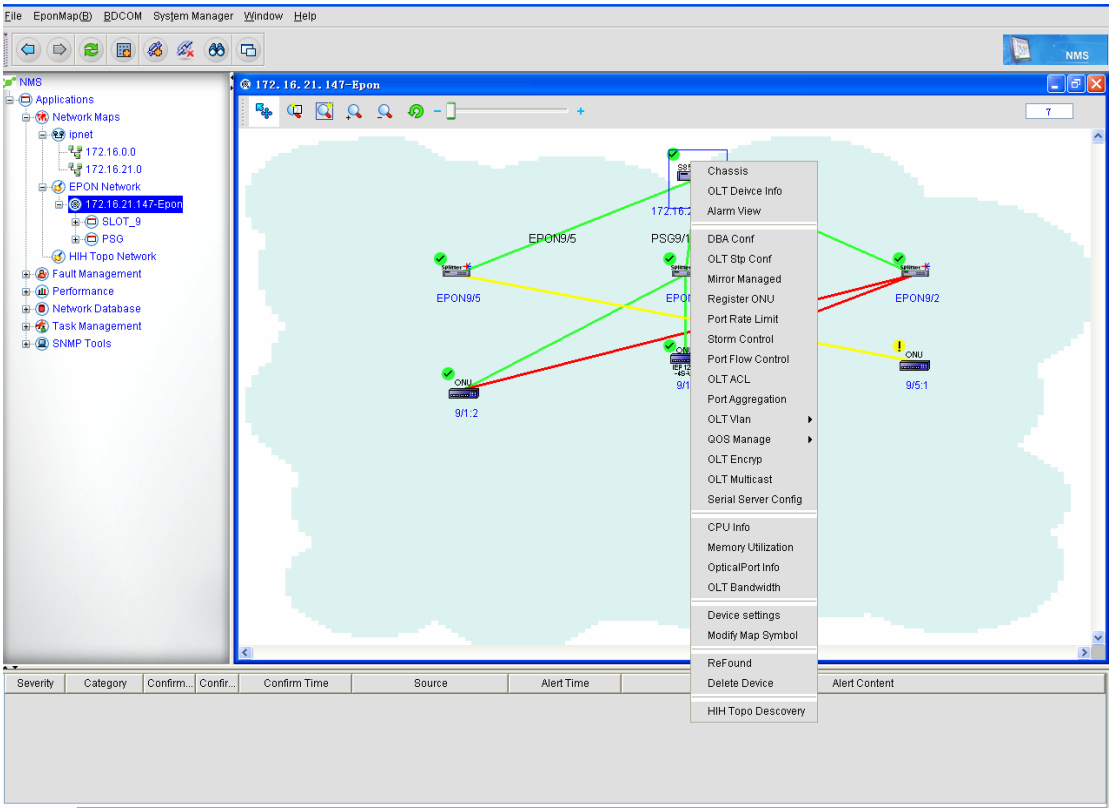




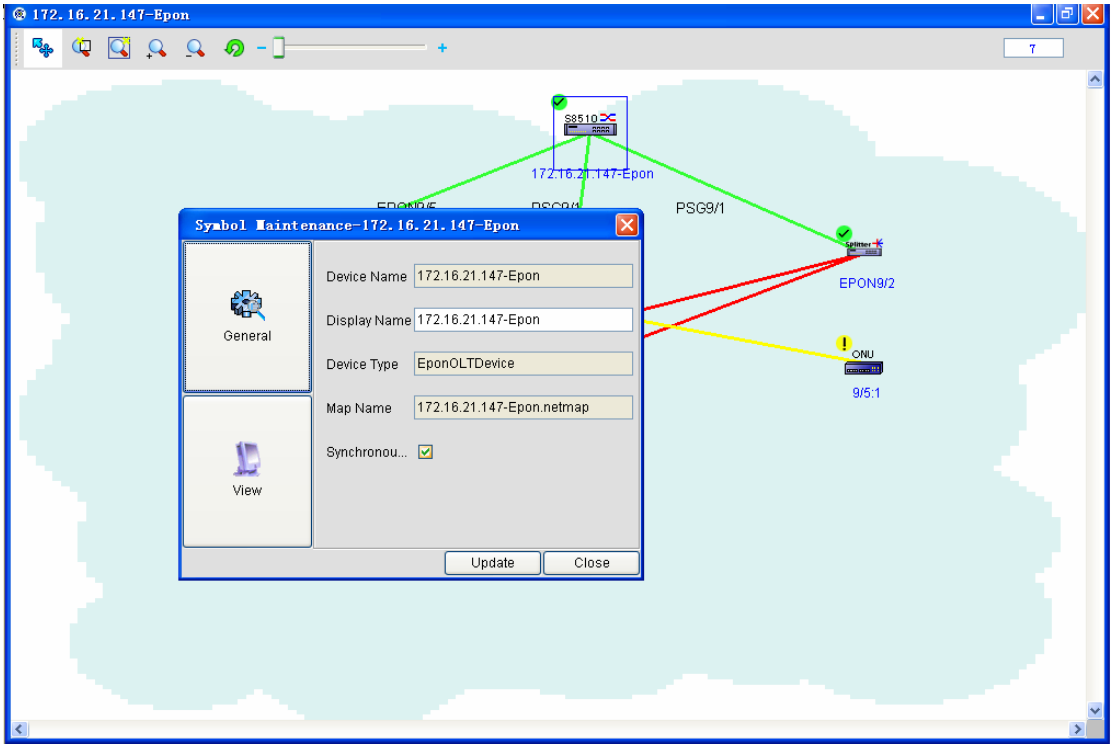
◆ Icon maintenance

The maintenance of the EPON network icon mainly refers to the changes of the widths, heights, positions, pictures and names of the related EPON devices in the EPON network topology. The maintenance of OLT, optical splitter or ONU is similar to that of EPON network icon. The following is an example based on OLT. Right click the OLT icon. The right-key menu appears.

Select **Modify Map Symbol**, as shown in the following figure:

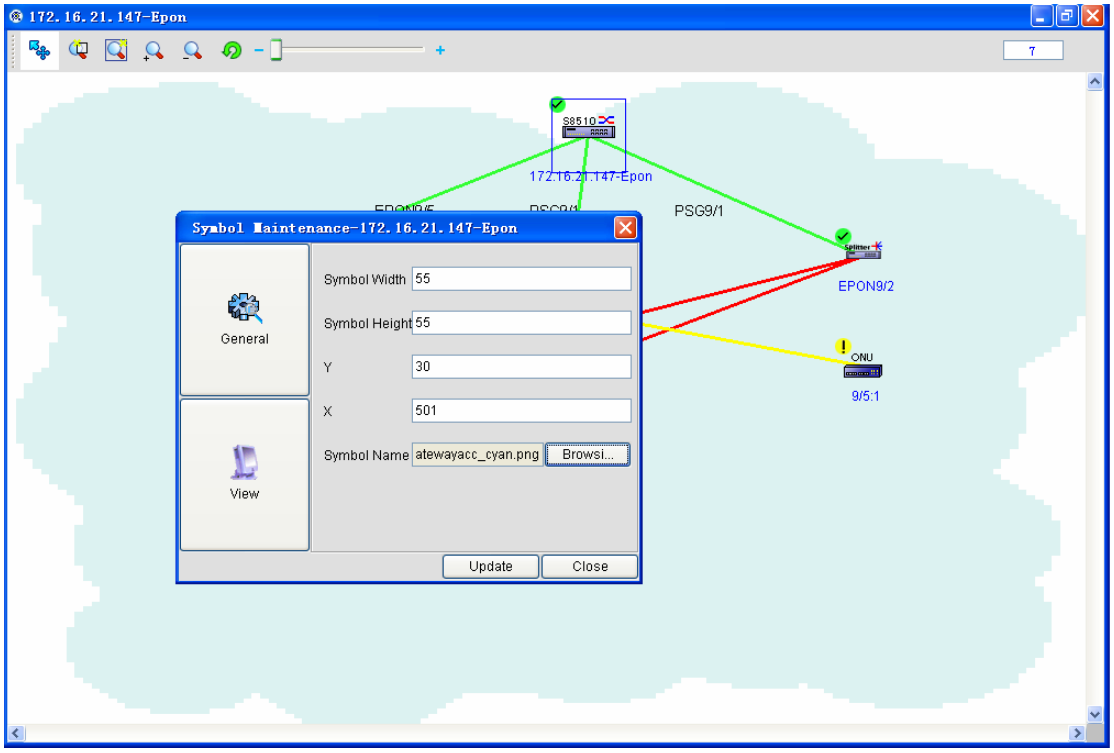


The **Maintain icon** page appears, as shown in the following figure:



In the **Common** option, the administrator can know the name and type of a device, the display

name and the current topology, among which the display name system shall support the **Edit** operation. In the **Show** option, the width, height, coordinate and name of an icon are included. All of them support the **Edit** operation.



After you set related data, click **Refresh** to refresh an icon.

◆ Anchor topology

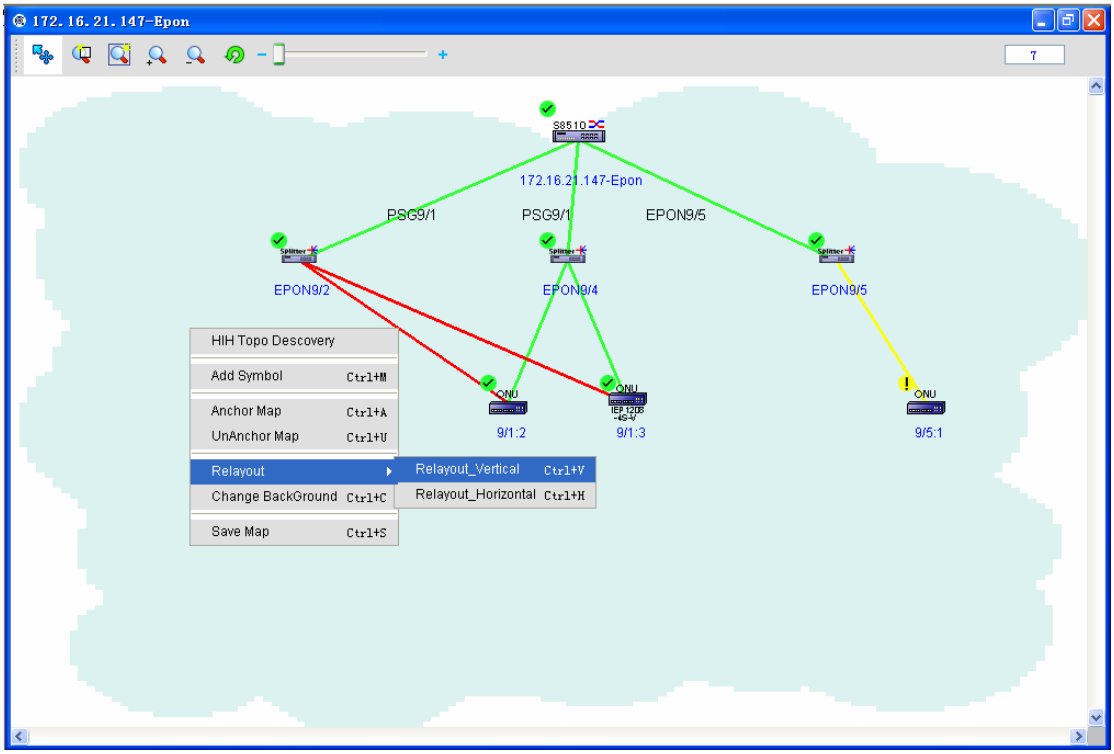
The anchor topology and cancelling the anchor are used as a pair. The anchor topology means that any icon in the current topology cannot be moved. In the menu, you can click **anchor topology** or  on the toolbar and then the topology is anchored.

◆ Cancel anchor

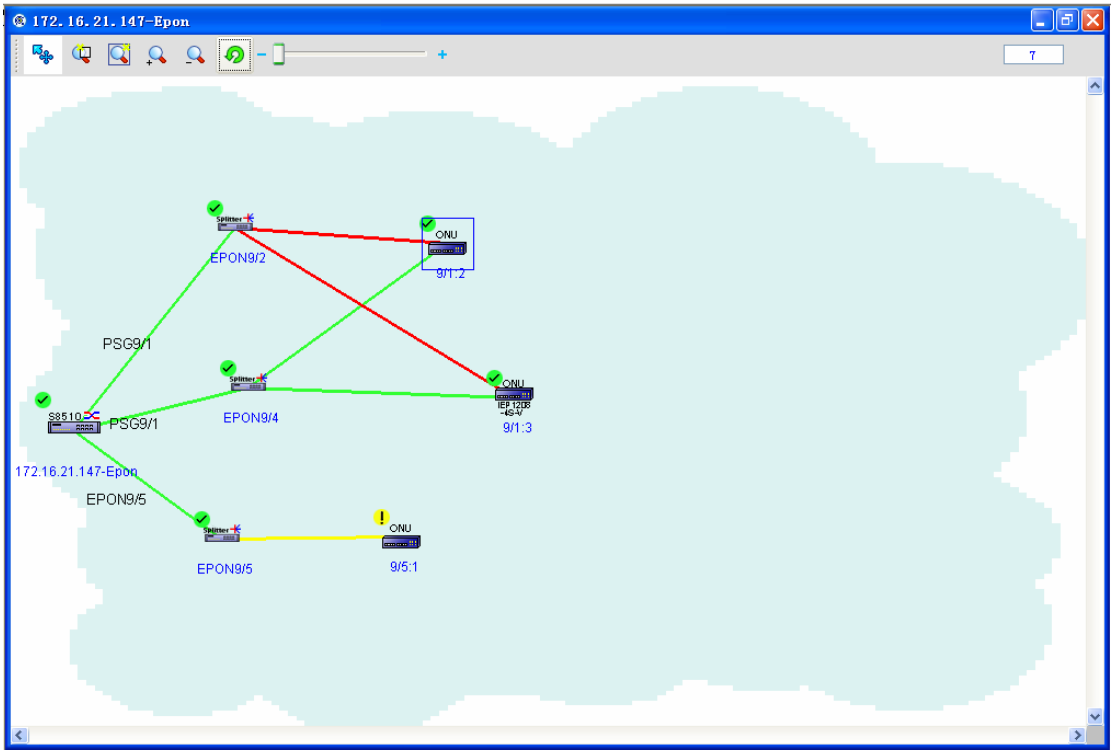
When you know to anchor a topology, it is very easy for you to cancel the anchor. In case a topology is anchored, you can click **cancel anchor** or the shortcut button  to cancel the anchor.

◆ Re-plan

Re-plan includes the vertical plan and the horizontal plan. See the following figure:

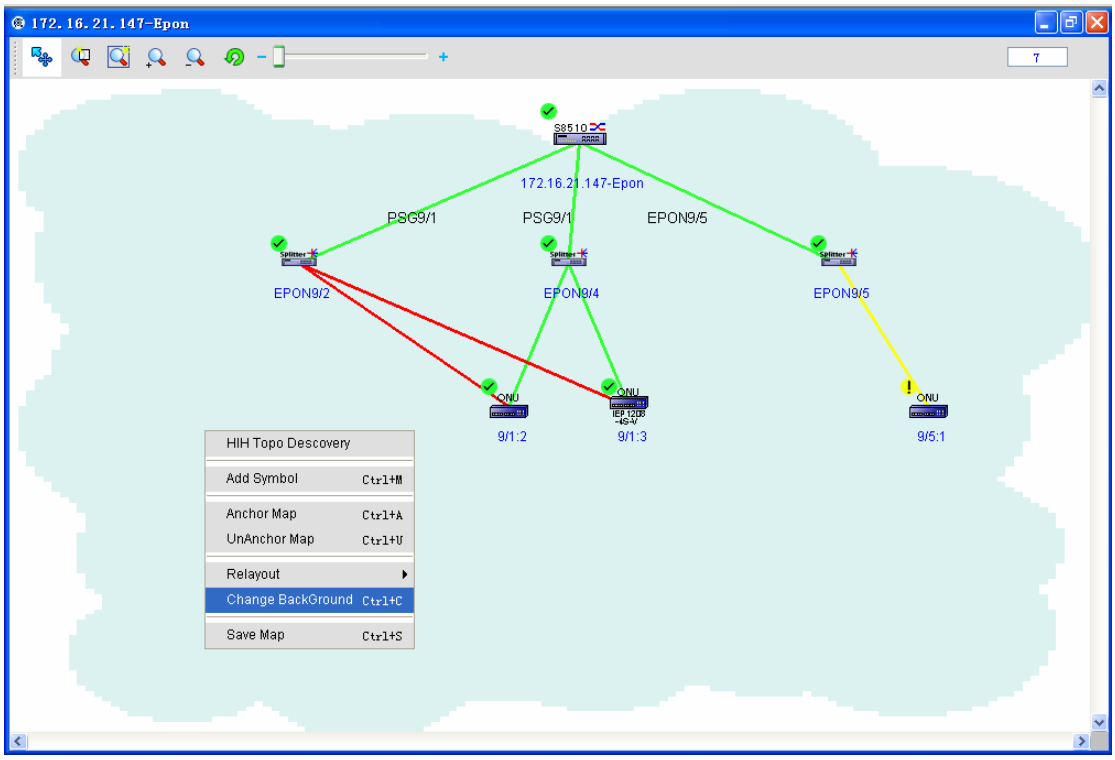


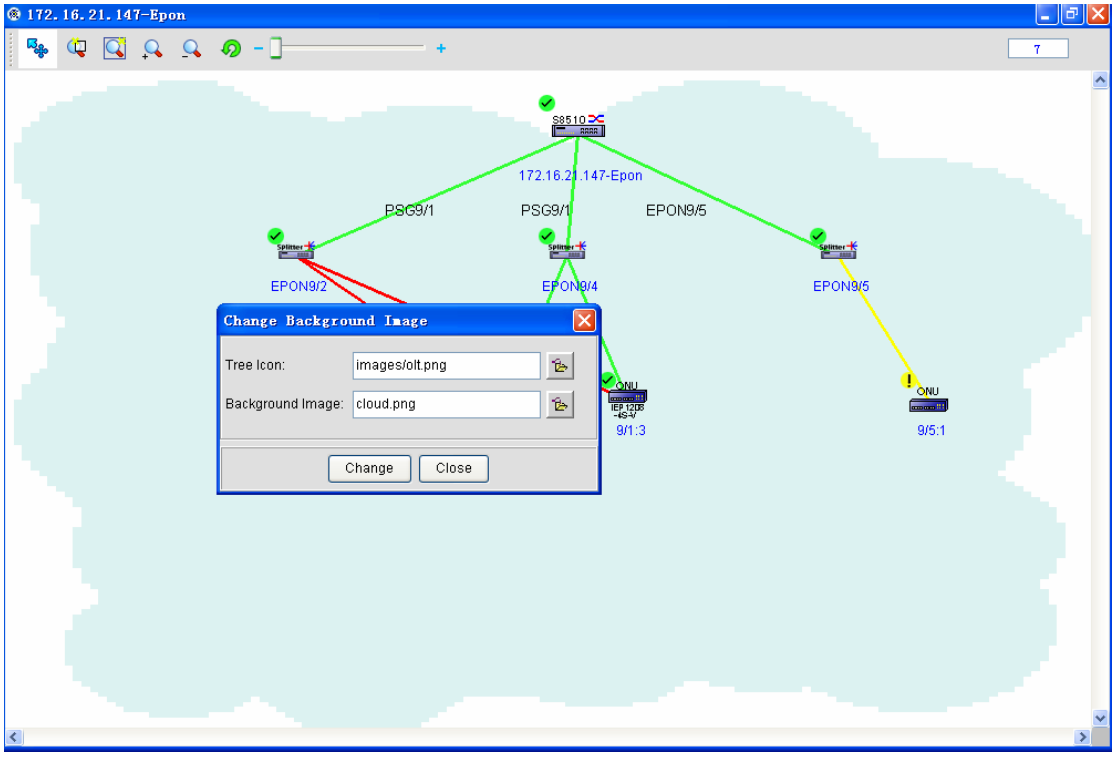
Here take the vertical plan as an example. The horizontal plan is similar to the vertical plan. It is noted that the completion of re-plan means the reordering of PON interfaces.



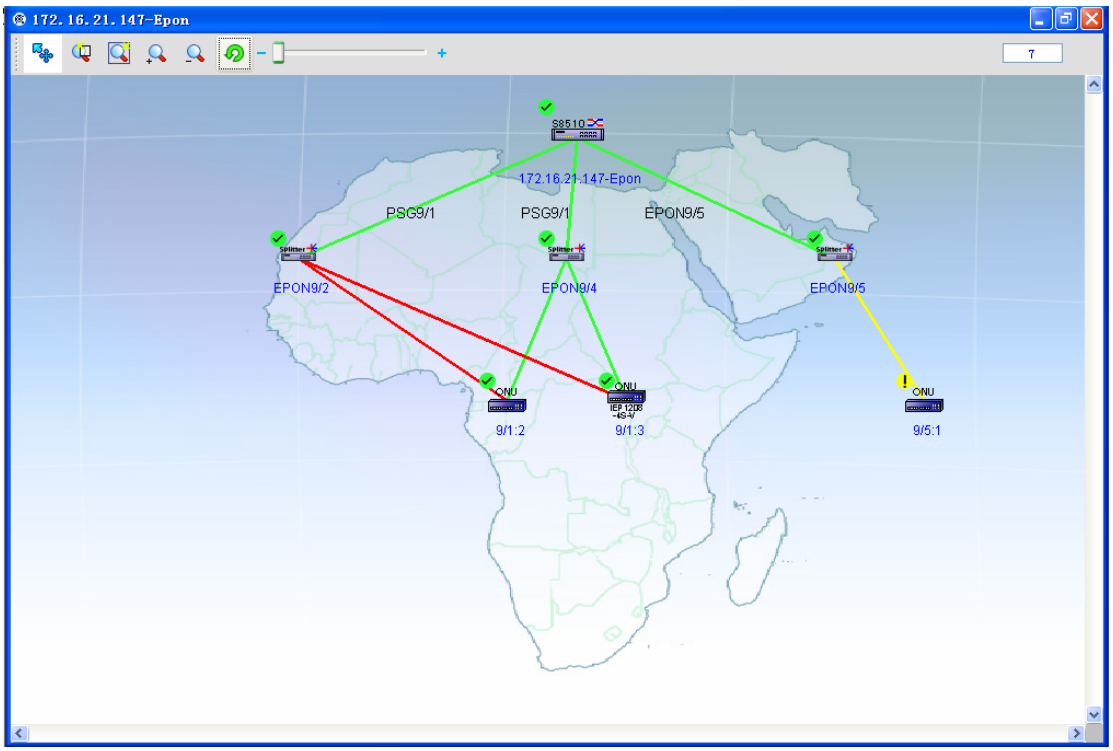
◆ Change background

The **Change background** operation is to change the tree icon and the background picture. Before the background is changed, it appears as the following figure:





After the background is changed, it appears as the following figure:



Note:

If you want to add more customized pictures, you can store related pictures at the following directories:

Installation directory\images\TreeIcons\ (for the tree node icons)

Installation directory\images\MapImages\ (for the background pictures)

◆ Save image

Save image means to store to the database the state of the EPON topology when it is closed, so that it resumes to the previous state when it is opened again.

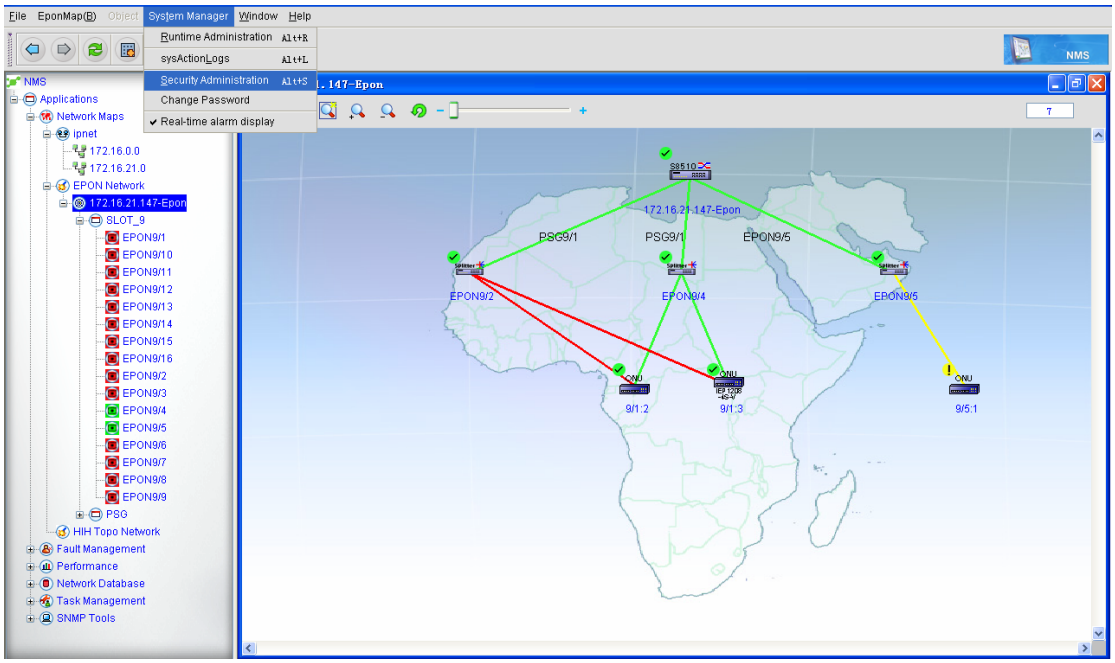
3 Security Management

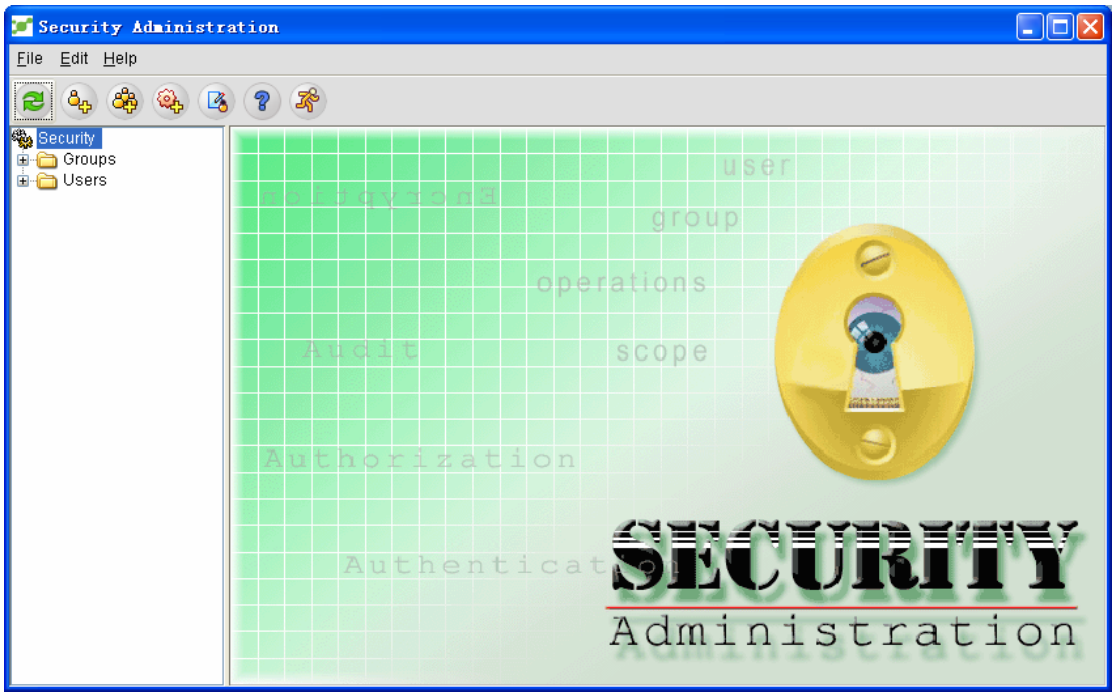
Security Management helps the system administrator to carry on the granular permission management based on user and user group.

The provided security management tasks can be divided into user definition and group definition, as shown in the following table:

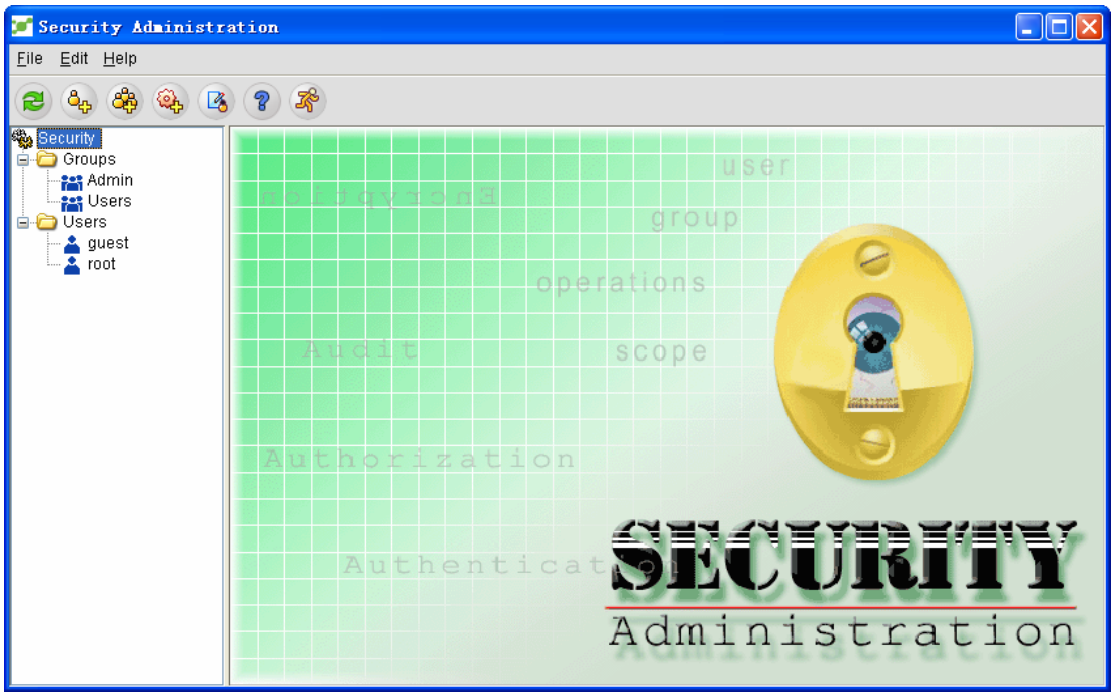
User Definition	Group Definition
Add users	Add groups
Add users to a group	Allocate users to a group
Set user description	Allocate operations for a group
Modify user's password	
Assign authorization to users	
User audits	
Delete user	
All user lists	

Click **System Management -> Security Management**, and the administrator can open the **security management** page, as shown in the following figure:





If you click the **group** node and the **user** node, all groups and users will be displayed.



3.1 Defining a User

3.1.1 Adding a User

The system administrator can follow the following steps to add a new user.

On the **security management** page, the administrator can use one of the following methods

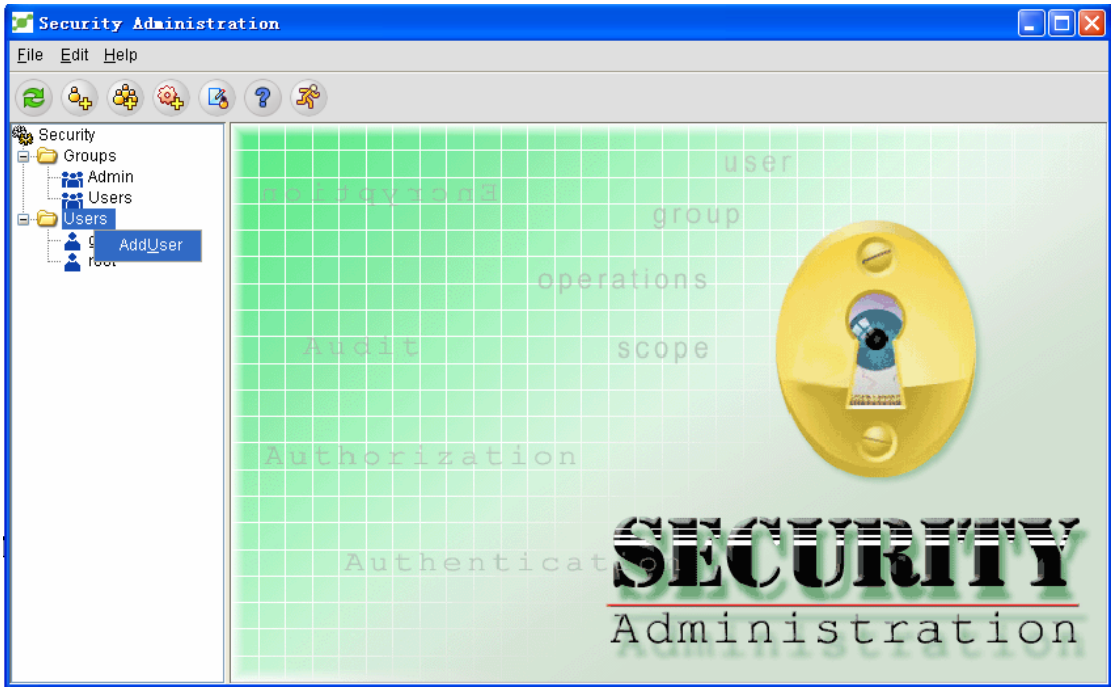
to open the **Add the user guide** window:

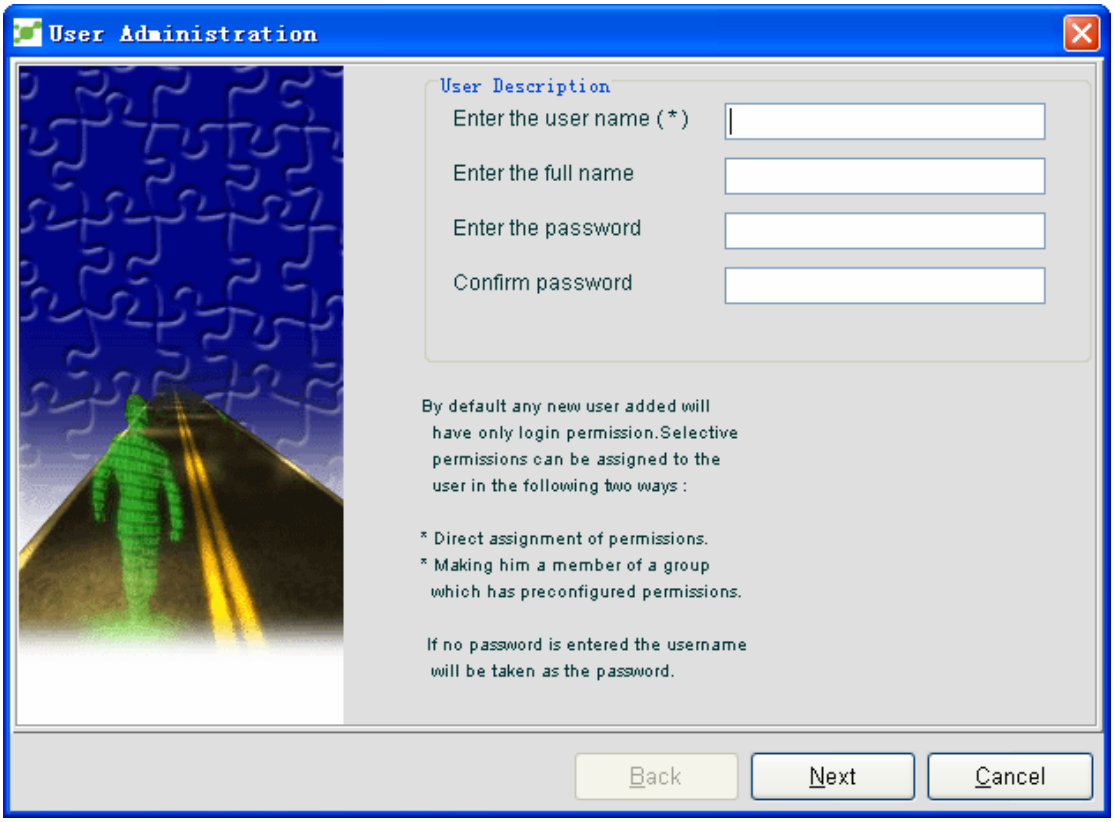
1 Click **File -> New -> Add user**.

2 Click the **Add a user** icon in the toolbar.

3 Right click the **User** node in the left tree and then choose the **Add a user** option.

The **Add the user guide** window is shown in the following figure:



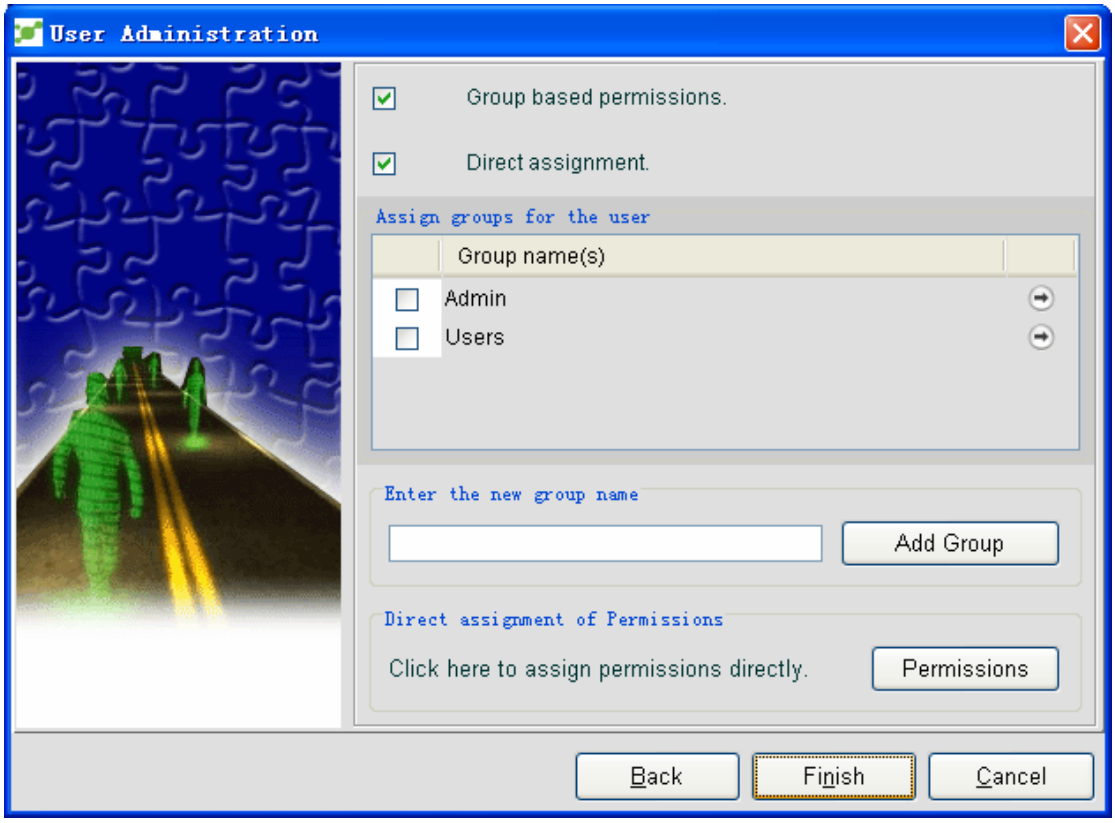


	Remark: When the administrator adds a new user in the **security management** window but does not set a password for it, the system will use the username as the password.

Enter the username and password to the corresponding textbox in the **Add the user guide** window and click **Next**, and then another window appears, as shown in the following figure:

This window shows the expiration date of the user account and its password. In default mode, both of them are 0, which means the user account and the password never expire. If the administrator needs to set a period for the user account and the password, he shall deselect the **Account ID never expires** checkbox and the **password never expires** checkbox, and then enter the days in the corresponding textbox.

After setting the expiration date for the account and the password, click **Next** and enter the last window of **Add the user guide**, as shown in the following figure:



The system administrator can distribute users the group permission or assign users the operation permission.

The administrator can enter the new group name in the **Add a group** textbox and then click the **Add a group** button to designate a new group for users.

The administrator can distribute users the corresponding group by clicking **group-based permission** and the corresponding group name. The administrator can browse the group's authorization operation by clicking .

Choose **Direct distribution**, and then the administrator can designate the authorization operation to users directly without adding users to any group. Click the **Permission** button in the **Direct distribution of the access permission** faceplate to pop up the **Designate the permission** window. The system administrator can designate the authorization operation to users.

After distributing users to the group or designating the authorization operation to users, the administrator click **Over** to confirm the above-mentioned settings. The newly-added users will be displayed under the **User** tree node.

Note: If the administrator wants some alteration, he or she can click **Back** to return to the previous window for necessary alteration before **Over** is clicked.

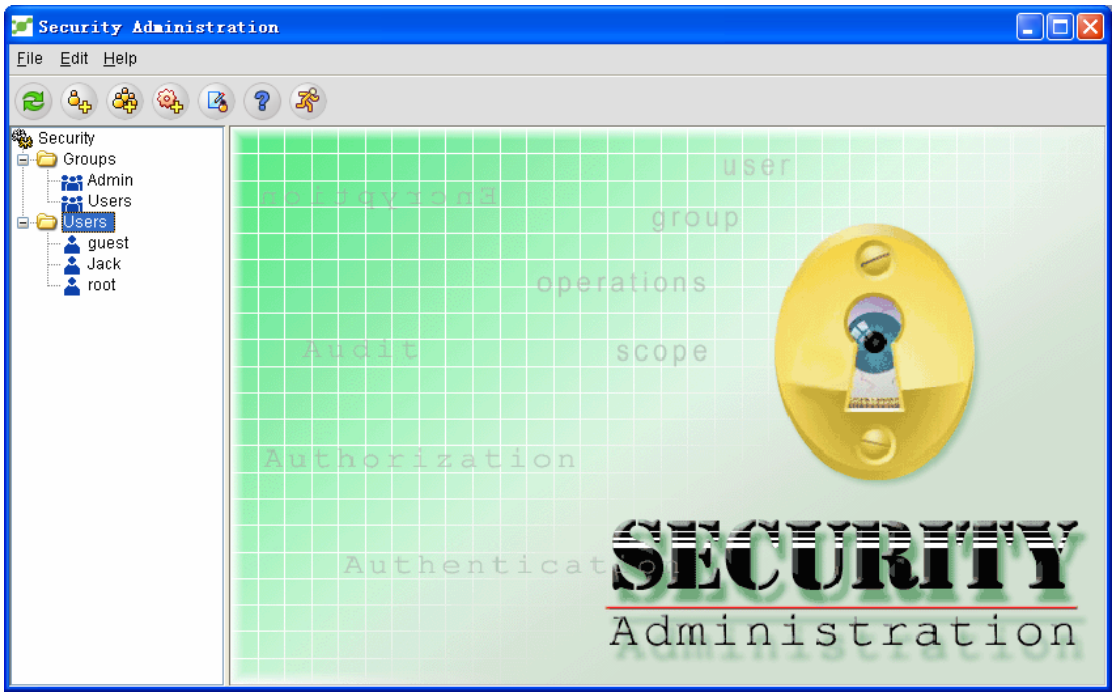
The system administrator can provide new users the following items: username, group, password and password confirmation, and their durations. If the administrator clicks the **Everlasting Password** checkbox and the **Everlasting Account** checkbox, the password and the account will never expire. If the administrator deselects the two checkboxes, he or she should set the efficient period for the password and the account. After the period, the password and the account will take no effect again.

If the username is already existing, the system will give an alarm information, notifying users cannot be created.

3.1.2 User Settings

3.1.2.1 Browsing all user lists

If you select the **User** tree node in the security management window, all users will be displayed in the sub-node, as shown in the following figure:

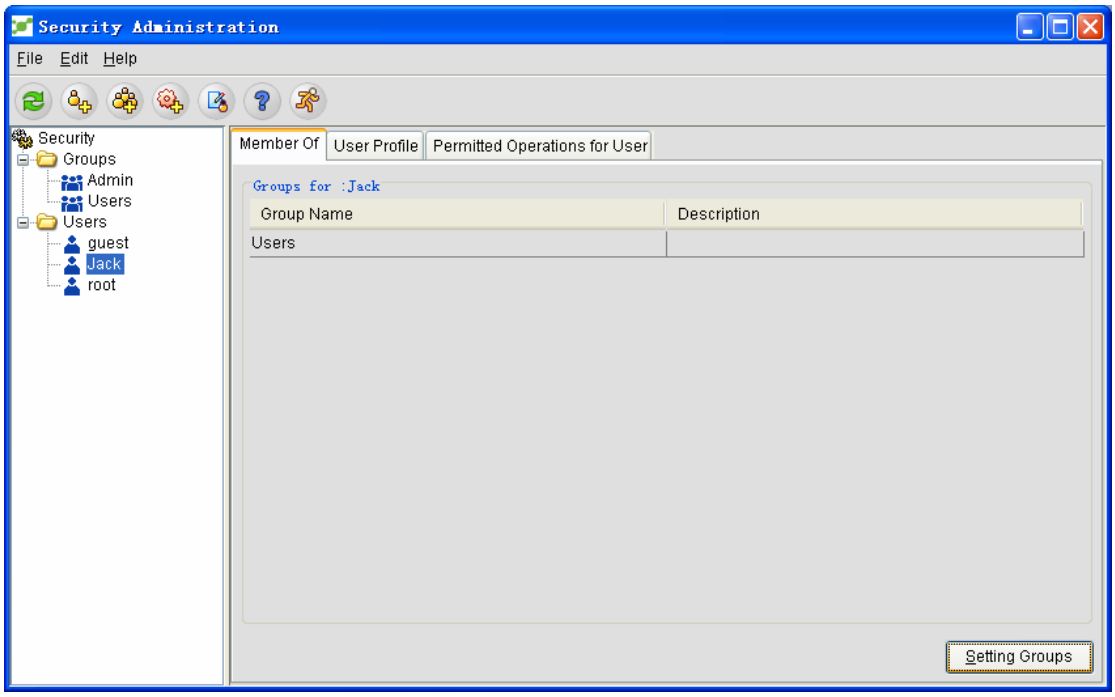


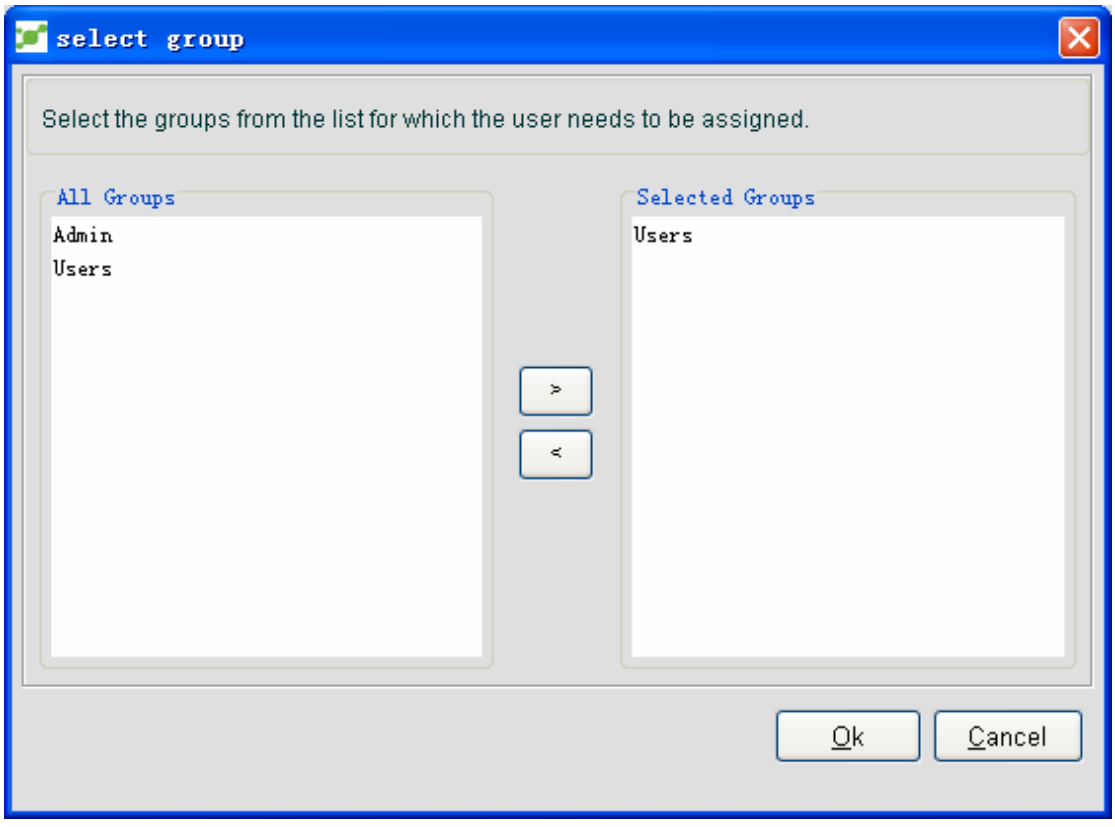
3.1.2.2 Distributing a group for users

The authorization service provided by the NMS module can limit users' access permission to the objects and instances. For example, users are limited in the authorization and can access only some specific devices.

The system provides the group-based authorization, and the administrator designates the corresponding groups to users according to actual needs. Thus users can be managed through the group authorization. The detailed procedure is shown below:

Select specific users in the **User** tree node, open the **User's group** attribute page, click **Set a group** and open the **Select a group** window, as shown in the following figure:



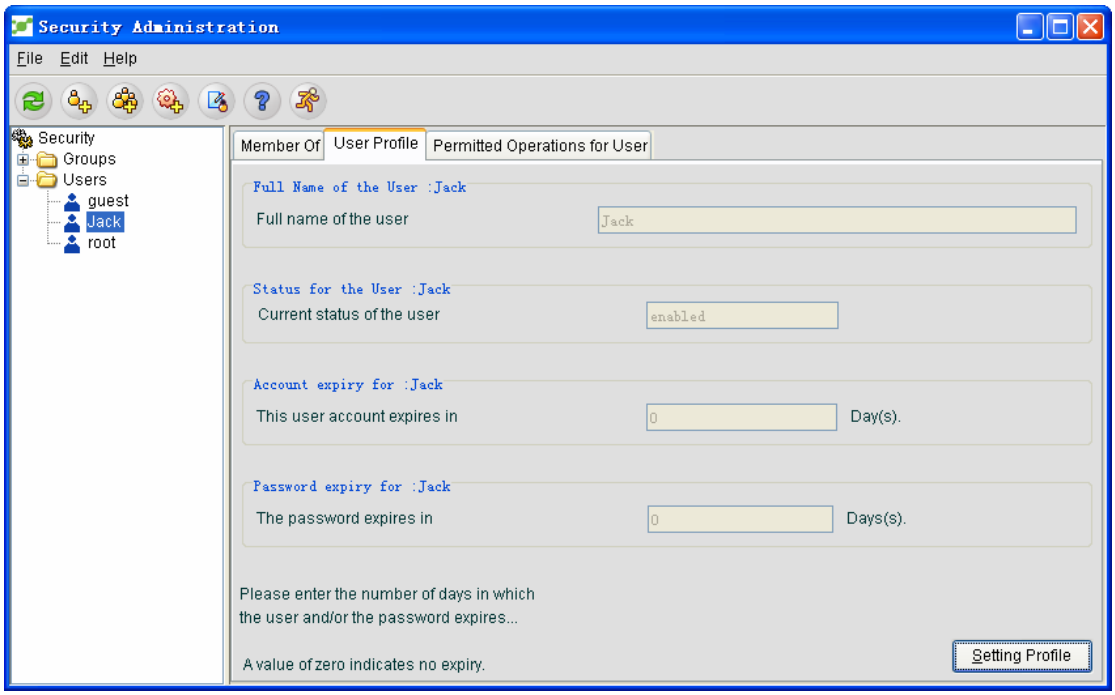


All groups are shown on the left of the window, while the groups that users are added to are shown on the right of the window. The administrator can select the specific group on the left, click ">" and add a user to the group. To remove a user from its group, select the corresponding user and click "<" to remove this user from its group.

3.1.2.3 Setting user description

NMS enables the system administrator to modify user's status, password, account and password's validation period.

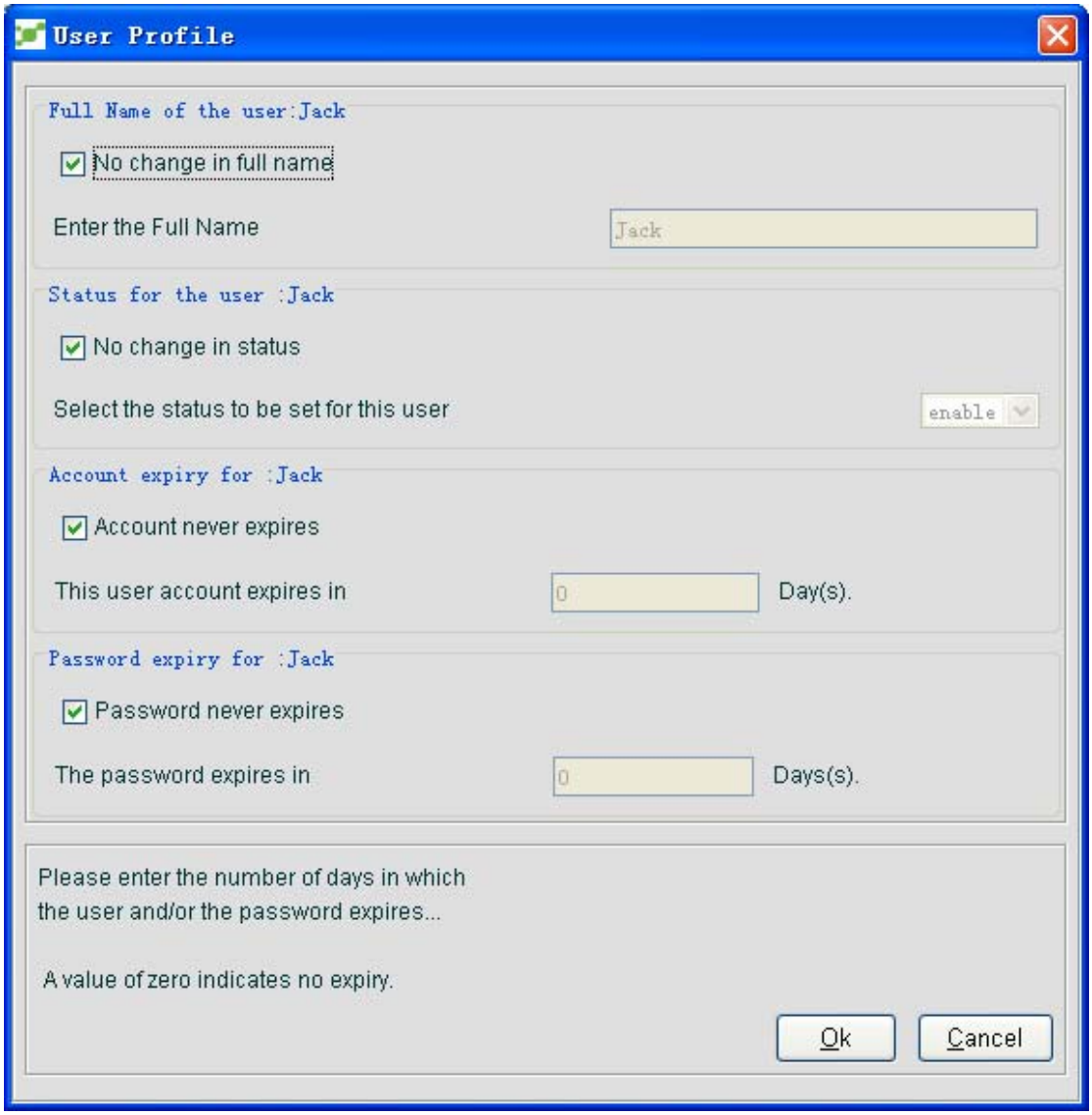
Select a specific user on the **User** tree node and open the **User Configuration File** page, on which the current user's status, the account's validation period and the password's validation period are displayed, as shown in the following figure:



The security management tool uses different icons to show the current status of a user. The icons that show different user statuses are listed in the following table:

Icon	Remarks
	The account is valid.
	The account is invalid and cannot be logged in.
	The account expires.
	The password already expires and need be reset.
	The user has been forced to log out of the server, just as the account cannot be activated.
	User's login fails.

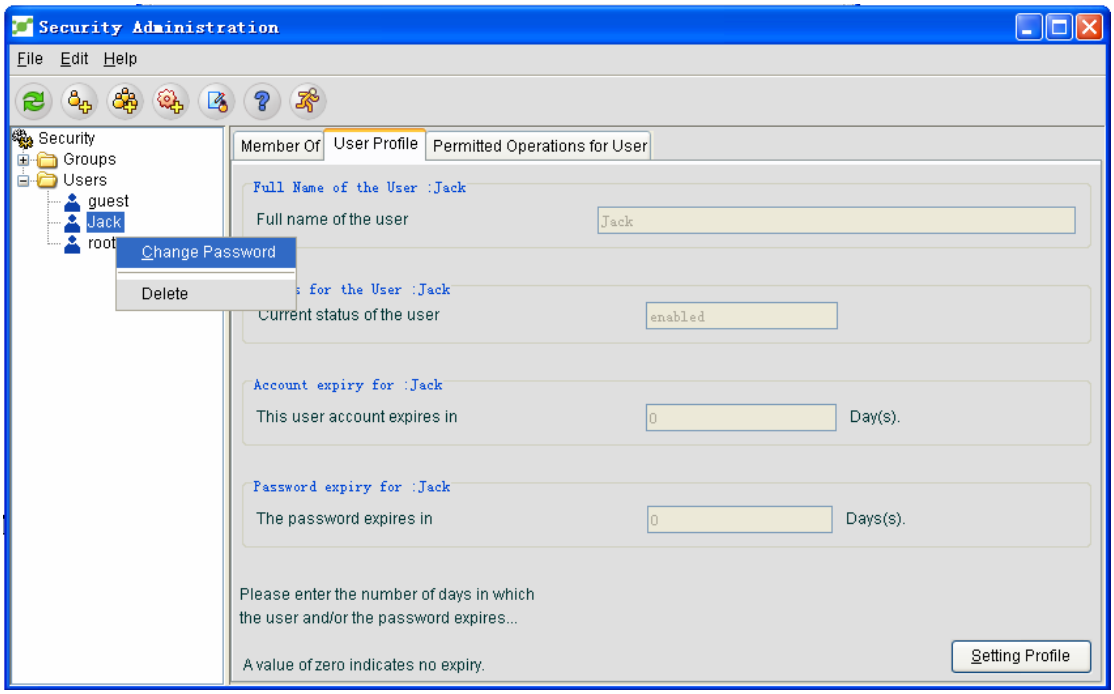
On the user settings page, click **Set the configuration file** to open the **User configuration file** window, as shown in the following figure:

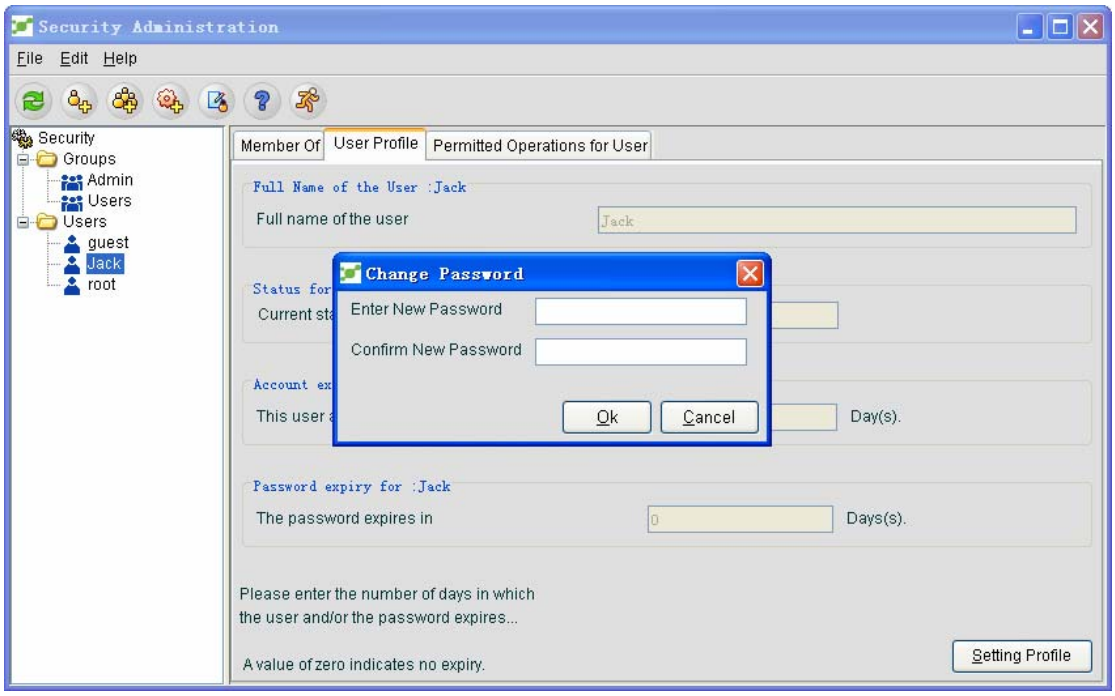


On this window, the administrator can set the corresponding user status, the account's period and the password's period for a user.
After some necessary alteration, click **Ok** to update the user settings.

3.1.2.4 Modifying the user's password

As to a selected user, the administrator can right click this user and select **Change password** or click **Edit -> Change password** in the security management window to modify the password, as shown in the following figure:



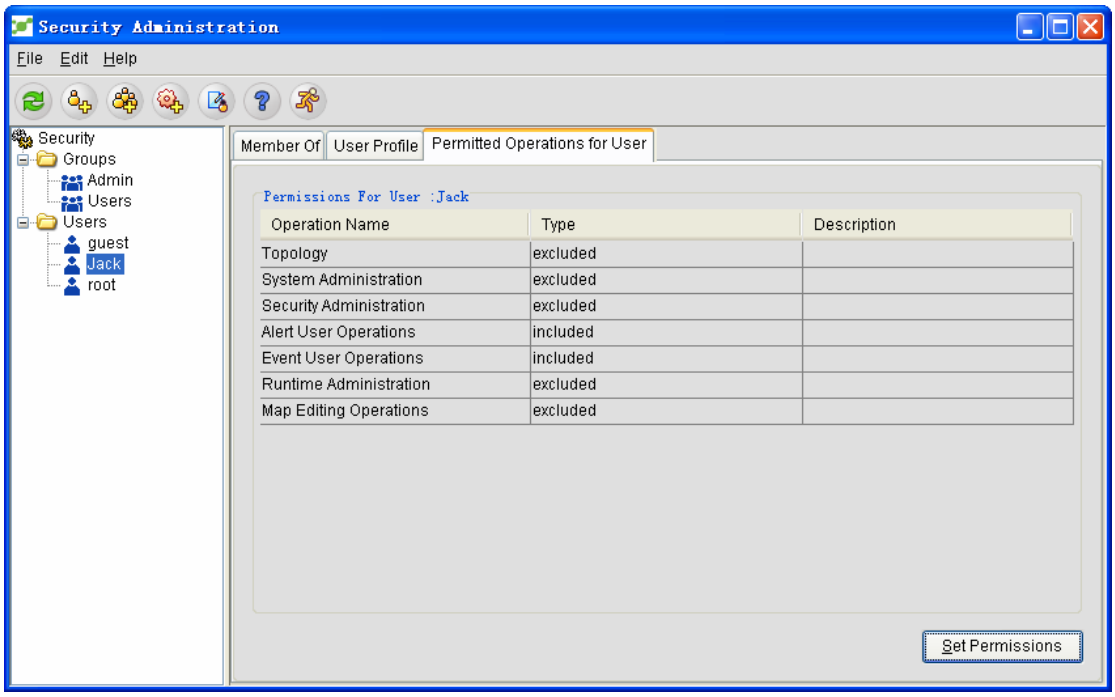


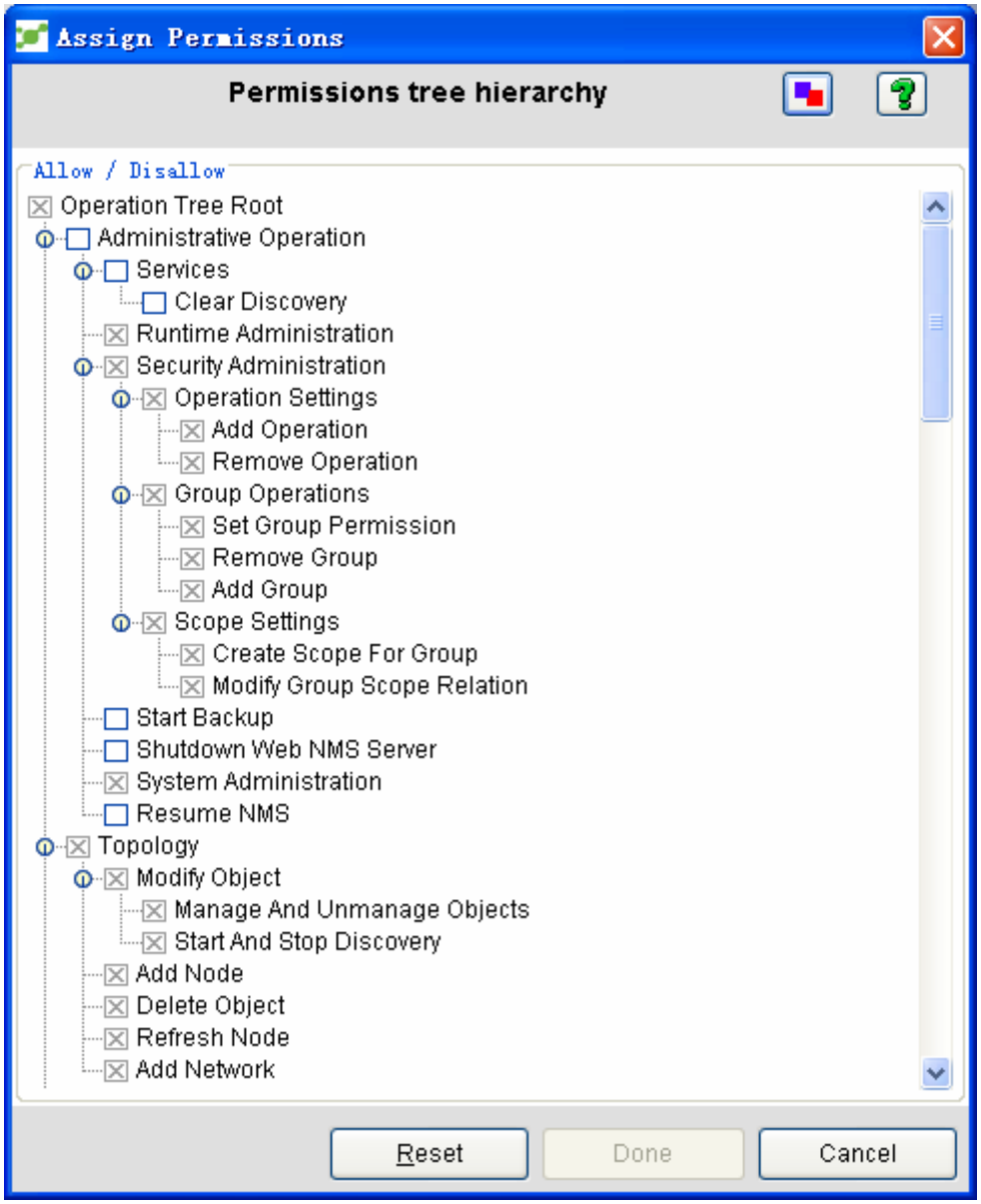
On the **Change password** textbox, enter a new password, confirm it and then click **Ok**.

3.1.2.5 Assigning authorization to users

The system administrator can follow the procedure below to assign authorization to users.

In the **User** tree node, select a specific user, open the **User access permission** page and click **Set permission**. The **Designate permission** window appears, as shown in the following figure:


Security Administration
File Edit Help
Security
Groups
Admin
Users
Users
guest
Jack
root
Member Of
User Profile
Permitted Operations for User
Permissions For User :Jack
Operation Name
Type
Description
Topology
excluded
System Administration
excluded
Security Administration
excluded
Alert User Operations
included
Event User Operations
included
Runtime Administration
excluded
Map Editing Operations
excluded
Set Permissions

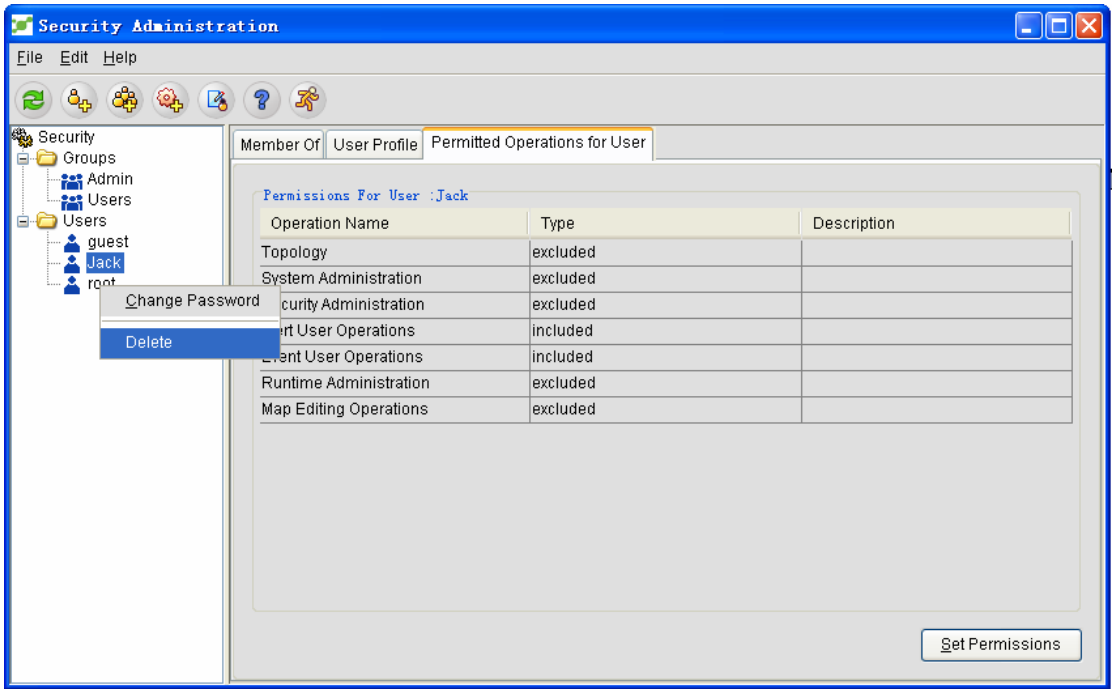


The permission tree displayed in the **Designate permission** window includes all authorization operations. The administrator can assign related authorization permissions to users by clicking the corresponding options. After the settings is done, click **Over**.

3.1.3 Deleting Users

The system administrator can perform the following operations to delete a user.

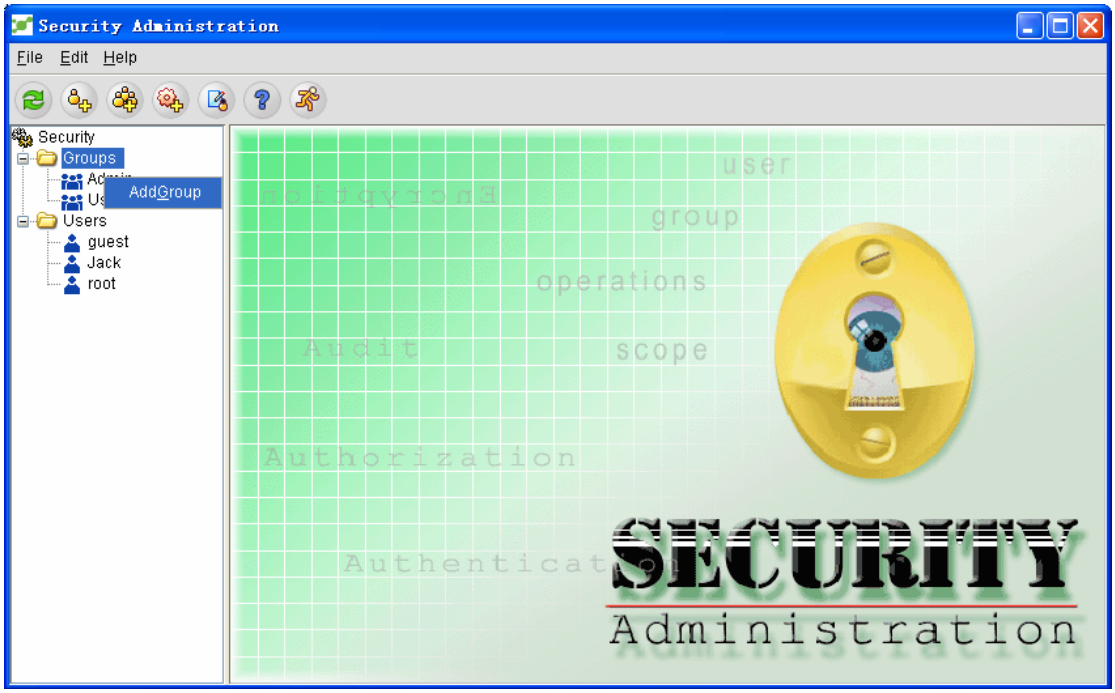
You can select a specific user in the **User** tree node, right click this user and then click **Delete** to delete this user, or you can do this by choosing a user and then clicking **Edit -> Delete**. See the following figure:



3.2 Defining a Group

3.2.1 Adding a Group

The system administrator can add a new group through the following steps:

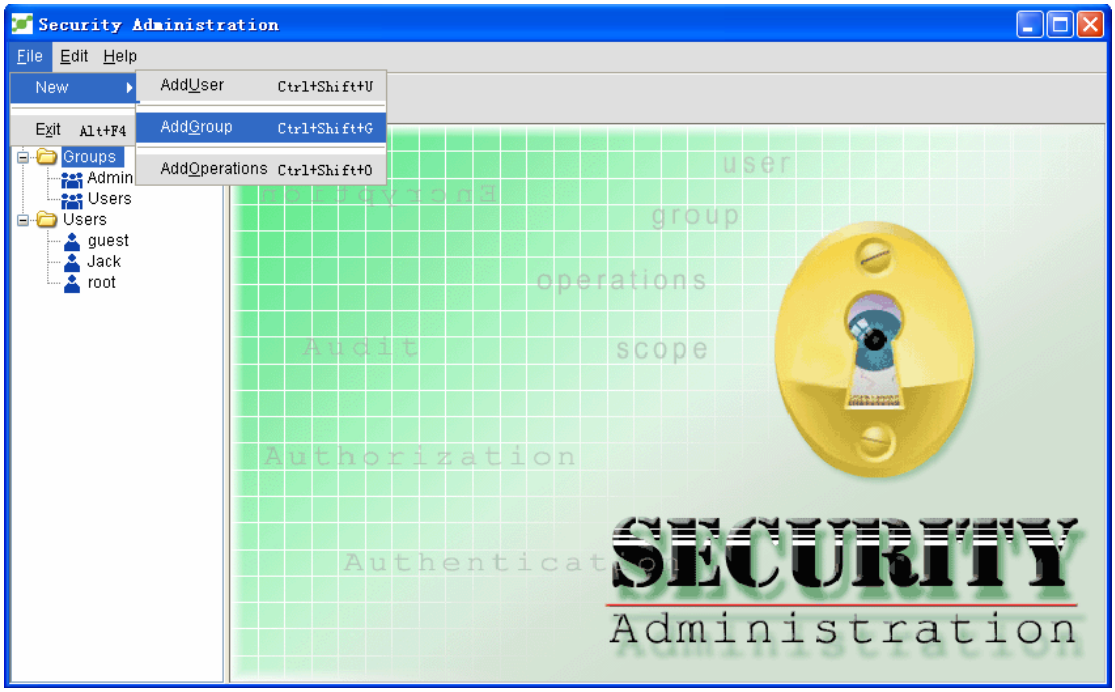


On the **security management** page, the administrator can use one of the following methods to open the **Add the group guide** window:

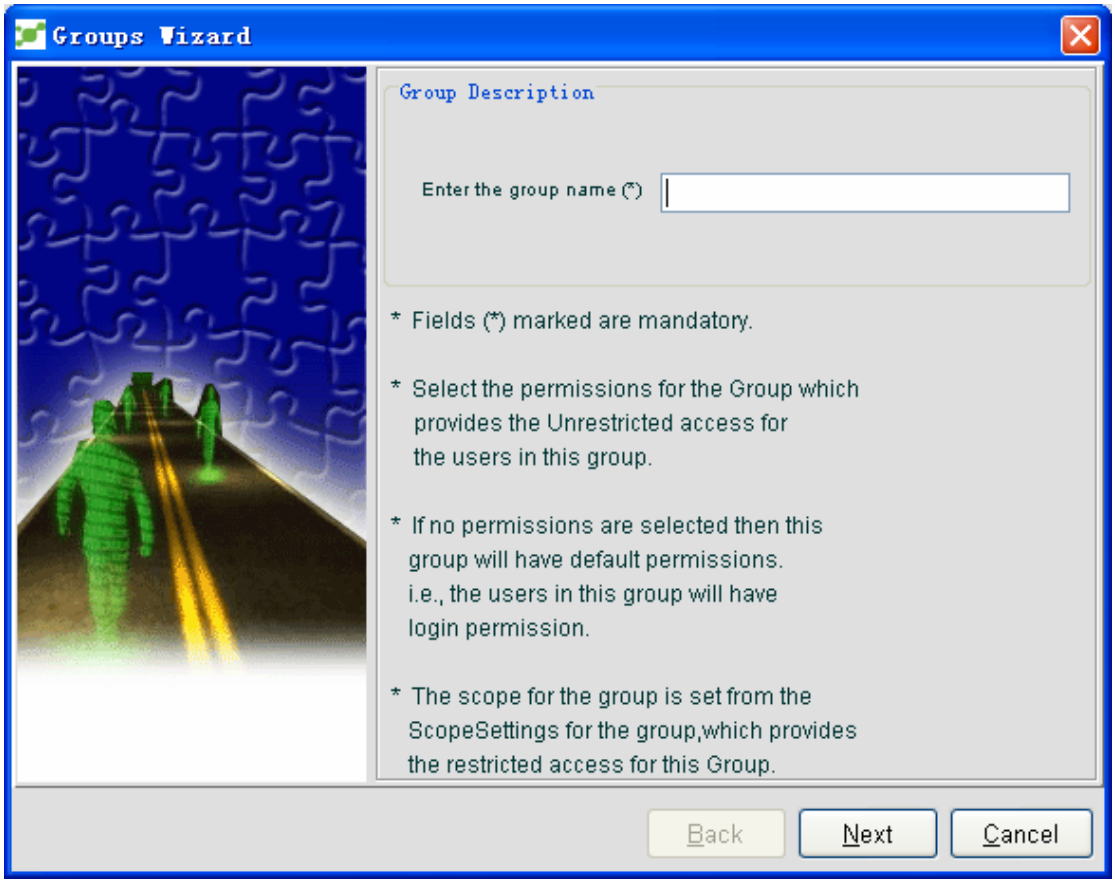
1 On the security management window, click **File -> New -> Add a group**.

2 Click the **Add a group** icon in the toolbar.

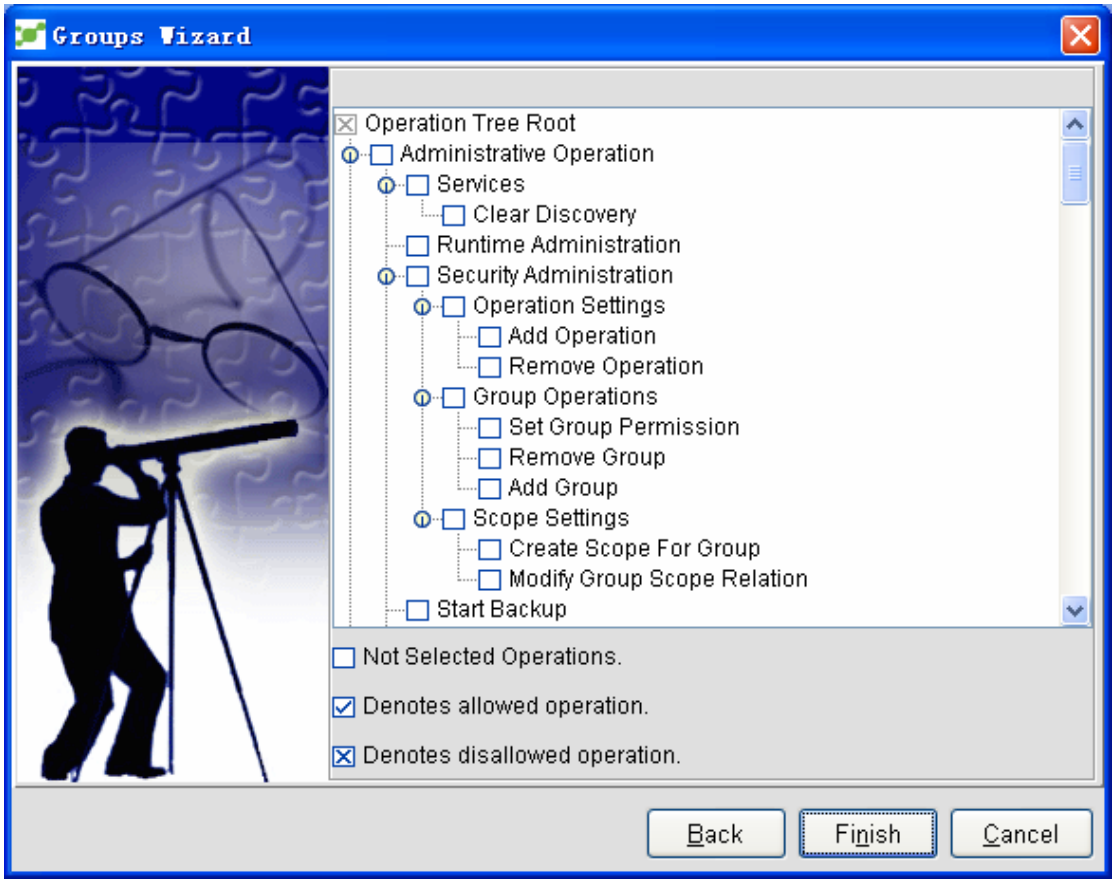
3 Right click the **Group** tree node and select the **Add a group** option.



The **Add the group guide** window is shown in the following figure:



If the administrator enters the new group name in the **Enter the group name** textbox in the **Add the group guide** window, the second **Add the group guide** window appears, as shown in the following figure:



In this window, the administrator can authorize the group operations through the following methods:

1. 1 Tick the **allowable operation** checkbox.
1. 1 Cross the **disallowable operation** checkbox.
1. 1 The unselected **operation** checkbox is null. Operating a null checkbox will not be regarded as the authorization operation.

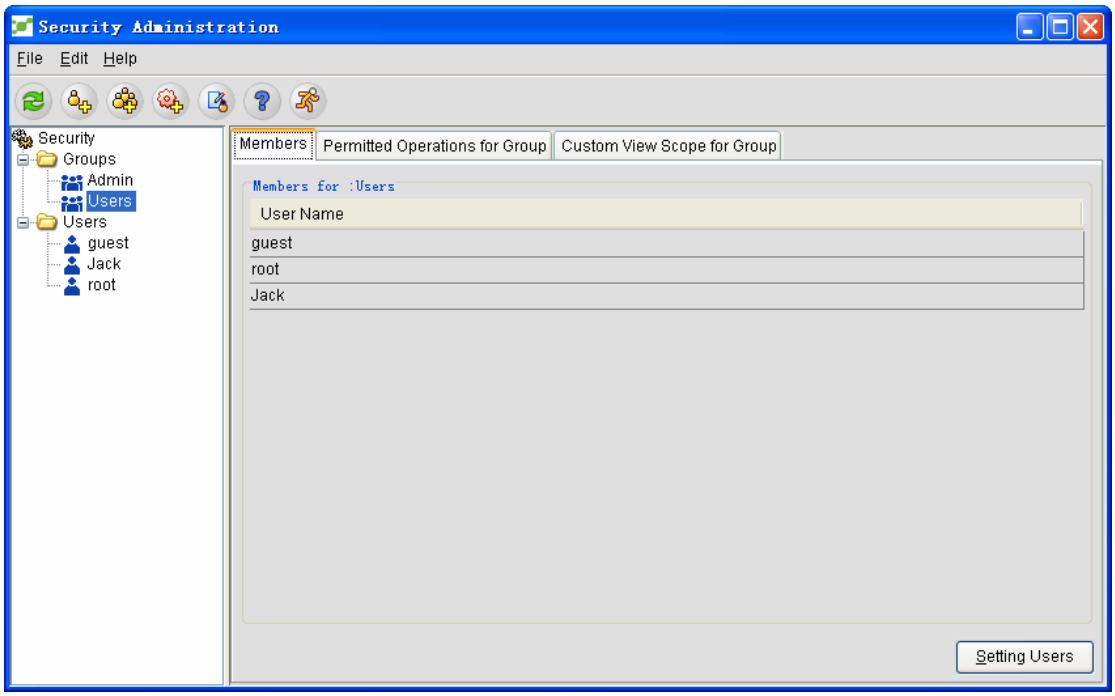
After the configuration is over, click **Finish**. The server will save the modification.

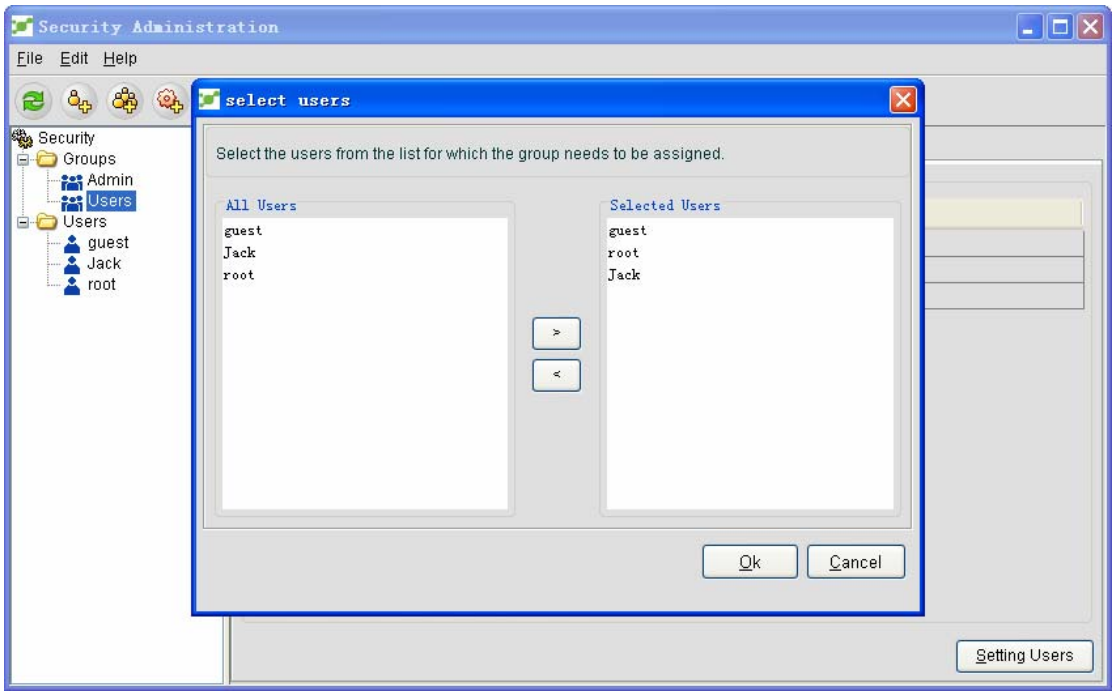
3.2.2 Group Configuration

3.2.2.1 Distributing users for a group

The system administrator can distribute users for a group by conducting the following steps:

Select a specific group under the **Group** tree node, open the **Member** attribute page, and click **Settings**. The **Select users** window appears, as shown in the following figure:





All users are displayed on the left of this window, while the selected users are displayed on the right of this window. The administrator can select a specific group on the left, click ">" and add the user to the group. To remove a user from its group, select the corresponding user and click "<" to remove this user from its group.

3.2.2.2 Designating the authorization operation for a group

The system administrator can follow the procedure below to assign authorization to users.

Select a specific group under the **Group** tree node, open the **Group permission** attribute page, and click **Set the permission**. The **Designate the permission** window appears.

On the **Designate the permission** window, the administrator can set operations for a group by selecting or deselecting the operations. After the settings is over, click **Finish**.

Note: If you click the **Reset** button, the group permission will be set through the default mode.

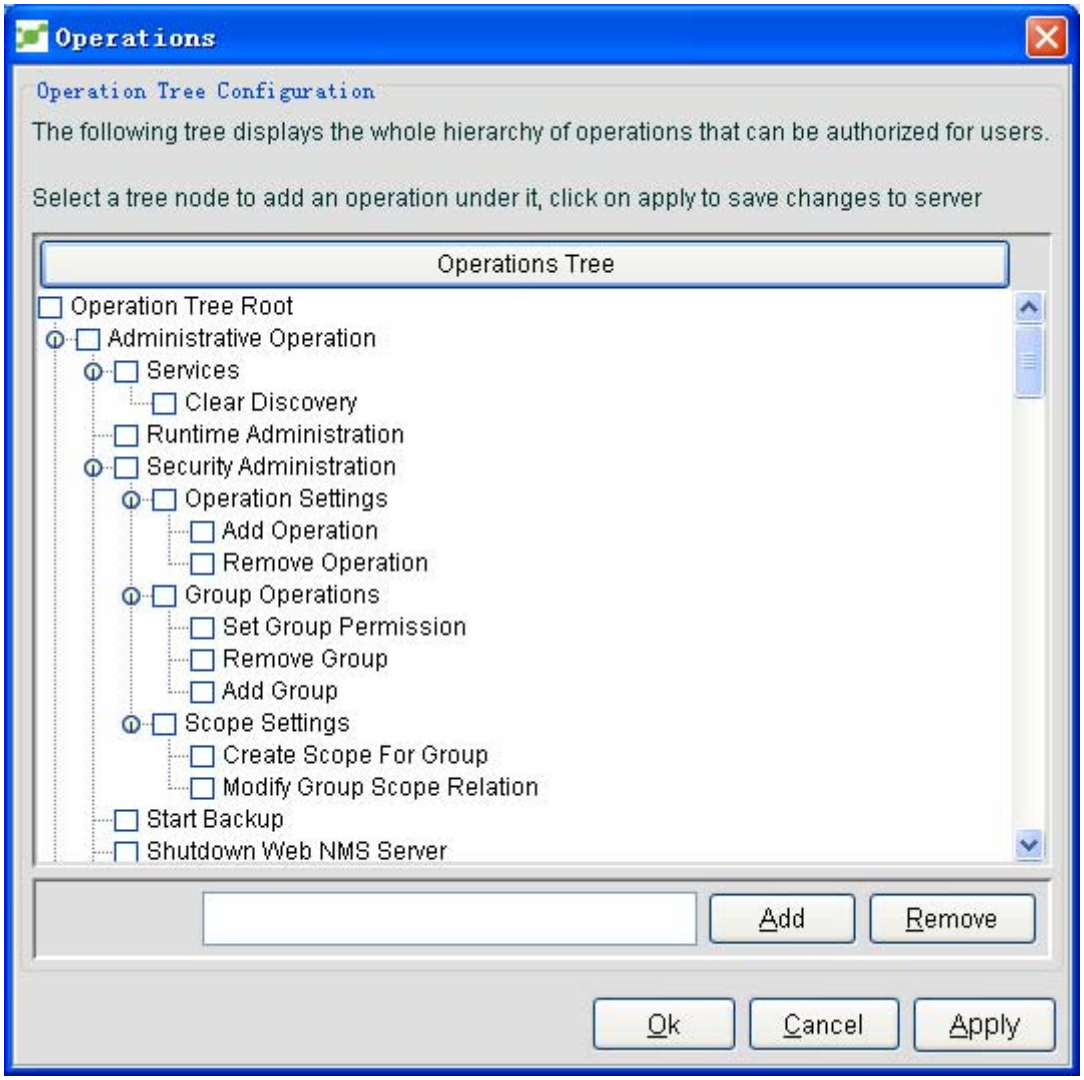
3.3 Operation Tree

The operations in NMS are listed out in a tree structure, including the parent operations and child operations. On the security management window, the administrator can add new operations through the following two methods:

1 Click **File -> New -> Add an operation**.

2 Click the **Add an operation** icon  in the toolbar.

If the administrator wishes to explore the operations in NMS, he or she can add new operations at the corresponding locations of the operation tree. The operation tree faceplate is shown in the following figure:



3.3.1 Adding an Operation

Choose the parent operations and then enter the to-be-added operation in the textbox.

Click **Add**.

The new operation is then added to the place under the parent operations.

3.3.2 Deleting an Operation

Select the to-be-deleted operation from the operation tree and then click **Remove**. The operation is then deleted.

3.3.3 Default Operation Tree

The operation tree includes the default operation list provided by NMS. The administrator can designate different operations for different users, which are given detailed explanation below:

The operations with relation to the administrator are shown in the following table:

Operation	Remarks
Service	
Delete discovery	When a discovery is terminated by some reason, you can use this operation to delete this discovery.
Start backup	It is used to enable the functionality of system backup.
Resume the server	If NMS stops running due to a certain reason during the backup process, you can perform this operation to resume all processes of the server.
Disable the NMS server	This operation is used to disable the NMS server.
Set the log level	This operation is used to provide logs for multiple modules, and of course set the logs.
Real-time management	It is used to conduct the settings for the running of NMS server.
Security Management	Security management includes ID authentication during login and access permission designation for each user.
System Management	It is used to process all operations of the administrator.

The operations towards the modules in NMS are listed below:

1. Administrator's Operations
2. Event
3. Topology
4. User Management
5. Alarm
6. Figure
7. EPON Settings

Administrator's Operations

Operation	Remarks
Delete discovery	Deletes the already discovered devices.
Disable server	Disables the network management server.
Security Management	Sets the permission of the user and user group.
System Management	Discovers and manages the devices in real time during running.

Event

Network event means a description of all statuses of network equipment. The event can bear not only the regular information but also the current status of a network device. The following table gives a description of all kinds of operations related with network events.

Operation	Remarks
Save the event to the file	It is used to save the selected events or those events on the event faceplate.
Print the event view	It is used to print the selected events or those events on the event faceplate.

Topology

The operation of related topologies is shown in the following table:

Operation	Remarks
Start and stop discovery	It is used to set the discovery status of a specific object during the running of the system.
Manage an object or cancel management	It is used to set the management status of a specific object during the running of the system.
Delete an object	It is used to delete a specific object from the topology database.
Refresh a node	It is used to refresh the polling status.

Alarm

If the system detects a trouble of a device in the network, it will generate an alarm. This alarm will be shown in the alarm view and users can browse alarms with a lot of levels, such as severe alarms, main alarms, secondary alarms and deleted alarms and so on. The operations related with alarm are shown in the following table:

Operation	Remarks
Set alarm's remarks	It is used to add an alarm remark.
Gain alarm details	It is used to browse the details of a specific alarm.
Save the alarm to the file	It is used to save the chosen alarms or those in the current alarm faceplate to a folder.
Print the alarm view	It is used to print the chosen alarms or those in the current alarm faceplate.
Delete alarm	It is used to delete alarms.
Obtain the alarm remark	It is used to browse the remarks of the existent specific alarm.
Obtain the history alarm	It is used to browse the history alarm, that is, the status change from the first to the last of an alarm.
Obtain the alarm	It is used to obtain alarms.
Delete the alarm	It is used to delete an uncared or resolved alarm.

EPON Settings

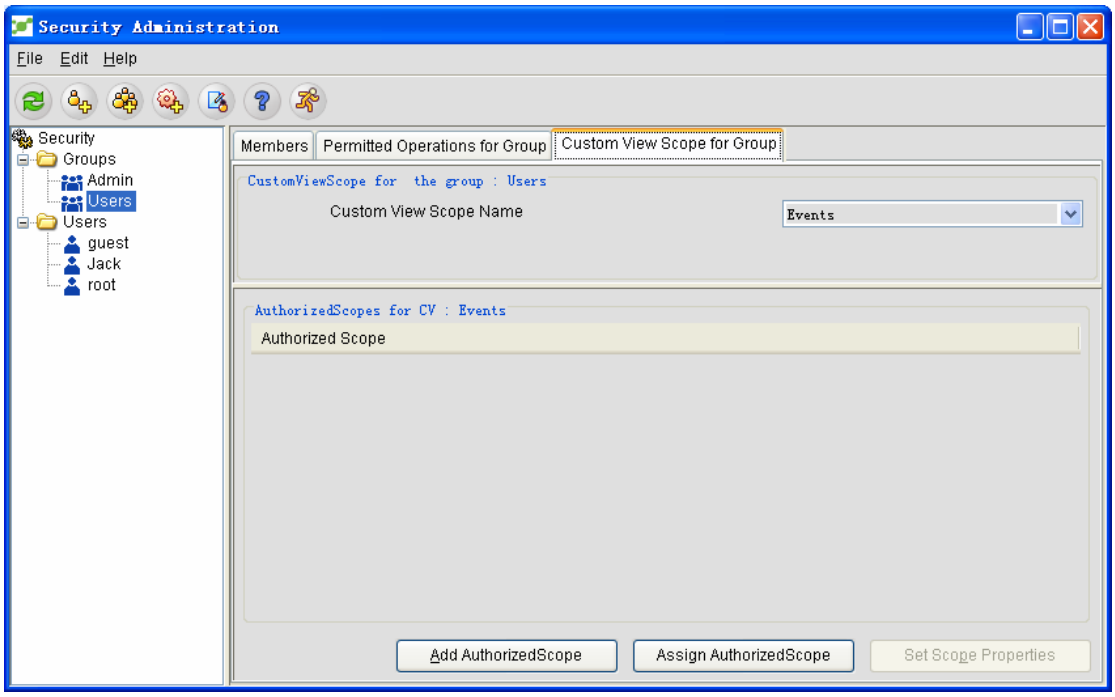
OLT settings	Includes the settings of dba, stp, multicast, acl, qos, vlan and so on.
ONU settings	Includes the management of ONU faceplates, qos and onu icons.
Other Settings	Browses the device faceplates and manages the slot information, the chip information, the SNMP attribute settings, rediscovery and CPU performance collection.

3.4 Customizing the View's Function Domain

You can customize the view's function domain to designate the read permission of a group.

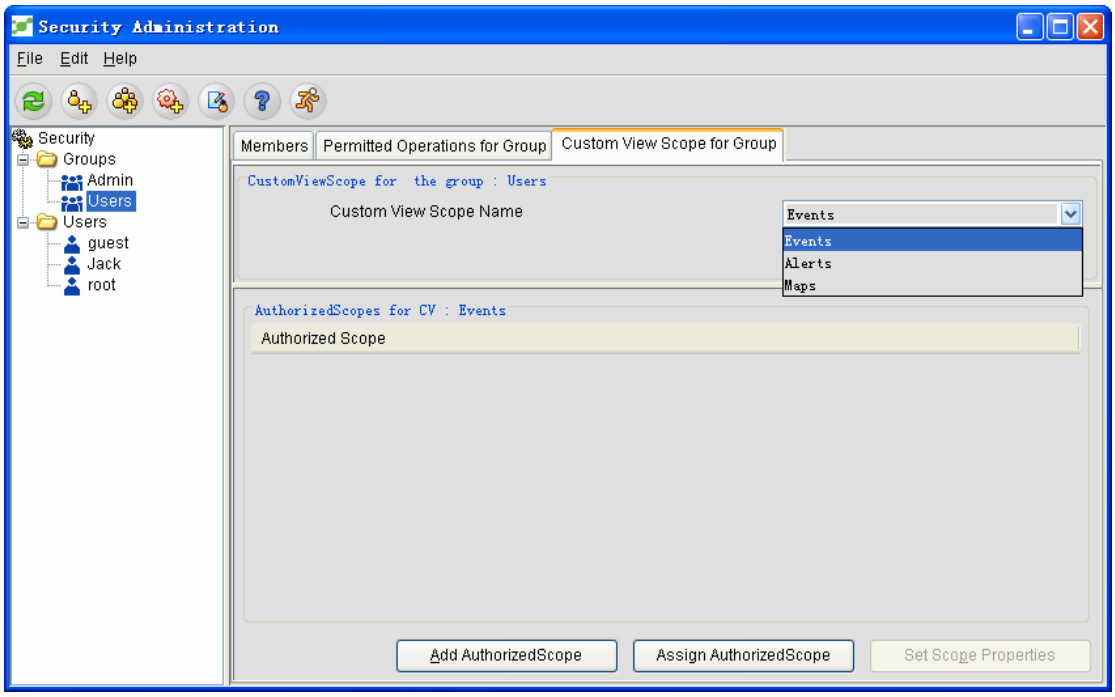
3.4.1 Adding the Authorization Function Domain

Click the **Group** tree node, as shown in the following figure:



On the configuration attribute page, click the **Customize the view's function domain** page.

On the **Customize the name of the view's function domain** option, you have the following names to choose from: Events, Alerts and Maps.

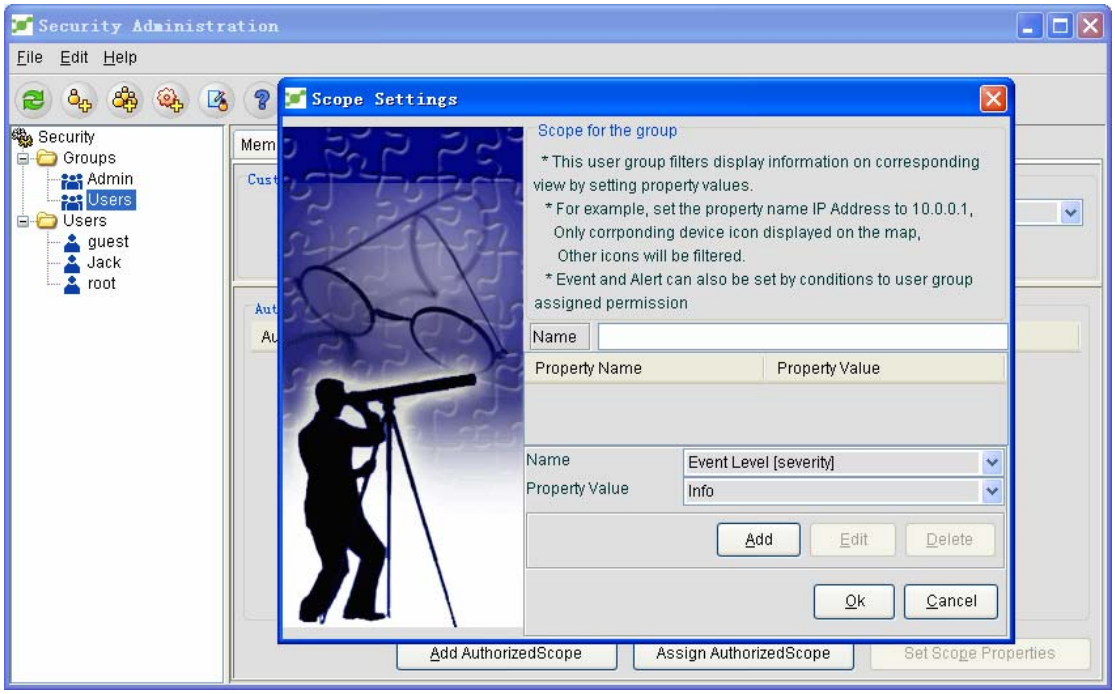


Maps: You can filter those unrequested maps according to actual needs, making user management more convenient and easier.

Alerts: You can filter those unrequested alarms and just keep those requested alarms.

Events: You can filter those unrequested events and just keep those requested events.

Click **Add the authorization function domain**. The following page then appears:



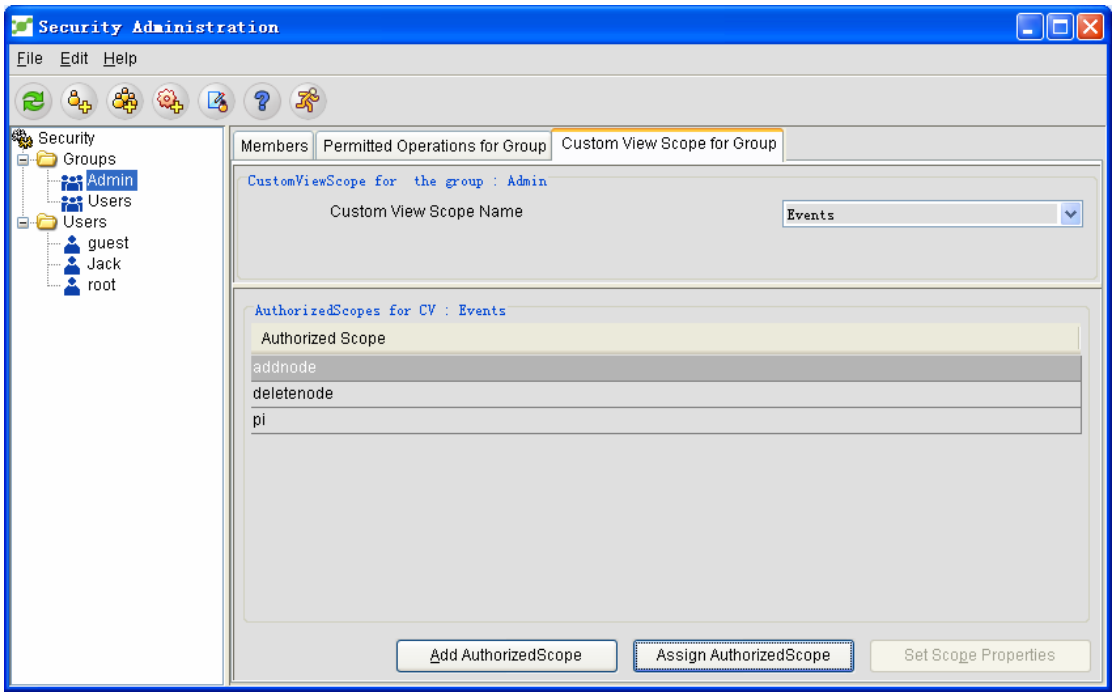
Name: It stands for the name of the group's function domain and you can enter a name according to your requirements.

Attribute name: You can click this button to choose a name, but its default name is **IP address [name]**.

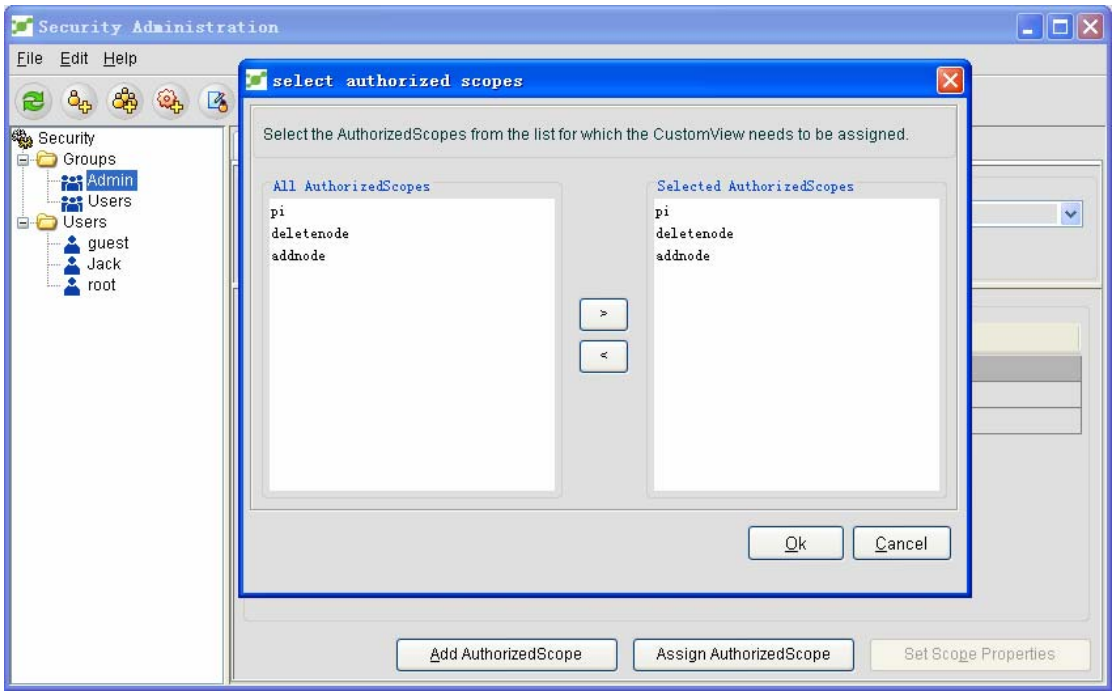
Attribute value: It stands for the filtration premises. For example, if you want to filter the network graphic whose IP is 172.16.21.1, just set the attribute name to be **IP address** and the attribute name to be **172.16.21.1**. Then you can find that only the icon of this device is displayed on the map and other icons about this device will be filtered. On options such as **Events** and **Alerts**, you can set the read permission of the user group. Click **OK** to save the added function domain.

3.4.2 Designating the Authorization Function Domain

On the existing authorization function domain, click **Designate the authorization function domain**, as shown the following figure:



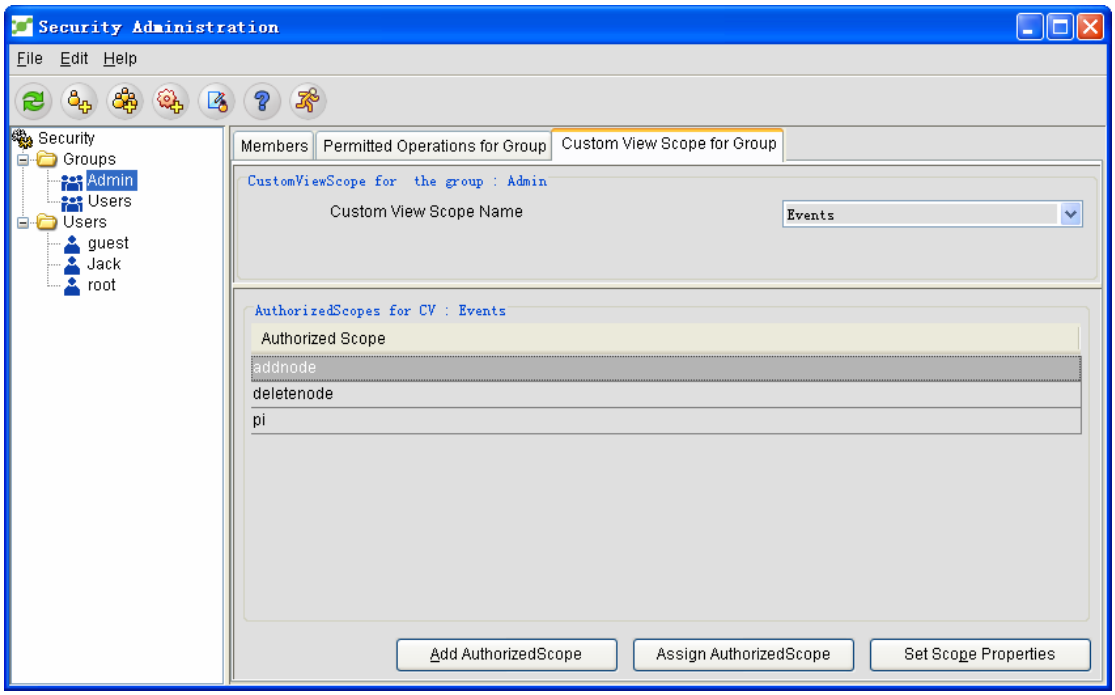
The following page appears, as shown in the following figure:



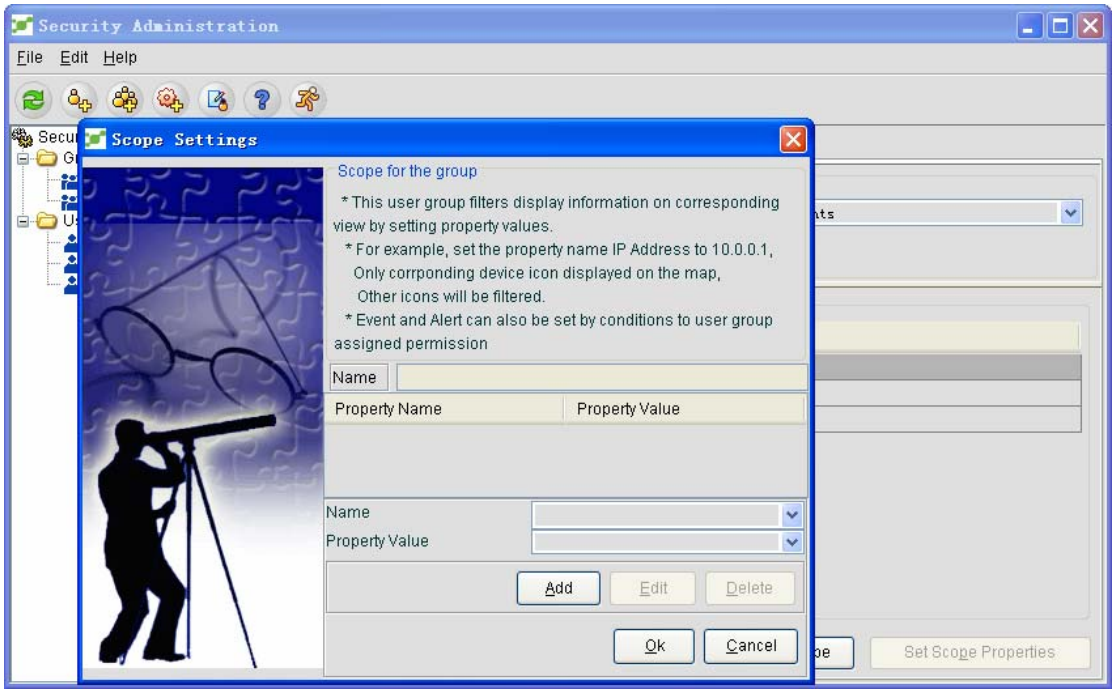
You can select a specific authorization function domain according to actual needs and add it to a user group. Click **OK** and the settings is successfully done.

3.4.3 Setting the Attributes of the Authorization Function Domain

You can set the existing authorization function domain, as shown in the following figure:



Select the to-be-set authorization function domain and click **Set the attribute of the function domain**. The following page then appears:

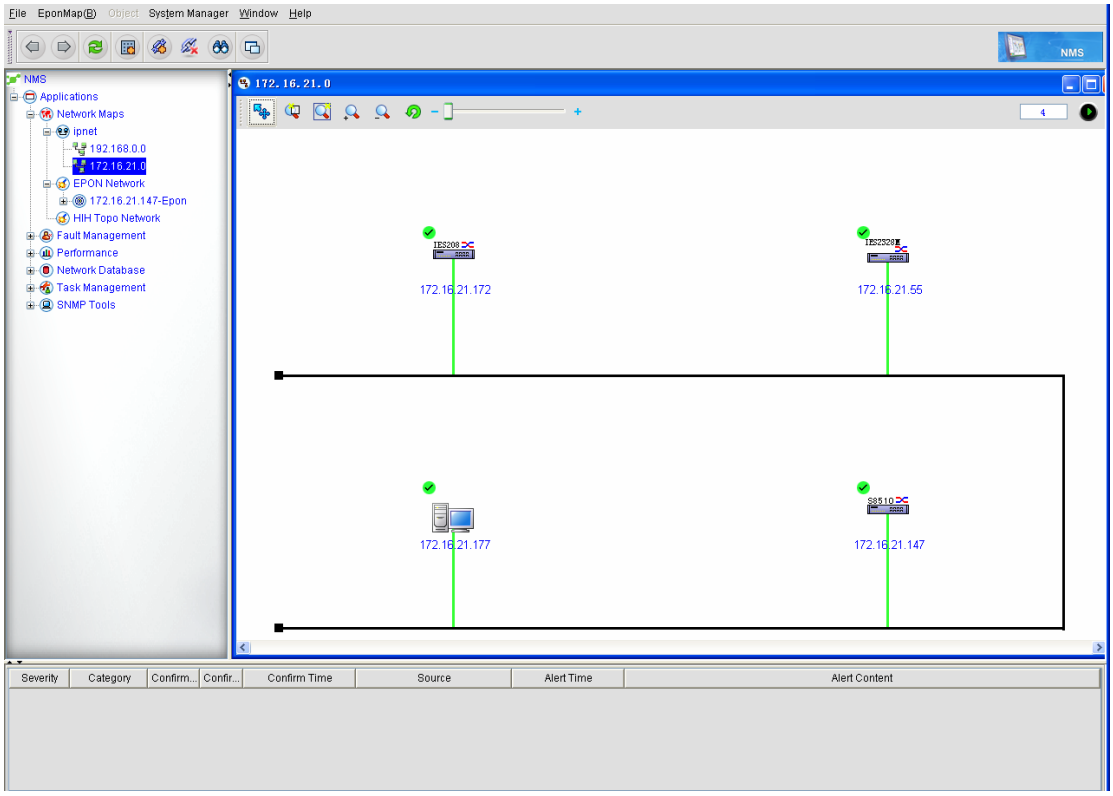


You can reset the authorization function domain.

4. Managing Devices in the IP Network

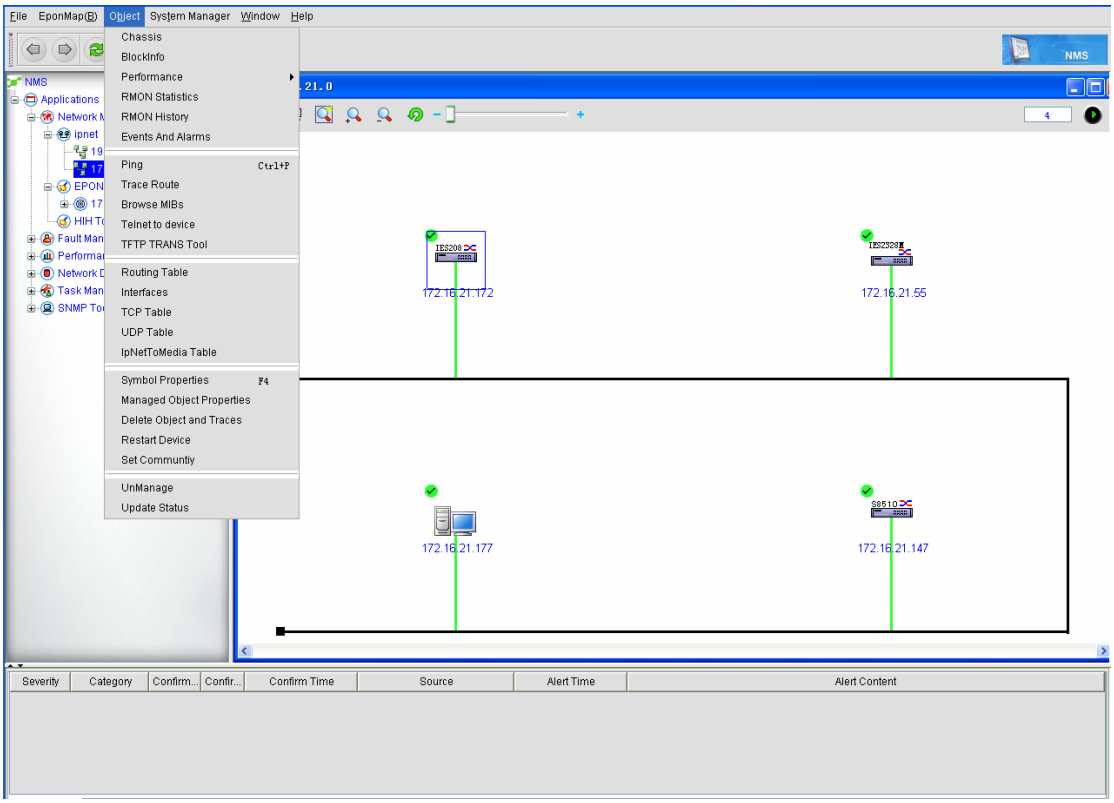
The Network Management Software (NMS) supports the discovery and management of multiple kinds of devices, including general switches and EPON devices. The management of the EPON device will be further described in the next section. NMS provides a lot of flexible management methods and enables you to browse all kinds of parameters of this device.

In the left tree menu, open the IP network and click the **Network** icon or directly open the **Network** option in the tree menu. Enter the **Network** view. Here, all managed devices in this network will be displayed. See the following figure:

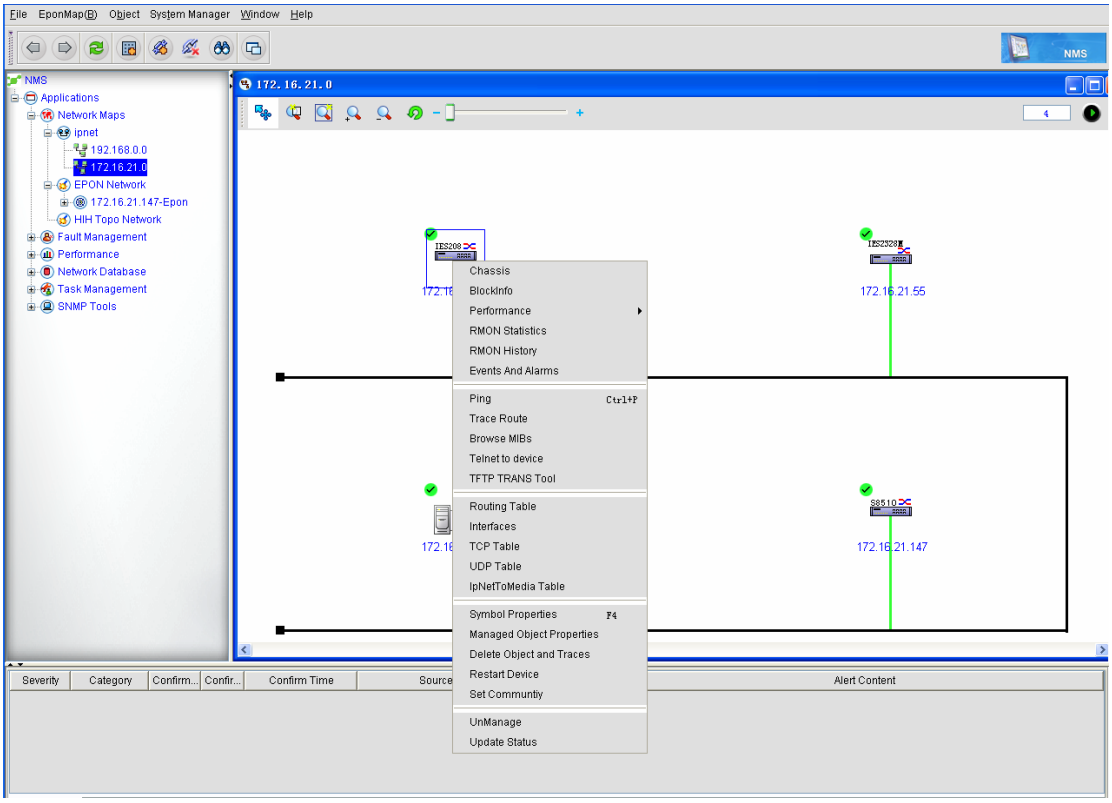


All managed devices are shown. These devices include the EPON devices, general switches and PCs.

If you then click **General device**, a menu option, Device Management, will appear on the top of the system window. Click **Device Management**. The menu options then appear, which are functions, as shown in the following figure:



Or click the **Device** icon and right click **Pop-up**, the menu options then appear.



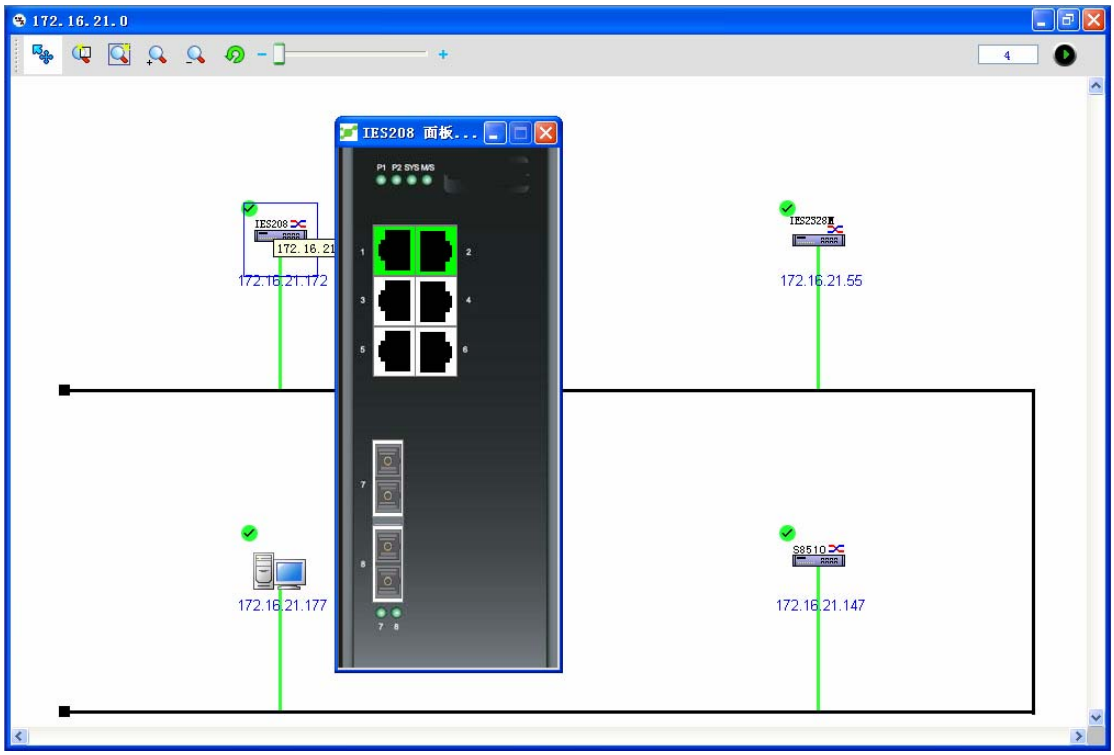
These menu options are described below:

4.1 Device Faceplate

The device faceplate graphic is displayed, including the port's status. Port's color: The color of a port is decided by the configuration and connection statuses of this port. If this physical port's configuration status is **Disable**, the color of this port is red. In the case that the physical port's configuration status is **Enable**, if the protocol is down the color of this port is white, and if the protocol is up the color of this port is green.

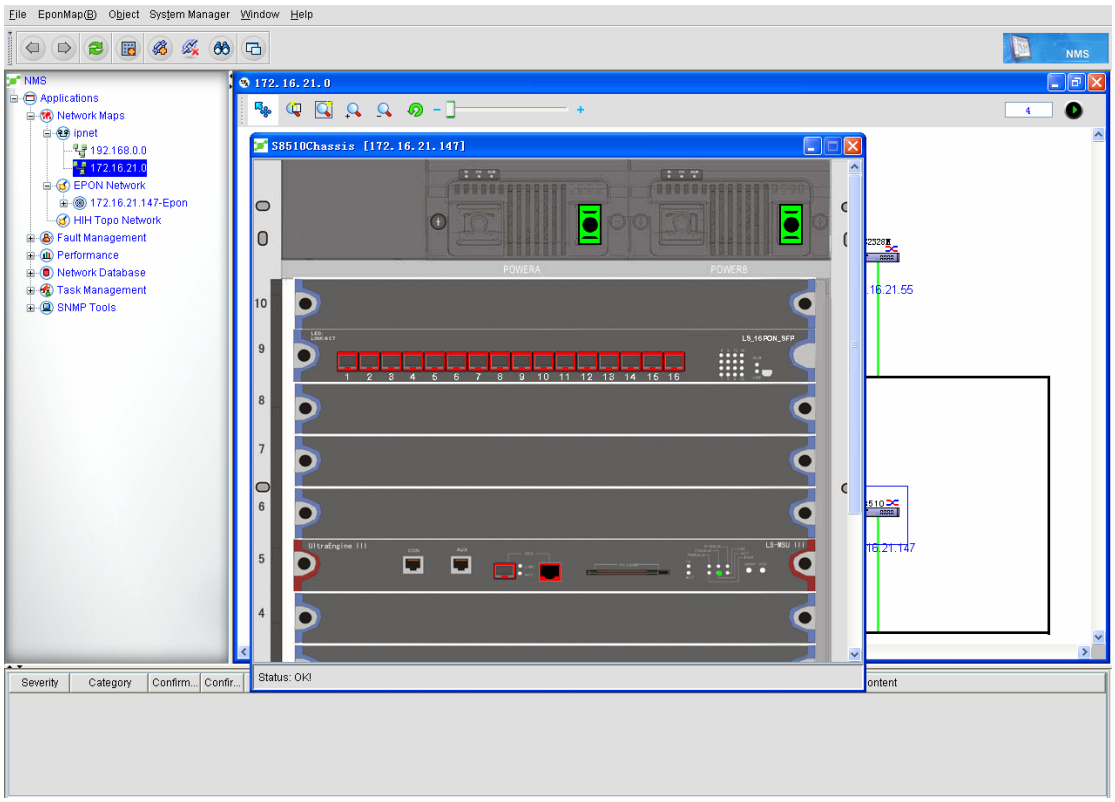
4.1.1 Views of General Switches and Routers

On general device faceplates, you can only find the statuses of devices. You, however, cannot operate their ports, as shown in the following figure:



4.1.2 EPON Faceplate Graphic

The EPON faceplate graphic enables you to operate the ports and the board cards. See the following figure:



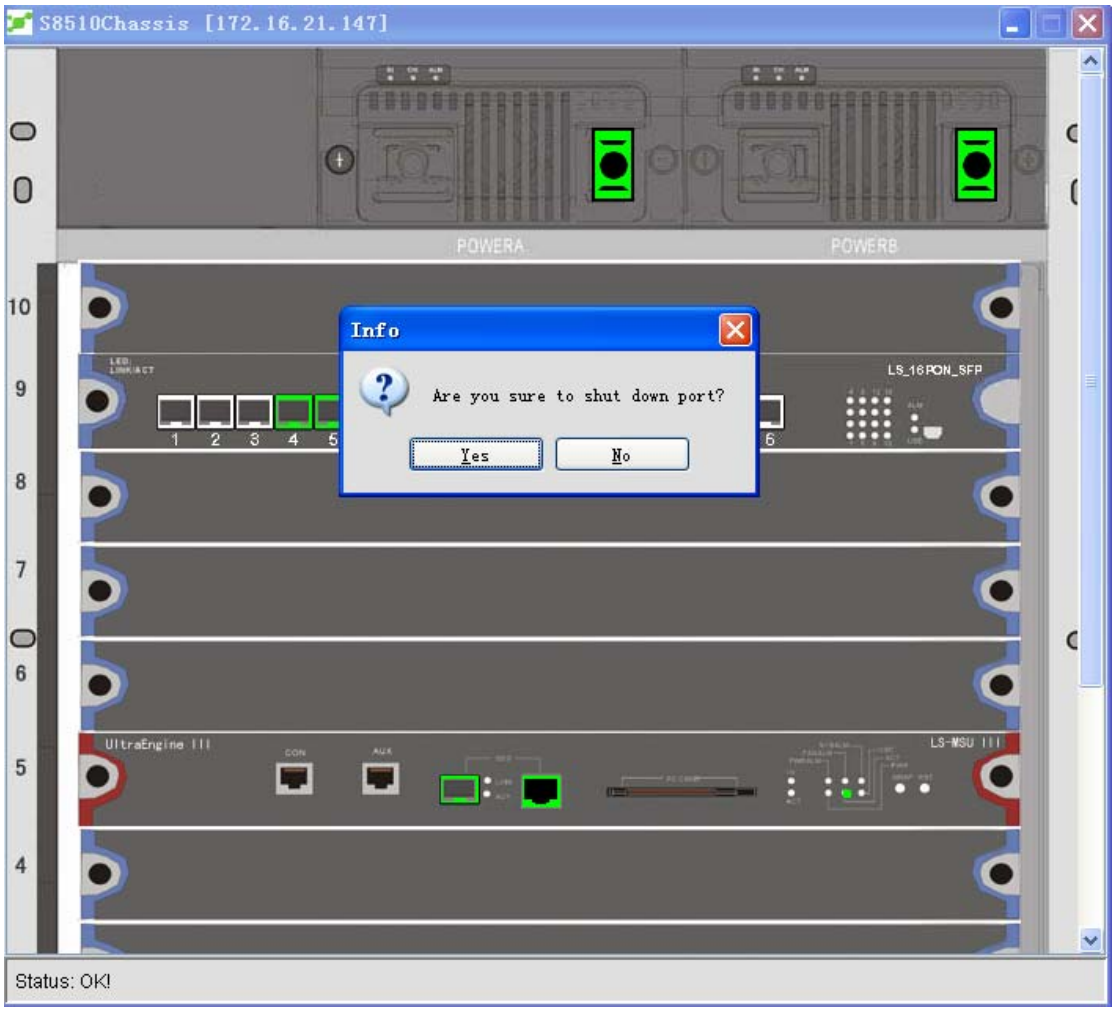
1. Main control functions: Right click the main controller board and the **master-backup-shift** option. When there are two main controller boards, the switchover of the main controller boards can be conducted.

2. Other equipment faceplates: Right click other device faceplates and then two options, **Reset the card** and **Forbid the slot**, appears.

Click **Reset the card** to enable this card again. Click **Forbid the slot** to forbid this slot. Only when the system is enabled can the card on this slot be identified.

3. Operating the port on the faceplate:

   a. The PON port on the PON card provides two options for port operation, that is, **shutdown** and **no shutdown**. Click the menu to conduct operations, as shown in the following figure:



b. The operations of the non-PON port include the VLAN settings, the port status operation, the port mode and the port rate. See the following figure:

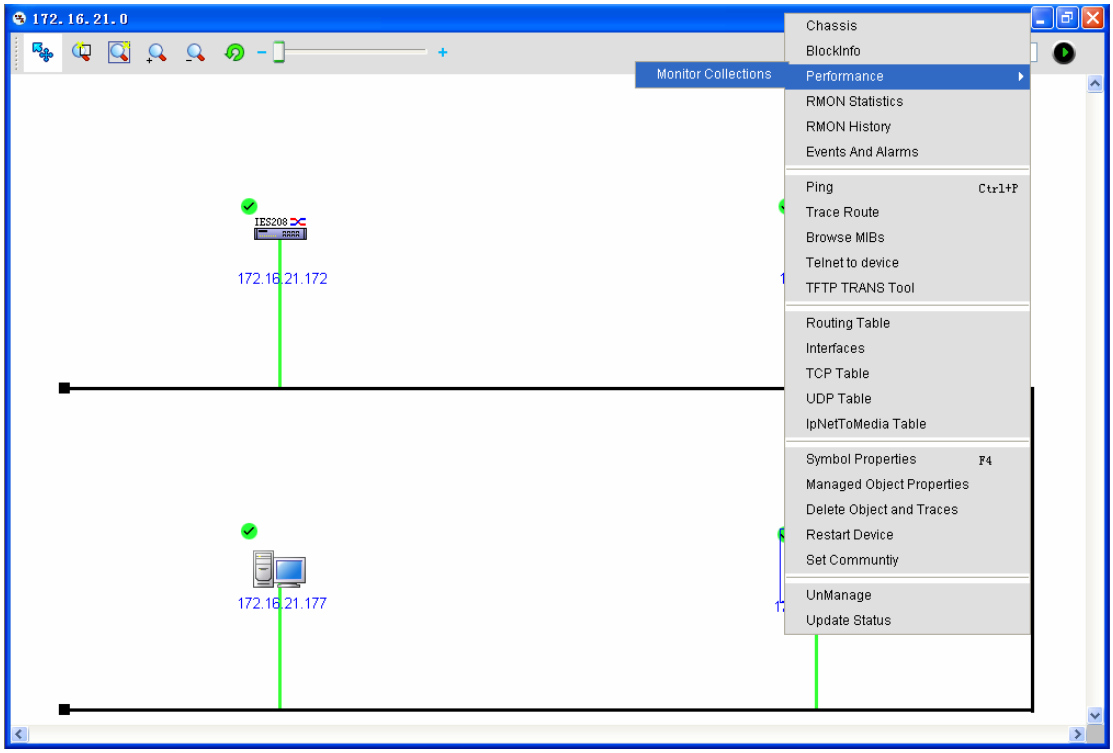
4.2 Common Functions

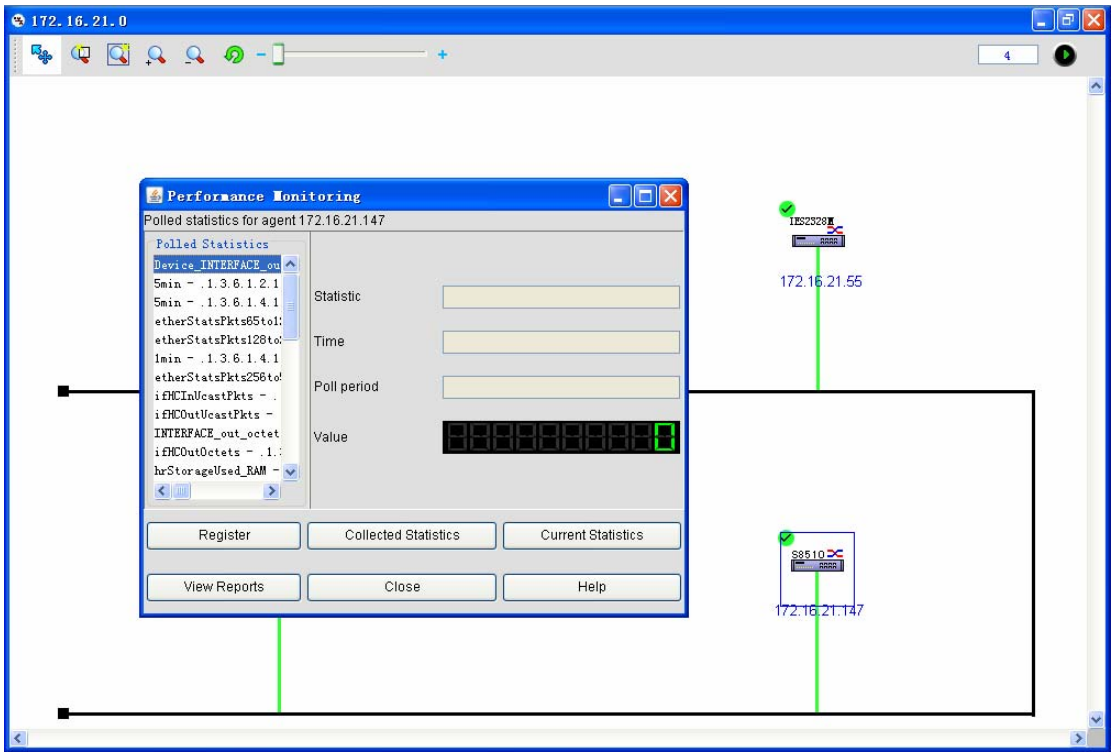
- BlockInfo: it is used to browse the block information.
- NAT monitor: it is used to browse and monitor L3 switching or routing equipment and the NAT list.
- Events and Alerts: It is the statistics of the events and alerts.
- **Ping: It is to ping other devices.**
- **Trace Router: It is to browse the information about trace router.**
- Browse MIB: It is to browse the MIB value of the device.
- Telnet: It is to control devices in a remote way.
- **TFTP: It is to upload the TFTP files.**

- **Routing table: It is to browse the routing table of a device, which only supports L3 routing or switching devices.**
- **Interface: It is to browse and query the interfaces of a device, including the information about the interface type and the interface speed.**
- **TCP table: It is to browse and query the TCP links of a device.**
- **UDP table: It is to browse and query the UDP links of a device.**
- IpNetToMedia table: It is the IP-MAC mapping table.
- **Cancel management: It means not to manage those managed devices.**
- **Start management: It is to re-manage a device.**
- **Update the status: It means that the system re-confirms the status of a device.**

4.3 Performance Management

The data about a device's performance can be obtained in time and presented by the statistics graphs so that the administrator can know the operation performance of the device in an objective way. If you click **Menu -> Performance management -> Collect monitors**, the following page appears:

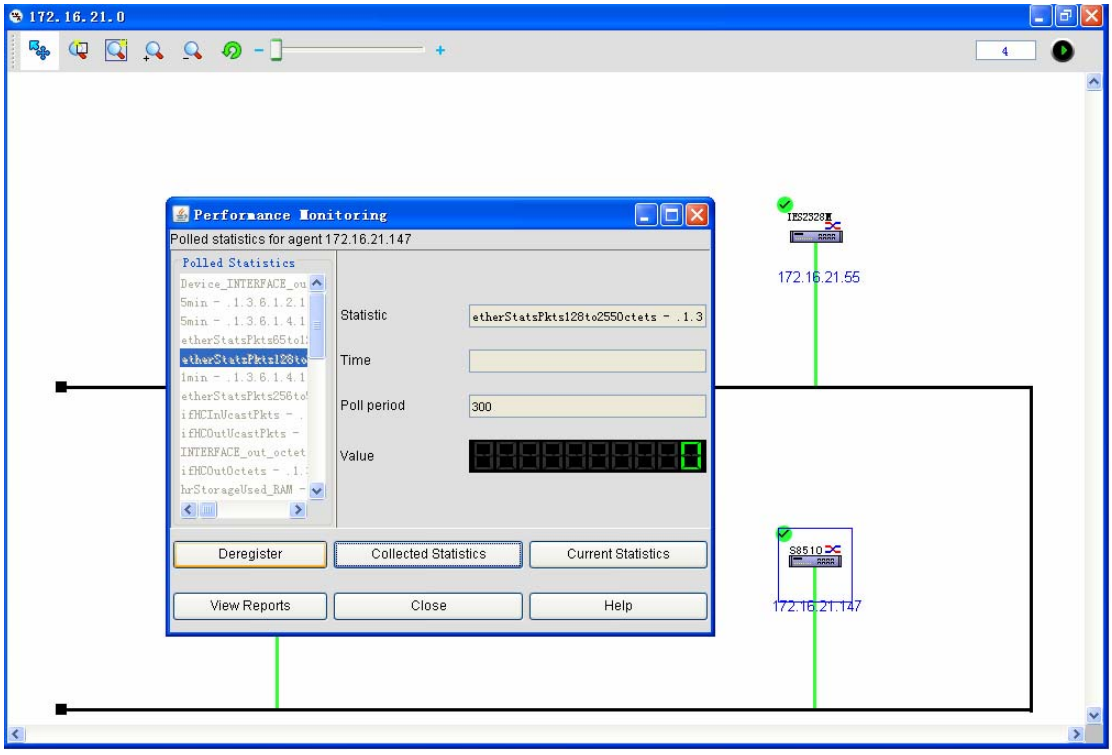


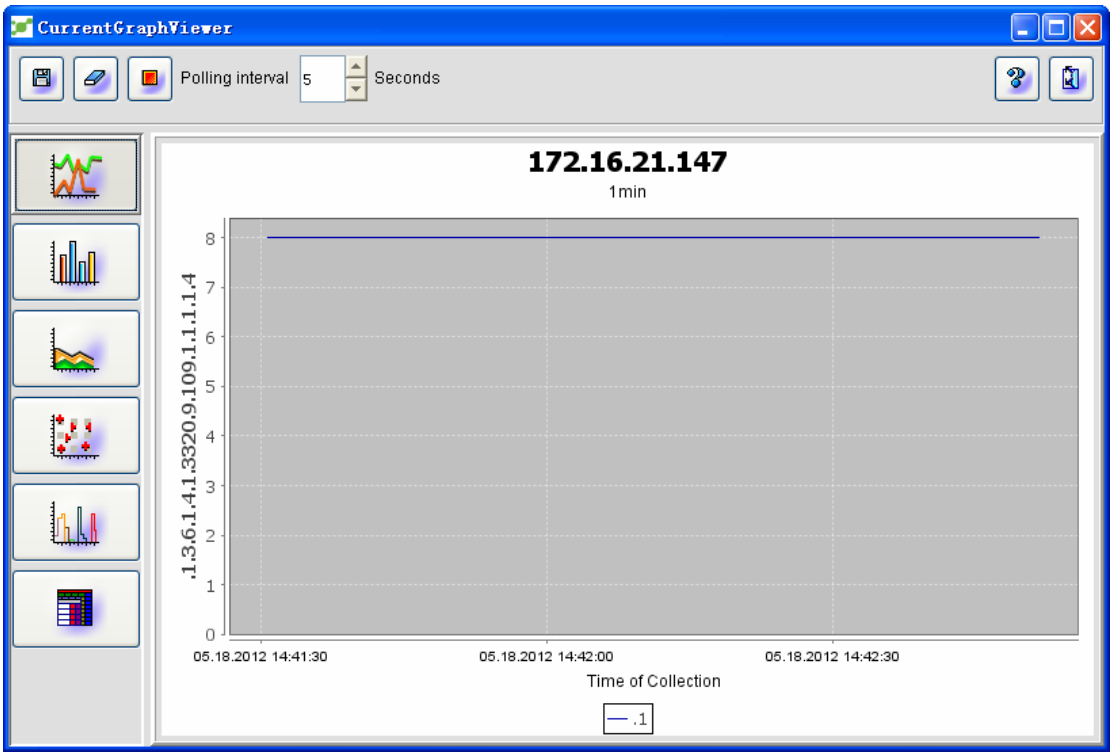


The related parameters are described blow:

Polling statistics data: standing for the data collection option obtained from a device

After the data collection option of polling is chosen, click **Register** and then you will find the system starts collection data. Click **Current statistics** and then you will find that the performance collection statistics graphic appears.

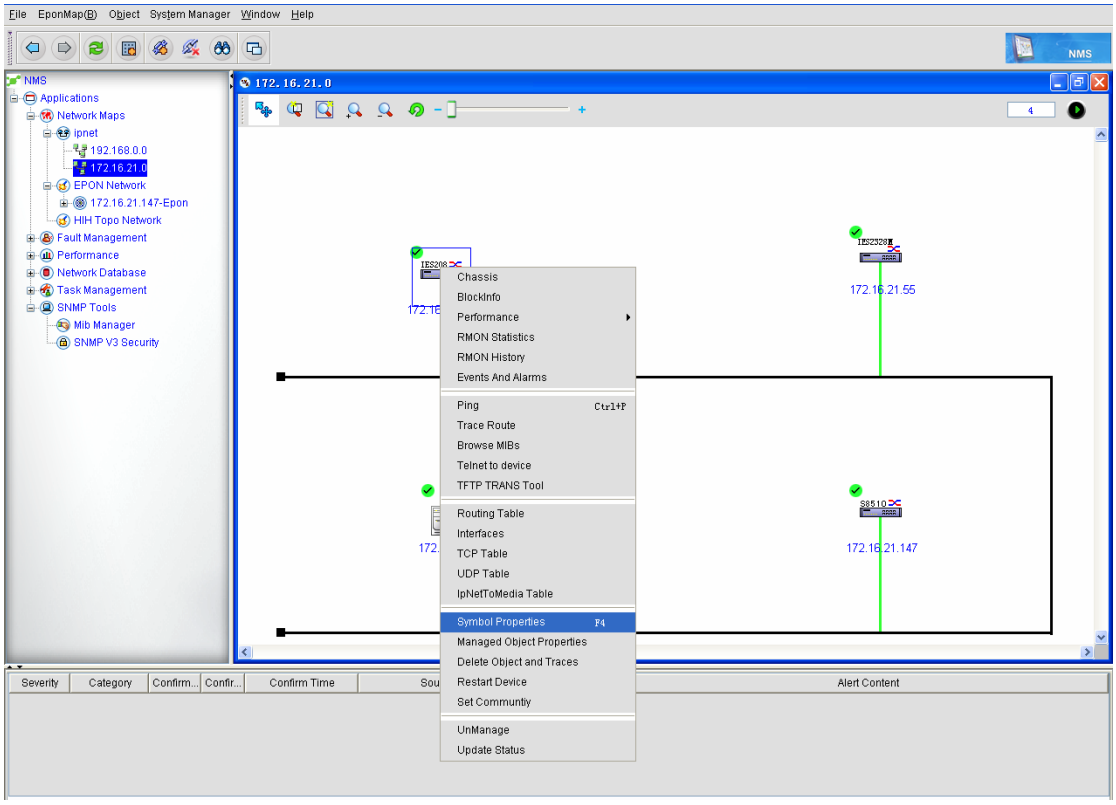


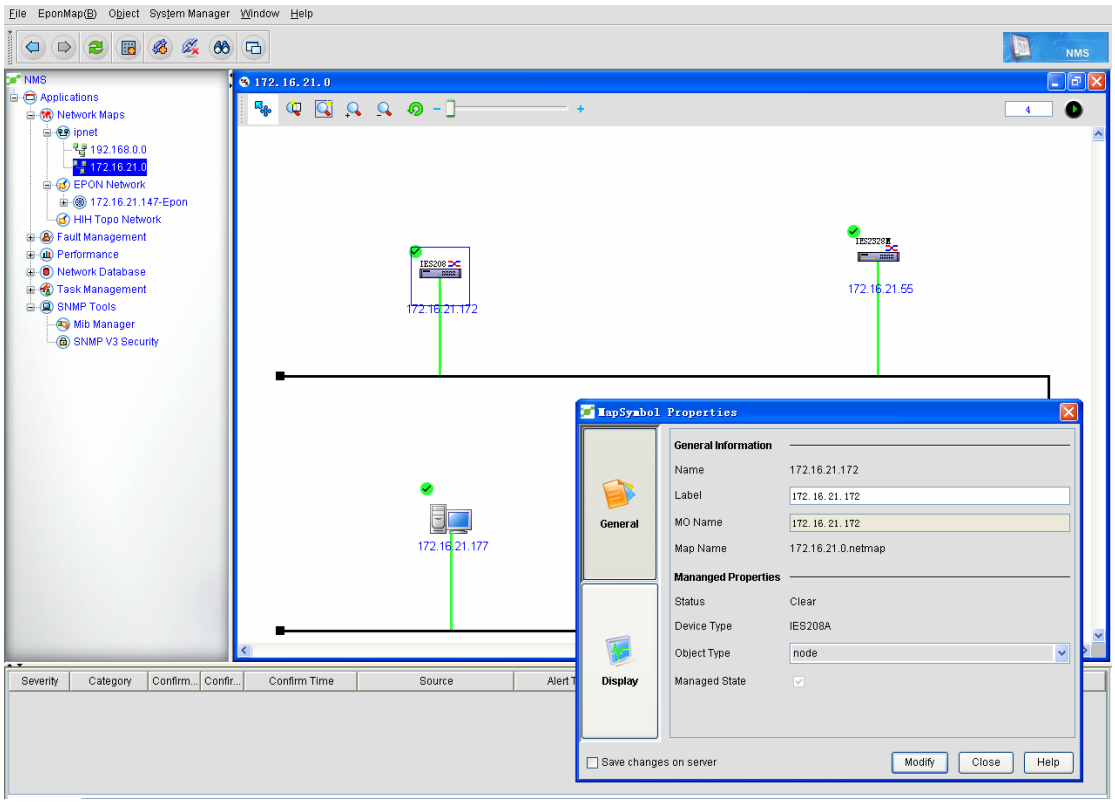


Collection statistics table: You can self-define the data statistics time to browse the statistics data.

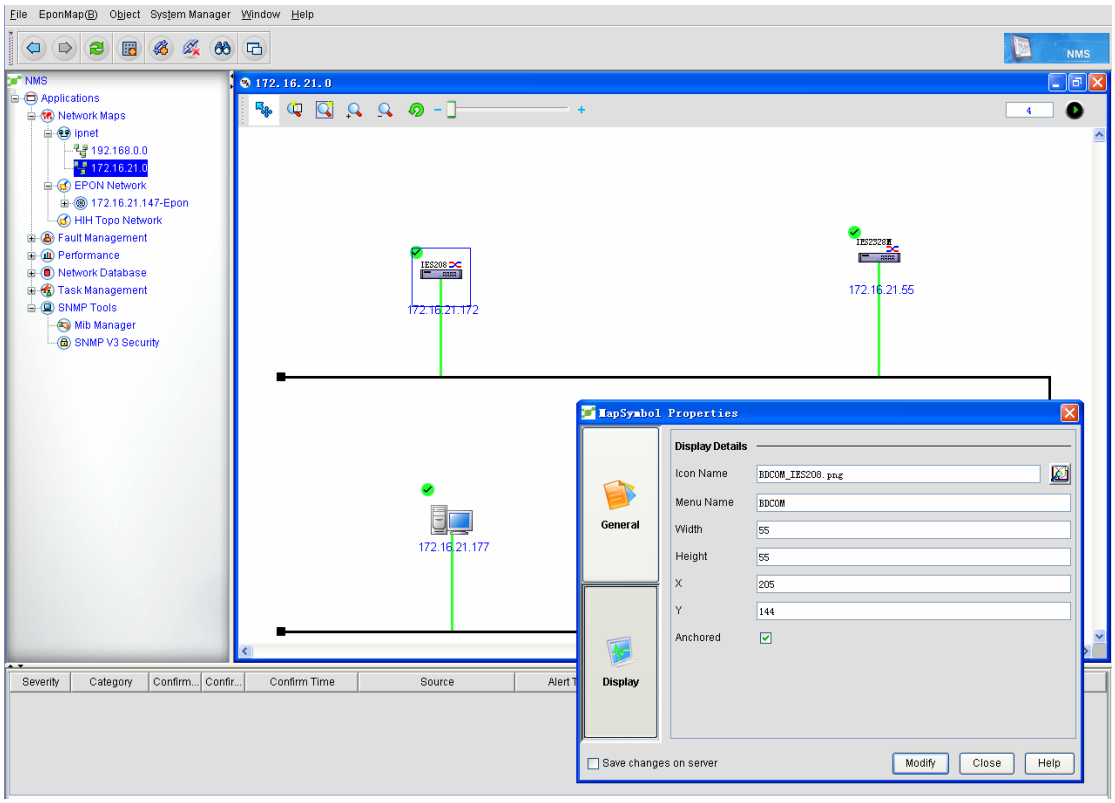
4.4 Symbol Attribute

The symbol attributes simply describe several attributes of a device, such as **Regular** and **Show**. The regular attributes are shown in the following figure:





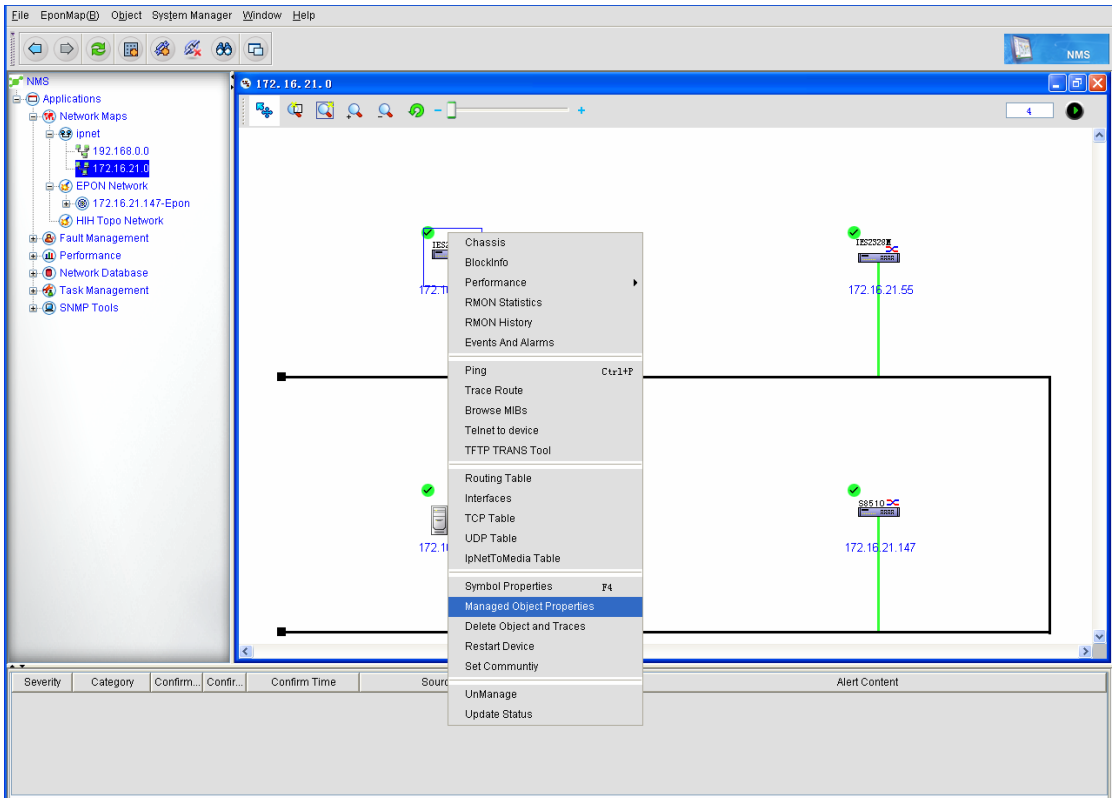
The **Show** attribute is used to set the display area, the map, the location and so on.

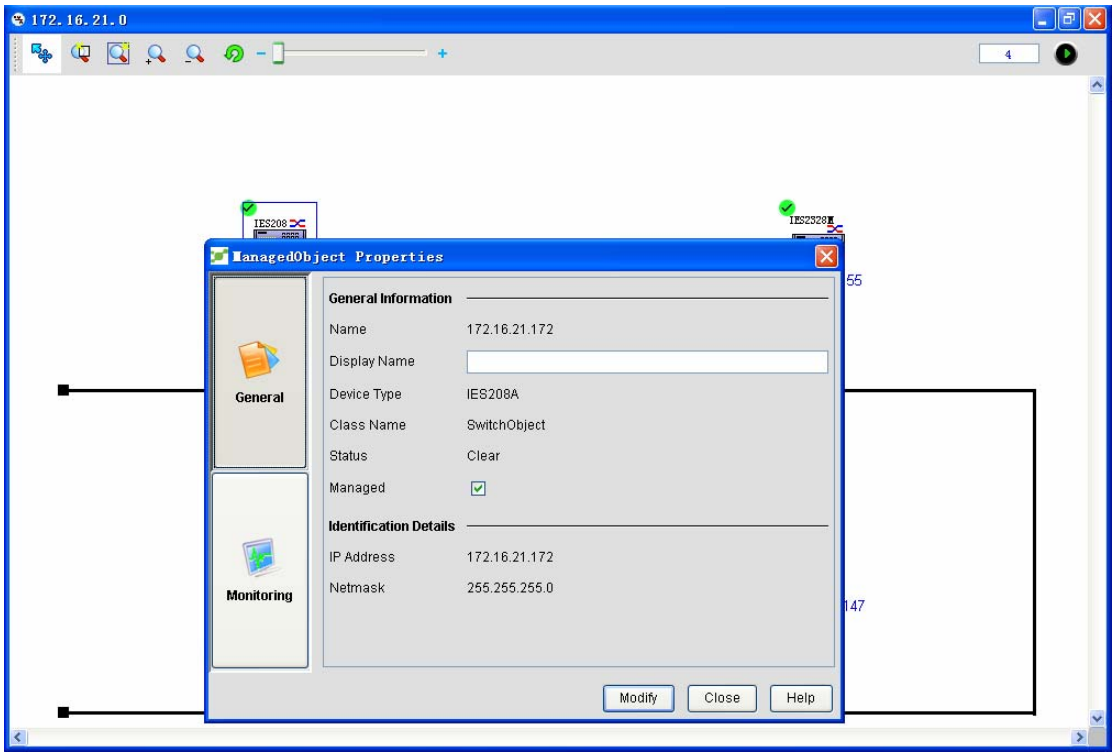


Click **Edit** to change the current attribute.

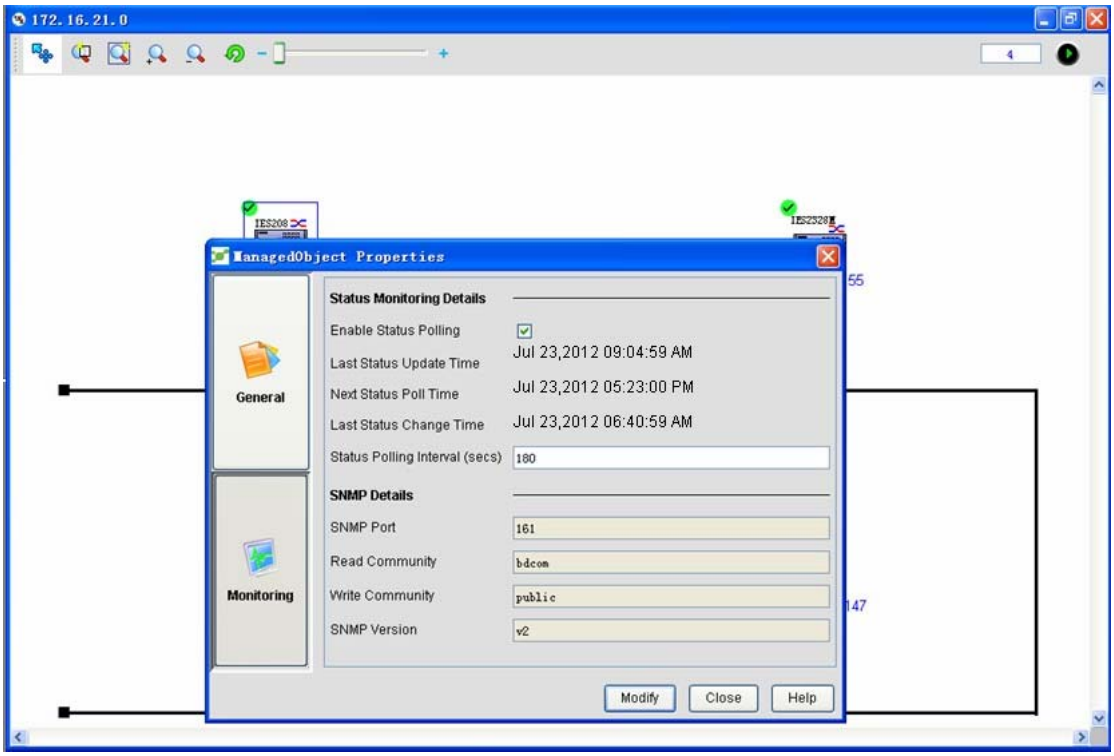
4.5 Attributes of the Managed Object

The attributes of the managed object show all kinds of data of the managed device, including SNMP. The section is similar to section 4.5. Some attributes are the same, such as the **Regular** attribute.





- **Monitor attribute:**

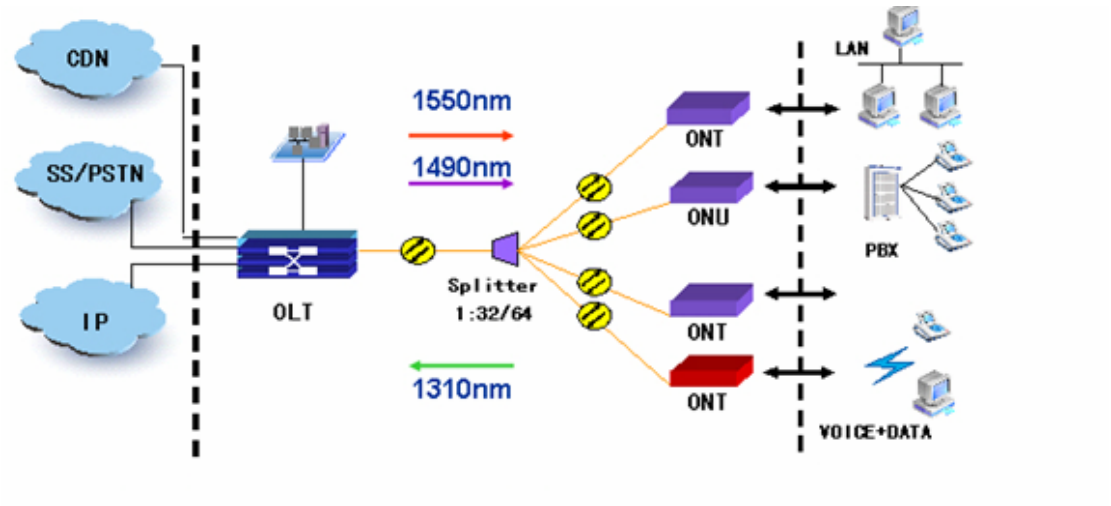


Here the polling and polling time of a device are displayed.

5 EPON Management

EPON is a new type of optical network access technology. It adopts the point-to-multipoint structure and the passive optical-fiber transmission. On the physical layer, EPON adopts the PON technology, while on the link layer, EPON uses the Ethernet protocol. The Ethernet access is realized through the topology of PON. Hence, it integrates the advantages of the PON technology and the Ethernet technology. These advantages include low cost, high bandwidth, expansibility, flexible and fast service regrouping, high compatibility and convenient management.

The regularly used EPON network structure is shown below:



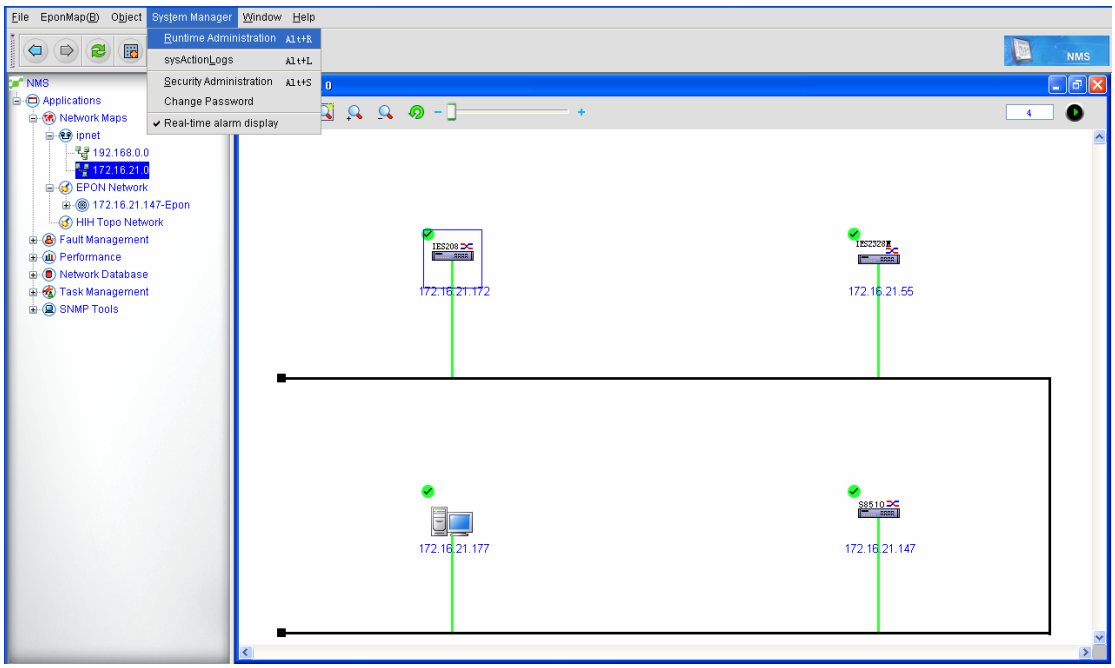
OLT-- optical line terminal
ONU--Optical Network Unit
ONT-- Optical Network Terminal
ODN -- Optical Distribution Network

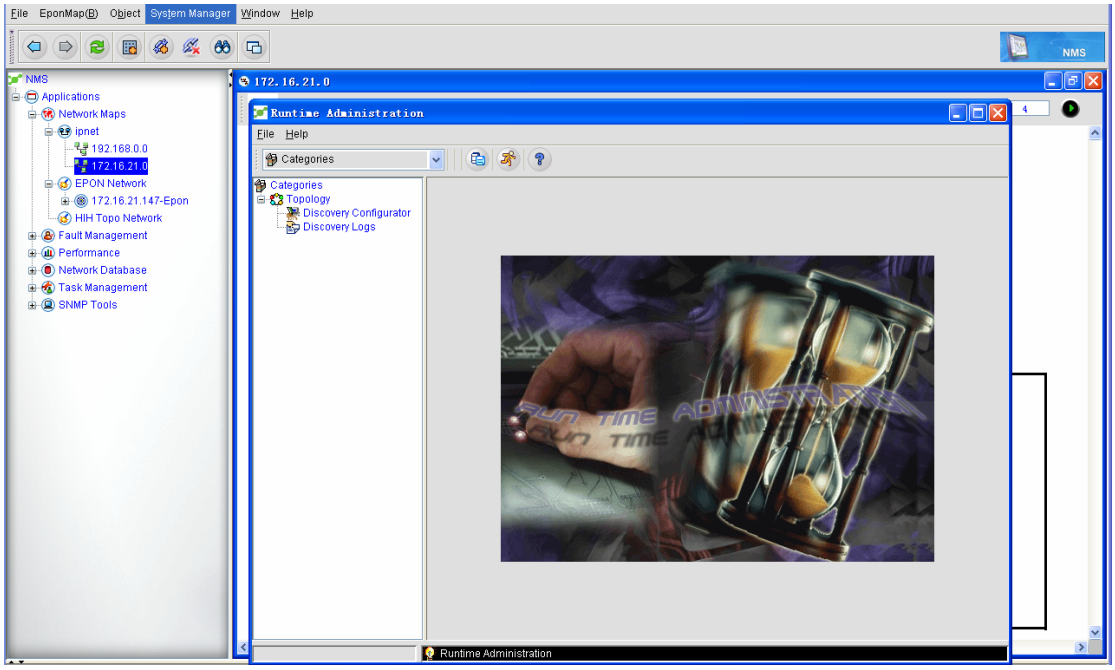
5.1 Device Discovery

Device discovery means to find devices in a network according to a designated parameter and then manage and maintain the devices in real time. In this section, the operation of discovering EPON devices through NMS will be mainly described.

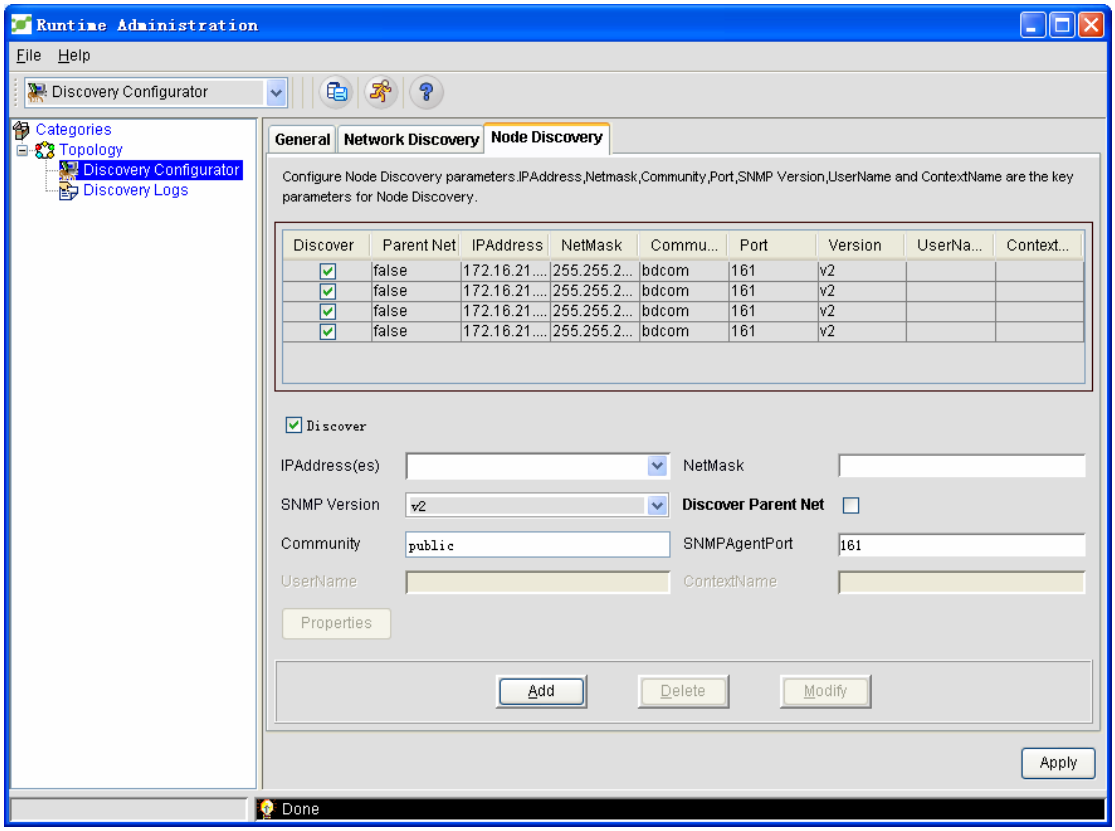
The operation procedure is shown below:

- Open the NMS client and pop up the homepage of NMS.
- Click **System Management -> Real-time Management**. See the following figure:





◆ Click **Topology -> Discovery Settings** on the real-time management window. Select **Node Discovery** and then enter the IP address and network mask of the to-be-discovered device. Click **Add**.

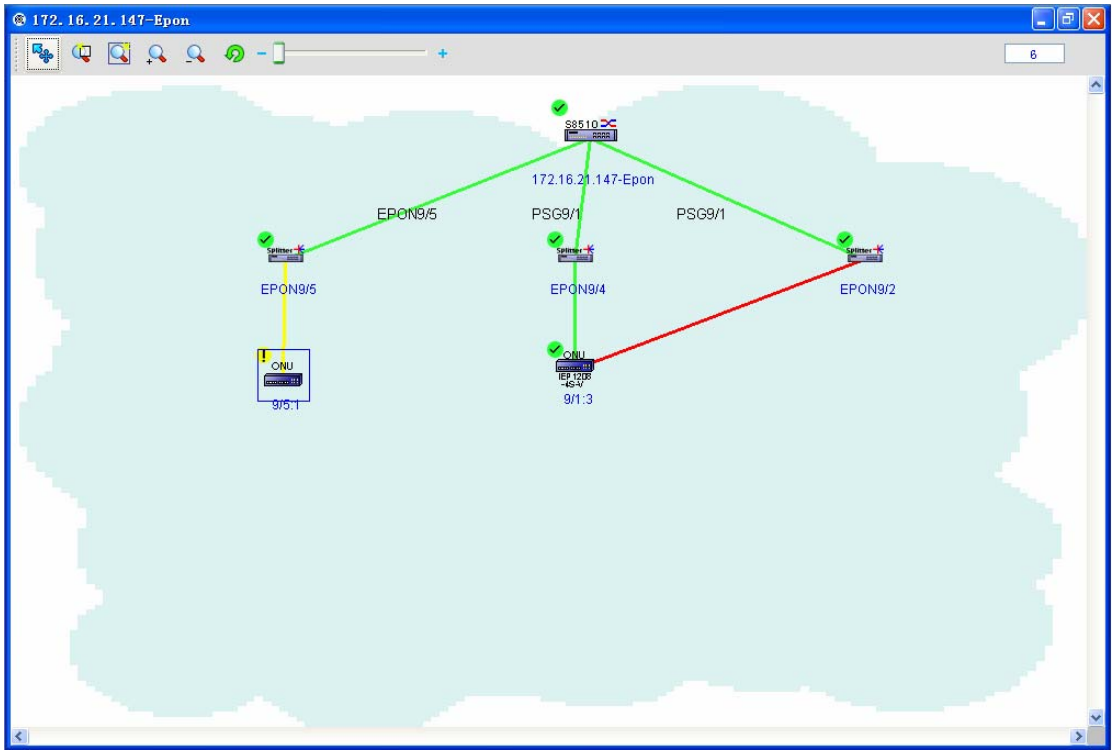


Parameter description

- The IP address must be the management address of OLT.
- The mask is entered according to the real mask of the local network, such as 255.255.255.0.
- SNMP (Simple Network Management Protocol) has three versions: v1, v2 and v3. You can select the version according to your equipment settings. At present, NMS support these three versions, but the default version is v2.
- If you choose the **Whether to discover the parent network** option, all manageable devices in the parent network where OLT belongs to will be displayed in the topology. You can make choice according to requirements.
- The community, a character string, is the text password between the management process and the agent process. It is used by SNMP to authenticate the SNMP control station from the SNMP agent; if a network is set to require authentication, SNMP will authenticate the community name and the IP address of the control station; if the authentication fails, SNMP will sent a trap message, showing a failed authentication, from the SNMP agent to the SNMP control station.
- The SNMP agent port is port 161 by default.

◆ Click **Apply**. The system then conducts device discovery according to the IP and network mask configured by the administrator.

◆ Close the real-time management window and then get the topology of the to-be-discovered device in the EPON topology. See the following figure:



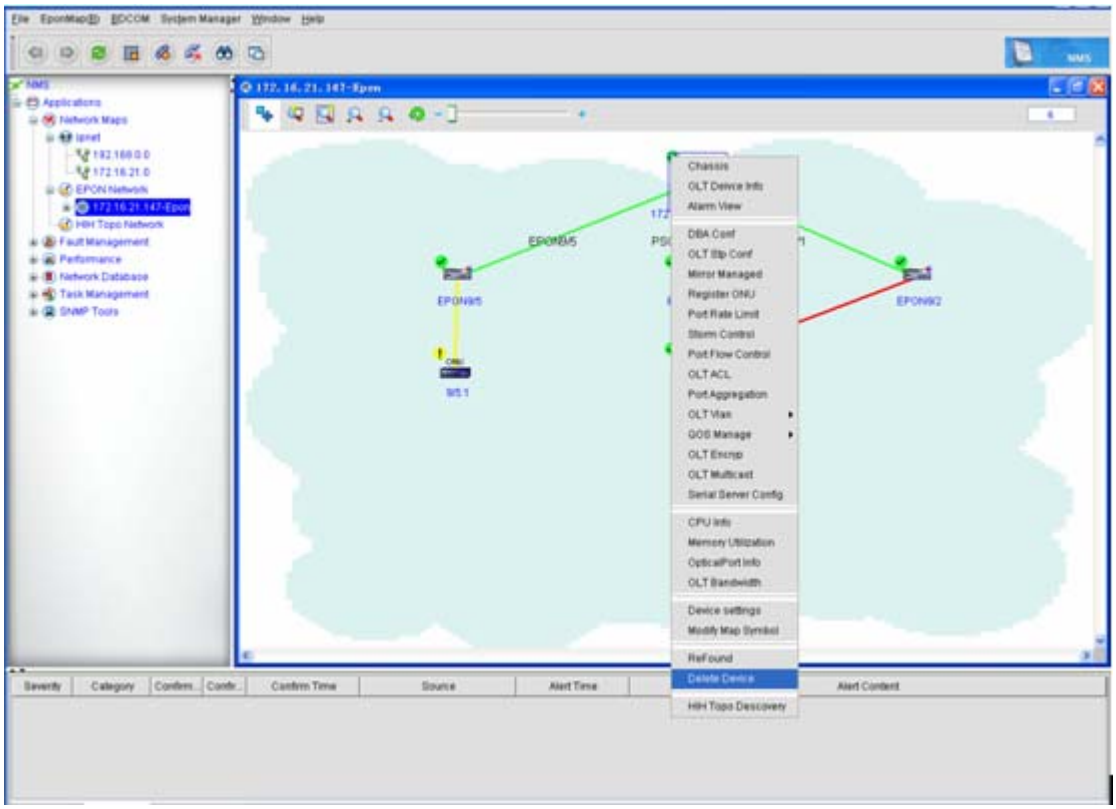
5.2 Deleting a Device

You can delete some devices that are not required management on NMS, which helps manage and maintain the network topology.

5.2.1 Deleting OLT

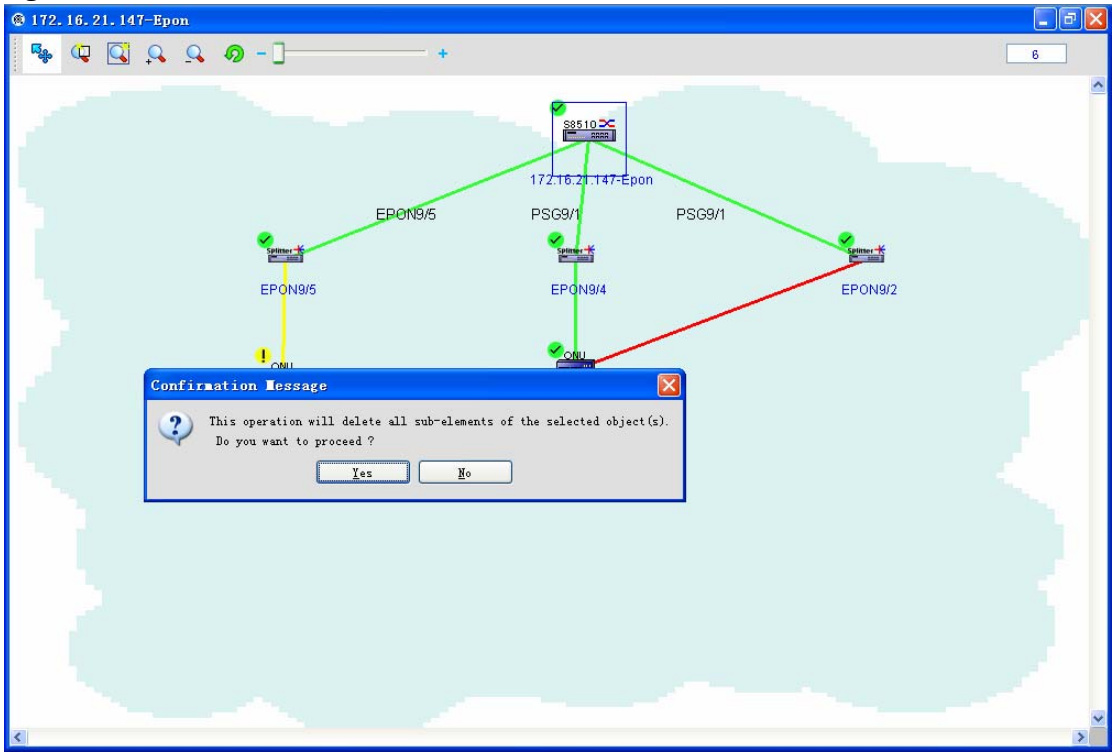
The operation procedure is shown below:

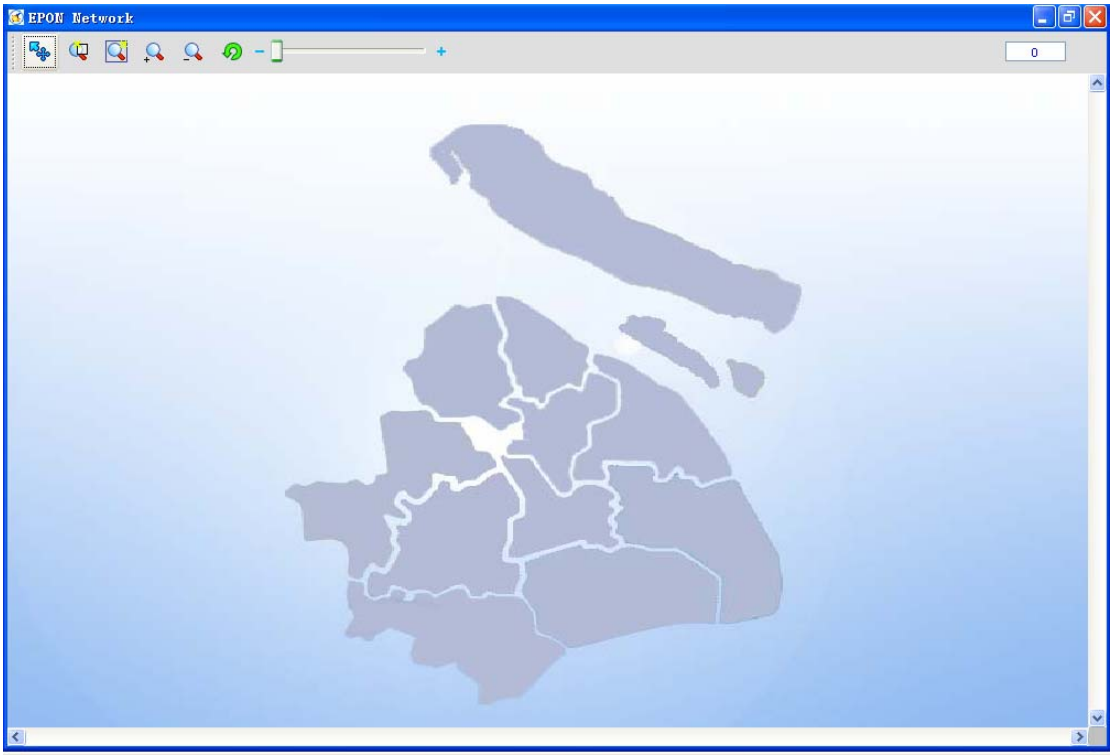
- Open the EPON topology and right click the OLT icon. The following menu appears:



- On the menu, choose **Delete a device**. The system will obtain related information according to OLT.

If you delete OLT, all other devices on OLT will also be deleted. See the following figure:



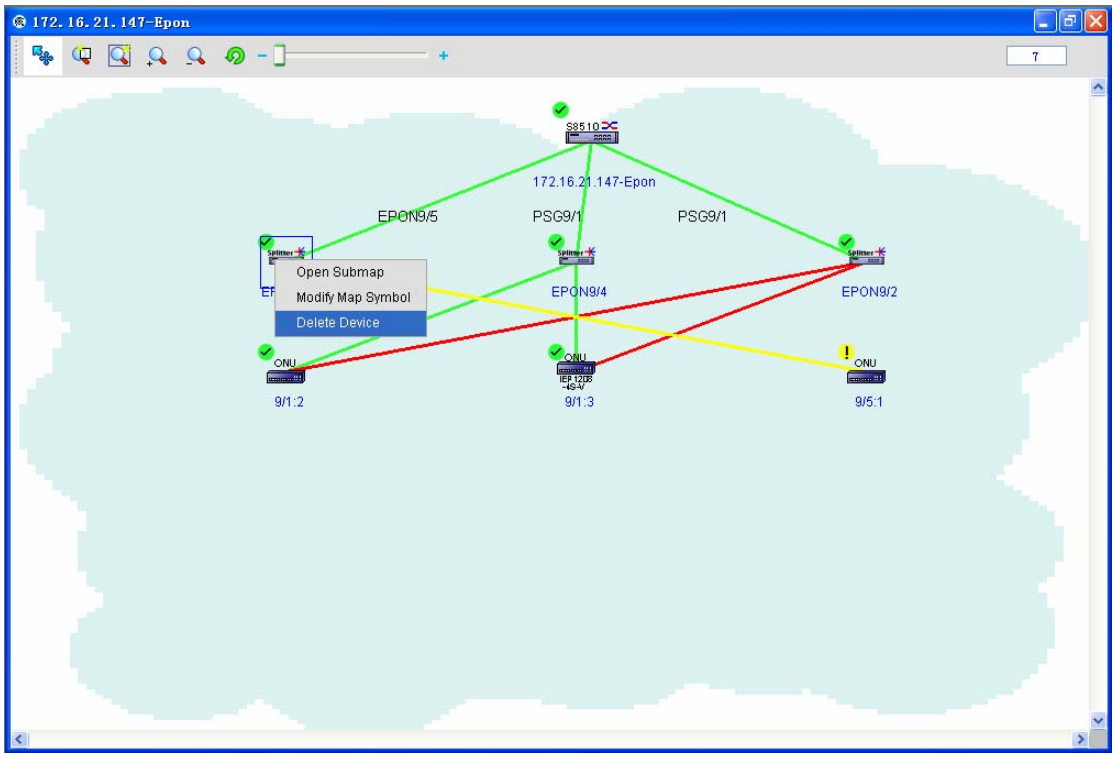


The administrator also needs to note that the deletion of OLT means to delete OLT itself and its connected devices, so the administrator shall confirm it before this operation.

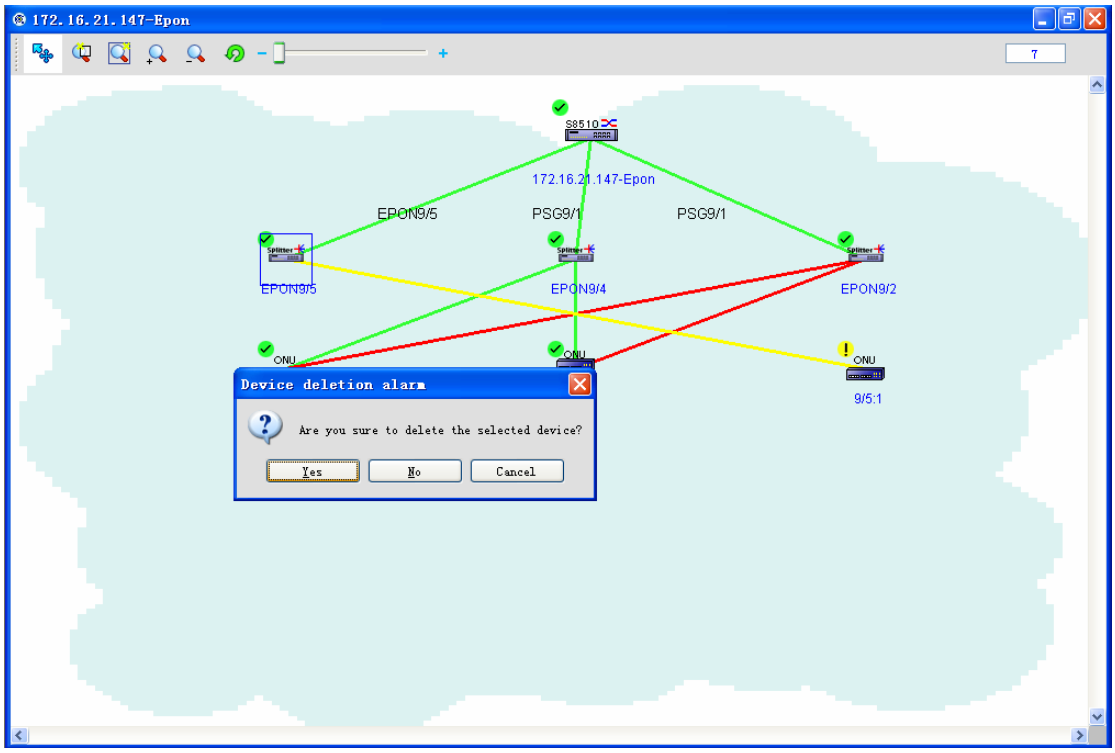
5.2.2 Deleting the Optical Splitter

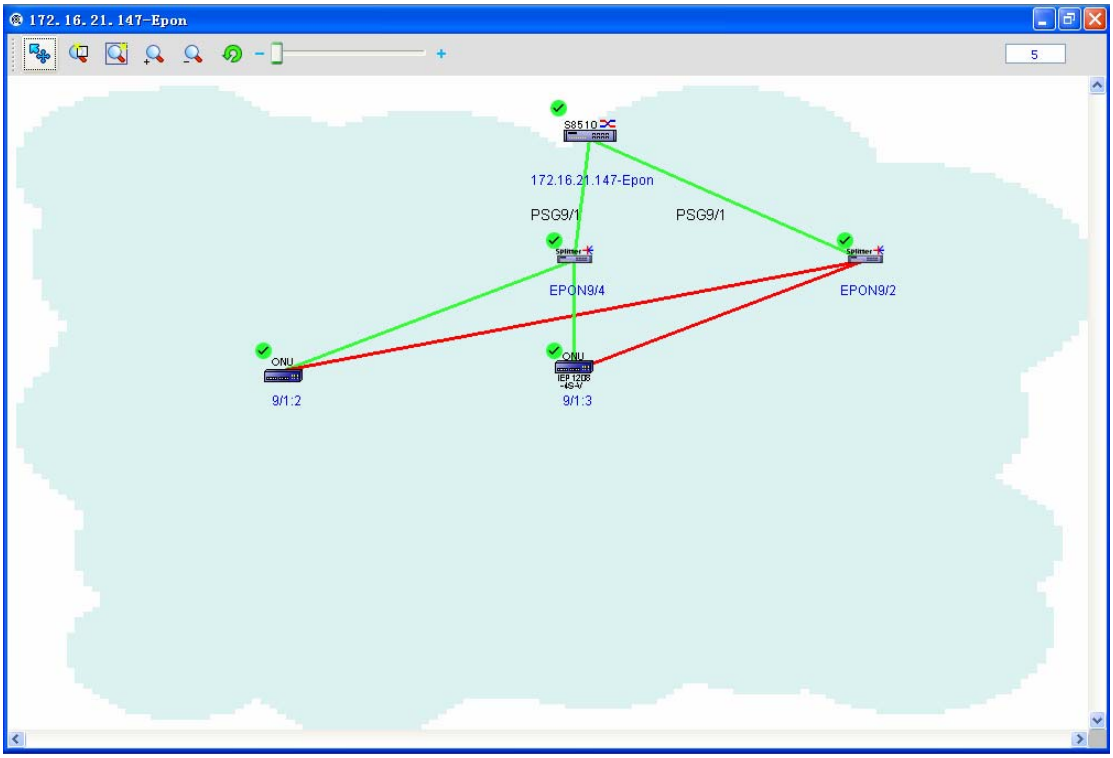
The operation procedure is shown below:

- Open the EPON topology and right click the Splitter icon. The following menu appears:



◆ Click **Delete a device**. The system obtains related data from a optical splitter that the administrator selects, and then delete the optical splitter. See the following figure:



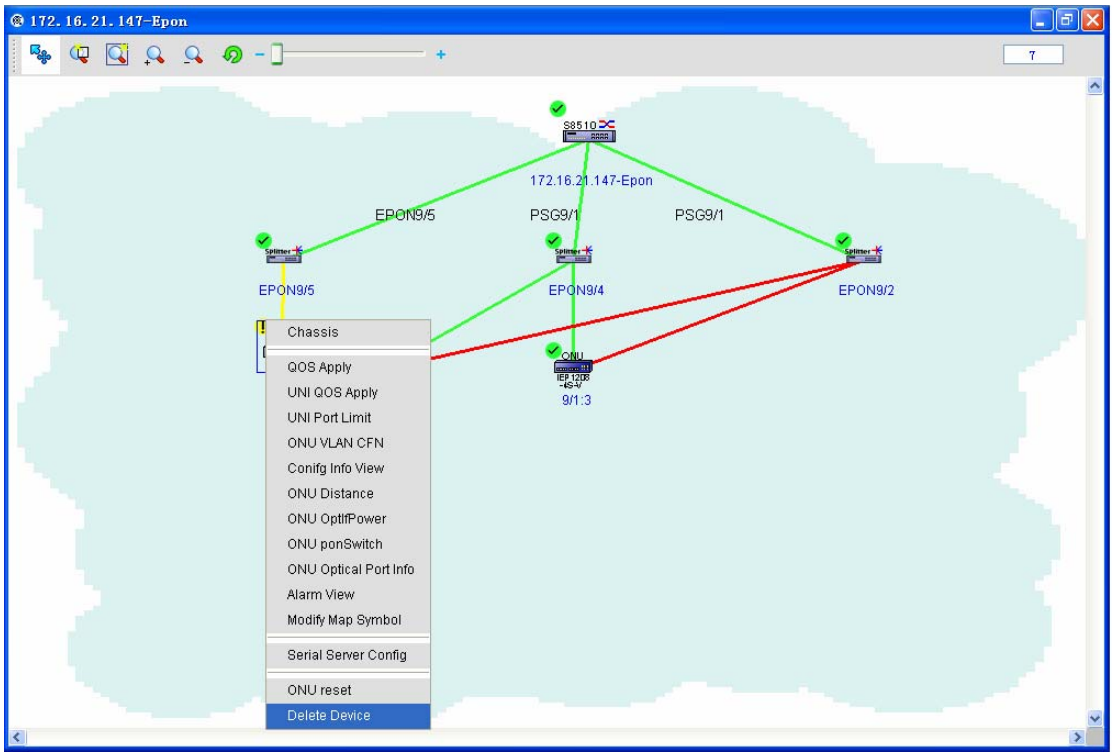


If you delete an optical splitter, all downstream ONUs, which connect the optical splitter, will also be deleted. The administrator must confirm your operation before performing it.

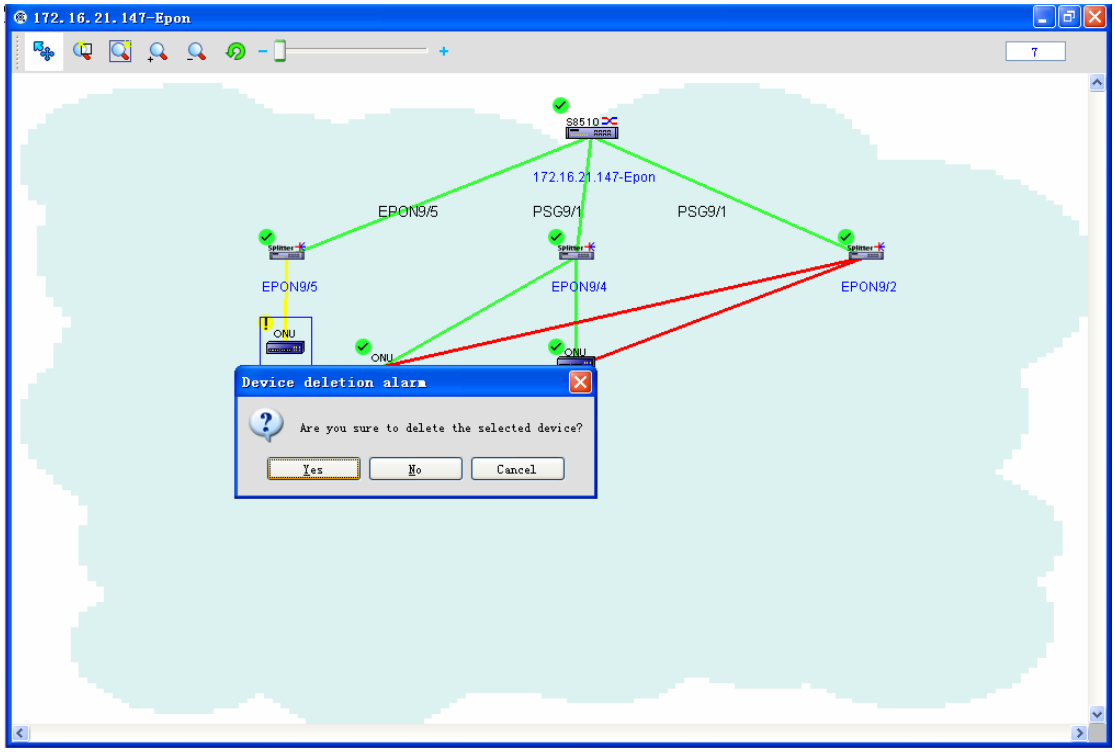
5.2.3 Deleting ONU

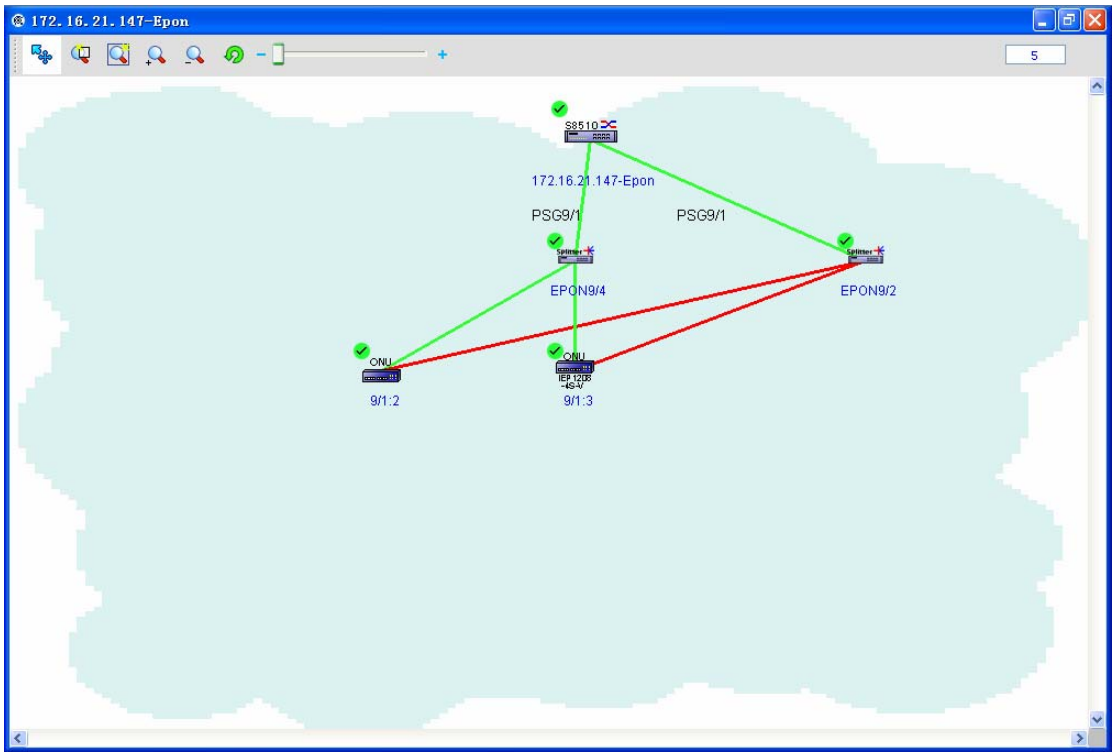
The operation procedure is shown below:

- Open the EPON topology and right click the ONU icon. The following menu appears:



After you confirm to delete it, you will find the results, as shown in the following figure:





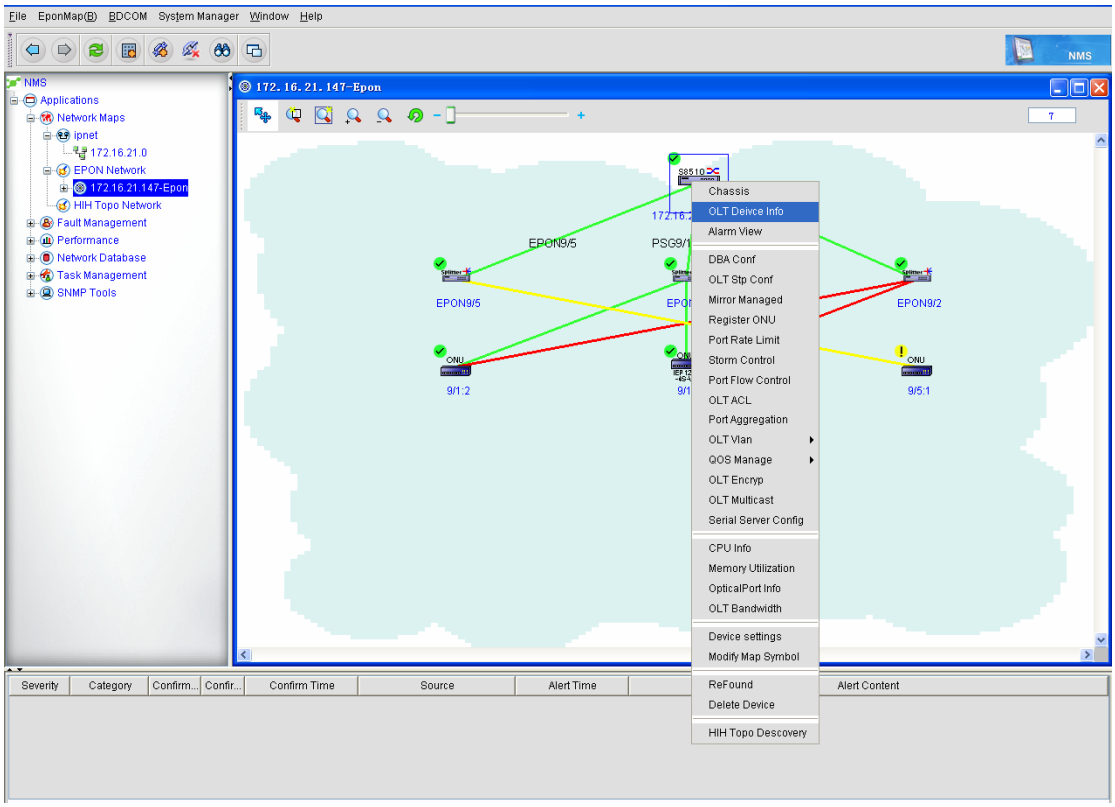
- Click **Delete a device**. The system deletes an ONU according to the related information about ONU that the administrator selects. What's more, during ONU deletion, the system will automatically judge the number of other ONUs that the same upstream optical splitter connects. If the number of ONUs is zero, the system will delete this upstream optical splitter at the same time; If the number is not zero, the upstream optical splitter will not be deleted.

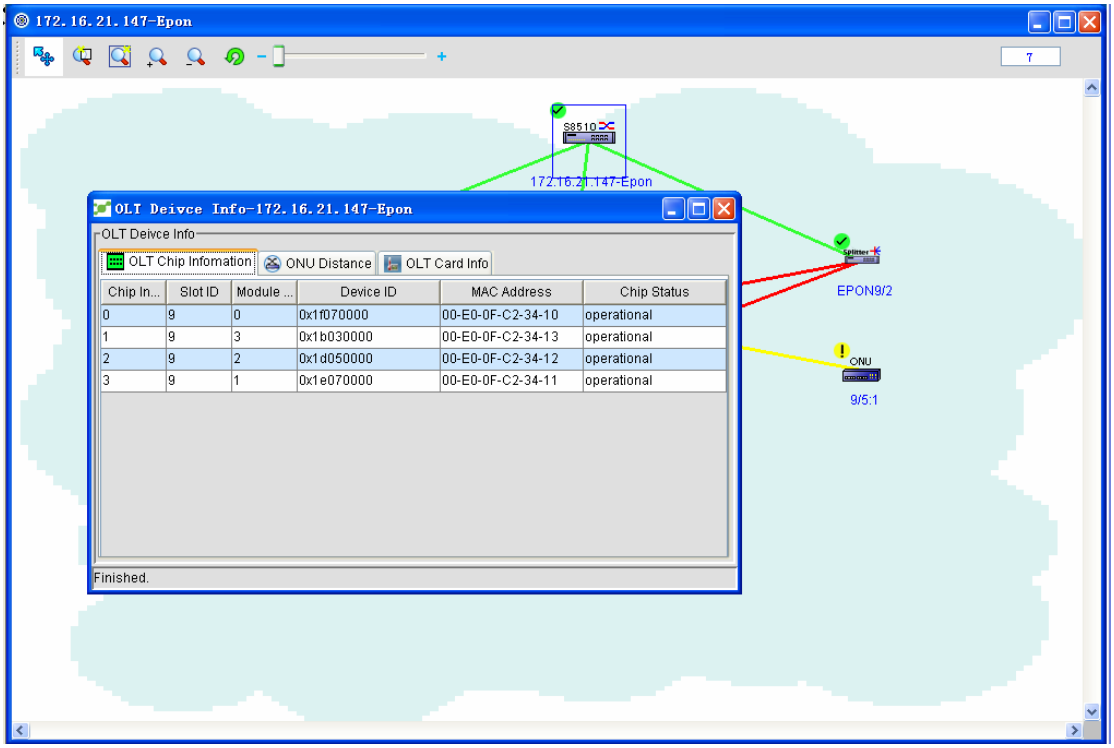
5.3 OLT Settings

OLT settings management includes: browsing basic OLT information, setting VLAN, DBA and multicast, registering and deleting ONU, and setting STP attributes.

5.3.1 Basic OLT information

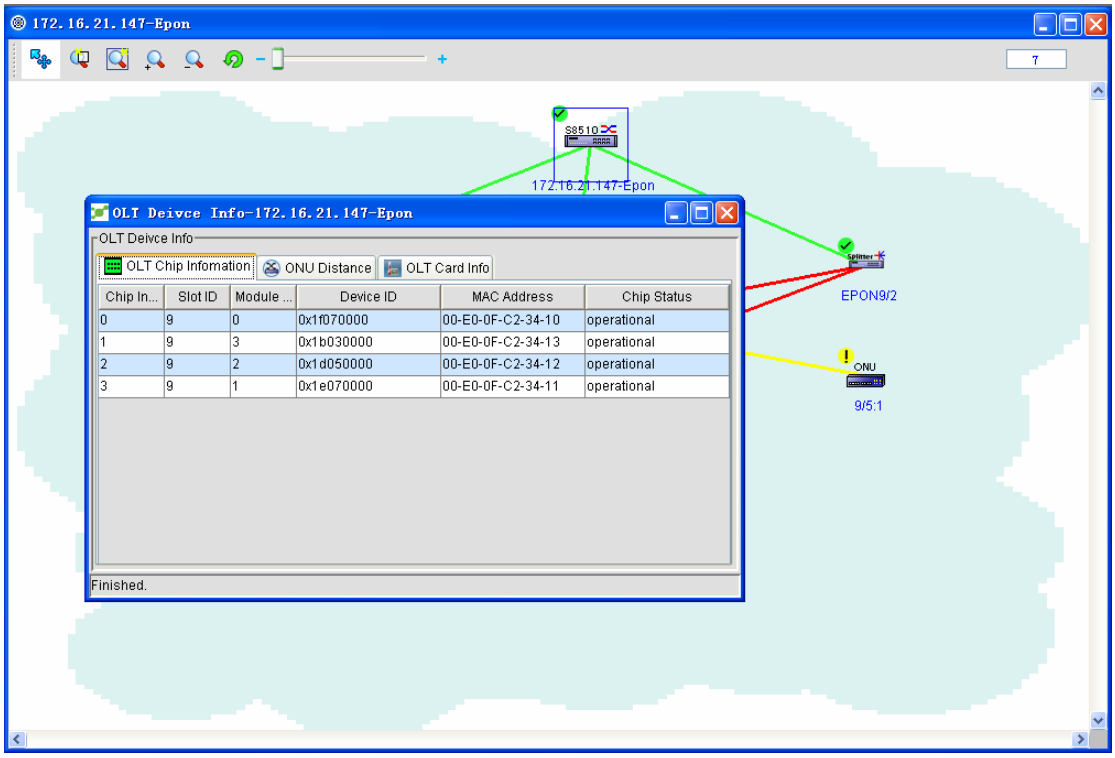
On the basic OLT information page, you can only browse OLT's slots, OLT's chips and ONU's distances. You have no right to access the basic OLT information at present. On the basic OLT information page, right click the OLT icon and then click **Basic information**. A page then appears, as shown in the following figure:



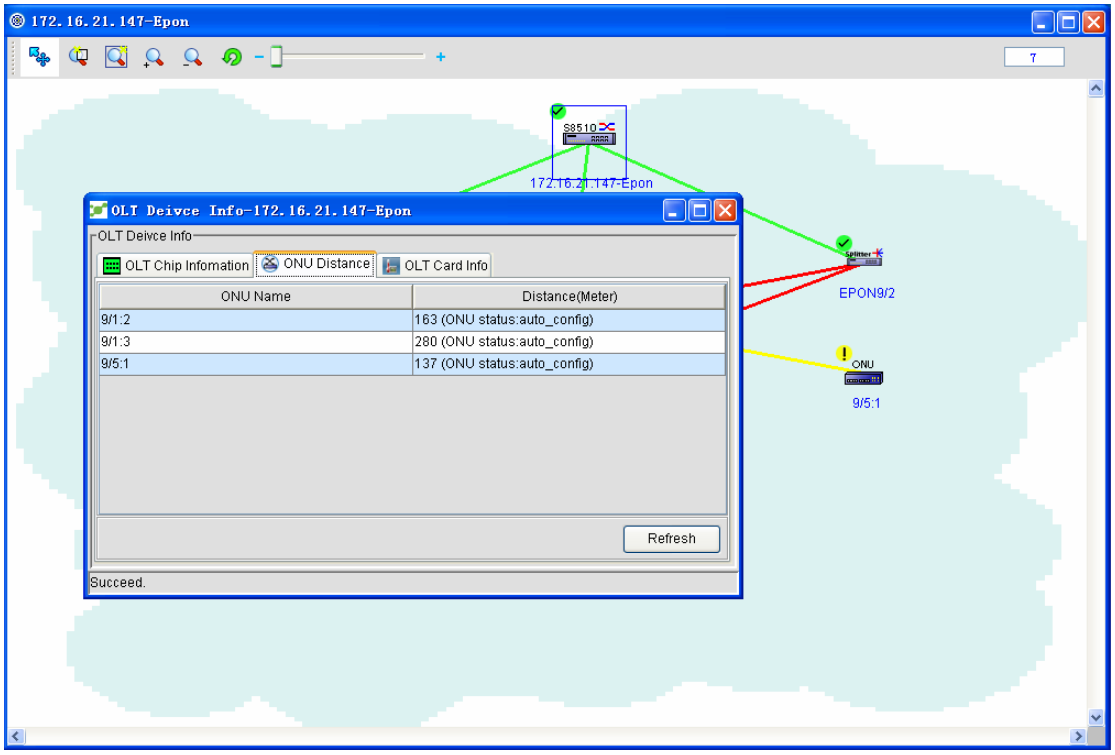


The figure above shows OLT's slots.

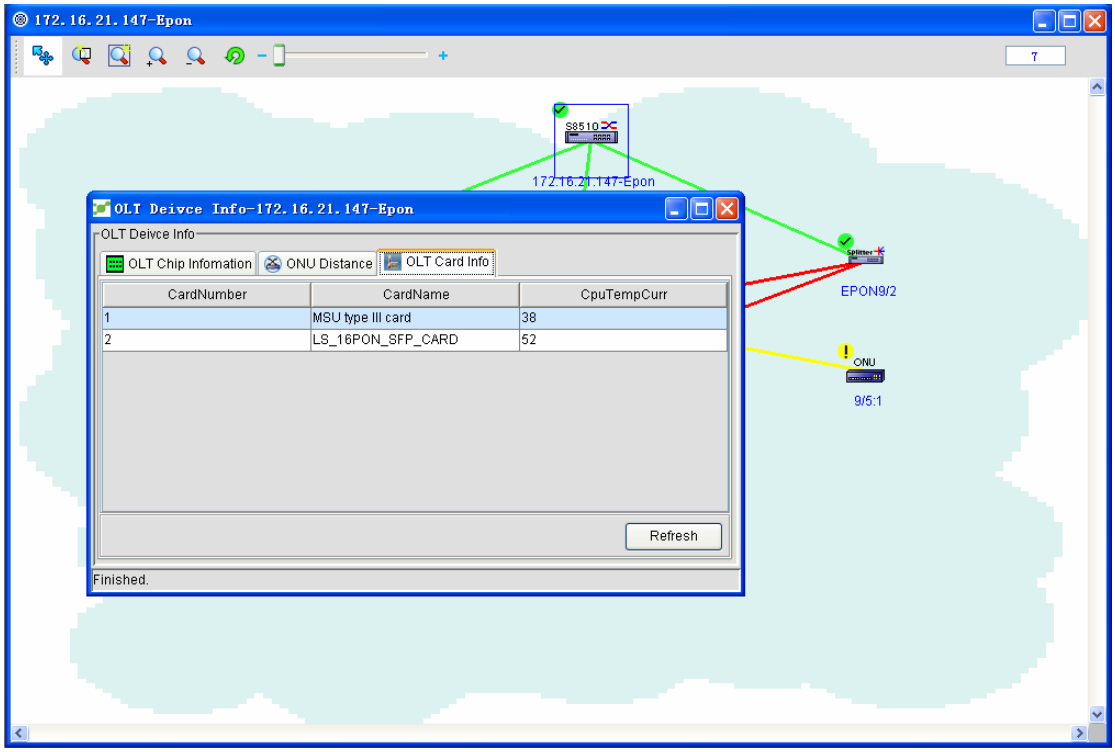
Click **Chip** and then you can browse the related information about chips. See the following figure:



Click **ONU's distance** and then you can browse the distance between ONU and OLT. See the following figure:

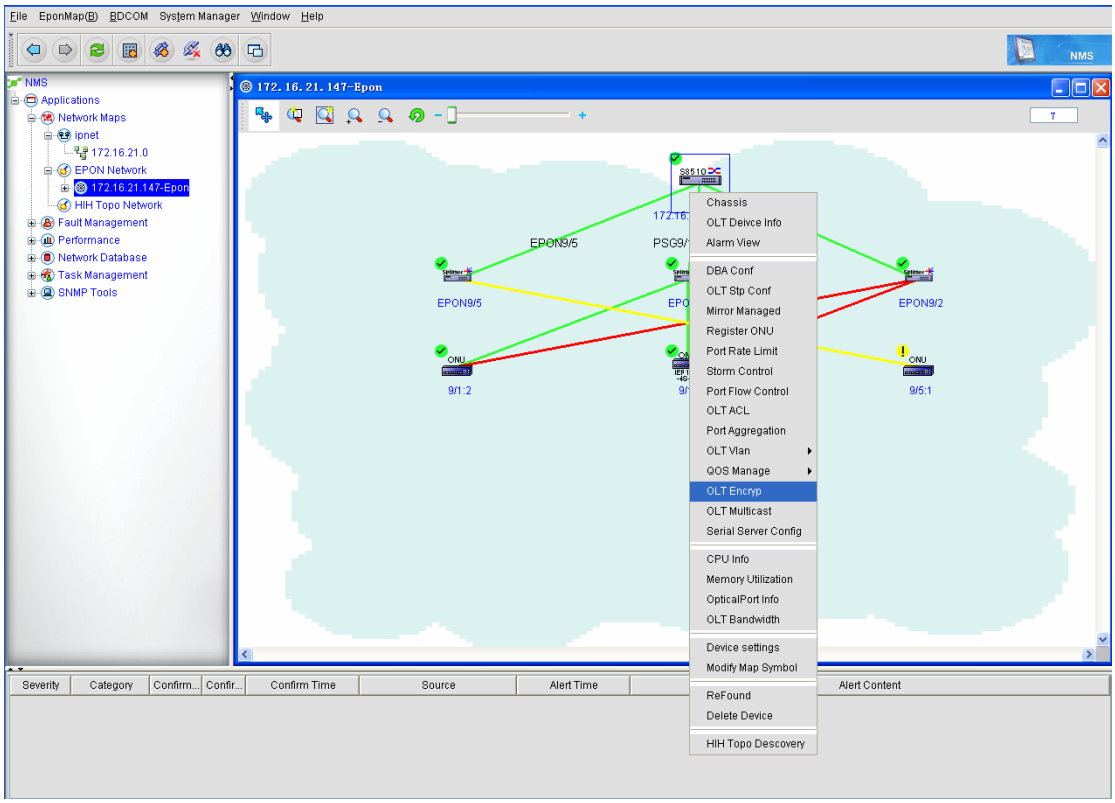


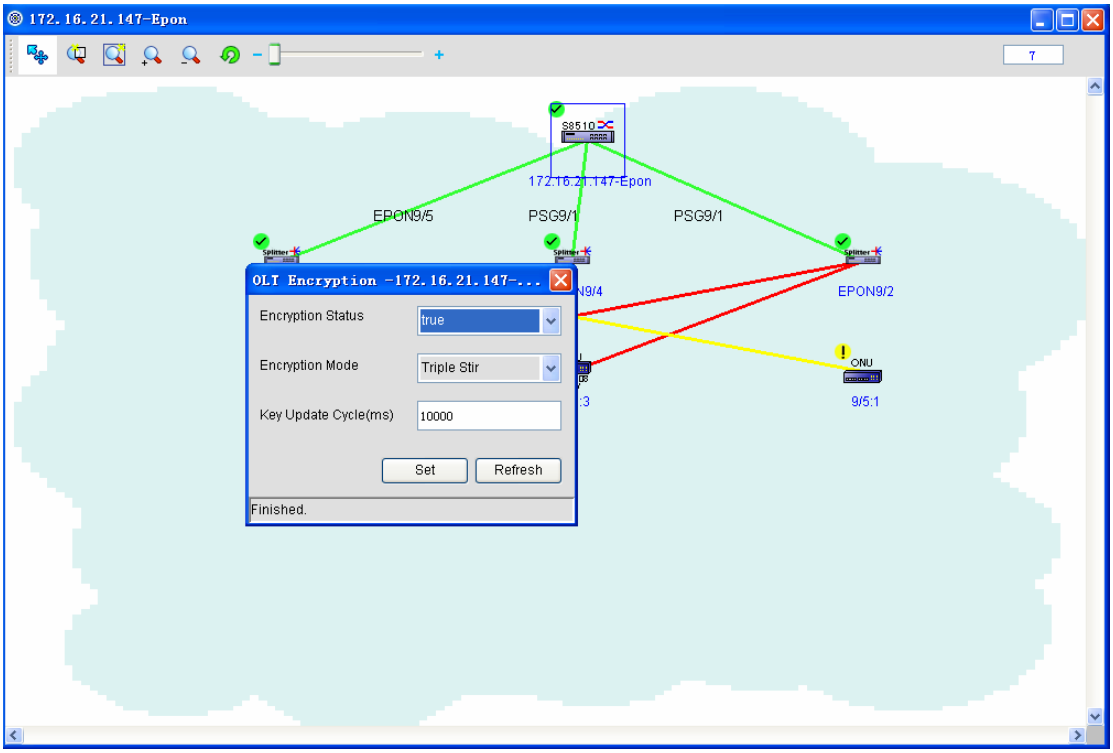
Click **Card's temperature** and you can browse the temperature of each OLT's card. See the following figure:



5.3.2 OLT encryption

OLT encryption means to set the encryption status, the encryption mode and the key update time. The encryption mode only supports CTC-churning (2) at present. If any need, other encryption modes will be added later. right click the OLT icon and then click **Encryption settings**. A page then appears, as shown in the following figure:



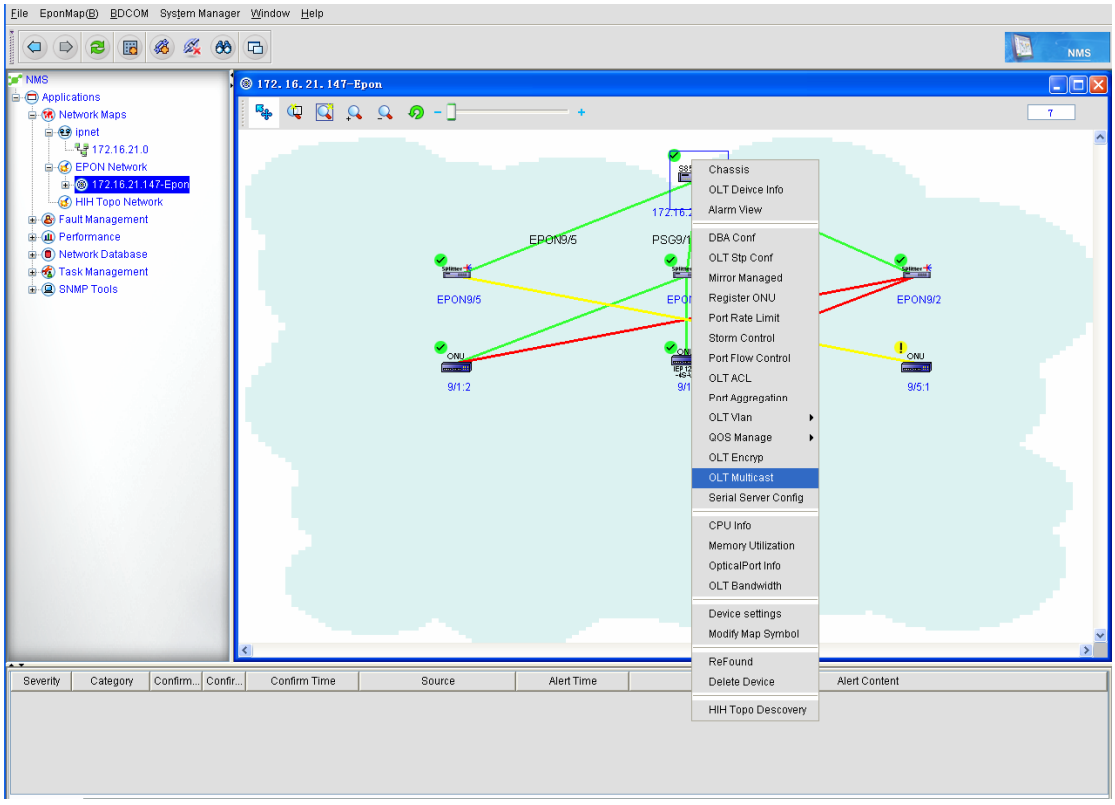


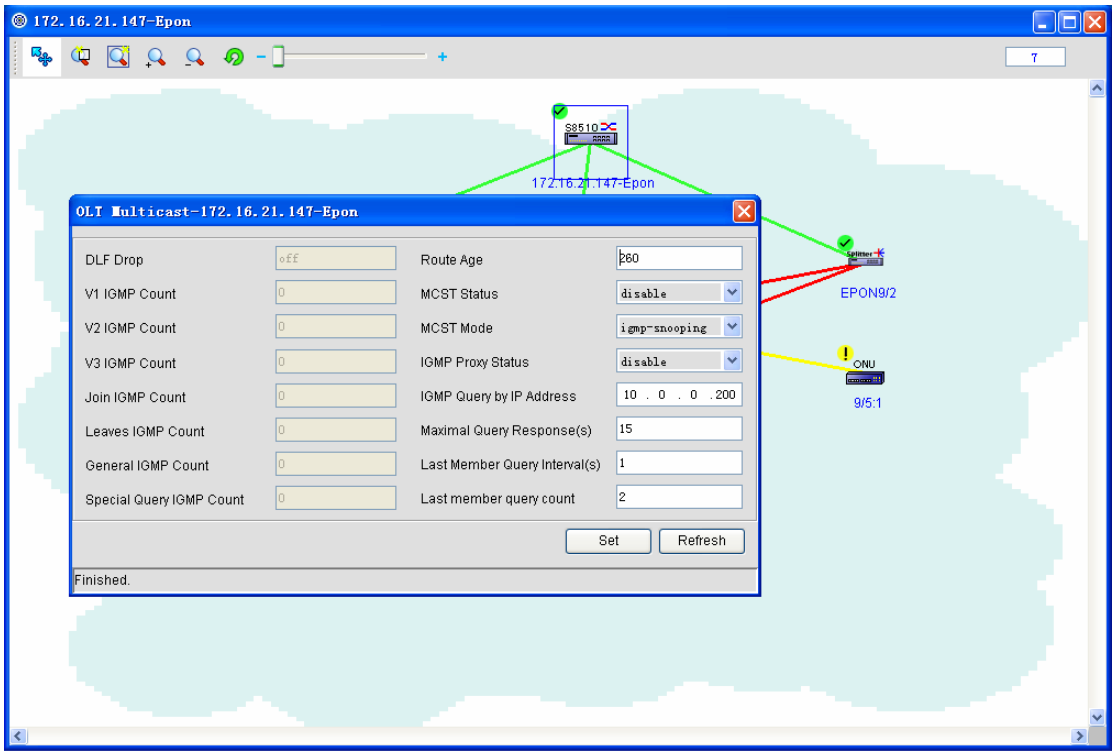
The configurations above are the default configuration, but you can set them according to your own requirements.

5.3.3 OLT multicast configuration

Multicast transmission: a point-to-multipoint connection between the sender and each receiver will be established. If a sender transmits the same data to multiple receivers at the same time, the sender only needs to copy a same packet. So multicast transmission improves the efficiency of data transmission, and reduces the possibility of congestion in the backbone network.
IGMP runs between the host and its directly-connected multicast router, through which the host notifies the local router to join in and receive the information from a specific multicast group and at the same time through which the multicast router checks periodically whether a known multicast member in LAN is in positive status (whether the network segment has a member to belong to a multicast group). IGMP has three versions: IGMPv1, IGMPv2 and IGMPv3. The following is OLT multicast settings.

You can set some global attributes on the OLT multicast configuration page. Right click the OLT icon and then click **Multicast settings**. A page then appears, as shown in the following figure:





Note: The grey part on the left of the figure above cannot be modified.

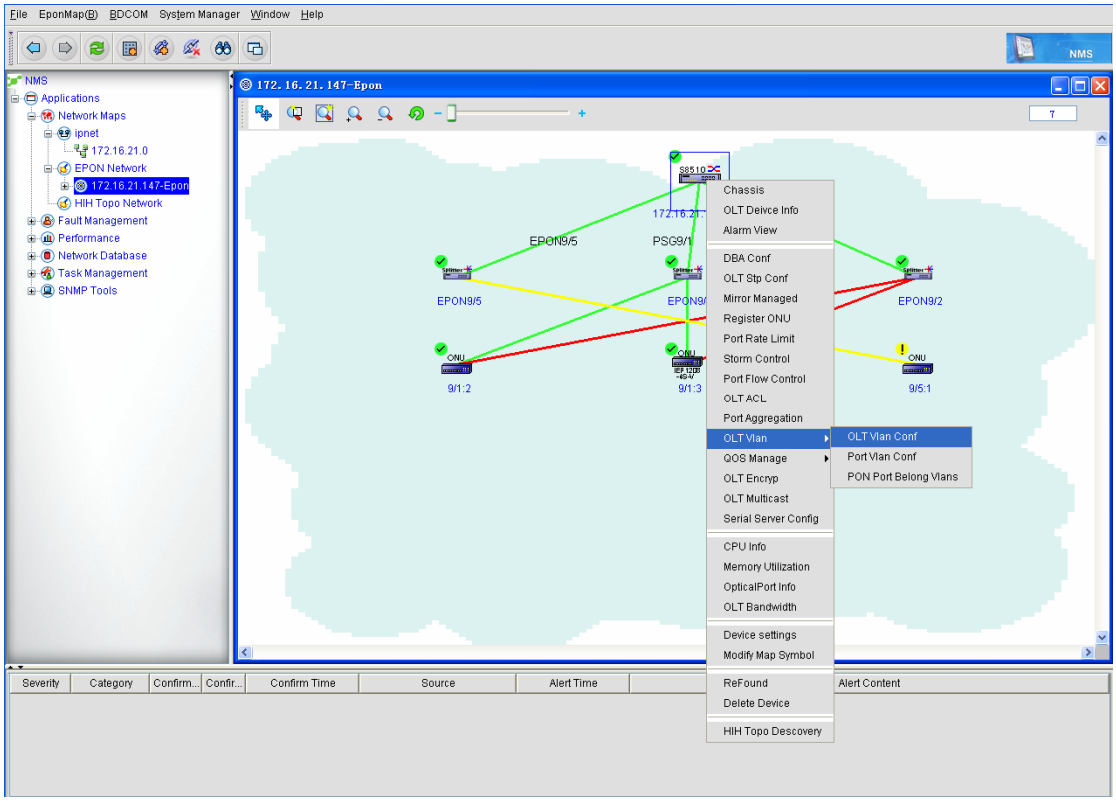
5.3.4 OLT VLAN settings

5.3.4.1 OLT VLAN

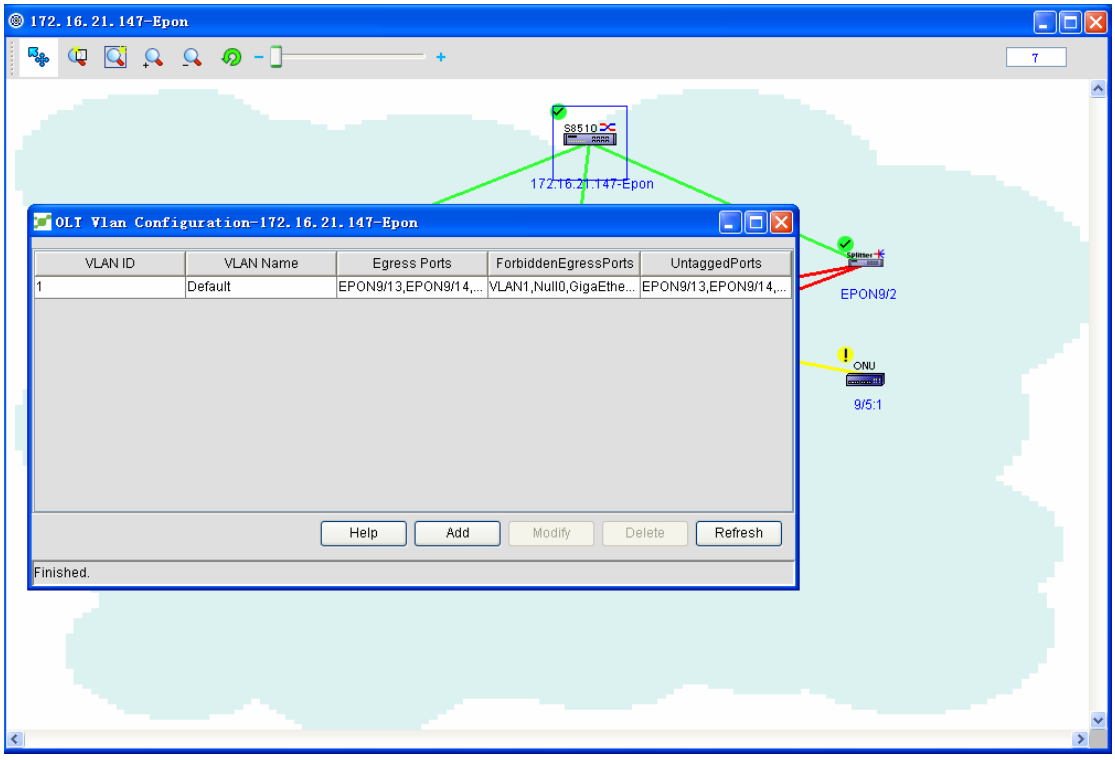
VLAN logically classes LAN equipment into different network segments and realizes the data exchange between different virtual groups. The emerging VLAN technology is applied in switches and routers, especially for the former. However, it does mean that all switches has this functionality , and only L3 switches with the VLAN protocol can own this functionality. You can browse the related information about the corresponding switches.

The emergence of VLAN is mainly to solve the problem that the broadcast cannot be limited during switches' interconnection in LAN. This technology can divide a LAN into multiple logical LANs. Each LAN functions as a broadcast area. The communication between hosts in VLAN is just like in one LAN and VLANs cannot directly interconnect. In this way, the broadcast packets are limited in one VLAN.

Right click the OLT icon and then click **VLAN management**. A page then appears, as shown in the following figure:



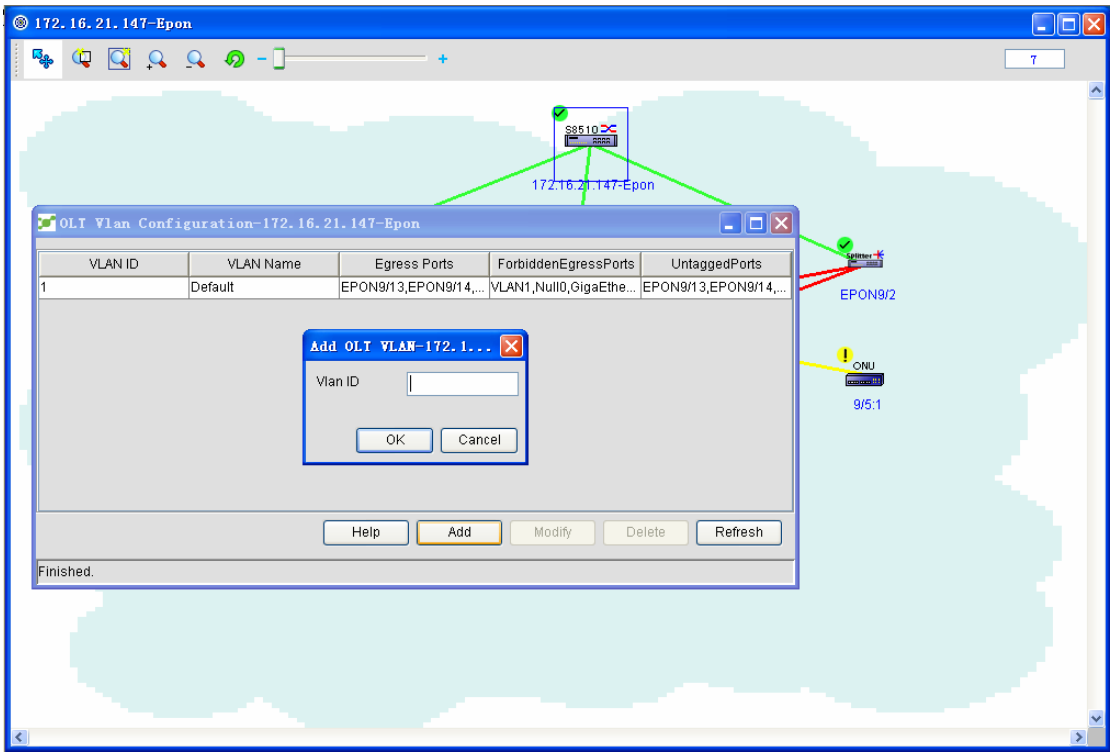
The VLAN configuration page is shown in the following figure:

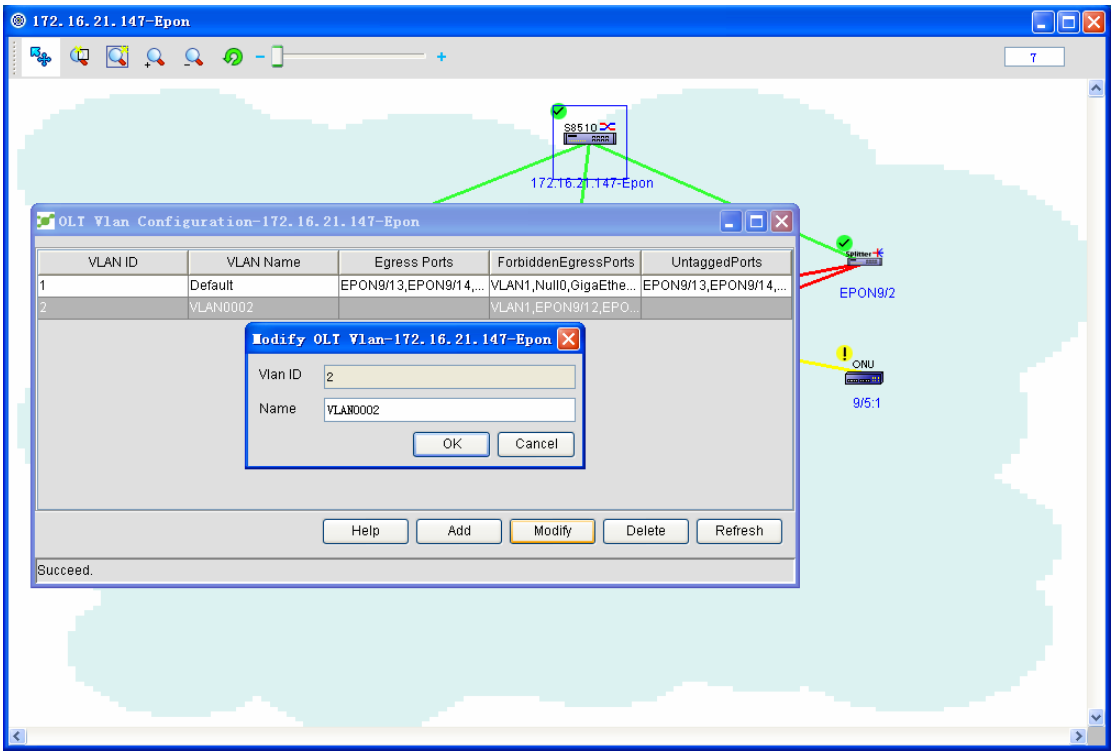


The VLAN settings has the following functions:

- Add a VLAN:

Click **Add**. A page appears, as shown in the following figure:

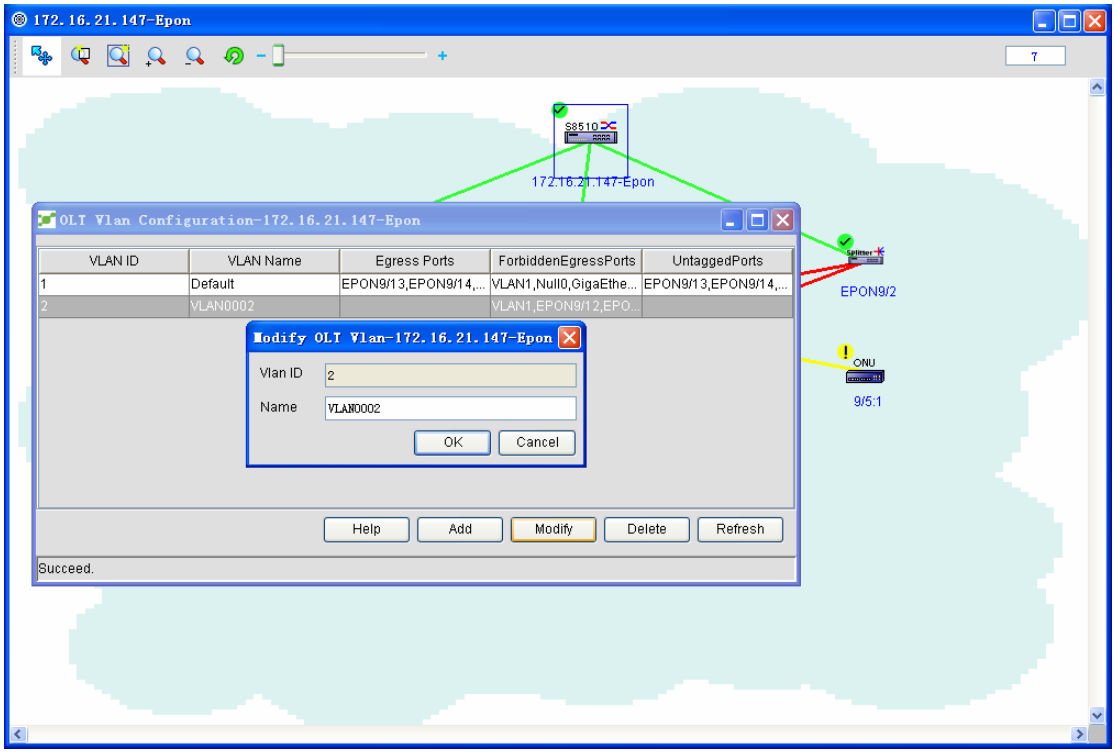




Enter a VLAN ID and then click **OK**. A VLAN is added. An existent VLAN ID cannot be added twice.

◆ Change the VLAN name:

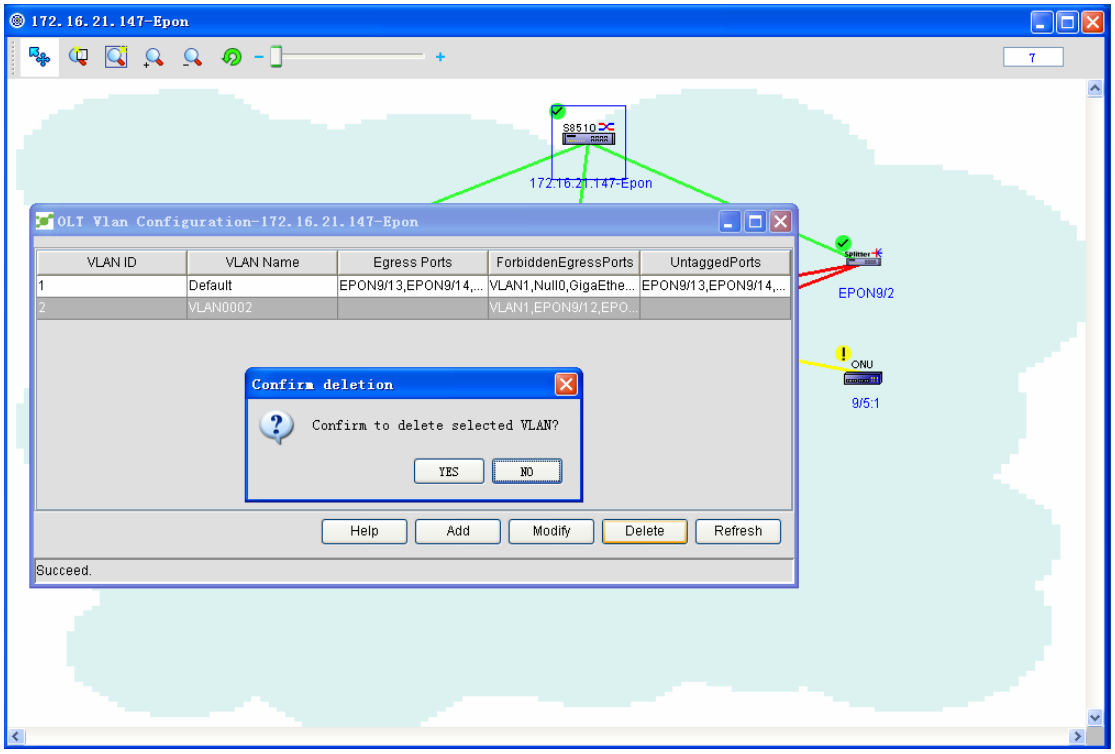
On the VLAN configuration page, if you select a VLAN and click **Edit**, the following page appears:



Note: The VLAN whose VLAN ID is 1 cannot be modified.

◆ Delete one or multiple VLANs:

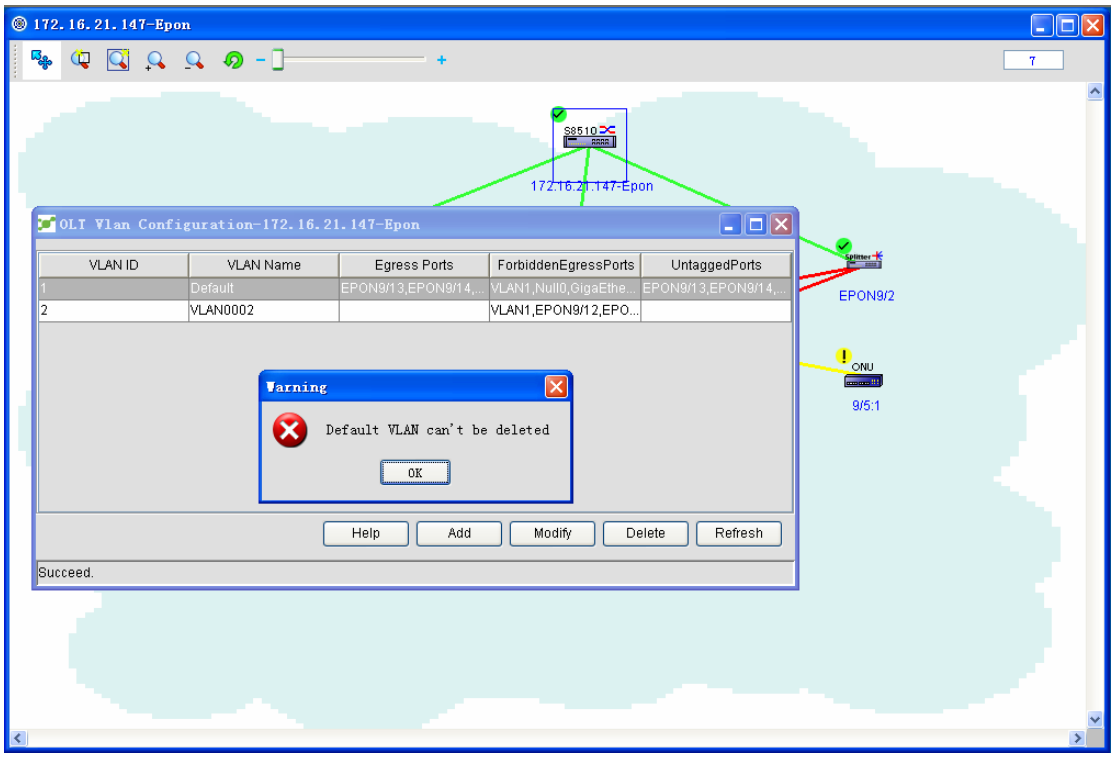
On the VLAN configuration page, if you select multiple VLANs and click **Delete**, the following page appears:



Click **Yes** and then you delete all selected VLANs; click **No** and then you do not delete the

chosen VLANs.

If you select the VLAN whose ID is 1, the following page appears and other VLANs will be deleted.



◆ Refresh

Click **Refresh** and you will obtain related VLAN information again.

Note: There are 4 fields on the figure above:

Vlan Id: Stands for each VLAN.

Vlan name: It is used to identify VLANs so that the administrator can manage them easily.

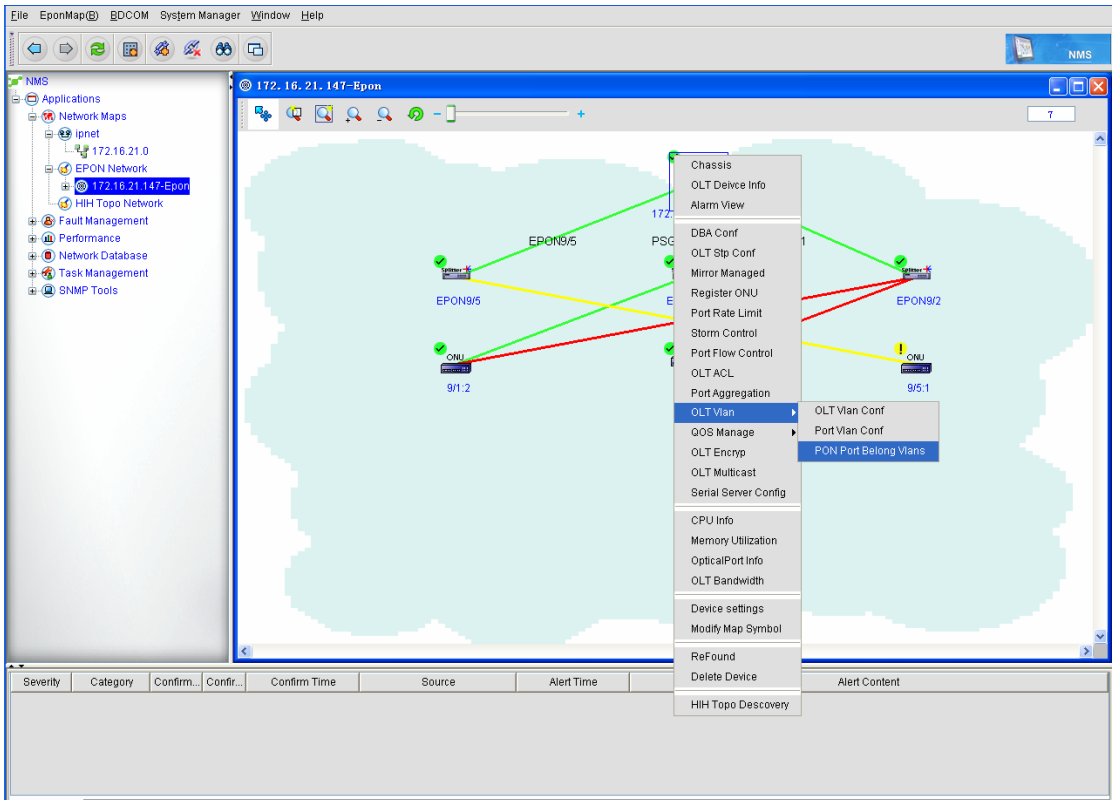
Egress Ports: It is a port contained in the local VLAN. You can browse it by double clicking it.

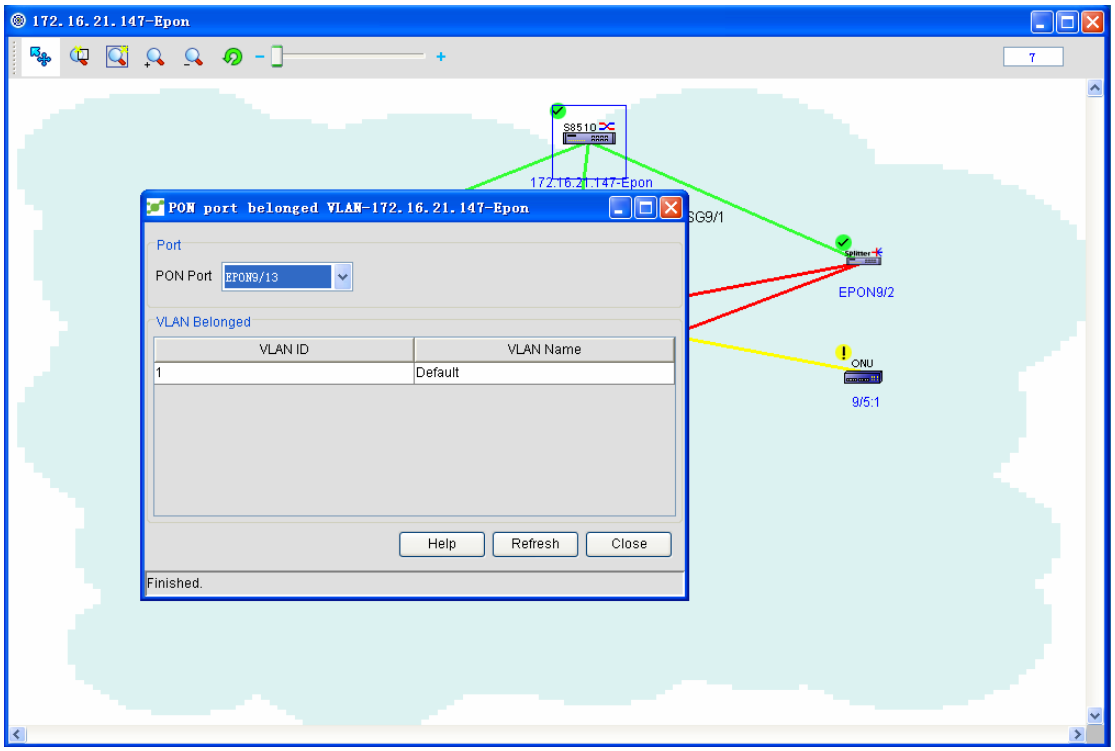
ForbiddenEgressPorts：It is a port that is not contained in the local VLAN. You can browse it by double clicking it.

UntaggedPorts: It stands for the untagged ports.

5.3.4.2 PON port's VLAN

Browsing a VLAN of a port helps you to browse which VLAN a specific port belongs to. Click **Browse a VLAN of a port** and you will find the following page appear:



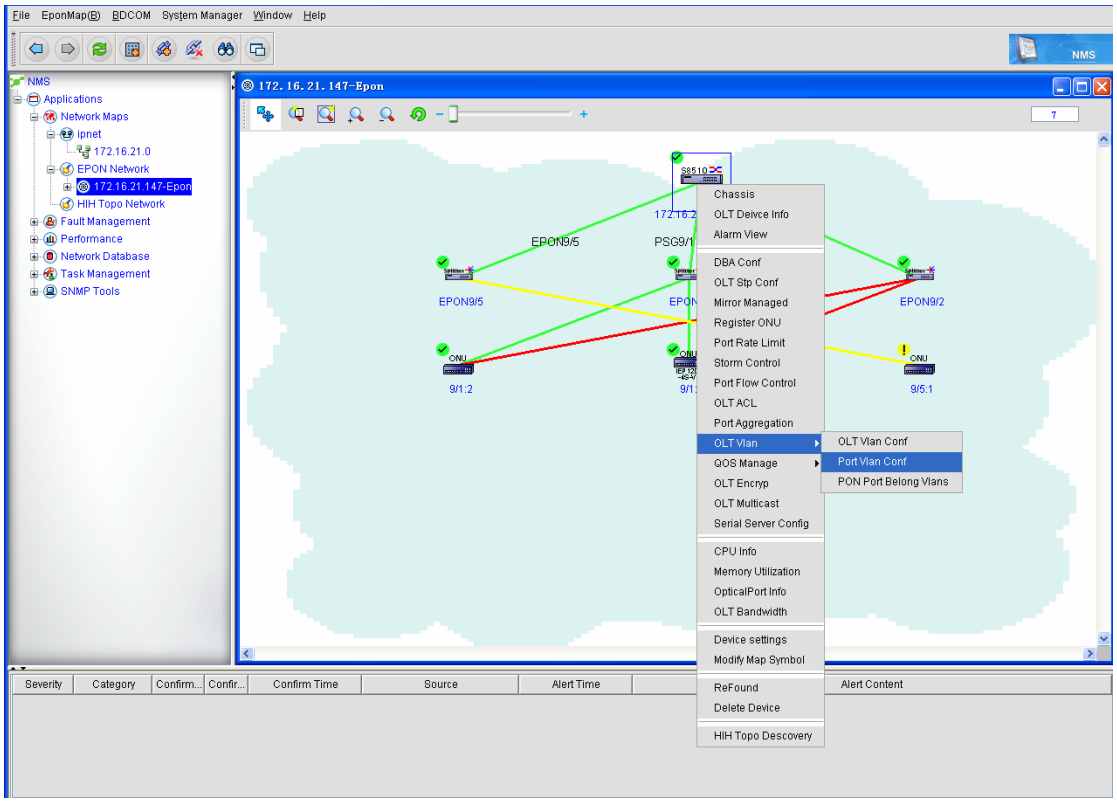


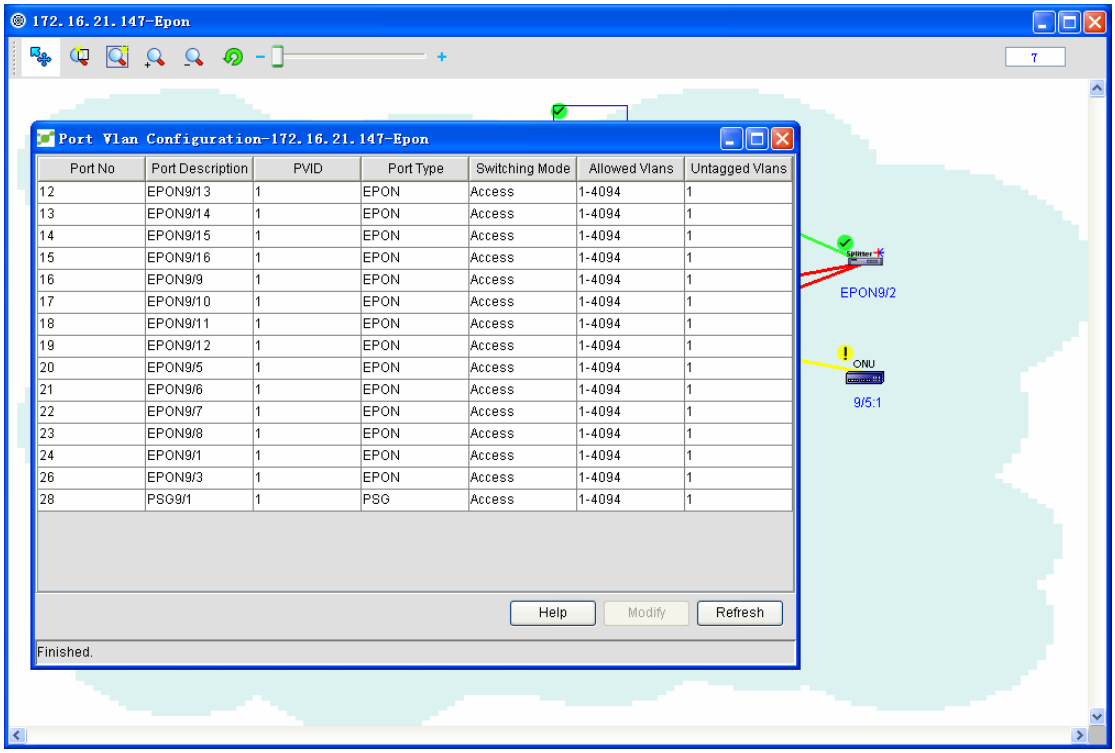
Select different PON ports from the PON port dropdown box. The VLAN that a PON port belongs to will be displayed in the affiliated VLAN list.

5.3.4.3 VLAN settings of a port

Different series of equipment have different port's VLAN configurations. The following describes the VLAN settings of the port of 3305 OLT and 8500 OLT.

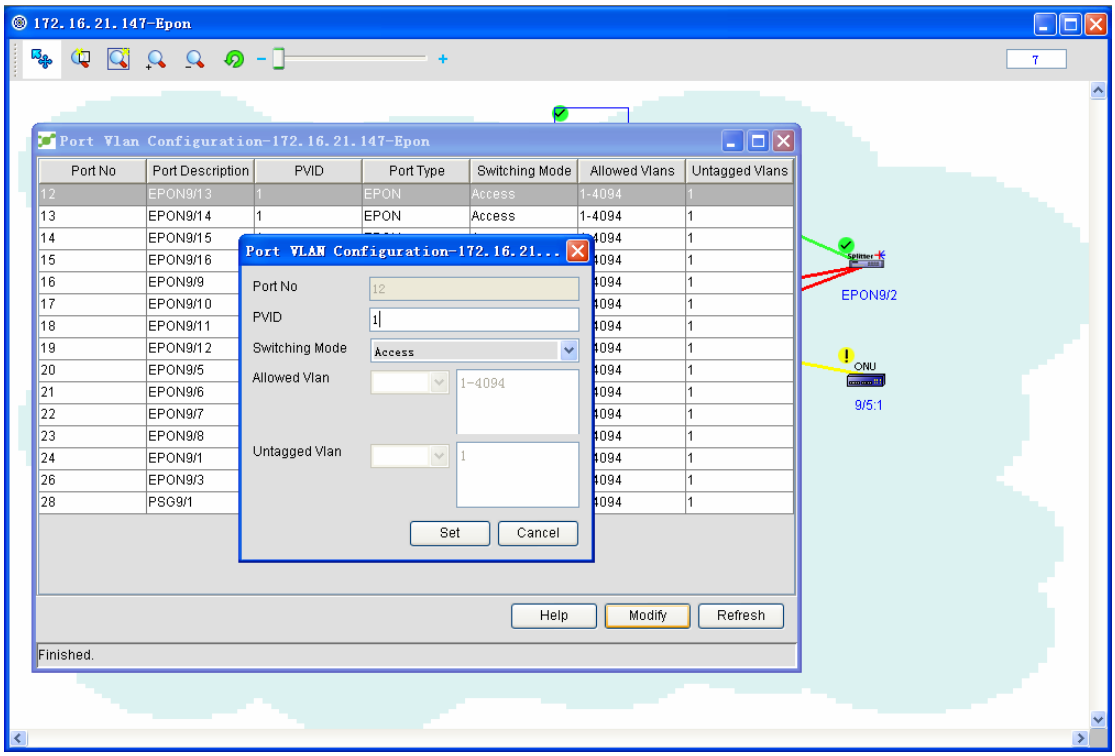
In the OLT menu, click **VLAN management -> port VLAN settings**. A configuration page appears, as shown in the following figure:





PVID stands for Port Vlan ID and relates with the VLAN tag when a port sends or receives data frames. The ports of a switch can be classified into two kinds: access ports and trunk ports. The former ones are used on the access layer to directly connect equipments, while the latter ones are used between equipments to be in charge of aggregation. The characteristic of an access port is to allow those flows that comply with PVID to pass through. Different from the access ports, trunk ports have their own native VLANs that send some data or flows like CDP and BPDU for equipment connection and management. The data frames generated by a device itself have no tags when being transmitted (it is because VID is equal to PVID and the tags are removed); when a peer device receives these untagged data frames, the peer device will add its native VLAN's information to these data frames as their tags, browse the forwarding table, and then make one of the following choices: if it finds the destination MAC address is its MAC address it removes the tags, or if the destination MAC address is not its MAC address it goes on forwarding them to other trunk ports and at the same time removes their tags.

In the port table, the port's PVID, the port types, the exchange modes, the allowed VLANs and the untagged VLANs are shown. Choose any row in the port table and then click **Edit**. A port configuration page appears, as shown in the following figure:



Only when the exchange mode is **trunk**, the allowed vlan and the untagged vlan can be set. The entered values can be 1, 3, 5, 7, or 1, 3-5, 7, or 1-7. The specific operation is shown below:

Allowed Vlan 1-9 ： Set the allowed vlans of this port to be vlan1 to vlan9.

Allowed Vlan add 1-9 ： Add the allowed vlans of this port to be vlan1 to vlan9.

Allowed Vlan except 1-9 ： All are allowed vlans except vlan1 and vlan9.

Allowed Vlan remove 1-9 ： Delete the allowed vlans of this port between vlan1 and vlan9.

Allowed Vlan all ： All vlans between vlan1 and vlan4094 are allowed vlans.

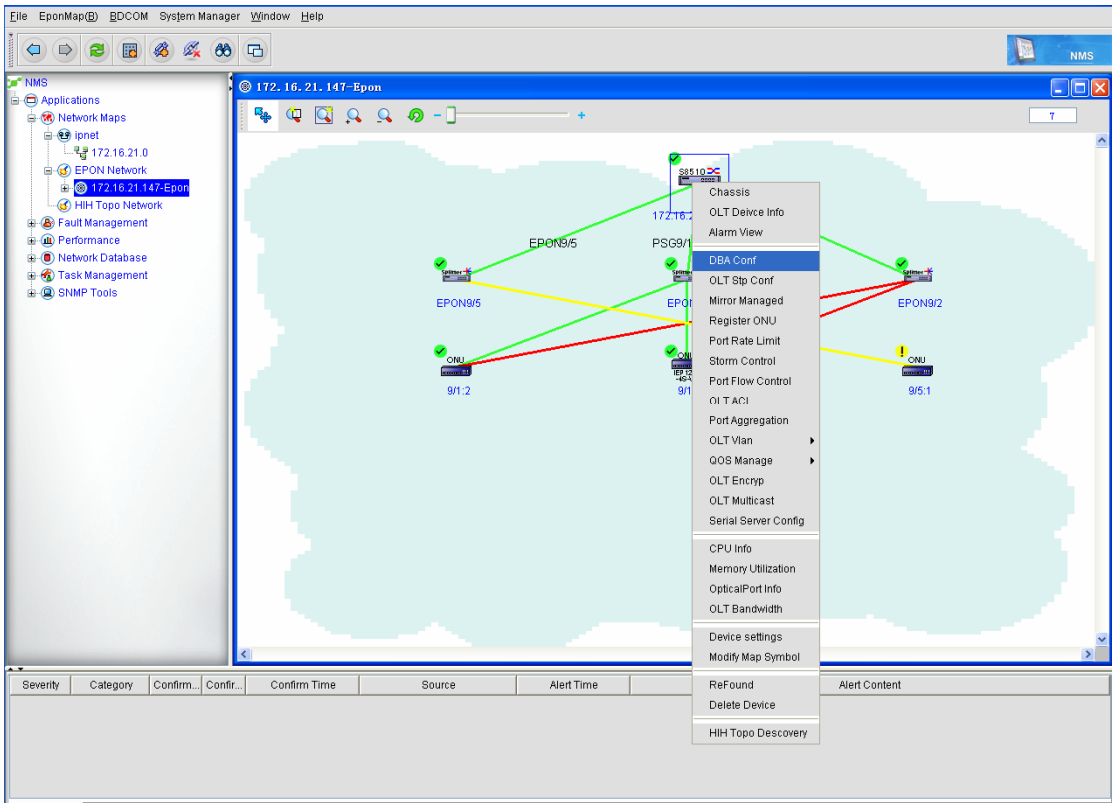
Allowed Vlan none ： This port has no allowed vlans.

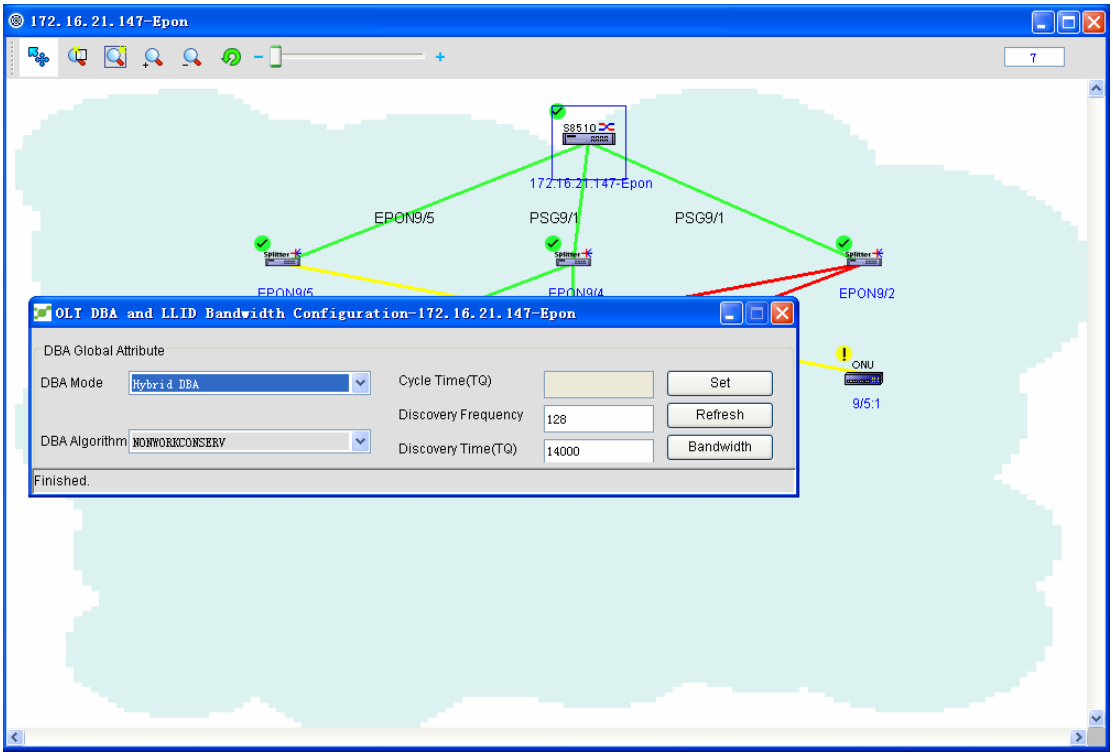
The operations about the untagged vlans are the same as those of allowed vlans.

5.3.5 OLT DBA Settings

DBA is a dynamic bandwidth distribution mechanism for the uplink broadband that can be done in a millisecond interval. The DBA settings of EPON is oriented for the uplink flows of each ONU.

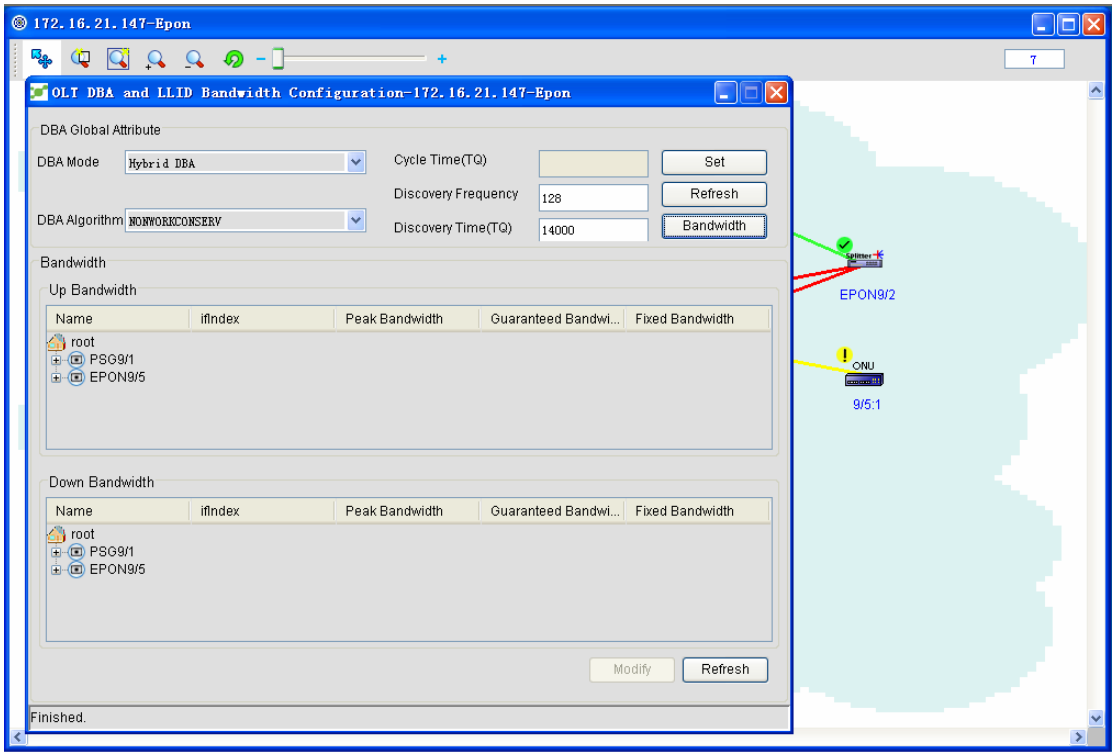
Right click the OLT icon and then click **DBA settings**. A page then appears, as shown in the following figure:



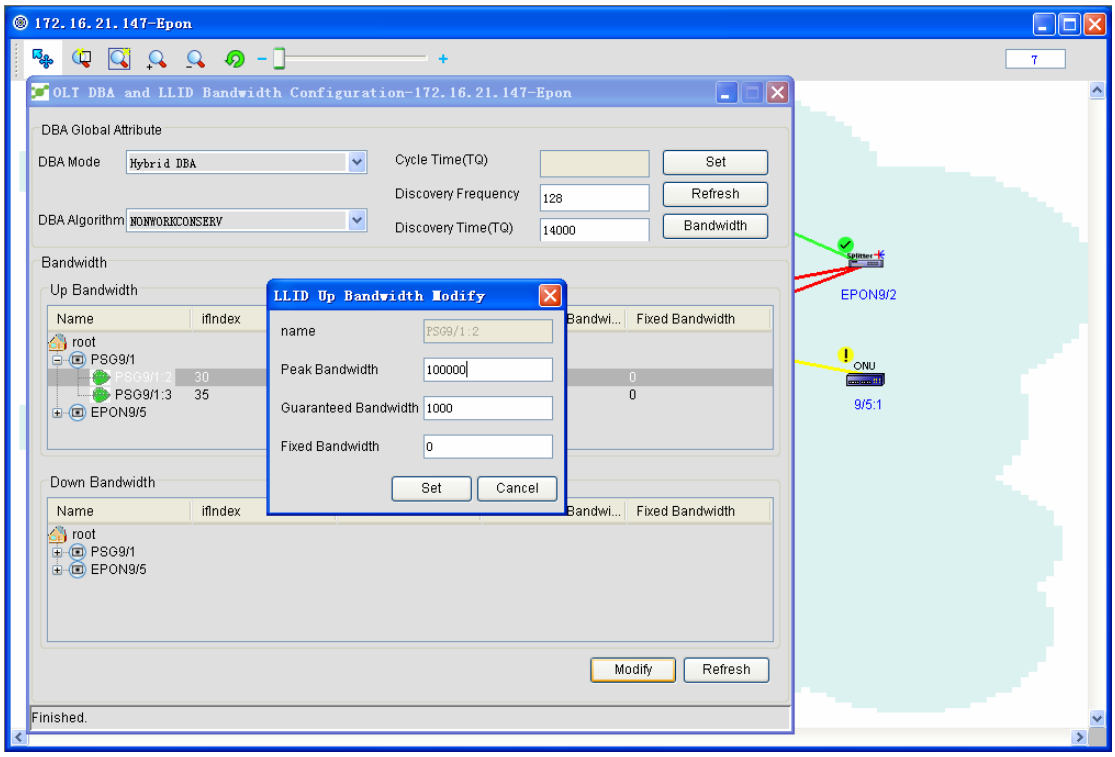


The figure above shows the global attributes of OLT DBA. You can click **Set** to configure the attributes or click **Refresh** to obtain the latest information about the device. During configuration, if the DBA mode is **hybrid DBA** or **Software DBA with dynamic cycletime**, the DBA cycletime cannot be set.

Click **Bandwidth**. A page appears, as shown in the following figure:



Select a leaf node of the tree in the figure above and click **Edit**. A page appears, as shown in the following figure:



You can modify the peak bandwidth, the certified bandwidth and the fixed bandwidth in the figure above. The fixed bandwidth, however, cannot be modified if the DBA mode is hardware DBA.

Click **Set** after modification. If the modification is successful, the above-mentioned page will be closed. Click **Cancel**. The entered value is invalid and the bandwidth cannot be set. The above-mentioned page will be closed.

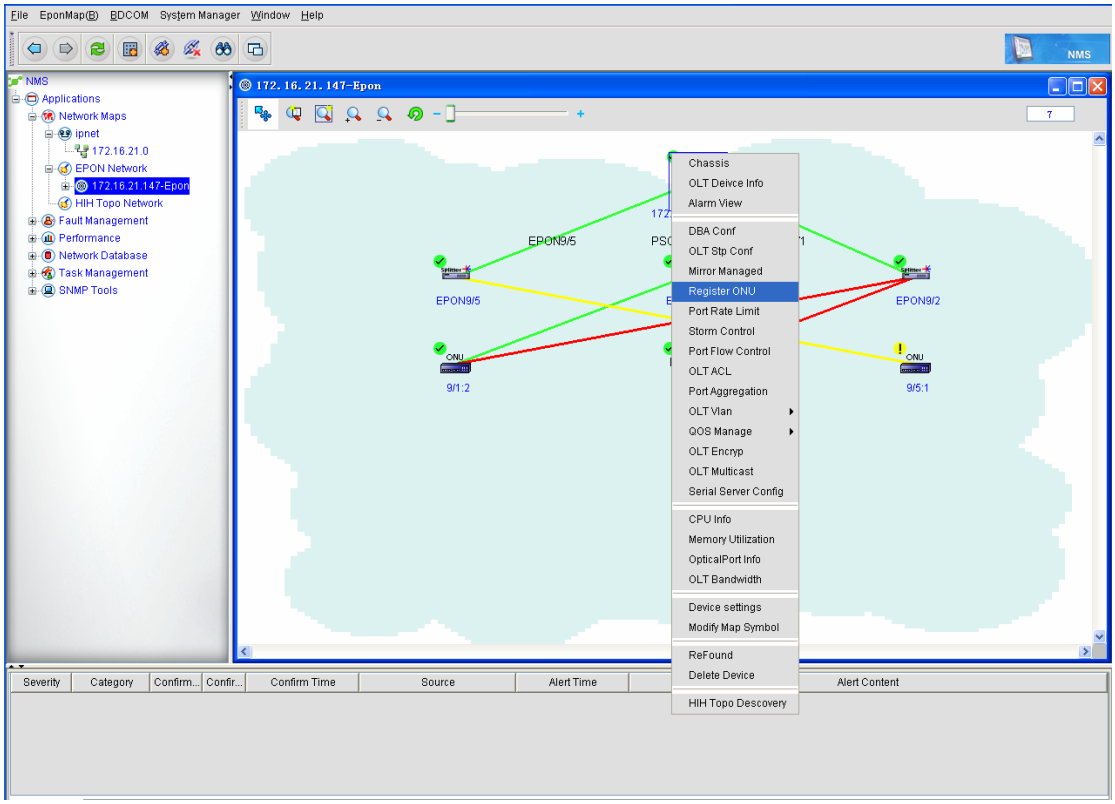
5.3.6 ONU Registration

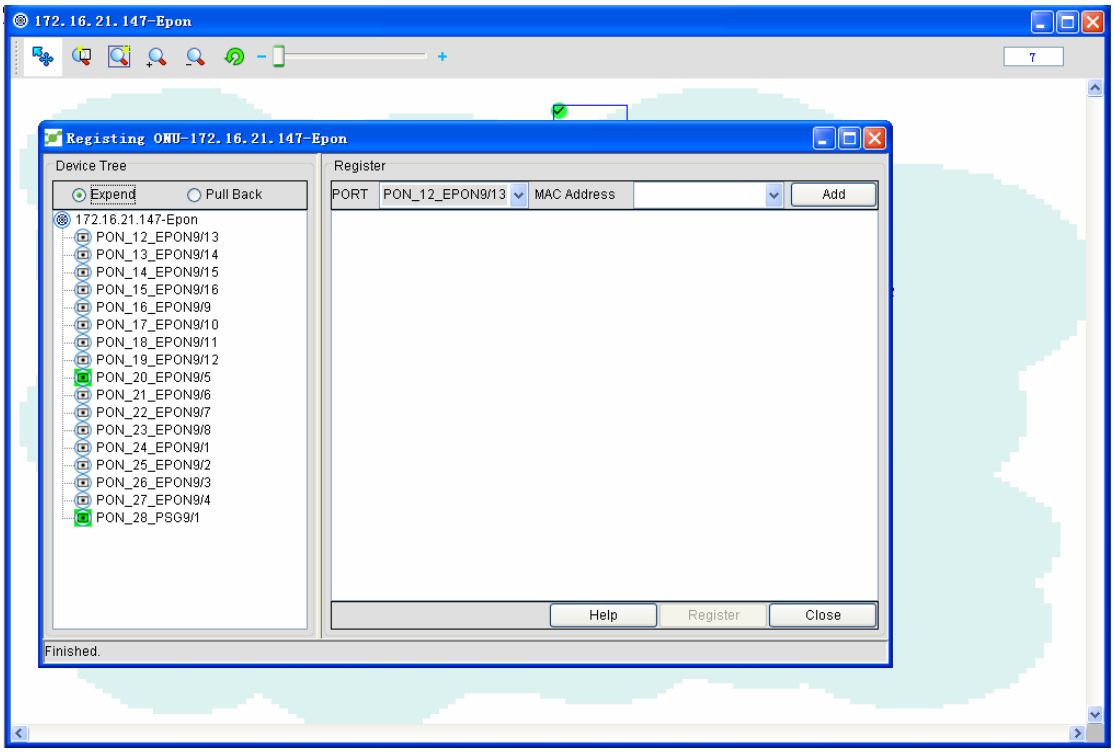
To make EPON work better, or manage ONU securely, ONU registration or deregistration is added to the EPON system. Only those ONUs that are authenticated by the port successfully can work normally.

EPON supports three ONU authentication modes: physical ID authentication, logical ID authentication and hybrid authentication.

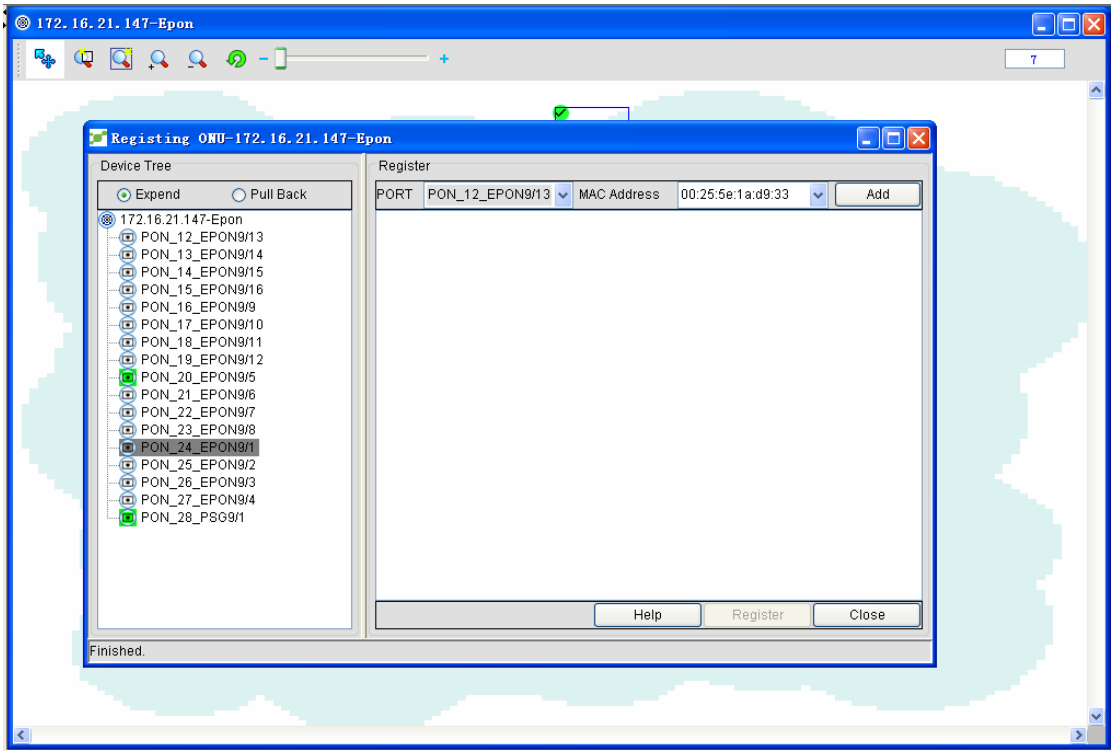
The ONU registration is shown below:

- Right click the OLT icon on which ONU will be registered, and then click **Register ONU**. The OUN registration page appears, as shown in the following figure:

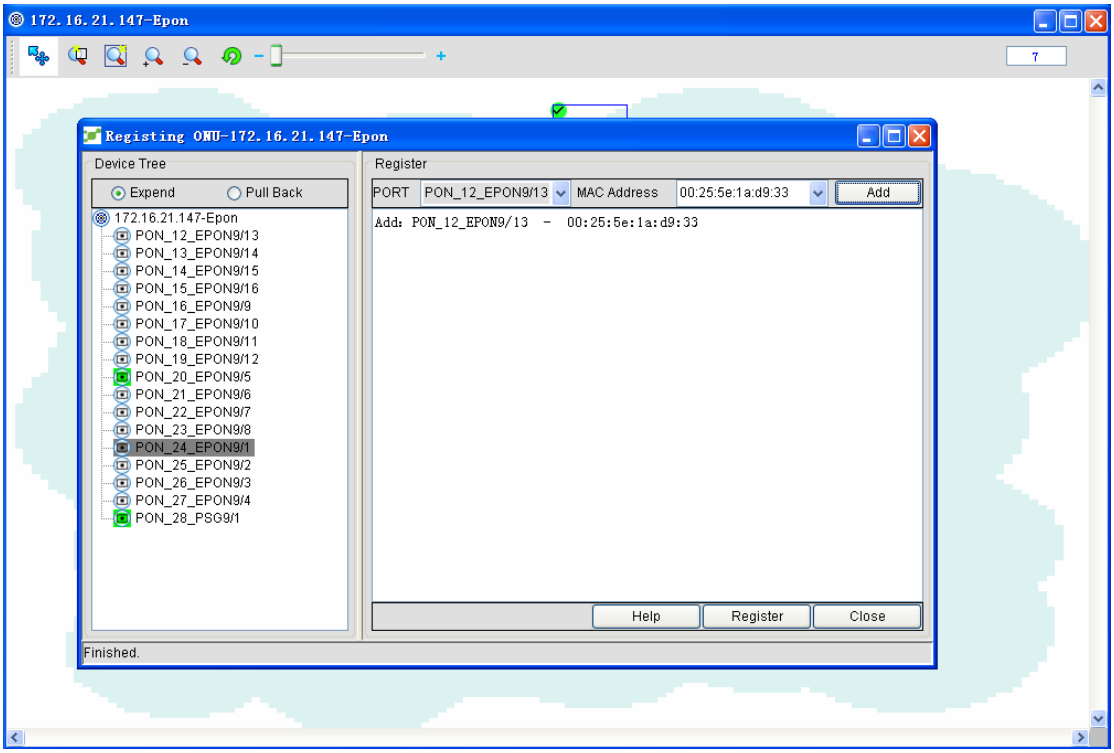




- In the ONU registration bar, select the to-be-registered OLT port and edit the MAC address of the to-be-registered ONU in the ONU MAC text box. After edition, click **Add**.

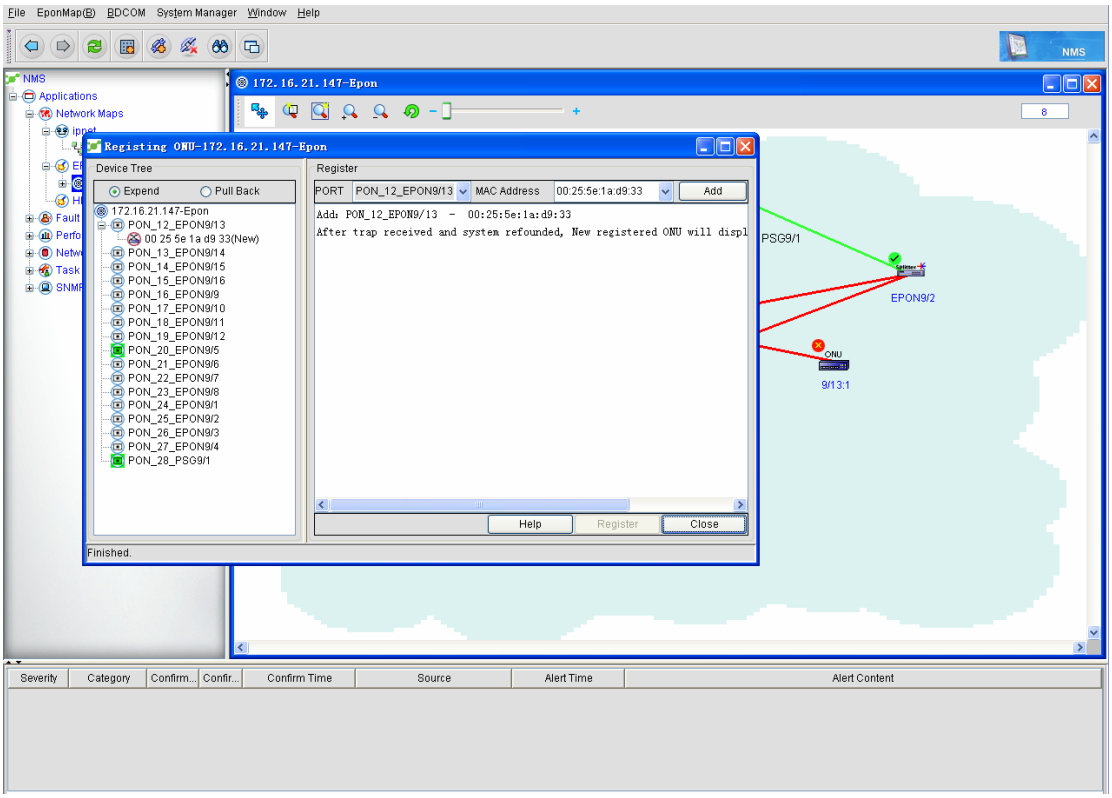


- The system prints and exports the MAC address of the to-be-added ONU to the following edition window. See the following figure:



Note: ONU registration supports multiple ONU registration on one port or on different ports.

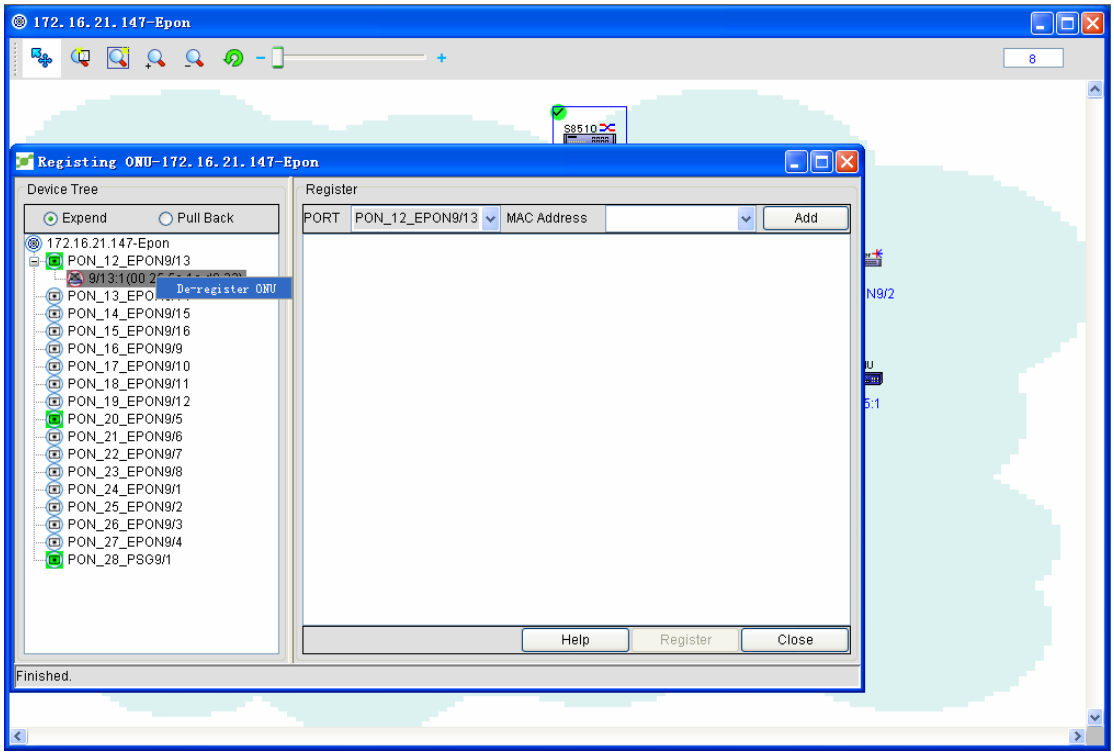
- Click **Execute** to register ONU. In this case the system will return the MAC addresses of unregistered ONUs back to the null window; if all registrations are successful, the null window will show that ONU registration is done.



The ONU deregistration is shown below:

- Select a to-be-deregistered ONU in the device tree node on the left of the ONU registration window and right click it. The following dialog box appears:

  The deregistered ONU will disconnect OLT and this ONU icon will be deleted from the topology. If you want to manage this ONU again, you need registering it again.



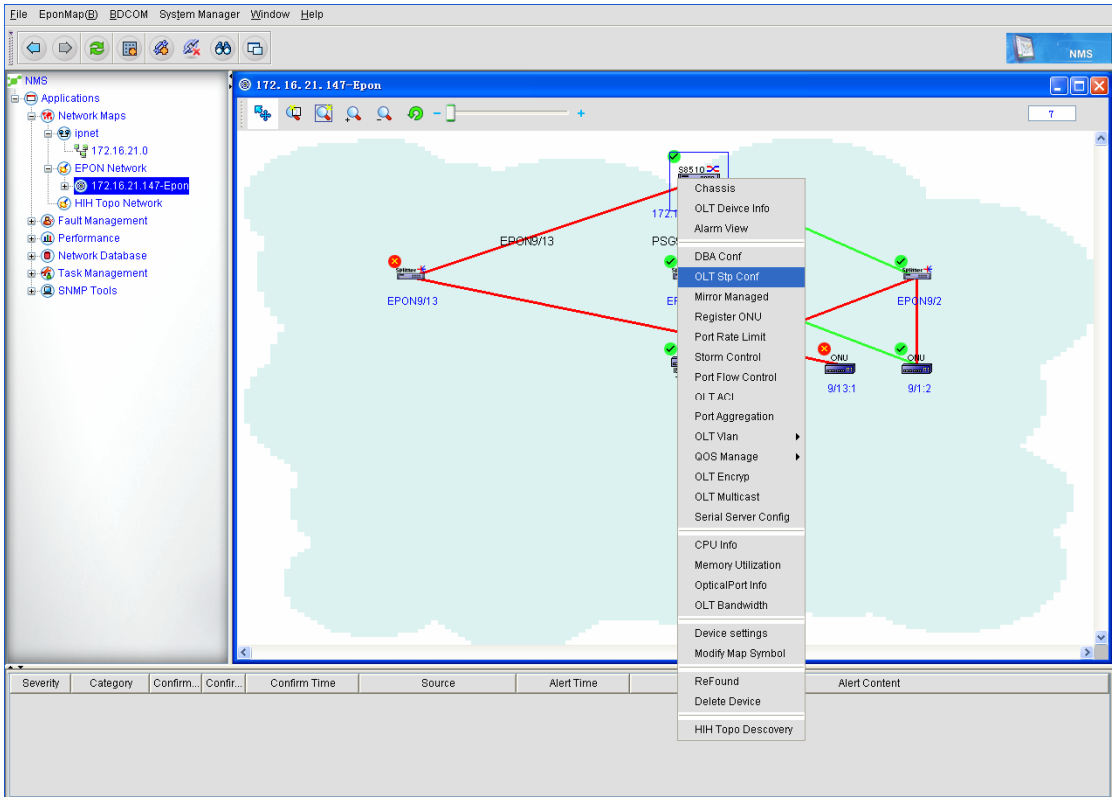
5.3.7 OLT STP Settings

Spanning-Tree Protocol (STP), defined in IEEE 802.1D, simplifies a LAN topology, which consists of several bridges, into a single spanning-tree, preventing network loopback and guaranteeing the stable operation of the network.

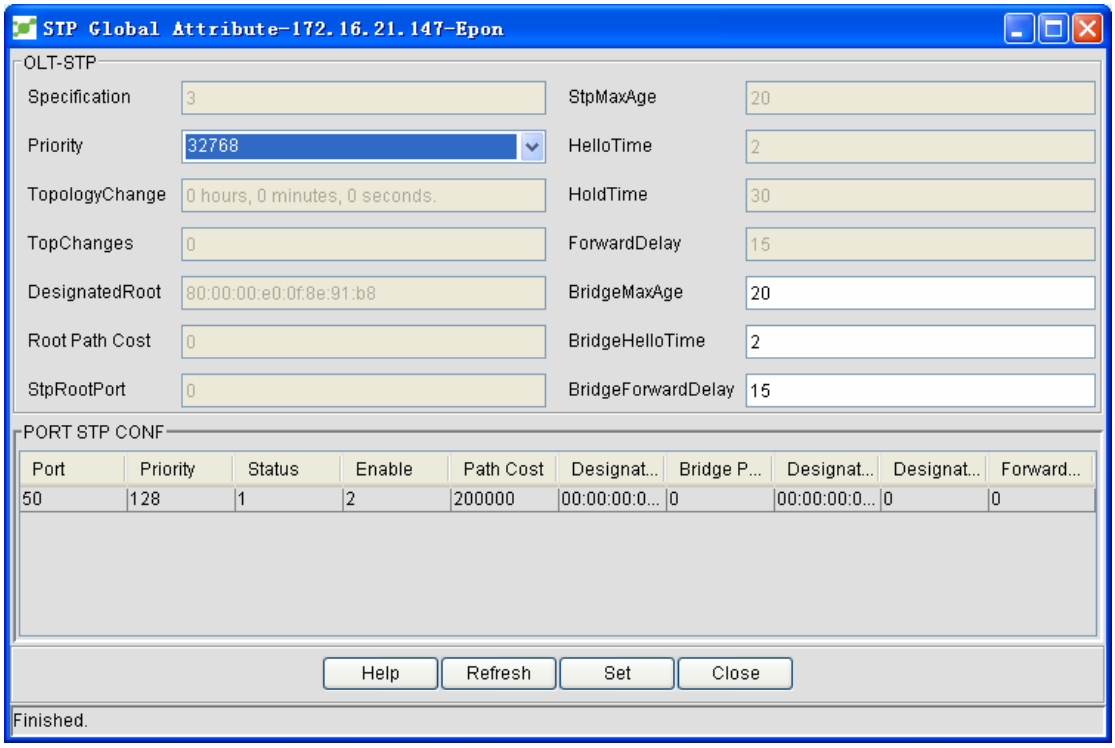
This section shows how to set OLT STP through NMS.

The detailed procedure is shown below:

- Open NMS and enter the EPON network topology. Select an OLT icon and right click it. See the following figure:



- Select **STP settings**. The STP settings page appears.



The options that the administrator can execute include:

Priority of global STP attributes, BridgeMaxAge, BridgeHelloTime, ForwardDelay, STP settings of a port on OLT. The value of **BridgeMaxAge** ranges between 6 and 40. The configuration of the **MaxAgeTime** of spanning tree decides the maximum lifetime of packets in the spanning tree when a switch is used as a root.

BridgeHelloTime ranges between 1 and 10. The configuration of **HelloTime** of spanning tree decides the packet transmission interval when the related switch works as a root.

ForwardDelay ranges between 4 and 30. The configuration of **Forward Delay Time** of spanning tree decides the switch's status switchover interval when the related switch works as a root.

When the administrator sets the above-mentioned parameters, the system will automatically identify their values. For those exceeded values, the system will automatically delete the data in the text box.

- After related data is configured, you shall click **Set**. The configuration of global STP attributes is then finished.

- STP settings of the OLT port: If you right click the port attribute list, you can get a detailed configuration menu. See the following figure:

- Select **STP settings**. The STP settings page appears.

The system supports to set the port's priority and the port's path cost. The port's path cost ranges between 1 and 65535.

- After configuration, click **Execute**. The **Default** button is used to resume the port's attributes to their original values.

5.3.8 Access Control List

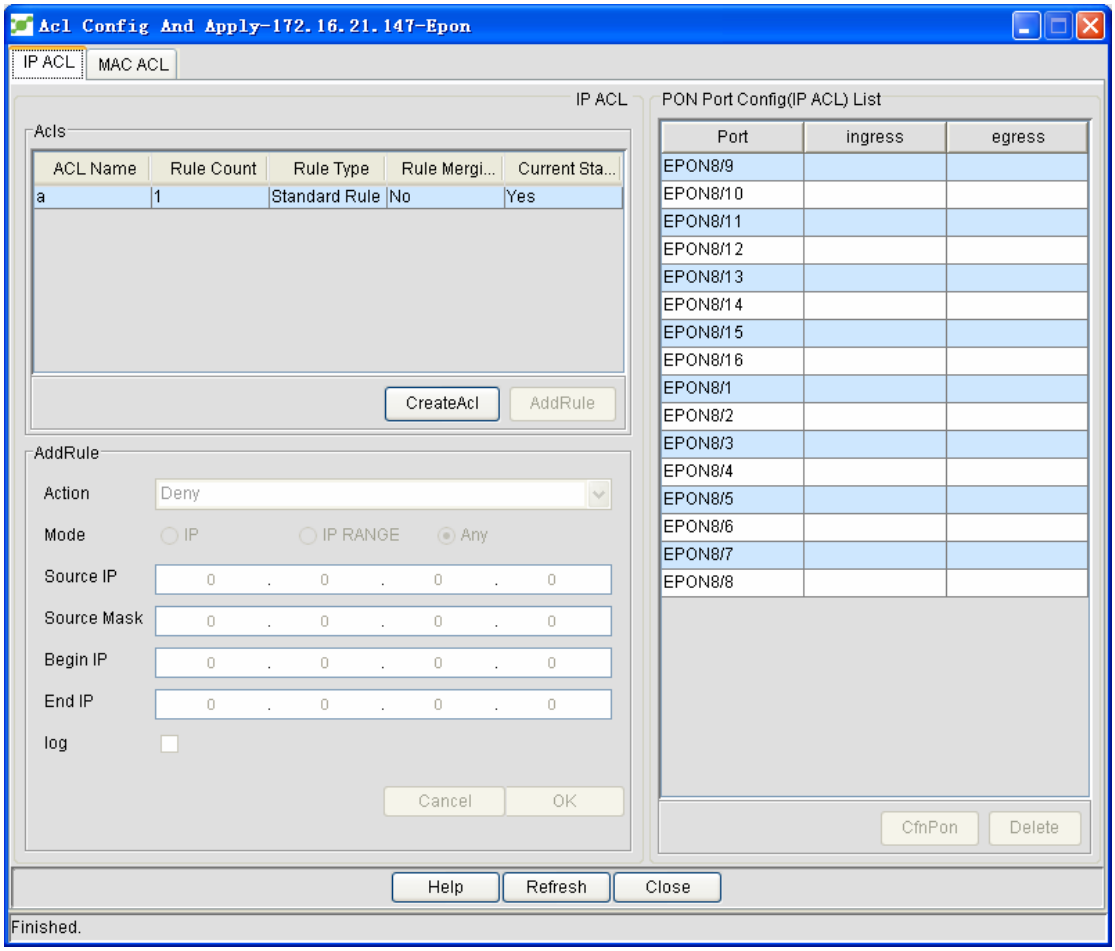
The Access Control List (ACL) is a list of instructions of routers and switch's interfaces and is used to control the incoming and outgoing packets on interfaces.
This section gives a detailed description of the operations of the ACL module in the NMS.
ACLs have two types:

- IP ACL
- MAC ACL

The ACL has the following operations:

- Configuring ACL (IP ACL, MAC ACL)
- Creating ACL
- Setting the configuration rules for ACL
- Applying ACL
  - Distributing ACL to the PON port
  - Distributing ACL to the LLID of ONU
  - Distributing ACL to ONU

To create an ACL, you have to open the corresponding ACL window. Then you have to open the ACL configuration and application window by clicking **OLT -> ACL management**. See the following figure:



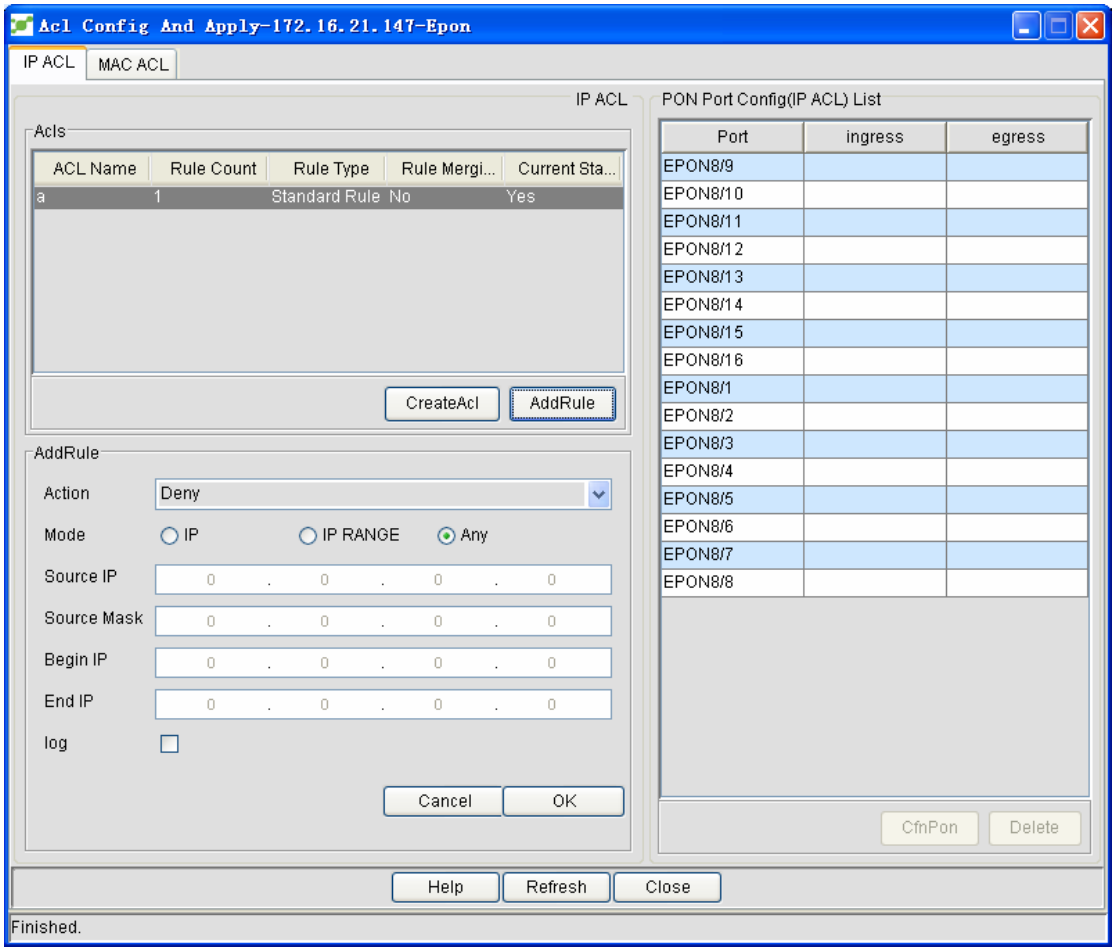
5.3.8.1 Creating IP ACL

Select the **IP ACL** option and then click **Create an item**. An ACL item can be created. In a window appearing later, enter an ACL name.

After an ALC item is created, the ACL item will be added to the ACL configuration and application window. The number of regulations, however, is still zero. You can add here the regulations of the opposite type. The operation procedure is shown below:

1. Select an ACL item to which you will add regulations. Then the **Add regulations** button avails automatically.

2. Click **Add regulations**. You can then set regulations in the **Add regulations** bar. After setting the regulations you can click **OK**. See the following figure:



Parameter description

Action: Deny and Permit When you choose **Deny**, it means the current ACL will be rejected. When you choose **Permit**, it means the current ACL is allowed.

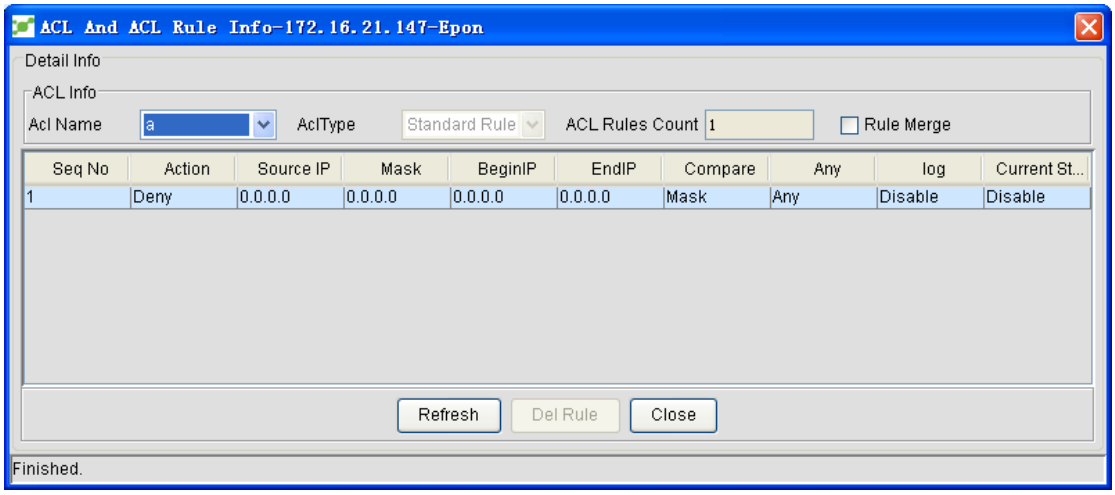
For detailed operations about MAC ACL creation and its regulation, refer to the description of the operations of IP ACL.

5.3.8.2 Browsing and operating IP ACL

- Browsing IP ACL and deleting ACL regulations

Right click an ACL item and then choose the **Detailed info** button. The regulations of the current ACL are shown. It is to be noted that if the number of regulations is 0 the system will automatically give notice and not show related information.

The following figure shows the ACL detailed information window.



The administrator can choose the to-be-browsed ACL regulations from the **Item name** dropdown menu in the ACL information bar. The system will download a corresponding regulation according to the chosen ACL item name.

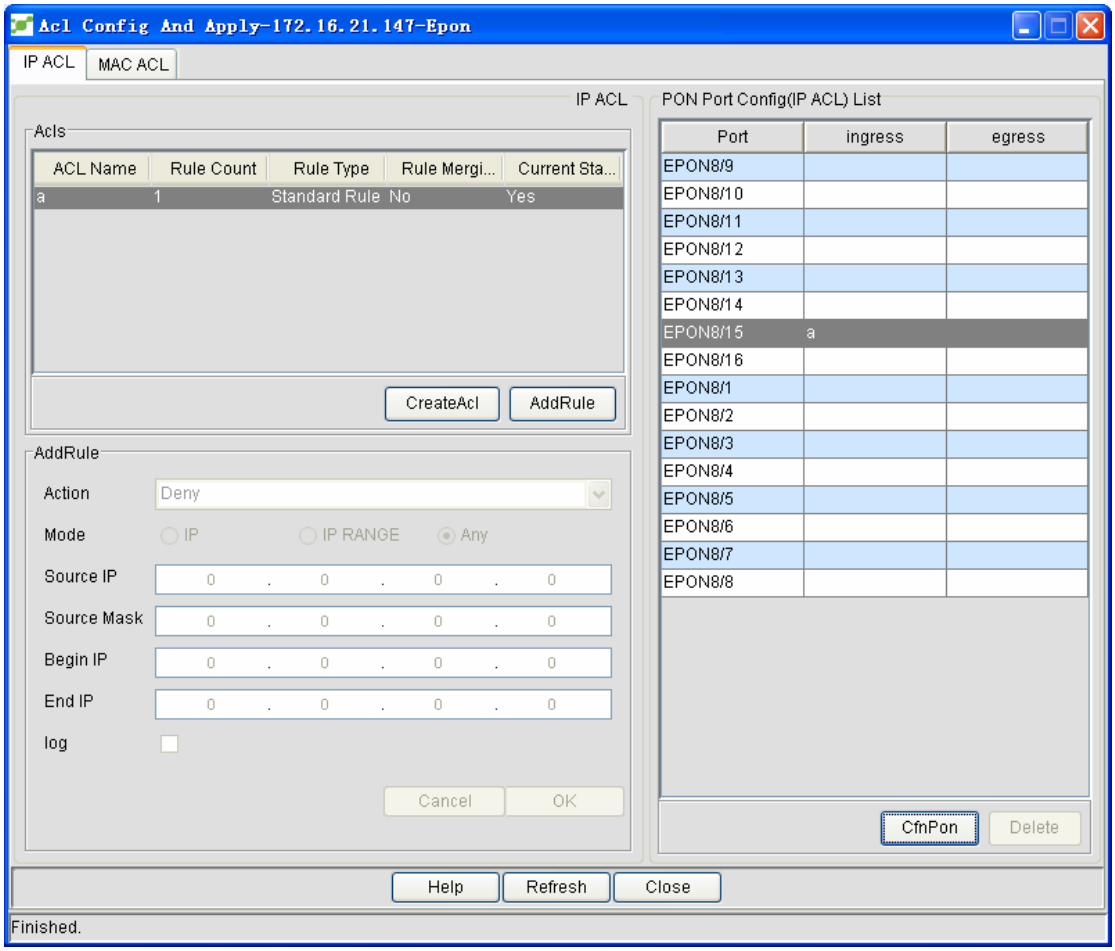
If you choose a regulation, the **Cancel regulation** button automatically avails. Click it and then the regulation is canceled.

- Canceling ACL

Click **Cancel ACL** in the right-key menu of the ACL. The chosen ACL items will be deleted.

5.3.8.3 Applying IP ACL

Applying IP ACL means to distribute the created IP ACLs to the PON port, realizing the filtration function. The ACL configuration area of the PON port in the ACL configuration and application window is shown in the following figure:



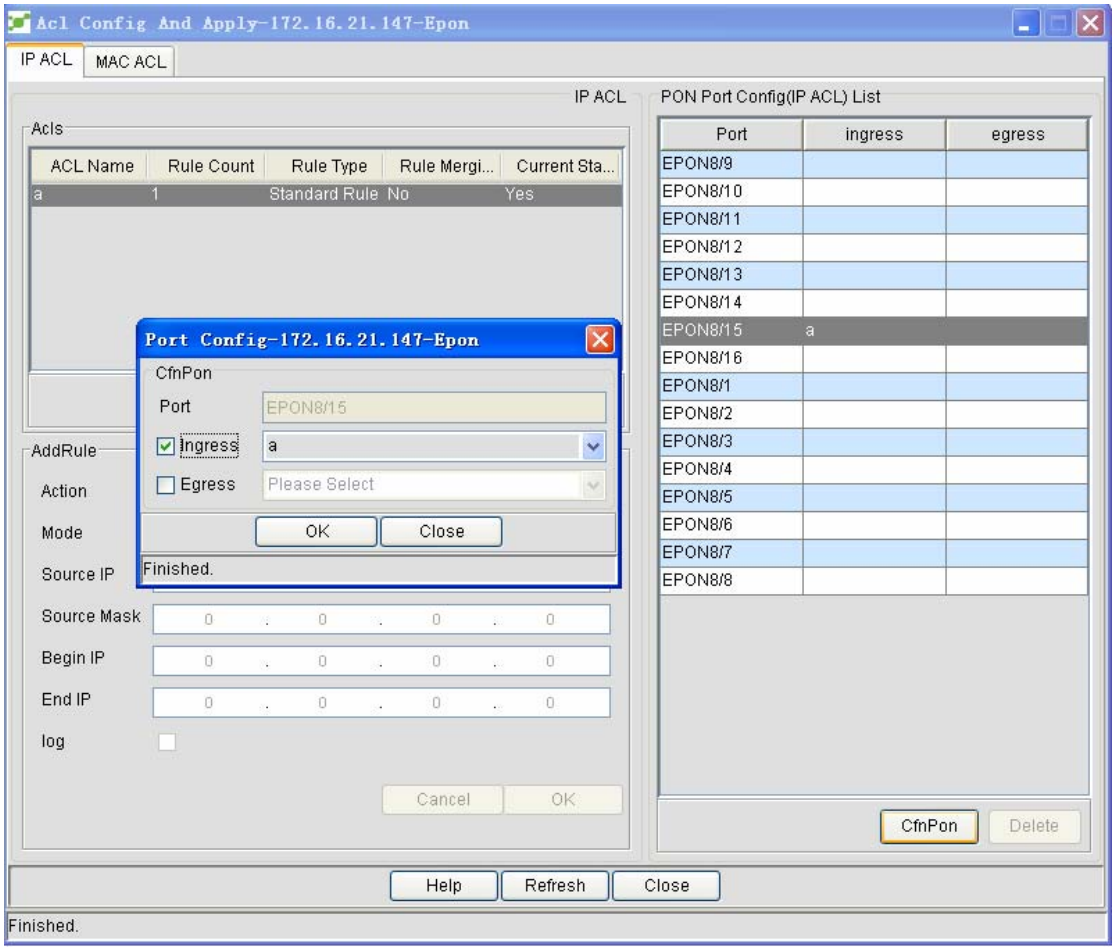
The operations about the PON port's settings are shown below:

- Configuration

Configuration here means to set ACL on the ingress or egress PON port. If you choose a to-be-configured PON port, the **Set** button automatically avails. See the following figure:

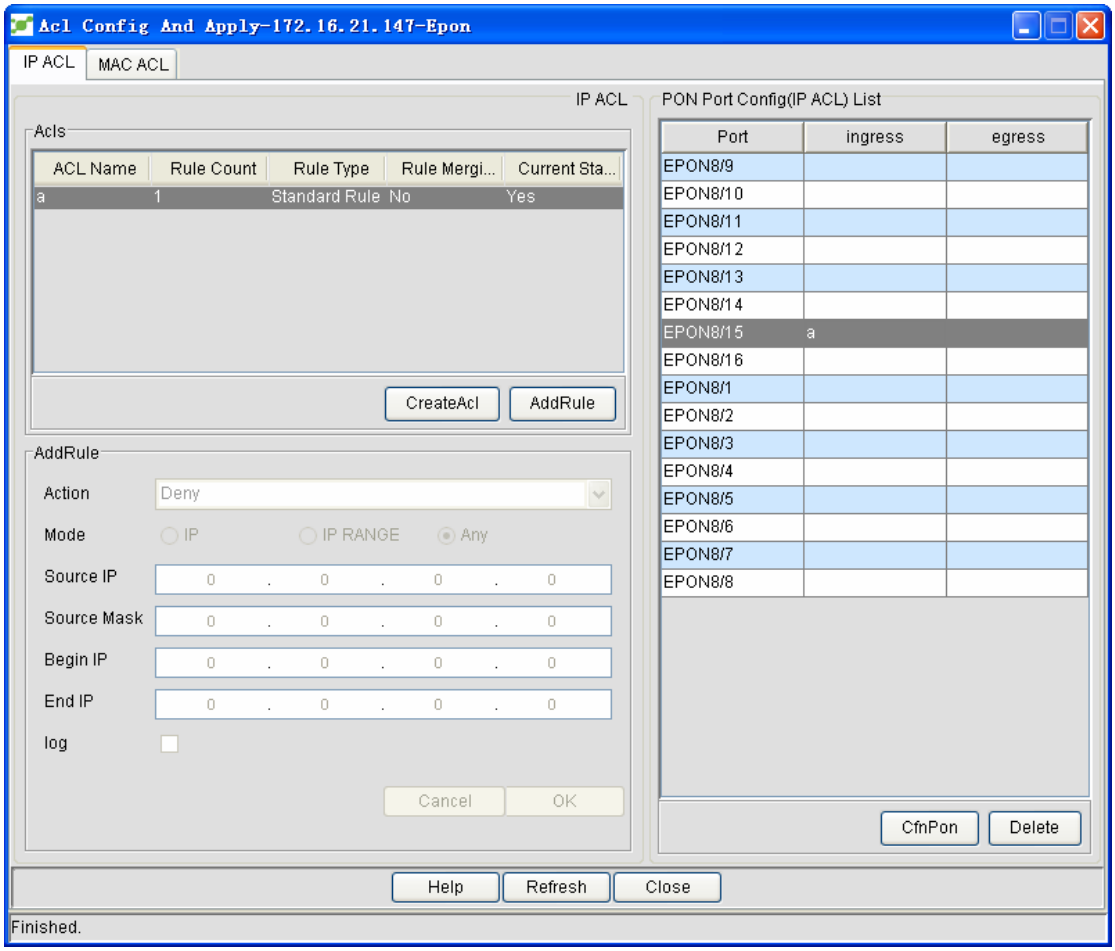
Ingress: stands for the ingress ACL.

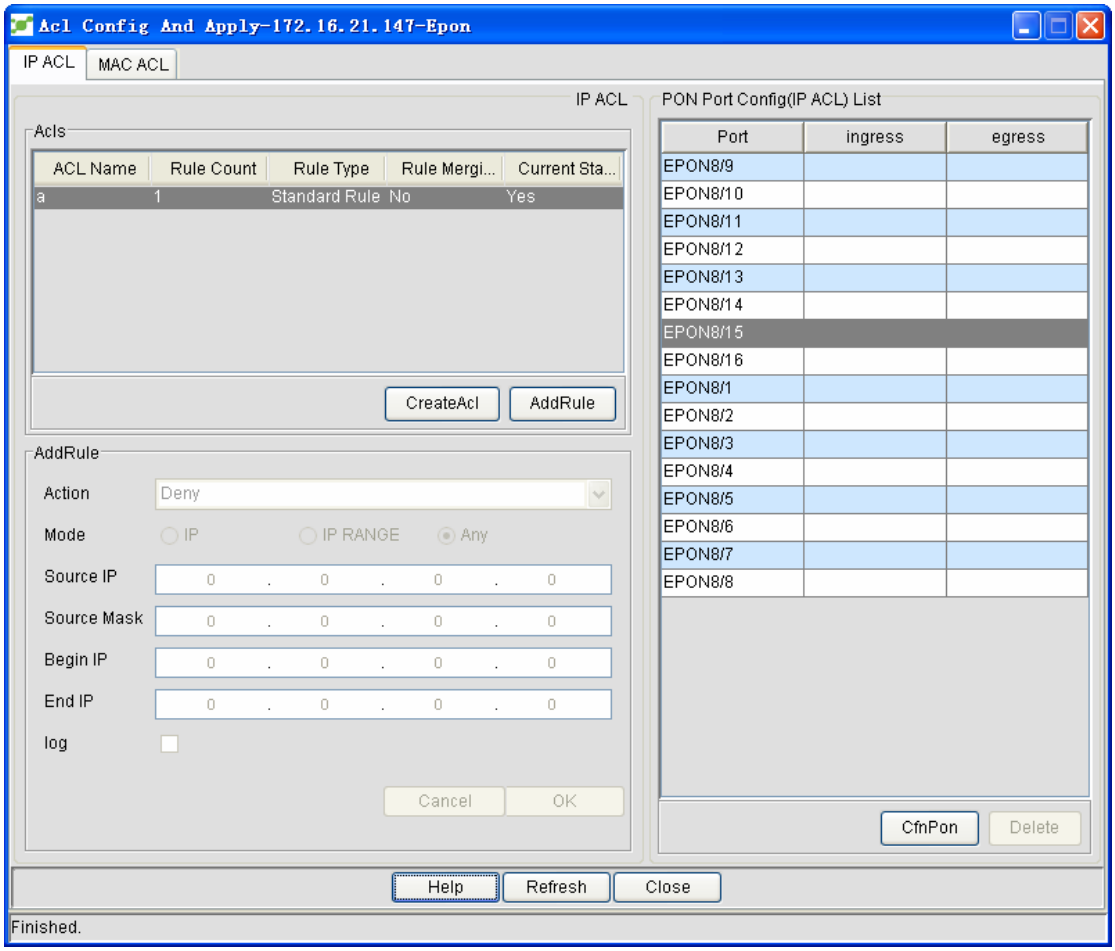
Egress: stands for the egress ACL.



- Delete

The operation means to delete the ingress or egress ACL items on the PON port. See the following figure:


Acl Config And Apply-172.16.21.147-Epon
IP ACL
MAC ACL
IP ACL
Acls
ACL Name
Rule Count
Rule Type
Rule Mergi...
Current Sta...
a
1
Standard Rule
No
Yes
CreateAcl
AddRule
AddRule
Action
Deny
Mode
IP
IP RANGE
Any
Source IP
Source Mask
Begin IP
End IP
log
Cancel
OK
PON Port Config(IP ACL) List
Port
ingress
egress
EPON8/9
EPON8/10
EPON8/11
EPON8/12
EPON8/13
EPON8/14
EPON8/15
a
EPON8/16
EPON8/1
EPON8/2
EPON8/3
EPON8/4
EPON8/5
EPON8/6
EPON8/7
EPON8/8
CfnPon
Delete
Help
Refresh
Close
Finished.



.

5.3.9 QoS Management

Generally, the device always works in Best-Effort served mode. In this mode, the device treats all flows equally and tries its best to deliver all flows. Under this circumstance, if congestion occurs, all flows have the same possibility to be dropped. However, different flows in an actual network have different importance. The QoS function of the device provides different services to different flows according to their importance, so those relatively important flows can get relatively good service.

As to classify the importance of flows, there are two main ways on the current network:

- The tag in the 802.1Q frame header has two bytes and 3 bits are used to present the priority of the packet. There are 8 priorities, among which 0 means the lowest priority and 7 means the highest priority.
- The DSCP field in IP header of the IP packet uses the bottom 6 bits in the TOS domain of the IP header.

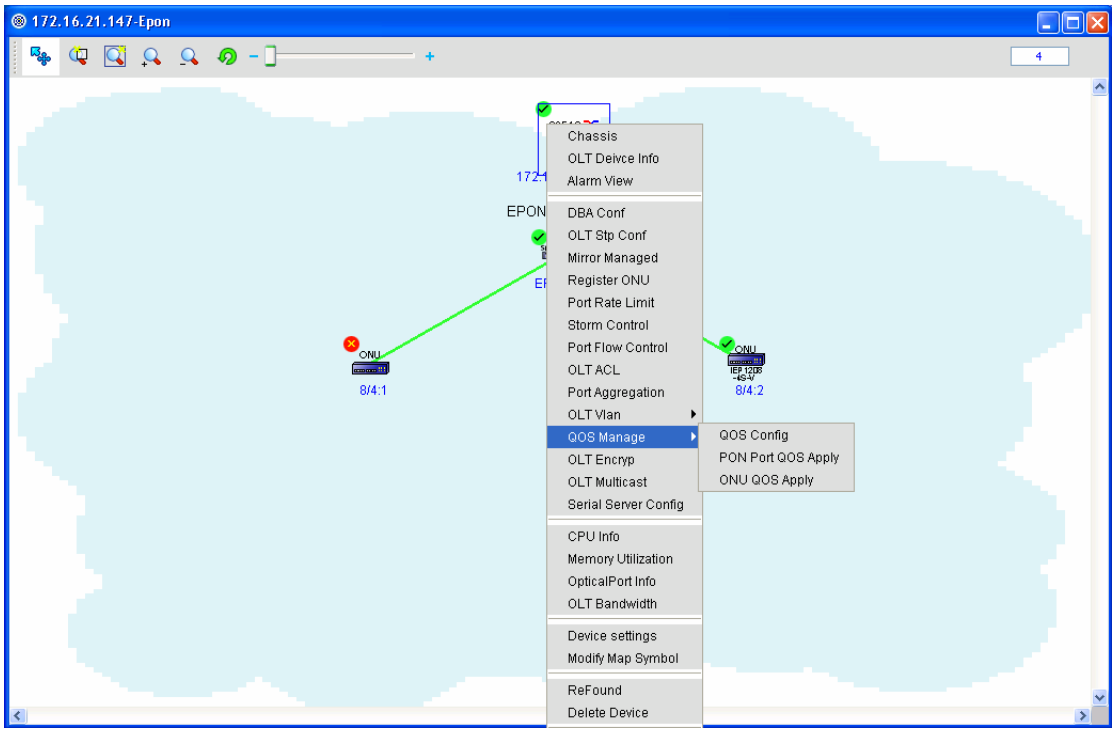
You can also set a device in a network to make it process those special packets specially. The special treatment of special packets is called as a one-hop behaviour.

The QoS function of the device enables the limited bandwidth to be used effectively, improving the performance of the entire network greatly.

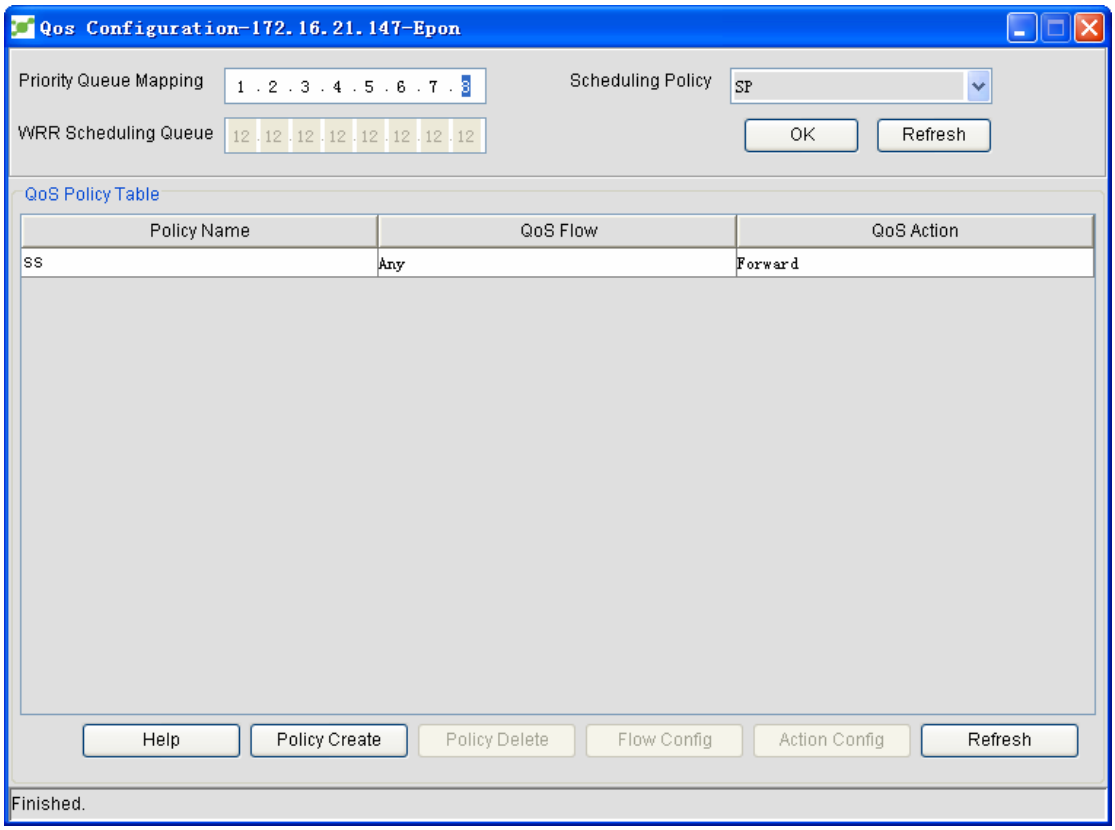
QoS management includes QoS settings, QoS application on the PON port and ONU QoS application.

5.3.9.1 QoS settings

Right click the to-be-configured OLT icon. The right-key menu appears, as shown in the following figure:



Click **QoS management -> QoS settings**. A page appears, as shown in the following figure:



- The global attributes of QoS settings are shown in the figure above:
- Priority queue map

  To configure the QoS priority queue is to map 8 IEEE802.1p-defined QoS CoS values to the priority queues of OLT. This type of OLTs have 8 priority queues. OLT adopts a corresponding schedule policy for a different queue, realizing QoS.

  In global mode, configuring the CoS priority queue will affect the CoS priority queue maps of all ports. When a priority queue is configured on a L2 port, the priority queue will be used on this L2 port; if not, please use the global configuration.

  Note: The CoS value ranges between 0 and 7, including 0 and 7.
- Default CoS values

  If a port receives a data frame without tag, OLT will add a default CoS priority to the data frame. Configuring a default global CoS value is to set the default CoS of the untagged data frame to a designated value.

  This OLT only supports the default global CoS. When all ports receive the untagged data frame, they will add a same CoS value for this frame.

- Schedule policy

  There are four kinds of schedule policies:

  SP (Strict Priority)

  WRR (Weighted Round Robin)

  SP+WRR

SP-EXOAM (Strict Priority Exclude OAM)

- WRR

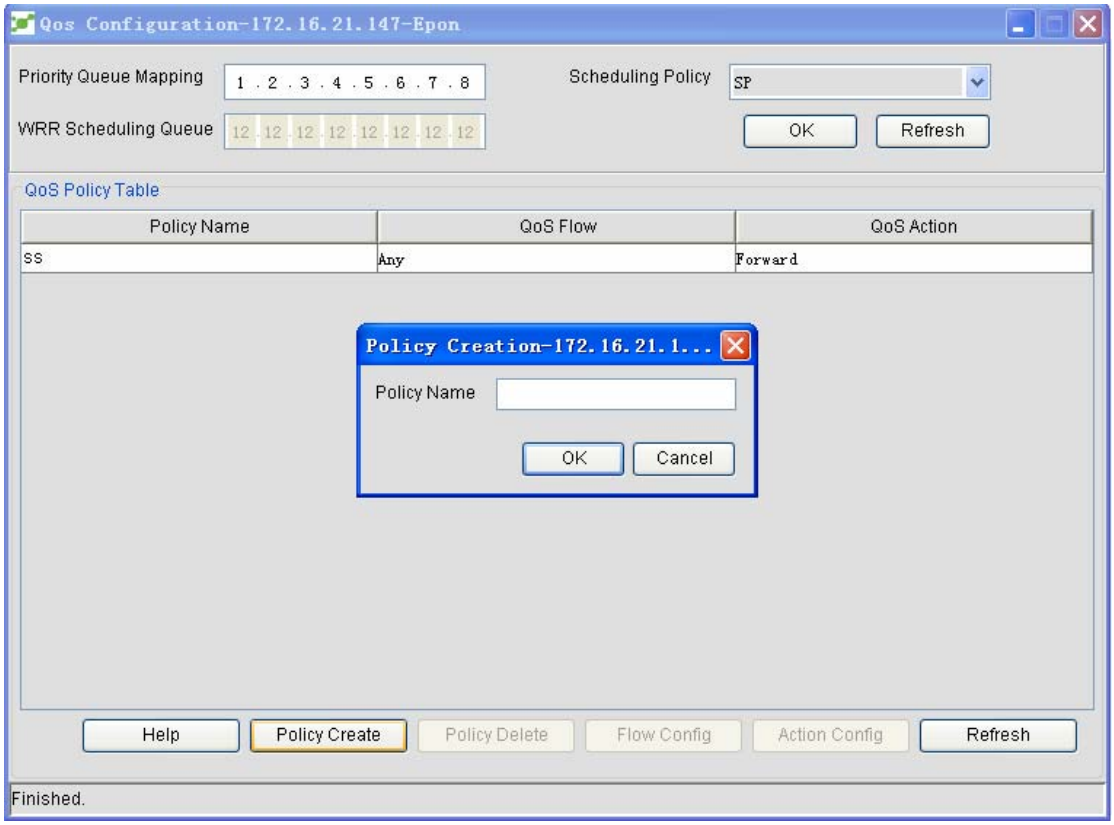
The bandwidth of priority queue means the bandwidth distribution ratio of each priority queue, which is set when the schedule policy of the CoS priority queue is set to WRR.

Note: The bandwidth value ranges between 1 and 255, including 1 and 255.

After the above-mentioned values are set, please click **OK** to distribute the values to related devices.

- The bottom part of the following figure is the QoS policy settings:
- Creating a policy

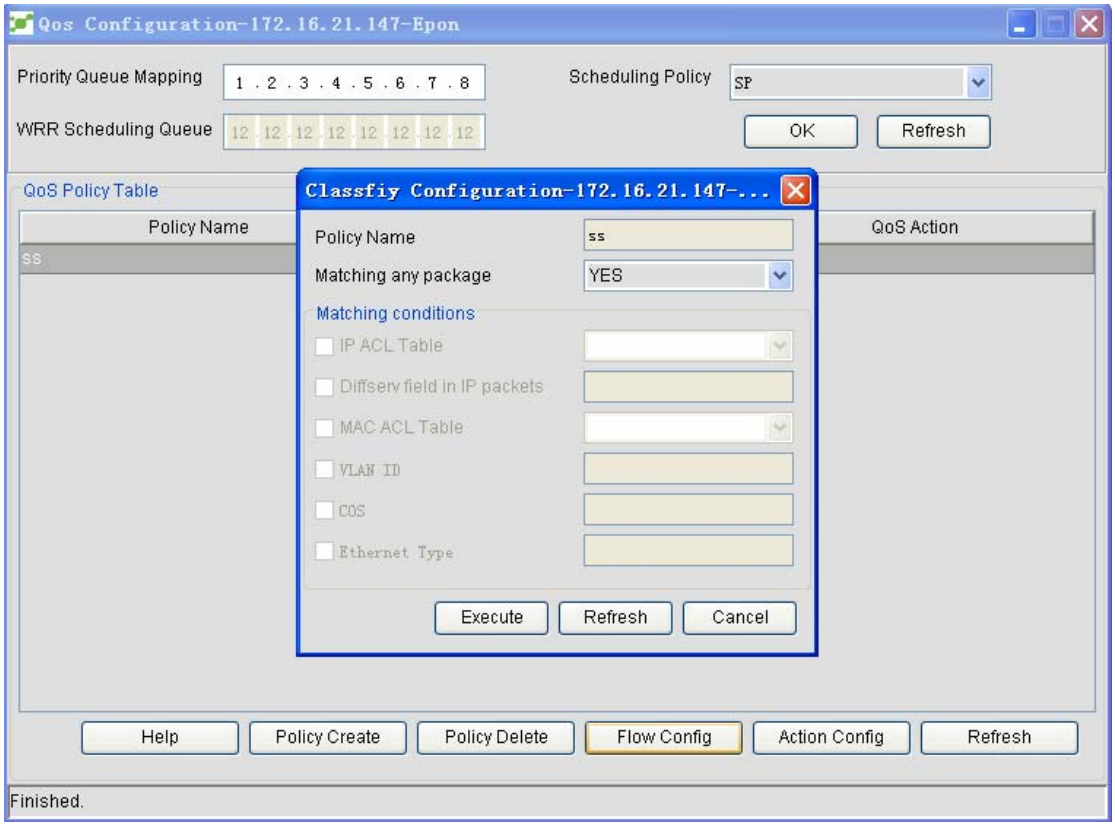
Click **Create a policy**, the following figure appears:



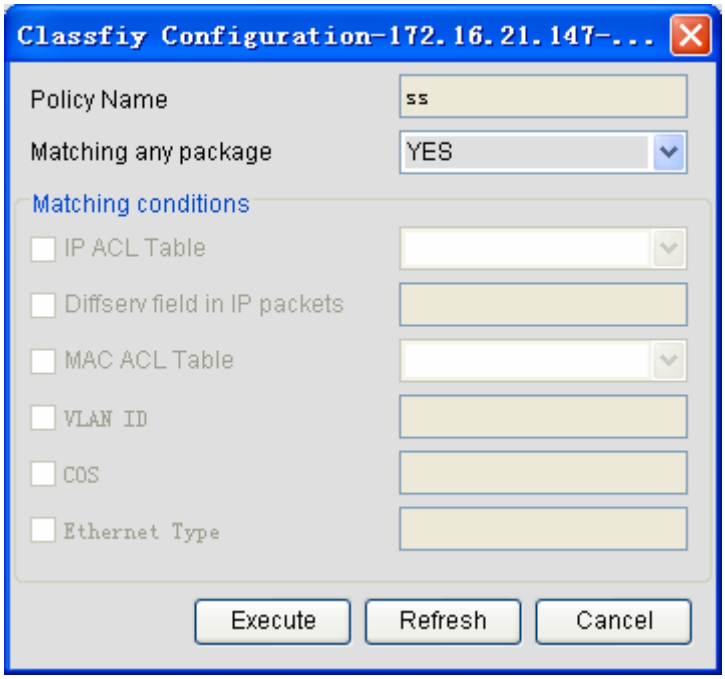
Enter a policy name and then click **OK** to create a policy.

- Setting flows

Choose one policy and then click **Flow settings**.See the following figure:



In the following dialog box, set the data flow which matches up with the above-mentioned policy. See the following figure:

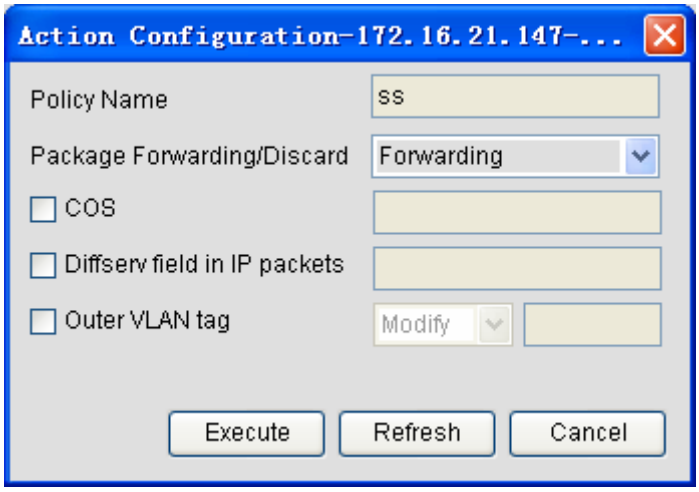


If you select **Yes** in the **Match any packet** dropdown list box, any data packet will be matched by default.

If you select **No** in the **Match any packet** dropdown list box, you shall then set the matchup conditions.

◆ Setting actions

Choose one policy and then click **Action settings**. A dialog box appears, on which you can set to forward or drop data flows.See the following figure:



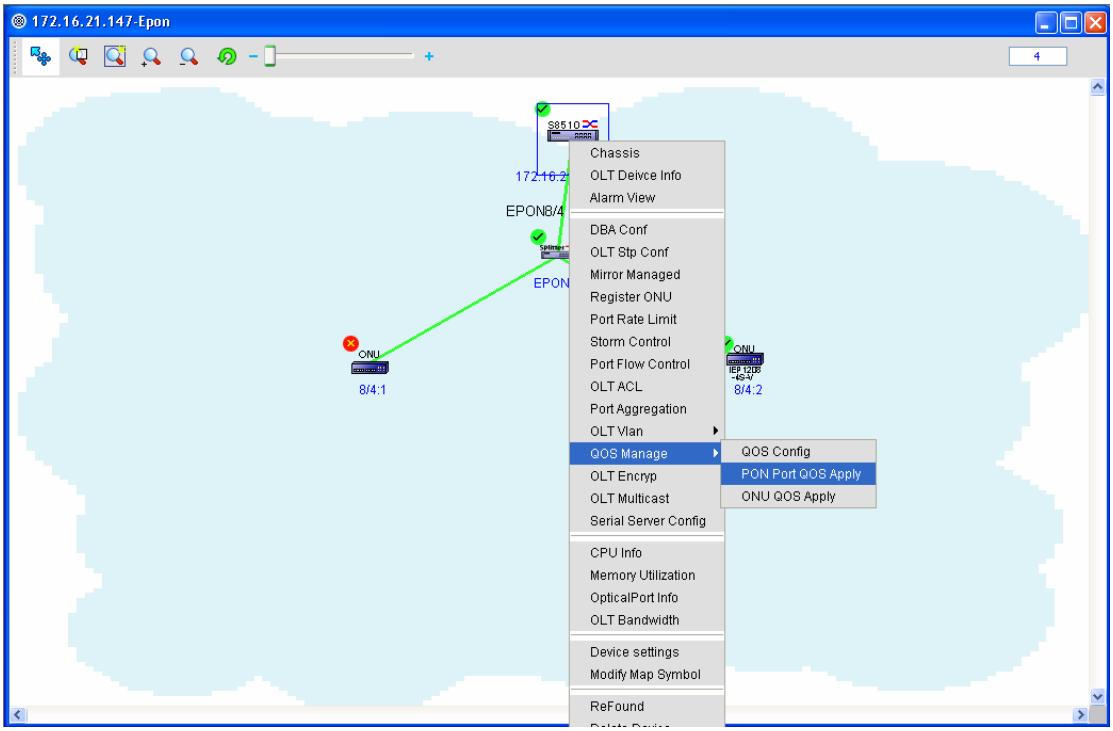
◆ Deleting policies

Choose one policy and then click **Cancel a policy**. A confirmation dialog box appears for to confirm whether to cancel the chosen policy.

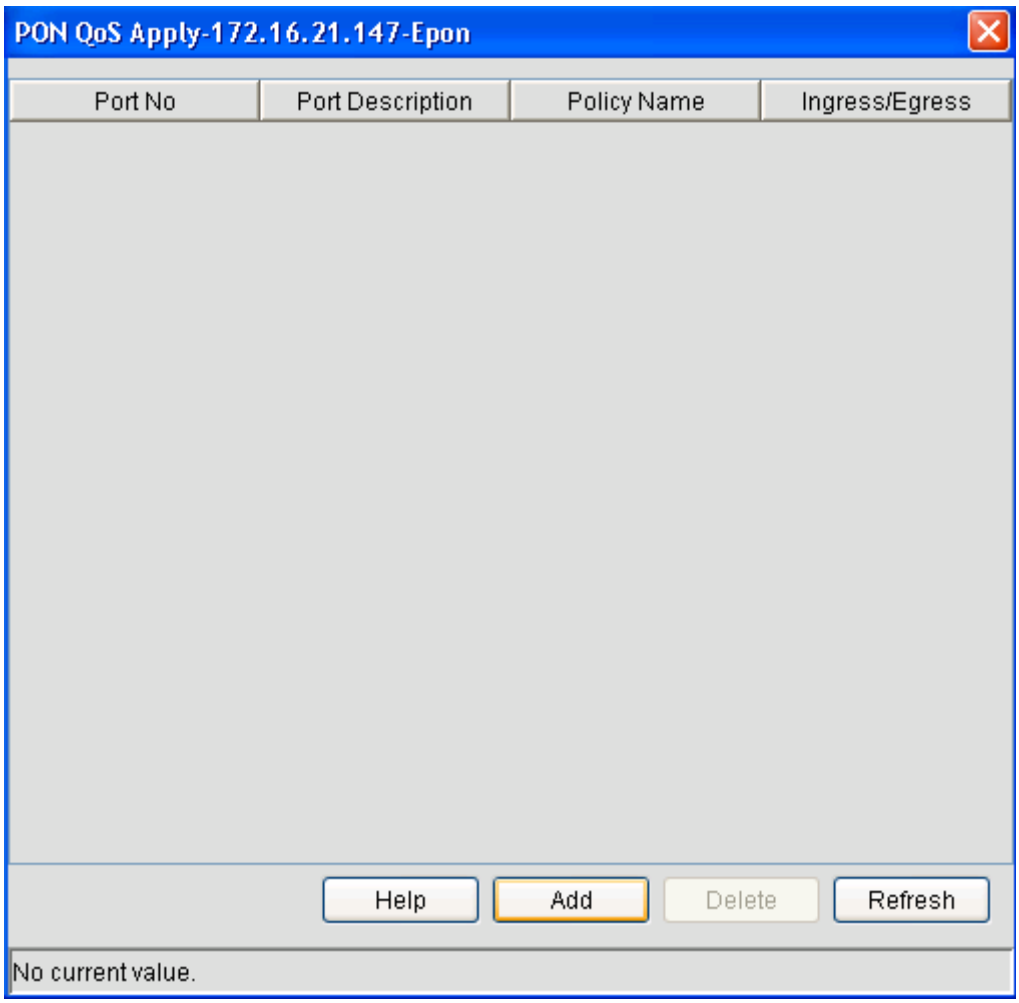
5.3.9.2 Applying QoS on the PON port

You can apply the QoS policies on a specific port. But this application is flexible and you can apply multiple policies on a same port or a policy on multiple ports.If two or more policies are applied on a same port, the firstly applied policy has the highest priority and the latter ones have the low priority.

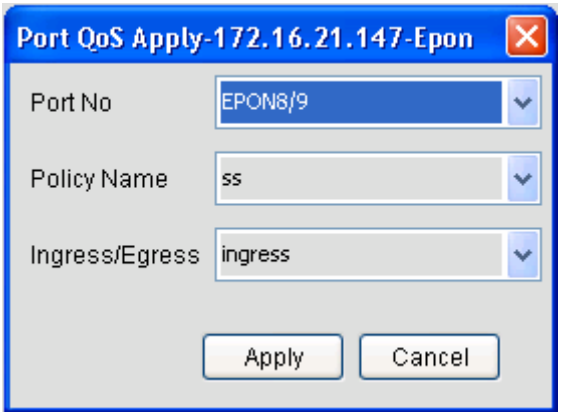
Right click OLT and in the right-key menu select **QoS management** and then **Apply QoS on the PON port**. See the following figure:



After **Apply QoS on the PON port** is clicked, the following window appears:



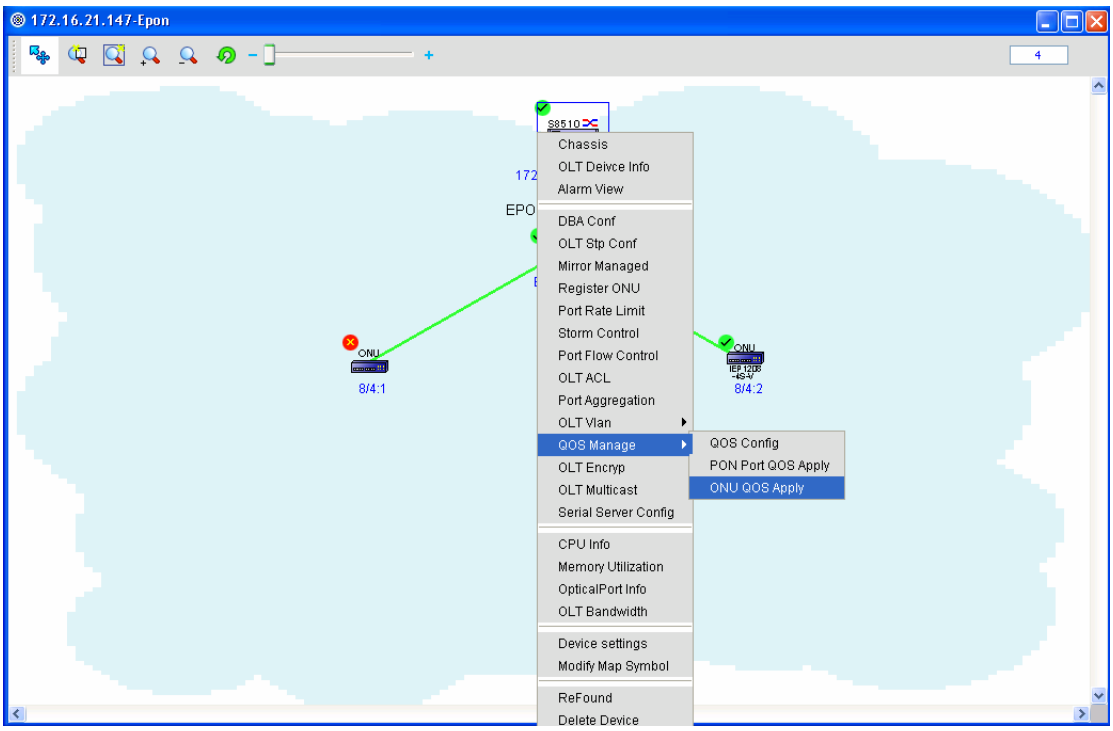
Click **Add**. A dialog box appears, as shown in the following figure:

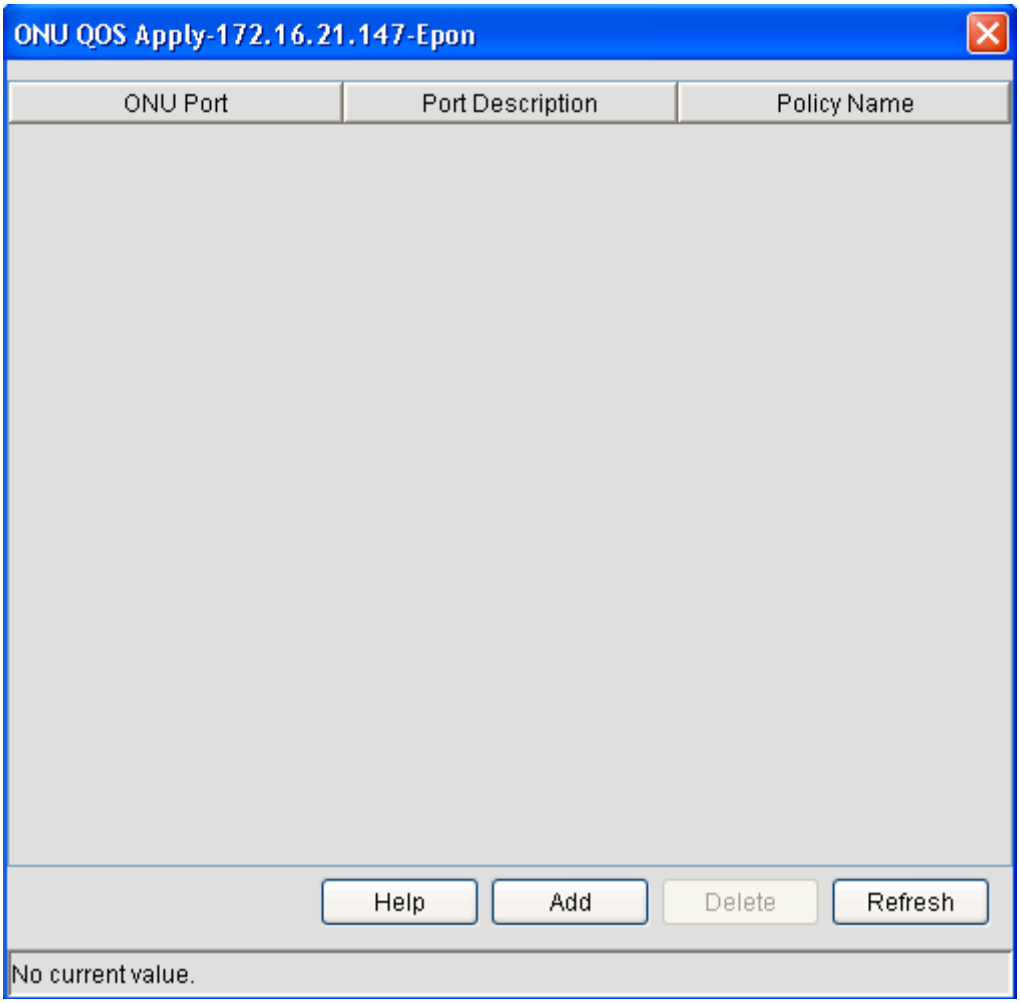


Select a PON port and a corresponding policy name, and then click **Apply** to apply this policy on the PON port.

5.3.9.3 Applying QoS on ONU

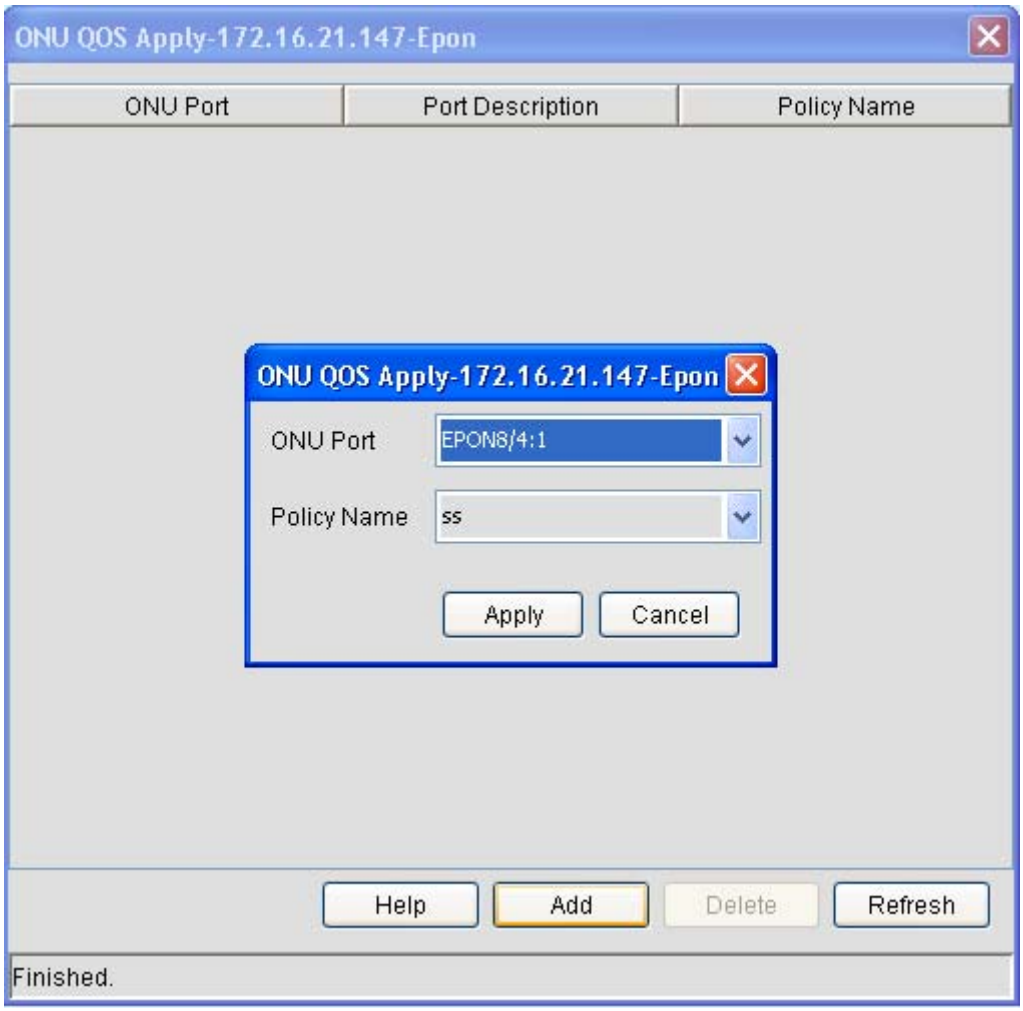
You can set the QoS of ONU through one of the following two methods:
Right click OLT and in the right-key menu select **QoS management** and then **Apply QoS on ONU**. See the following figure: See the following figure:





Click **Add**. A QoS policy is added on ONU.

2. Select the **ONU** icon on the topology and choose **Apply QoS** on the right-key menu.See the following figure:



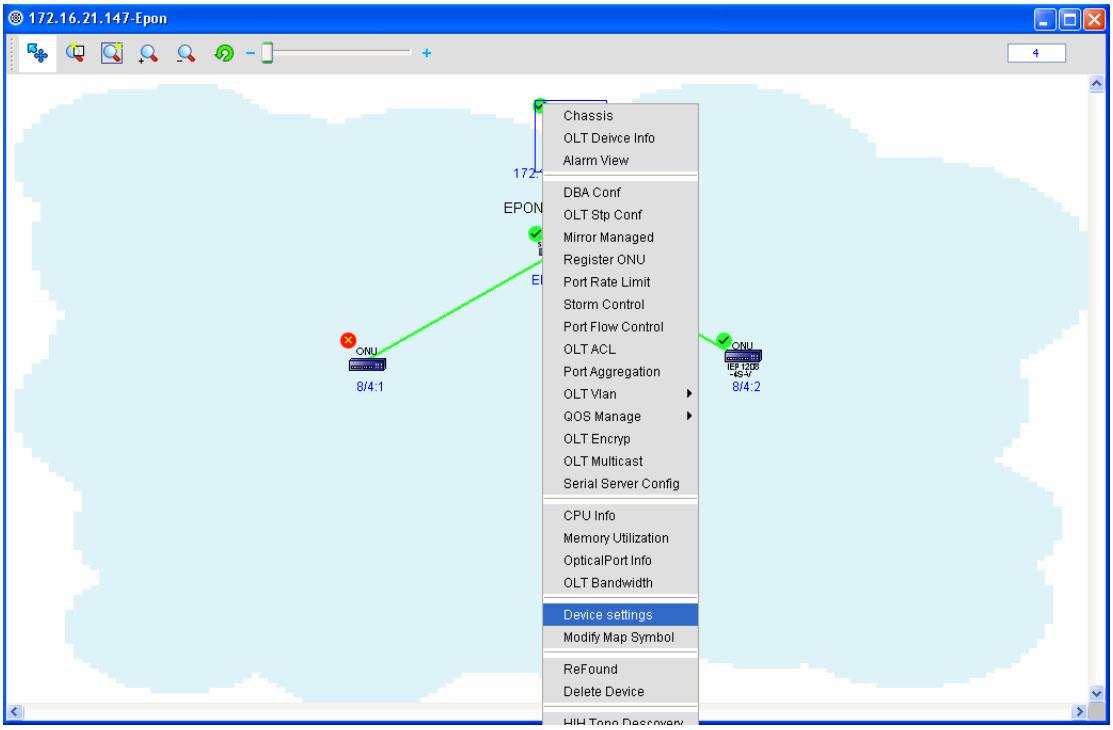
5.3.10 Saving the Settings

To save the settings means to save all the current OLT settings, and the saved settings will remain all the same even after rebooting.If the current OLT settings is not saved, all settings will be gone after rebooting.

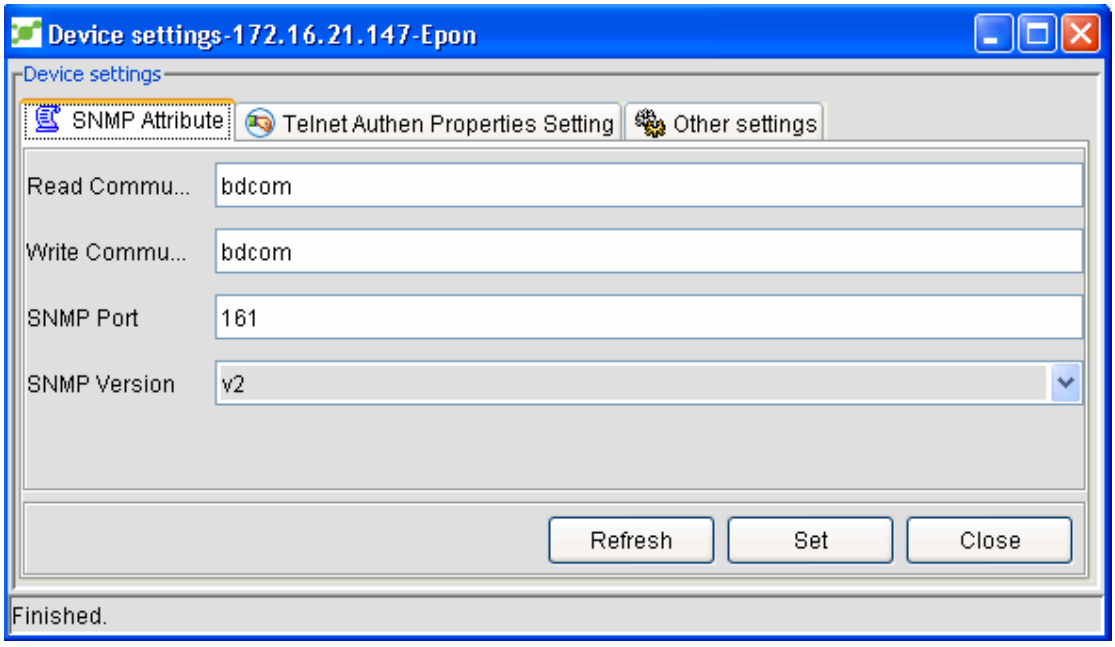
5.3.11 Attribute Settings

The detailed procedure is as follows:

Right click OLT and then choose **Set attributes**. See the following figure:



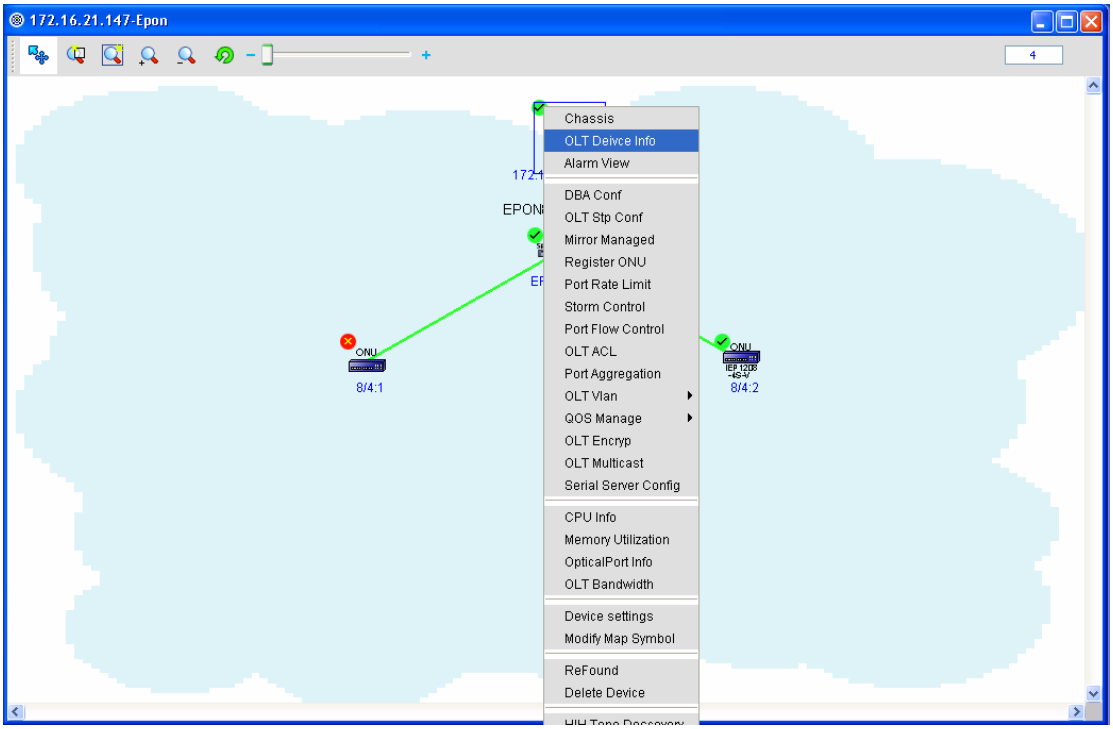
After **Set attributes** is clicked, a window appears, as shown in the following figure:



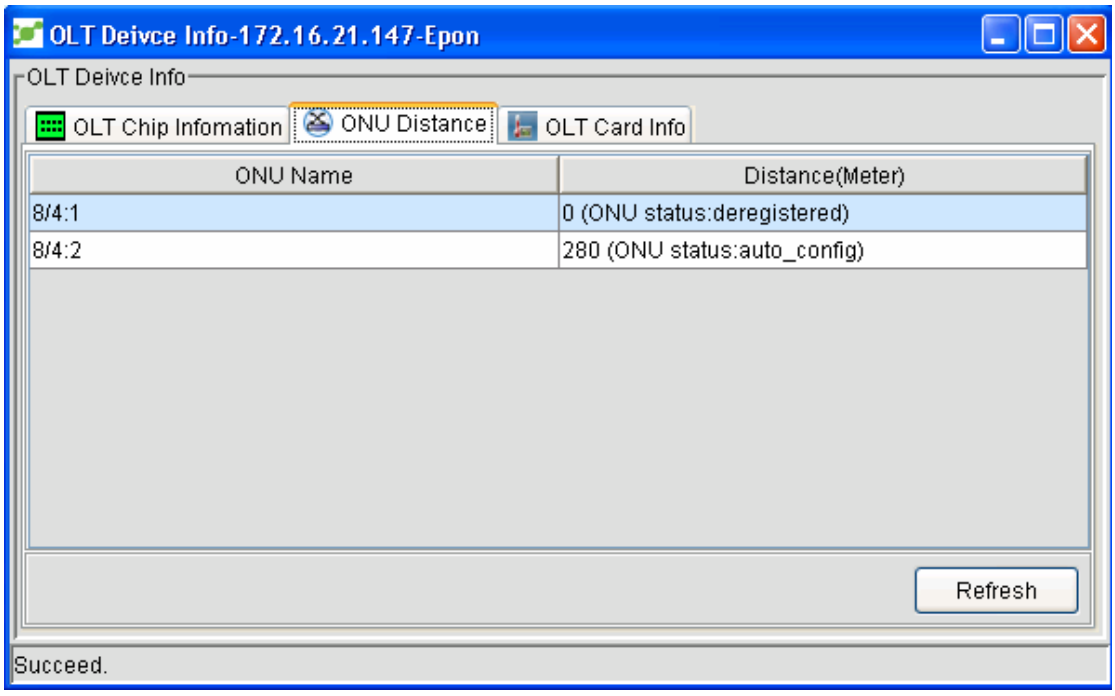
5.3.12 Distance Measurement of ONU

OUN distance measurement means to test the distance between the PON port and each downlink ONUs of the current OLT.Right click OLT on the topology and select **Basic Info**, as

shown in the following figure:



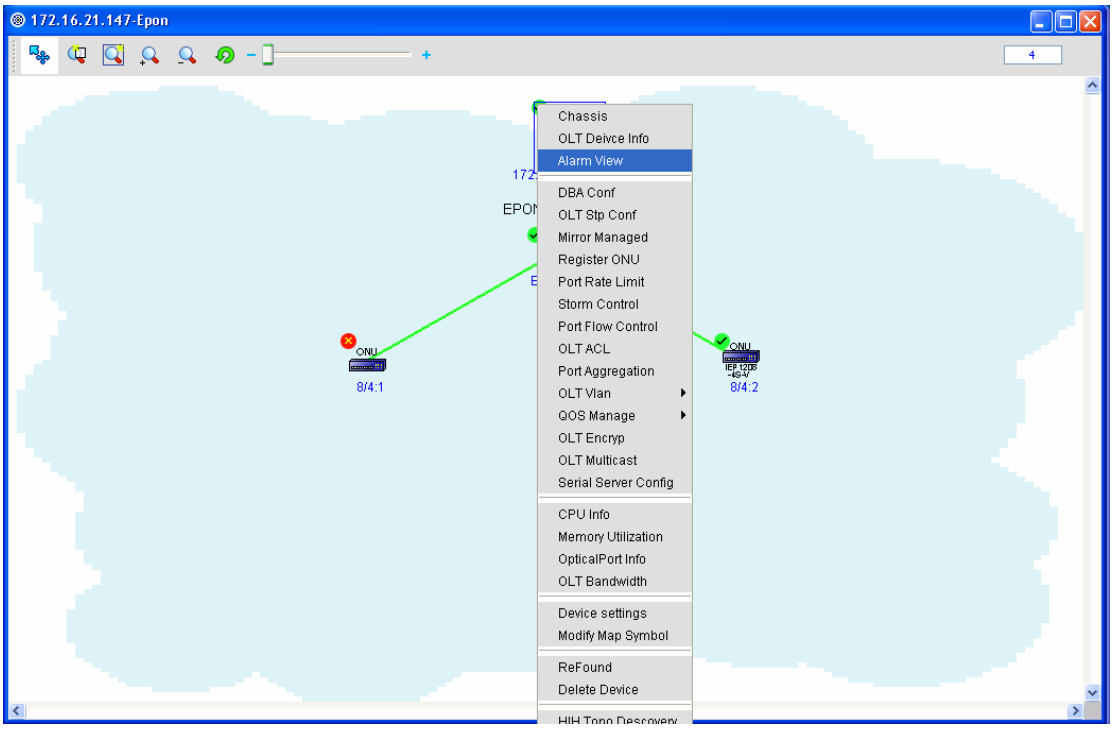
After the **Basic Info** is clicked, a window appears, as shown in the following figure. In this window, select the **ONU distance measurement** tab.

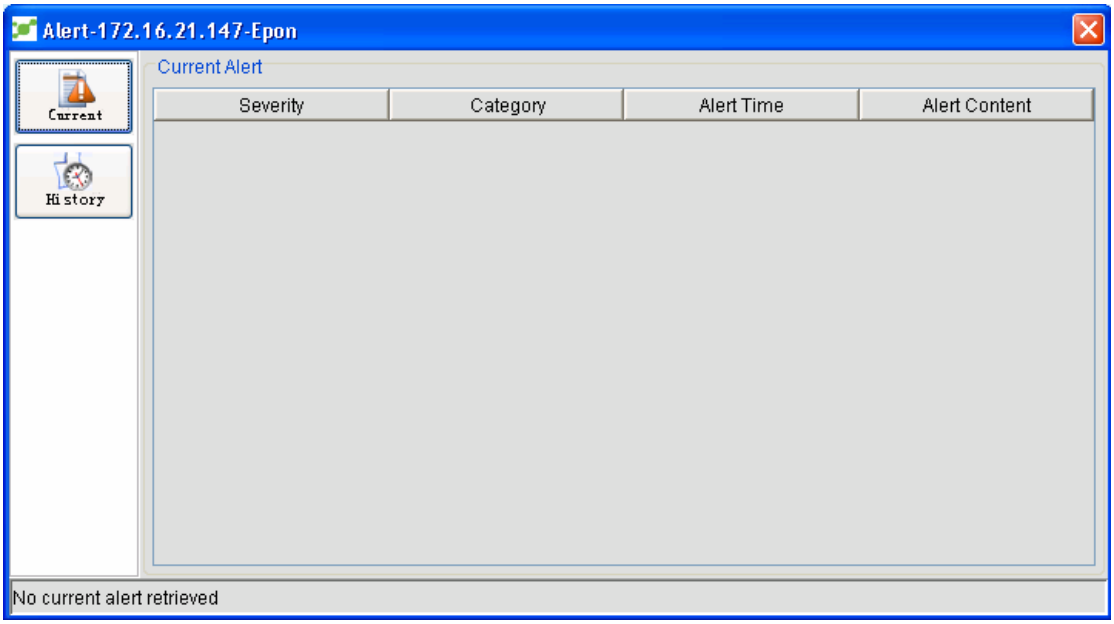


5.3.13 Browsing Alarms

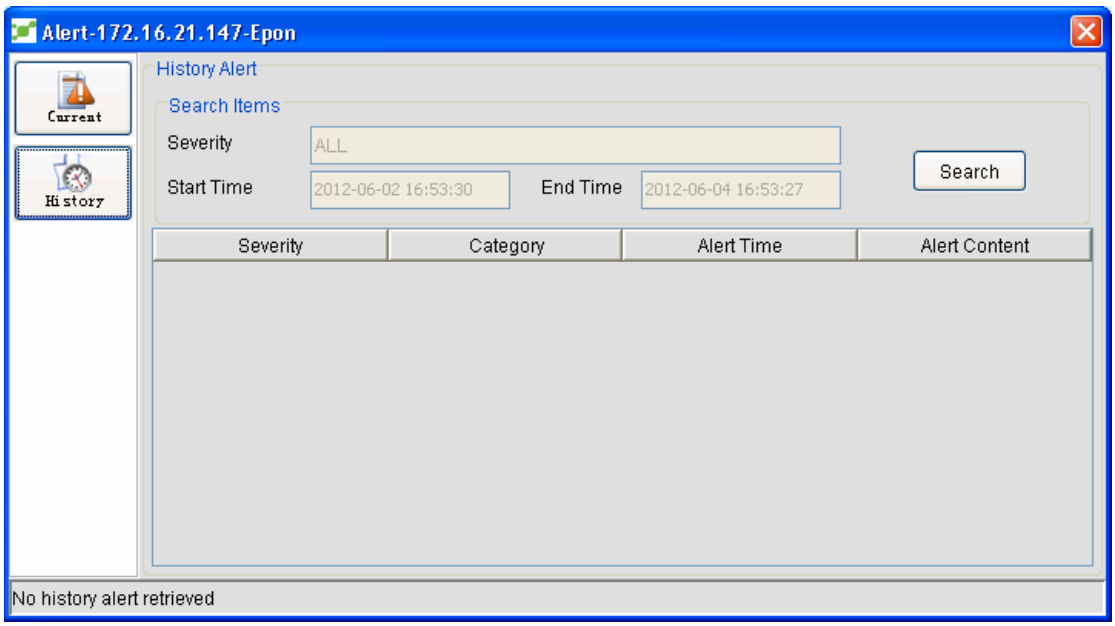
Browsing OLT alarms includes browsing the current alarms and the past alarms.The current

alarms mean the ongoing alarms at present.The past alarm means the alarms that happended already.Right click OLT and then choose **Browse alarms**. See the following figure:





Click **Past alarms**. The following window appears:



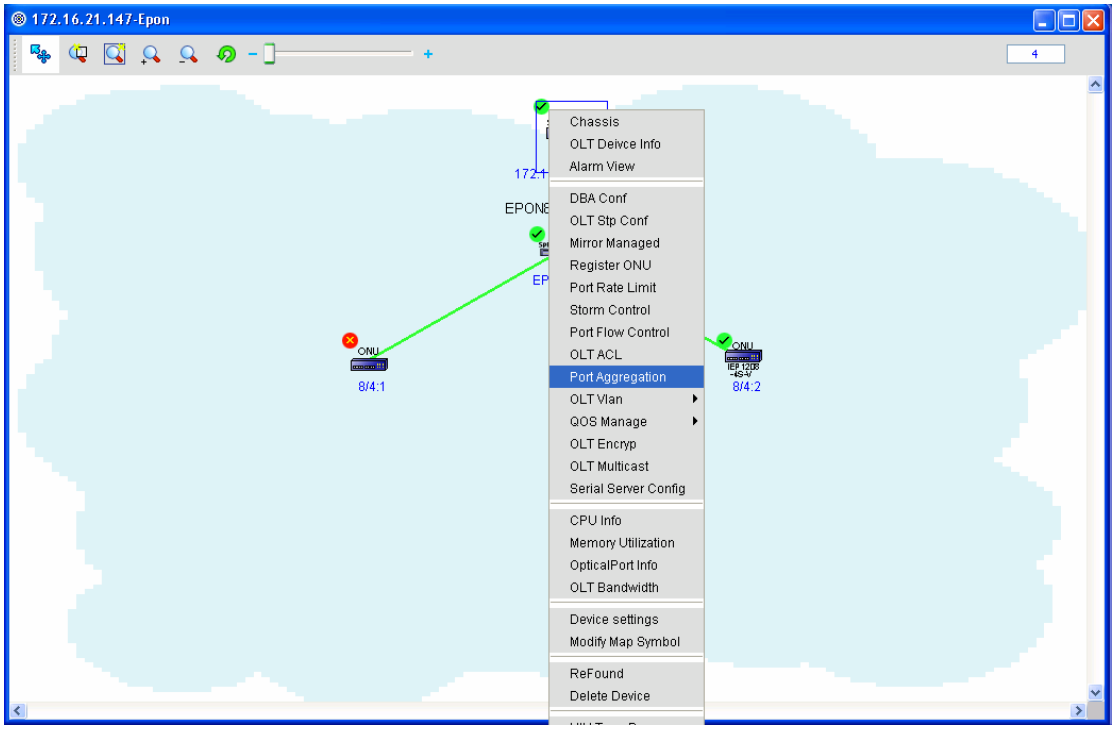
5.3.14 Link Aggregation

Link aggregation means to combine two or more data channels into a single channel, which shows as a logic link with larger bandwidth.Link aggregation is always used to connect one or multiple devices if they require a lot of bandwidth, such as the servers or server group in connection with the backbone network.

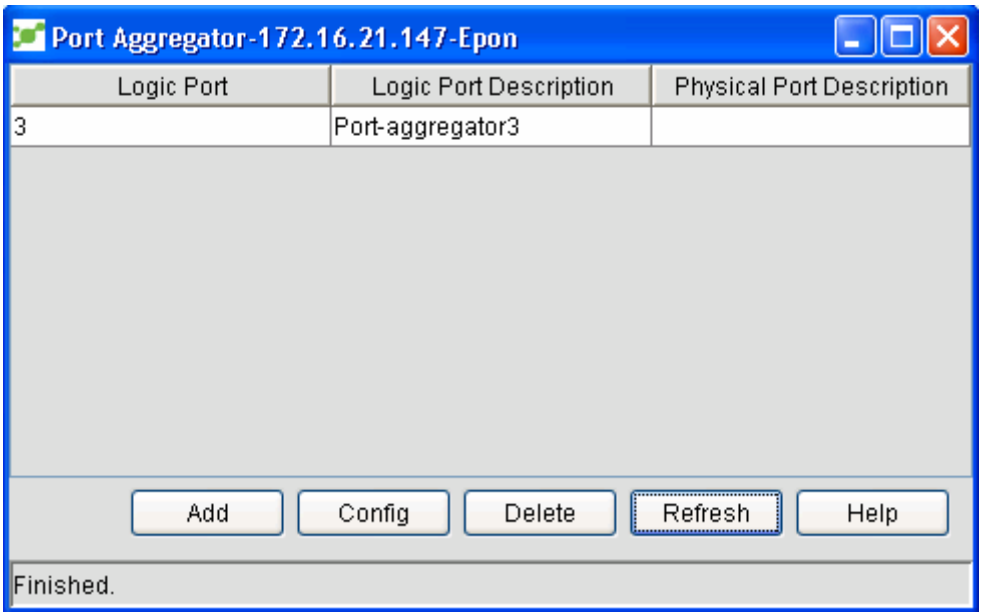
Link aggregation mainly realizes port aggregation on the network manager, that is, binding several physical ports, which are similar in their attributes, into a logic channel.

The operation procedure is shown below:

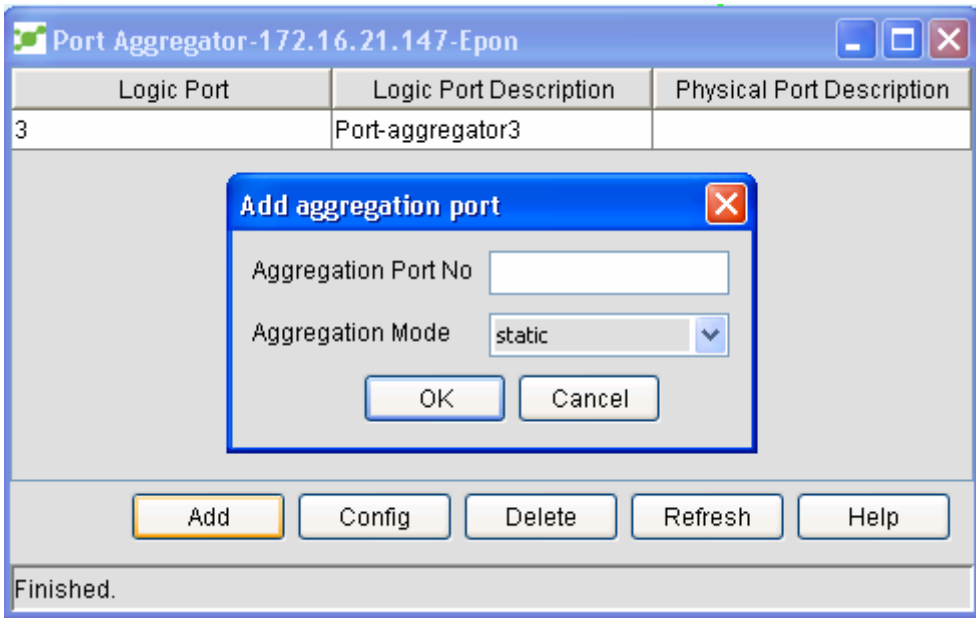
1. Open NMS.
2. Right click OLT.



3. Click **Link aggregation**. The following window appears:

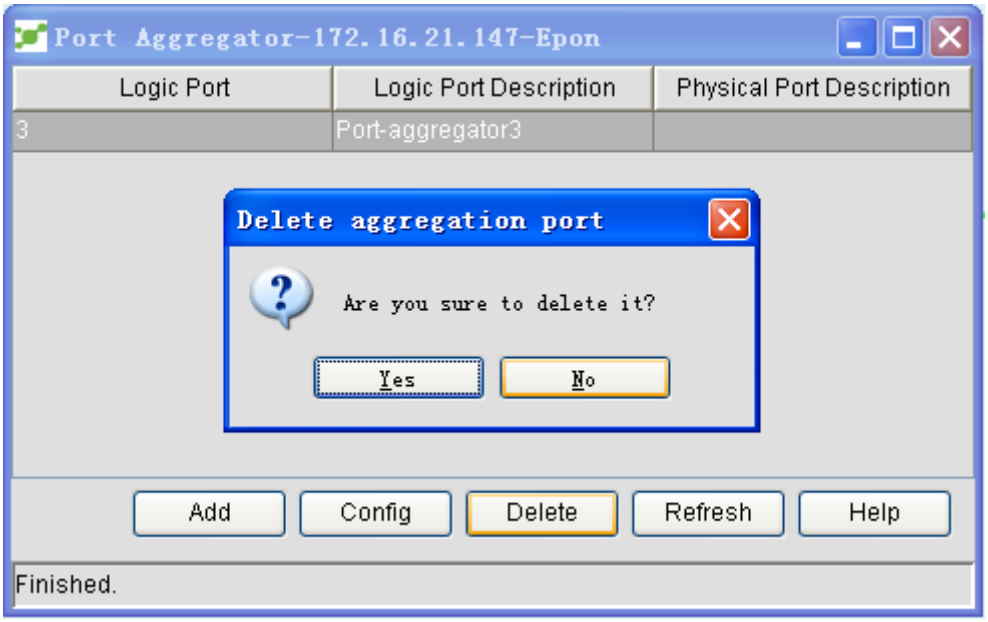


4 Add a logic port and click **Add**. Then you have to enter the port ID and the aggregation. Note: the port ID cannot be duplicate and cannot surpass the allowable value range.



5. Select a logic port and click **Set** to set this logic port.To combine multiple physical ports into a logic port, select to-be-aggregated port IDs and then click **Execute**.If the physical ports you have chosen are already aggregated into a logic port, these physical ports, after **Execute** is clicked, will not belong to their previous logic port and be aggregated into a new logic port.

6. Select a logic port and click **Cancel**. The logic port will be deleted.



5.3.15 Setting the Serial-Interface Server

OLT serial configuration of OLT includes the global session configuration and the attribute configuration of each serial interface.Right click OLT with the serial interface and select **Set the serial interface server**.

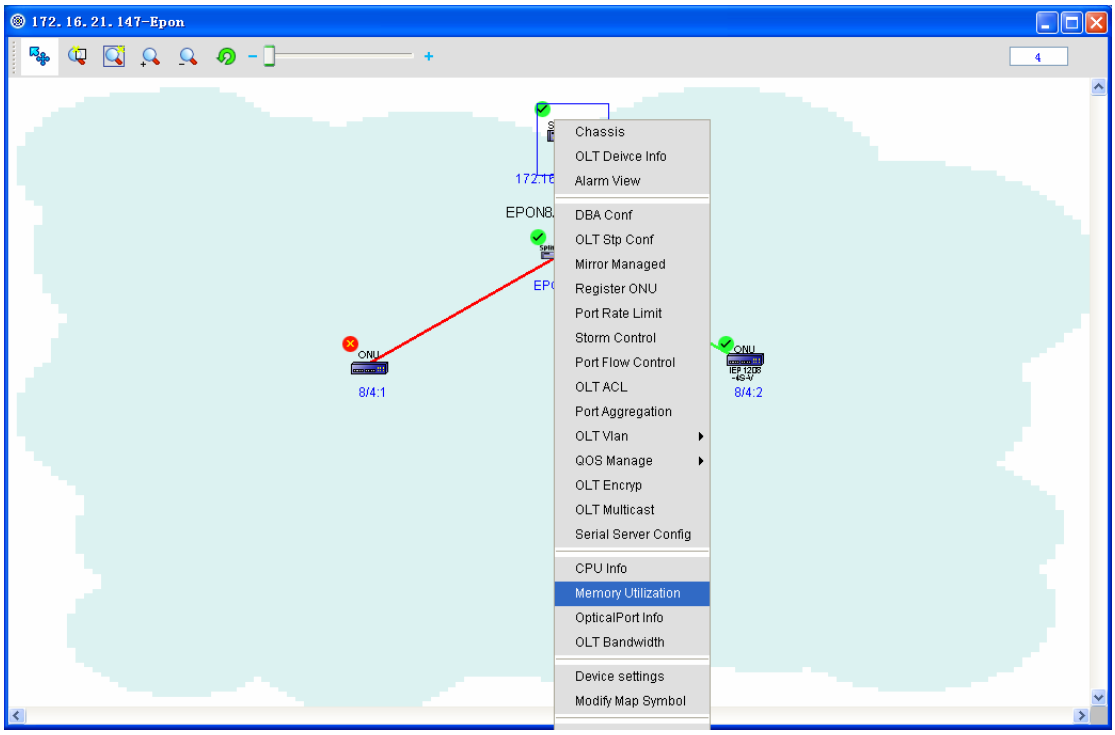
The above-mentioned figure shows the session configuration, which is effective to all serial interfaces.Click **Set serial interface**.

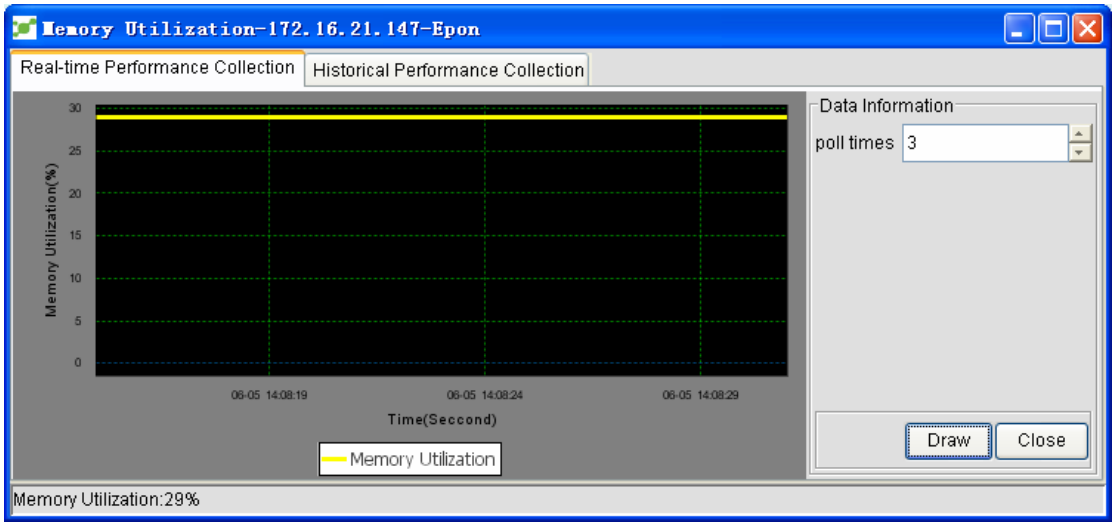
Click one row in the serial interface configuration list, that is, click some serial interface. The **Setup** button avails. Click **Setup**. A window for setting this serial interface appears.

5.3.16 Memory Usage

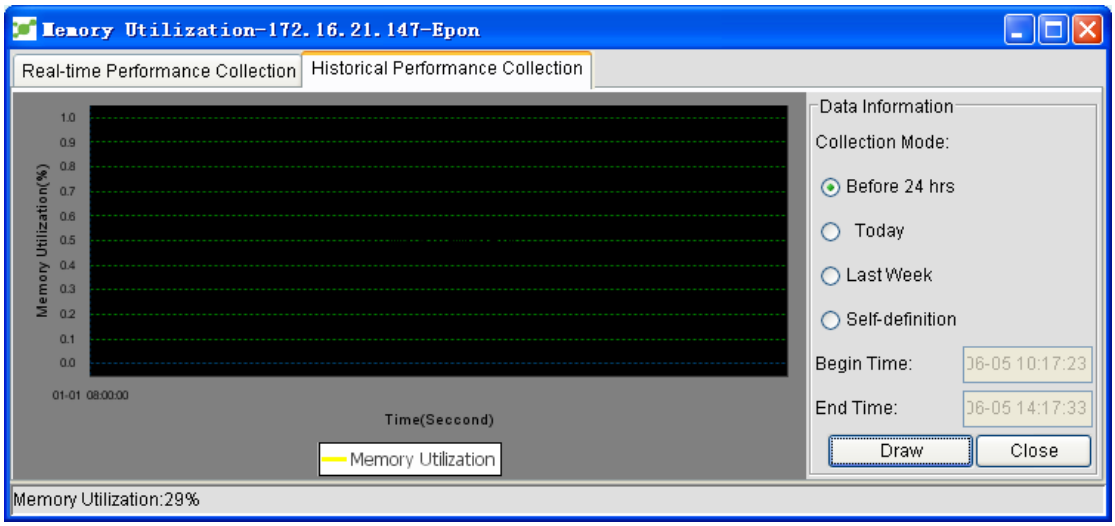
Open NMS.

Right click OLT and then the **Memory usage** option. The following figure appears. To set the polling interval, click **Draw map**. See the following figure:





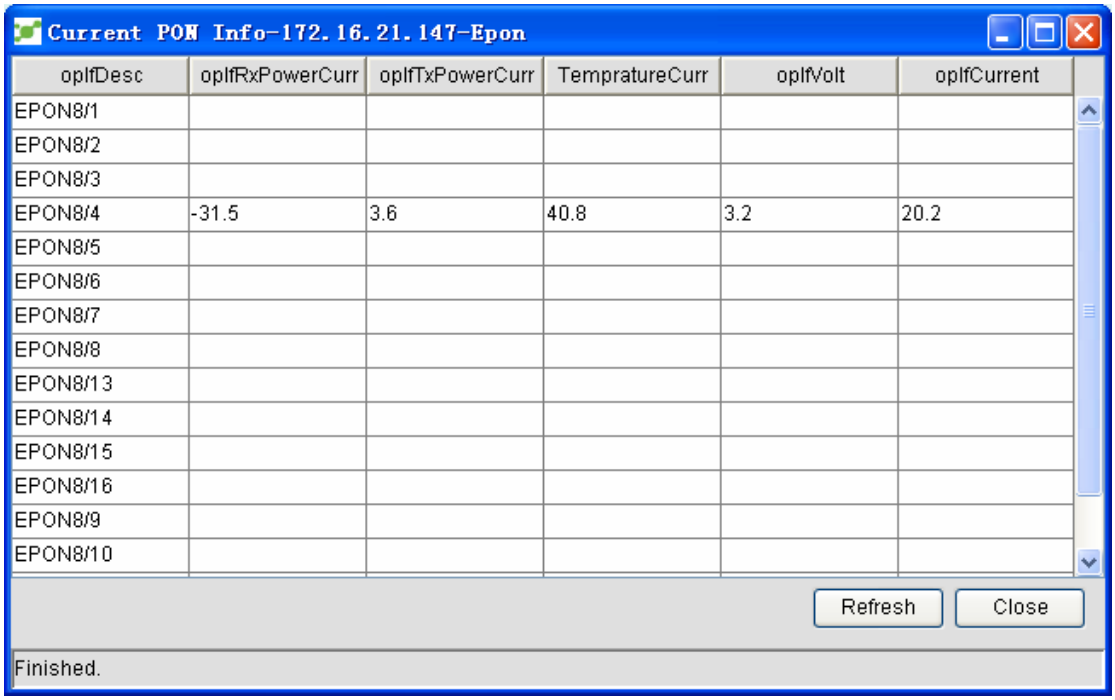
History statistics: Click the **Historical Performance Statistics** tab and then choose conditions.Click **Draw map**.See the following figure:



5.3.17 Information About Optical Modules

Open NMS.

Right click OLT and click **Parameters of optical module**. The following figure appears:



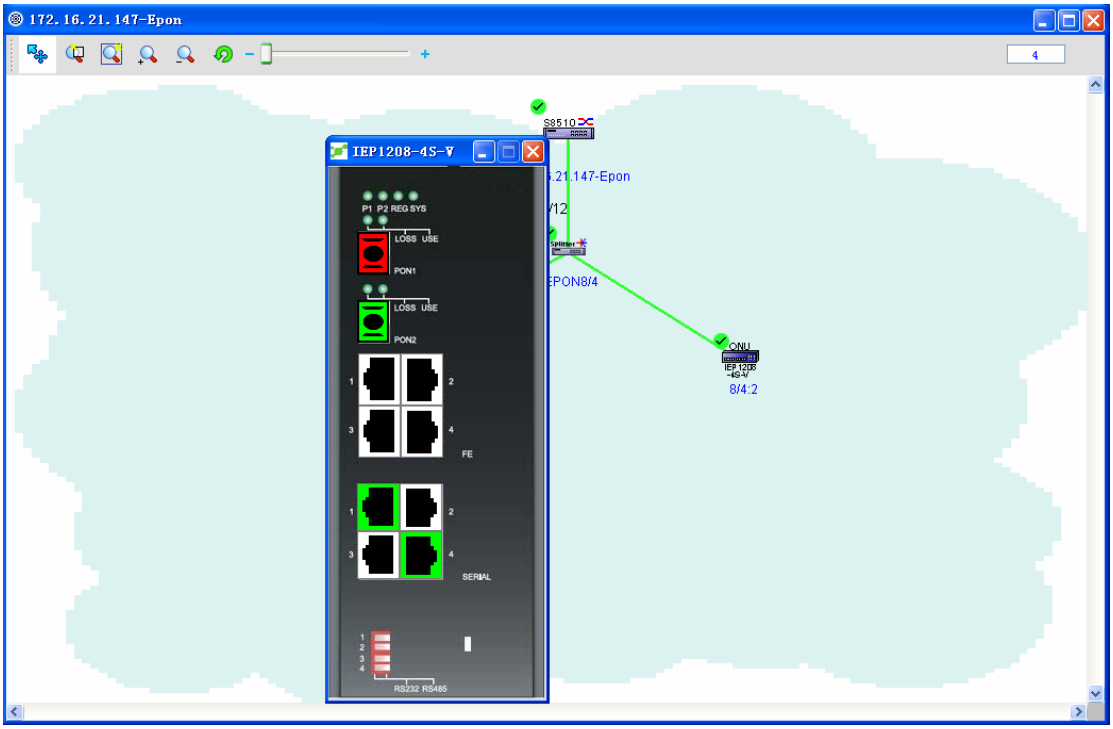
opIfDesc	opIfRxPowerCurr	opIfTxPowerCurr	TempratureCurr	opIfVolt	opIfCurrent
EPON8/1					
EPON8/2					
EPON8/3					
EPON8/4	-31.5	3.6	40.8	3.2	20.2
EPON8/5					
EPON8/6					
EPON8/7					
EPON8/8					
EPON8/13					
EPON8/14					
EPON8/15					
EPON8/16					
EPON8/9					
EPON8/10					

Note: If there is no data about a PON interface, the parameters of this PON interface are empty.

5.4 ONU Settings

Right click ONU and select **Device faceplate**. The device faceplate appears.In the faceplate,

there are PON ports and common ports. On the 85 model, there are also the active and standby faceplates. These ports and faceplates have related operation menus.
The device’s faceplate is shown in the following figure:

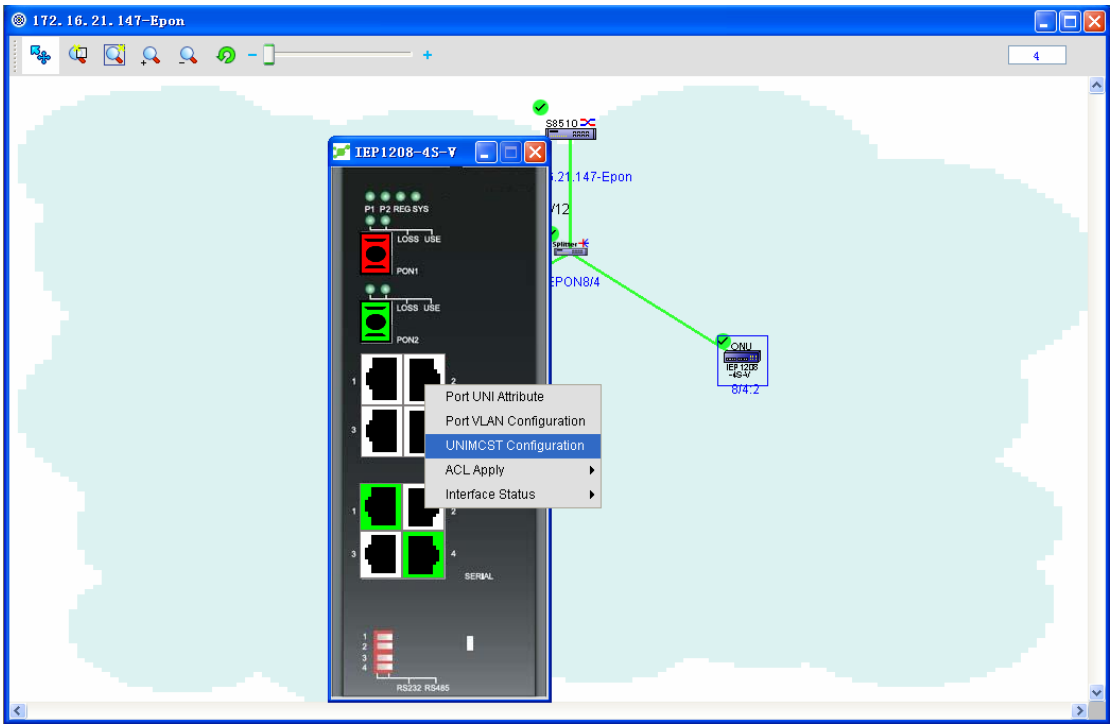


Port’s status: If the port is red, it means that the port cannot be used.If the port is white, it means that the port can be used but is not connected to a network device.If the port is green, it means that the port can be used and has connected a network device.

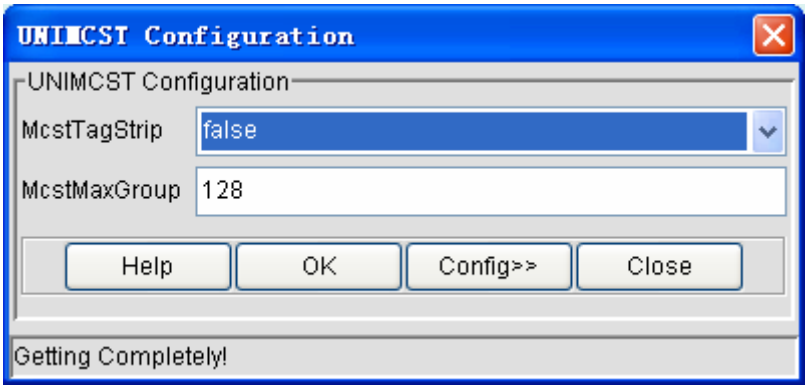
5.4.1 Multicast Configuration

5.4.1.1 Configuring TagStri and MaxGroup

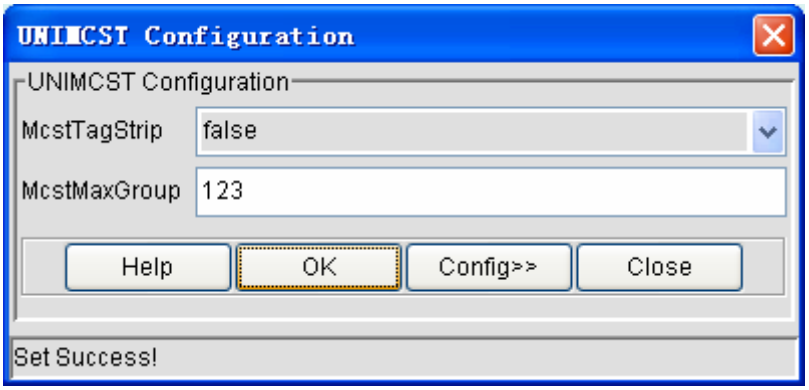
Right click the ONU icon and select **Device's faceplate** and then right click **Ethernet interface** on the faceplate.See the following figure:



Click **Multicast Setup**. A window appears, as shown in the following figure:

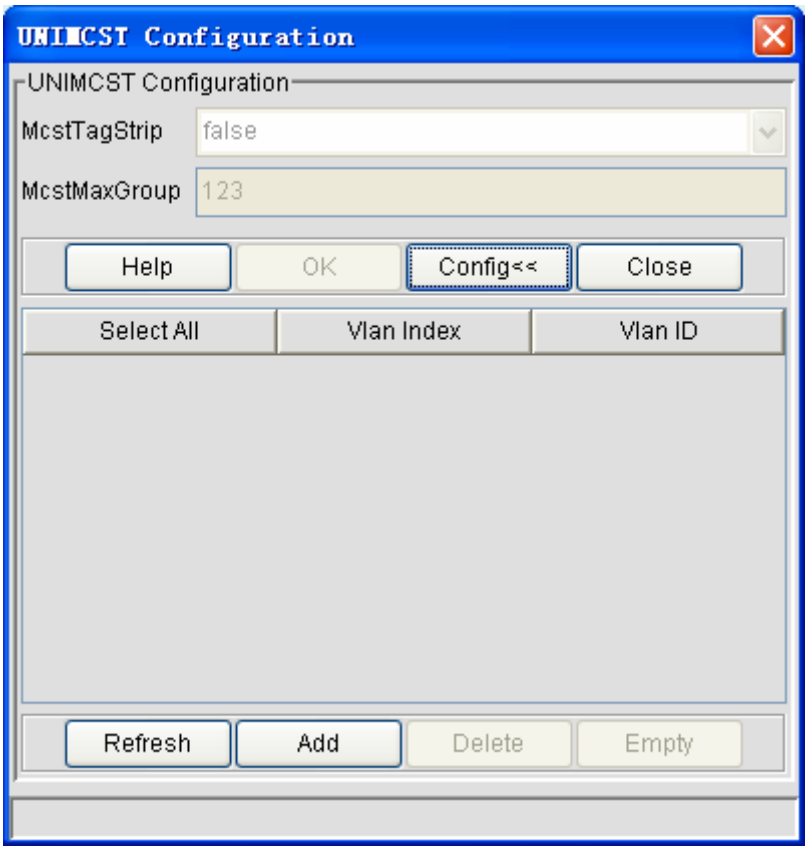


On this window, you can set TagStrip and MaxGroup.Set TagStrip and MaxGroup to **true** and **123** respectively and then click **OK**.See the following figure:



5.4.1.2 Configuring the VLAN of a port

Click **Set**>>. The following page appears:

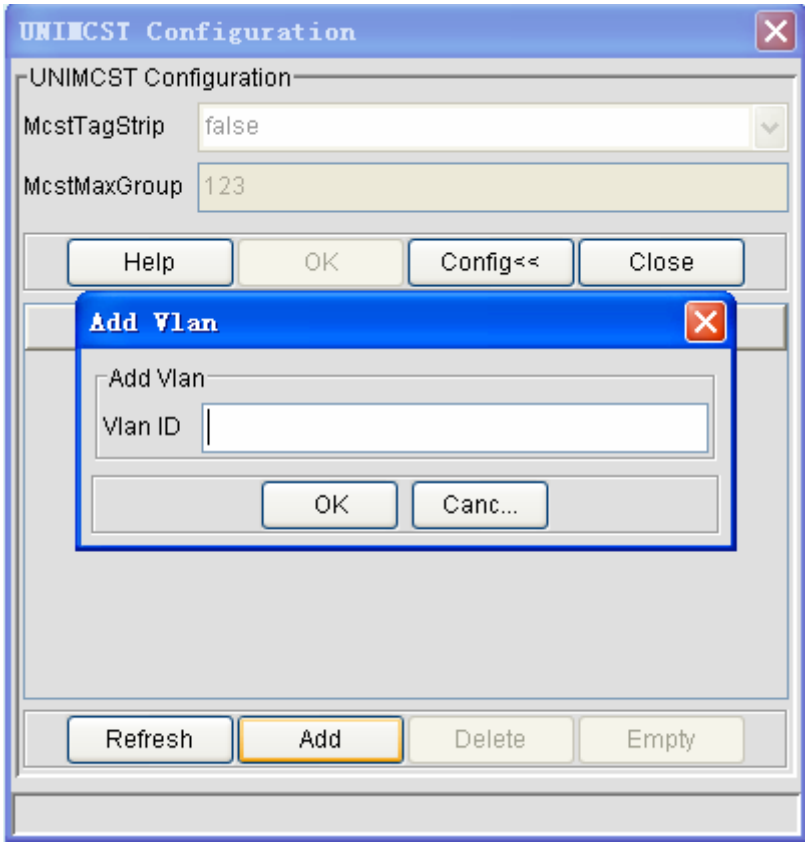


The VLANs for corresponding ports are shown in the figure above.You can add, delete and clear the VLAN of a port.

- Adding VLAN

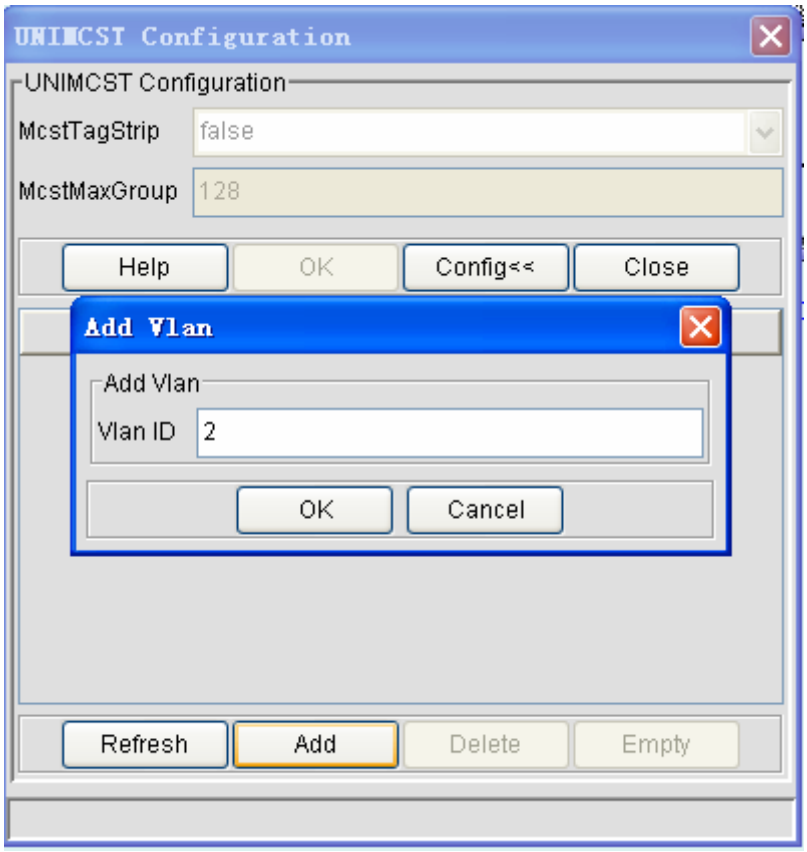
When adding VLAN, you should note that you can add at most 64 VLANs (VlanID range: 2-4094).

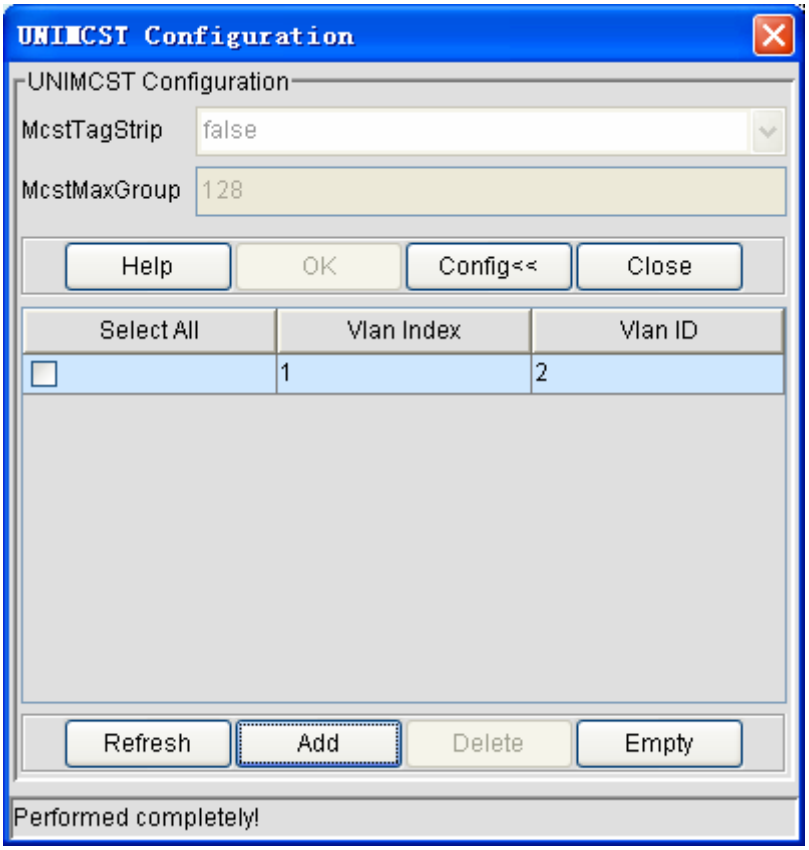
Click **Add**. The following page appears:



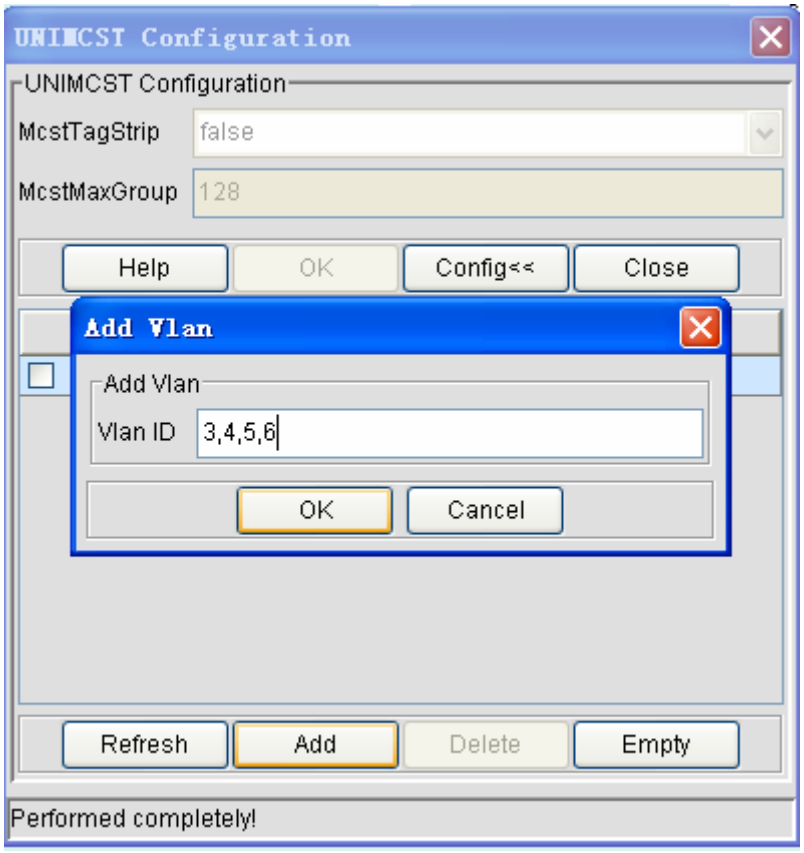
In the **Add VLAN** text box, you can add one or multiple VLANs.

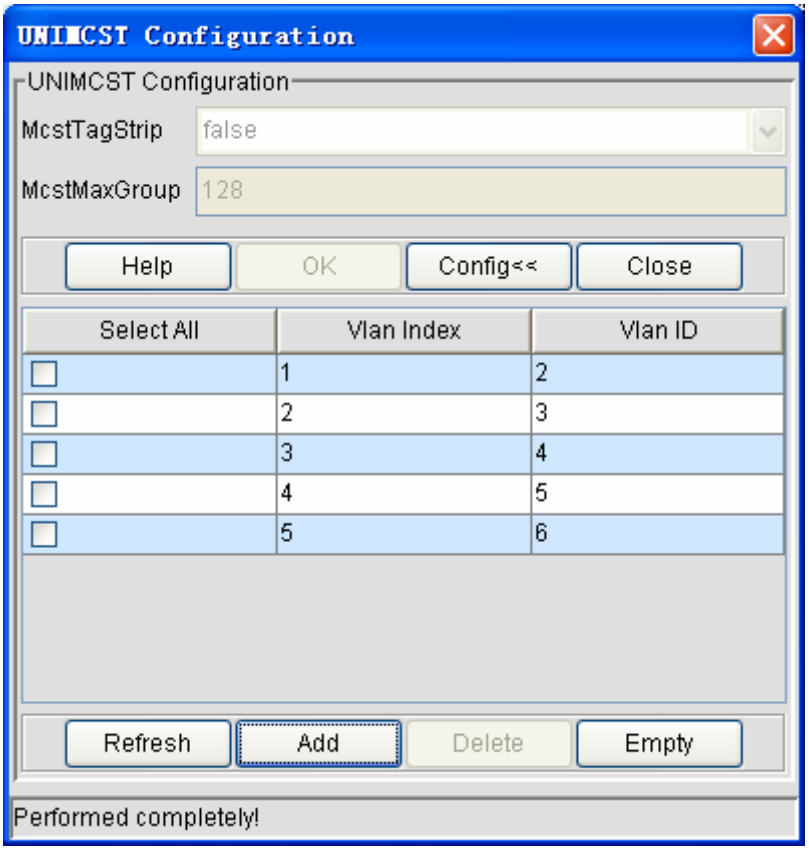
As to adding a single VLAN, see the following figure:

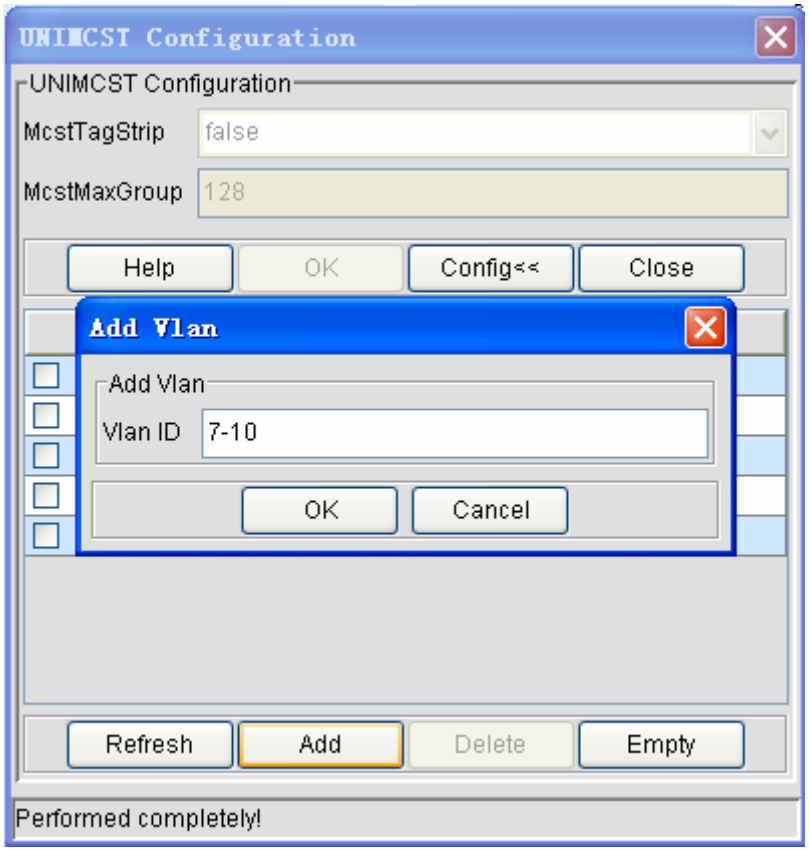


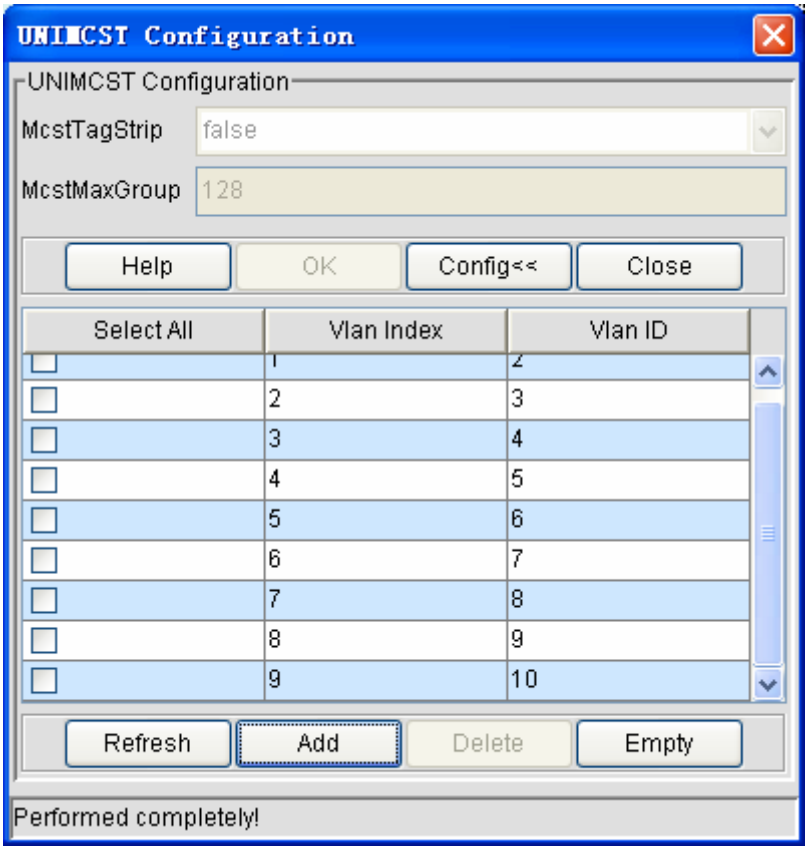


As to adding multiple VLANs, see the following two figures:



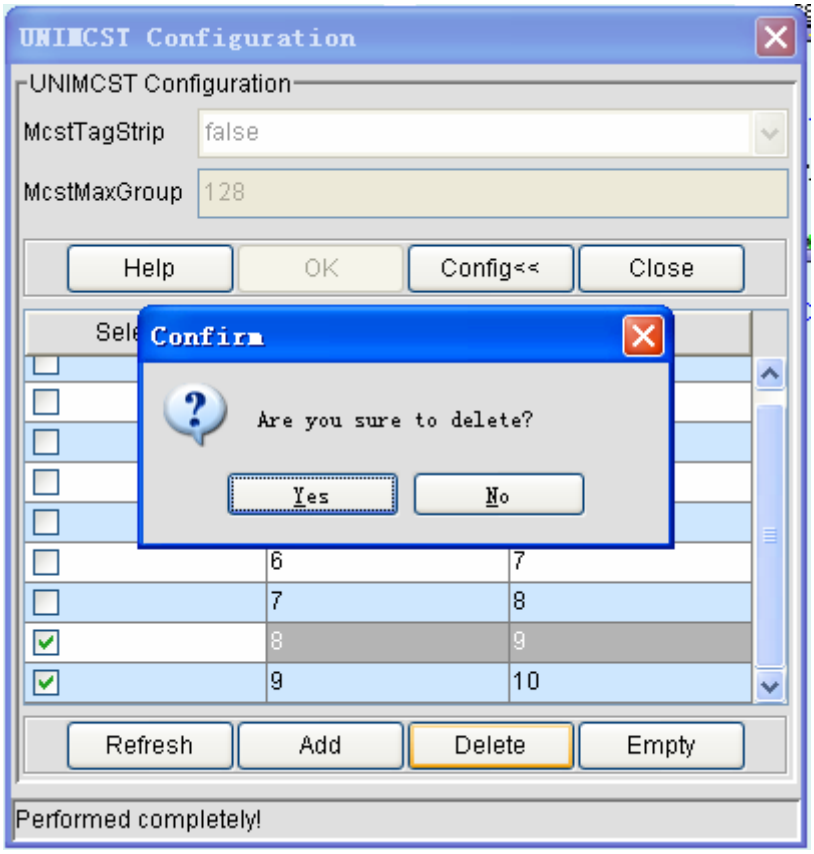

UNIMCST Configuration
UNIMCST Configuration
McstTagStrip
false
McstMaxGroup
128
Help
OK
Config<<
Close
Select All
Vlan Index
Vlan ID
1
2
2
3
3
4
4
5
5
6
Refresh
Add
Delete
Empty
Performed completely!


UNIMCST Configuration
UNIMCST Configuration
McstTagStrip
false
McstMaxGroup
128
Help
OK
Config<<
Close
Add Vlan
Add Vlan
Vlan ID
7-10
OK
Cancel
Refresh
Add
Delete
Empty
Performed completely!

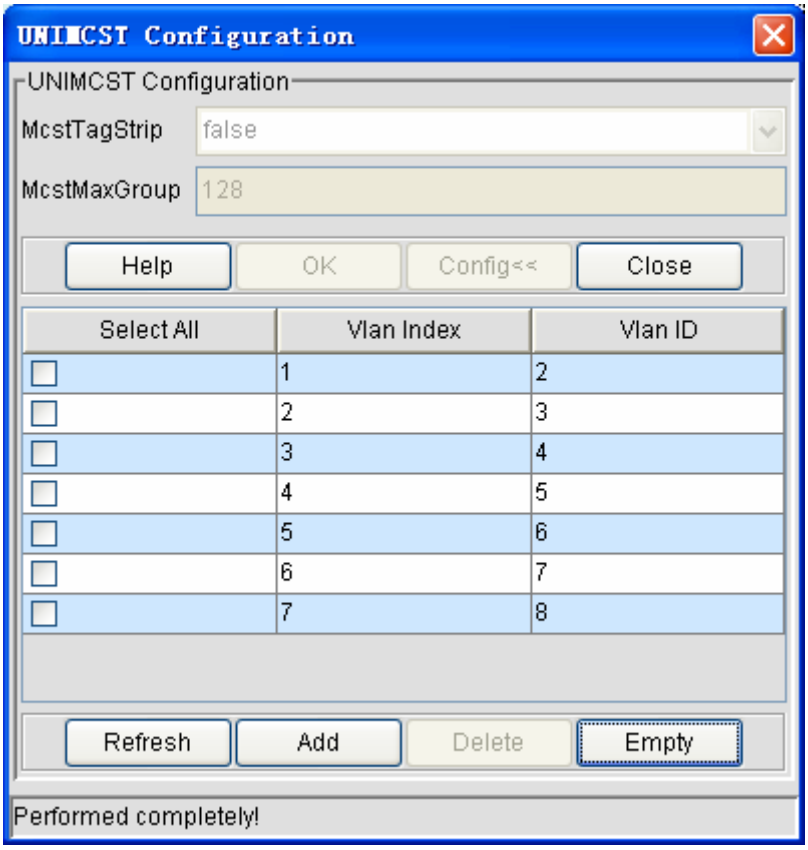


➢ Deleting the VLAN of a port

Select a VLAN and then click **Delete**.See the following figure:

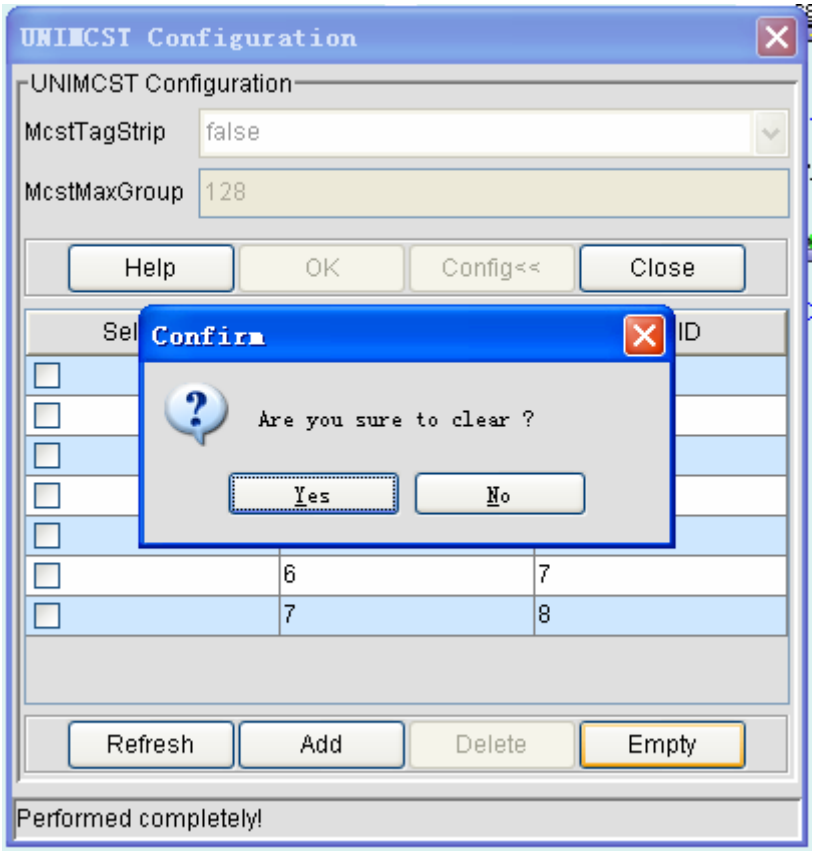


Click **OK**. The selected VLAN is deleted.See the following figure:

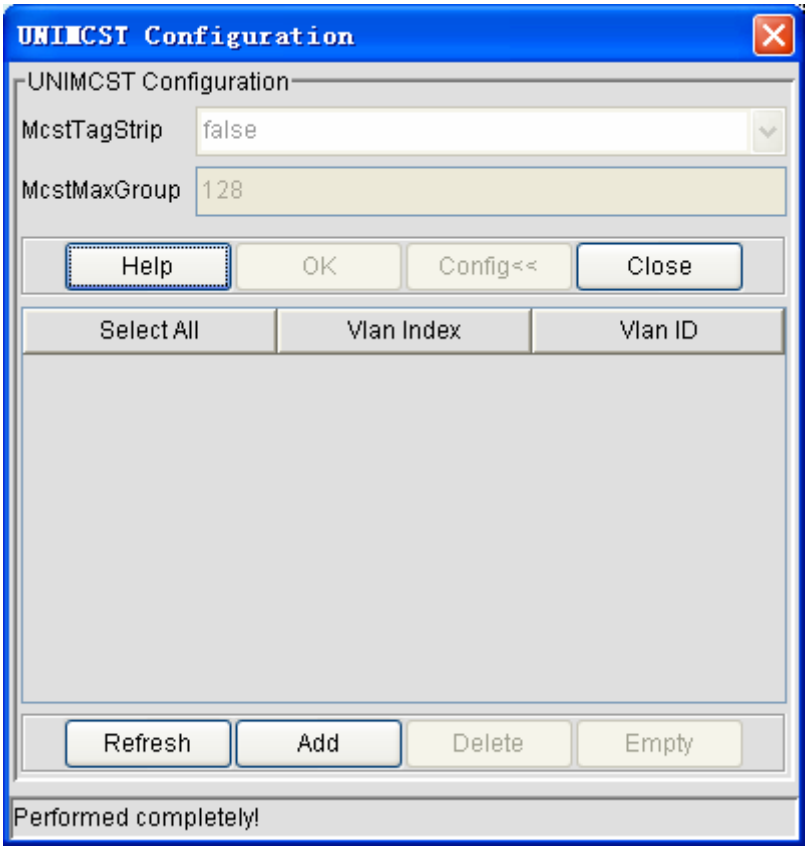


If you click **All Select** and then **Delete**, all VLANs here will be deleted.

To clear all VLANs of a port, click **Clear**. See the following figure:



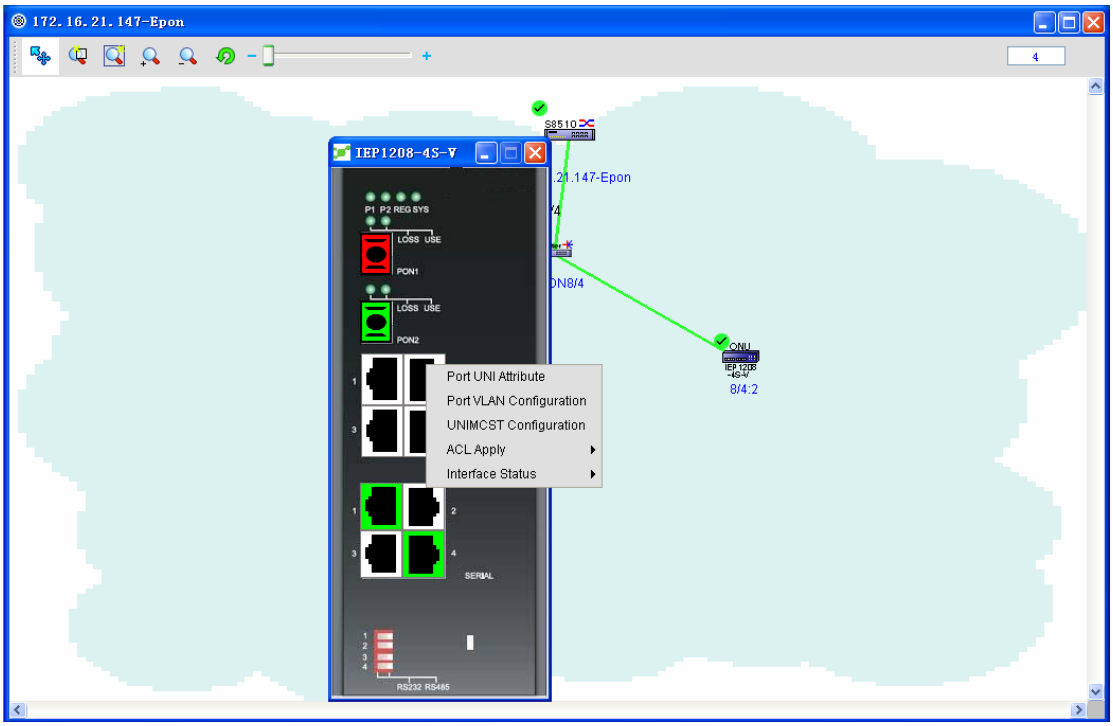
Click **OK**. All VLANs of the port will be cleared.See the following figure:



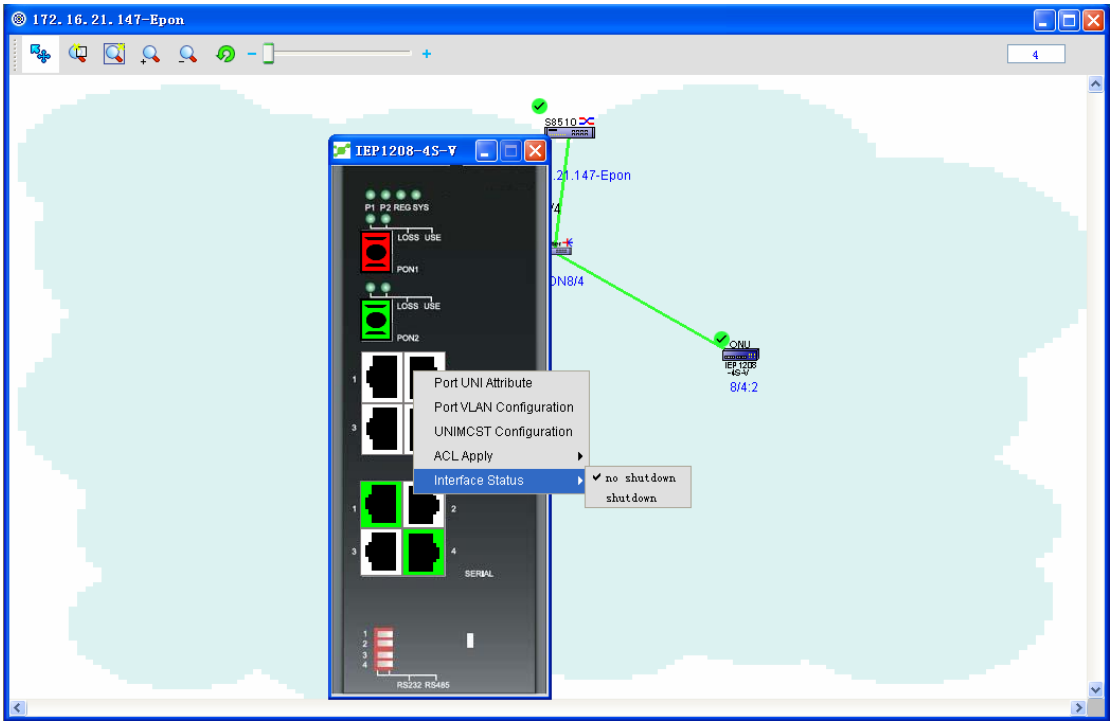
5.4.2 Changing the Status of a Common Port

Common ports here mean the GigaEthernet ports and the FastEthernet ports.
If you want to change the status of a common port, you should follow the following procedure:

Right click the ONU icon and select **Device's faceplate** and then right click **Common port** on the faceplate.See the following figure:

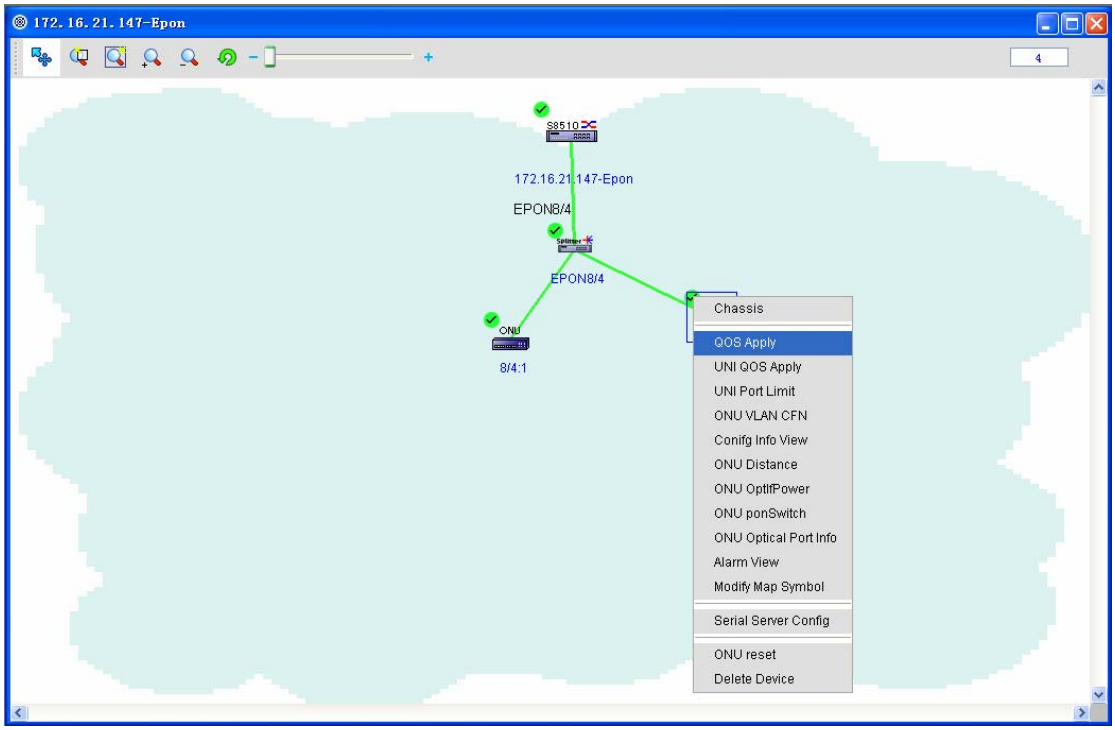


Click **Port’s status** and then select one of the two options: **shutdown** and **no shutdown**. The status of this port is changed.See the following figure:



5.4.3 QoS Application

In the topology, right click ONU. A menu appears, as shown in the following figure:



For more details, refer to "Applying QoS on the PON Port" and section 4.4.1 "Changing the Status of a Common Port."

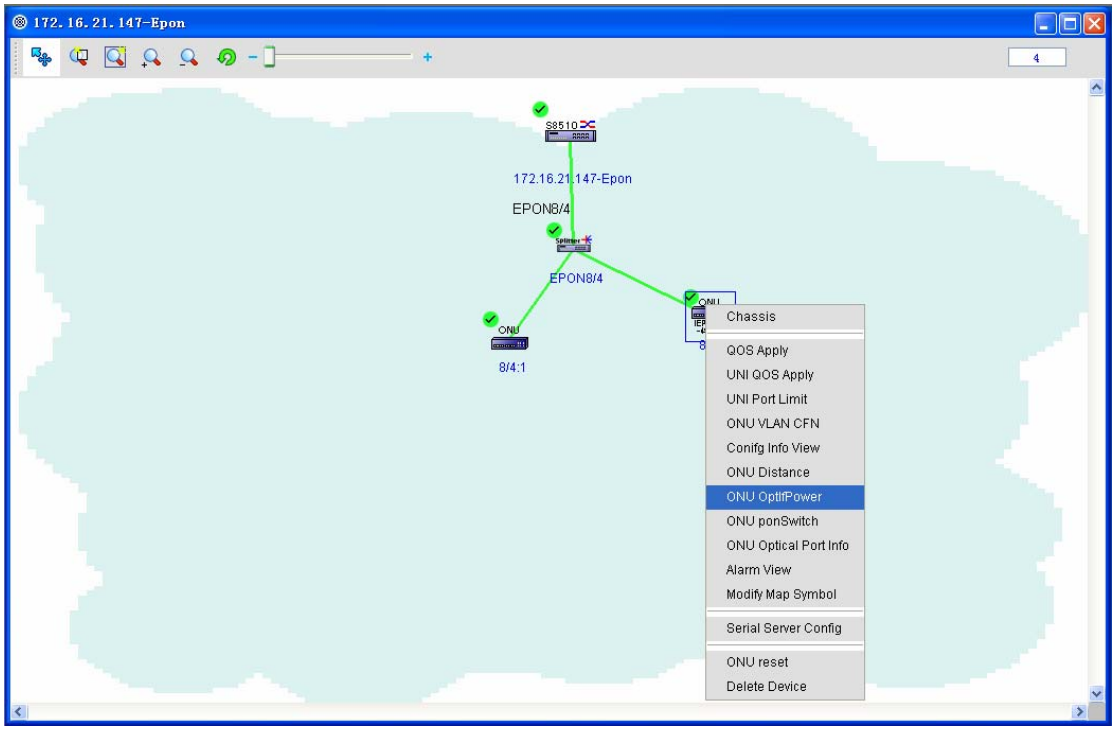
5.4.4 Optical Power Application

Due to the distance between devices and the transmission medium, the signal attenuates during transmission.

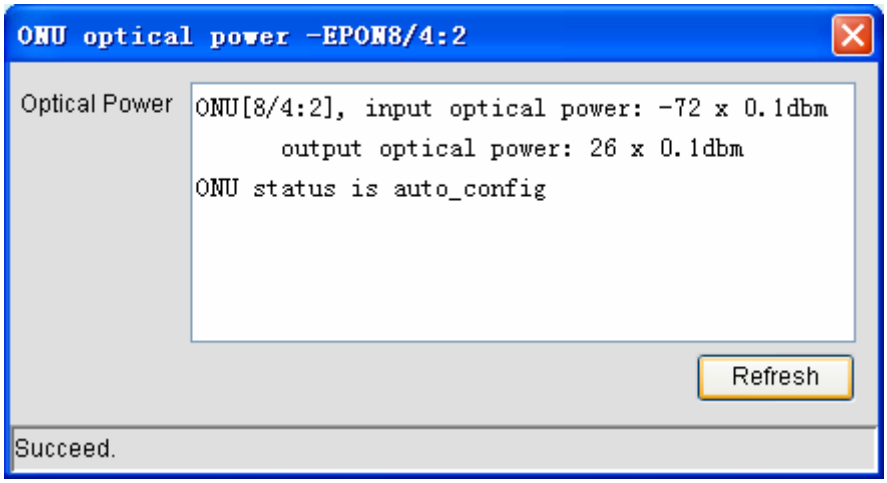
This function enables EPON NMS to browse the optical power of ONU.

The procedure is listed below:

1. Open NMS and right click the ONU icon in the EPON topology.See the following figure:

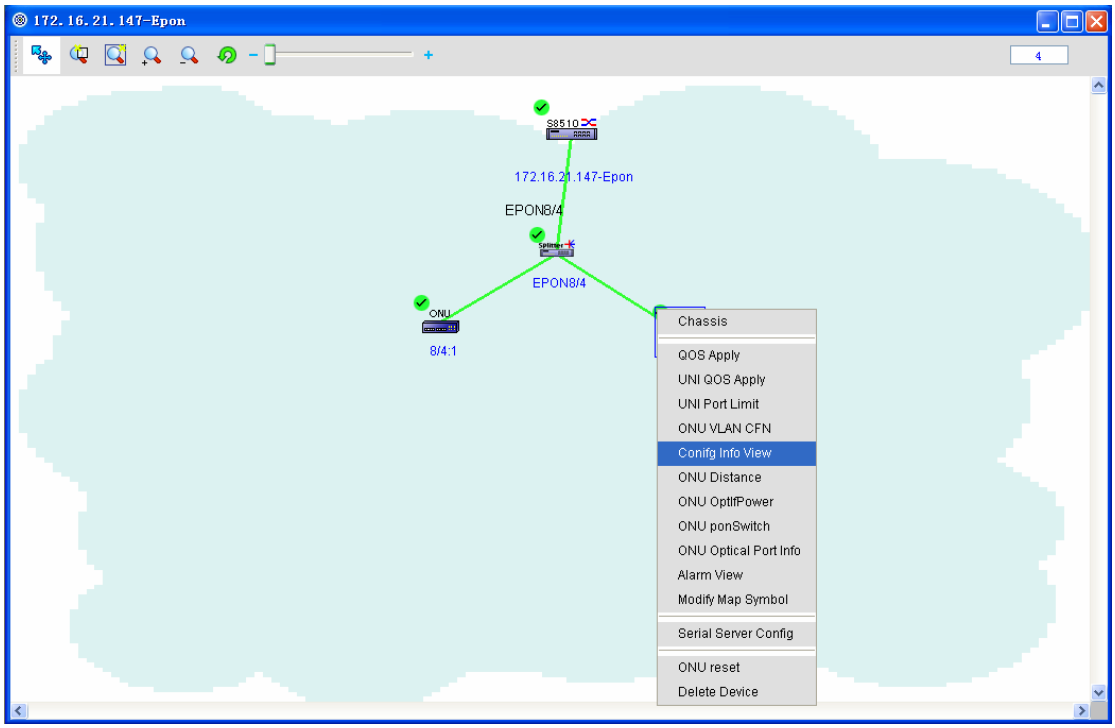


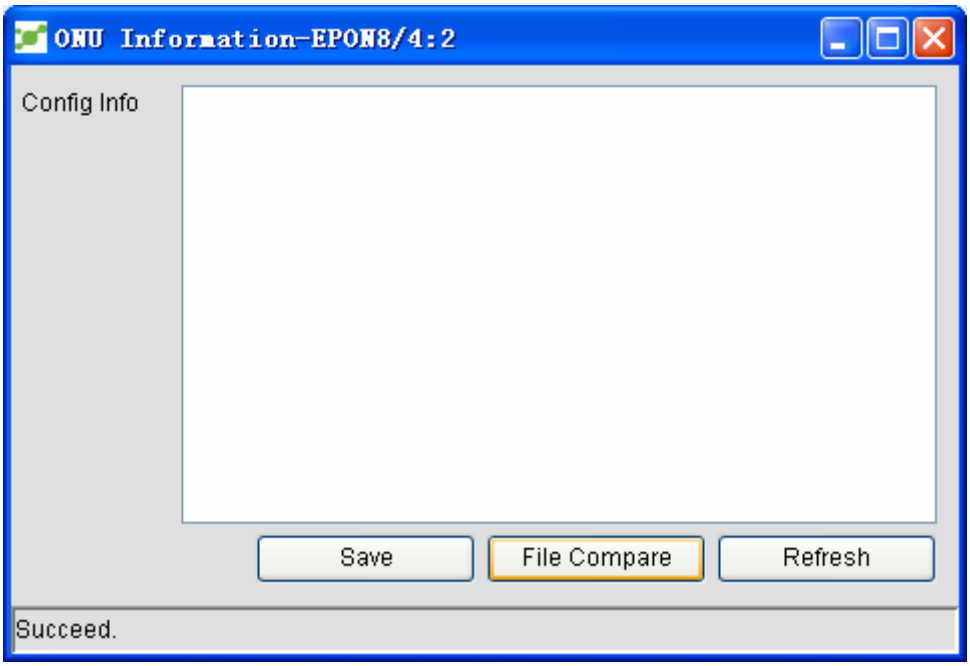
2. Select **Apply the optical power**. A page will appear to show the current optical power.See the following figure:



5.4.5 Browsing the Settings

Browsing the settings here means browsing the current ONU settings, saving the current settings to the local file, and comparing two ONUs' settings.Right click **Browse the settings**. A window appears, as shown in the following figure:





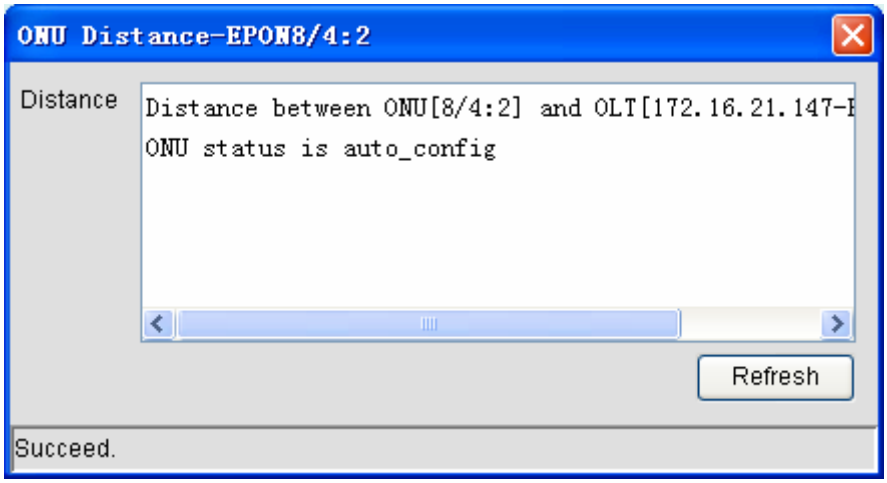
The **Save** button can be used to save the current ONU settings to the local file.

The **File compare** button can be used to open a comparision tool to check the settings of two

ONUs.

5.4.6 Distance Measurement of ONU

ONU distance measurement is to check the distance between ONU and the PON port.Right click ONU and then choose **ONU distance measurement**. A window appears, as shown in the following fiugre:

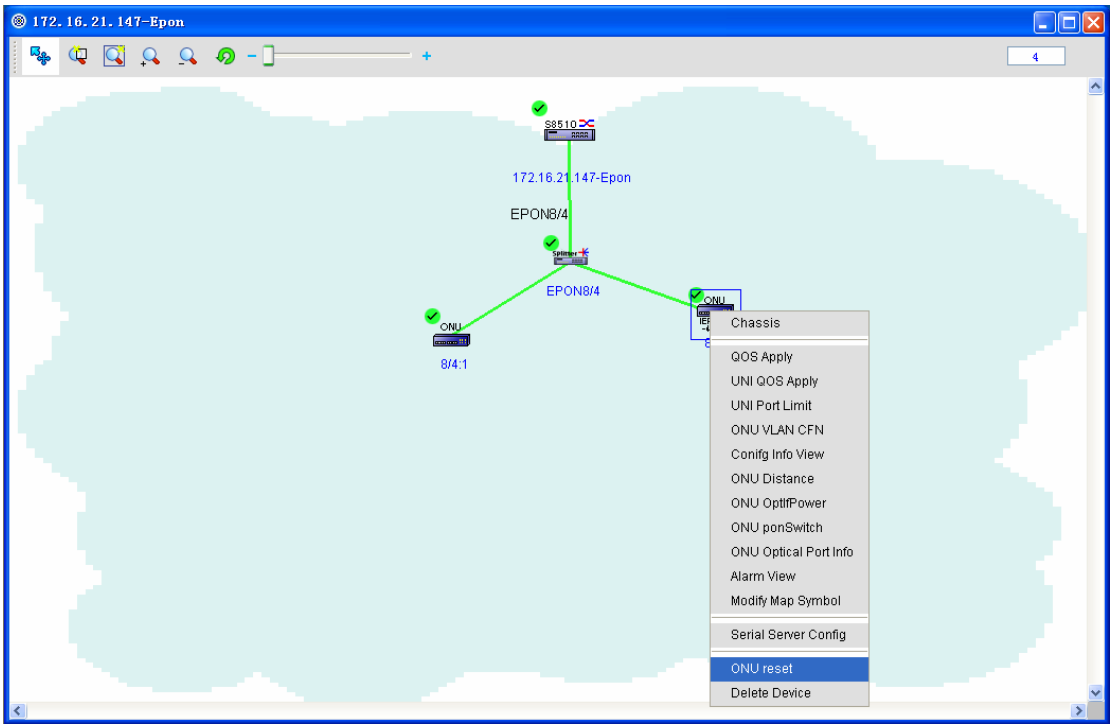


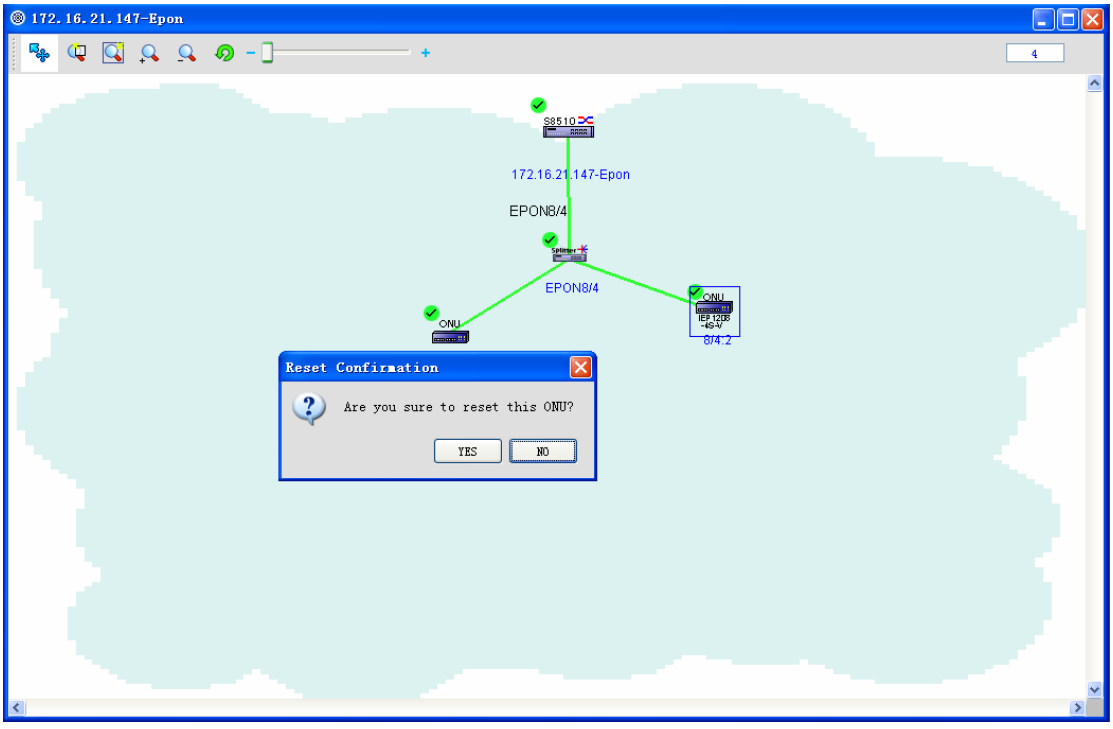
5.4.7 Browsing Alarms

Browsing alarms is similar to browsing OLT alarms. Please refer to browsing OLT alarms.

5.4.8 Rebooting ONU

Choose and right click an ONU icon and **Reboot ONU**. The **Reboot ONU** dialog box appears. If you choose **Yes**, this ONU will be restarted; if you choose **No** or close the dialog box, this ONU will not be restarted.See the following figure:



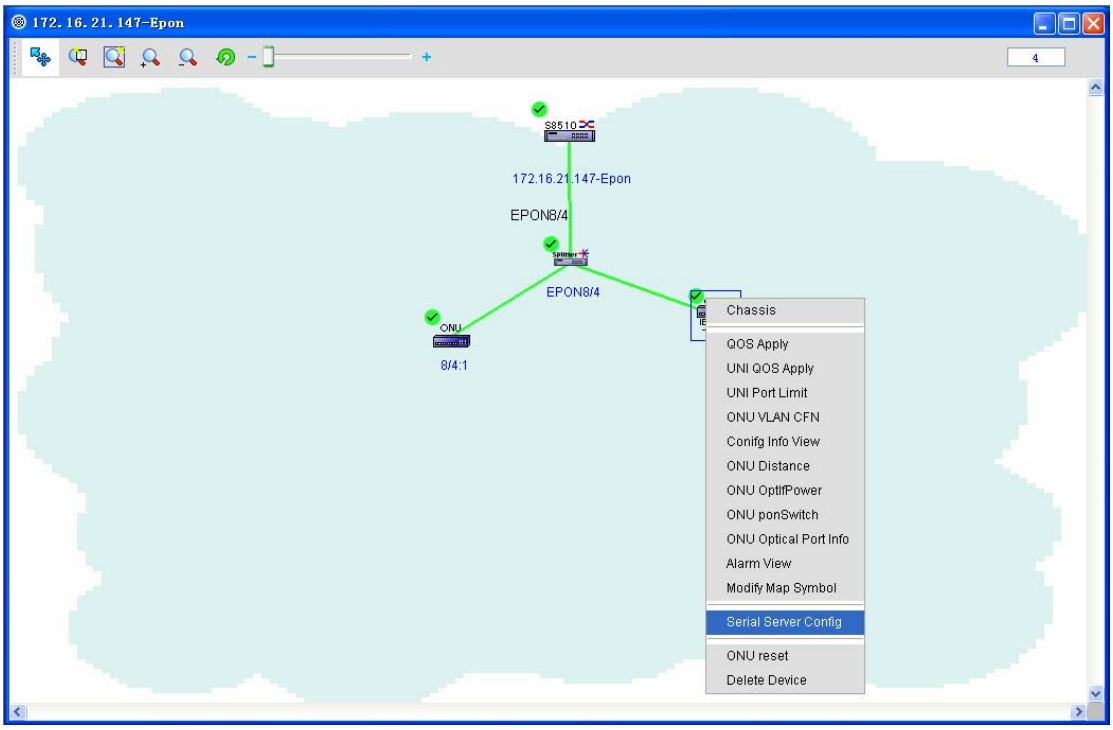


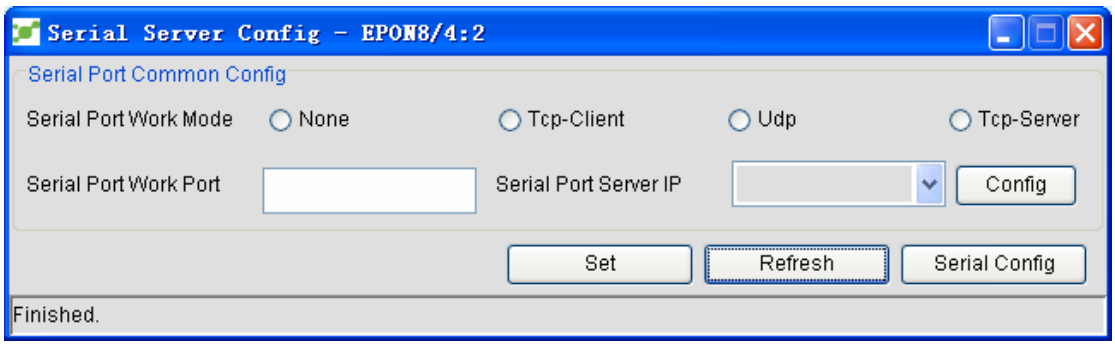
5.4.9 Setting the Serial-Interface Server

The settings of ONU serial-interface server includes setting global attributes of the serial interface and setting a single serial interface. The settings of a single serial interface includes setting its

basic attributes and the attributes of its data cache area, and loopback shutdown and enabling.

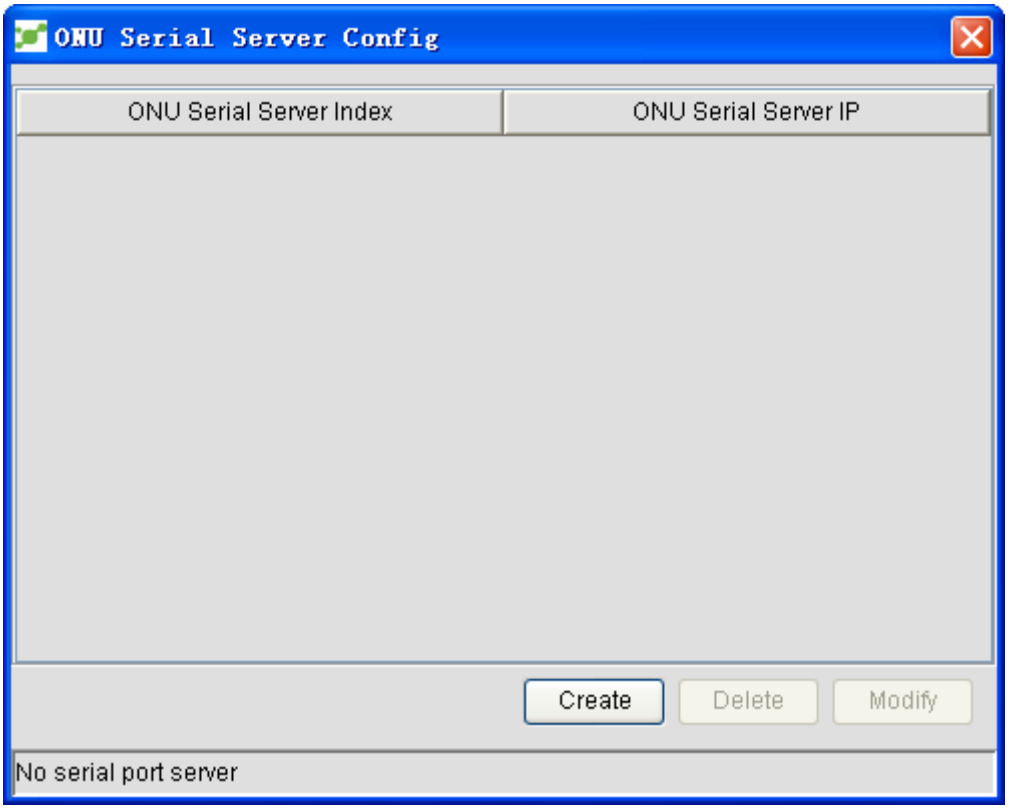
Right click ONU with the serial interface and select **Set the serial interface server**. The following window appears:



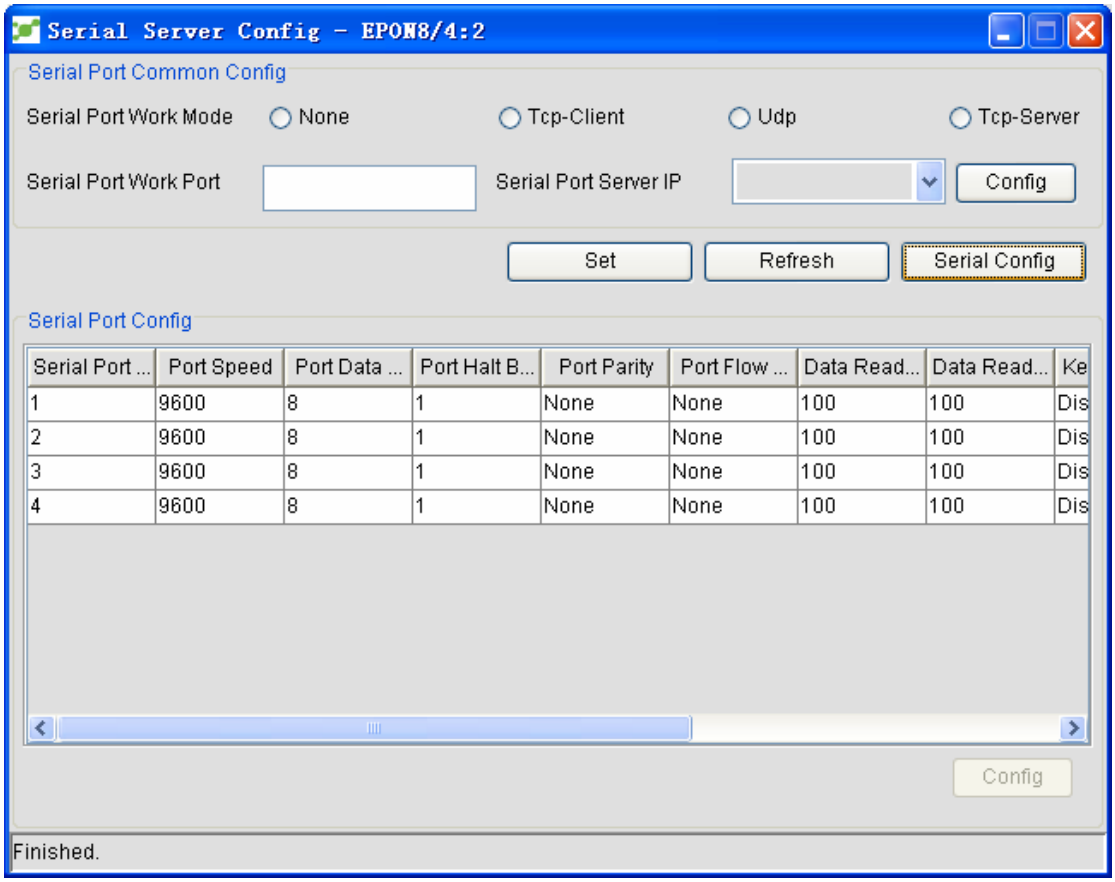


The **Setup** button is to distribute the modified options to ONU.

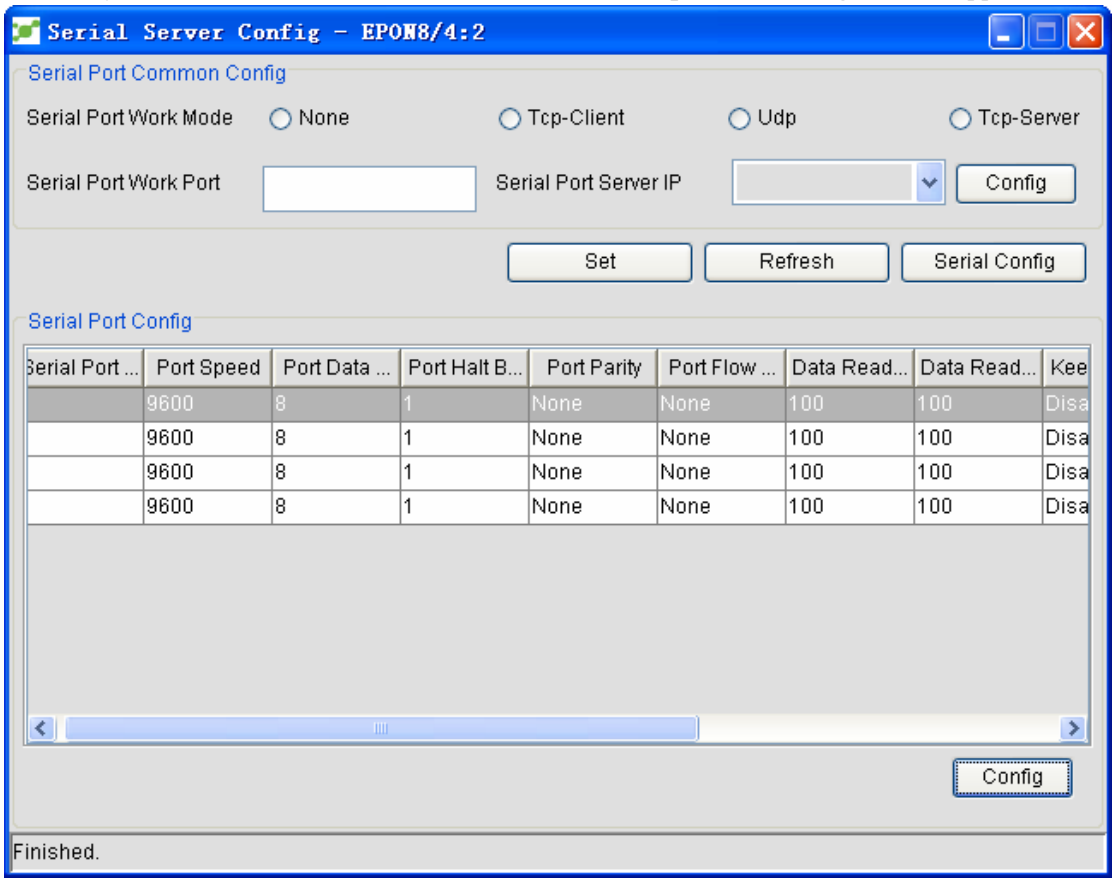
Click **Setup**. The **Set the serial interface's address** window appears, as shown in the following figure:

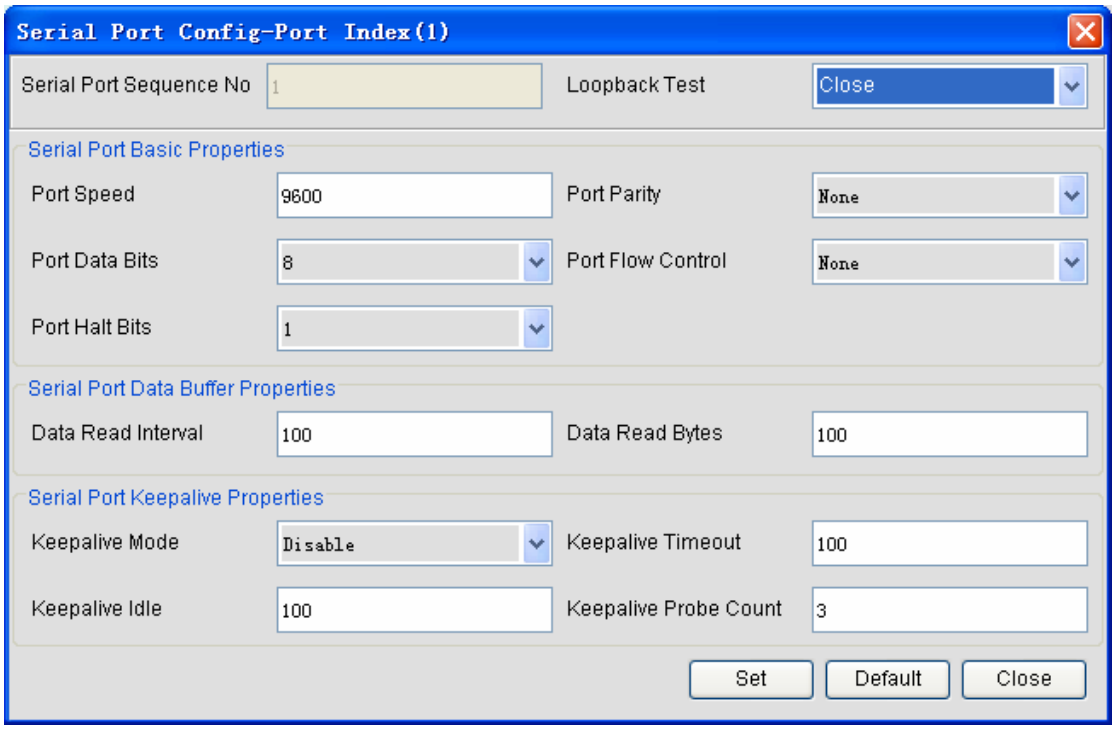


In the window above, you can add, delete and modify the address of the serial interface of ONU. Click **Set the serial interface**. A dialog box appears, as shown in the following figure:



The serial interface settings shown in the figure above is for the settings of each serial interface of ONU. If you select a random serial interface and click **Setup**, the following window appears:

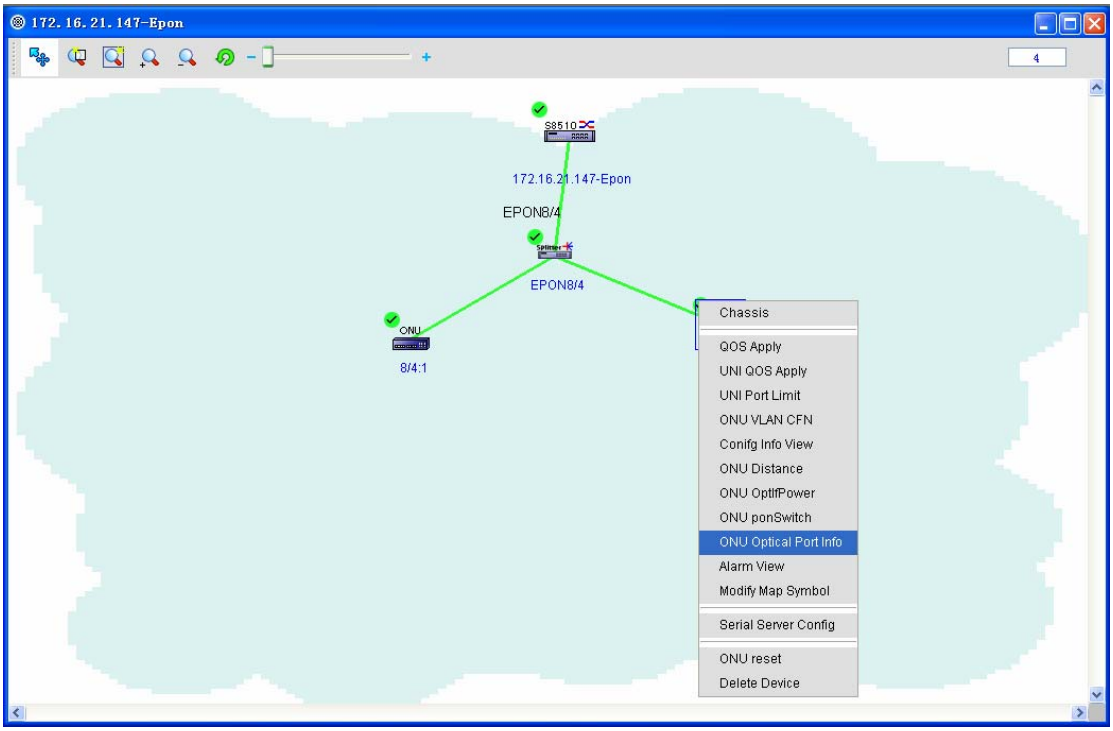


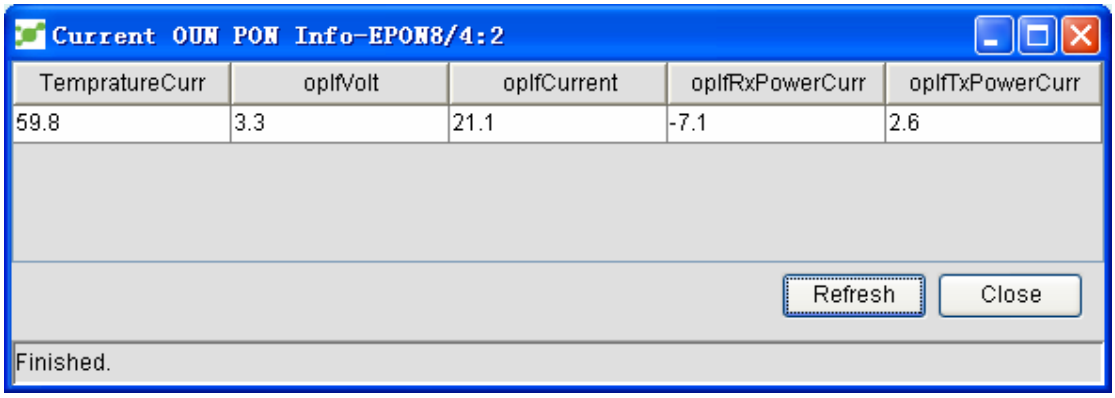


5.4.10 Information About Optical Modules of the PON Port

Open NMS.

Right click ONU and click **Info about optical modules of the PON port**. The following figure appears:

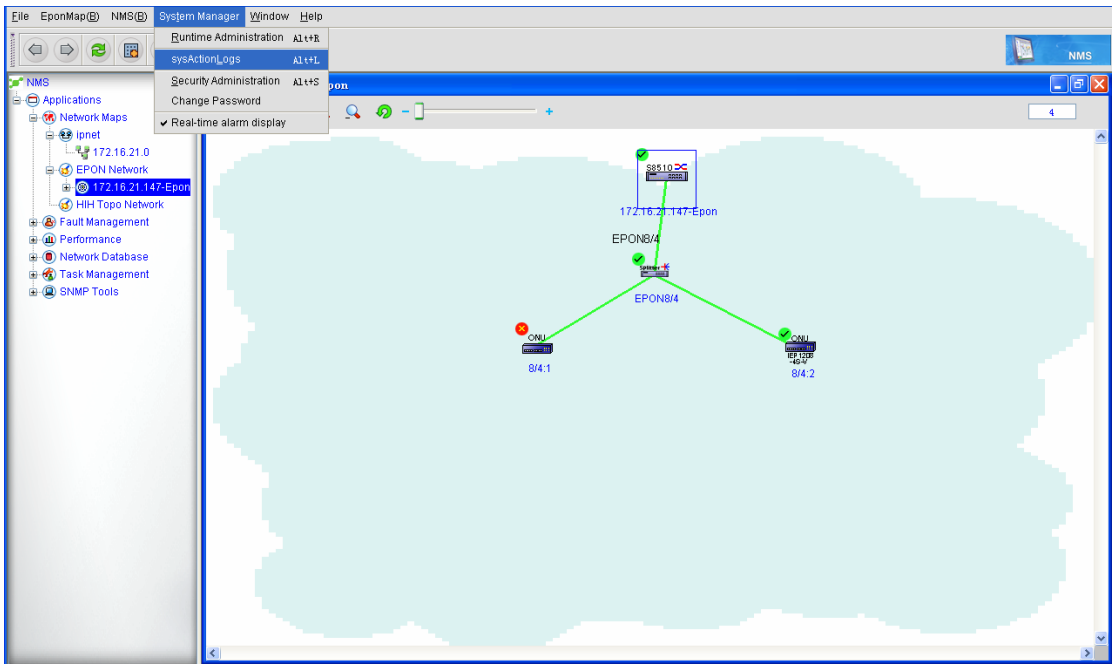


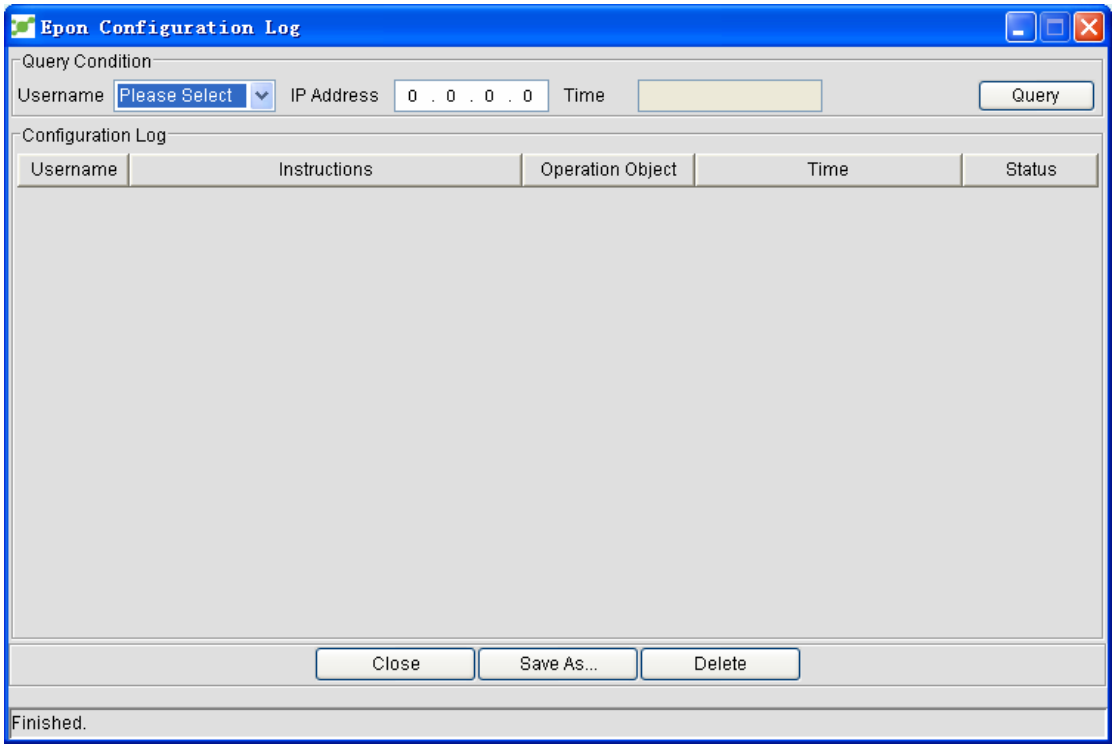


5.5 Operation Log

The system will record all kinds of operations done by users.

Click **System Management -> Operation log**. The following page appears:





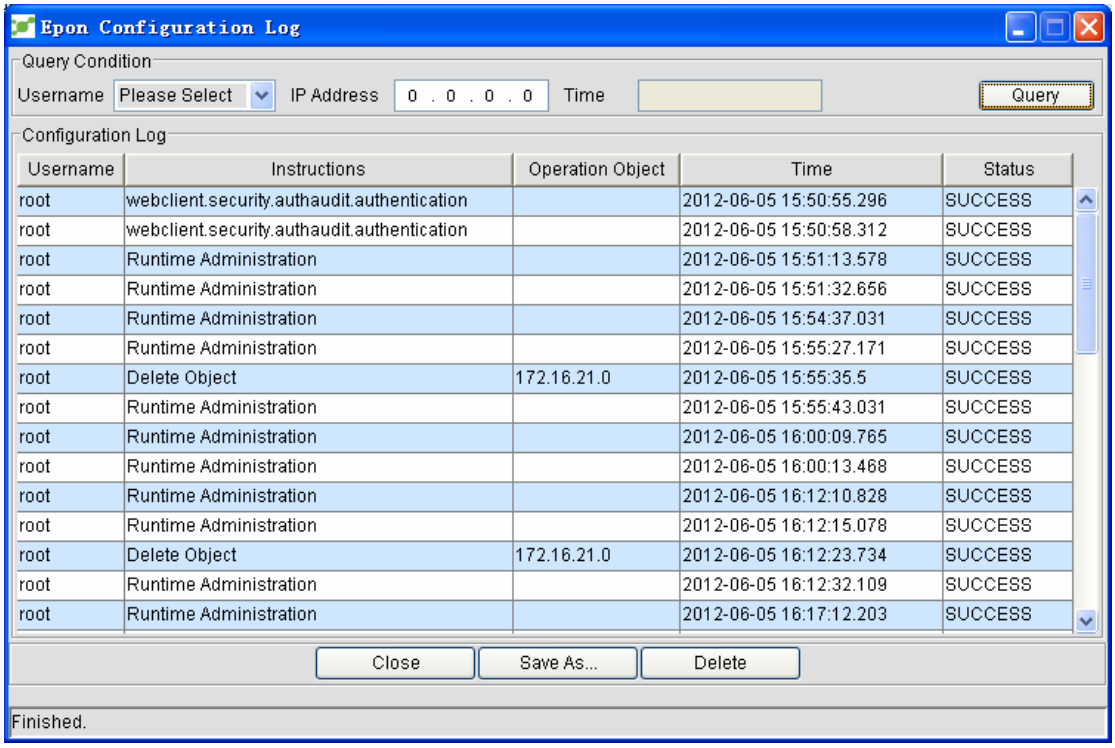
Query conditions:

1. Administrator: the login name of the administrator will be displayed in this option.

2. IP address: it means the IP address of a device. It can be used to query the to-be-operated device. You can enter no parameter here, which means a lot of operation logs will be displayed.

3. Time: It is for you to select the time of recording logs.If you enter no time, all logs will be queried.

After all the above-mentioned parameters are set, you can click **Query**. The results are shown, as shown in the following figure:



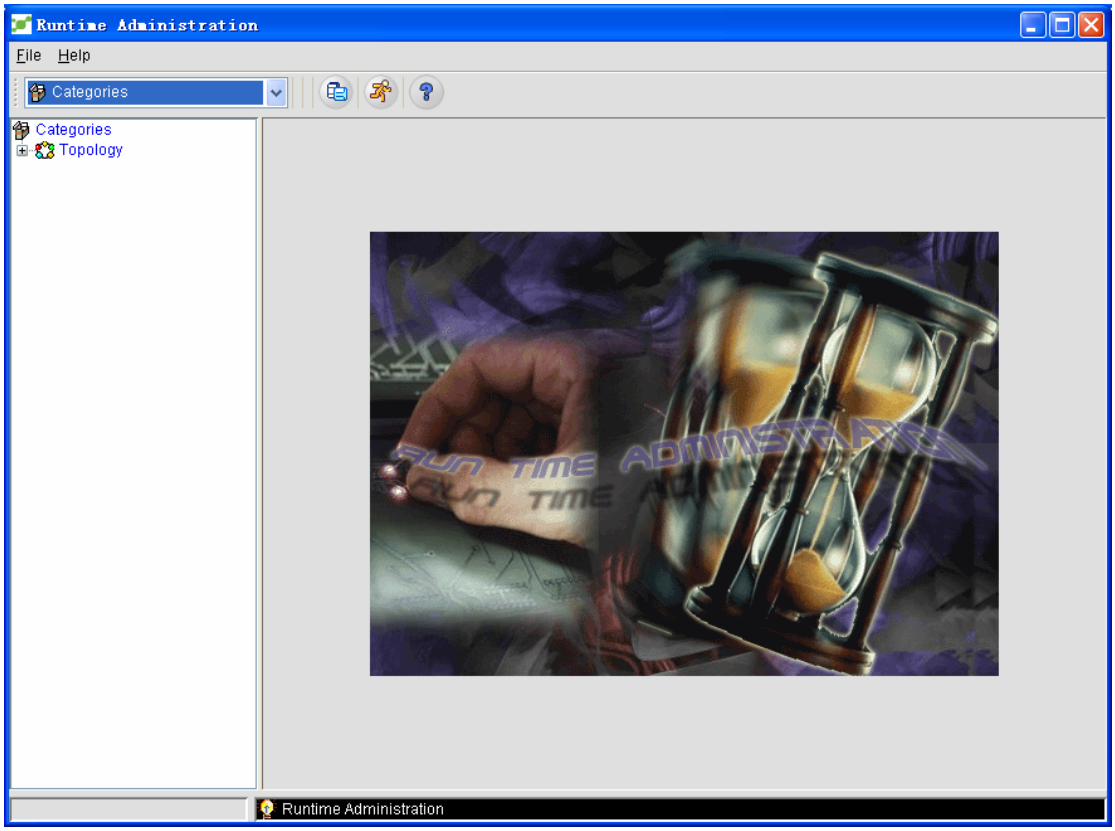
In the **Status** column, the operation results are shown. **SUCCESS** means this operation is successful and **FAILURE** means this operation fails. If you select a row and then click **Delete**, the selected record will be deleted.

5.6 Device Discovery and Log Deletion

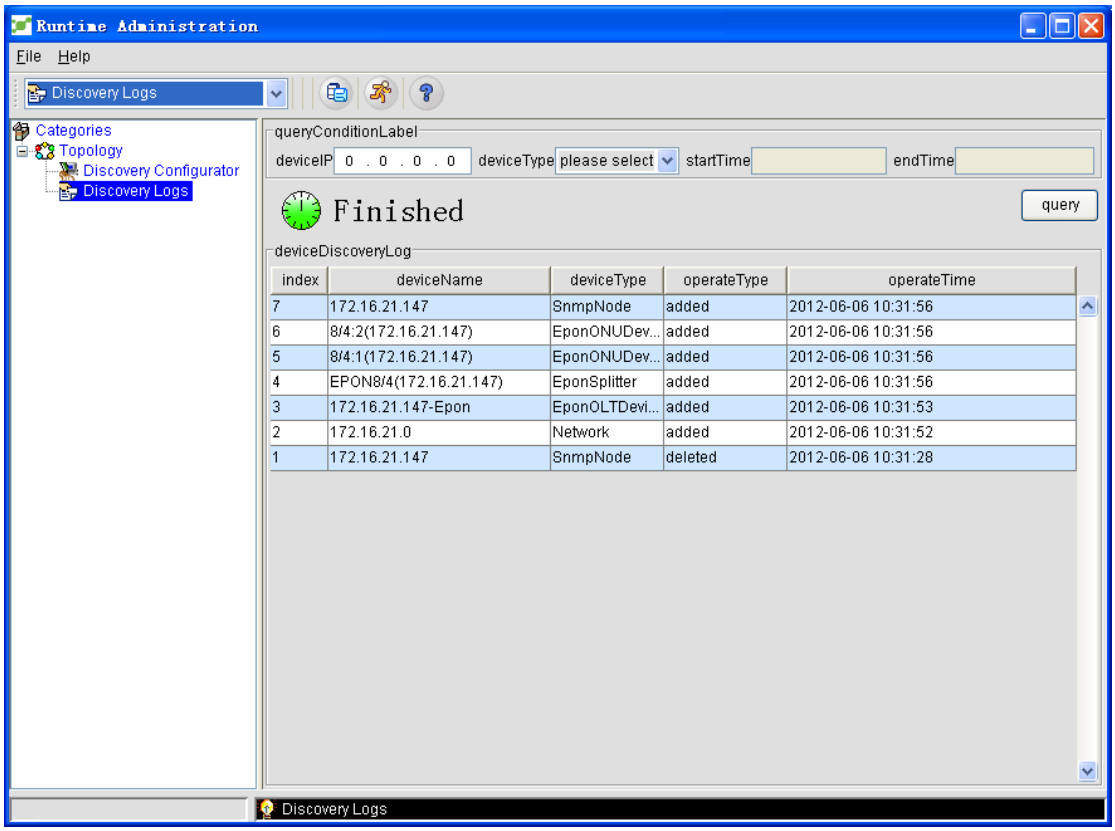
This function is to discover and delete the devices in the system, record the related operations and browse the operation status of the system.

The procedure is listed below:

1. Click **NMS -> System Management -> Real-Time Management**. See the following figure:



2. Unfold the **Topology** node and select **Device discovery log**.See the following figure:

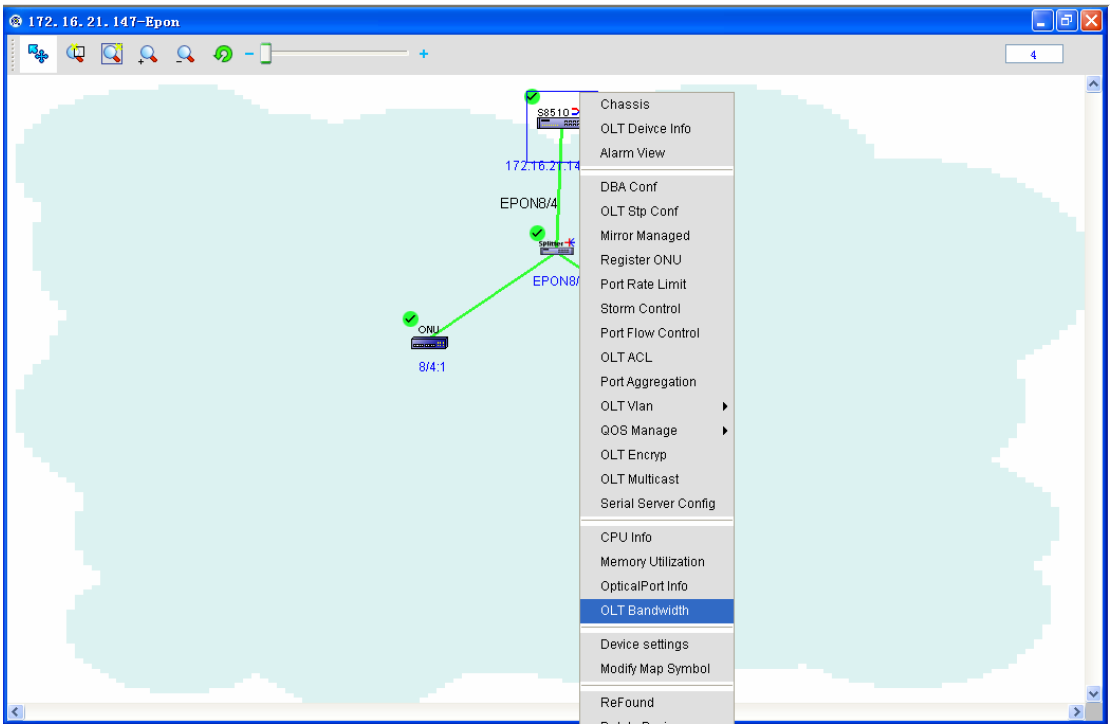


Different from figure 4 and figure 8, this figure shows the device type: Node, NetWork, EPONONUDevice and EPONSplitter. The default device type is null.

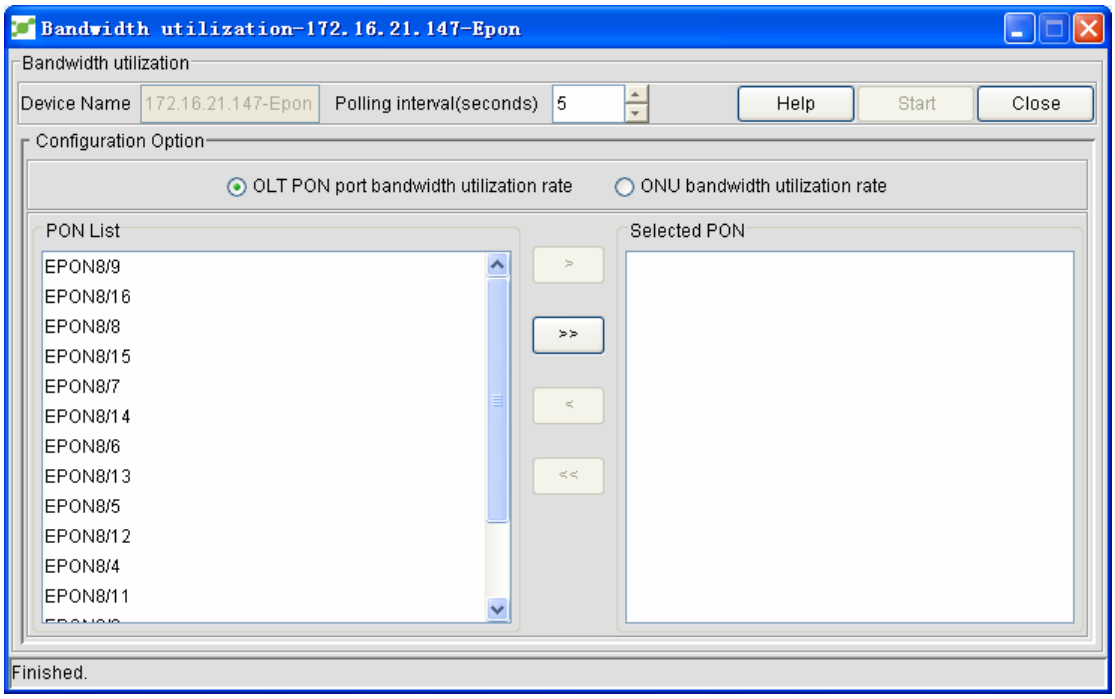
5.7 Bandwidth Usage

Bandwidth usage is designed for monitoring the bandwidth occupancy of a device.The administrator can browse the bandwidth usage of a device so that he or she can regulate the bandwidth and make full use of network resources.The specific operation is shown below:

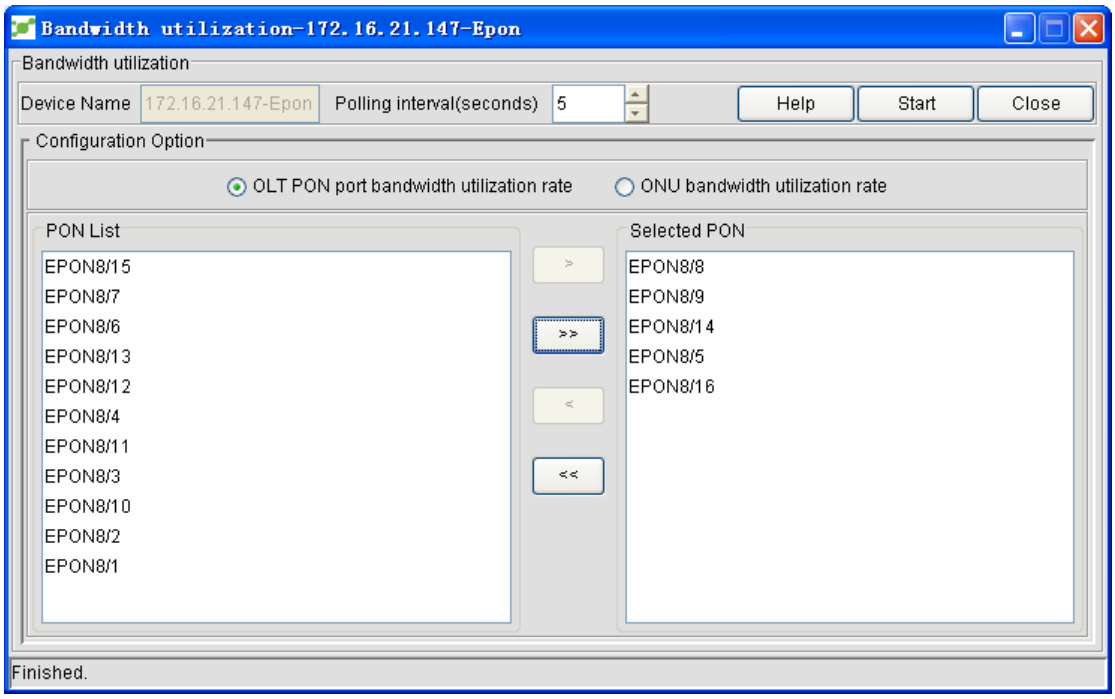
1. Select OLT and right click it.See the following figure:



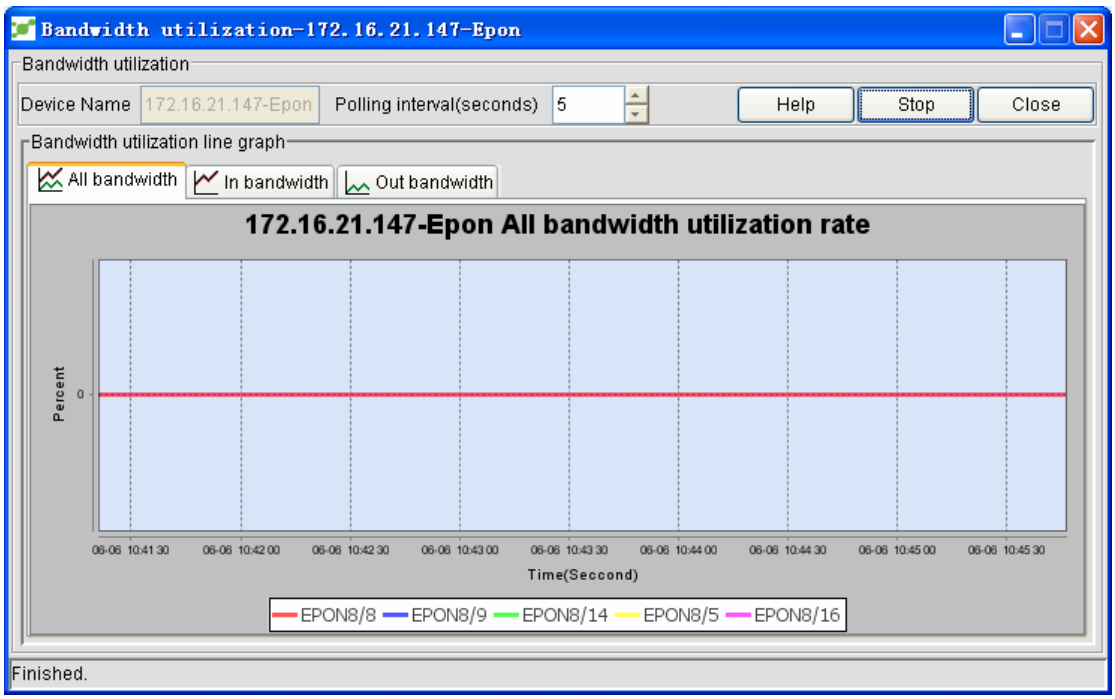
2. Click **Bandwidth usage**, as shown in the following figure:



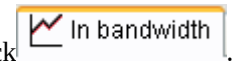
3. Set the polling interval (default interval: 5s), select a port, and click > to add this port to the monitor list or click >> to add all ports to the monitor list.See the following figure:



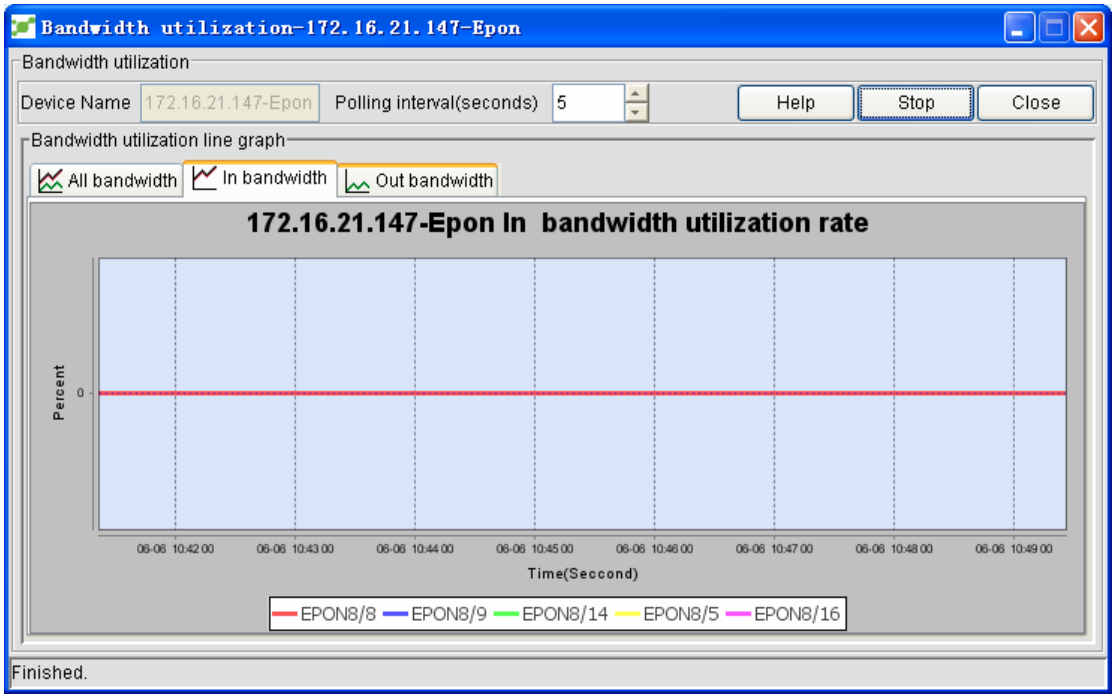
4. Click **Start**. The selected ports will be monitored.See the following figure:



By default, the total bandwidth usage is displayed.Here, you can browse the incoming bandwidth usage and the outgoing bandwidth usage.You just need to click the corresponding tab.For example,

if you want to browse the bandwidth usage, click 

. See the following figure:



6 Fault Management

If you can browse the information about corresponding trouble, it will be much convenient for network management.The administrator can locate the troubled devices and the reasons and make a rapid troubleshooting according to the information of network troubles.

This section gives a detailed description of alarm levels:

Alarms can be classified into five levels:

Critical，**Major**，**Warning**，**Info**，**Clear**

Critical: it refers those dangerous alarms which are shown in red, such as device's trouble or the disconnection of an interface.

Major: It means those serious alarms which are in yellow, such as node's trouble.

Warning: It refers to those general alarms not related with the device's troubles. These alarms are shown in blue.

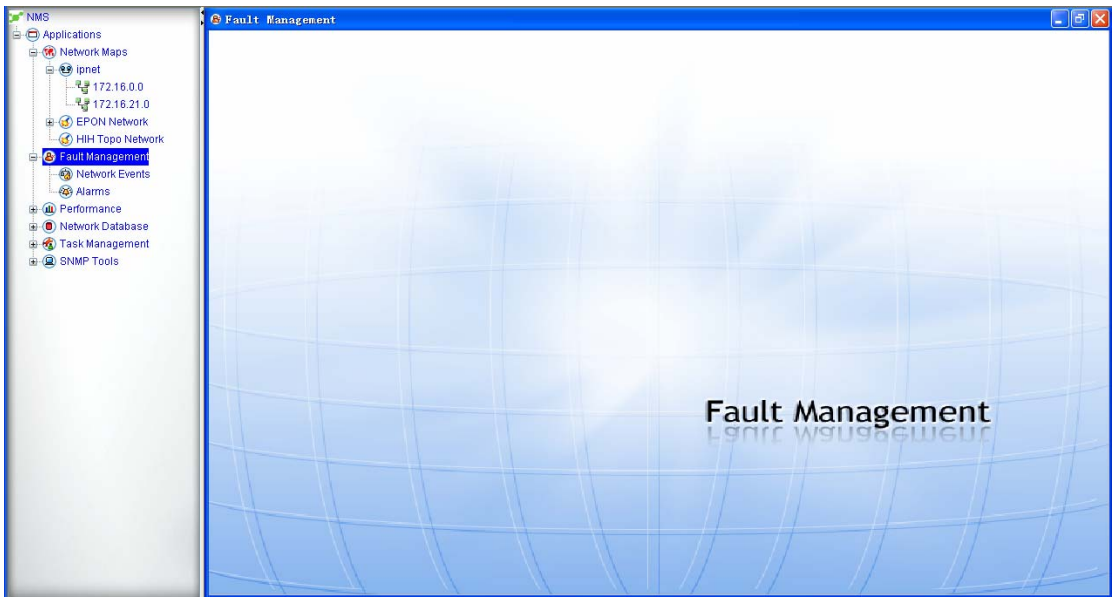
Info: it refers to the general information, such as general network events.They are not shown in color.

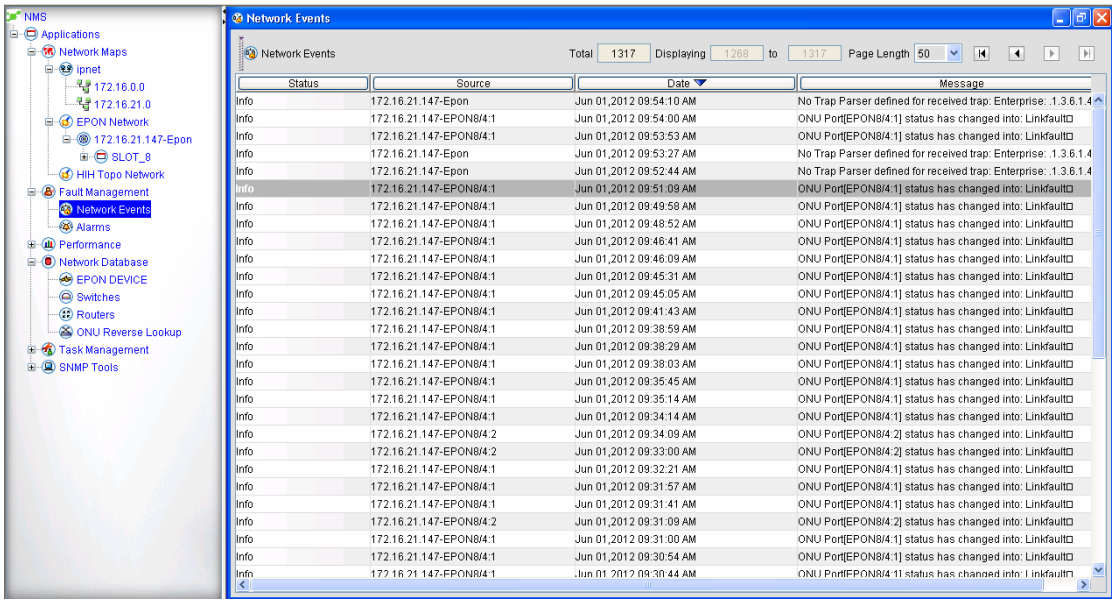
Clear: It refers to clear-away alarms. When **Critical** or **Major** appears and the status gets normal again, a clear-away alarm will be generated, marking that the device has already got rid of alarm and functioned normally again.This kind of alarms are shown in green.

NMS provides the administrator detailed information, including network events and alarms.

6.1 Network Events

Network events list all information about status changes of all managed devices, such as node trouble, node recovery, port status change, failed polling and management information of NMS platform.Click **Network events**. The following page appears:



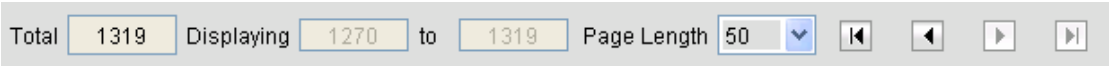


The above-mentioned list shows all network events.The following are some explanations about the above-mentioned list:

- Status: It stands for the alarm types: critical, major, clear and info. For more information, see their definitions.
- Source: It represents the device or the port on which a network event occurs.
- Date: It refers to the specific time when a network event occurs.
- Info: It represents the detailed explanation of an event.

If you double click a column in the list, you can make ordering of this list. For example, if you double click the **Date** column, the content in the list will be sequenced according to time.

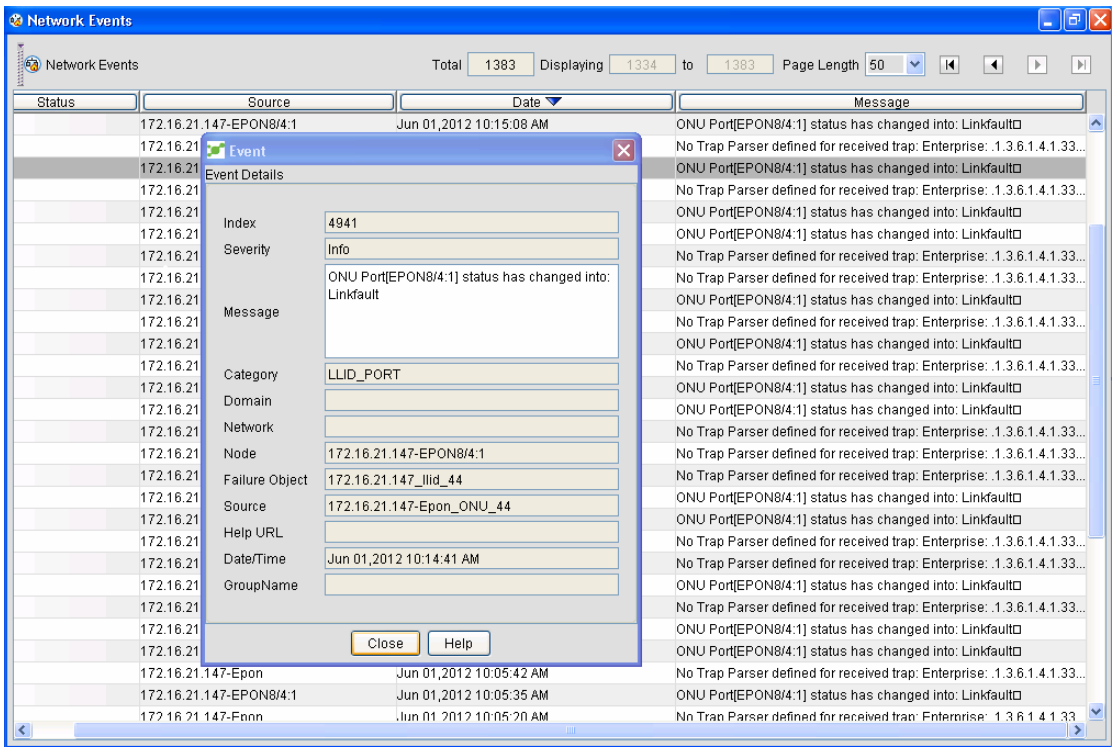
In order to browse the information conveniently, you can add related "show" operations on the right top of the list, as shown in the following figure:



Total: It shows the total number of all events. 

: You can designate the range of displayed events. Page length: It represents the number of events displayed in every page.  : They stand for the page-turn button.

If you double click an event, the following page appears:

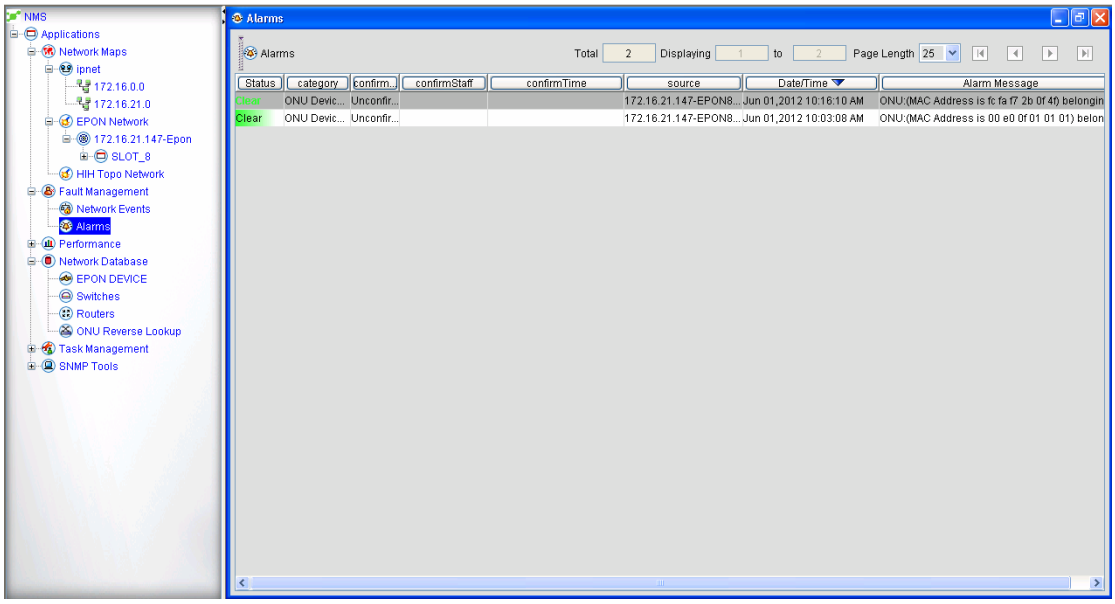


The above-mentioned page shows the detailed information about this event.

6.2 Network Alarms

Network alarms record the alarms of a device and provide solutions for related alarms, including the alarm notifications and alarm confirmations.

Click **Network alarms**. The **Network alarms** page appears, as shown in the following figure:

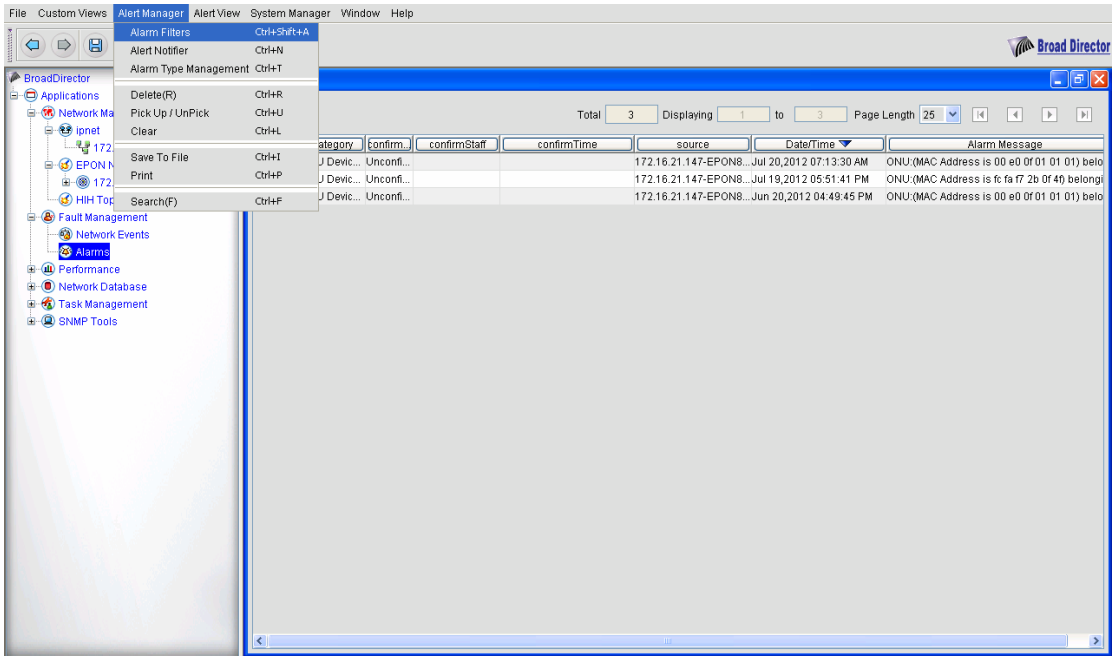


6.2.1 Alarm Notification

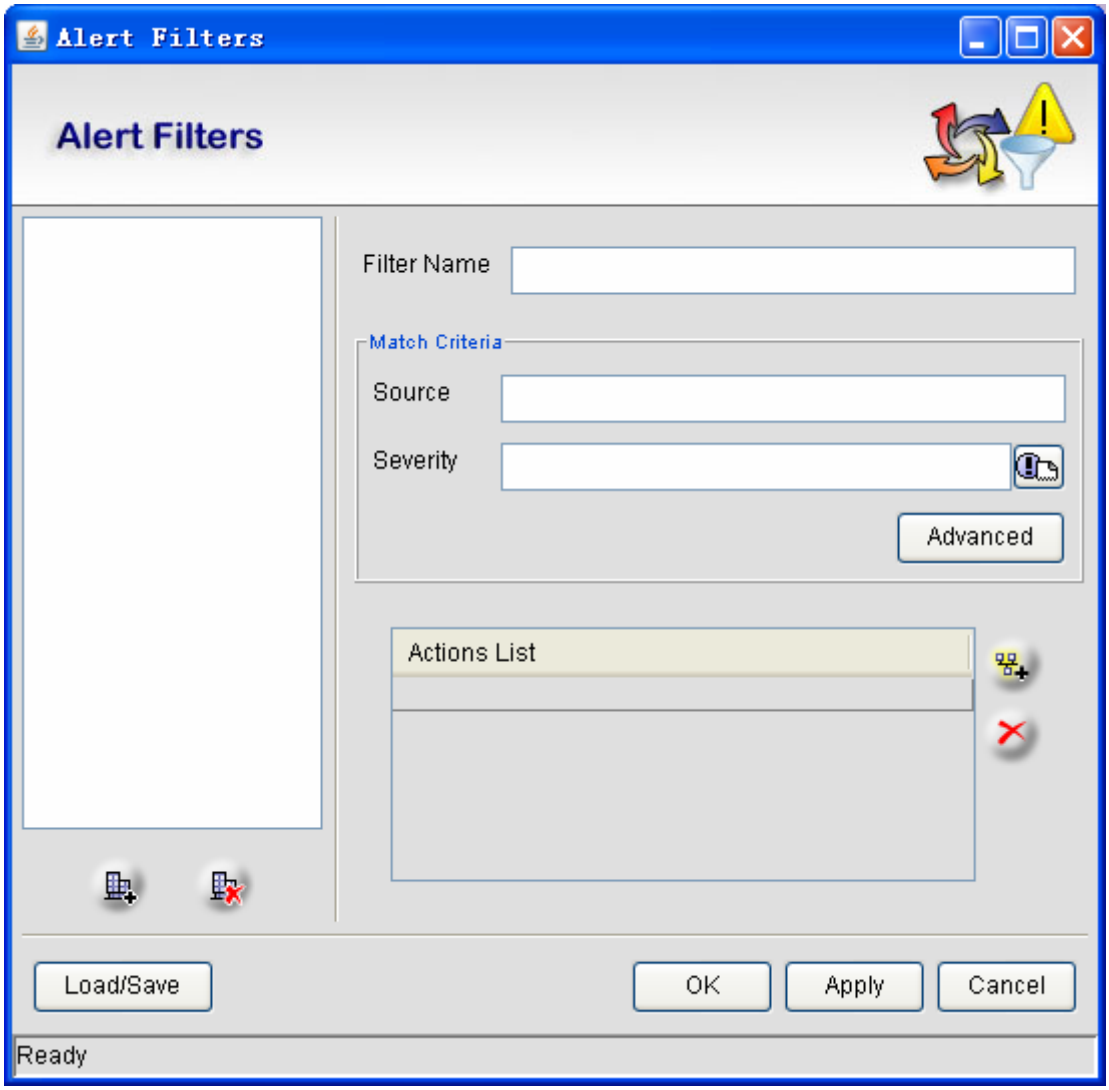
The alarm notification is added so that the administrator can know the network alarms on time. The alarm notification includes action limit, command running and E-mail generating.

6.2.1.1 Adding the alarm notification

Click **Network Alarms -> alarm management -> Set alarm notification**.See the following figure:



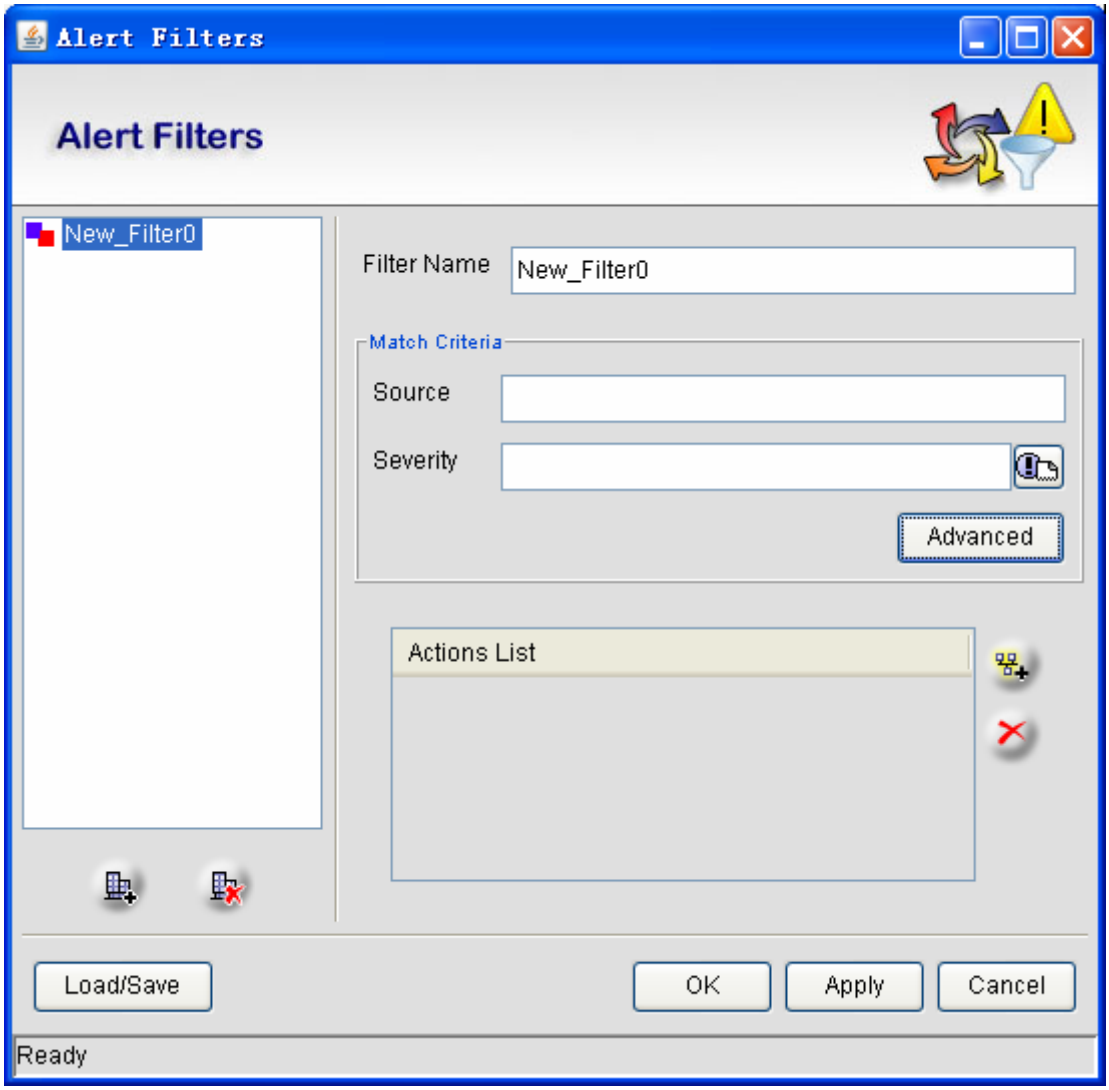
Click **Set alarm notification**:



The alarm notification settings consists of two parts: one part is to set the matchup conditions of the alarm notification, and the other part is to set the action of the alarm notification.Before the alarm notification settings, you shall set **Alarm Filter and Matchup Standard**, and then **Action**.

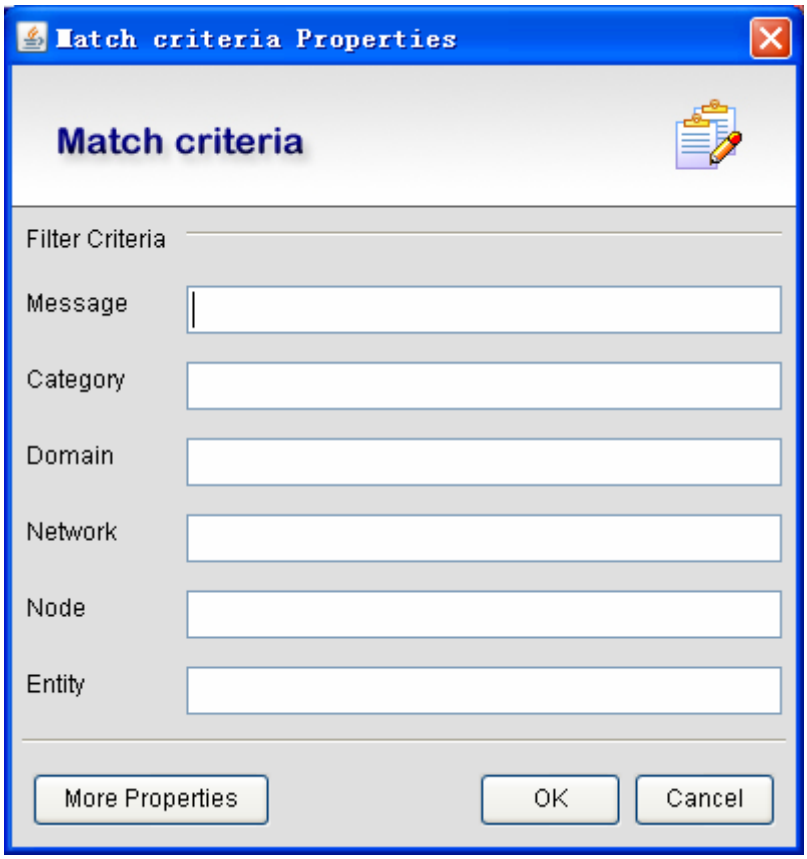
Note: The **Alarm Notification** menu is  and the **Alarm Notification's Action** menu is  .

Click **Add**  **.** The page is available for entering information, as shown in the following figure:

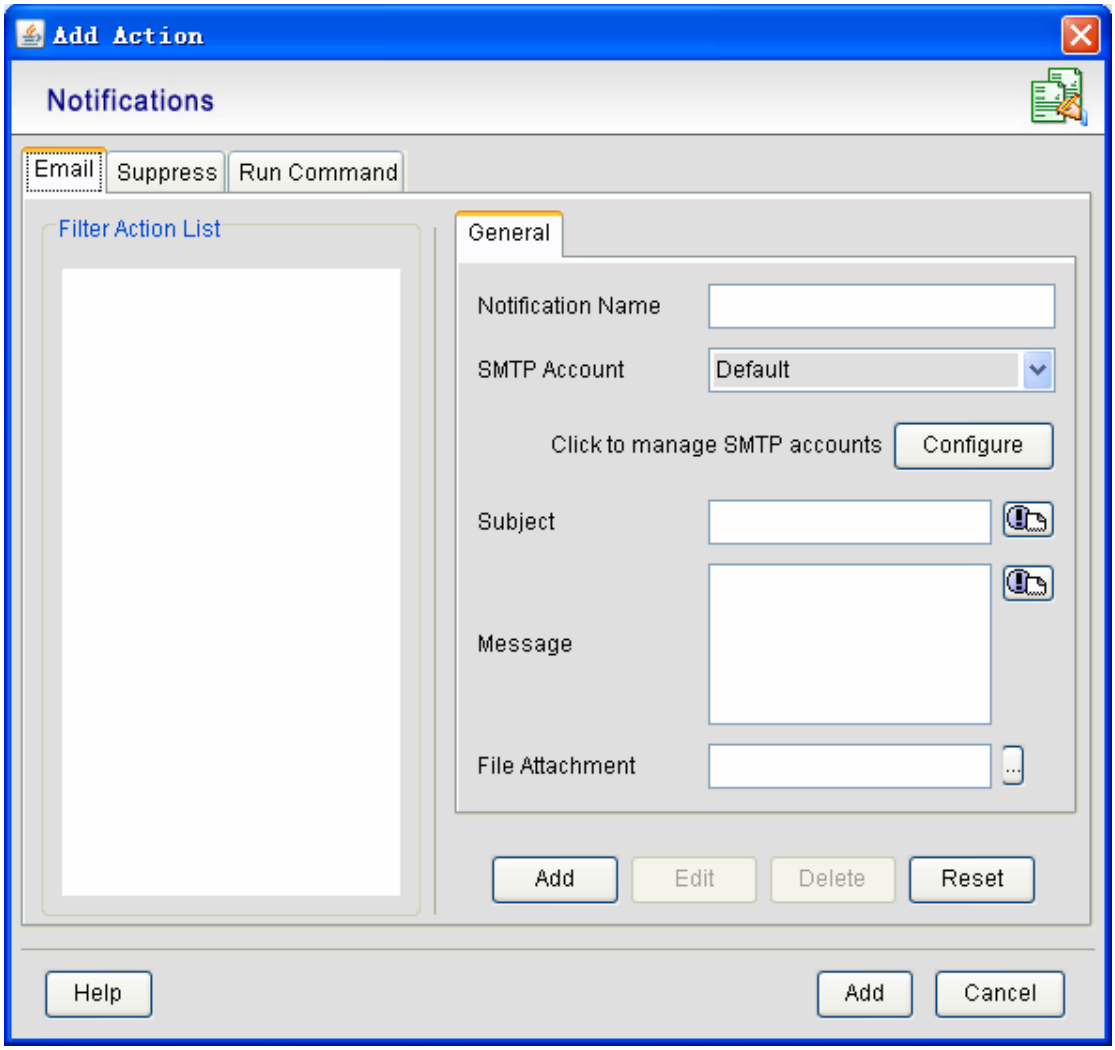


The parameters in the above-mentioned figure are explained below:

- Filter's name: It stands for the name of the alarm notification.
- **Alarm source: It shows on which device the alarm occurs.It is equivalent to the filtration condition of alarms.**
- **Importance: There are five options (Critical, Major, Minor, Warning, Clear), which correspond to different alarm levels.It is equivalent to the alarm filter.**
- **Advanced: If you click it, a page will appear for you to define the filtration conditions of alarms.See the following figure:**



After the above-mentioned parameters are selected, you can click  . The following window appears:



On this step, the alarm notification settings is done. Nextly you need to set **Trigger of alarm notification action**.**There are three options on the above-mentioned figure: E-mail, limit, and execute the command.The following are their explanations:**

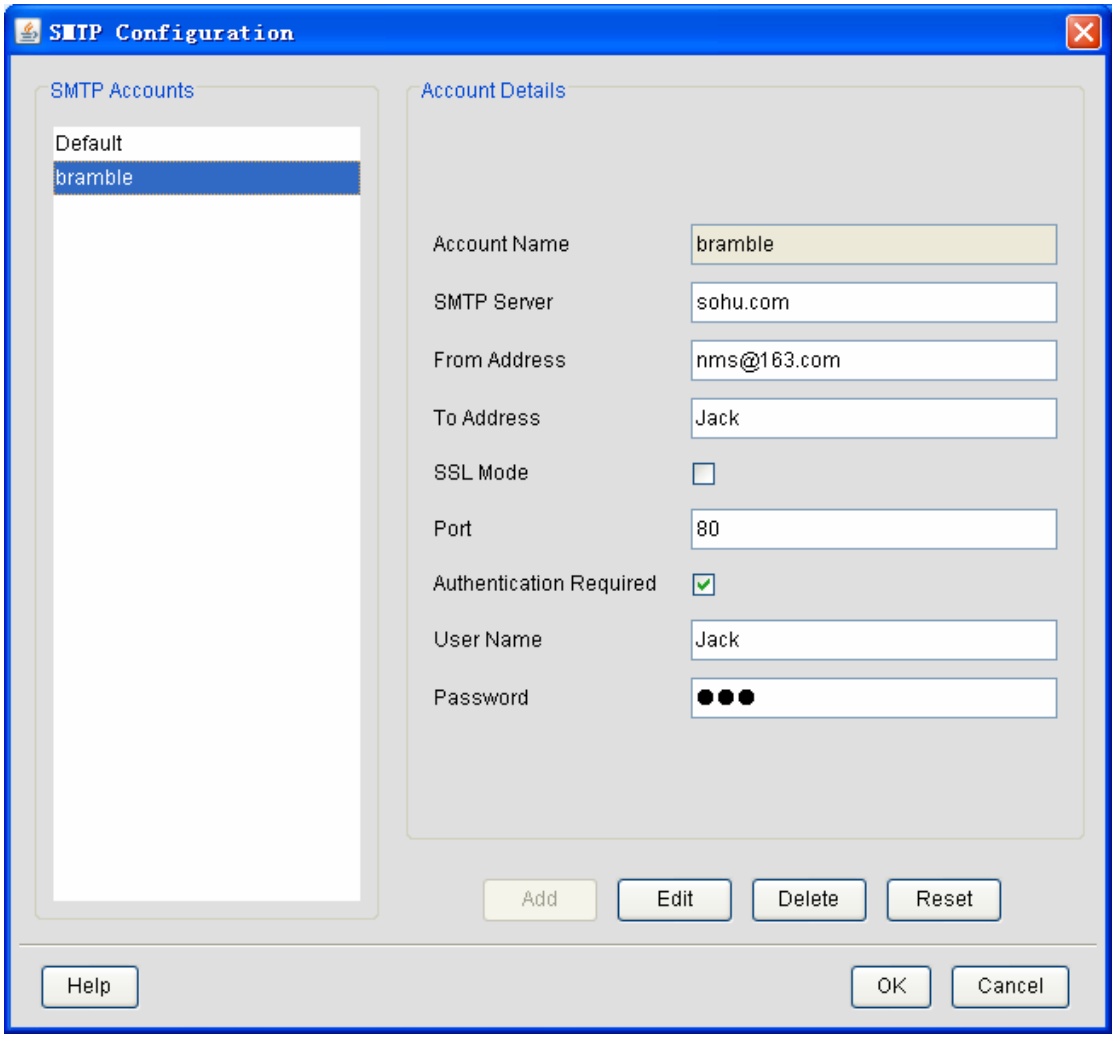
- **E-Mail:**
  If you click **E-Mail**, the figure above appears.

The following are explanations of five parameters on the above-mentioned figure:

A. Notification's name: It is the unique name for action trigger, consisting of letter, number and underline.

B. SMTP account: It stands for the information about the SMTP account which sends E-mail. You shall click 

to add, delete or modify the corresponding SMTP account, as shown in the following figure:



- **Account's name: It is a unique name of the SMTP account.**
- **SMTP server: It is the address of the SMTP server.**
- **Sender: It means the address of mail transmission.**
- **Receiver's address: It means the address of the mail receiver.**
- **SSL mode: It means whether to conduct SSL encryption.**
- **Port: It stands for the ID of the mail transmission port.**
- **Checkup: It means whether this E-mail needs checkup.**
- **Username: It means the user name in the E-mail server.**
- **Password: It means the password which corresponds to the user name in the E-mail server.**

C. **Subject: It means the subject of E-mail.**

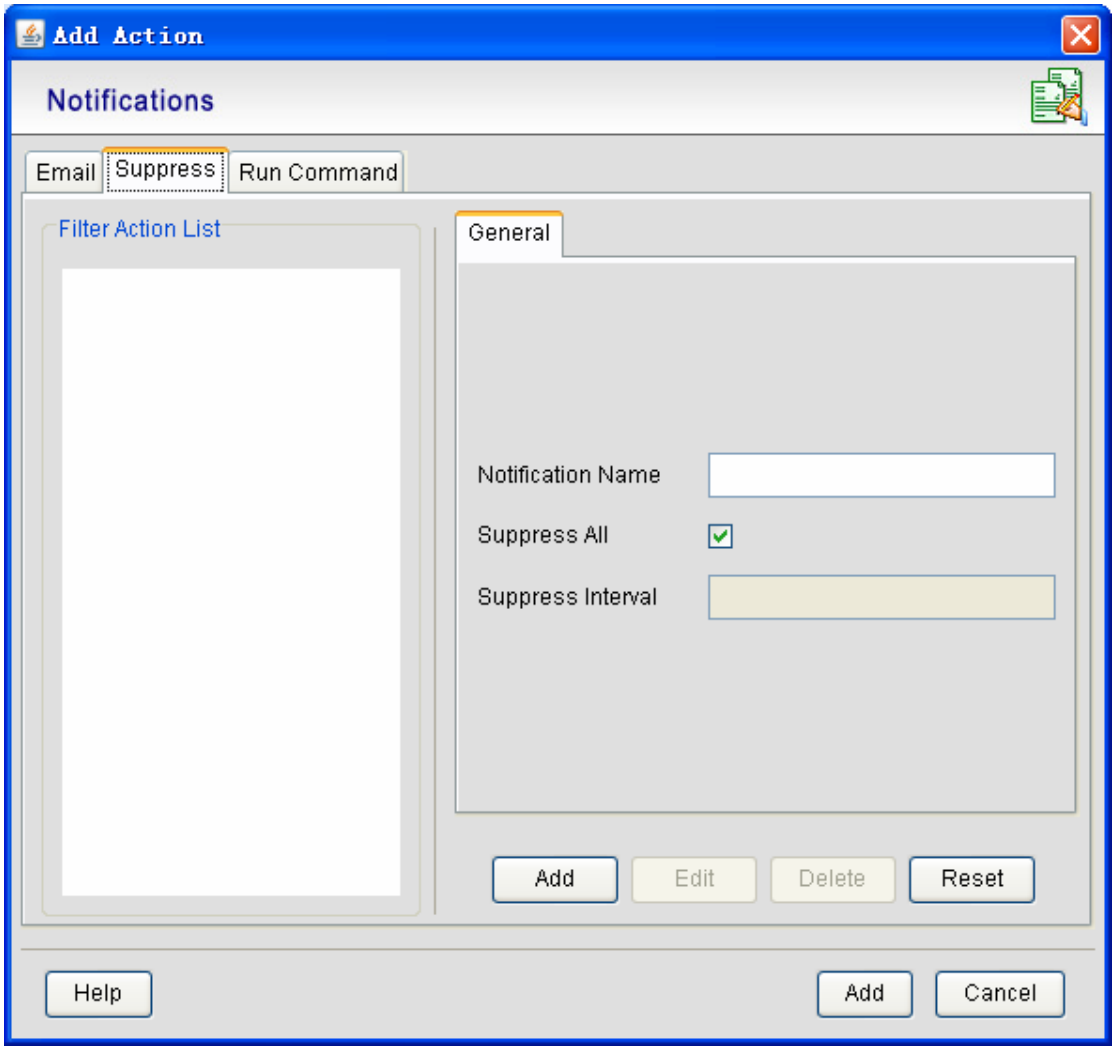
D. **Message: It means the body of the E-mail.**

E. **Appendix: Click it and the E-mail can carry other files.**

If you click **Send**, the configuration is done.

- **Limit:**

  If you click **Limit**, the following window appears:



In the right part of the above-mentioned figure, there are three parameters : **notification name**, **limit all**, and **limit interval**.They are defined below:

A. **Notification name:** it is the name of a notification, which consists of letter, number and underline.

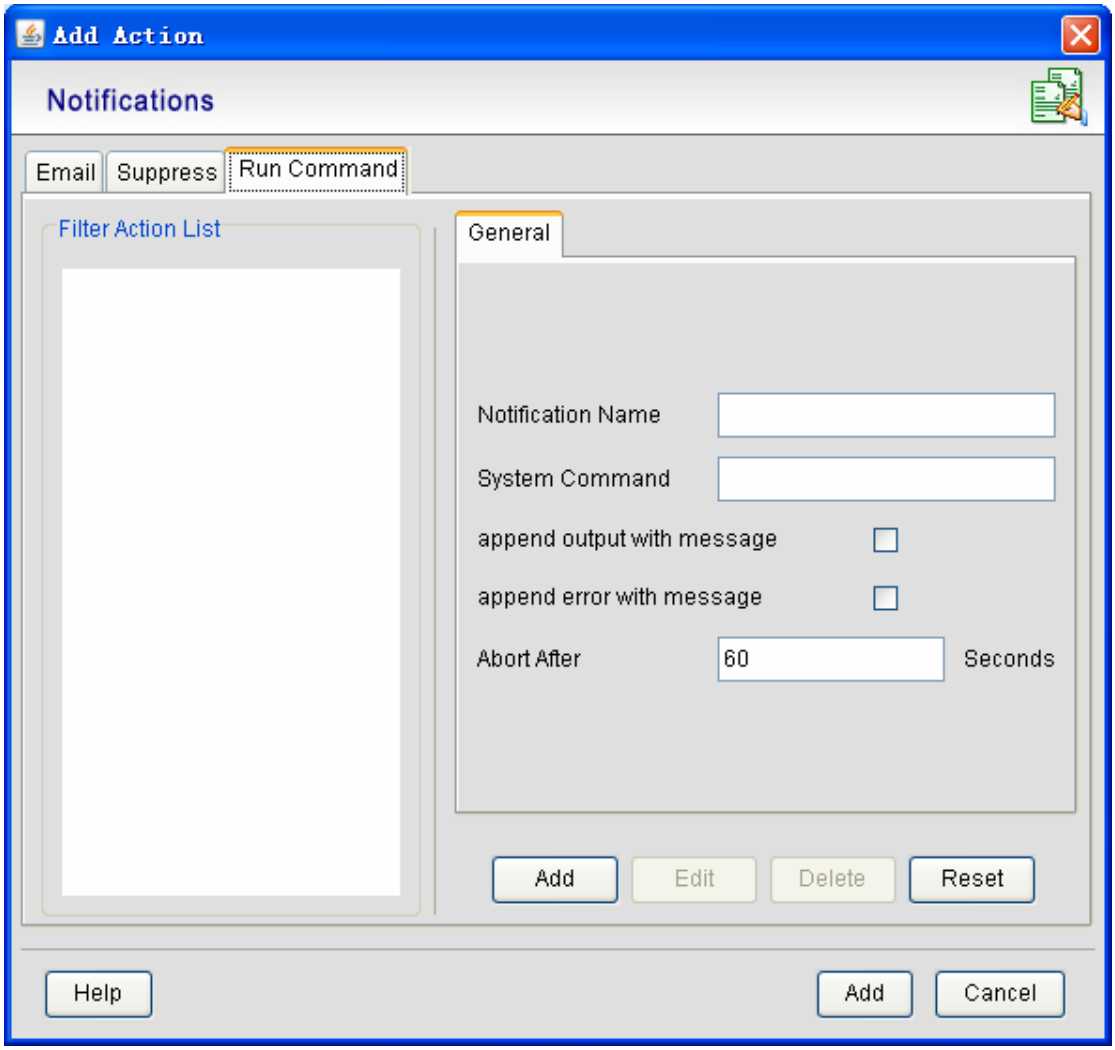
B. **Limit all:** If you choose tick out this parameter, the alarms will not appear and the system will automatically restrain this operation.

C. **Limit interval:** If **limit all** is selected, this option is unavailable.If **limit all** is deselected, this option is available and can be set to a number, meaning the interval for the alarm reminder to appear.

After the above-mentioned parameters are set, the **Limit** settings is done.

- **Command execution:**

  If you click **Command execution**, the following window appears:



In the right part of the above-mentioned figure, there are five parameters: **Notification name**, **Systematic command**, **Add the output to the Info**, **Add errors to the Info**, and **Forced end time**.They are explained below:

A. **Notification name:** it is the name of a notification, which consists of letter, number and underline.

B. **Systematic command**: it represents any program name that can be executed in the command line.

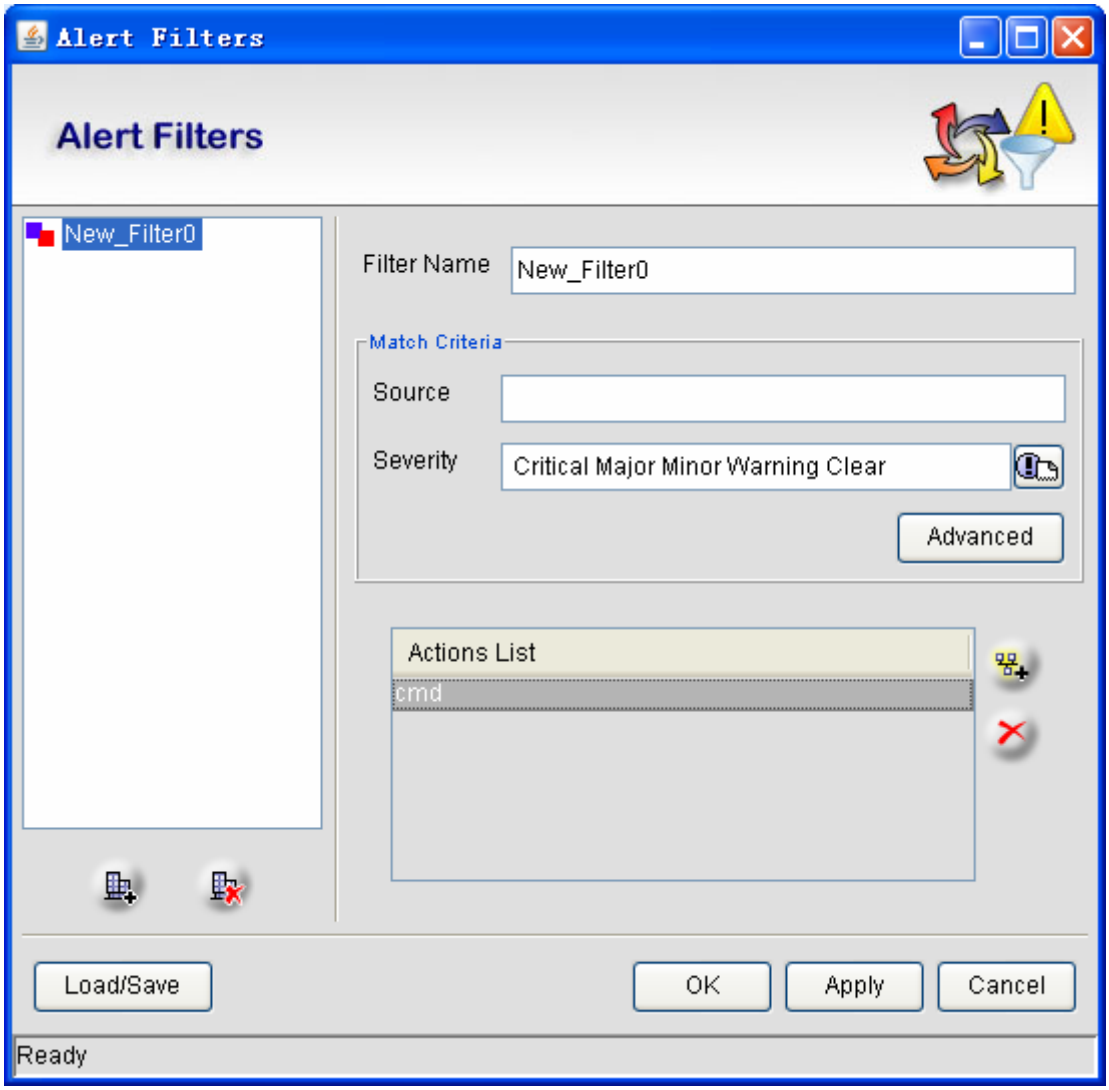
C. **Add the output to the Info**: It is to add the results of an execution command to the information.

D. **Add errors to the Info:** It is to add the errors of an execution command to the information.

E. **Forced end time**: If a command is still running after the forced end time, this command will be forced to end.

After the above-mentioned parameters are set, the **Command execution** settings is done.

After the above mentioned information is set, click **Add**, all the current settings will relate with the corresponding alarm filter.The view that appears in this case is shown below:

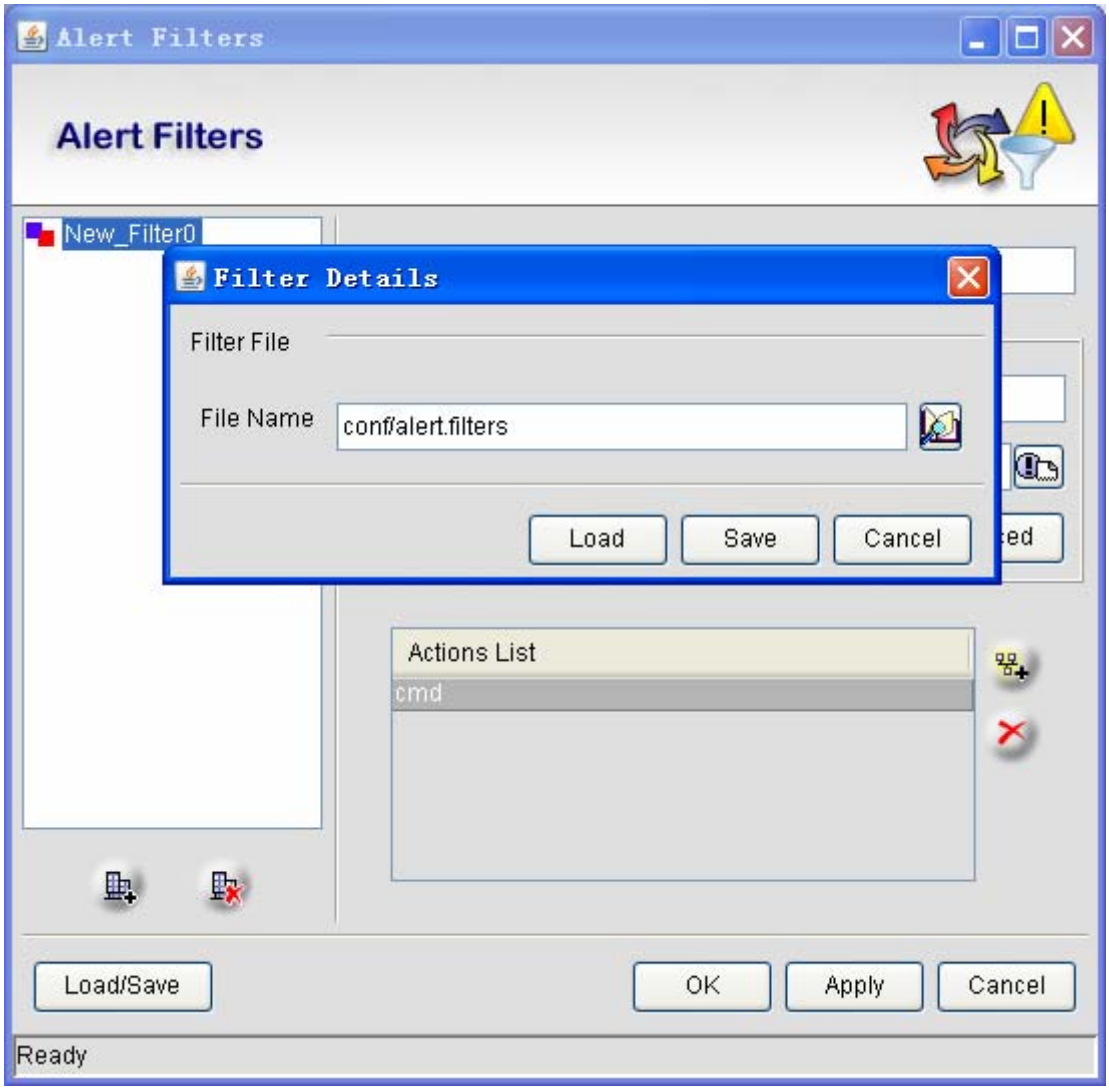


Click **OK**.The settings of alarm notification is finished.

There are also the following settings:

1、 Installing or saving files:

Click **Install/save file**. The file textbox appears:



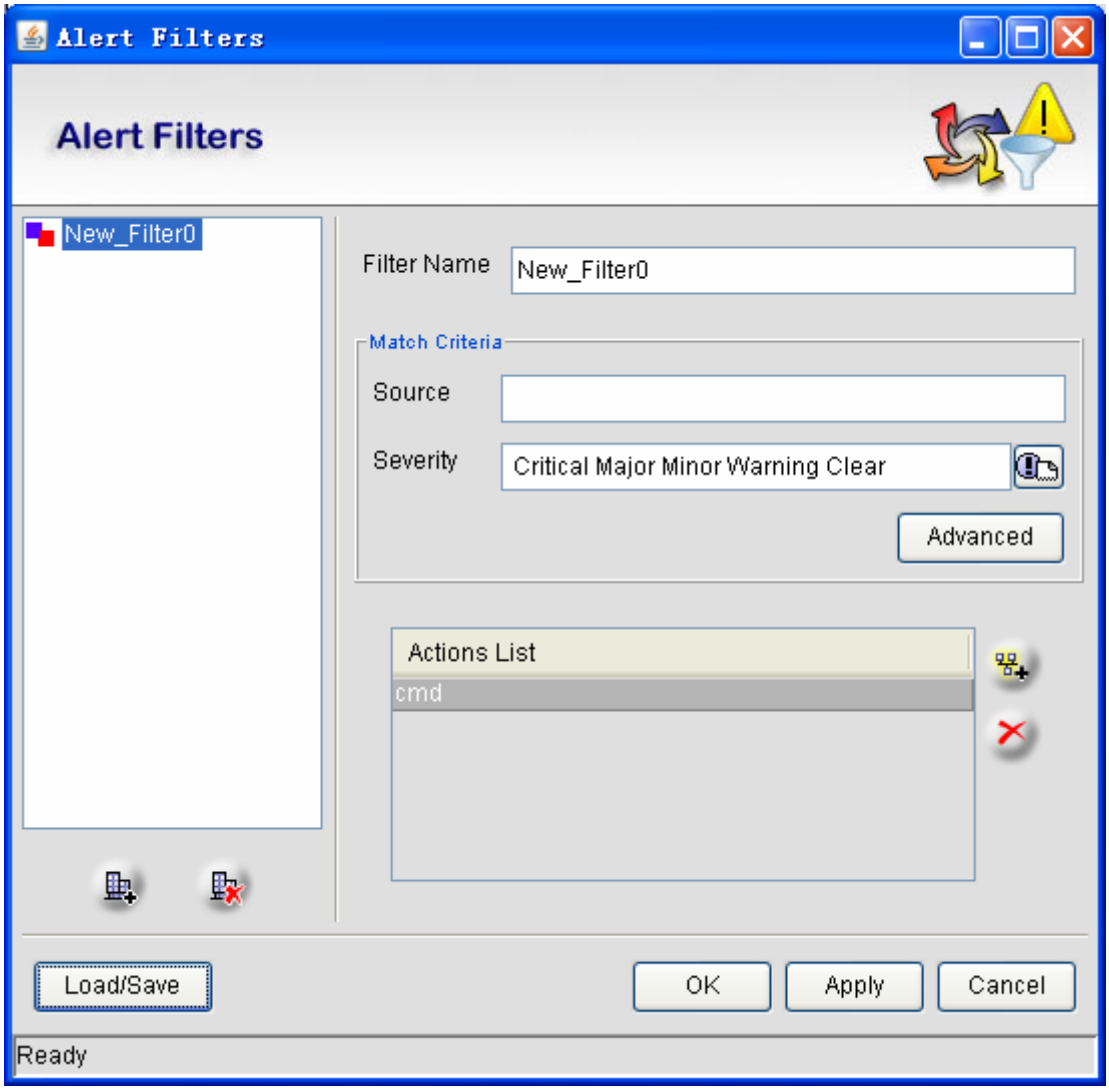
The **File name** option in the above-mentioned text box cannot be modified, or the alarm notification will take no effect. Click **Save** and then **Apply**. The settings then takes effect.

2、Download from the file:

Download the settings directly from the file.

6.2.1.2 Canceling the alarm notification

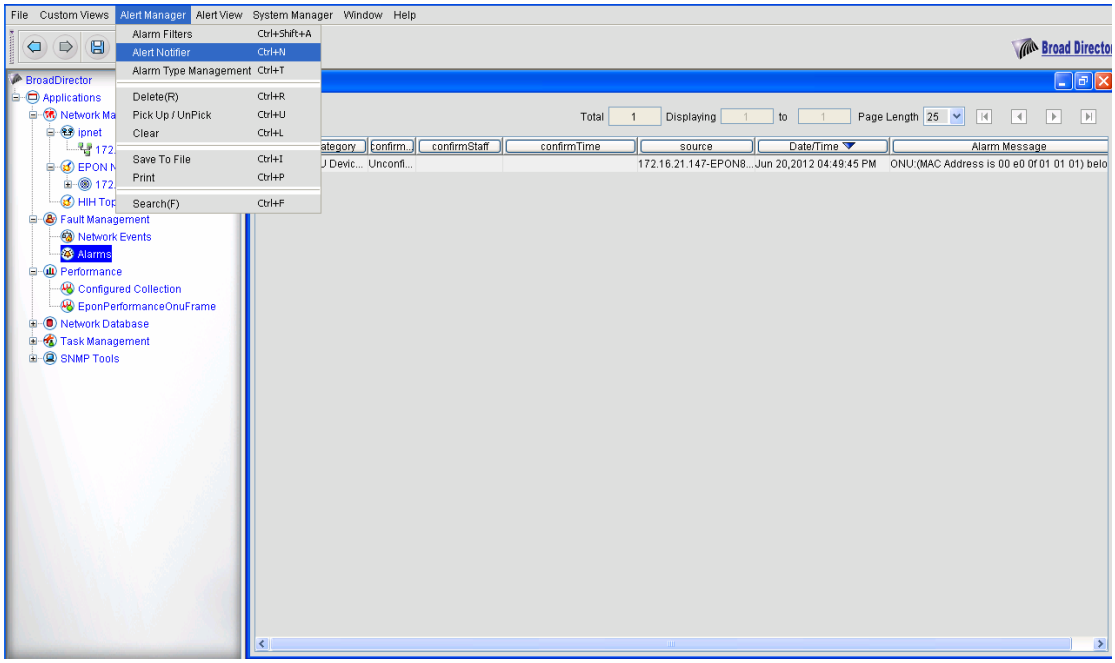
The **Cancel the alarm notification** page appears as follows:



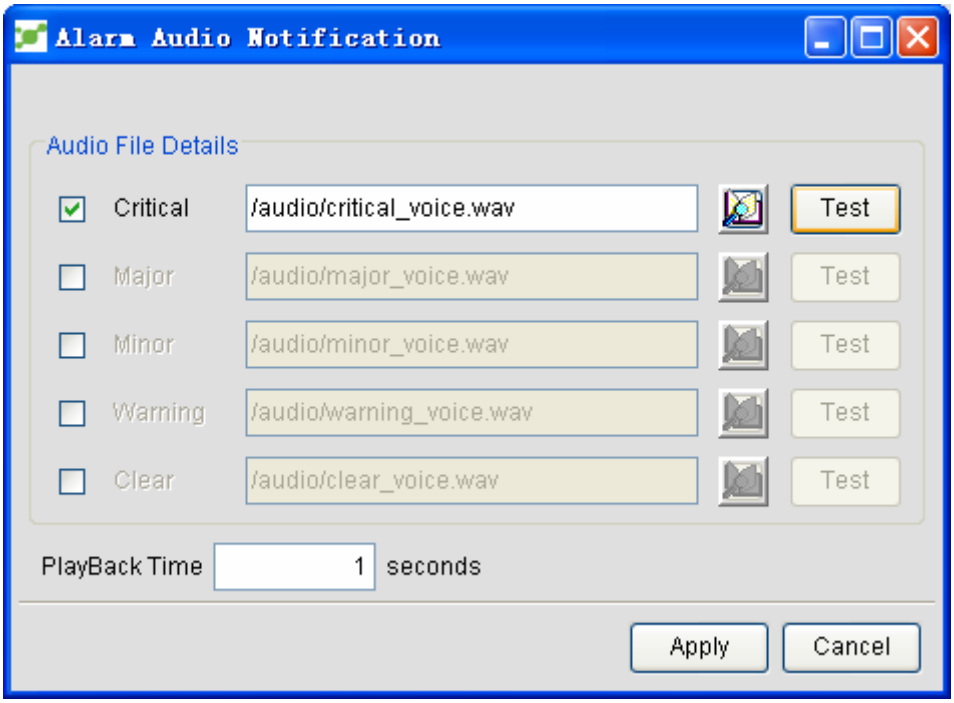
In the above-mentioned figure, there exists one alarm notification. To delete this alarm notification, select this alarm notification and click  .

6.2.1.3 Sound of the alarm notification

Click **Network Alarm -> Alarm Management**. A menu appears, as shown in the following figure:



Click **Sound of the alarm notification**. The following window appears:



On this window, you can select or cancel the sound of the corresponding alarm level by ticking or not.

Replay time: It means the time that the sound of alarm notification lasts (if the audio lasts too short, it will be replayed).

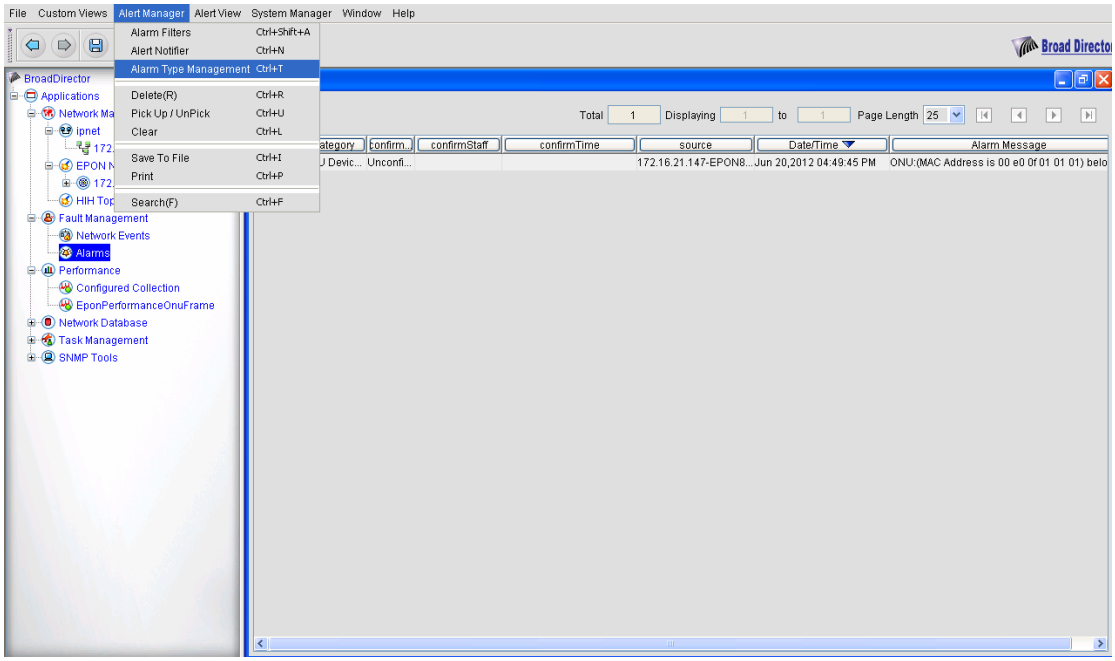
Test: This button is for you to test the sound beforehand.

 Open file: You can select any audio file by clicking it.

Note: The audio files are all stored in the **/audio** sub-directory of the installation path.

6.2.1.4 Alarm type management

Click **Network Alarm -> Alarm Management**. A menu appears, as shown in the following figure:

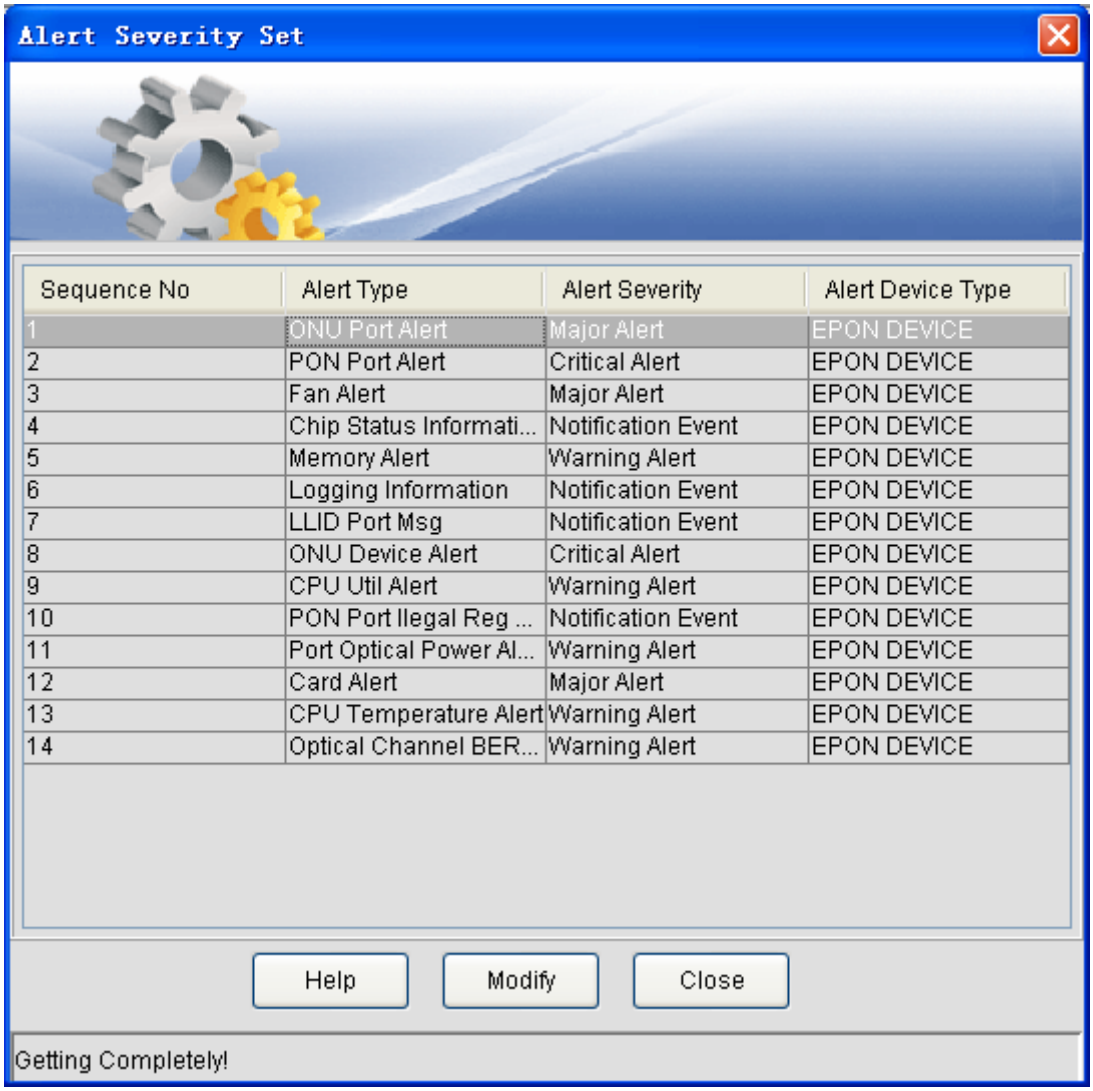


Click **Alarm type management**. A window appears, as shown in the following figure.

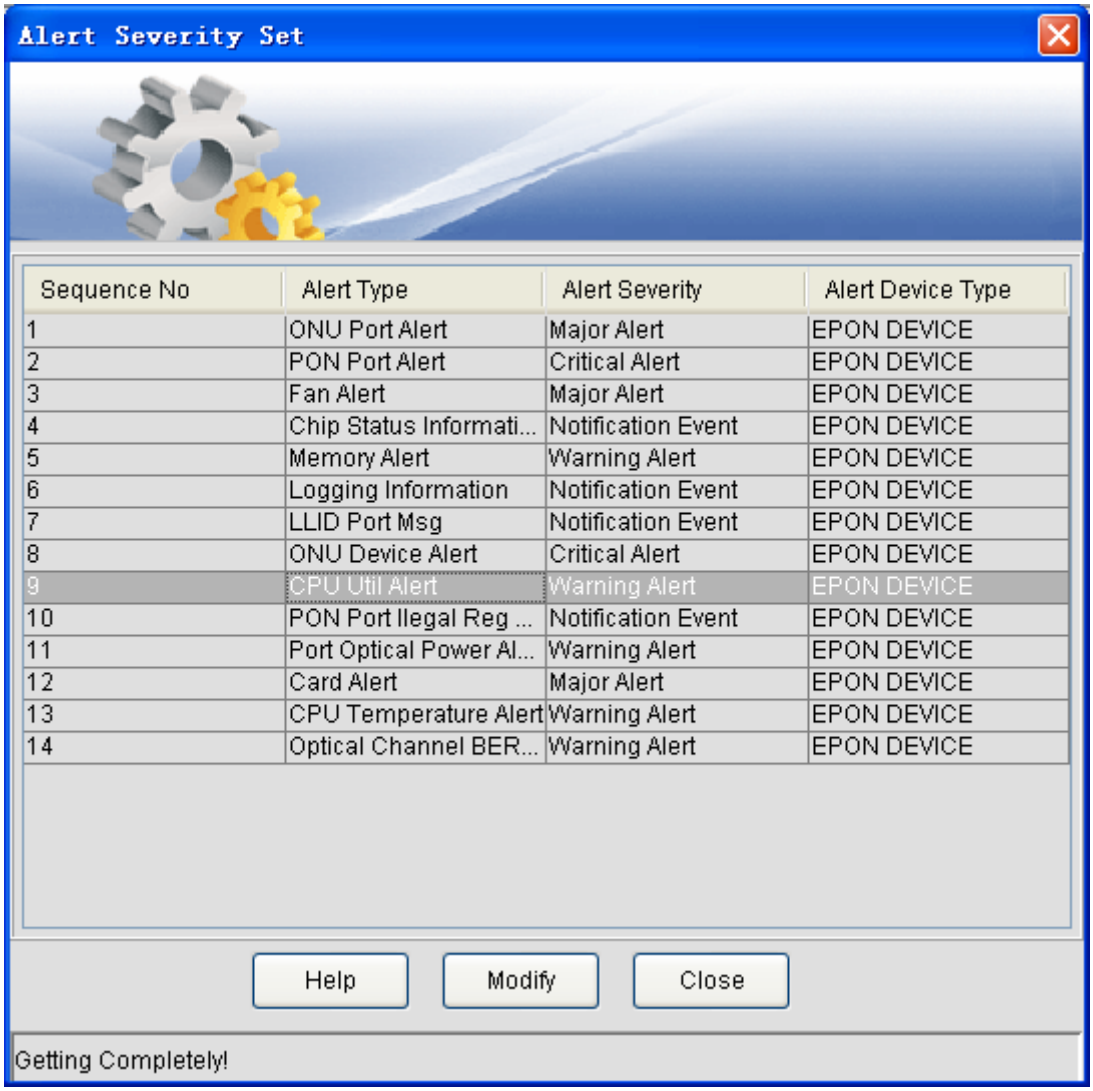
The following figure shows all kinds of alarms that the current NMS supports and their alarm levels.

Note: The frequent alarms include port’s alarms (port up/down), CPU alarms, fan alarms, memory alarms, card alarms, and optical channel’s error-code alarm.Additionally, this NMS also lists out specific EPON alarms, such as ONU port’s alarms, chip's state alarm and PON port’s alarms.

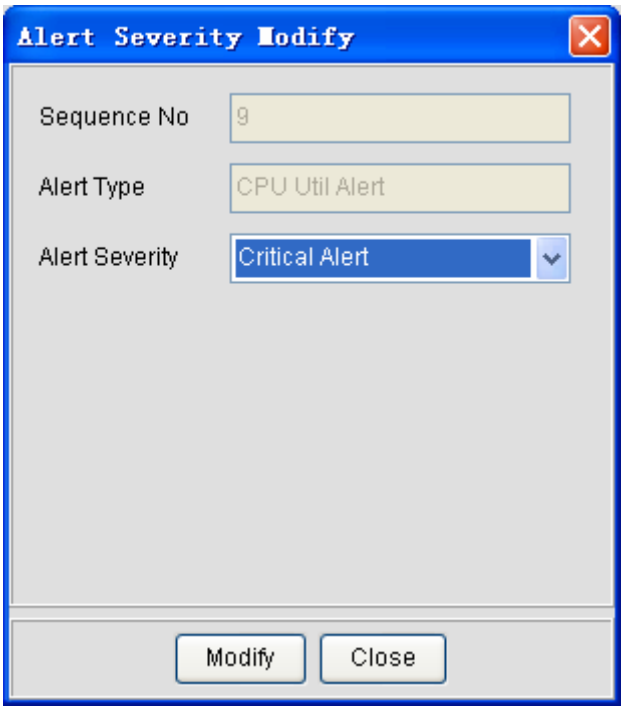
Each alarm type has a default alarm level, but users can modify the alarm levels.



As to how to modify the alarm levels, we take CPU usage alarm as an example. If you wamt to edit the alarm level of the CPU usage alarm from from **Warning Alert** to **Critical Alert**, first click **CPU Util Alert**, as shown in the following figure:



Then click **Modify**, a window appears, as shown in the following figure:

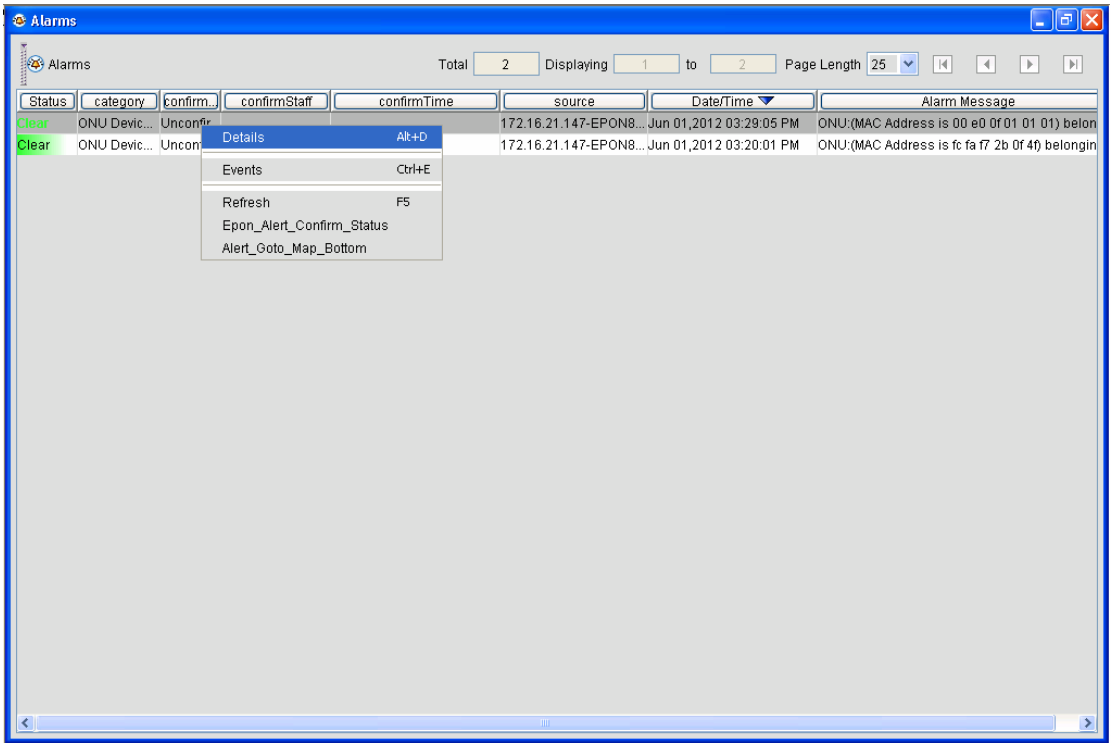


Select the corresponding alarm level in the **Alarm Severity** drop-down box and finally click **Modify**. The modified alarm level is stored to and applied on the NMS.

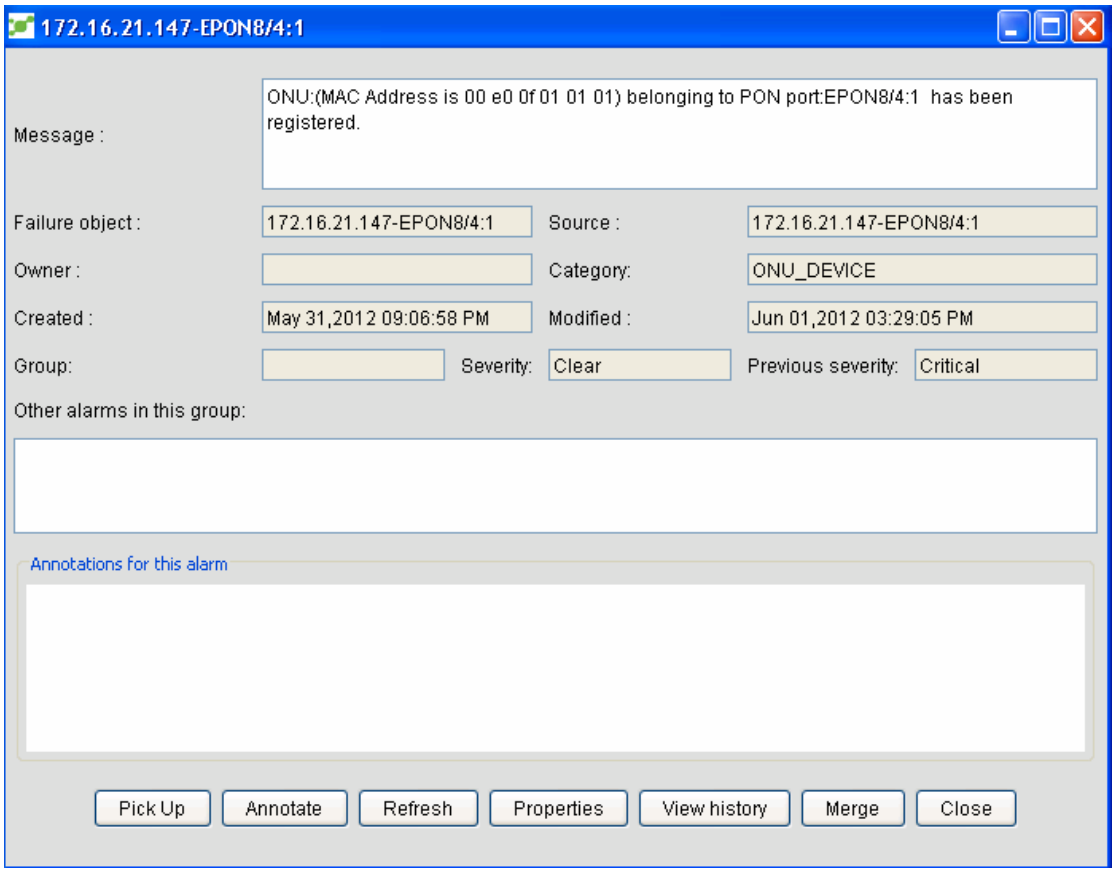
6.2.2 Right-Key Operations of Alarms

6.2.2.1 Alarm Details

If you click a specific item in the **Network alarm** list, a corresponding right-key menu appears, as shown in the following figure:



Click **Details**. The following window appears:



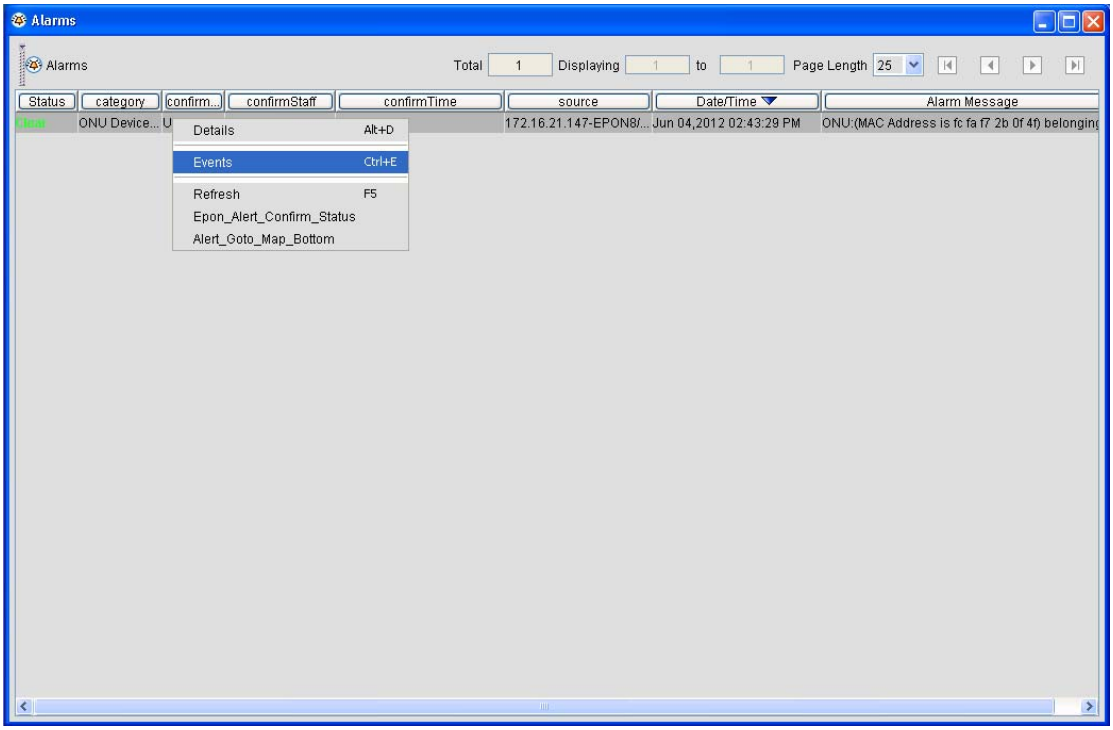
In the above-mentioned window, all detailed information about the corresponding alarm is listed out.

Pick: means the current user conducts the **Pick** operation to the current alarm.This operation records when and who to access the alarm. Different users can conduct this operation many times.

Note: means users can record the alarm processing suggestion to the current alarm.
Update: means the latest alarm information can be gained from the server.This function is similar to the **Update** function in the right-key menu in the alarm list.
Attribute: means some fields that users themselves define.
Browse history: means users can browse the alarms before the current alarm.
Combine: means to display the history alarms and the alarm processing suggestion together.

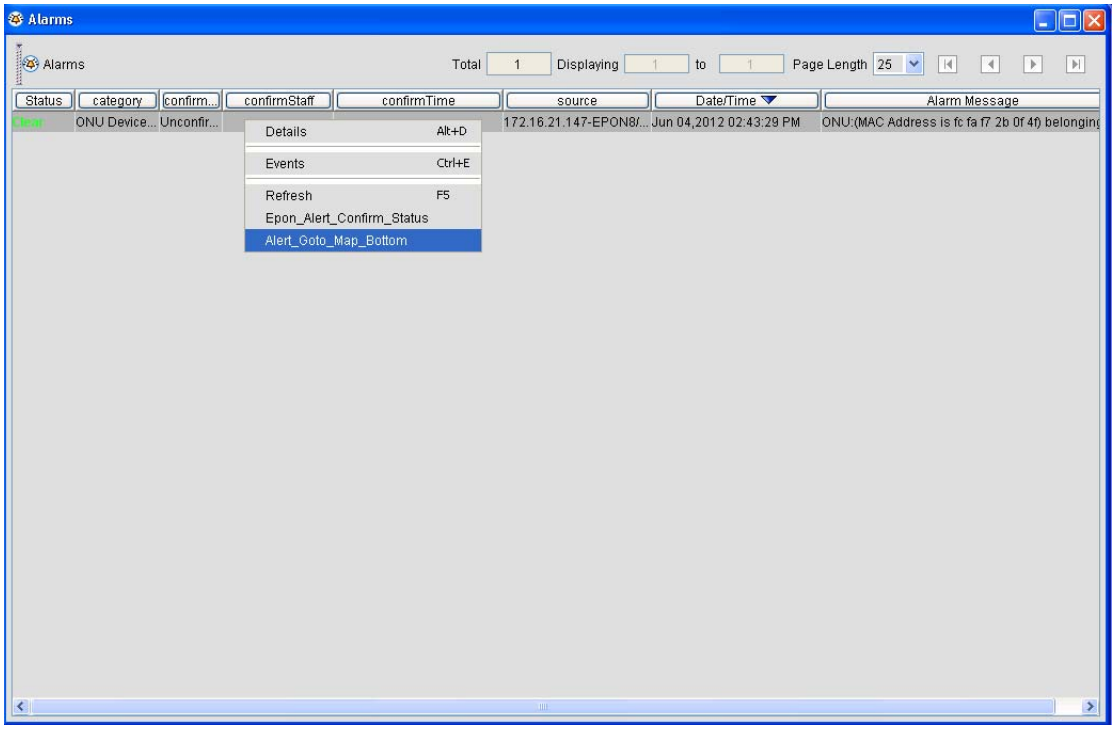
6.2.2.2 Event

If you select **Event** in the right-key menu in the alarm list, the system will list out all historical events related with the current chosen alarm.



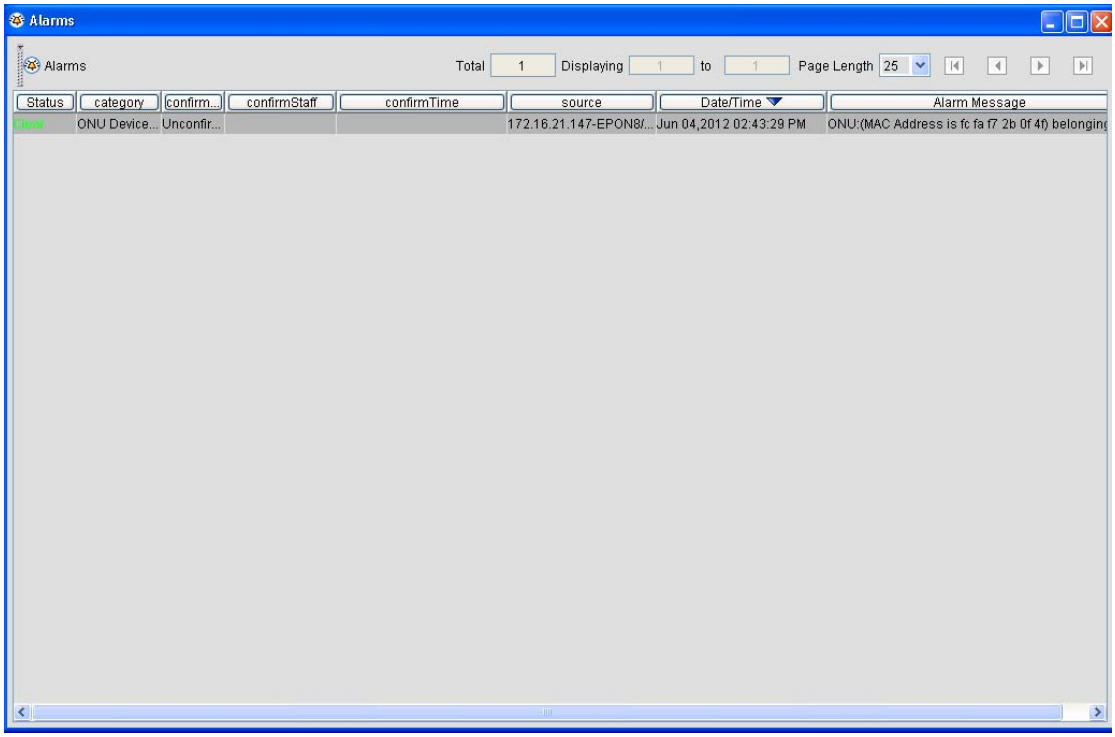
6.2.2.3 Locating alarms

If you select **Locate alarm** in the right-key menu in the alarm list, the system will automatically locate the network source of the current alarm to a specific network topology.
Note: In case that the EPON network is contained, the system will automatically search the EPON network topology and locate a specific network component.



6.2.2.4 Confirming alarms

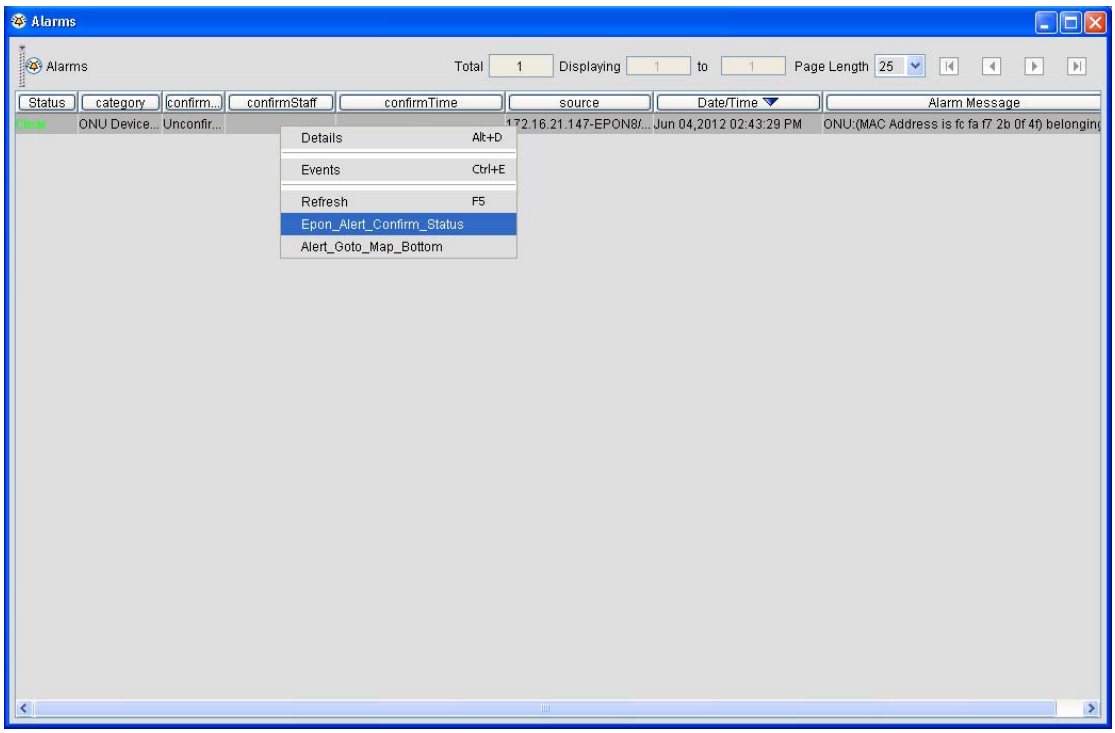
Click **Alarm**. The network alarm page appears.



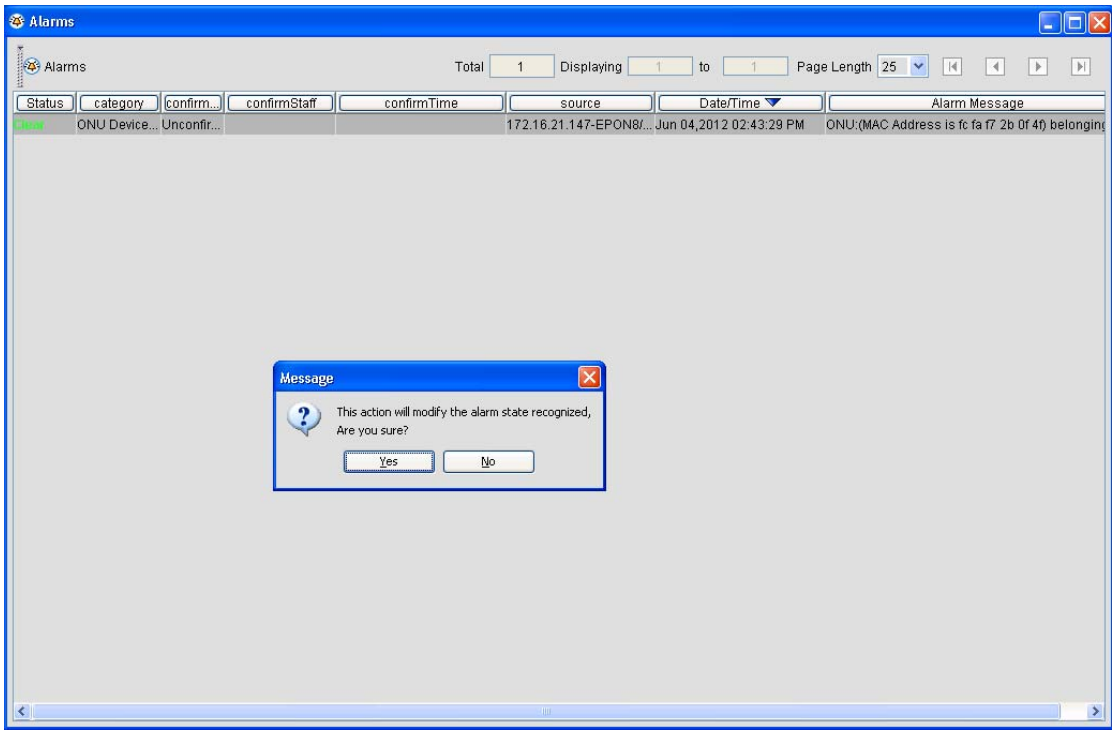
In the above-mentioned figure, two alarms are shown. Alarm confirmation includes **Confirmation Status**, **Confirmation Person**, and **Confirmation Time**.To confirm an alarm, choose the alarm

row, right click it and choose **Confirm alarm**.

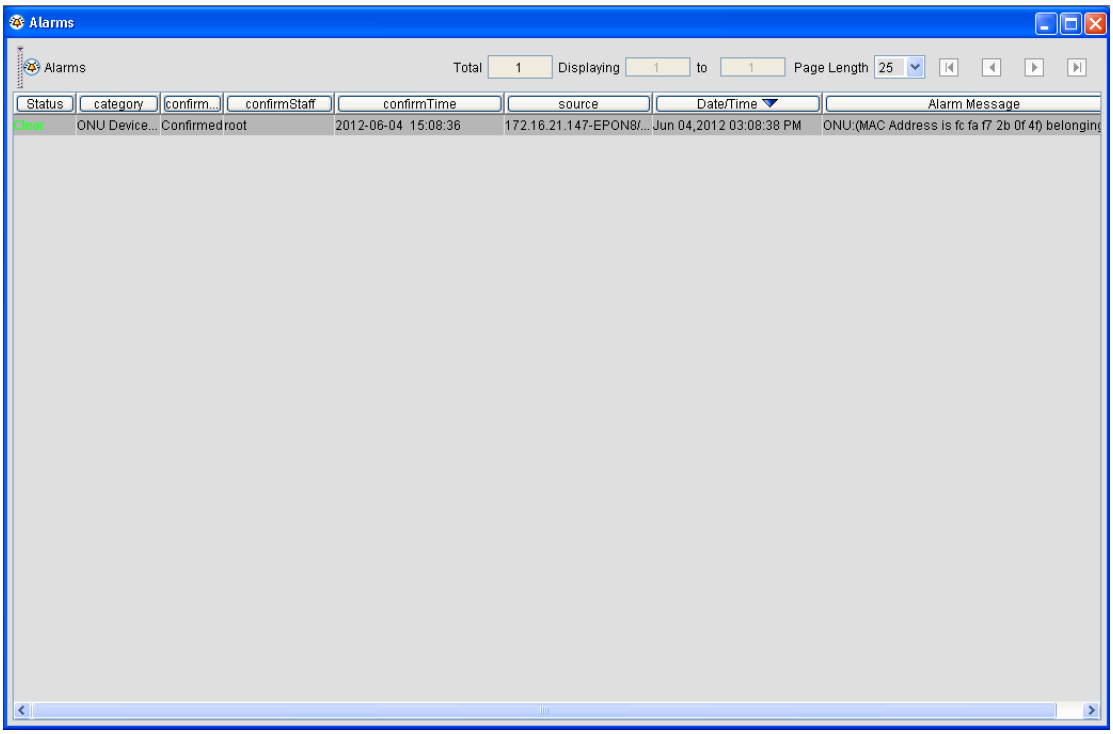
See the following figure:



Click **Confirm alarm**. The following dialog box appears.



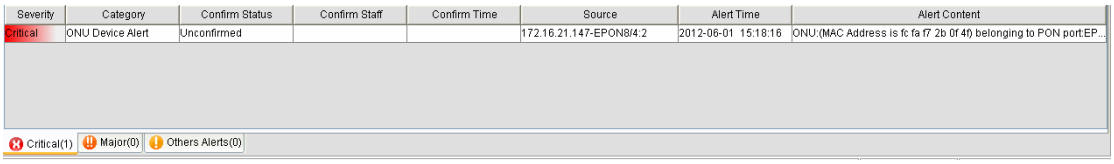
Click **Yes**.



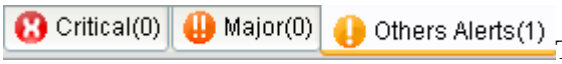
This alarm is then confirmed.The confirmation persion is the current administrator. The confirmation time is the time to confirm this operation.The confirmation status is **Confirmed**.

6.3 Alarm Toolbar

For the convenience of the administrator, NMS has the alarm toolbar at the bottom of its window.See the following figure:

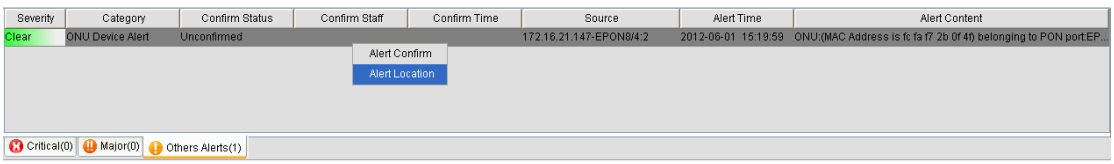


The above-mentioned figure is same to the alarm list, so please refer to the previous section.

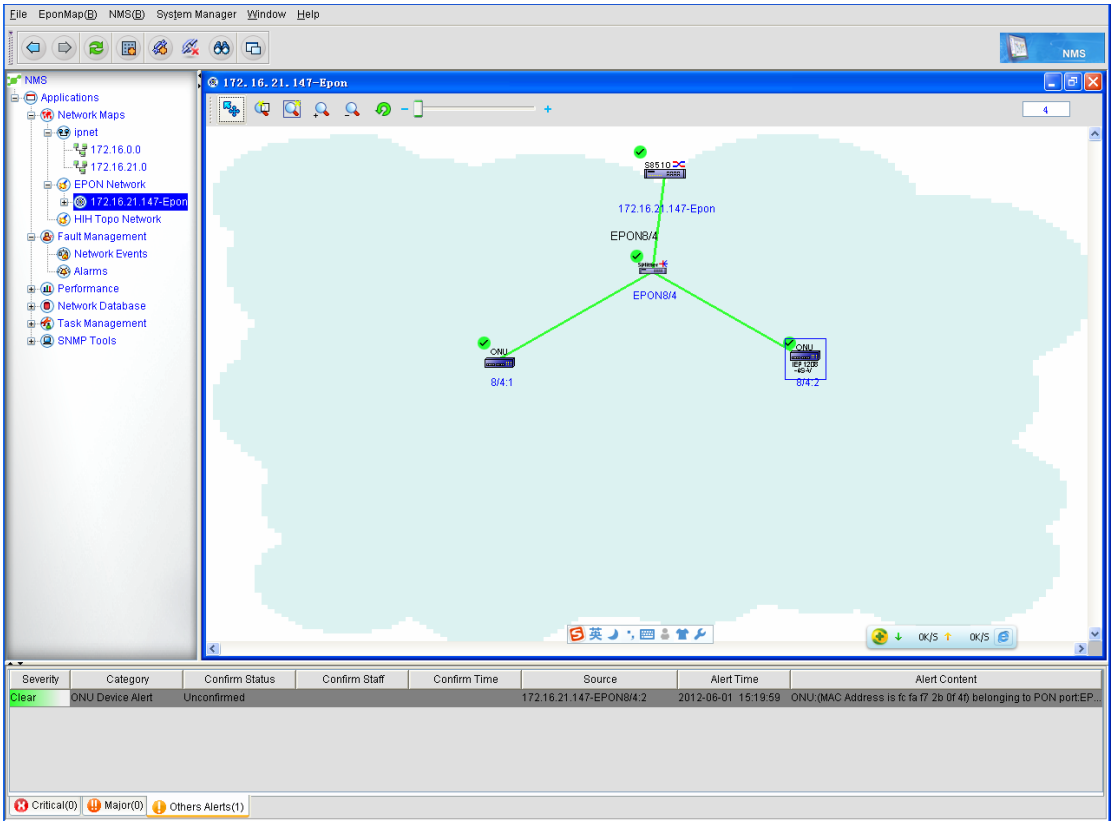


This small figure is shown at the left bottom of the above-mentioned figure.This small figure consists of three tabs: **Emergency Alarm**, **Important Alarm**, and **Other Alarm**.If you these tabs, the corresponding alarm levels will be shown.**Emergency Alarm** corresponds to the **Critical** level, **Important Alarm** the **Major** level, and **Other Alarm** the **Clear** level.

Select the alarm row and right click it. A menu appears, as shown in the following figure:



- **Confirm alarm**: please refer to section "**Confirming alarms**."
- **Locate alarm**: If you click it, the **Network** page will be opened. On this page you can select the alarm source.See the following figure:



7 Performance Management

This chapter gives a detailed description of the performance statistics mode.Performance statistics means to browse the operation parameters of a device in a period of time and present these parameters on the statistics graphic on the window, so performance statistics helps you to know the running status of the device in a period of time.

This chapter consists of **CPU performance statistics** and **port’s traffic statistics**.

CPU performance statistics: means to collect the information about CPU usage.

Port’s traffic statistics: means to collect the information about traffic on some ports.

ONU port’s traffic: means to display the traffic on each port of ONU. This option does not include the historical data.

Performance statistics is classified into **Real-time performance statistics** and **Historical performance statistics**.

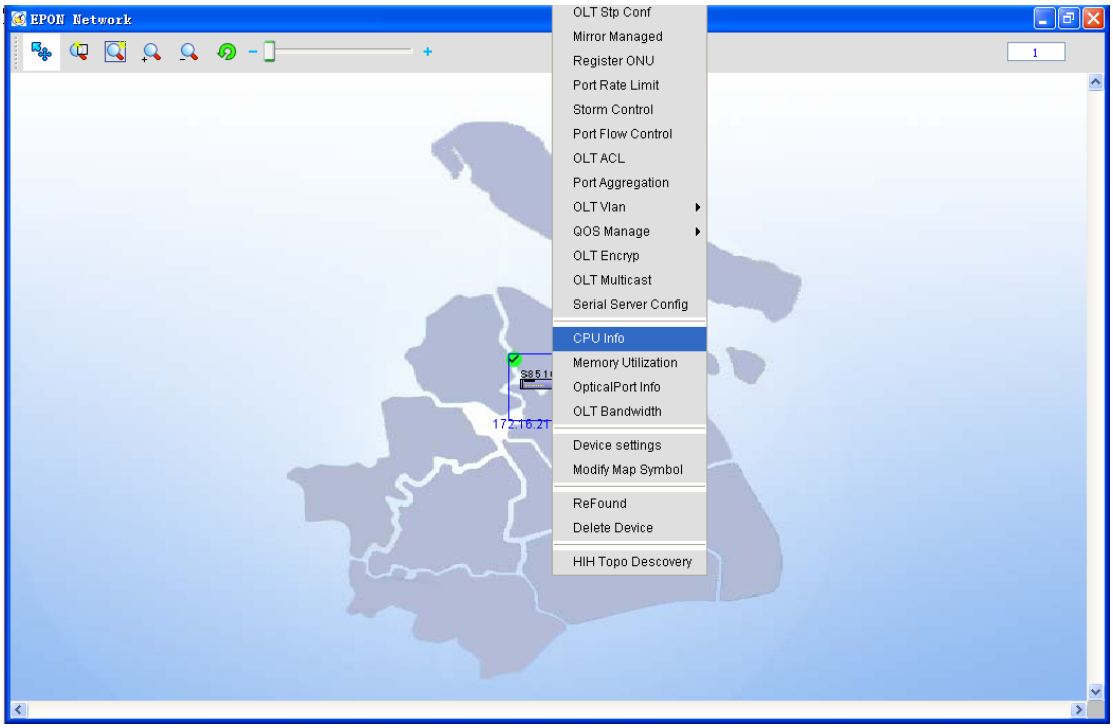
Real-time performance statistics: means to collect the real-time data of a device and display these data in real time.

Historical performace statistics: means to browse the running data of a device during a past period.

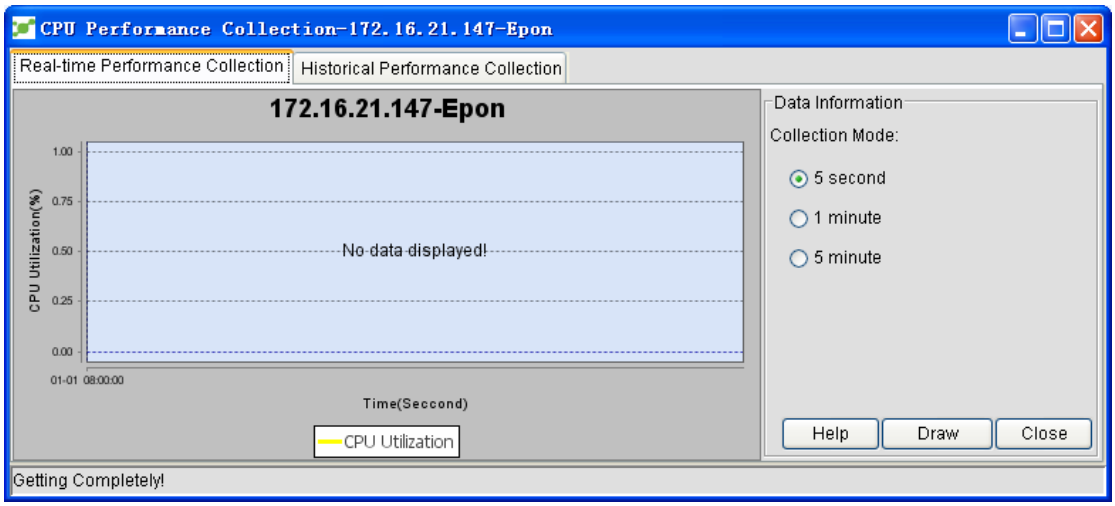
7.1 CPU Performance Statistics

CPU performance statistics means to collect the information about CPU usage.

Click **EPON network -> EPON device -> CPU performance statistics** on the NMS window, as shown in the following figure:

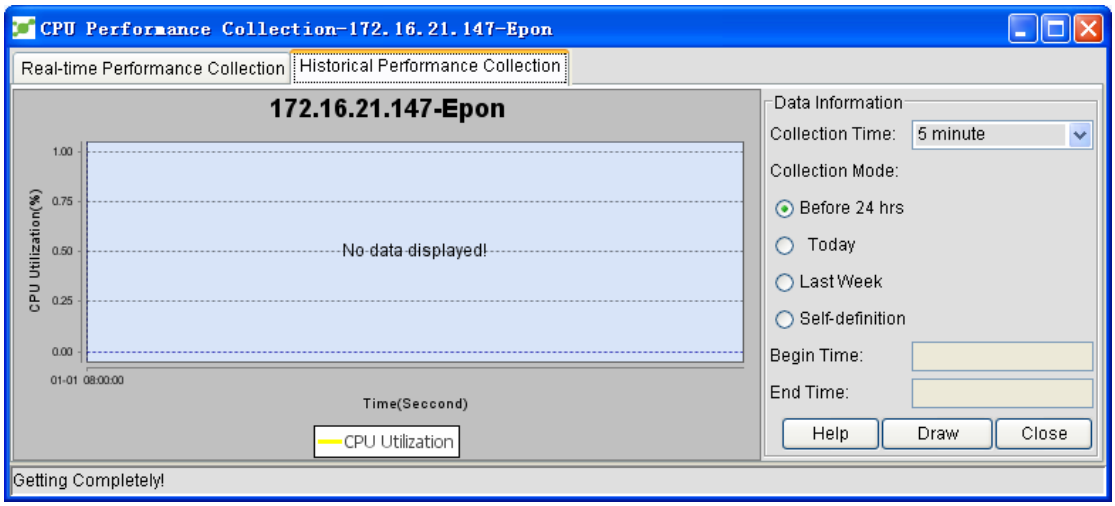


The CPU performace statistics page appears:



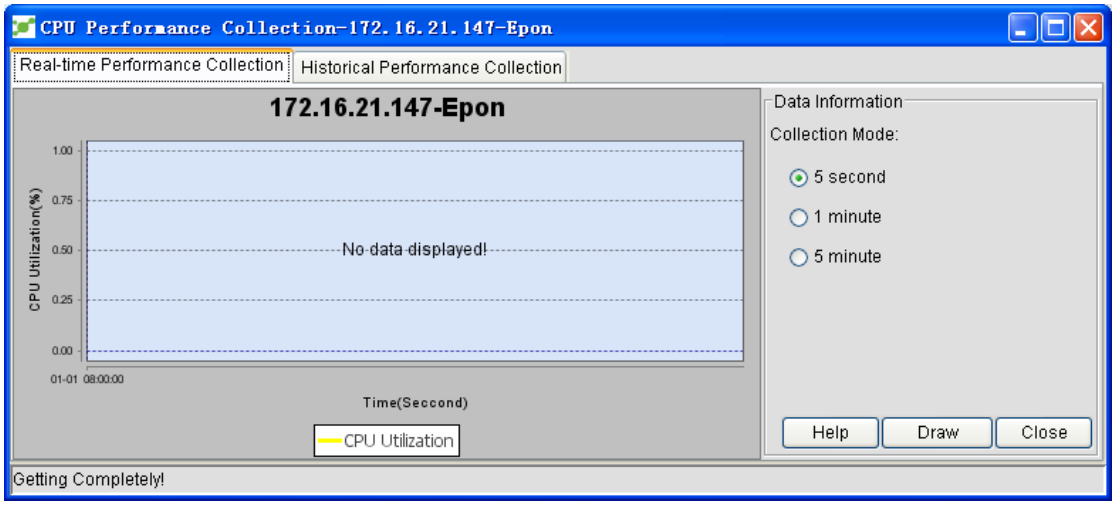
Performance statistics is classified into **Real-time performance statistics** and **Historical performance statistics**.

The above-mentioned figure shows the real-time performance statistics page.The figure below shows the historical performance statistics page.

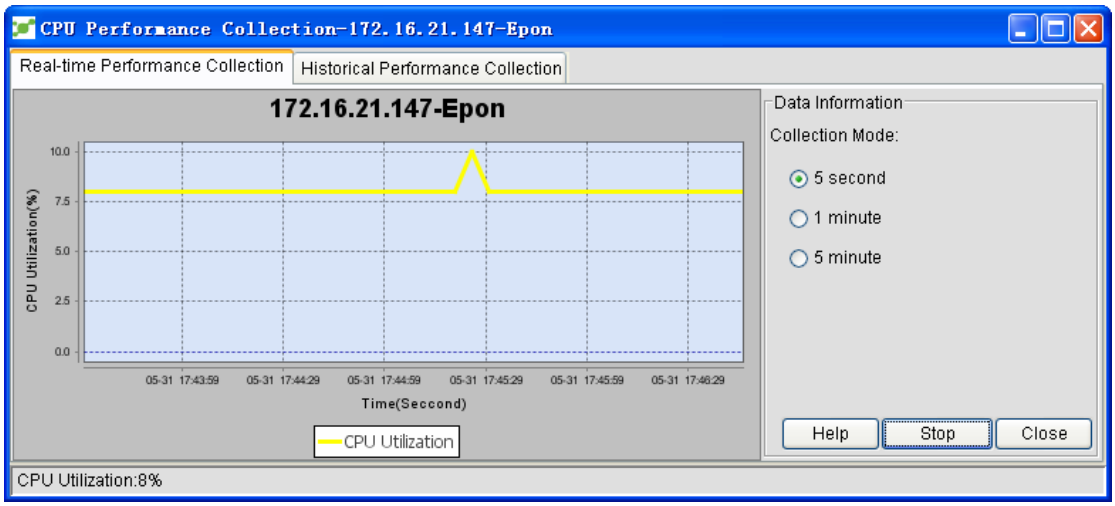


7.1.1 Real-Time Performance Statistics

Choose **CPU performance statistics** to enter the real-time performance statistics page:



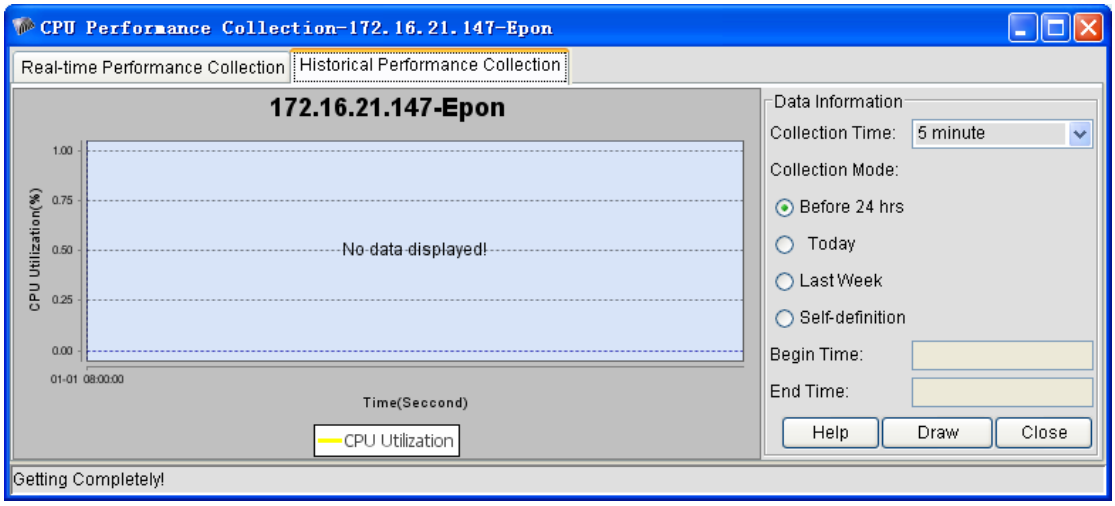
On the page you can choose the statistics interval. If you click **Draw map**, real-time performance statistics will be conducted.If you choose 5 seconds as the statistics interval, the corresponding statistics window is shown in the following figure:



Each point in the curve stands for the CPU usage.The distance between points stands for the statistics interval.If you click **Stop**, the real-time CPU performance statistics will be stopped.

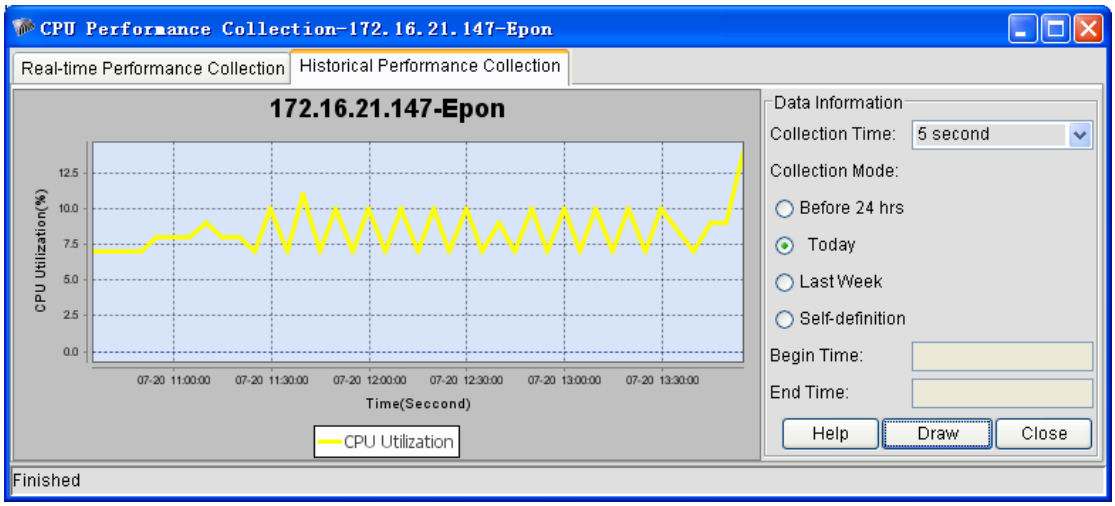
7.1.2 Historical Performance Statistics

Click **CPU performance statistics -> Historical performance statistics** to enter the historical performance statistics page.



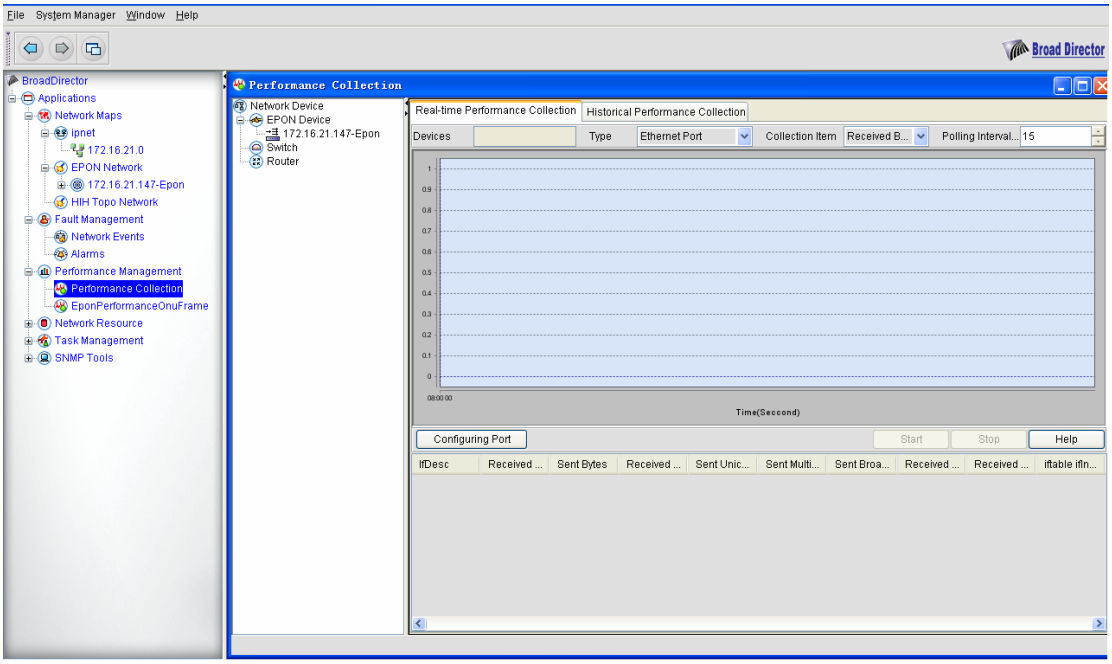
Statistics time stands for the interval of CPU usage statistics. Statistics mode stands for the data statistics period, which can be self-defined.

The following figure shows the statistics time is 5 seconds and the statistics mode is self-defined:

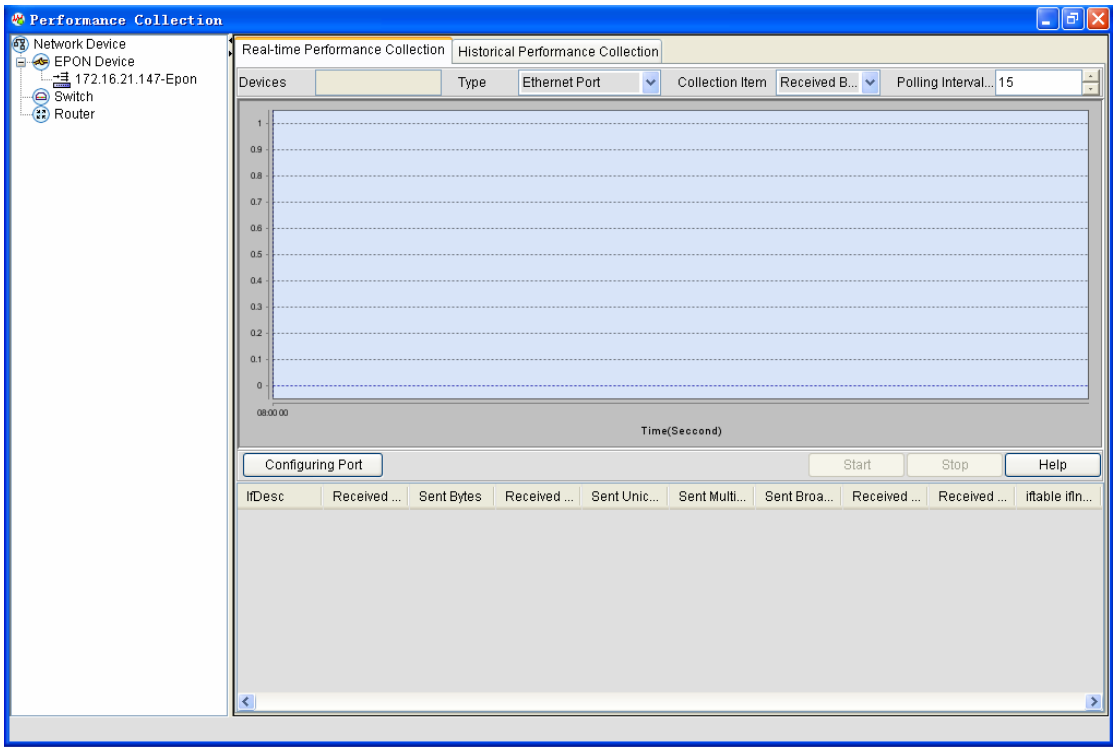


7.2 Port's Traffic Statistics

Port's data flow statistics means to collect the information about flows on a designated port.It is also classified into **Real-time performance statistics** and **Historical performance statistics**. Click **Performance management-> Performance statistics** in the NMS window, as shown in the following figure:

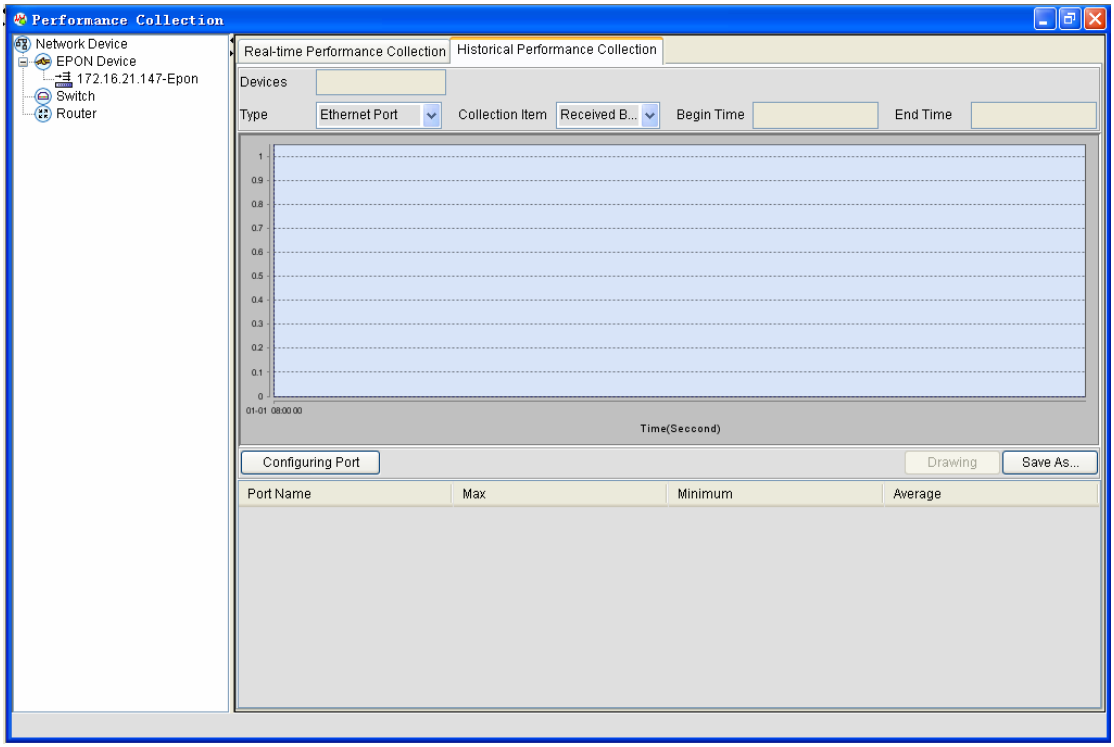


The performance statistics page appears, as shown in the following figure:



In the above-mentioned figure, its left part shows the classified devices and its right part shows the performance statistics page.The right part of the above-mentioned figure shows the real-time performance statistics page.

The figure below shows the historical performance statistics page.



7.2.1 Real-Time Performance Statistics

It is to collect the information about the real-time traffic on some ports of a device.

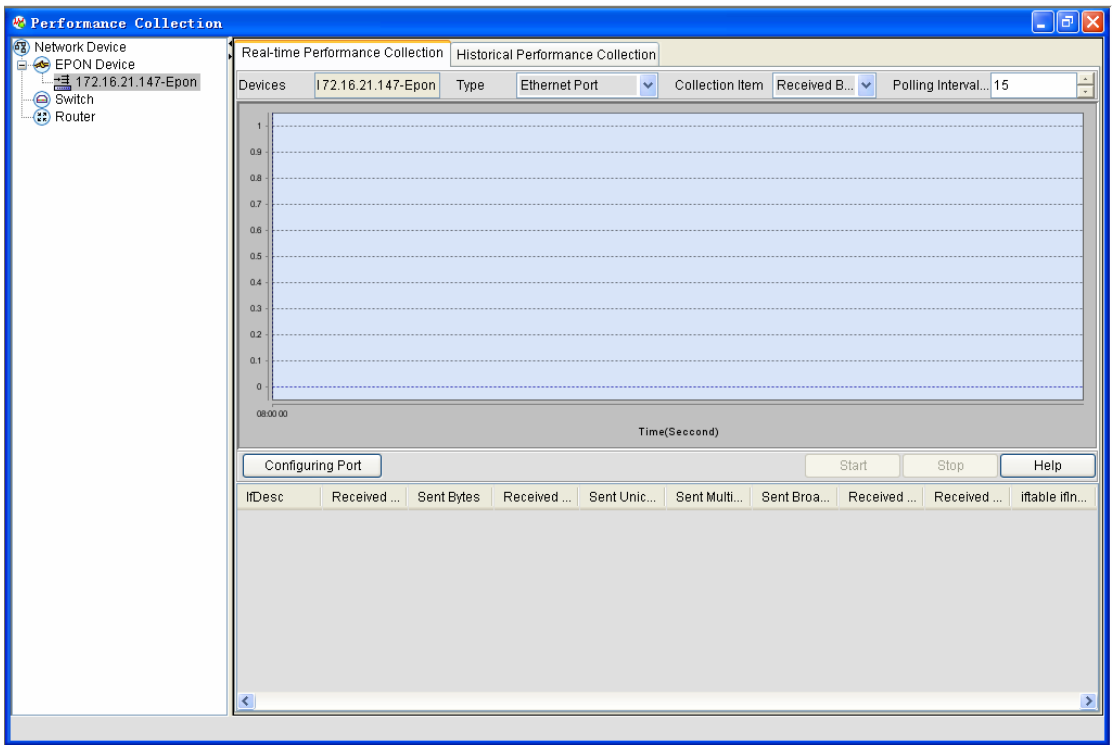
Statistics options include **Port type**, **Statistics item**, and **Polling interval**.

Here **Port type** contains **Ethernet port** and **PON port**.

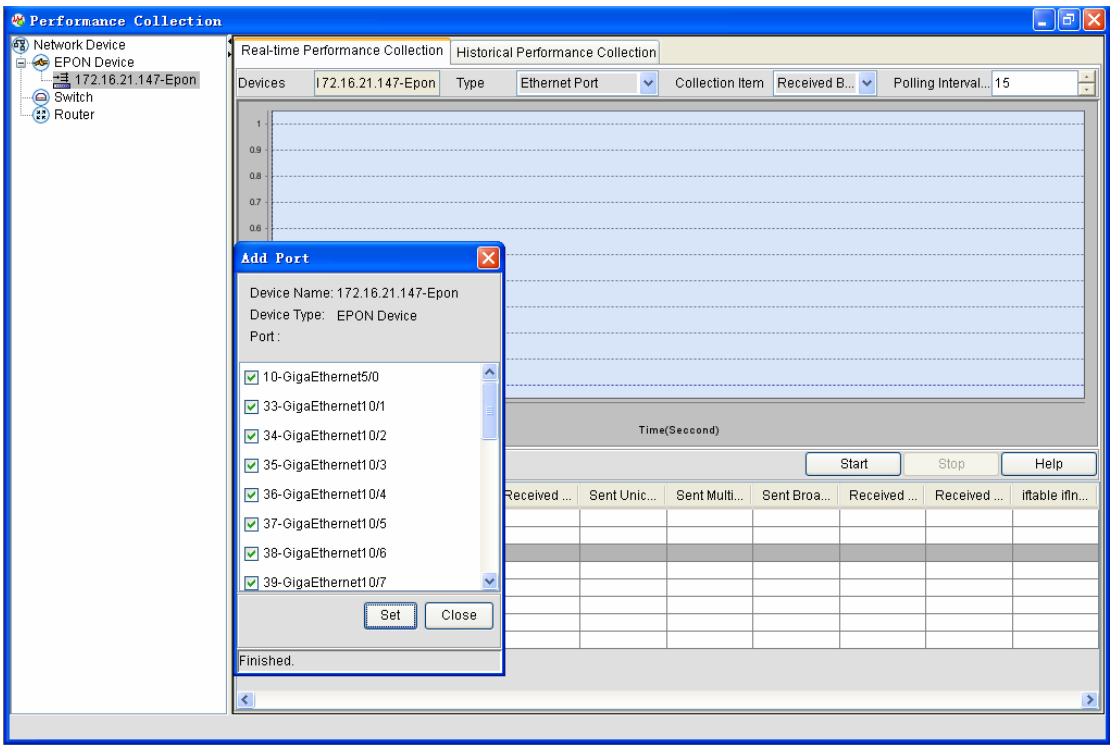
Statistics item contains **Port's incoming flow (Bps)**, **Port's outgoing flow (Bps)**, **Number of received unicast packets**, and **Number of transmitted unicast packets**.

Polling interval means the statistics interval, whose smallest value is 10 seconds.

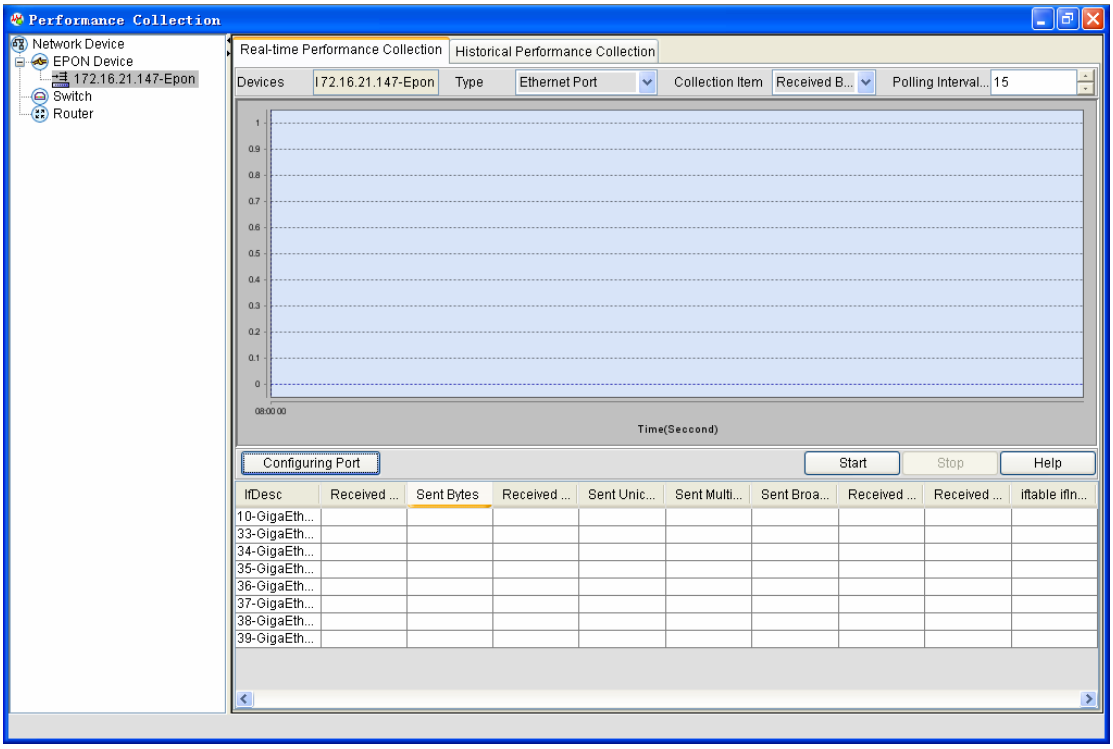
If you click **Performance statistics**, the **Real-time performance statistics** page appears:



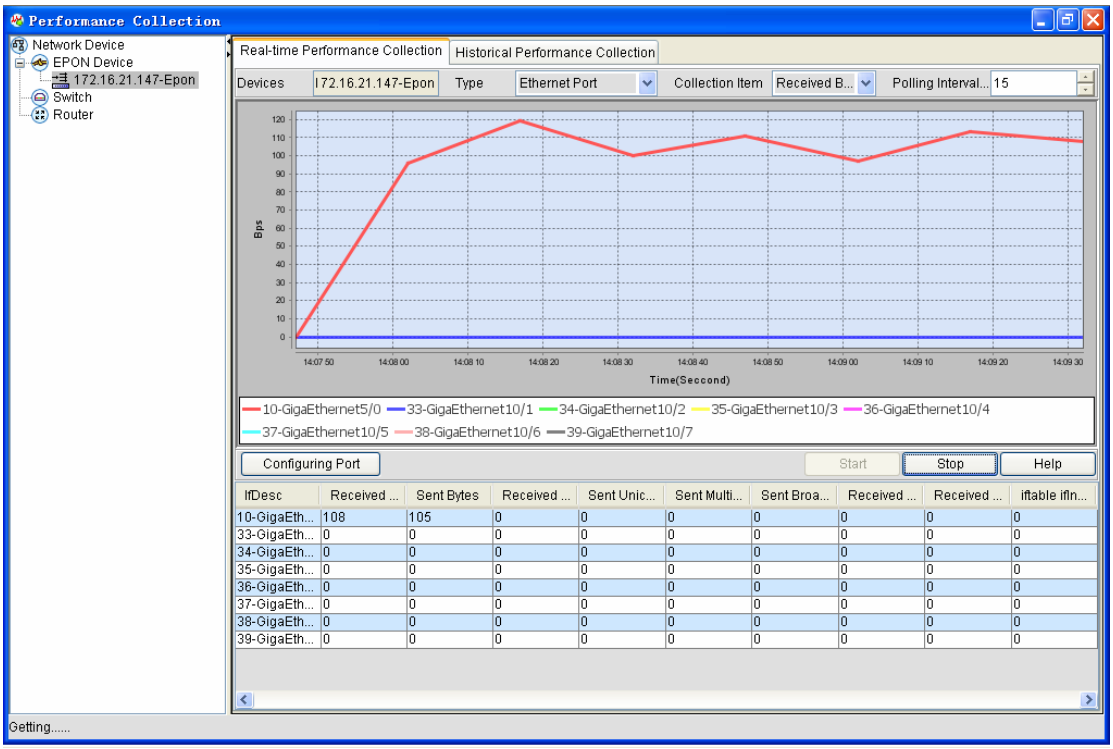
In the device list of the above-mentioned figure, double click an IP and enter a name in the **Device** textbox. Data statistics will be performance on this device.After the port type, statistics item and polling interval are set, click **Set port** tp set all ports on which data statistics will be conducted.See the following figure:



The figure above shows that 172.16.21.147-Epon is chosen, the port type is the Ethernet port, the statistics item is port's outgoing flow, the polling interval is 10 seconds and the **Set port** option stands for all Ethernet ports.After the settings, a window appears, as shown in the following figure:



On the above-mentioned figure, if you click **Start**, the data statistics will begin.The following figure shows data statistics:



The collected data can be classified into two parts: the upper part is the curve, representing the real-time data change,and the bottom part shows the port's traffic statistics list,in which the column stands for the port type.

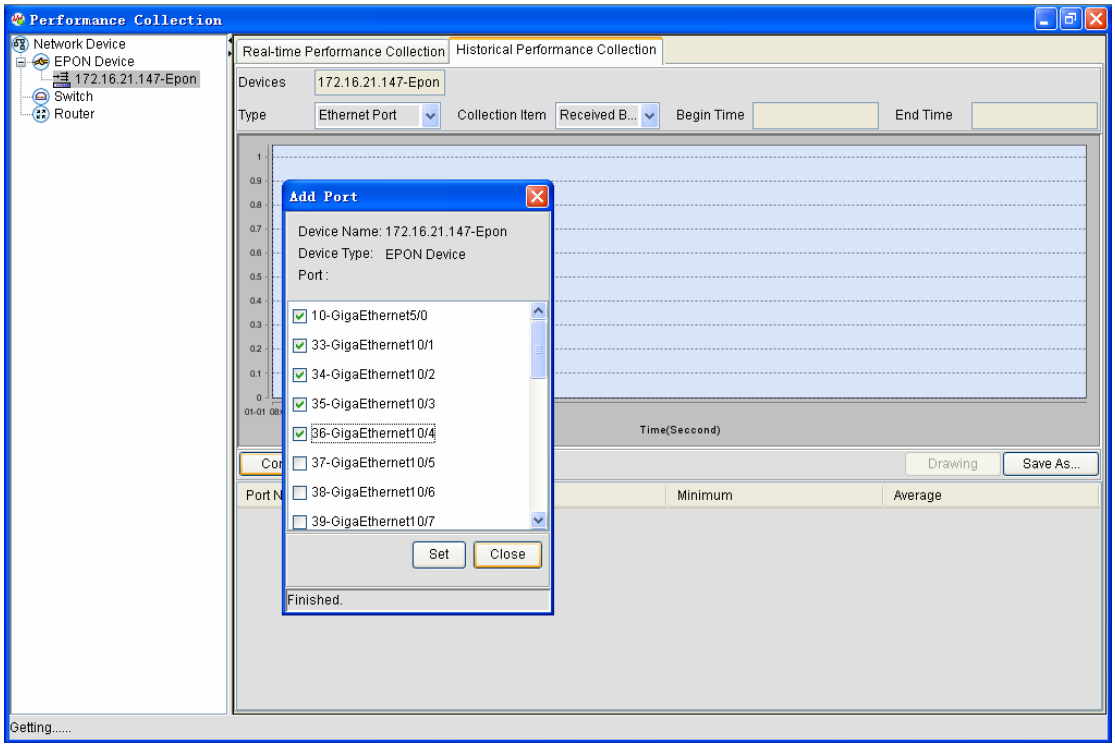
The statistics items corresponding to the Ethernet port are **Port's incoming flow (Bps)**, **Port's outgoing flow (Bps)**, **Number of received unicast packets**, **Number of transmitted unicast packets**, **Number of transmitted multicast packets**, **Number of transmitted broadcast packets**, **Number of received multicast packets** and **Number of received broadcast packets**.

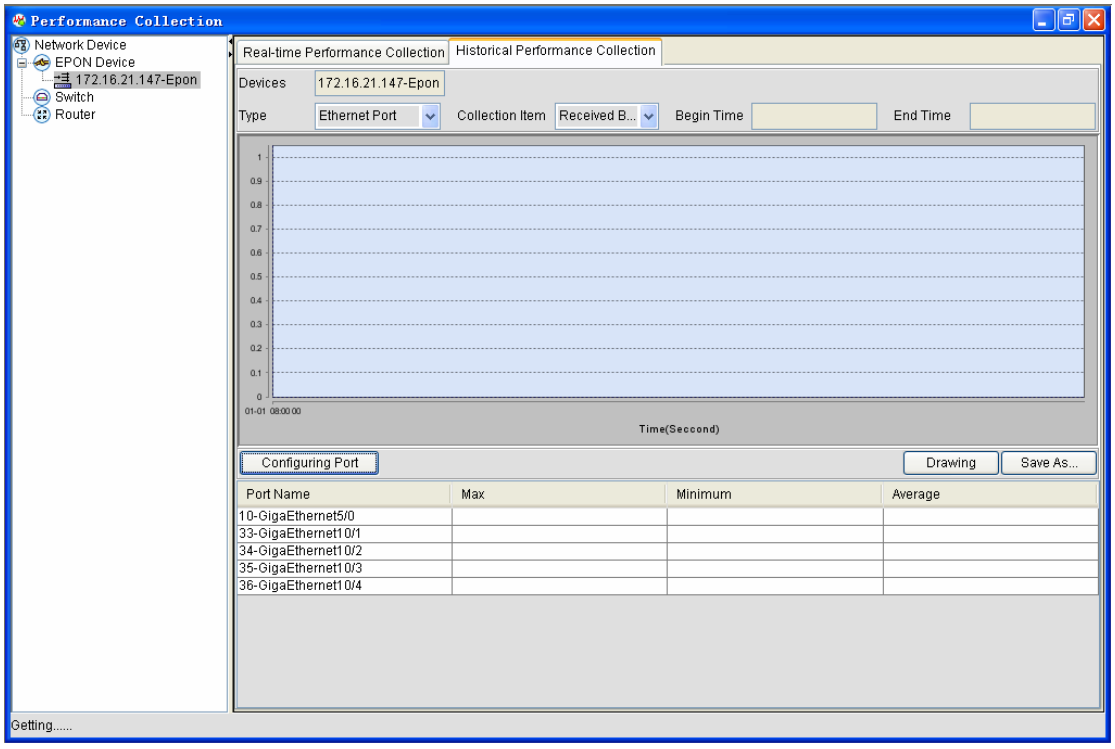
The statistics items corresponding to the EPON port are **Number of received correct packets**, **Number of transmitted correct packets**, **Number of received error packets**, **Number of transmitted error packets** and as well as all statistics items of the Ethernet port.

7.2.2 Historical Performance Statistics

Historical performace statistics means to browse the data of a device during a past period.The statistics procedure is performed by the back-stage program of the NMS and the statistics interval is generally 300 seconds.

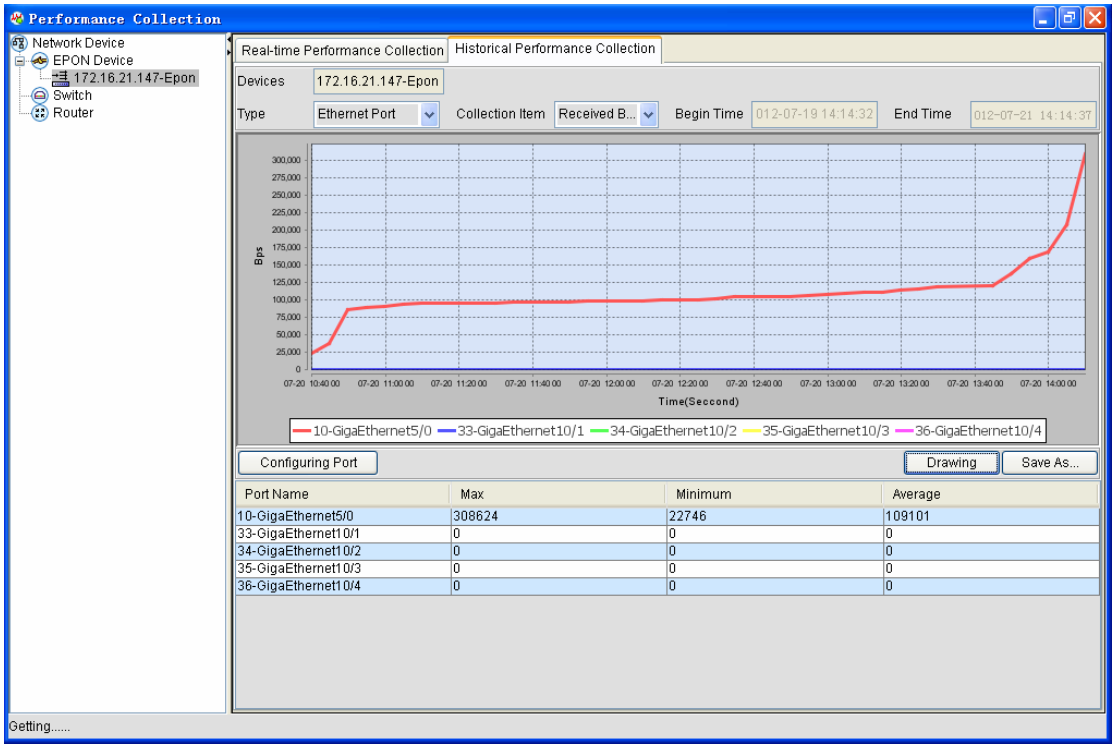
Click **Historical performance statistics**. The **Historical performance statistics** window appears, as shown in the following figure:





Like real-time performance statistics in the previous section, you have to set the statistics items before browsing the data.

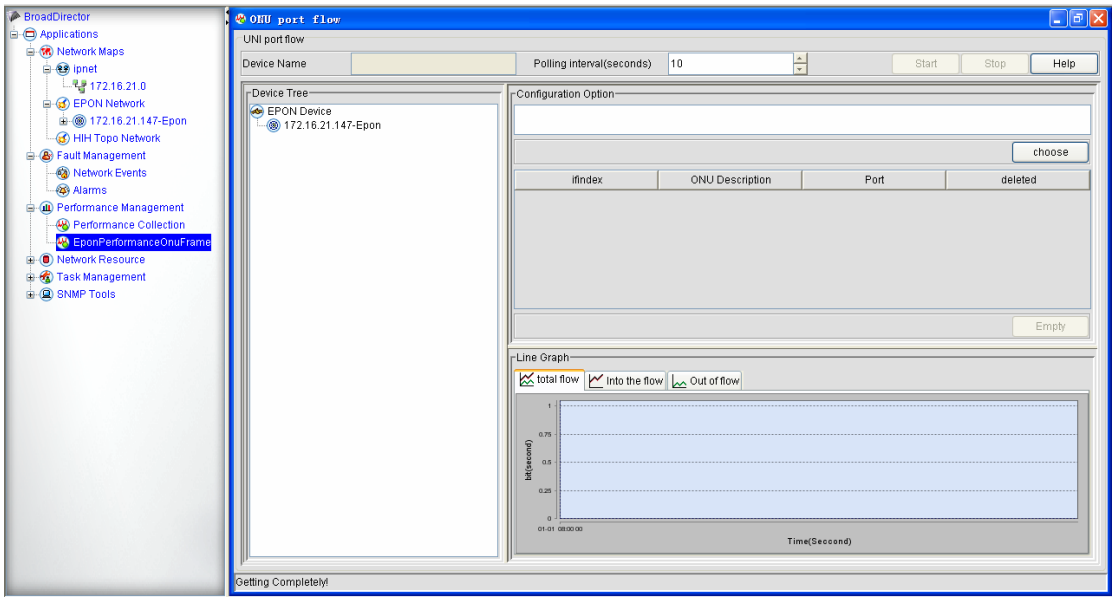
If you click **Draw map**, the historical data of all ports will be presented in the list.The following figure shows that the data is being read.



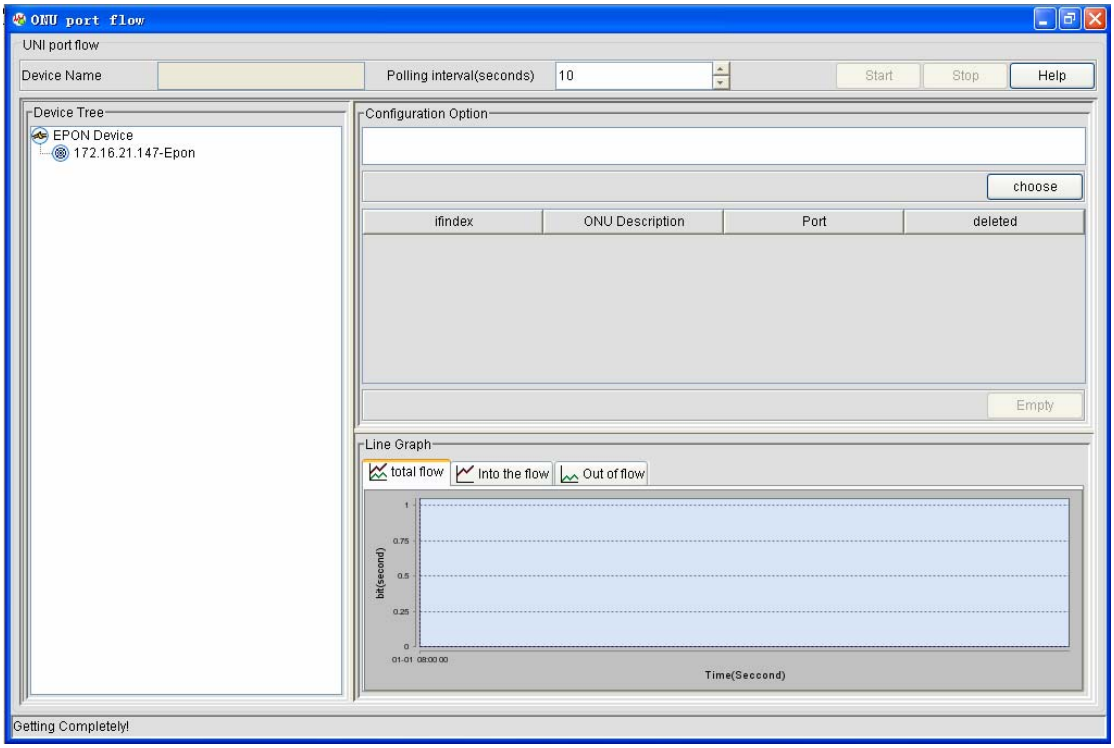
7.3 ONU Port's Flow

ONU port's flow is designed for users to know the ONU flow in time.This function is only for ONU and the displayed data are all real-time data.

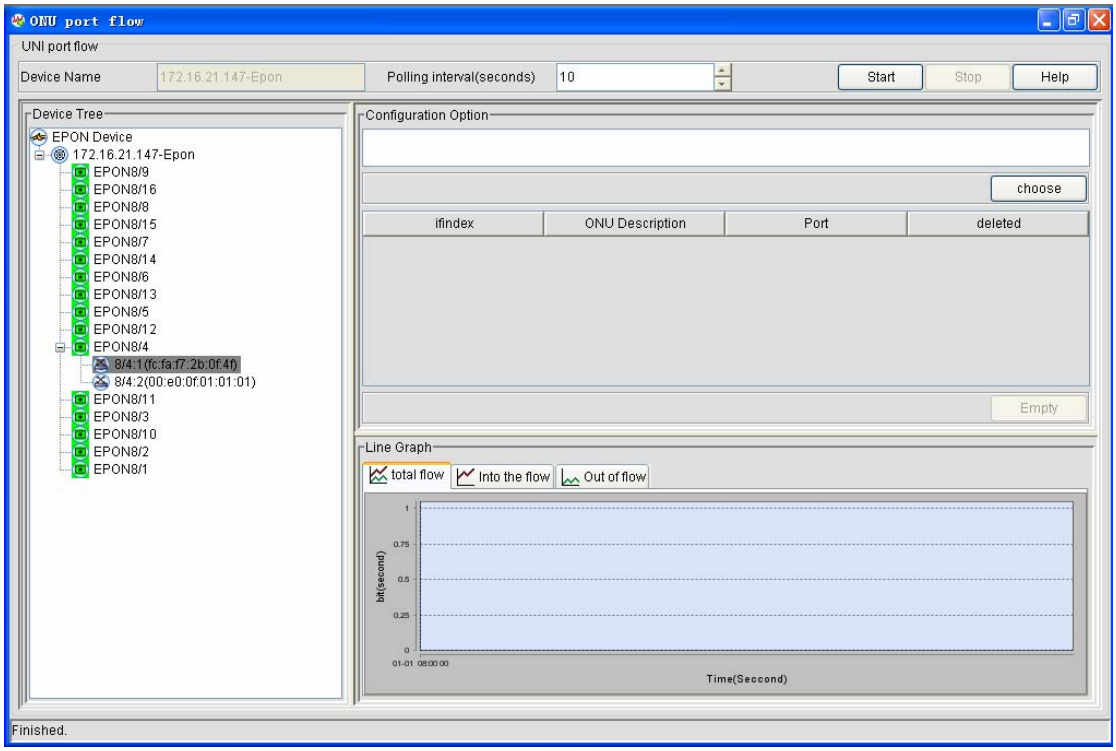
Click **ONU port's flow**, as shown in the following figure:



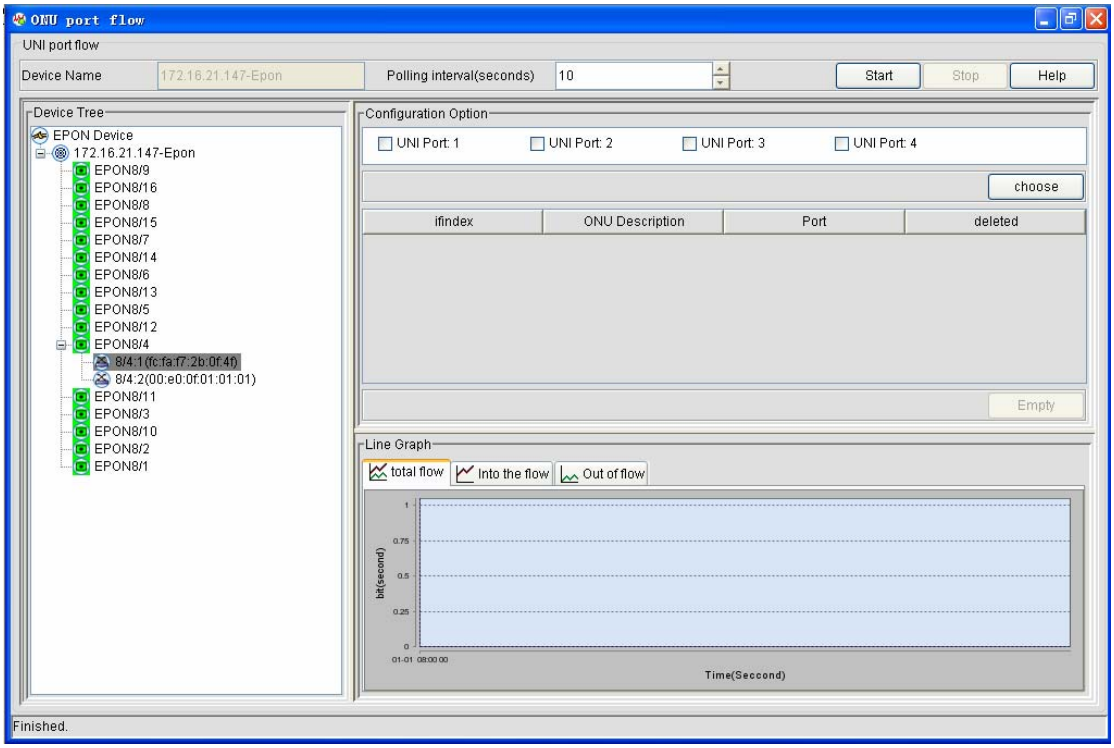
The **OUN port's flow** page appears, as shown in the following figure:



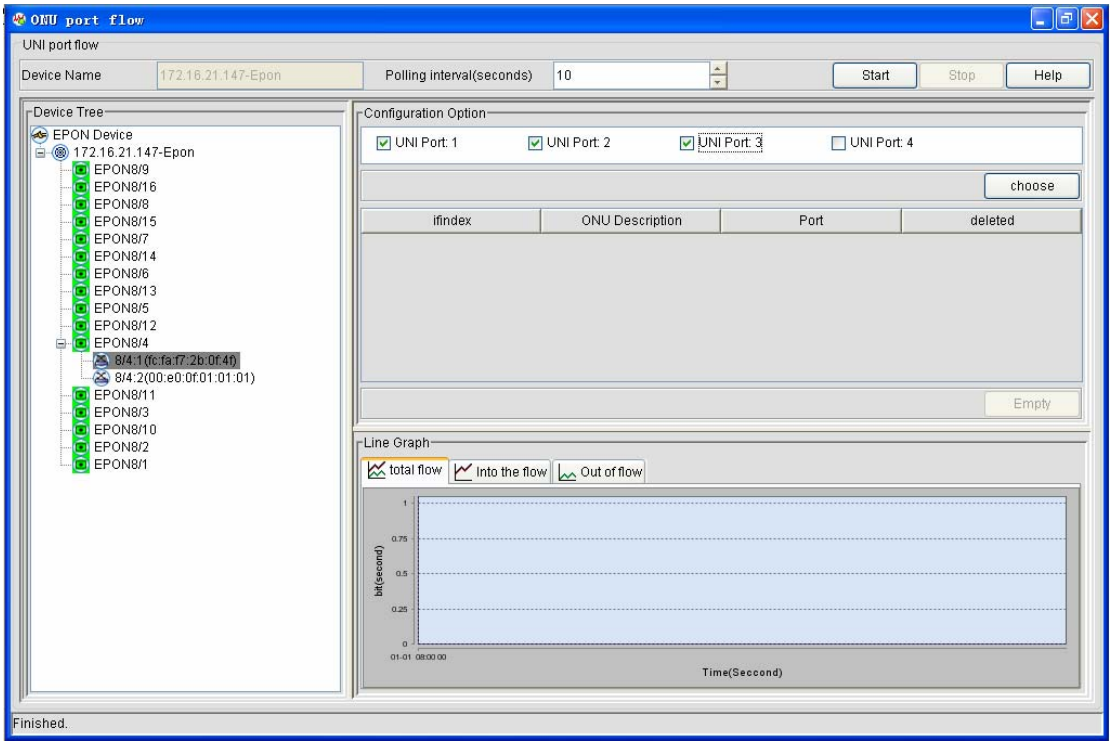
The left part of the above-mentioned figure shows the device tree list, where only EPONs are supported.If you double click EPON, its PON ports and their mounted ONUs are listed out. See the following figure:



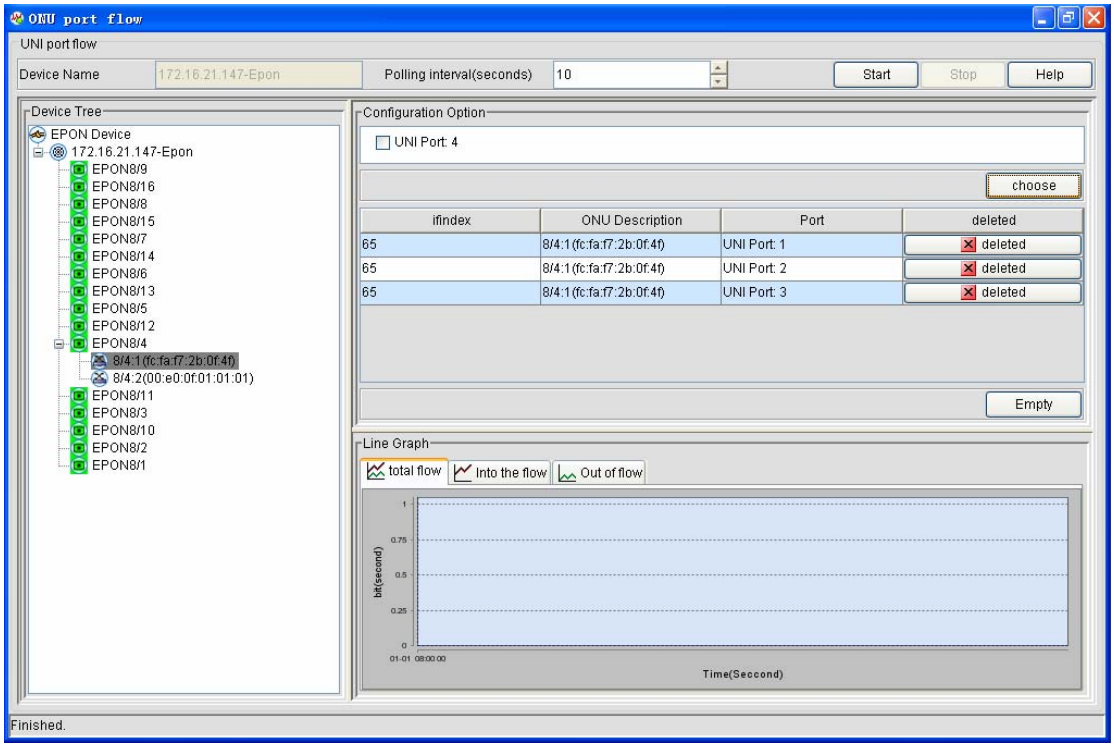
If you then double click an ONU, the ports of this ONU will be displayed on the left part.



In the left part, that is, the **Configuration choice** sub-window, you can choose the port whose flow you want to check:

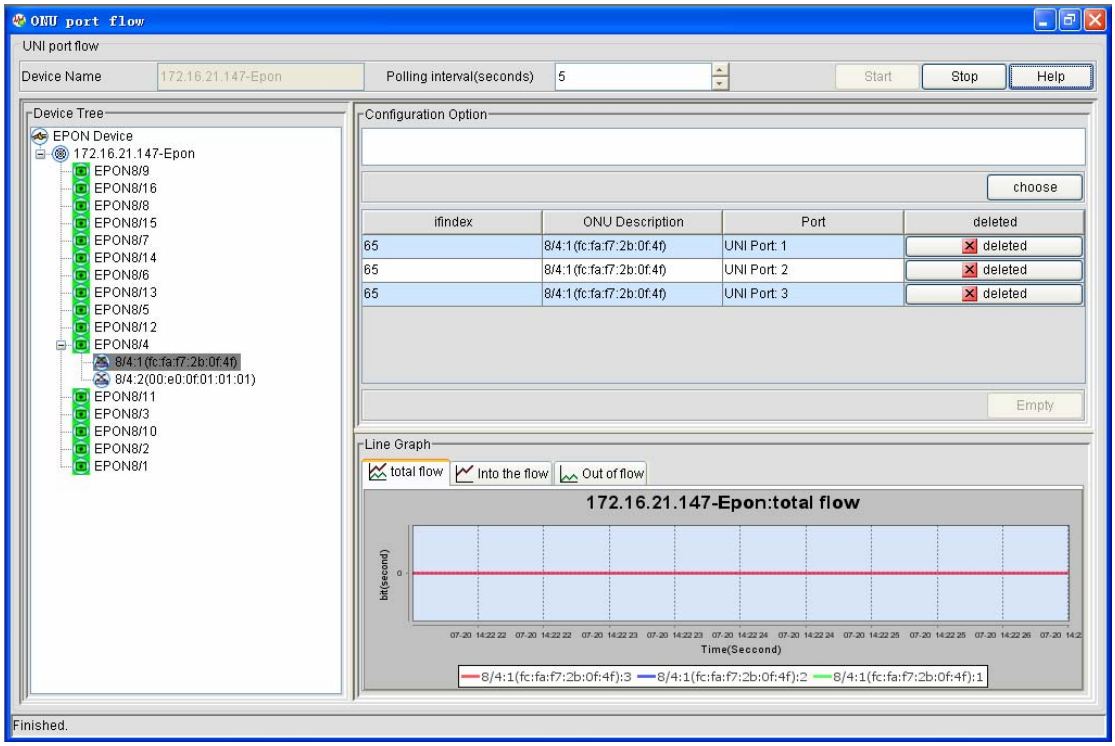


Click **Select**. A page appears, as shown in the following figure:



In the above-mentioned figure, there still exists a port, which is not selected during statistics.If you want to delete a chosen port, click **delete**.

Select **Polling interval** and click **Begin**. The system will make statistics of the flows of all ports in the list.The broken line at the right bottom part will shows the changes of these data:



The broken line contains three options: **Total traffic**, **Incoming traffic** and **Outgoing traffic**.You can click each of them to see the statistics data of the three traffics.

If you want to reselect ports or ONUs, you shall stop statistics and repeat the above-mentioned statistics procedure. To stop statistics, please click **Stop**.

8 Network Resource

Network resource is also called as Resource management. It is to summarize the basic attributes and project information about the currently discovered and managed devices and their related devices. They can be classified into 4 types according to the device type:

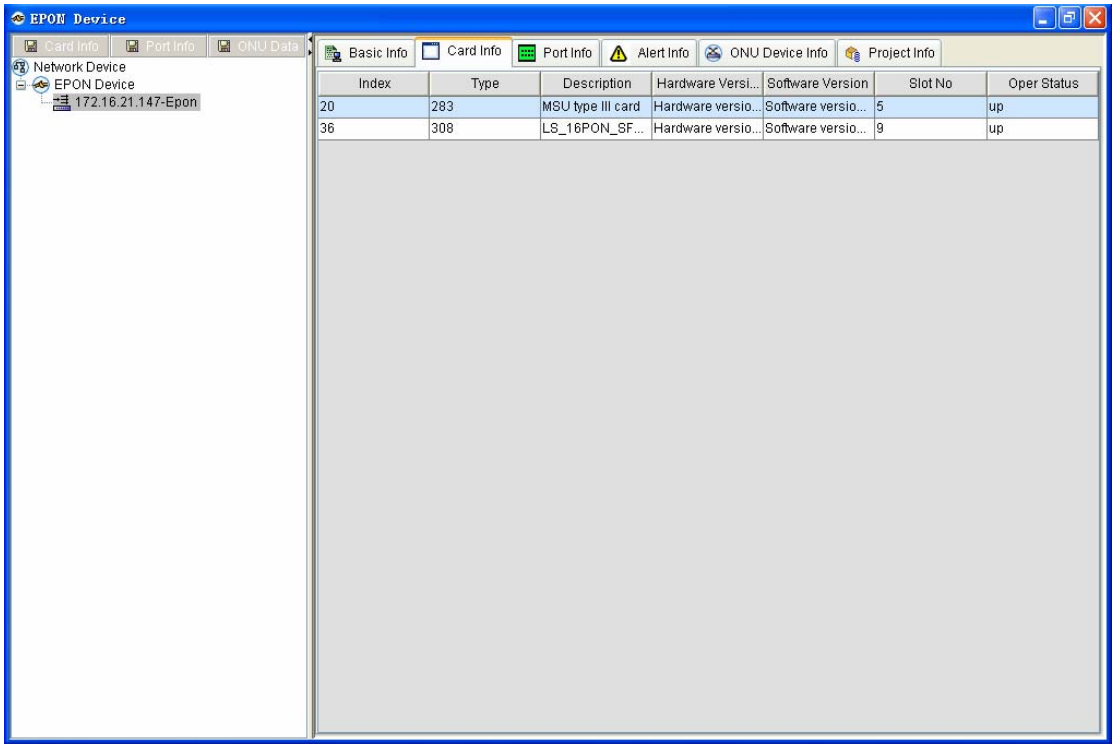
- EPON devices
- Switches
- Routers
- ONU devices

It deserves special attention that NMS in the EPON devices supports the backup of the project information (saving as the Excel list), which will be described in detail.

8.1 EPON Devices

The EPON devices include EPON OLTs and EPON ONUs, which summarize and manage uniquely all the managed devices in the current EPON network.

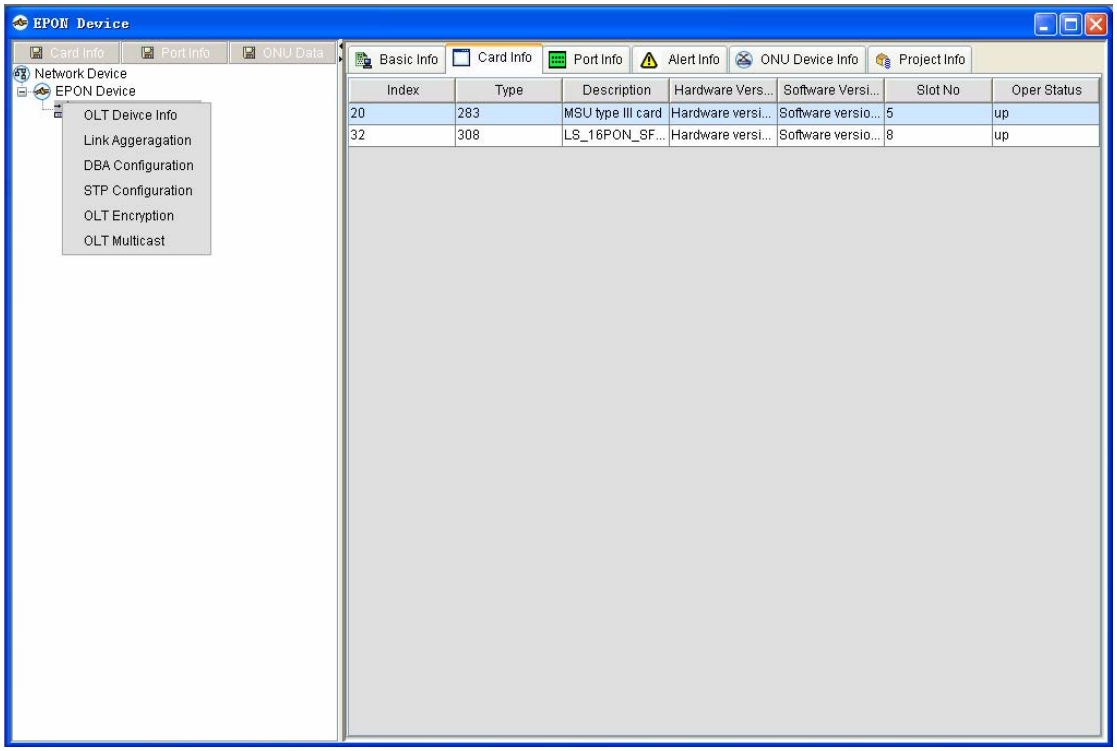
The NMS can automatically obtain EPON OLTs and present them in the device tree on the left, as shown in the following figure:



You can find from the above-mentioned figure that each EPON OLT has the following tabs: **Basic**

Info, **Card Info**, **Port Info**, **Alarm Info**, **ONU Info** and **Project Info**.

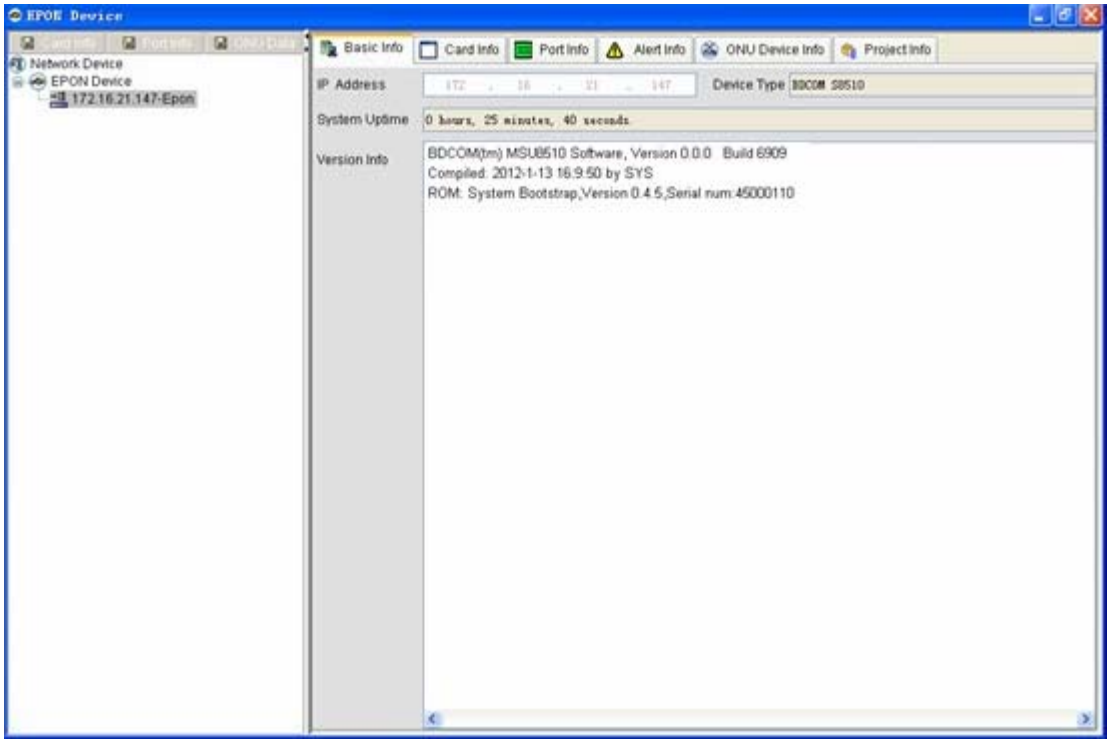
You can do some simple configuration to the current EPON OLT on the left device tree node. For example, if you click **172.16.21.147-Epon**, the following window appears and on this window you can do specific configuration.



To browse the data about an EPON OLT, you just need to click this EPON OLT icon in the left tree node. The system then automatically reads the corresponding data according to the chosen device name and displays them in the right sub-window.The following sections all take **172.16.21.147-Epon** as example.

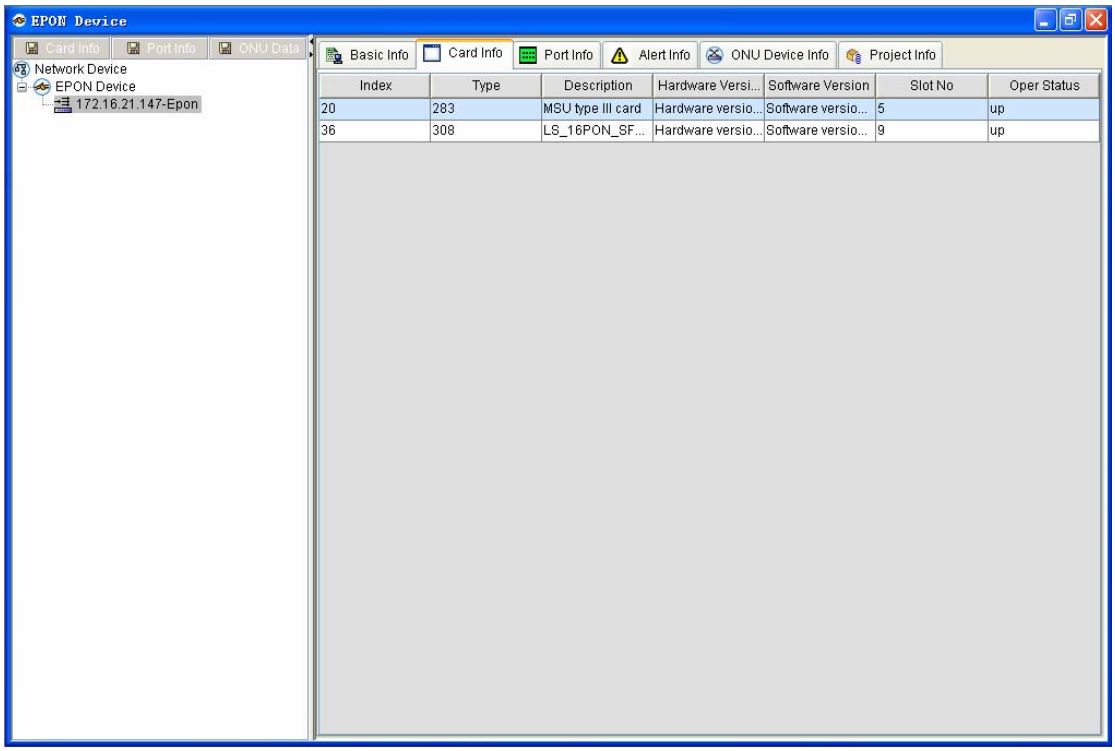
8.1.1 Basic Info

The basic information about the current EPON OLT includes the IP, the device type, the running time, and the version.

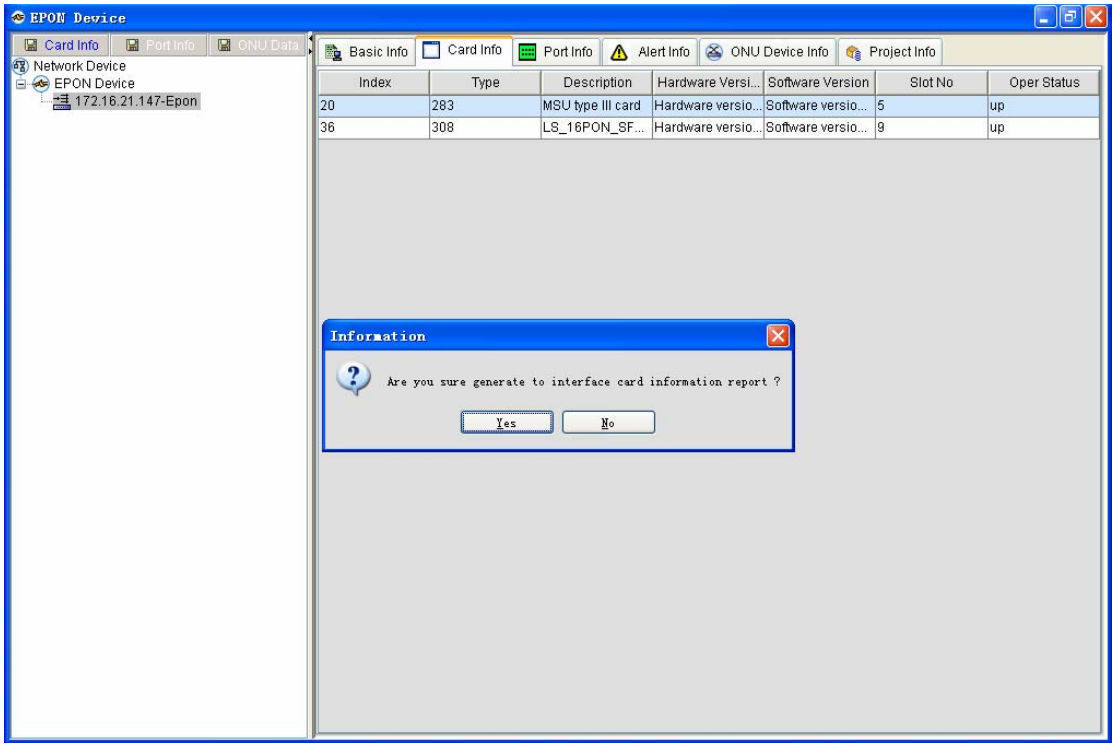


8.1.2 Card Info

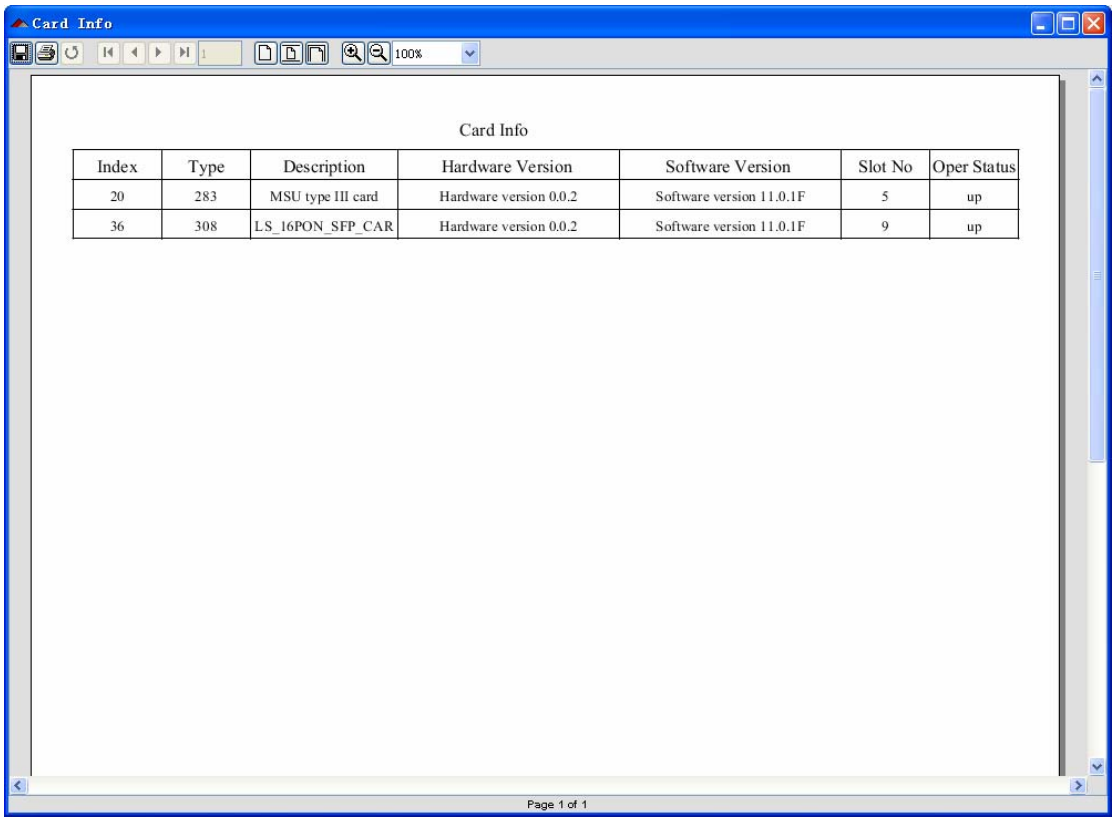
The card information refers to the basic data of one or multiple cards on the current EPON OLT. The system presents the basic data of each card to users, as shown in the following figure:



Additionally, the card-info form can also be obtained.To obtain the card-info form, choose the corresponding device and then click **Card-info form**;



Click **Yes**.

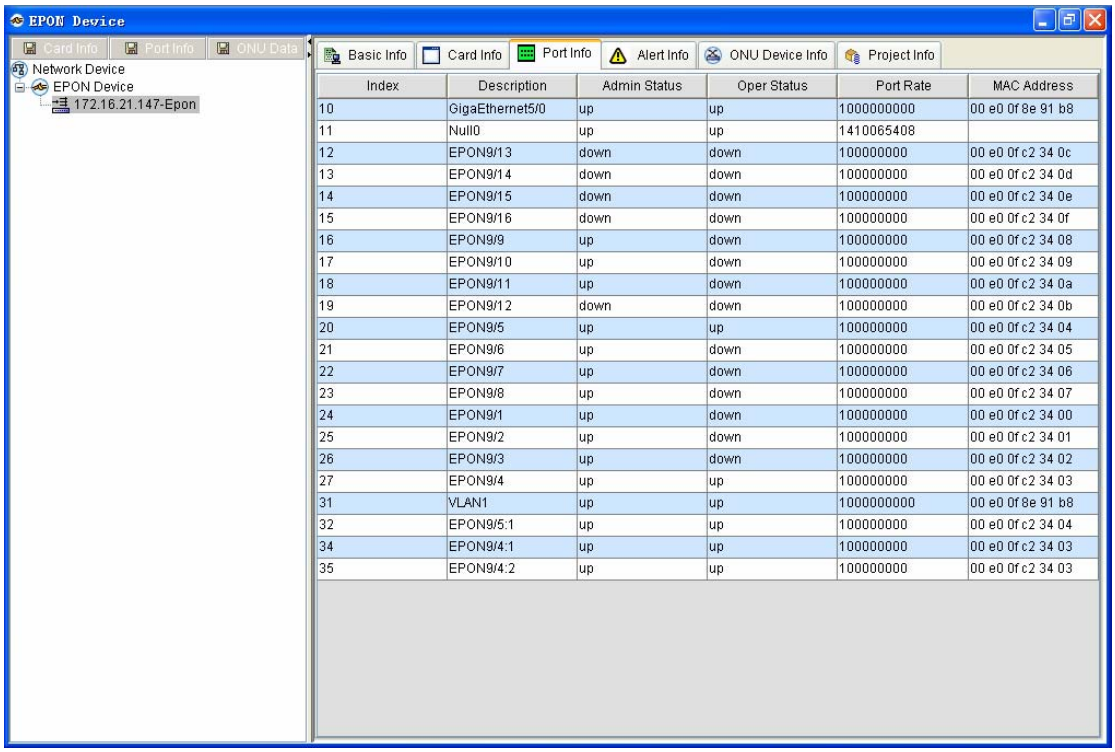


The card-info form is displayed.To save this form, click  .

Select **File type** and name this form.

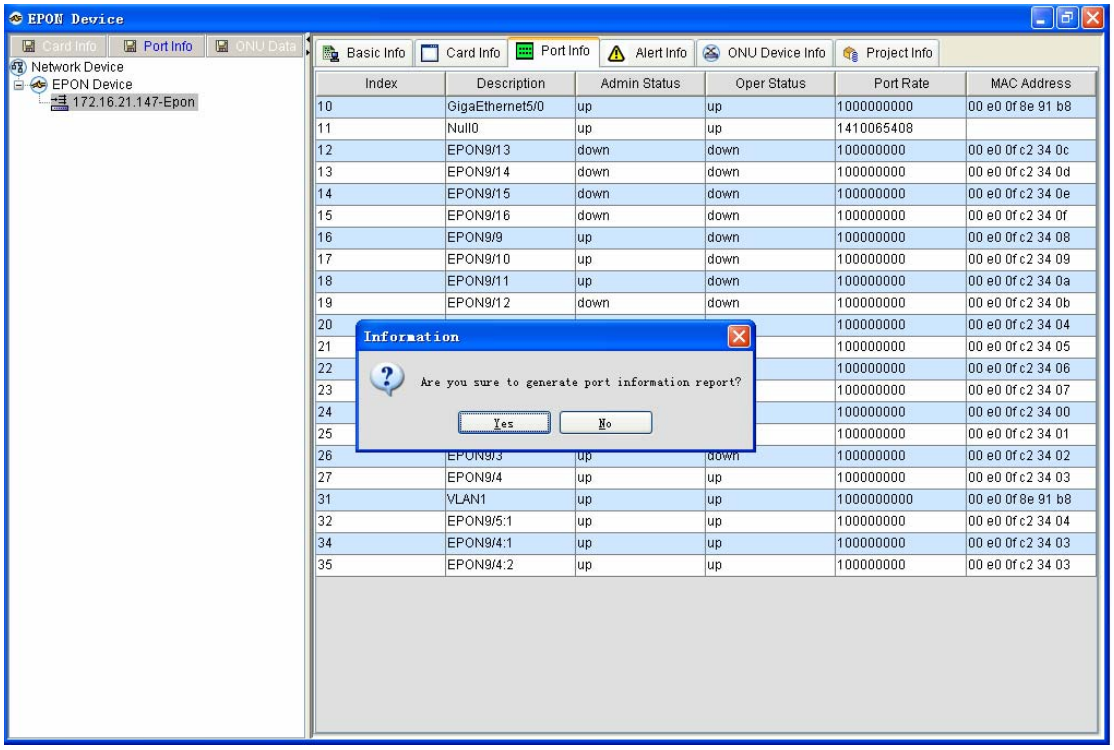
8.1.3 Port Info

Port information refers to the basic information about the ports on EPON OLT, including **Index**, **Description**, **Management status**, **Operation status**, **Port's rate** and **MAC**.



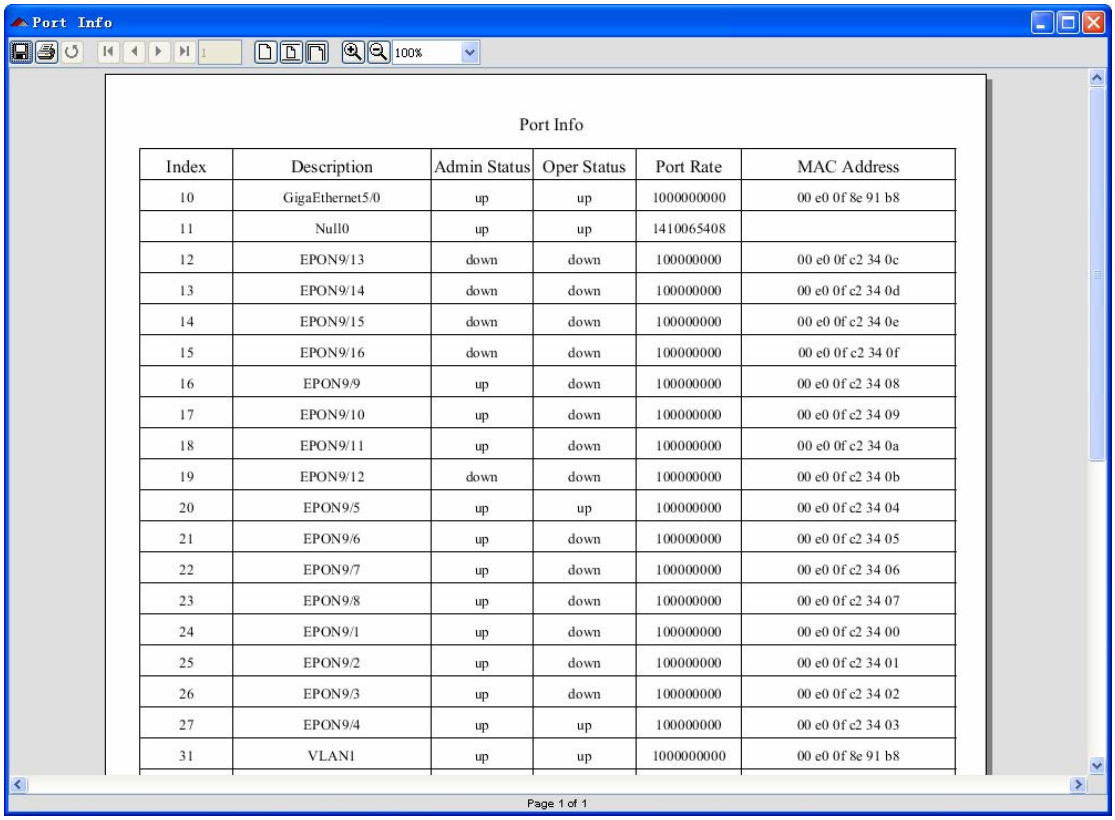
Index	Description	Admin Status	Oper Status	Port Rate	MAC Address
10	GigaEthernet5/0	up	up	1000000000	00 e0 0f 8e 91 b8
11	Null0	up	up	1410065408	
12	EPON9/13	down	down	100000000	00 e0 0f c2 34 0c
13	EPON9/14	down	down	100000000	00 e0 0f c2 34 0d
14	EPON9/15	down	down	100000000	00 e0 0f c2 34 0e
15	EPON9/16	down	down	100000000	00 e0 0f c2 34 0f
16	EPON9/9	up	down	100000000	00 e0 0f c2 34 08
17	EPON9/10	up	down	100000000	00 e0 0f c2 34 09
18	EPON9/11	up	down	100000000	00 e0 0f c2 34 0a
19	EPON9/12	down	down	100000000	00 e0 0f c2 34 0b
20	EPON9/5	up	up	100000000	00 e0 0f c2 34 04
21	EPON9/6	up	down	100000000	00 e0 0f c2 34 05
22	EPON9/7	up	down	100000000	00 e0 0f c2 34 06
23	EPON9/8	up	down	100000000	00 e0 0f c2 34 07
24	EPON9/1	up	down	100000000	00 e0 0f c2 34 00
25	EPON9/2	up	down	100000000	00 e0 0f c2 34 01
26	EPON9/3	up	down	100000000	00 e0 0f c2 34 02
27	EPON9/4	up	up	100000000	00 e0 0f c2 34 03
31	VLAN1	up	up	1000000000	00 e0 0f 8e 91 b8
32	EPON9/5:1	up	up	100000000	00 e0 0f c2 34 04
34	EPON9/4:1	up	up	100000000	00 e0 0f c2 34 03
35	EPON9/4:2	up	up	100000000	00 e0 0f c2 34 03

Additionally, the port-info form can also be obtained.To obtain the port-info form, choose the corresponding device and then click **Port-info form**.See the following figure:



Index	Description	Admin Status	Oper Status	Port Rate	MAC Address
10	GigaEthernet5/0	up	up	1000000000	00 e0 0f 8e 91 b8
11	Null0	up	up	1410065408	
12	EPON9/13	down	down	100000000	00 e0 0f c2 34 0c
13	EPON9/14	down	down	100000000	00 e0 0f c2 34 0d
14	EPON9/15	down	down	100000000	00 e0 0f c2 34 0e
15	EPON9/16	down	down	100000000	00 e0 0f c2 34 0f
16	EPON9/9	up	down	100000000	00 e0 0f c2 34 08
17	EPON9/10	up	down	100000000	00 e0 0f c2 34 09
18	EPON9/11	up	down	100000000	00 e0 0f c2 34 0a
19	EPON9/12	down	down	100000000	00 e0 0f c2 34 0b
20				100000000	00 e0 0f c2 34 04
21				100000000	00 e0 0f c2 34 05
22				100000000	00 e0 0f c2 34 06
23				100000000	00 e0 0f c2 34 07
24				100000000	00 e0 0f c2 34 00
25				100000000	00 e0 0f c2 34 01
26	EPON9/3	up	down	100000000	00 e0 0f c2 34 02
27	EPON9/4	up	up	100000000	00 e0 0f c2 34 03
31	VLAN1	up	up	1000000000	00 e0 0f 8e 91 b8
32	EPON9/5:1	up	up	100000000	00 e0 0f c2 34 04
34	EPON9/4:1	up	up	100000000	00 e0 0f c2 34 03
35	EPON9/4:2	up	up	100000000	00 e0 0f c2 34 03

Click **Yes**.



Index	Description	Admin Status	Oper Status	Port Rate	MAC Address
10	GigaEthernet5/0	up	up	1000000000	00 e0 0f 8e 91 b8
11	Null0	up	up	1410065408	
12	EPON9/13	down	down	100000000	00 e0 0f c2 34 0c
13	EPON9/14	down	down	100000000	00 e0 0f c2 34 0d
14	EPON9/15	down	down	100000000	00 e0 0f c2 34 0e
15	EPON9/16	down	down	100000000	00 e0 0f c2 34 0f
16	EPON9/9	up	down	100000000	00 e0 0f c2 34 08
17	EPON9/10	up	down	100000000	00 e0 0f c2 34 09
18	EPON9/11	up	down	100000000	00 e0 0f c2 34 0a
19	EPON9/12	down	down	100000000	00 e0 0f c2 34 0b
20	EPON9/5	up	up	100000000	00 e0 0f c2 34 04
21	EPON9/6	up	down	100000000	00 e0 0f c2 34 05
22	EPON9/7	up	down	100000000	00 e0 0f c2 34 06
23	EPON9/8	up	down	100000000	00 e0 0f c2 34 07
24	EPON9/1	up	down	100000000	00 e0 0f c2 34 00
25	EPON9/2	up	down	100000000	00 e0 0f c2 34 01
26	EPON9/3	up	down	100000000	00 e0 0f c2 34 02
27	EPON9/4	up	up	100000000	00 e0 0f c2 34 03
31	VLAN1	up	up	1000000000	00 e0 0f 8e 91 b8

The port-info form is displayed.To save this form, click  .

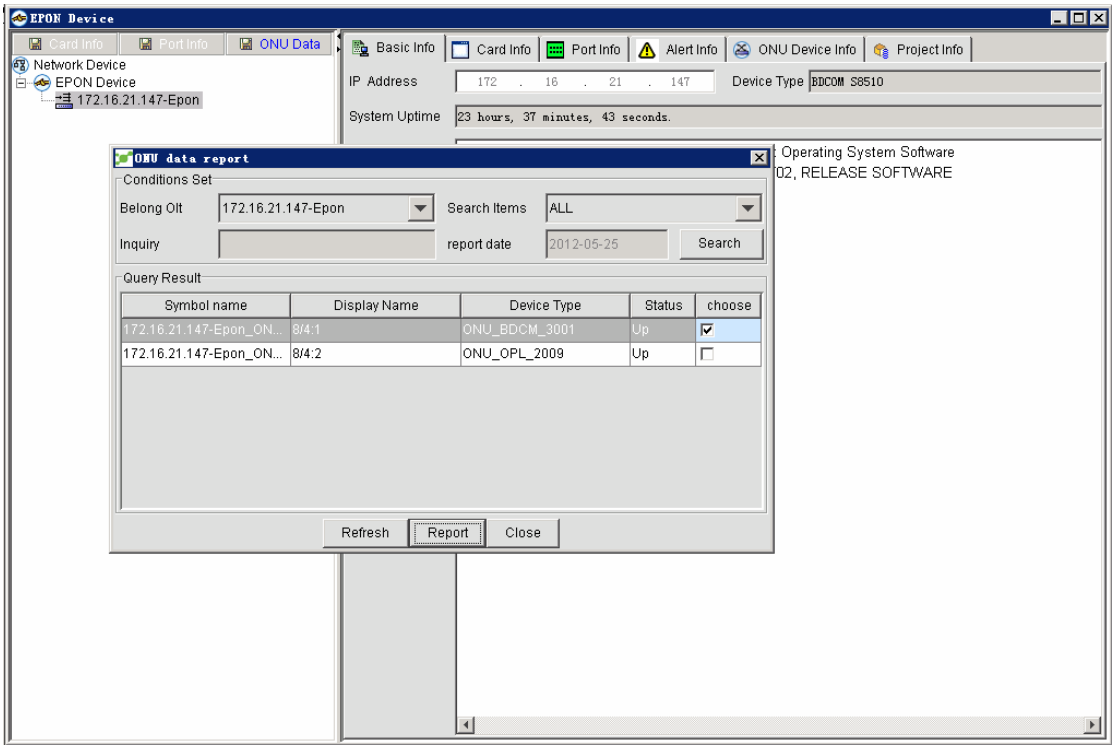
Select **File type** and name this form.

8.1.4 ONU Data Form

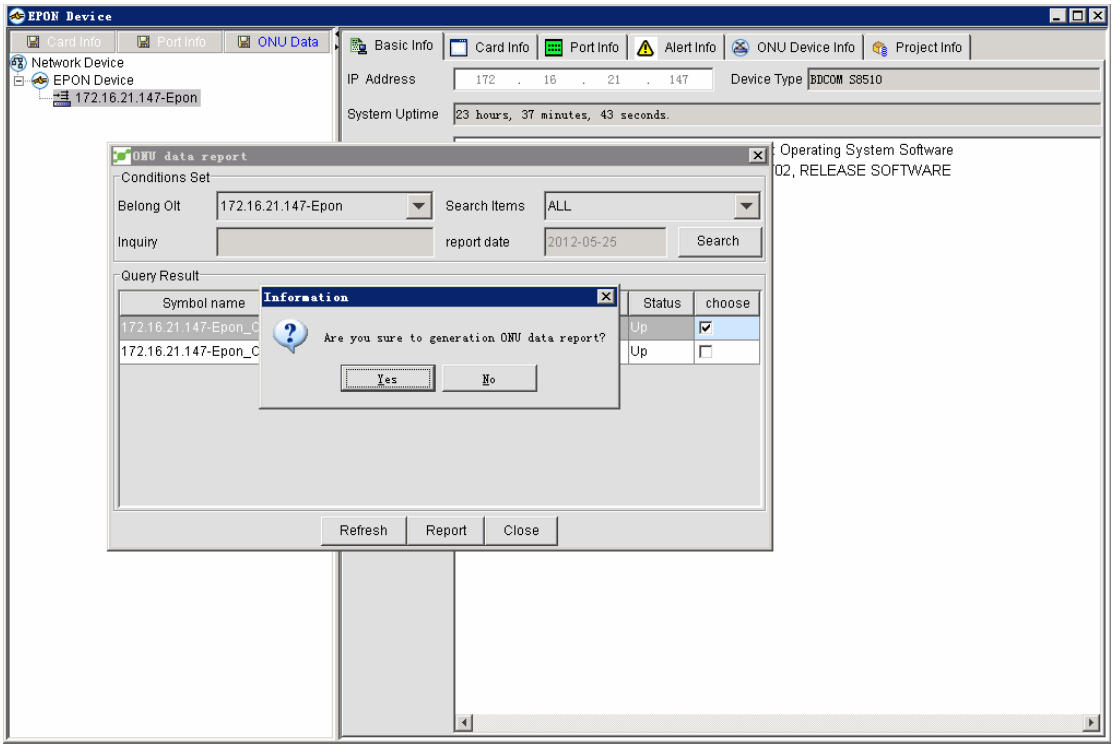
The system makes statistics of the incoming traffic and outgoing traffic on each ONU port every hour,and then draws line maps. All these will be shown in the ONU data form.

The detailed procedure is as follows:

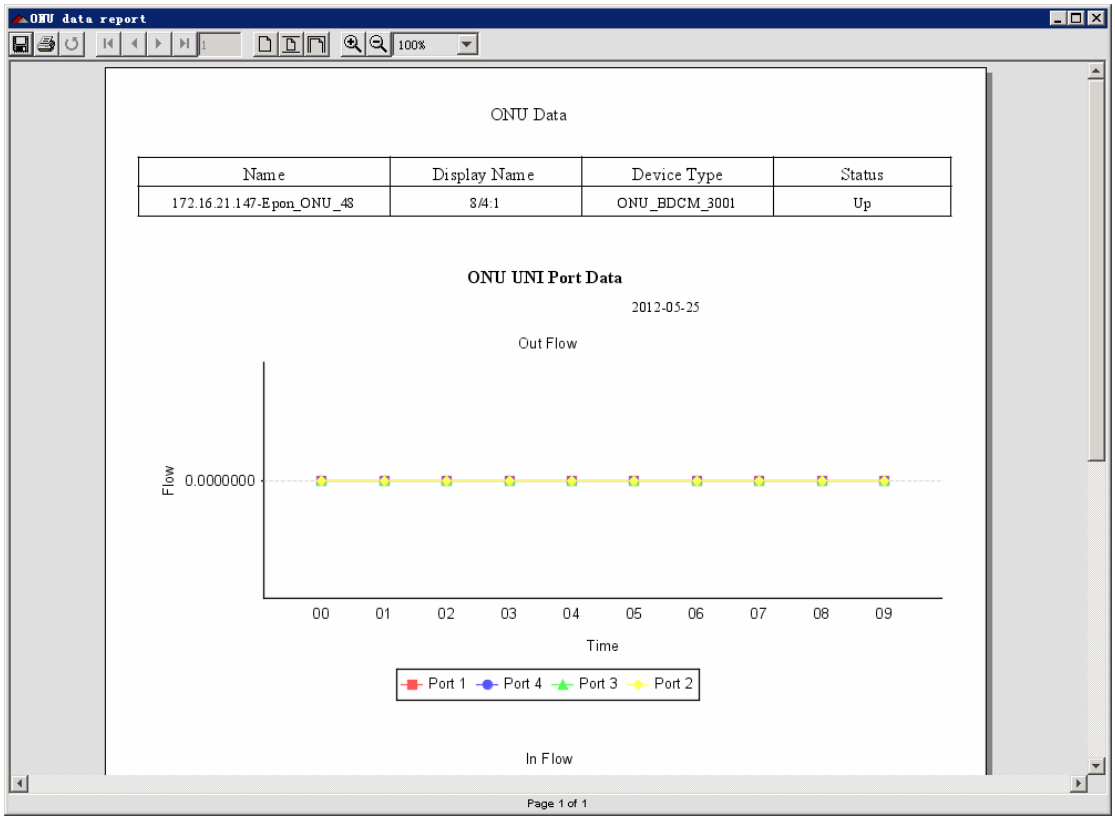
Click **Resource Management -> EPON device -> ONU data form**, as shown in the following figure:



Choose an entry in **Query Result** by ticking it and then click **Form**.See the following figure:



Click **Yes**. The form is then generated.See the following figure:

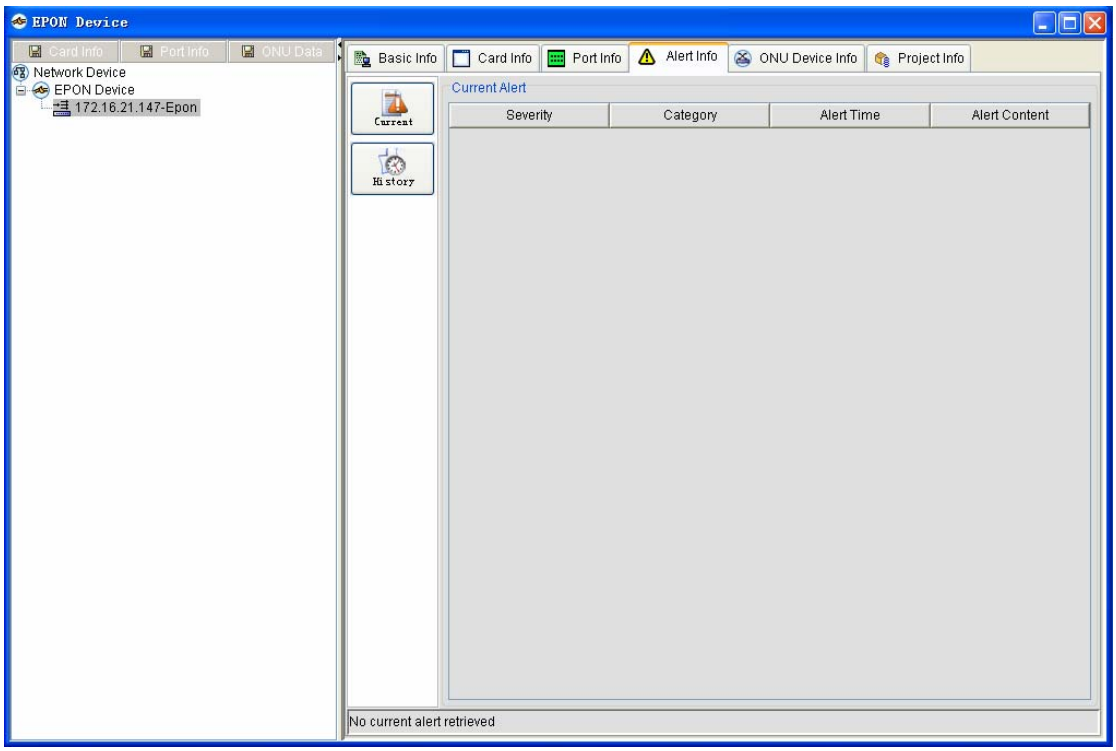


8.1.5 Alarm Info

The alarm information refers to the events and alarm indicators that the current EPON OLT sends to the NMS. The alarm information includes two parts: Current alarm information and Historical alarm information.

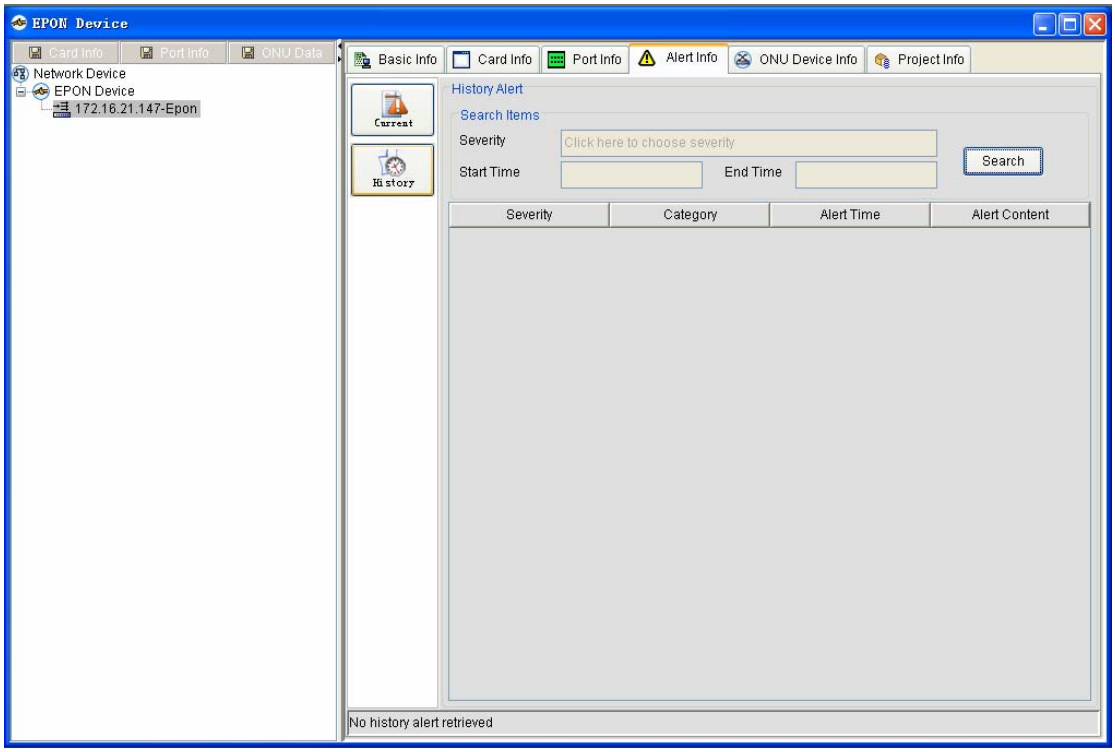
- **Current alarm**

It refers to the information that the device sends to the NMS currently, including **Alarm level**, **Alarm type**, **Alarm time**, and **Alarm content**.See the following figure:



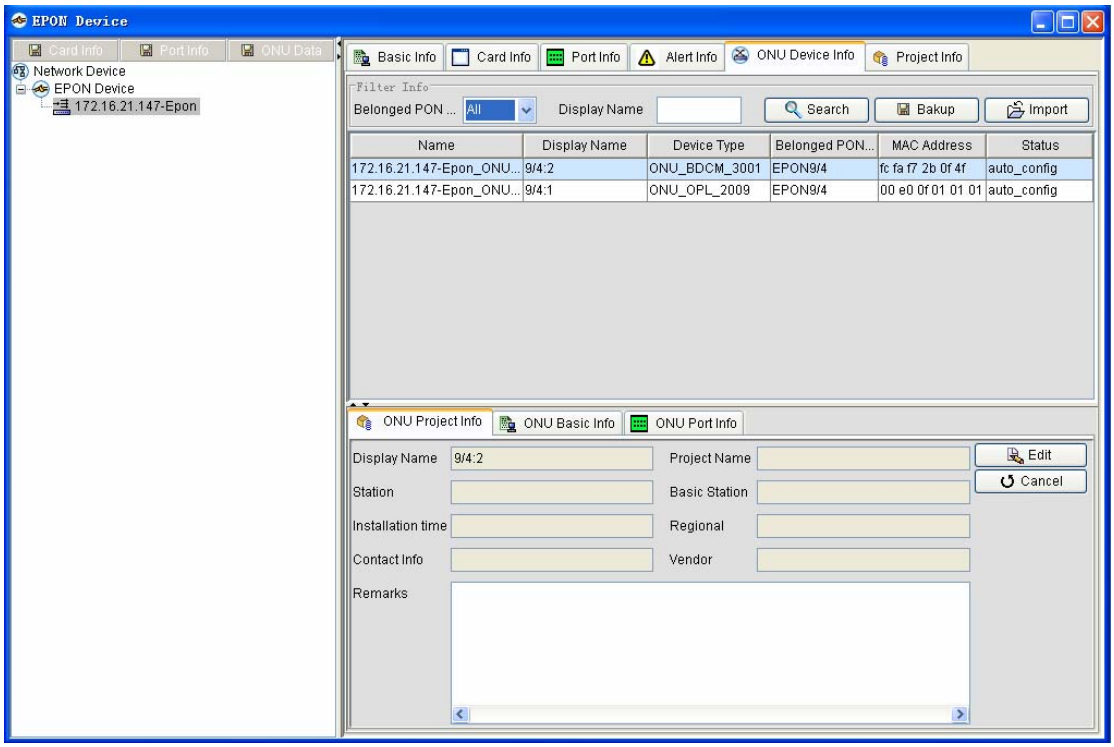
■ **Historical alarm**

It refers to the historical records of the alarms. The to-be-queried content is same to the previous section.The difference is that you can browse the alarm record according to the alarm level, the start time and the end time.See the following figure:



8.1.6 ONU Information

ONU information includes the EPON ONU summary information, EPON ONU project information, EPON ONU basic information, EPON ONU ports' information, backup and introduction of EPON ONU project information. See the following figure:



■ **EPON ONU summary**

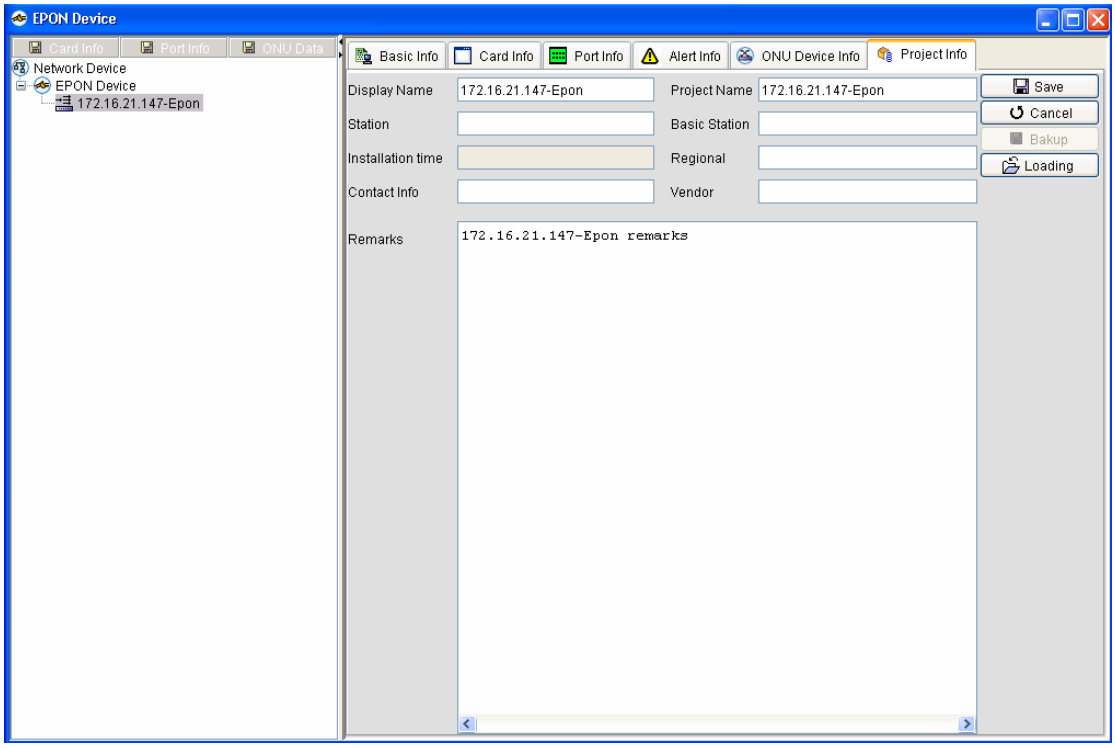
In the initialized window, the system displays all ONUs, which are connected to all PON ports of the chosen EPON OLT. ONU information includes **Name**, **Displayed Name**, **Device Type**, **PON Port**, **MAC**, and **Status**.

■ **EPON ONU project information**

If you select an ONU and double click it in the previous queried ONU list, the system will automatically read its ONU project information according to the chosen ONU name. The above-mentioned figure shows that the project information about ONU **0/4:1** is null.You can edit the project information of ONU according to actual requirements and save the project information.

Step 1: Select the t0-be-queried ONU and double click it;

Step 2: Click **Edit** on the **ONU project information** tab. All attributes of ONU project information are then available to edition, as shown in the following figure:



Step 3: Enter a value for each attribute and then click **Save**(The previous **Edit** button changes into the **Save** button). The current ONU project information is then saved.Of course you can click **Cancel** not to save the current settings.

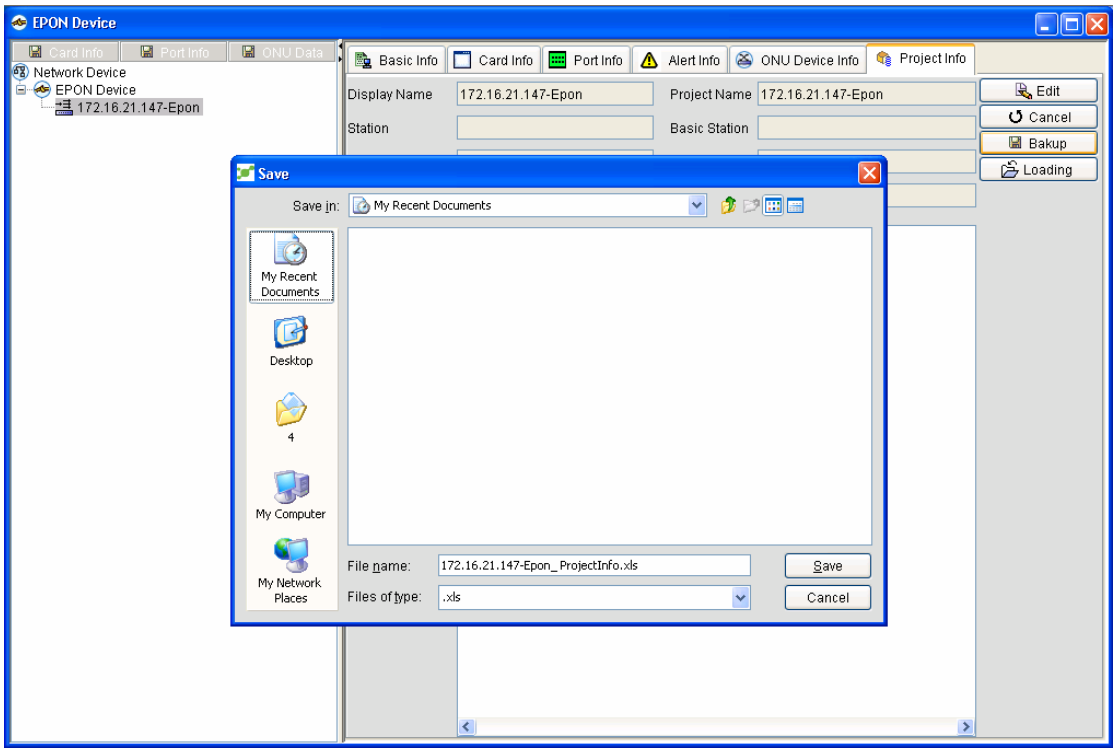
The **Backup** and **Import** functions are also provided for the EPON ONU project information.

✧ **Backup**

Backup means to save all the EPON ONU project information in the EXCEL format, which will be used as the import file later.

Step1: Click **Backup** after the EPON ONU project is modified and saved.

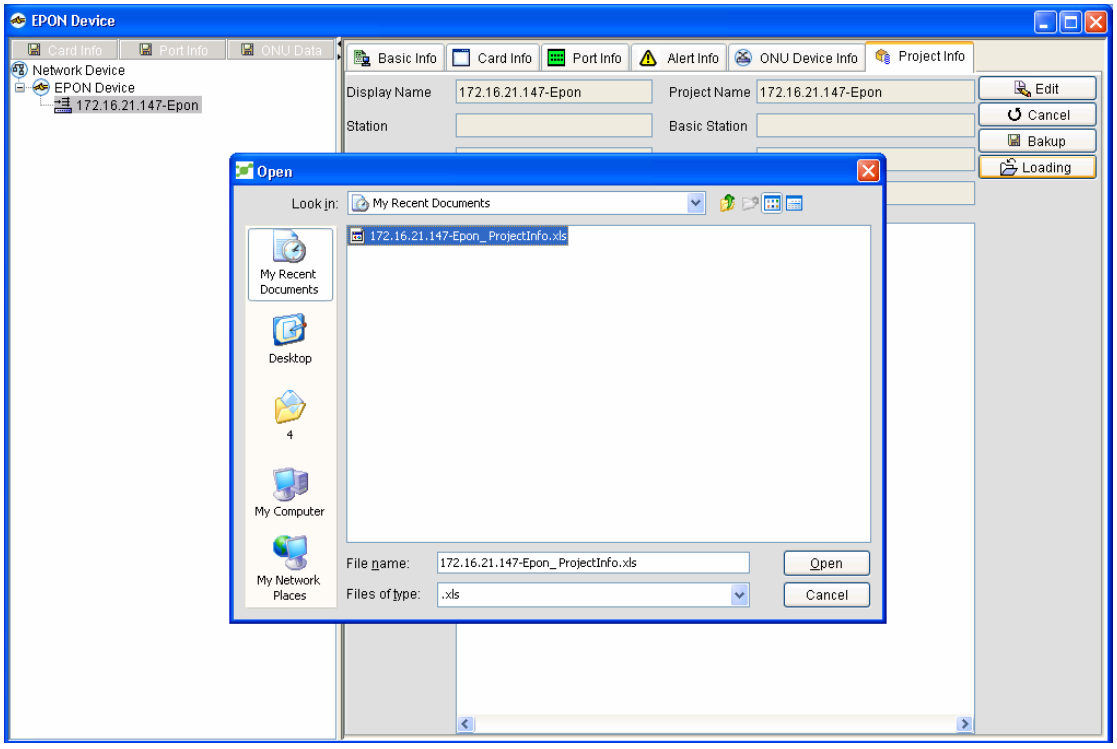
Step2: Specify the backup file's storage location and name in the corresponding dialog box, as shown in the following figure:



Note: If there is no special need, do not change the content of the backup file, or the import of the ONU project information will fail.

✧ **Import**

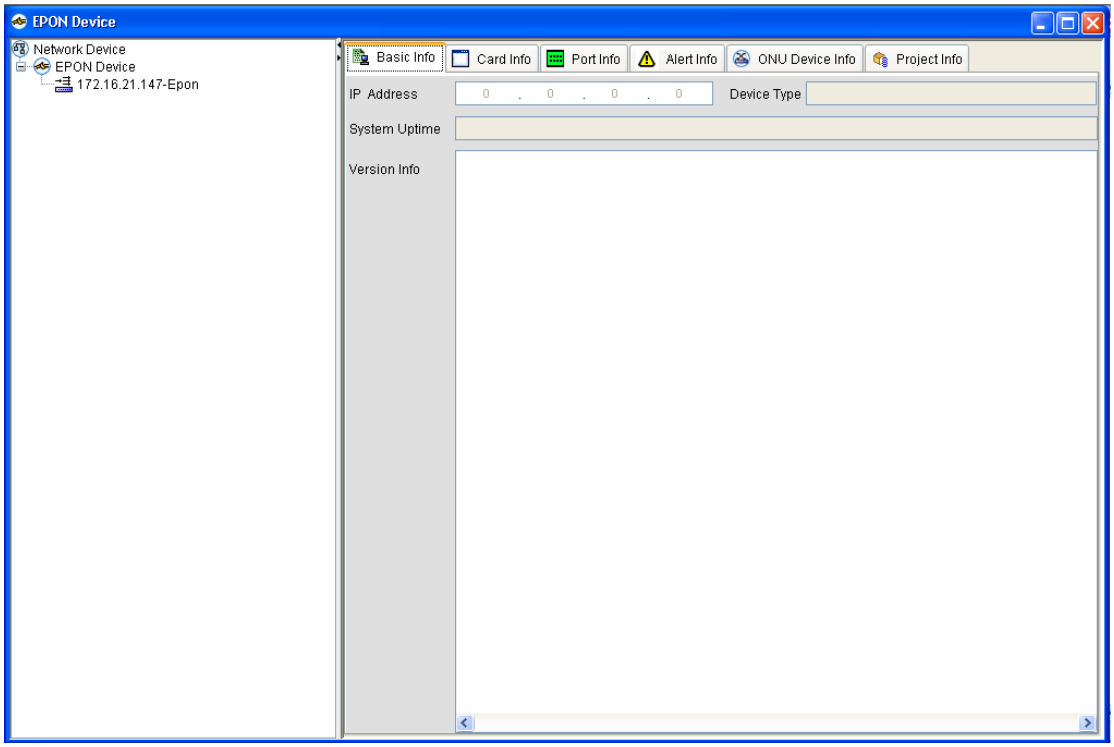
Import means to upload the stored EPON ONU project file to the system, avoiding the trouble of editing EPON ONU project information one by one. Click **Import** and select the to-be-imported file in the following dialog box.



■ **EPON ONU basic information**

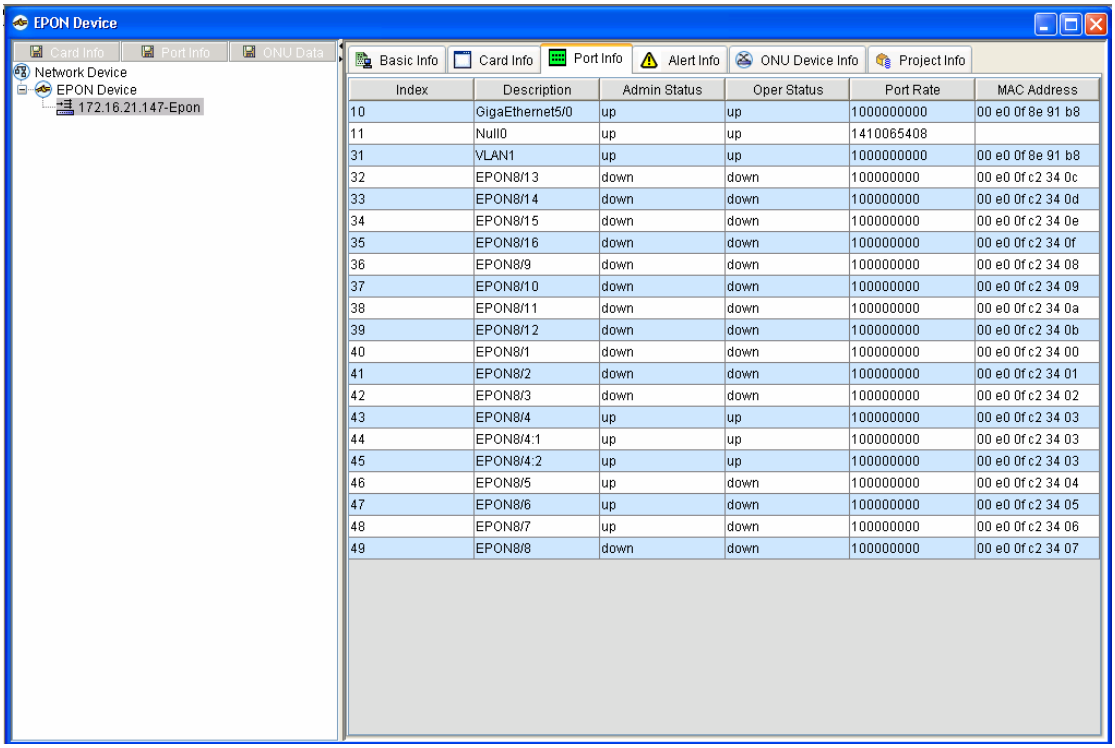
After you edit and save the EPON ONU project information, click the **Basic info** tab. The system

will then read the corresponding device information automatically according to the chosen ONU's name, as shown in the following figure:

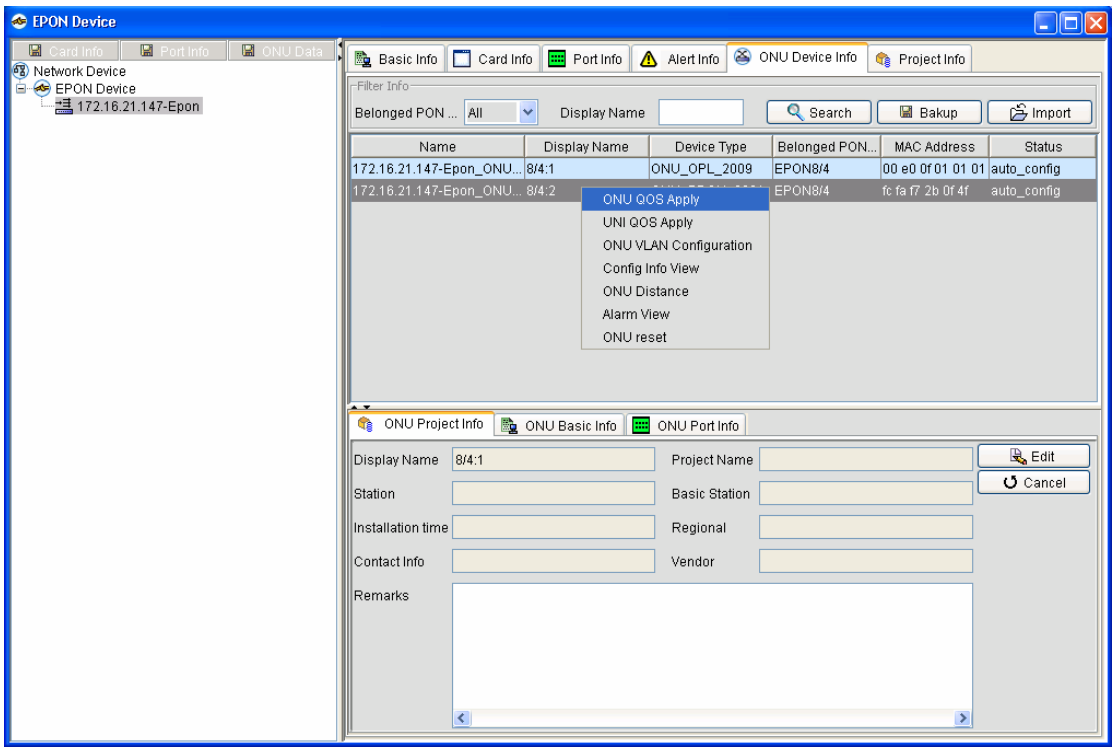


■ **EPON ONU port information**

If you click the **ONU port info** tab, you can obtain the port's information.

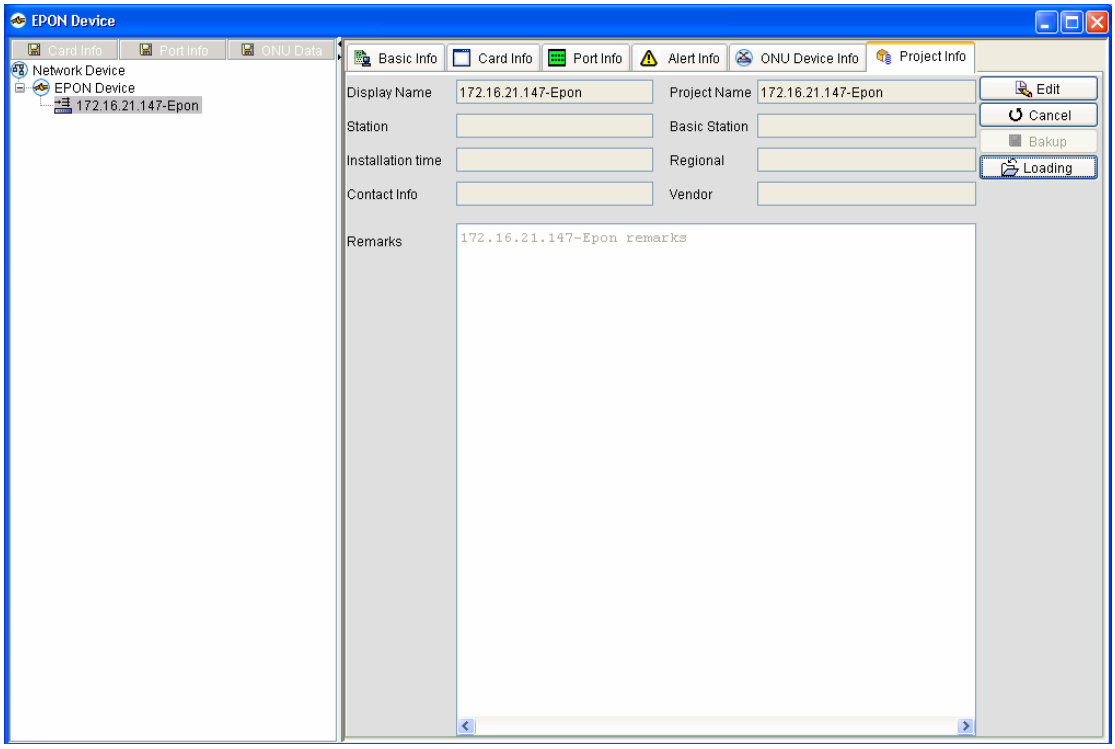


Note: In the right-key menu of **ONU information**, you can conduct the basic EPON settings to the currently chosen ONU.See the following figure:



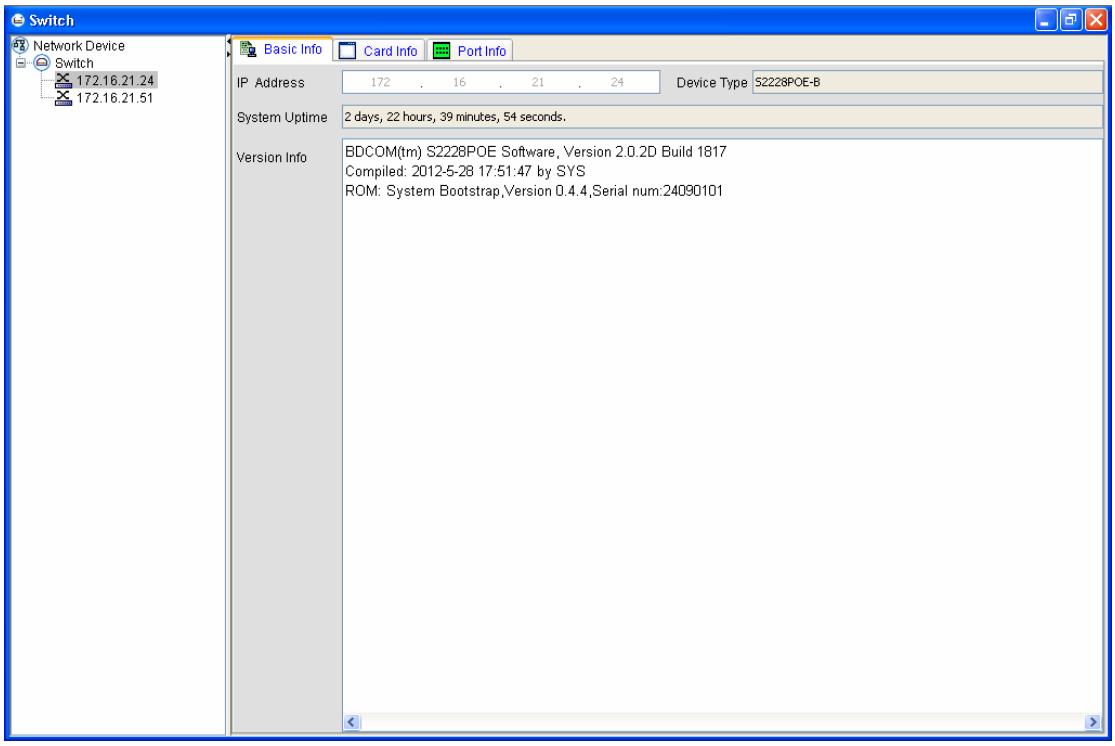
8.1.7 Project Information

Here it means the EPON OLT project information. Its operations are same to those of the EPON ONU project information. For related operations, refer to the previous section.



8.2 Switch

This function means that the NMS uploads the discovered and managed switches to the network device node tree on the left automatically for users to browse a node's information.As shown in the following figure, you can read the switch's information, including **Basic Info**, **Card Info** and **Port Info**.Take switch 172.16.21.29 as an example:

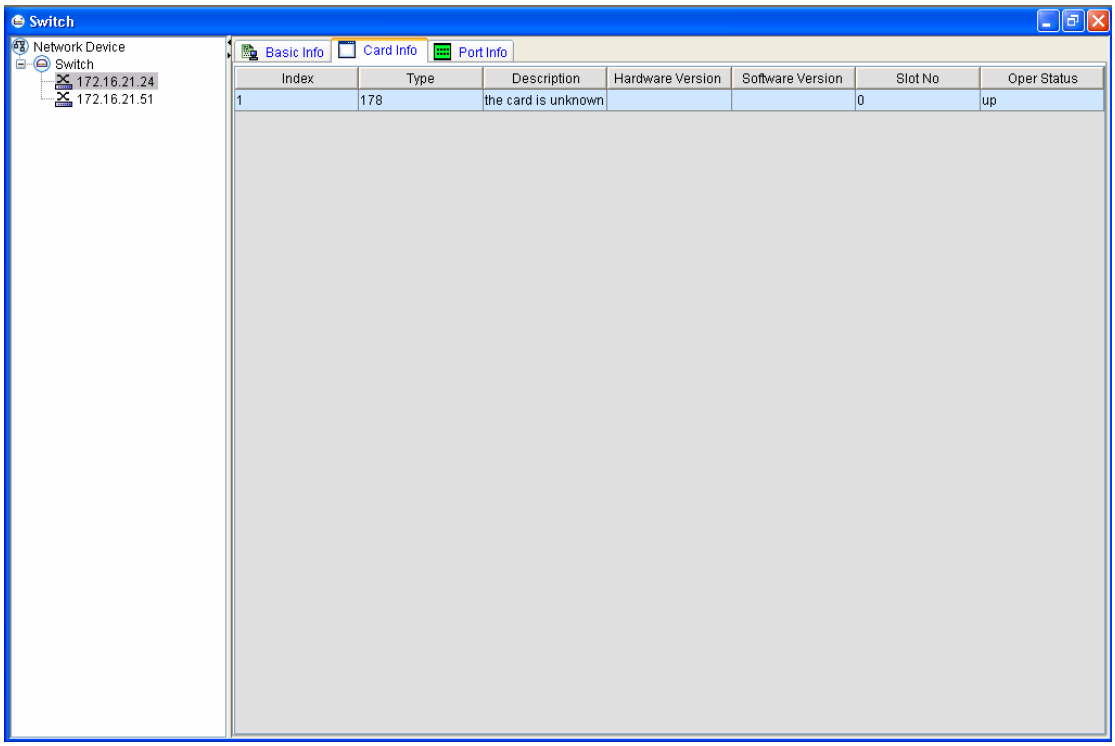


8.2.1 Basic Info

If you choose a to-be-browsed device and click it, the system will automatically read and show you the basic configuration information about this device, including **IP**, **Device Type**, **Running Time** and **Version**.

8.2.2 Card Info

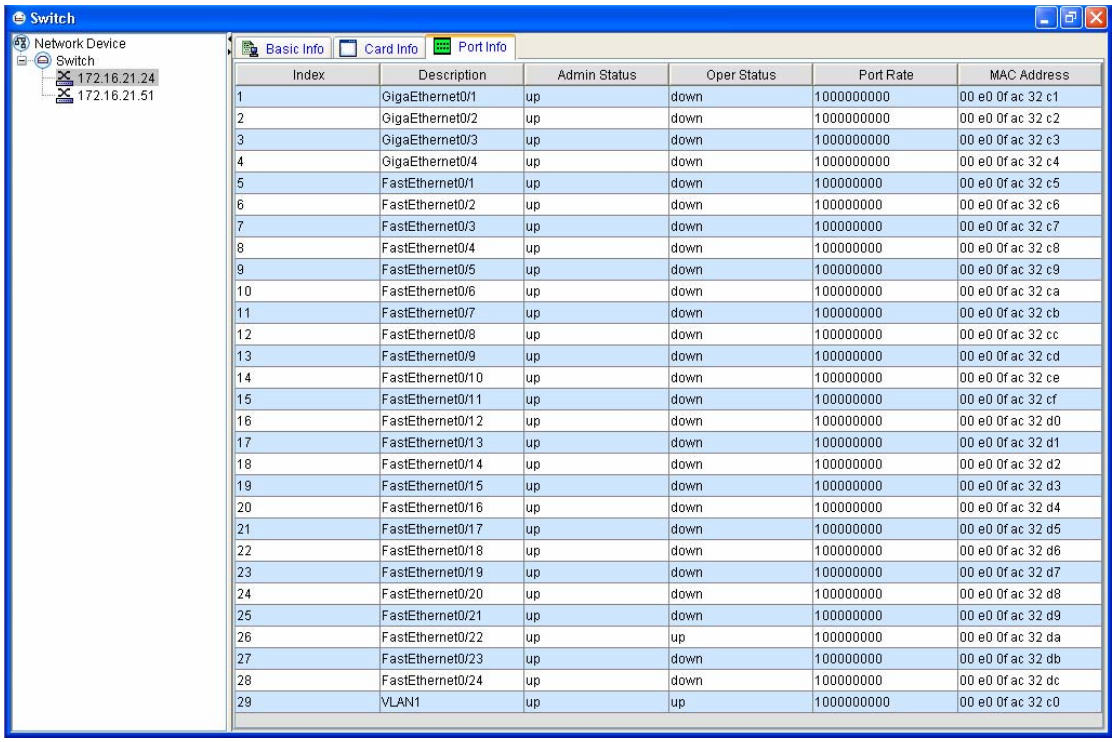
If you click a to-be-browsed device, click it and then select **Card Info**, the system will automatically read and show you the basic configuration information about this card, including **Index**, **Type**, **Description**, **Hardware Version**, **Software Version**, **Slot ID** and **Operation Status**. See the following figure:



You can know from the above-mentioned figure that the currently chosen switch has a 2228 mother card, whose operation platform is up.

8.2.3 Port Info

Select a to-be-browsed device node, click it and then select **Port Info**. The system will automatically read and show you the information about this device's ports, including **Index**, **Description**, **Management Status**, **Operation Status**, **Port's Rate** and **MAC**. See the follwing figure:



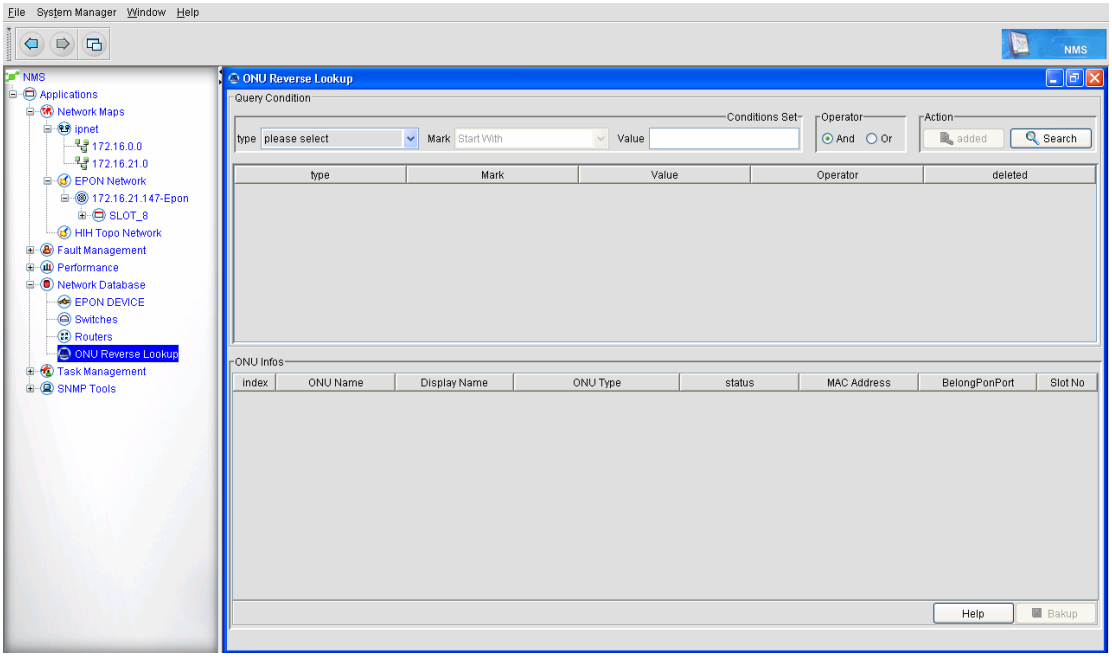
Index	Description	Admin Status	Oper Status	Port Rate	MAC Address
1	GigaEthernet0/1	up	down	1000000000	00 e0 0f ac 32 c1
2	GigaEthernet0/2	up	down	1000000000	00 e0 0f ac 32 c2
3	GigaEthernet0/3	up	down	1000000000	00 e0 0f ac 32 c3
4	GigaEthernet0/4	up	down	1000000000	00 e0 0f ac 32 c4
5	FastEthernet0/1	up	down	100000000	00 e0 0f ac 32 c5
6	FastEthernet0/2	up	down	100000000	00 e0 0f ac 32 c6
7	FastEthernet0/3	up	down	100000000	00 e0 0f ac 32 c7
8	FastEthernet0/4	up	down	100000000	00 e0 0f ac 32 c8
9	FastEthernet0/5	up	down	100000000	00 e0 0f ac 32 c9
10	FastEthernet0/6	up	down	100000000	00 e0 0f ac 32 ca
11	FastEthernet0/7	up	down	100000000	00 e0 0f ac 32 cb
12	FastEthernet0/8	up	down	100000000	00 e0 0f ac 32 cc
13	FastEthernet0/9	up	down	100000000	00 e0 0f ac 32 cd
14	FastEthernet0/10	up	down	100000000	00 e0 0f ac 32 ce
15	FastEthernet0/11	up	down	100000000	00 e0 0f ac 32 cf
16	FastEthernet0/12	up	down	100000000	00 e0 0f ac 32 d0
17	FastEthernet0/13	up	down	100000000	00 e0 0f ac 32 d1
18	FastEthernet0/14	up	down	100000000	00 e0 0f ac 32 d2
19	FastEthernet0/15	up	down	100000000	00 e0 0f ac 32 d3
20	FastEthernet0/16	up	down	100000000	00 e0 0f ac 32 d4
21	FastEthernet0/17	up	down	100000000	00 e0 0f ac 32 d5
22	FastEthernet0/18	up	down	100000000	00 e0 0f ac 32 d6
23	FastEthernet0/19	up	down	100000000	00 e0 0f ac 32 d7
24	FastEthernet0/20	up	down	100000000	00 e0 0f ac 32 d8
25	FastEthernet0/21	up	down	100000000	00 e0 0f ac 32 d9
26	FastEthernet0/22	up	up	100000000	00 e0 0f ac 32 da
27	FastEthernet0/23	up	down	100000000	00 e0 0f ac 32 db
28	FastEthernet0/24	up	down	100000000	00 e0 0f ac 32 dc
29	VLAN1	up	up	1000000000	00 e0 0f ac 32 c0

8.3 Router

The way of browsing the configuration information about a router is same to that about a switch, so you can refer to the previous section for the similar operation.

8.4 Querying ONU

The function to query ONU is different from the above-mentioned three functions: EPON device, switch and router. It means to detect an EPON ONU according to the set query conditions first and then query the PON ports and slots of the EPON OLT which connects the detected EPON ONU. See the following figure:



Step1: Set the type of query condition, which including MAC, device type, telephone ID and OLT.

MAC: it refers to the MAC addresses of all EPON ONUs.

Device type: It refers to the types of all currently managed EPON ONUs, such as ONU_8016_D201.

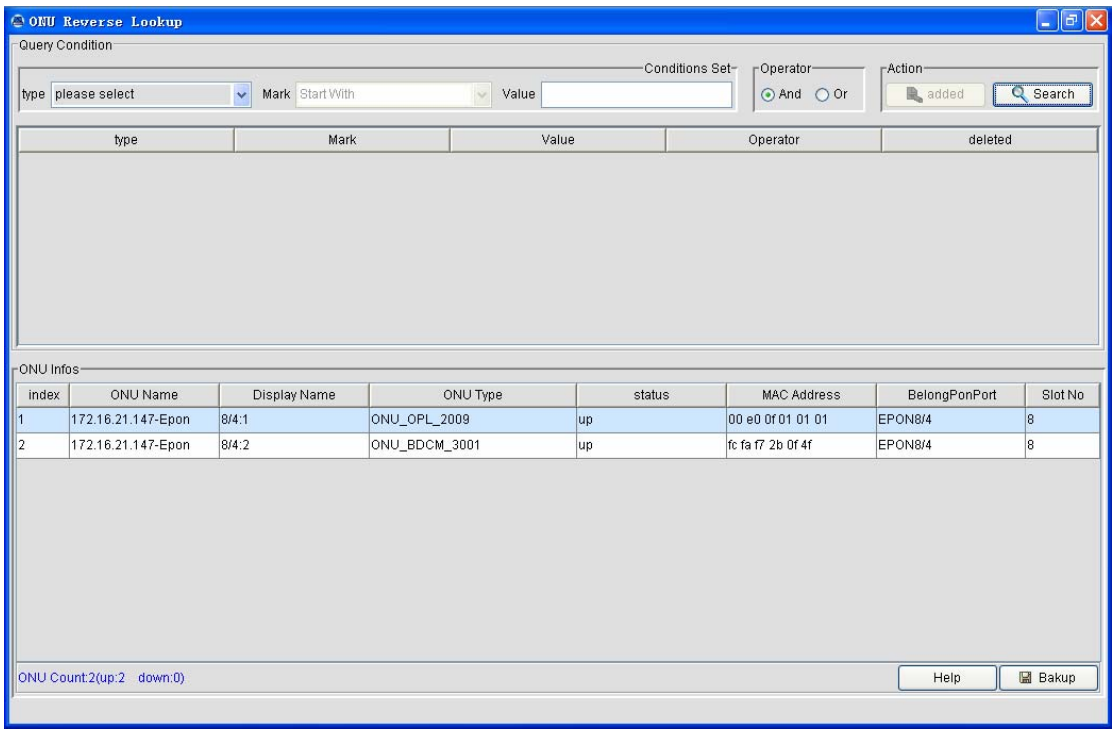
Telephone ID: It refers to the telephone ID in the project information that stores in each EPON ONU.

OLT: it refers to the EPON OLT that each EPON ONU connects.

Choose a condition type, set its value, select the operational character of the query condition (and/or), and click **Add**.The currently set query condition will then be added to the query condition set (query condition summary area).

Step 2: Delete the unnecessary conditions by choosing them in query condition summary area and clicking **Delete**.

Step3: Choose the query conditions and then click **Query**. The EPON ONU’s information, which complies with the query conditions, is displayed, including **Name**, **Displayed Name**, **Device Type**, **Status**, **MAC**, **Uplink PON Port**, **Slot ID**. If you directly click **Query** without setting the query conditions beforehand, the system will query all currently managed EPON ONUs by defaul.See the following figure:



At the bottom of the query results, you can find the summary information about the query results, including the totol number of ONUs, number of online ONUs and number of offline ONUs.
At the same time the system supports to backup the current query results.You can save the query results in the excel format by clicking **Backup**.

9 Task Management

Task policy configuration provides users some simple and visuable batch task processing tasks, reducing repeated operations and saving the configuration time of device initialization.Task policy configuration also provides the functions such as adding the time policy and executing related tasks in a designated time auatomatically, which enable users to arrange network management time freely.

Task policy configuration includes the following functions:

- Backuping the database
- Distributing the version file of the IP device
- Distributing the ONU version file
- Distributing the configuration file of the IP device
- Distributing the ONU configuration file
- Distributing the line-card version file
- Distributing the PON chip's drive
- Backuping the version file of the IP device
- Backuping the configuration file of the IP device
- Backuping the ONU configuration file

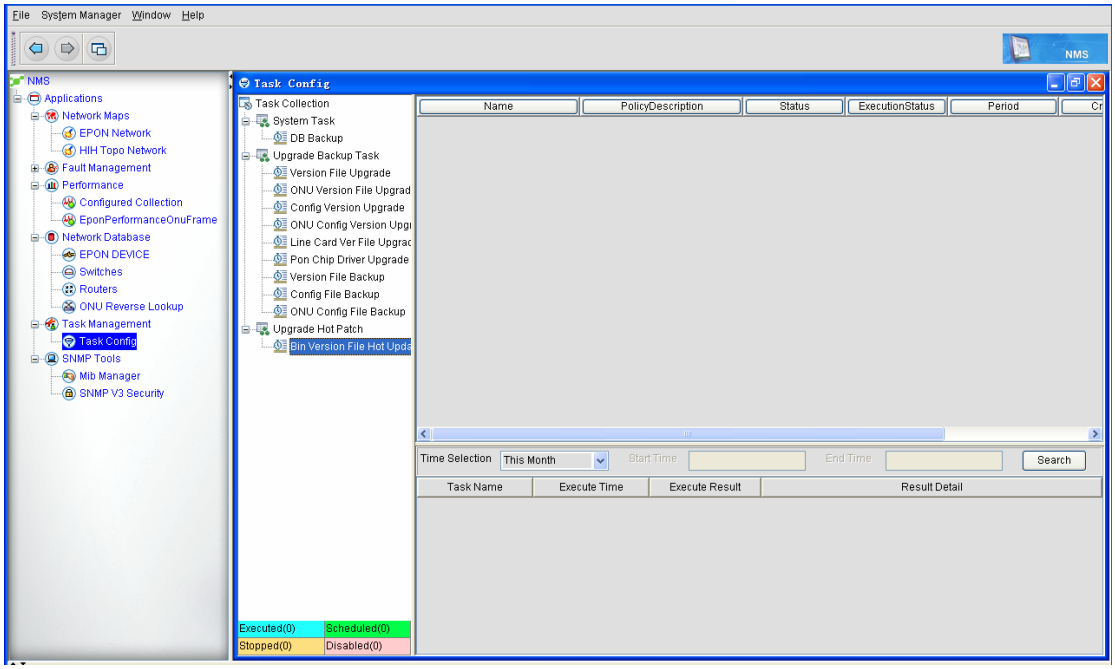
Task policy configuration includes the following operations:

- Adding the task policy
- Changing the task policy
- Deleting the task policy
- Modifying the execution interval of the task policy
- Stopping the task policy

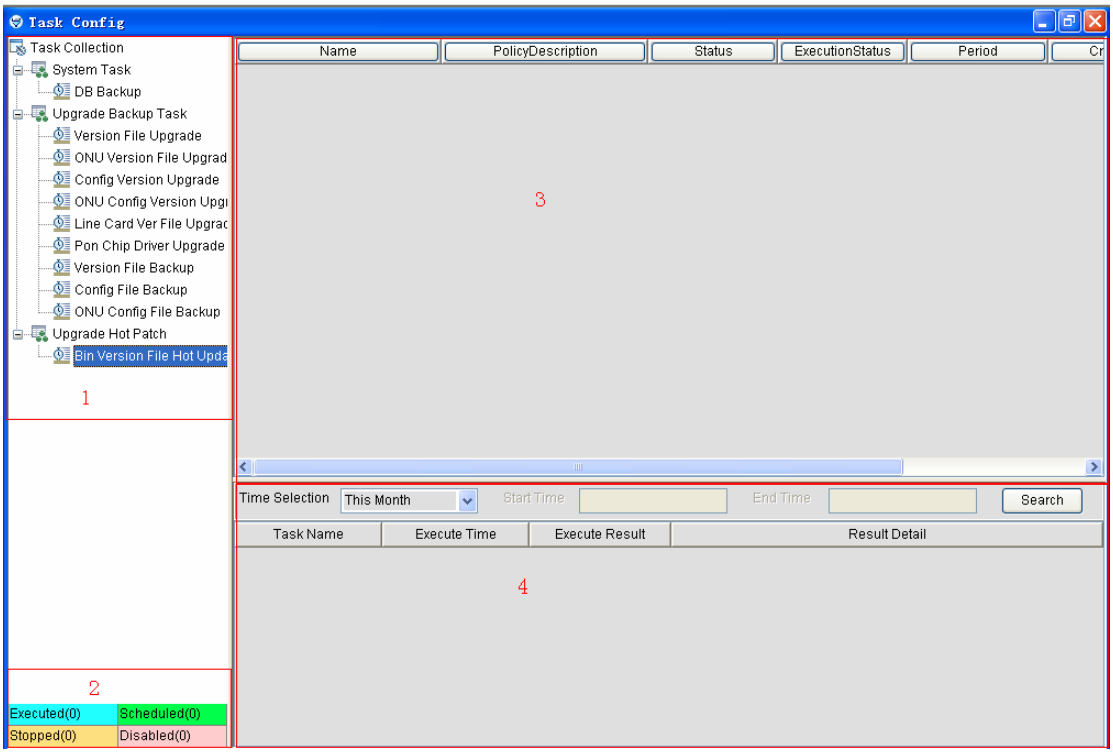
The above-mentioned functions and operations are described below:

9.1 Functions of Task Policy Configuration

9.1.1 Starting the Functions of Task Policy Configuration



On the NMS client, open the NMS program tree on the left, click **Task Management** and then **Task Configuration**. The following window appears:



All the functions of task policy configuration are set on this window, and all running results are displayed on this window: The following are some descriptions about this window:

Area 1 is the task function list, in which all task finctions supported by NMS are listed.

Area 2 is where the running statuses of all tasks are shown. The statuses include:

- Running: means the number of the running tasks.
- To be run: means the number of to-be-run tasks whose time policies are already set.
- Stopped: means the number of stopped tasks.
- Invalid: means the number of tasks that are labeled as invalid.

Area 3 is the task list, in which all tasks will be shown, including:

- Name: means the name of a task, which is used to differentiate and define the tasks.
- Task description: it is used to give a detailed description of the task's function.
- Enablement status: It means whether a task is forbidden. If a task is defined as invalid, this task cannot be executed.
- Running status: It means the running status of a task.
- Cycle: it means the execution cycle of a task. The task will be automatically performed when the cycle comes.
- Creation user: it means the username that is used by the task creator to log in to NMS.
- Creation time: It means the time when a task is created.

Area 4 is where the running results of a task are shown. You can select a time segment to query the historical running results of the corresponding task, including **Task Name**, **Running Time**, **Running Results** and **Detailed Info**.

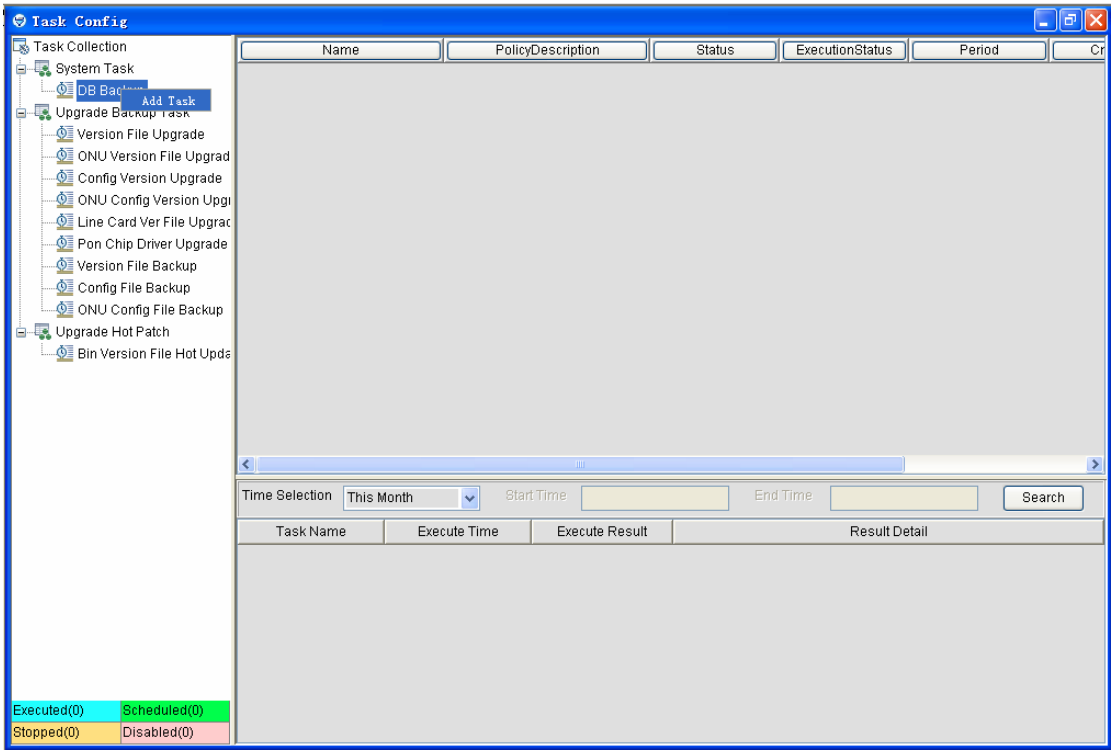
9.1.2 Backuping the Database

The database backup function supports the manual or fixed automatic backup and saves all the running information of NMS.In case of system breakdown, this function can resume all the running information, including all discovered device information, topologies and all the database's information.

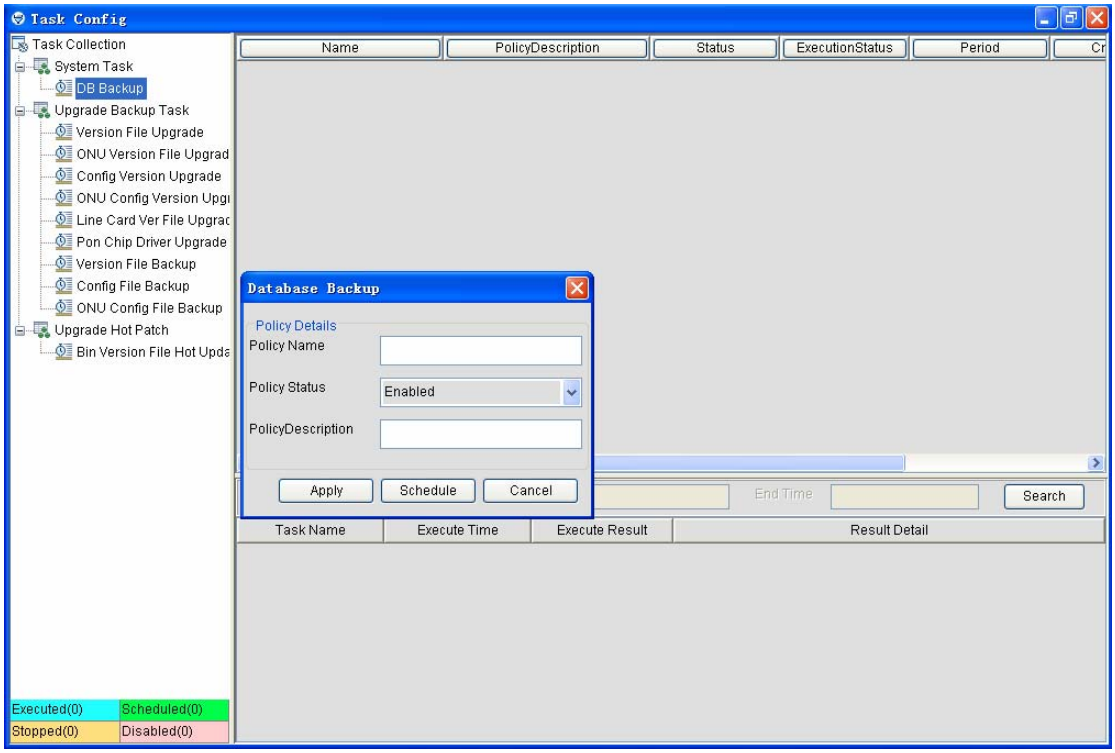
Note: All the information that is stored in the configuration files will not be backuped. For example, the configured discovery information need be reset.

■ The procedure of adding a database backup task is shown below:

1. Click **Task Collection -> System Task -> Database Backup** and then right click **Database Backup**. The **Add task** button appears, as shown in the following figure:



2. Click **Add task**. The following window appears:



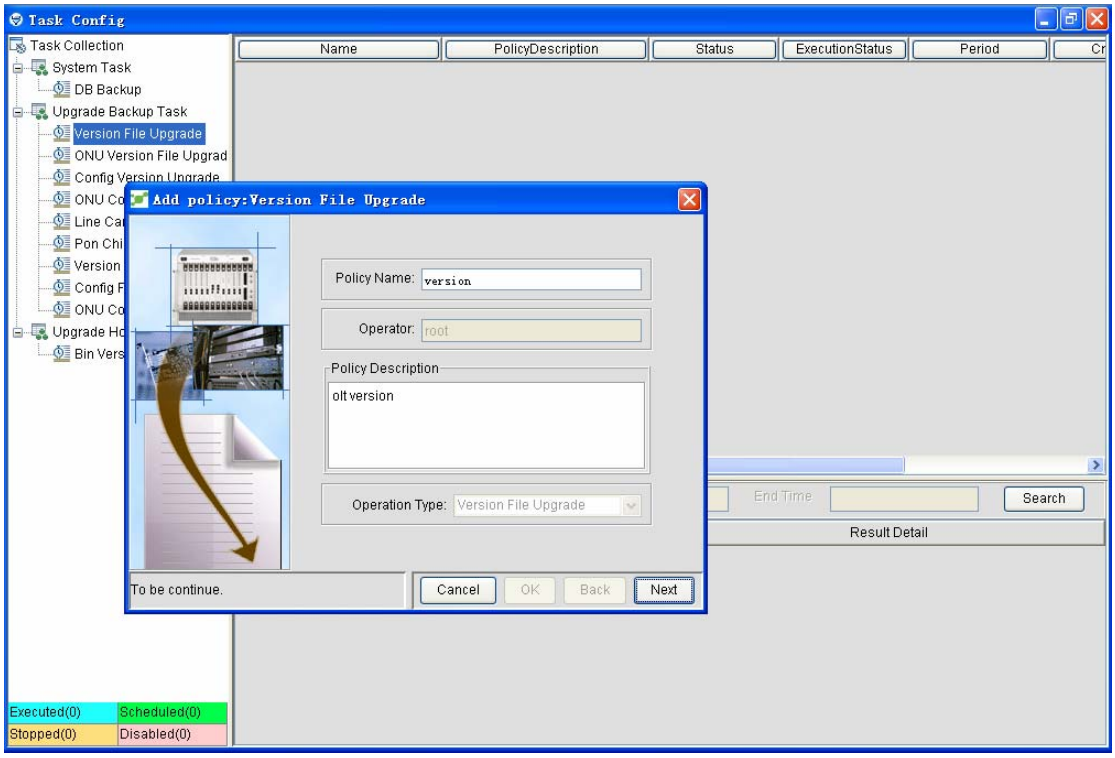
3. Set the policay name, the enablement staus and the task description, and then click **Apply**. The database backup task is done.

If you select **Invalid** in the **Enablement status** dropdown box, the task will not be performed; if you do not click the time table, the task should be manually performed.For how to set the time policy in the time table, see section 8.3.5.2.

9.1.3 Distributing/Backuping Devices

Step 1: Start this task, that is, enter the basic information of this task.

Click **Task Collection -> System Task -> Distribute/Backup** and then right click **Distribute/Backup**. The **Add task** button appears. Click **Add** task to open the following window:



You must enter values in the **Task name** textbox and the **Task description** textbox. The task name cannot be same to other task names, or the task cannot be added successfully.The adder is the name of the current user who logs in to NMS. The operation type is alos the current operation.

Step 2: Select a target device.

When you add a task, you must add a target device to execute this task.The target devices have the following types:

- IP management device

1. Router
2. Switch
3. OLT

- Non-IP management device

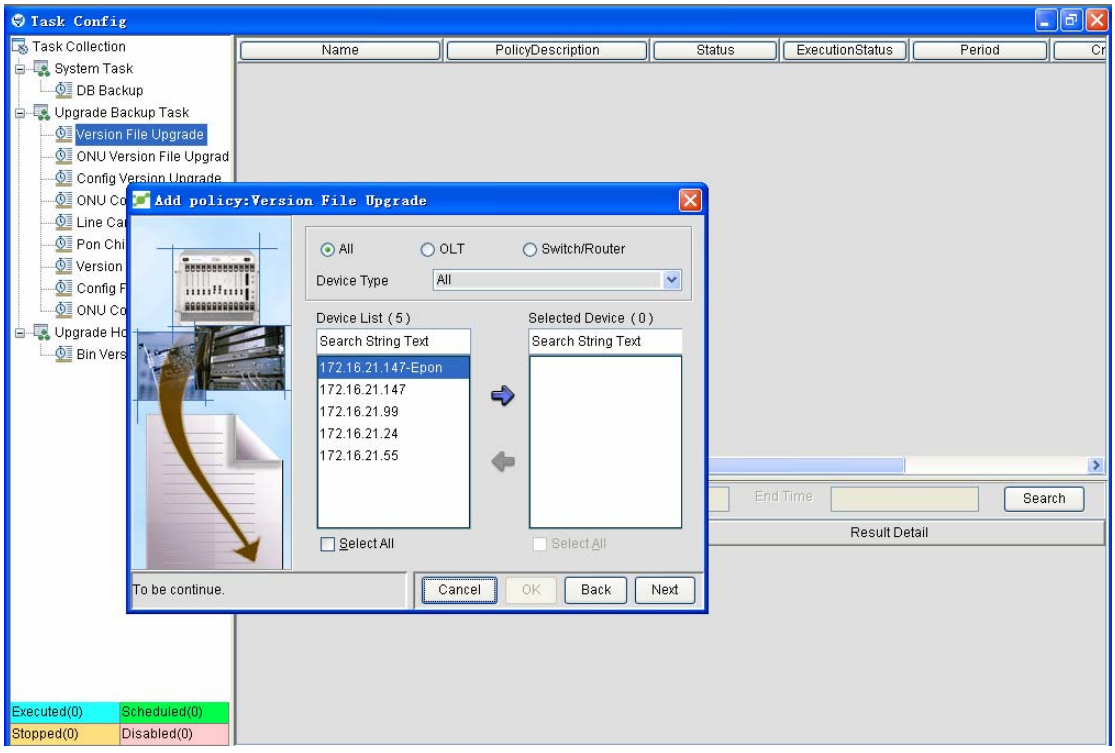
1. ONU

The following table shows the relationship of the device type and the operation type:

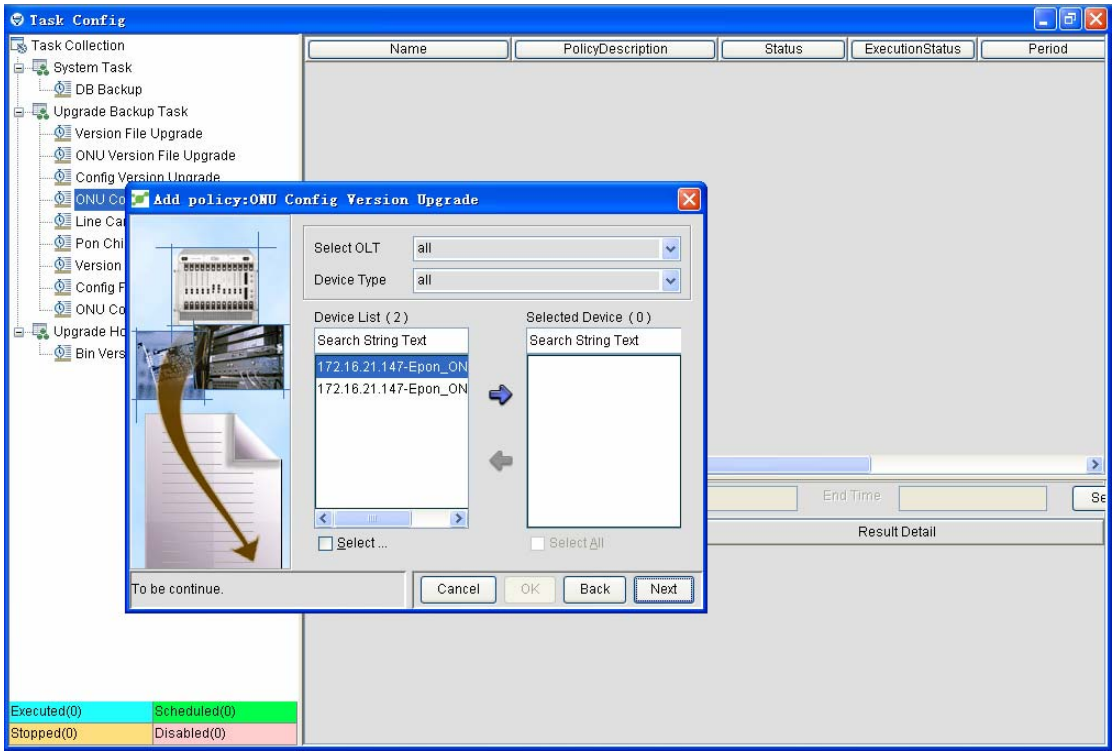
	Router	Switch	OLT	ONU
Distributing the version file of the IP device				
Distributing the ONU version file				
Distributing the configuration file of the IP device				
Distributing the ONU configuration file				
Distributing the line-card version file				
Distributing the PON chip's drive				
Backuping the version file of the IP device				
Backuping the configuration file of the IP device				
Backuping the ONU configuration file				

The following shows the window to select each type of device:

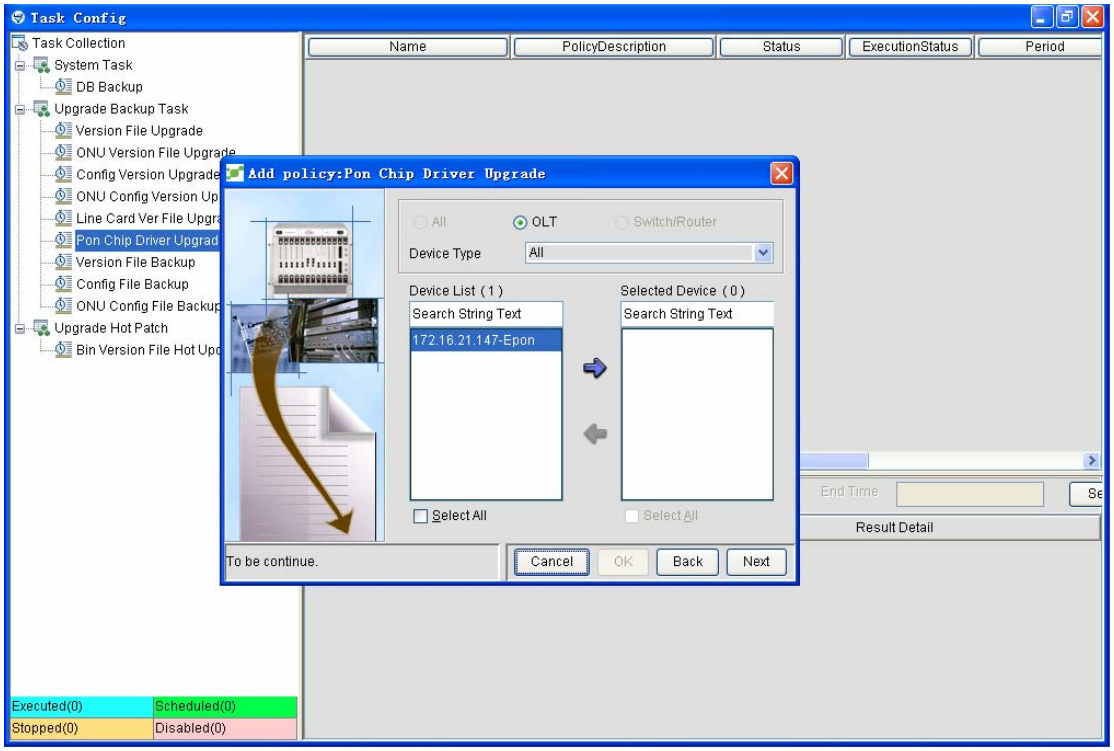
- **IP device selection window**



■ **ONU device selection window**



■ **OLT device selection window**



■ **Filter**

The **Filter** option is on the right top of each window.

✧ When selecting IP devices, you can filter them by selecting OLT/switch/router and then conduct detailed filtration through the device type.

- ✧ Before selecting ONU, you can select an OLT and then filter ONUs through the ONU type.
- ✧ When selecting OLT, you can filter OLTs only through the device type.

■ **Select**

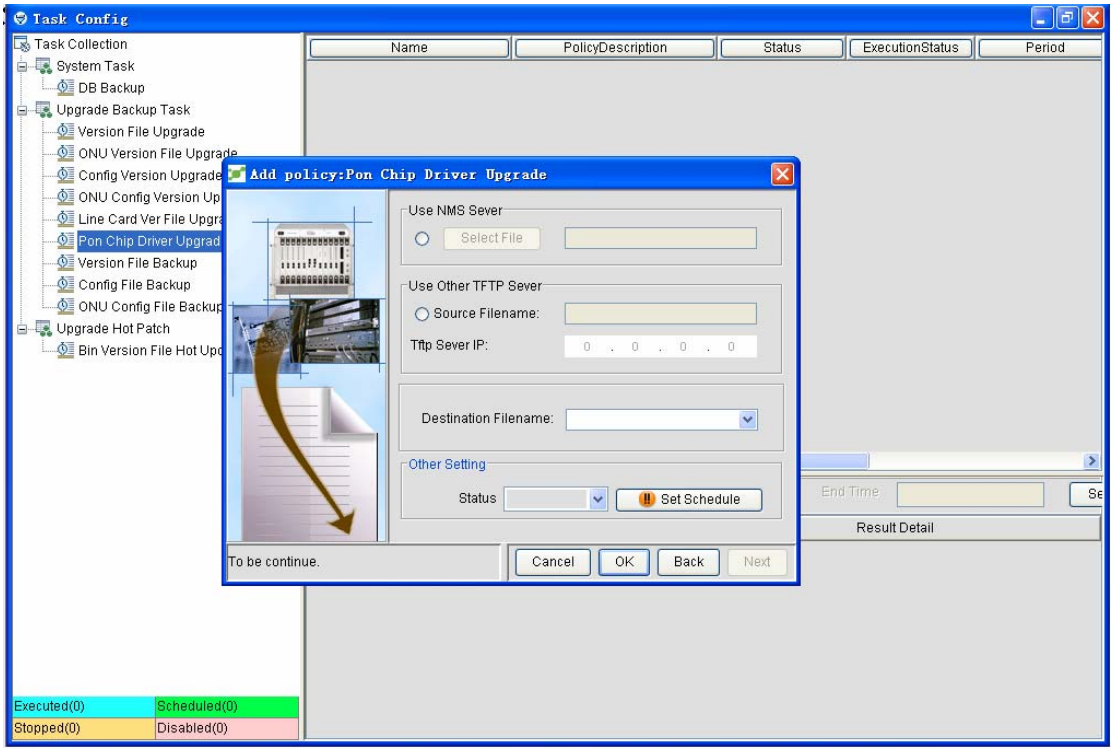
The right bottom of the window is the filtered device list and the selected device list:

- ✧ [Device list] means the number of the filtered devices.You can enter the device name in the **Search** textbox to further select them.

Step 3: Complete the task policy configuration.

It is the last step of task policy configuration. All functions have only two kinds of differences: the backup difference and the distribution difference.

■ **Last configuration of the distribution task**



You need to set the following attributes in this last configuration:

■ Source location of the distributed file

- ✧ From the NMS server: Click a selected file to open a window for selecting files in the NMS root directory.
- ✧ From the third-party TFTP server: Enter the IP address of TFTP and the source file name.

■ Destination file's name in the device

Here you shall select a name as the file name of the source file which has been distributed to the device. The file names include:

- ✧ Switch.bin: It is recommended to name the switch's bin files.
- ✧ Router.bin: It is recommended to name the router's bin files.
- ✧ olt_blob: It is recommended to name the drive file of the PON chip.
- ✧ LS16PON_bin: It must be used to name the version file of the 16PON line-card.
- ✧ LS24GE_bin: It must be used to name the version file of the 24GE line-card.
- ✧ LS12GE_bin: It must be used to name the version file of the 12GE line-card.

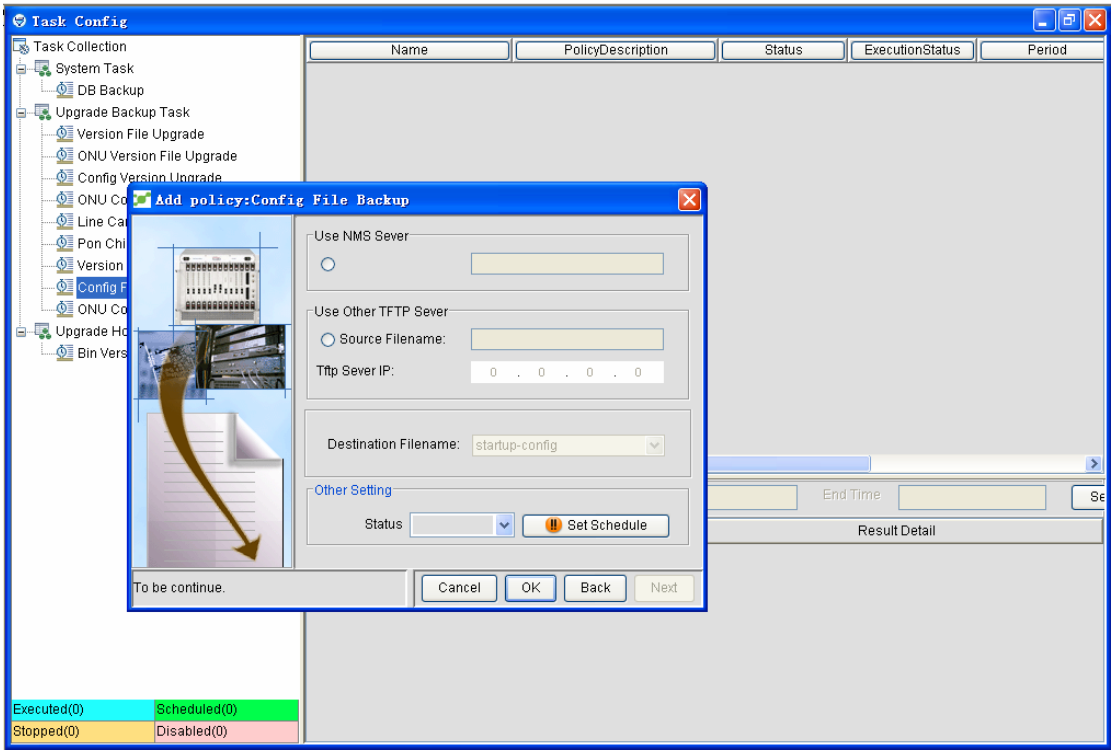
- ✧ LS24FE_bin: It must be used to name the version file of the 24FE line-card.
- ✧ LS48FE_bin: It must be used to name the version file of the 48FE line-card.
- ✧ ONU.zblob: It must be used to name the version file of the ONU.
- ✧ For those recommended file names, you can name the destination files by yourself.

■ Task Status

- ✧ Invalid policy: it means that this policy cannot be executed.
- ✧ Valid policy: it means that this policy can be executed.

■ Setting the time table

■ Last configuration of the backup task



You need to set the following attributes in this last configuration:

■ Source location of the distributed file

- ✧ From the NMS server: Click a selected file to open a window for selecting files in the NMS root directory.
- ✧ From the third-party TFTP server: Enter the IP address of TFTP and the source file name.

■ Destination file's name in the device

Here you shall select a name as the file name of the source file which has been distributed to the device. The file names include:

- ✧ Switch.bin: It is recommended to name the switch's bin files.
- ✧ Router.bin: It is recommended to name the router's bin files.
- ✧ olt_blob: It is recommended to name the drive file of the PON chip.

- ✧ LS16PON_bin: It must be used to name the version file of the 16PON line-card.
- ✧ LS24GE_bin: It must be used to name the version file of the 24GE line-card.
- ✧ LS12GE_bin: It must be used to name the version file of the 12GE line-card.
- ✧ LS24FE_bin: It must be used to name the version file of the 24FE line-card.
- ✧ LS48FE_bin: It must be used to name the version file of the 48FE line-card.
- ✧ ONU.zblob: It must be used to name the version file of the ONU.
- ✧ For those recommended file names, you can name the destination files by yourself.

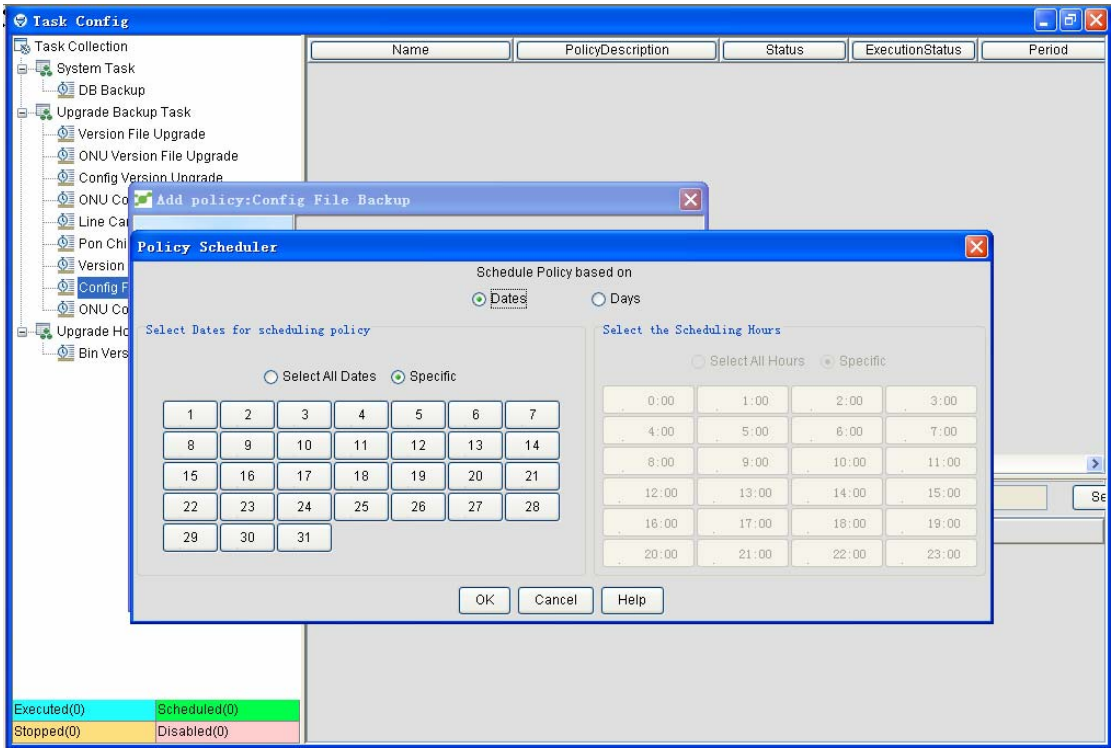
■ Task Status

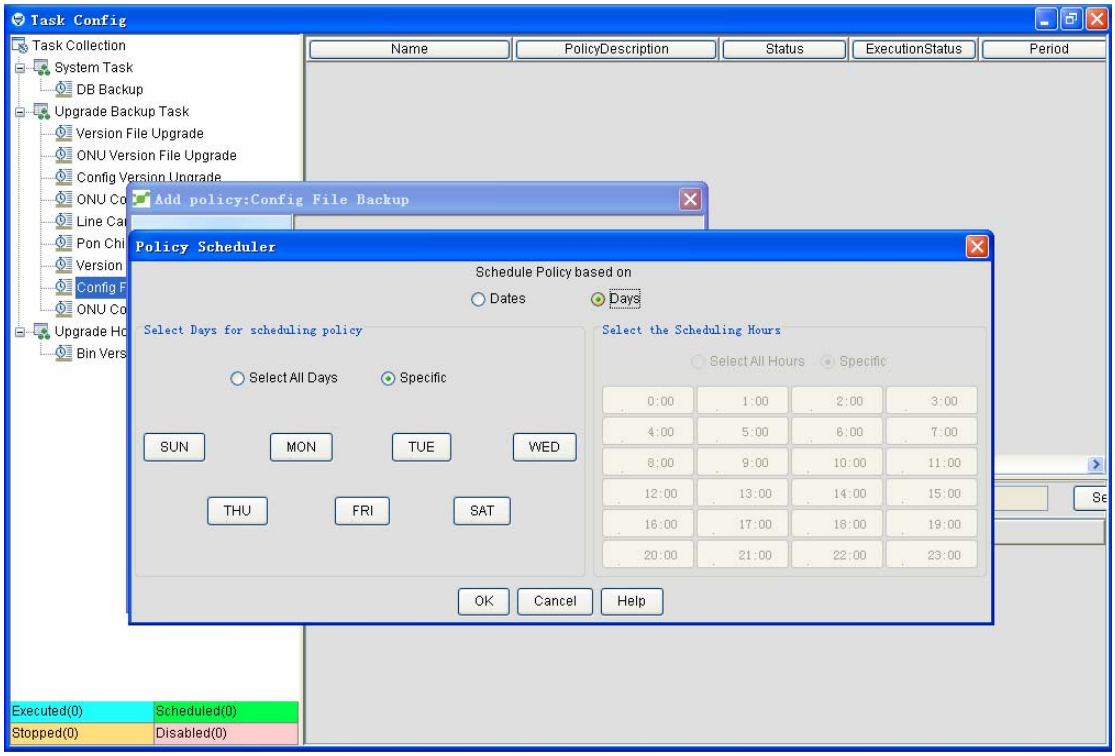
- ✧ Invalid policy: it means that this policy cannot be executed.
- ✧ Valid policy: it means that this policy can be executed.

■ Setting the time table

For details, see section 8.2.1.2.

9.1.4 Setting the Time Policy of Task Execution





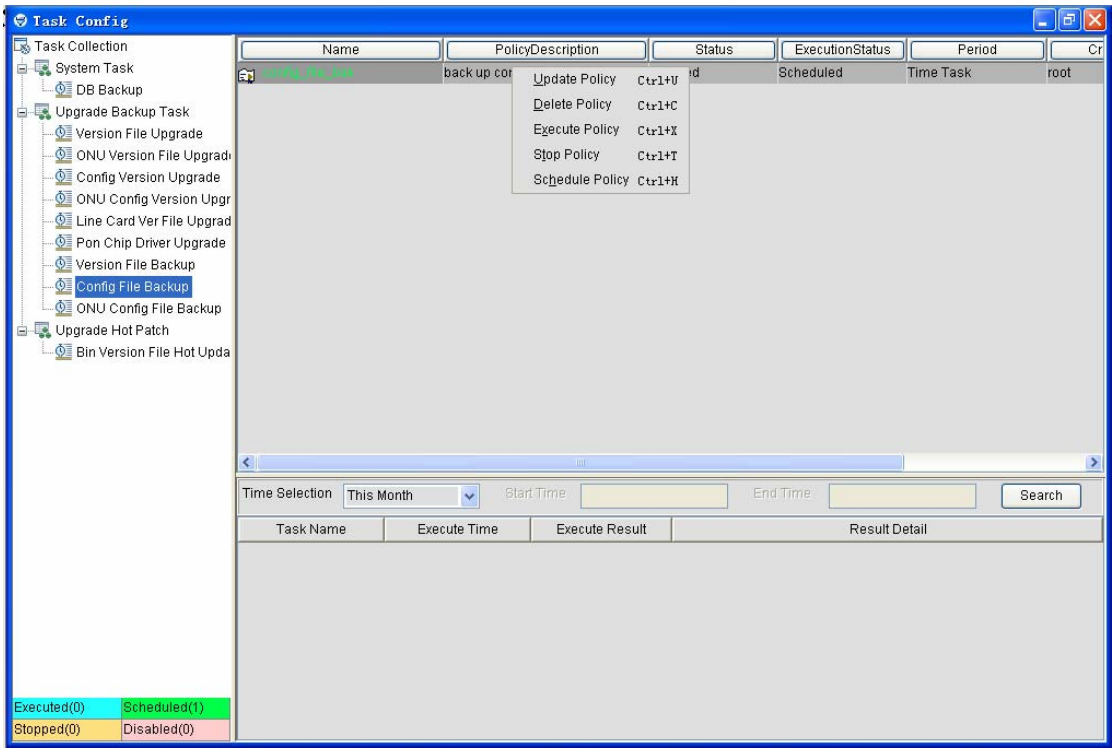
The time policy settings are shown in the above-mentioned two figures.

- On the left part, you can select the date.
  - ✧ When the time policy is based on the date, select a date between 1 and 31. It means that the task will be automatically executed on the date of each month.
  - ✧ When the time policy is based on the day, select a week day between Sunday and Saturday. It means that this task will be automatically executed on this week day.
- On the right part, you can select the specific time.
- You can also select all the hours in this day.

After you set the time policy, click **OK**. If the task policy is valid, the task will be executed at the designated hour(s).

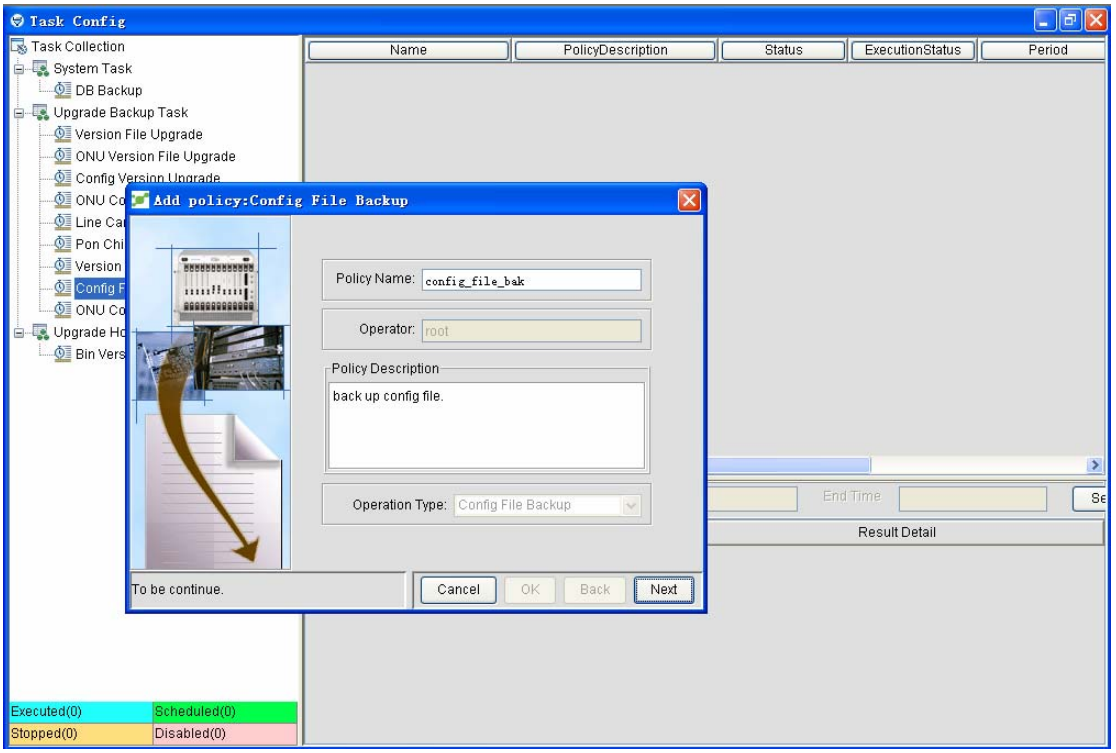
9.2 Operations of Task Policy

The operations of task policy are shown below:

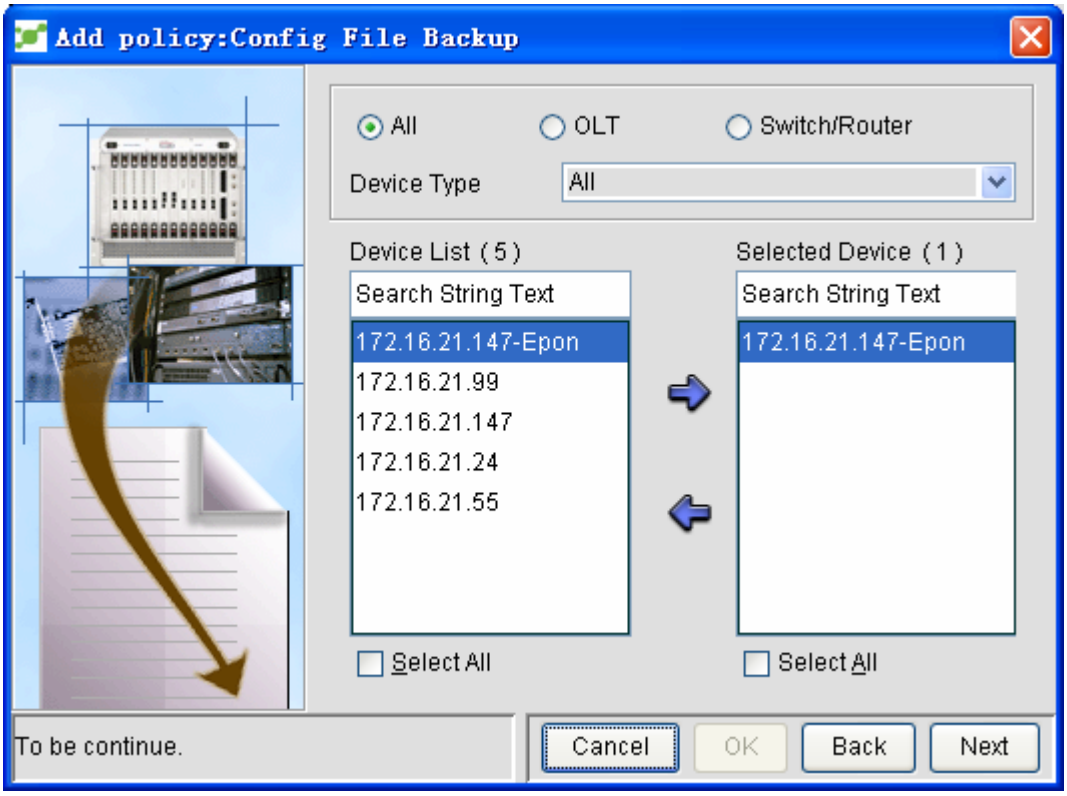


- Adding the task policy

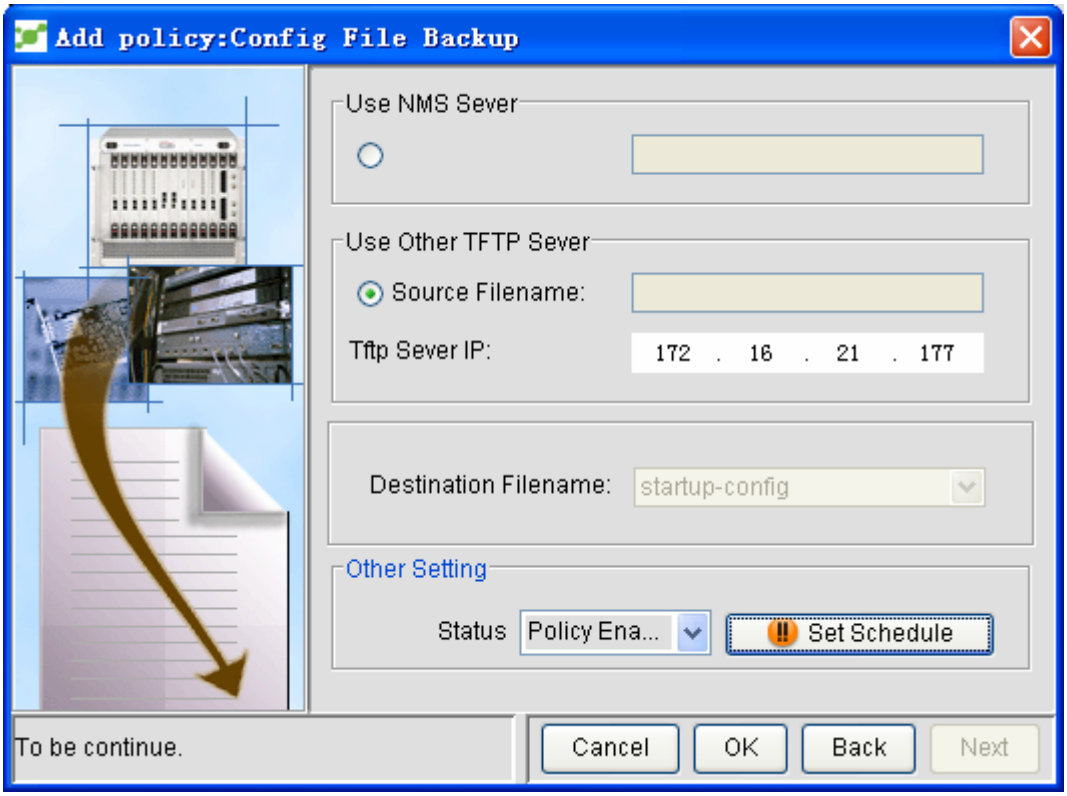
Step1:



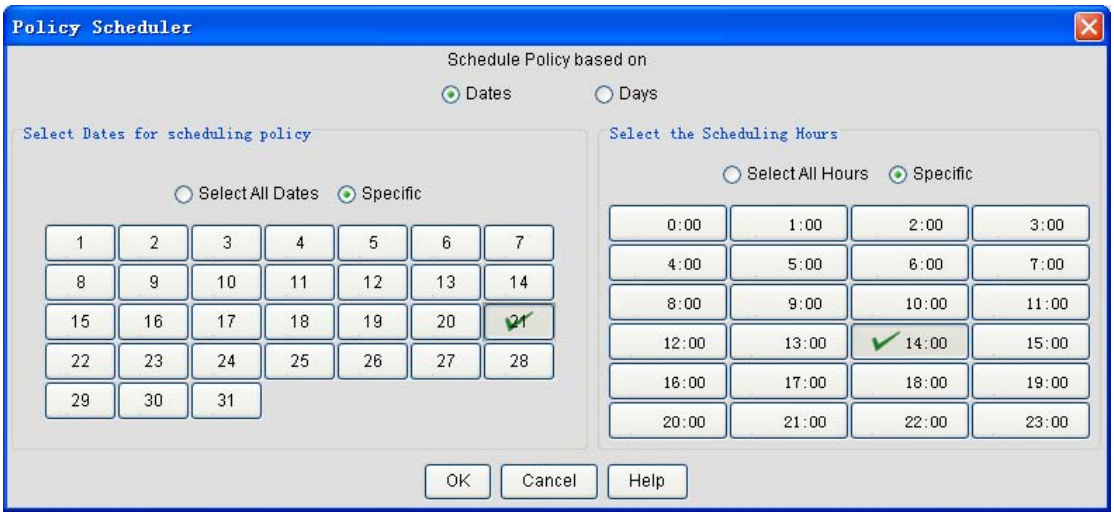
Step2:


Add policy:Config File Backup
All
OLT
Switch/Router
Device Type
All
Device List (5)
Search String Text
172.16.21.147-Epon
172.16.21.99
172.16.21.147
172.16.21.24
172.16.21.55
Selected Device (1)
Search String Text
172.16.21.147-Epon
Select All
Select All
To be continue.
Cancel
OK
Back
Next

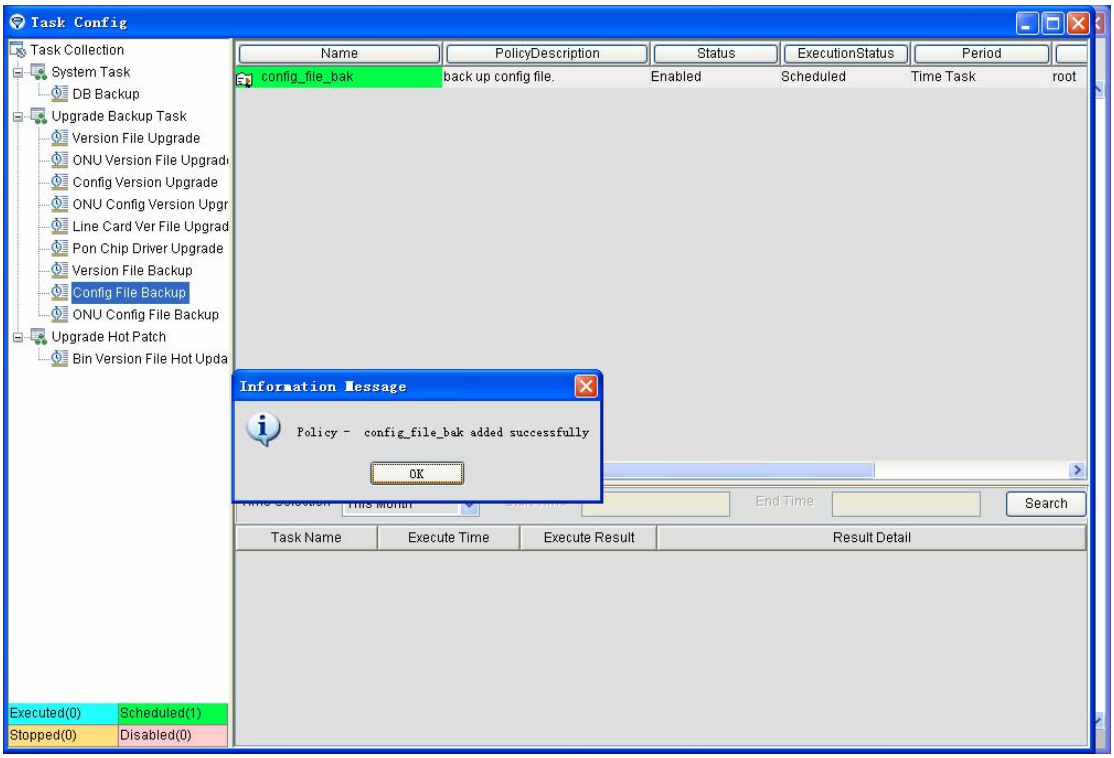
Step3:


Add policy:Config File Backup
Use NMS Sever
Use Other TFTP Sever
Source Filename:
Tftp Sever IP:
172 . 16 . 21 . 177
Destination Filename:
startup-config
Other Setting
Status
Policy Ena...
Set Schedule
To be continue.
Cancel
OK
Back
Next

Step 4:



Step 5:



- Changing the task policy

  Select a task in the task policy list, right click it and select the update policy. The corresponding dialog box appears. It is similar to adding the task in section 9.1. However, the task name cannot be modified.

- Deleting the task policy

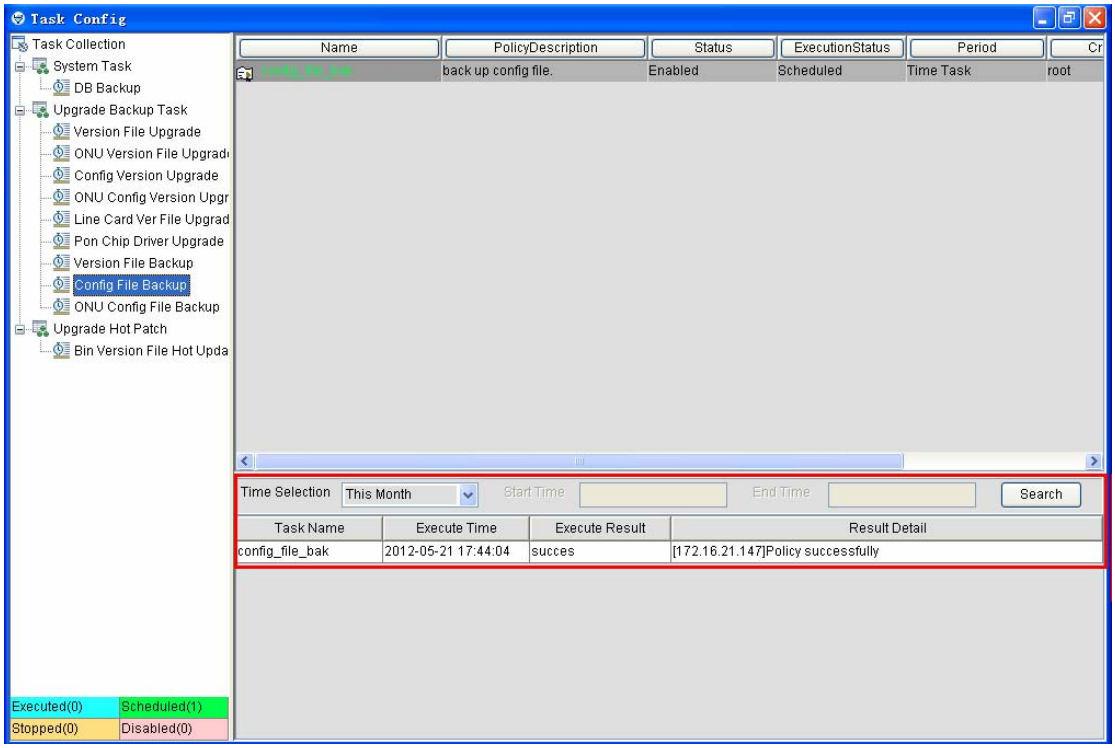
  Select a task in the task policy list, right click it and select **Delete**. The corresponding

dialog box appears. Click **OK** to remove the task from the database.

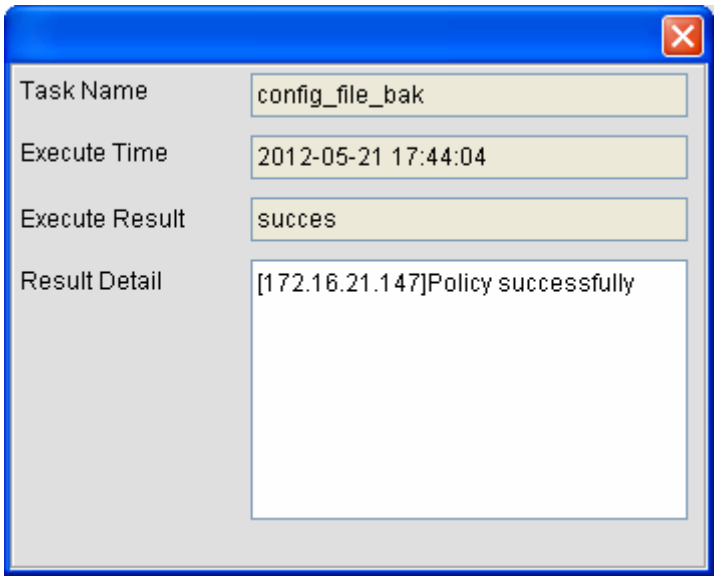
- Modifying the execution interval of the task policy
  Refer to section 9.1.4.
- Stopping the task policy
- Select a task in the task policy list, right click it and then click **Stop**. The time policy of this task will be stopped.

9.3 Browsing the Results of Task Policy

After a task is done, the corresponding results will be shown in a window. See the following figure:



- Time selection: it is for you to designate a time segment. After you set a time segment and click **Query**, the task running information in this time segment will be shown.
  - ✧ This month: The running information about all tasks in this month will be shown.
  - ✧ This week: The running information about all tasks in this week will be shown.
  - ✧ Today: The running information about all today's tasks will be shown.
  - ✧ Self-define: The running information about all tasks in the self-defined time segment will be shown.
    - ✓ **Start time** and **End time** need be designated.
- If you double click a running result, yopu can get the detailed running information about this task.

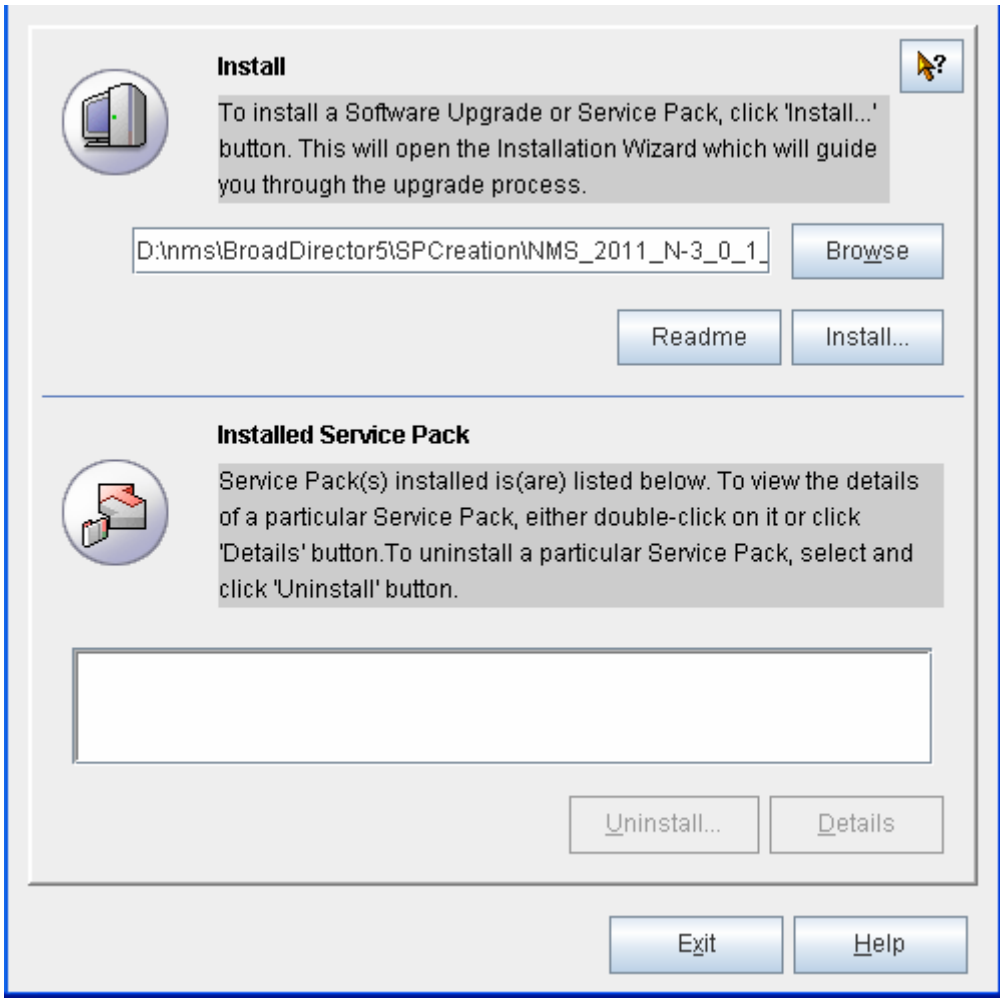


10 Patch Upgrade

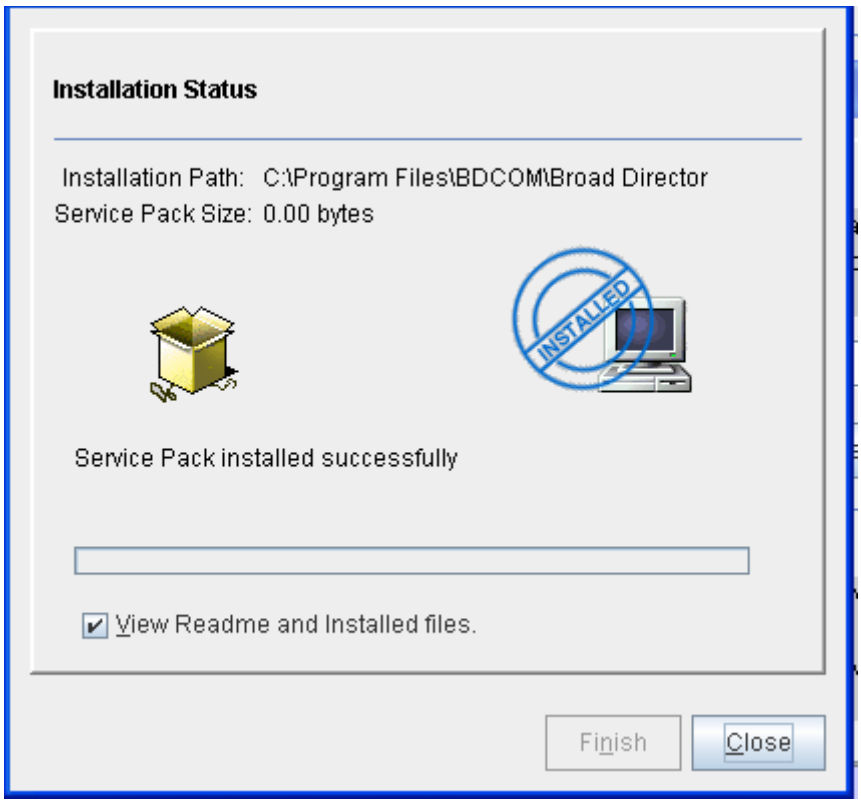
Pathc upgrade helps users to update their software to the lastest version and guarantees users to use new functions normally.NMS releases these upgrade patches irregularly to add new functions or fix safety problems.

10.1 Installing the Upgrade Program

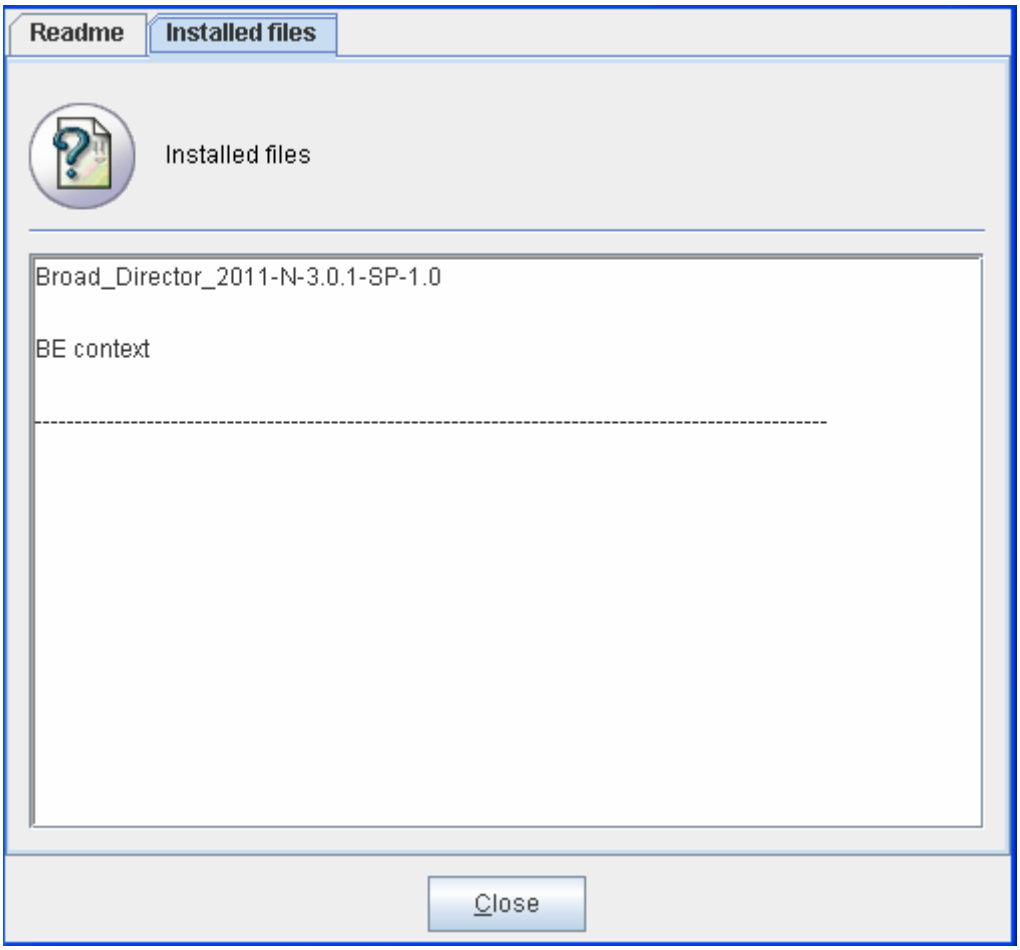
Open the installation directory of the NMS server, find the **UpdataManager.bat** upgrade tool in the **bin** folder, and double click the upgrade tool. The following window then appears:



The top part of this window is for users to install the upgrade program, while the bottom part of this window is to show the installed upgrade program.Click **Browse** to choose the path of the existing upgrade program.Click the **Install...** button. The following figure appears:

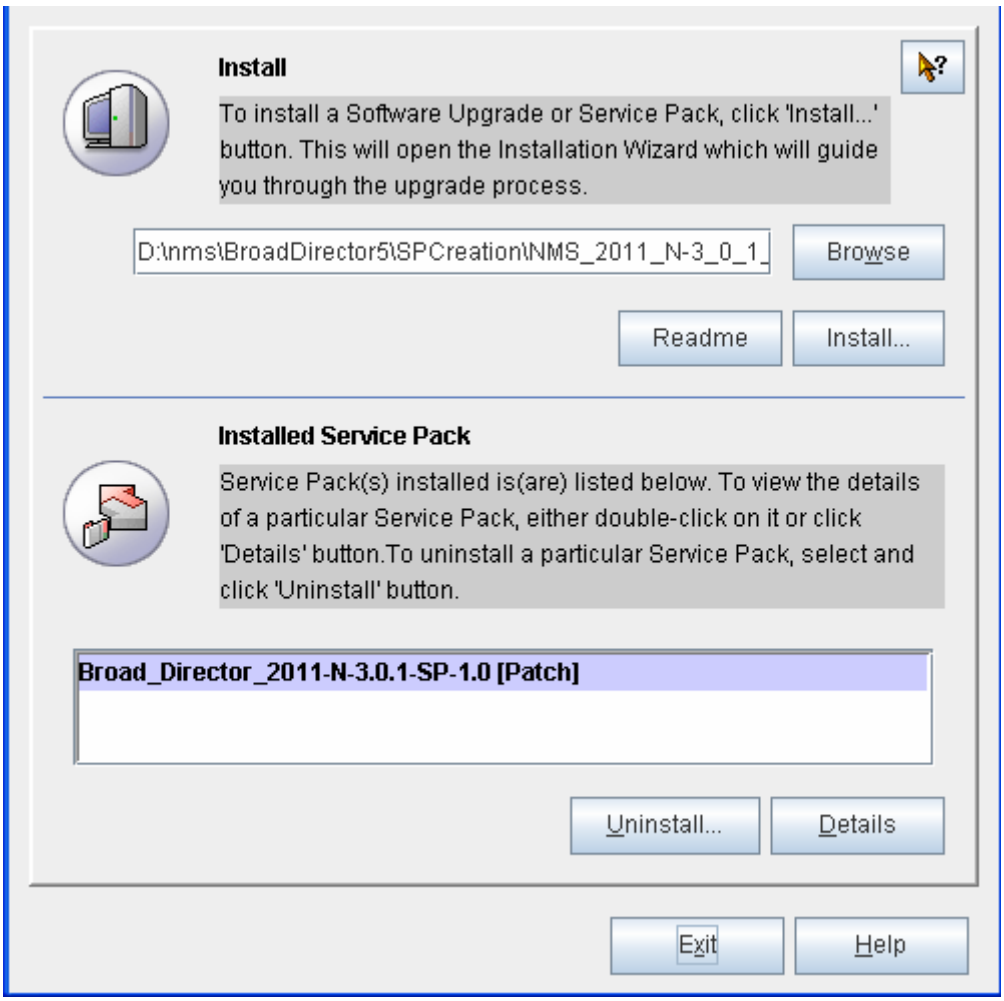


When the installation of the upgrade program shows 100%, the upgrade is successful. If you want to browse the detailed information about the upgrade description file and updates, click **Browse the installation file and its description file**. Then the following window appears:

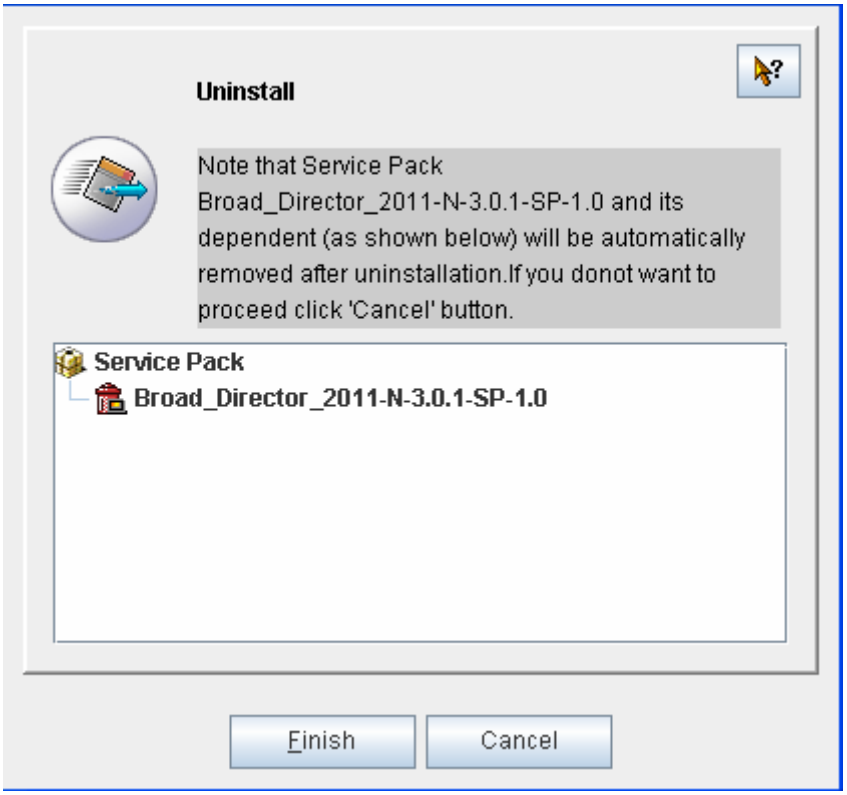


10.2 Uninstalling the Upgrade Program

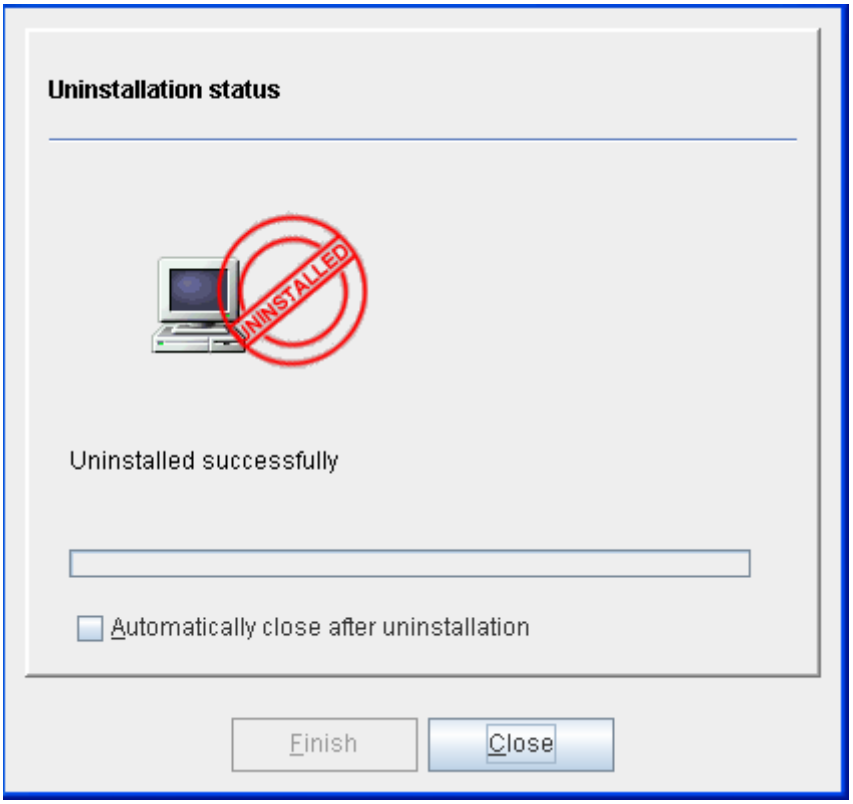
Open the installation directory of the NMS server, find the **UpdataManager.bat** upgrade tool in the **bin** folder, and double click the upgrade tool. The following window then appears:



At the bottom part of this window, select a installed upgrade program and then click **Uninstall**. Then the following window appears:



Click **Finish**. The system then uninsta;;s the selected upgrade program automatically, as shown in the following figure:



Click **Close** after the uninstallation is done.

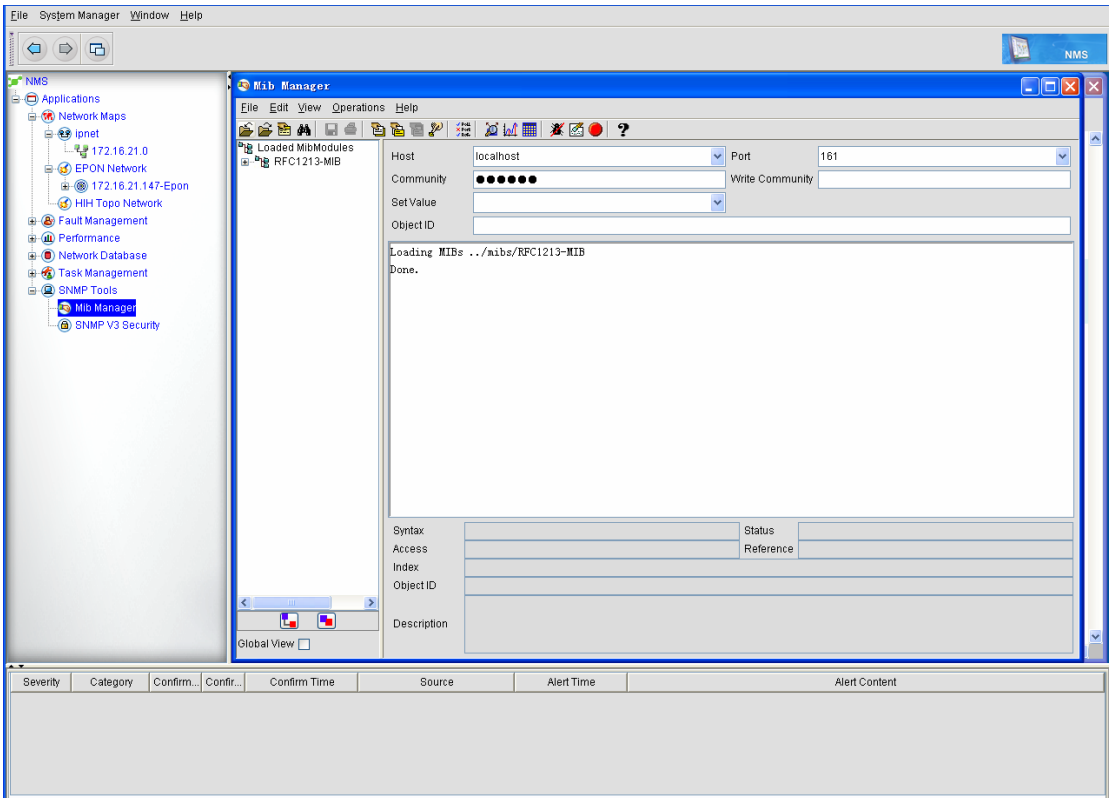
11 SNMP Tool

SNMP stands for Simple Network Management Protocol. This chapter will describe how to manage SNMP, including how to set the MIB browser and SNMPv3 parameters.

11.1 MIB Browser

MIB is a defined attribute set for managed objects.Each attribute of a managed object in MIB has a unique ID, which consists of the object type, read/write permission, the size limit and the range.MIB is an abstract data interface provided by the managed device, not a physical object.

NMS provides the MIB browser, helping users to obtain or browse the MIB information through graphic window.Click **SNMP tool -> MIB browser** to open the MIB browser, as shown in the following figure:



11.1.1 Toolbar

The toolbar lies on the top of the MIB browser, as shown in the following figure:

You can conduct the operations related to the MIB browser by clicking the corresponding icons in the toolbar.If the cusor is put on an icon, the function of this icon will be shown.To show or hide the toolbar, you can click **Show -> Toolbar**.

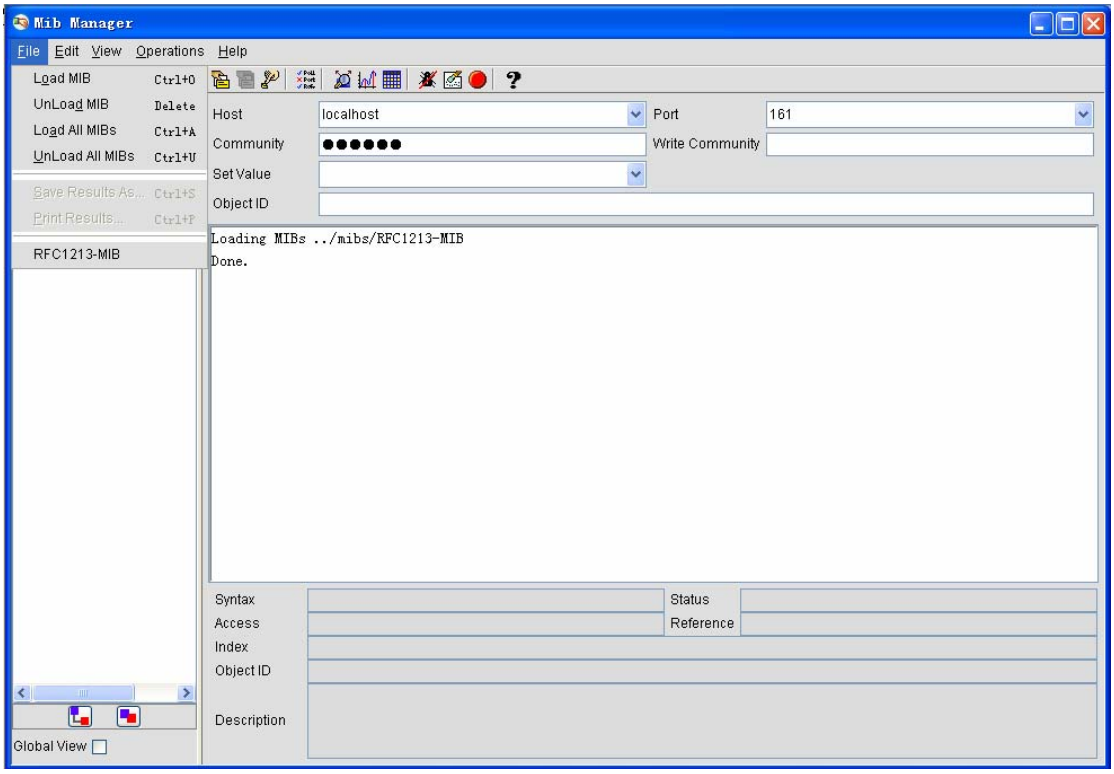
The following table shows the functions of each icon in the toolbar:

Icon	Name	Remarks
	**Install MIB**	It is used to download the MIB files in the MIB browser.If you click this icon, a dialog box appears for you to enter the URL or filename of a MIB file.
	**Uninstall MIB**	It is used to uninstall the installed MIB.
	**Description**	It is used to see the detailed description of a MIB node after you select this MIB node.
	**Browse the MIB node**	It is used to find a specific node in the MIB tree.
	**Save the results of the MIB browser**	It is used to save the results of the MIB browser. If you click this icon, a window appears for you to enter a file name. After you enter this file name, the results will be saved in this file.
	**Print the results of the MIB browser**	It is to print the results of MIB query.
	**Get SNMP**	It is to designate a MIB node and a MIB instance and then conduct a GET operation.
	**Get NEXT SNMP**	It is used to conduct a GET NEXT operation.If you click this icon, you will get the value of the next variable of the designated variable.
	**Get Bulk SNMP**	Click this icon and you will get the next object of the designated object.
	**Set SNMP**	It is to designate a MIB node to conduct a SET operation.
	**Set the MIB browser**	It is used to set the MIB browser.
	**Trap observer**	It is used to browse the received traps in a designated port.
	**Check the real-time graphic**	It is used to browse a designated OID curve.
	**Check the SNMP data form**	It is used to check the SNMP data form.
	**Debug**	It is used to browse the debug output.
	**Clear the displayed results**	It is used to clear the displayed results in the textbox.
	**Stop the query**	It is to stop the query.
	**Help**	It is used to browse the online help of the MIB browser.

11.1.2 Menu Description

The menu of the MIB browser are desribed below:

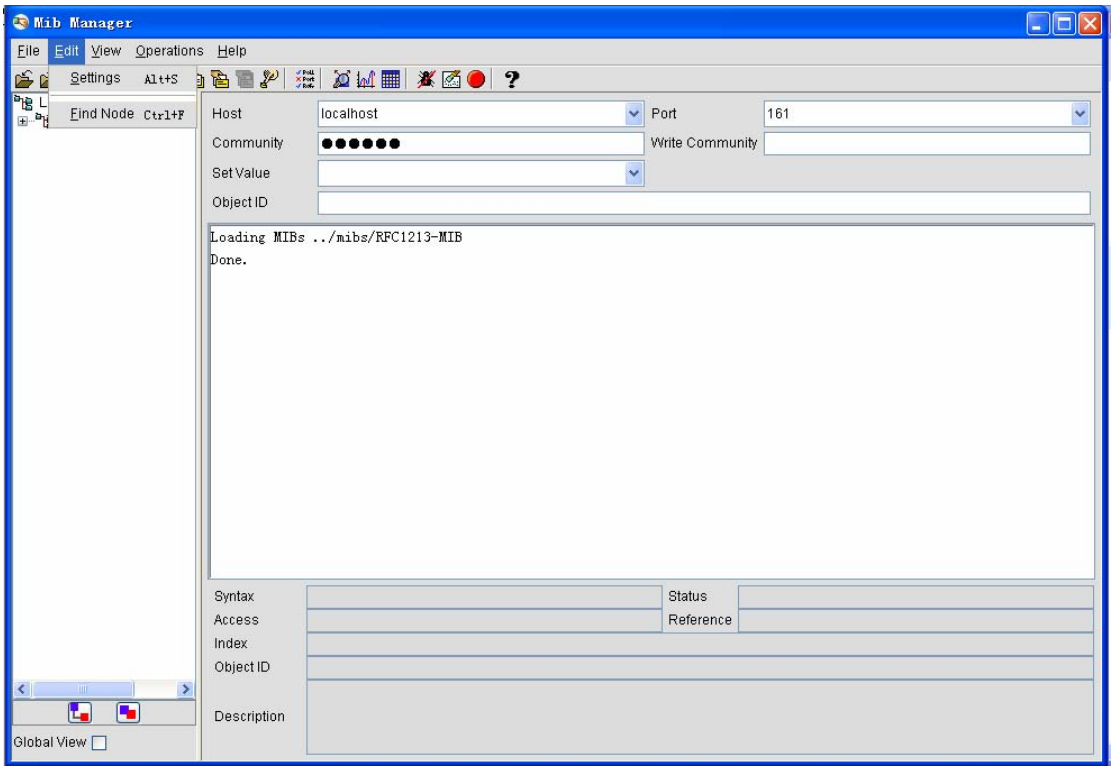
- **File menu**



- Upload MIB: Upload the MIB file in the MIB browser.
- Uninstall MIB: Uninstall the selected MIB files.
- Upload all MIBs: Upload all previously uploaded MIBs.
- Uninstall all MIBs: Uninstall all uploaded MIB files from the MIB tree.
- Save results: Save the MIB query results.
- Print results: Print the MIB query results.

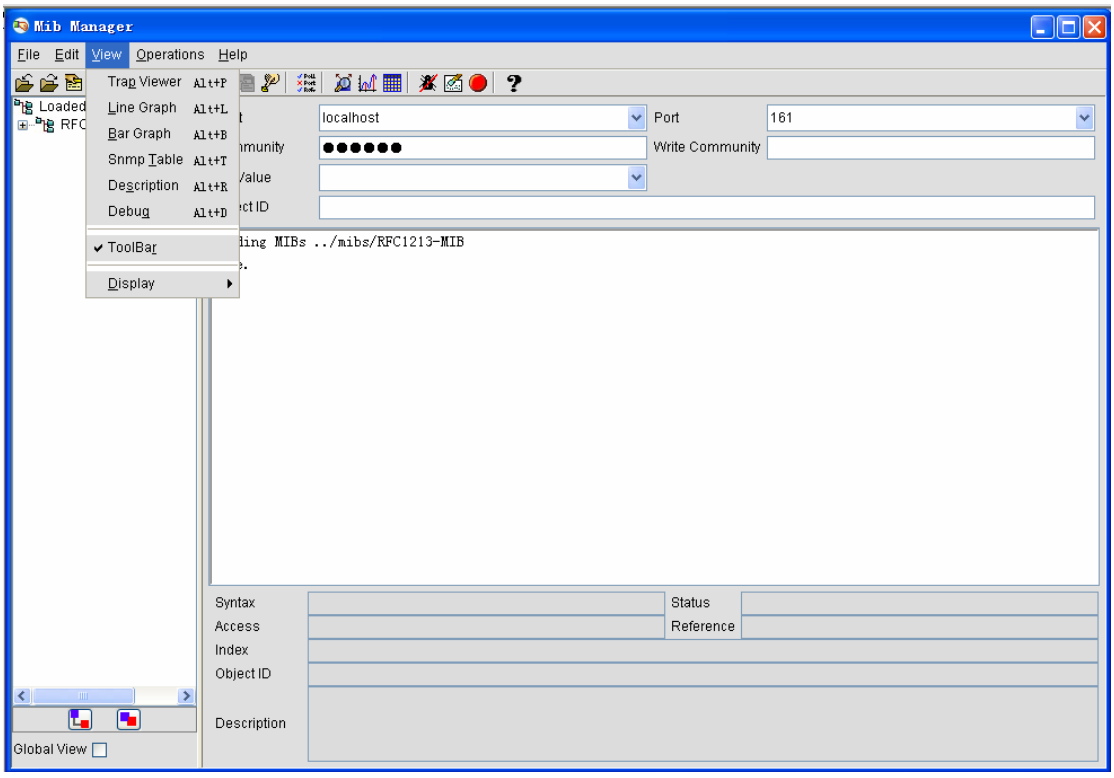
All lately uploaded MIBs (stores up to 5 file names) are listed out in the bottom of the menu.

- **Edit menu**



- Set: It is used to set the MIB browser.
- Browse the node: It is used to search for a required node.

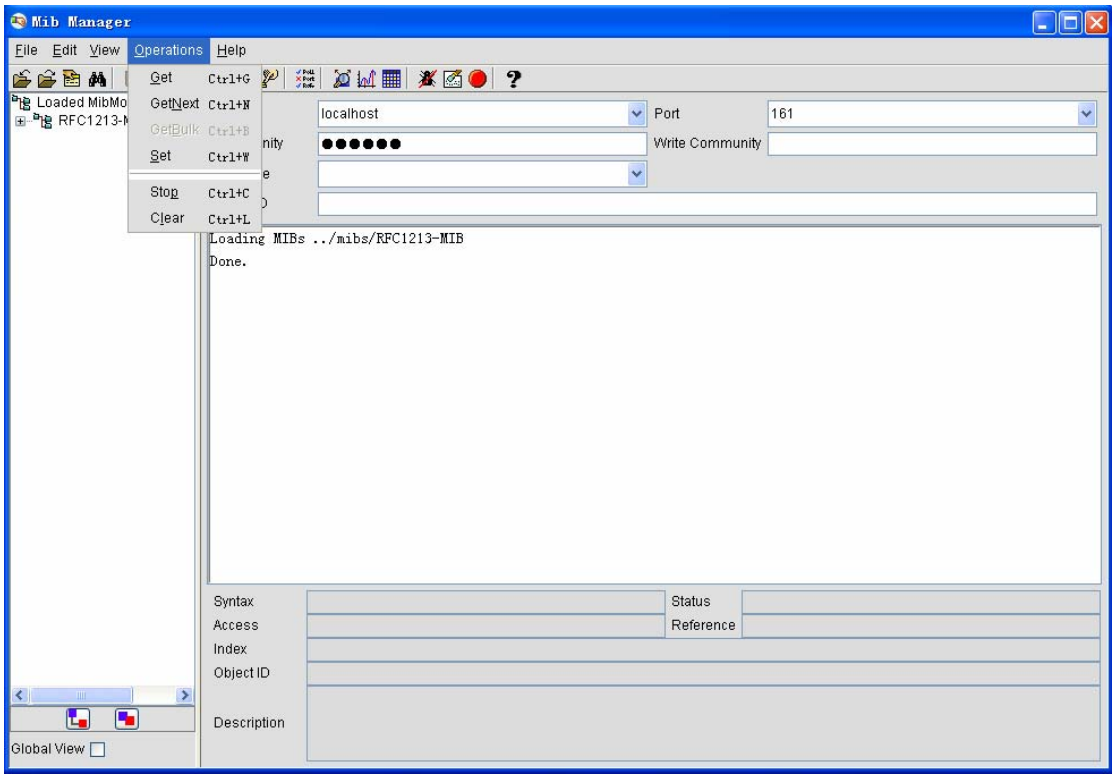
- **Show menu**



- Trap observer: It is used to browse and resolve all received traps.

- Linear graphic: It is to browse the value in the linear graphic.
- Histogram: It is to browse the value in the histogram.
- SNMP table: It is used to browse the SNMP table.
- Description: It is used to browse the description of a selected node.
- Debug: It is used to browse the debug output.
- Toolbar: It is used to show or hide the toolbar.
- Show: It is used to switch over the current view.

- **Operation menu**

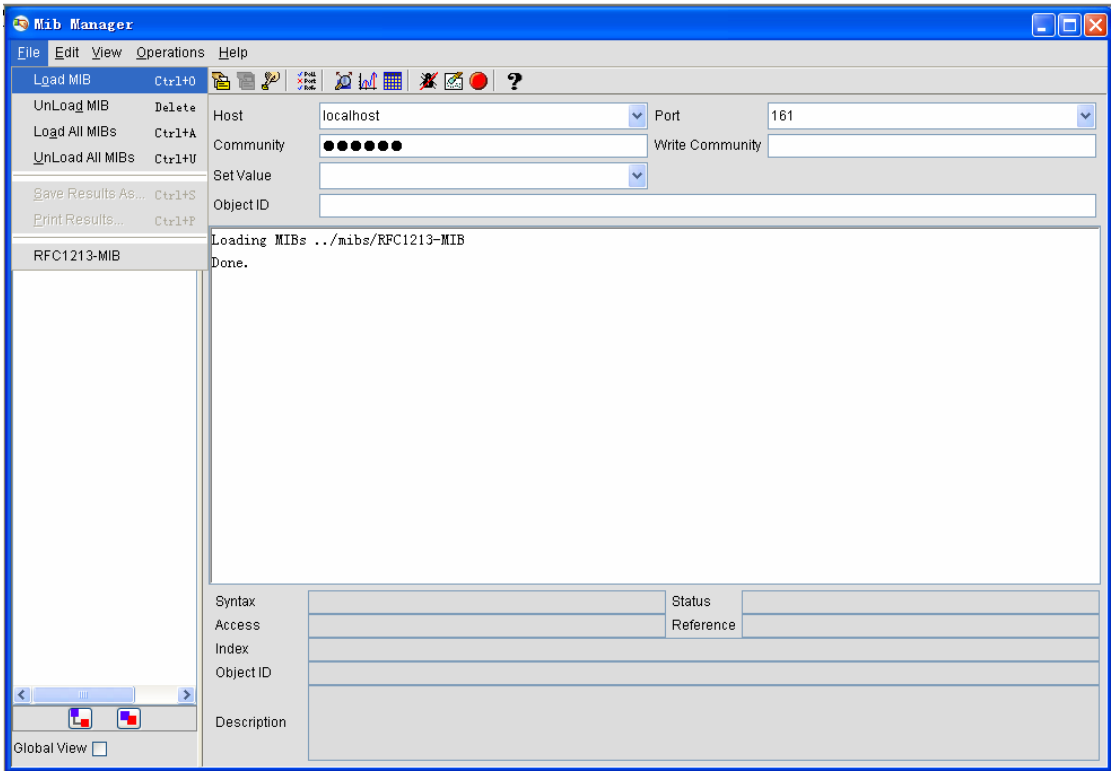


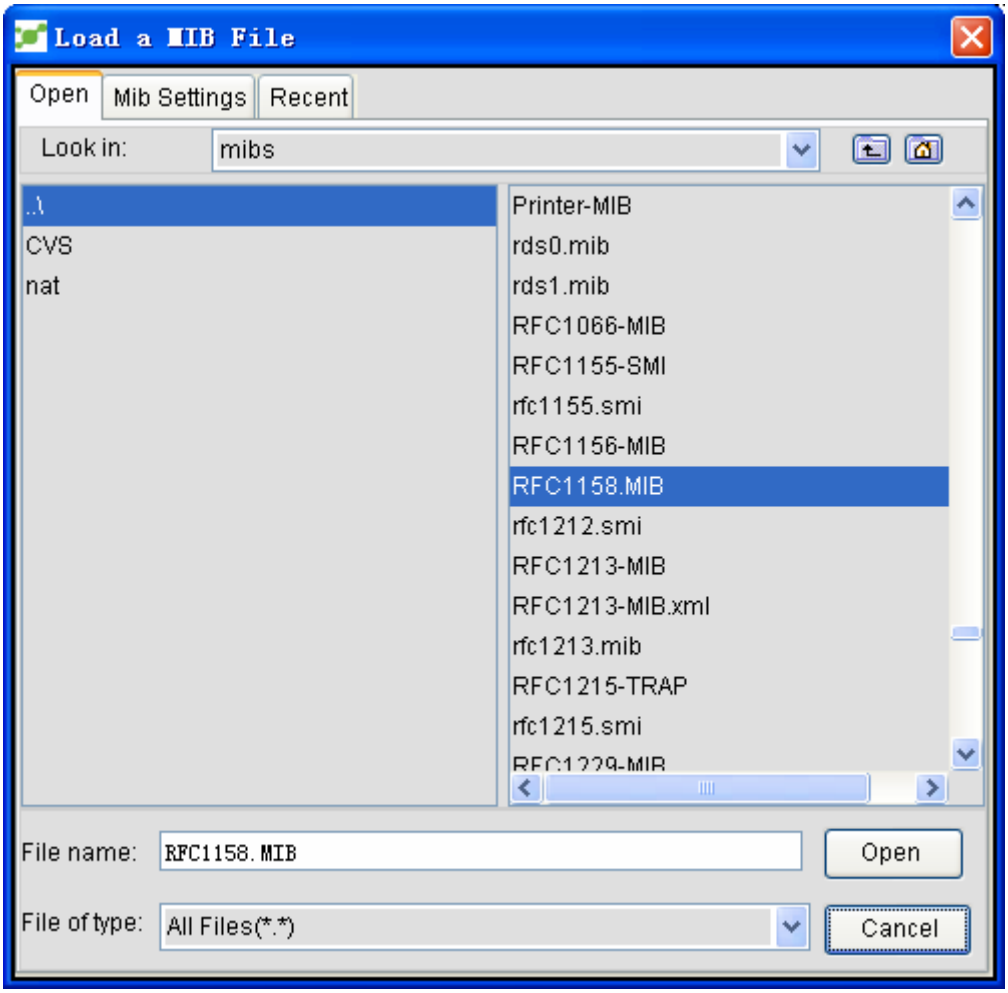
- Get: It is used to conduct a SNMP GET operation.
- GetNext: It is used to conduct a SNMP GetNext operation.
- GetBulk: It is used to conduct a SNMP GetBulk operation, v2c & v3.
- Set: It is used to conduct a SNMP Set operation.
- Stop: It is to stop the query.
- Clear: It is used to remove the query results in the textbox. information.

11.1.3 Uploading MIB

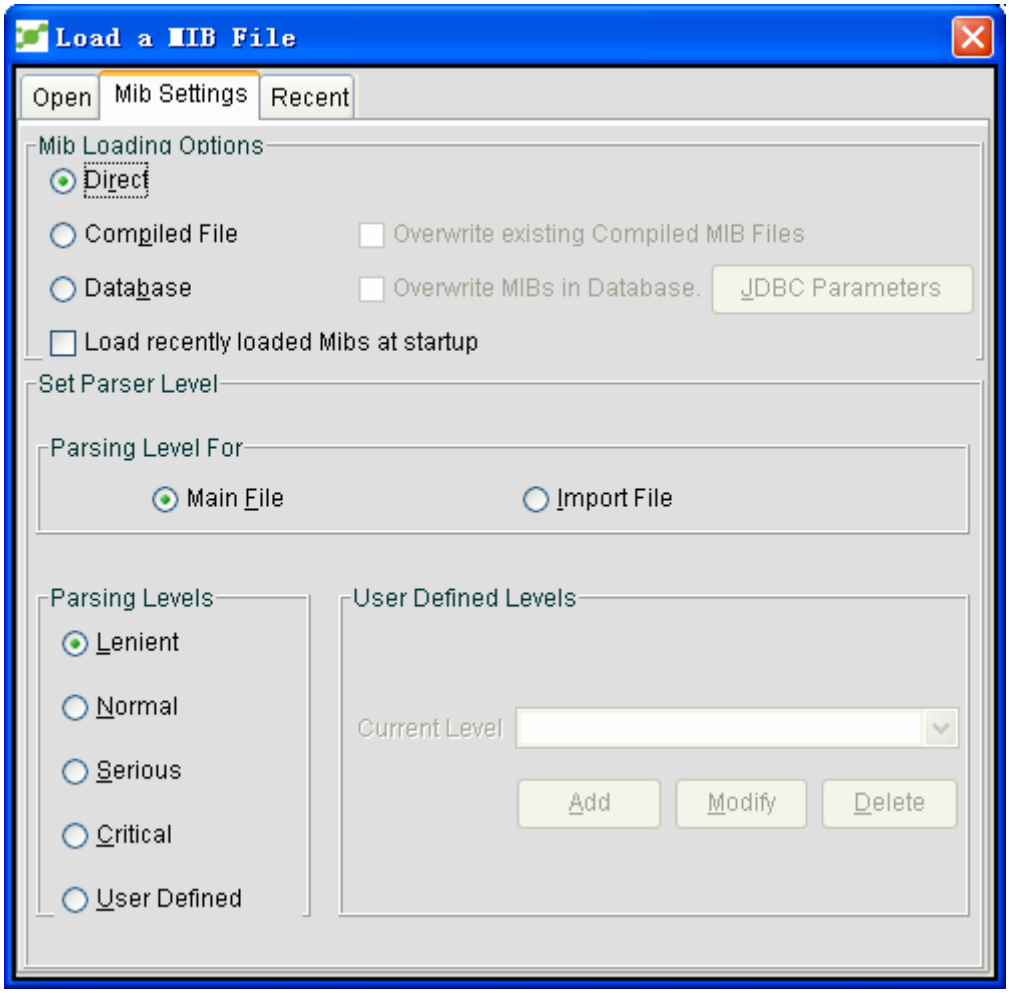
To upload the MIB files, do as follows:

Click **File -> Upload file** or directly click in the toolbar. The **Upload MIB** dialog box opens, as shown in the following figure:


Mib Manager
File Edit View Operations Help
Load MIB Ctrl+O
UnLoad MIB Delete
Load All MIBs Ctrl+A
UnLoad All MIBs Ctrl+U
Save Results As... Ctrl+S
Print Results... Ctrl+P
RFC1213-MIB
Global View
Host localhost
Port 161
Community
Write Community
Set Value
Object ID
Loading MIBs ../mibs/RFC1213-MIB
Done.
Syntax
Status
Access
Reference
Index
Object ID
Description



Click **MIB Settings**. The **MIB setup** window appears, as shown in the following figure:



The MIB browser provides the following options to upload the MIB:

- Directly upload MIB.
- Upload MIB from the encoded files.
- Upload MIB from the database.

11.1.4 Uninstalling MIB

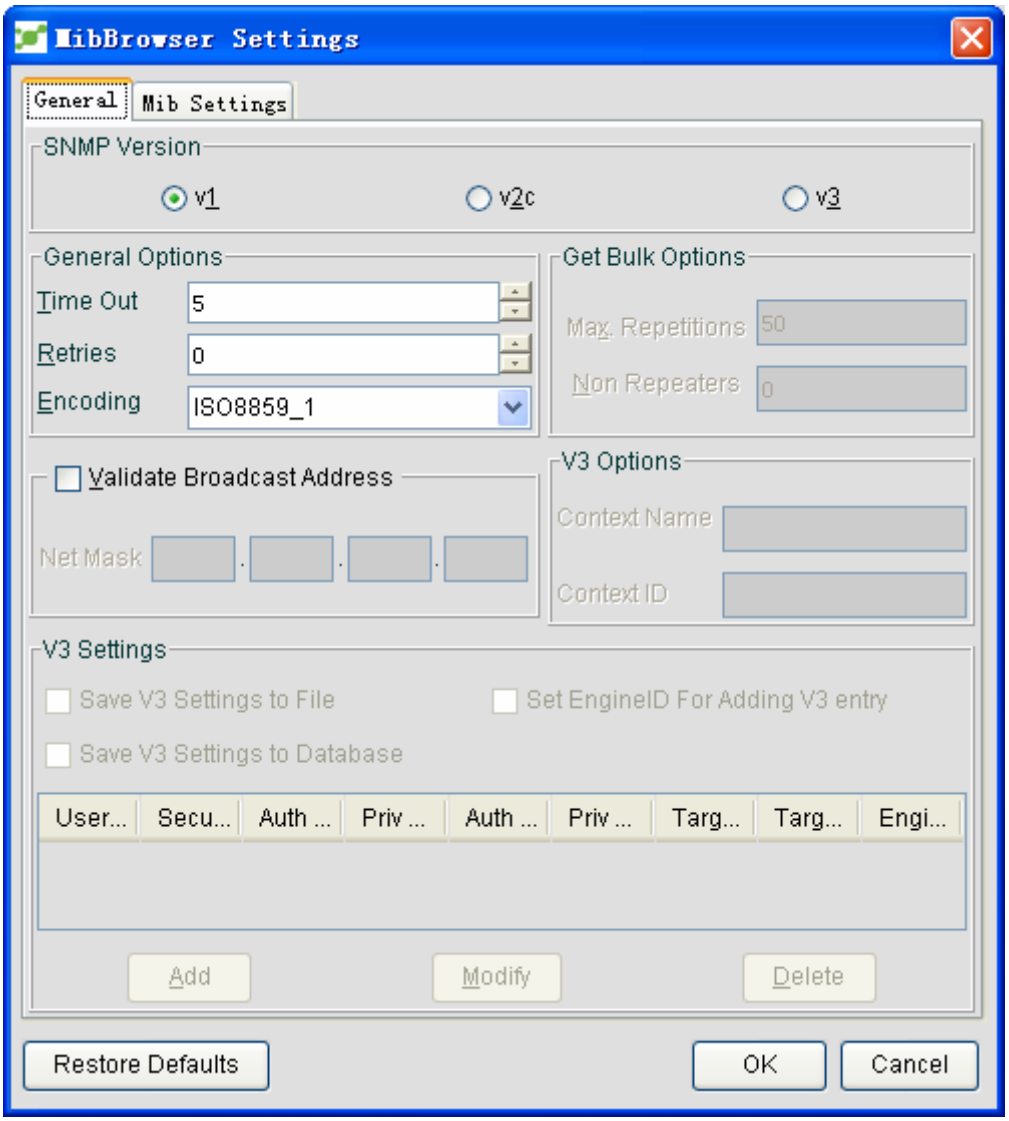
You can uninstall the uploaded MIBs through the following method:

Select a node in the MIB tree, and then click **File -> Uninstall MIB** or directly click to uninstall this MIB.

11.1.5 MIB Browser—Setup

You can set the MIB browser through the following operation:

Click E**dit -> Setup** or directly click The MIB browser setup window opens, as shown in the following figure:



The options in the **Common** attribute page of the **MIB browser setup** window are shown below:

Option	Default Value	Other Values
SNMP version	V1	V2c or V3
Timeout	5 seconds	User-defined value
Retry	0	User-defined retry times
Maximum repeated times	50	User-defined value
Diagram type	Linear graphic	Histogram
Trap port	182	User-defined port
Encode	ISO8859_1	User-defined value
Non-transmitter	0	User-defined value

11.1.6 MIB Browser – SNMP Operations

You can conduct some regular SNMP operations through the MIB browser, such as GET, GET NEXT, GET BULK and SET.

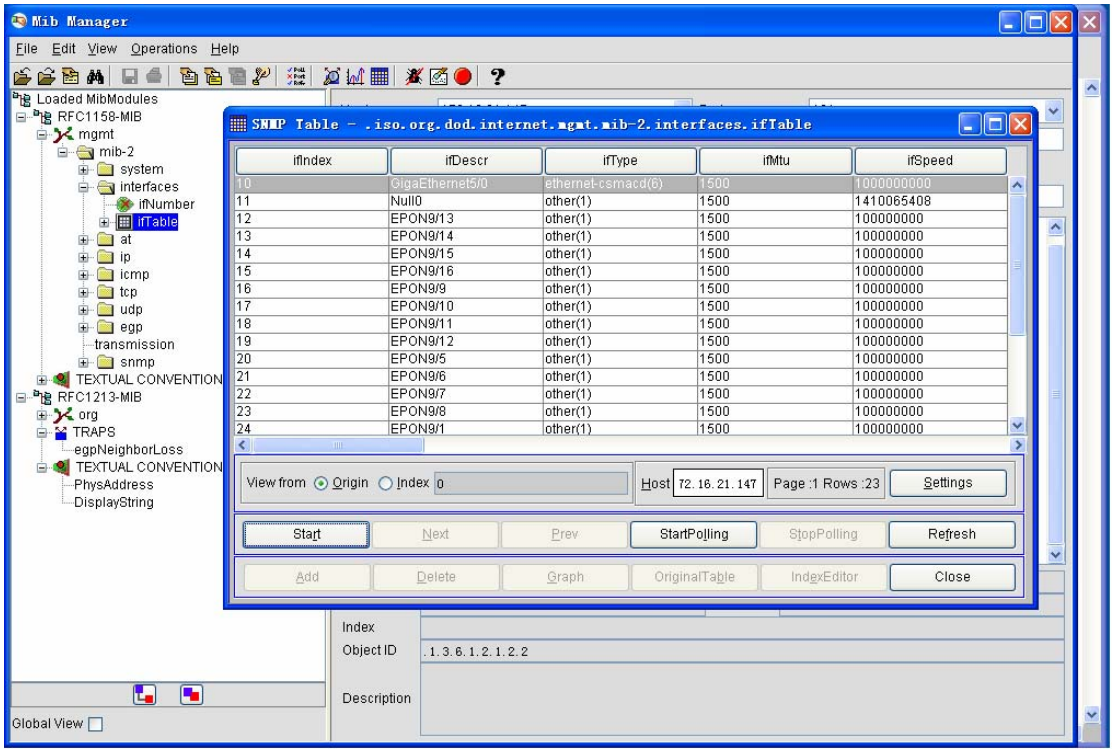
- To conduct a GET operation, select a node in the MIB tree and click or **GET**. The value of the selected MIB variable will be obtained.
- To conduct a GETNEXT operation, select a node in the MIB tree and click or **GetNext**. The value of the next variable of the selected variable will be obtained.
- To conduct a GETBULK operation, select a node in the MIB tree and then click or **GetBulk**.A series of next objects of the designated object will be obtained.
- To conduct a SET operation, select a node in the MIB tree, enter values in the textbox and then click **Set** or .

11.1.7 MIB Browser – Table Operations

The MIB browser provides a friendly window for users to browse the data in the SNMP table.You can browse the information in the SNMP table by performing the following procedure:

- Designate the host agent's name or IP in the host textbox in the MIB browser.
- Upload MIB in the MIB browser.
- Designate a valid OID (OID must be an OID table).

To browse the SNMP table, you must select a table variable and click the SNMP table. The system then displays the SNMP table.Click **Start** to get the details.See the following figure:

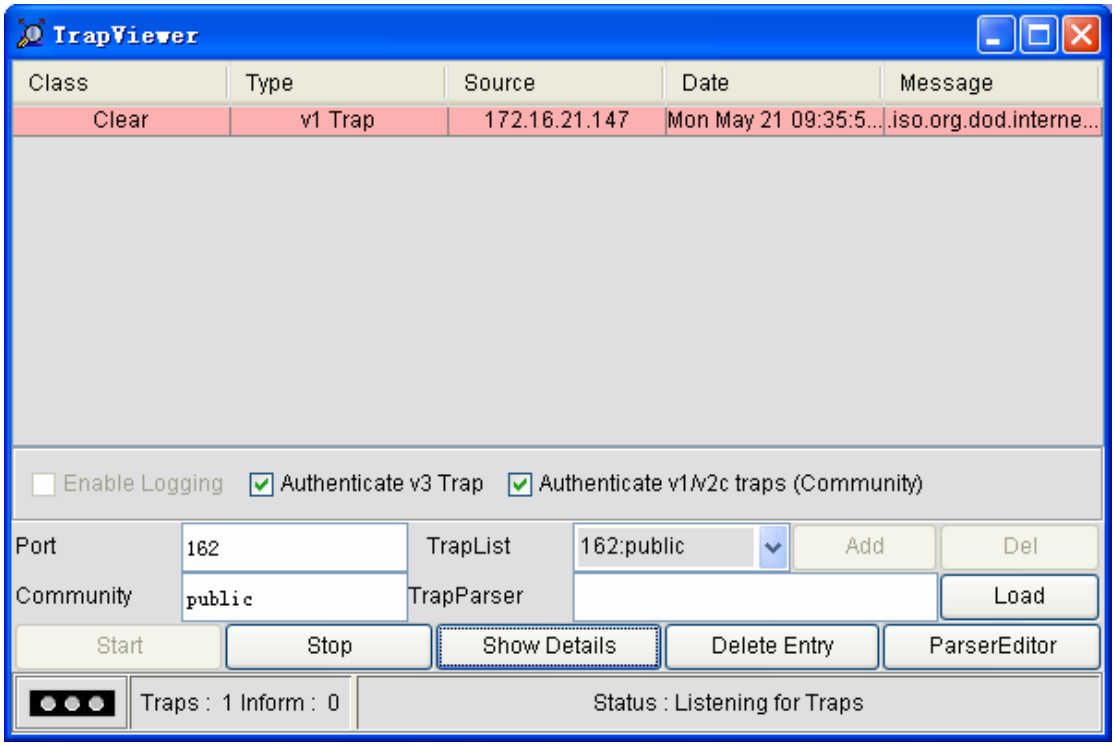


The related operations in the SNMP table faceplate are described below:

- Page: It has two options, that is, **Start** and **Index**.If the **Start** option is chosen, the table will be searched from its beginning.If the **Index** option is chosen, you need to set an index value in the textbox and the table will be searched from the designated value.
- Host: It is used to designate the host's name.
- Set: If you click it, a dialog box appears. You need to set the following options in the dialog box:
  - Polling interval: It is used to set the interval of table search.Its default value is 5 seconds.
  - Page size (row): It is used to set the number of rows in the search table.
  - Number of rows: It is used to set the number of rows shown in the SNMP faceplate.The default number of rows is 5.
  - Port ID: It is used to set the ID of a required port.
  - SNMP version: It is used to set the version of SNMP.
  - Search mode: It is used to set the search mode for getting the SNMP table's information.
- Start: It is used to start the search of the table.
- Next, Previous: They represent the next row and the previous row in the table respectively.
- Start polling: It is used to start the polling of this table.
- Stop polling: It is used to stop the polling of this table.
- Update: It is used to update the data in the table when the polling is stopped.
- Add: It is used to add a row to the table.
- Delete: It is used to delete a row from this table.
- Curve: It is used to show the change trend of a selected variable.

11.1.8 MIB Browser – Trap Oberser

The trap oberser is used to receive traps.After you set the port ID and the community name in the trap oberser, the received trap information will be displayed in the table.See the following figure:



Related explanations about the trap observer are shown below:

- Trap table: It is used to list all received traps.
- Port: It is used to designate the port which the observer will monitor.
- Community: It is used to set the value of the community.
- Trap list: It is a trap list dropdown box.
- Trap resolver: It is used to upload the trap resolver files.
- Start and Stop: They are used to start and stop trap monitoring respectively.
- Details: It is used to check the detailed information about a trap.
- Delete trap: It is used to delete a trap from the trap list.
- Resolution editer: It is used to open the resolution editer.

11.1.9 MIB Browser -- Curve

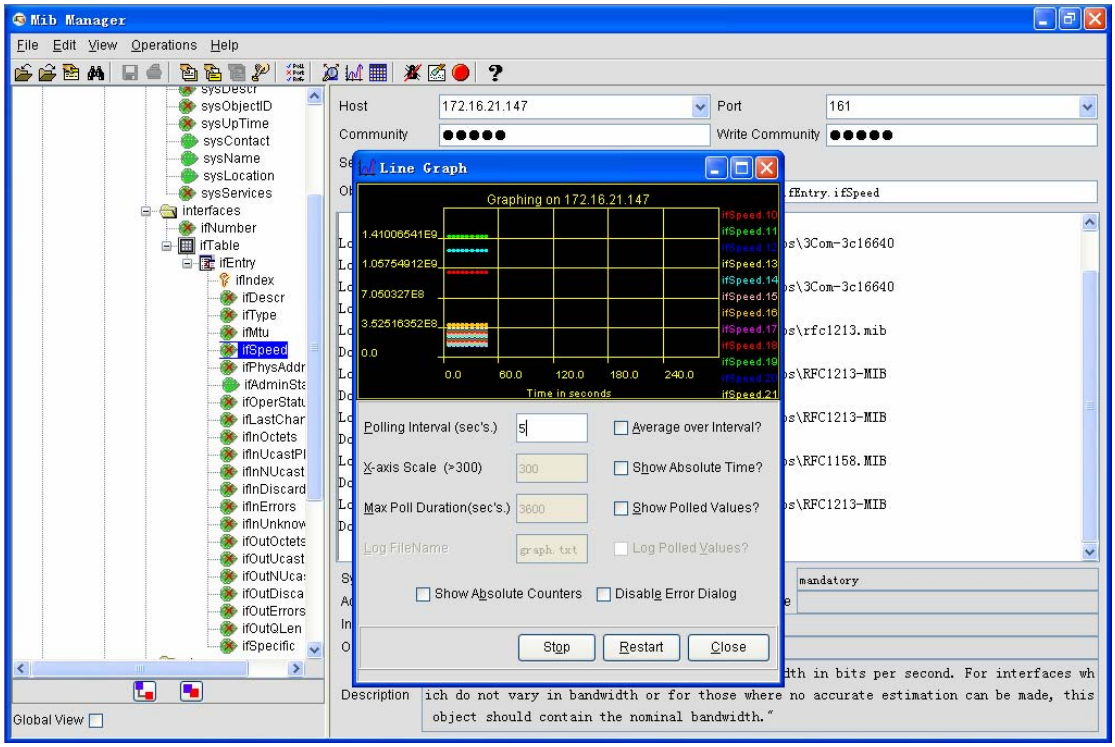
The MIB browser can draw the curve of SNMP data in real time.The system supports two kinds of curves: Linear diagram and histogram.The polled SNMP variable must be an integer or no-character integer.

You can follow the following procedure to draw the curves of the SNMP data:

- Designate the host agent's name or IP in the host domain in the MIB browser.
- Upload MIB in the MIB browser.
- Designate a valid variable (note: this variable must be an integer or a non-character integer).

Click Show -> **Linear diagram/Histogram** or directly click . An automatically updated diagram appears, showing the OID polling results of the designated agent.By default, a polling will be conducted every 5 seconds.

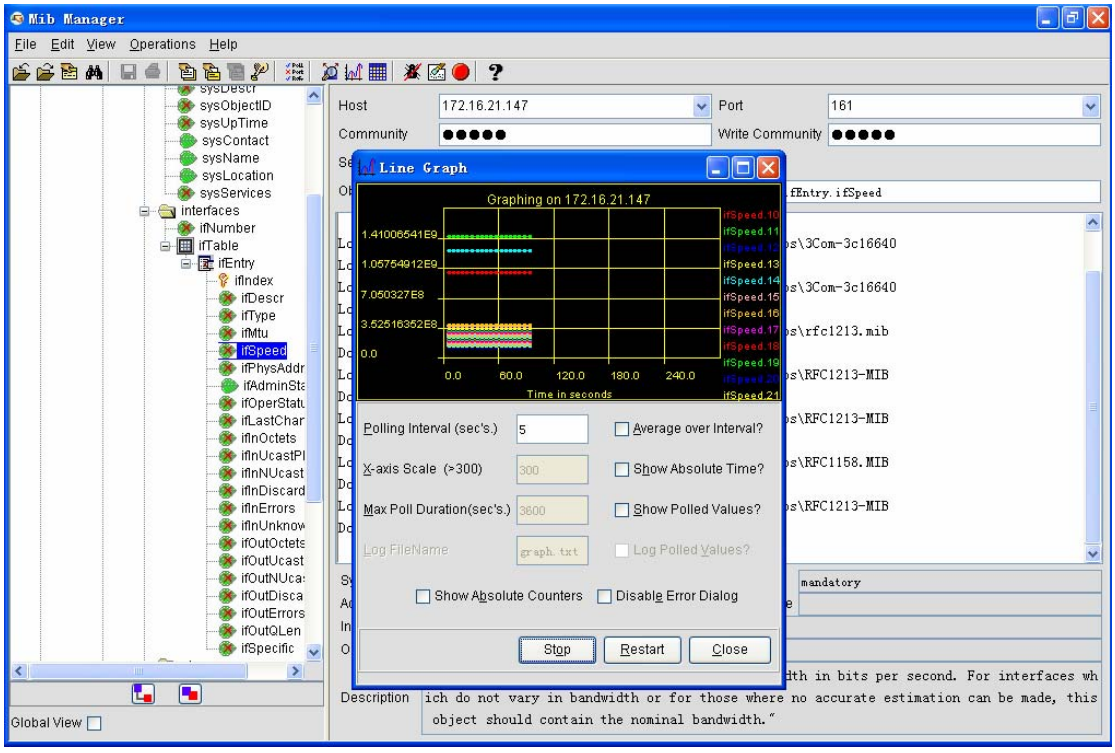
The following is a simple linear diagram:



You can set the related options on the above-mentioned window:

- Polling interval: you can enter a value as the polling interval, whose default value is 5 seconds.
- Get the average value of the polling interval: It is used to get an average value of a given polling interval.
- X axis' scale: It is used to set the X axis' scale, whose minimum value is 300 seconds.
- Show absolute time: It is used to show the time in the "hour:minute" format or in the "second" format.
- Maximum polling time: It is used to set the maximum time that the curve can draw.The default value is 3800 seconds.

- Show the polling value: If it is selected, all polling values will be shown in an accurate cycle.By default, it is forbidden.
- Log file name: It is used to set the name of a log file.By default, the log file is named as **graph.txt**.If you select **Write polling values into the log**, all polling values will be recorded in the file.
- Write polling values into the log: If it is clicked, all polling values will be recorded.By default, it is forbidden.
- Show the absolute counter: It is used to show the absolute values.By default, the curve only draws the differences between two values.
- Stop: It is used to stop the variable polling.Reboot: It is used to restart the polling.Close: It is used to close the curve.

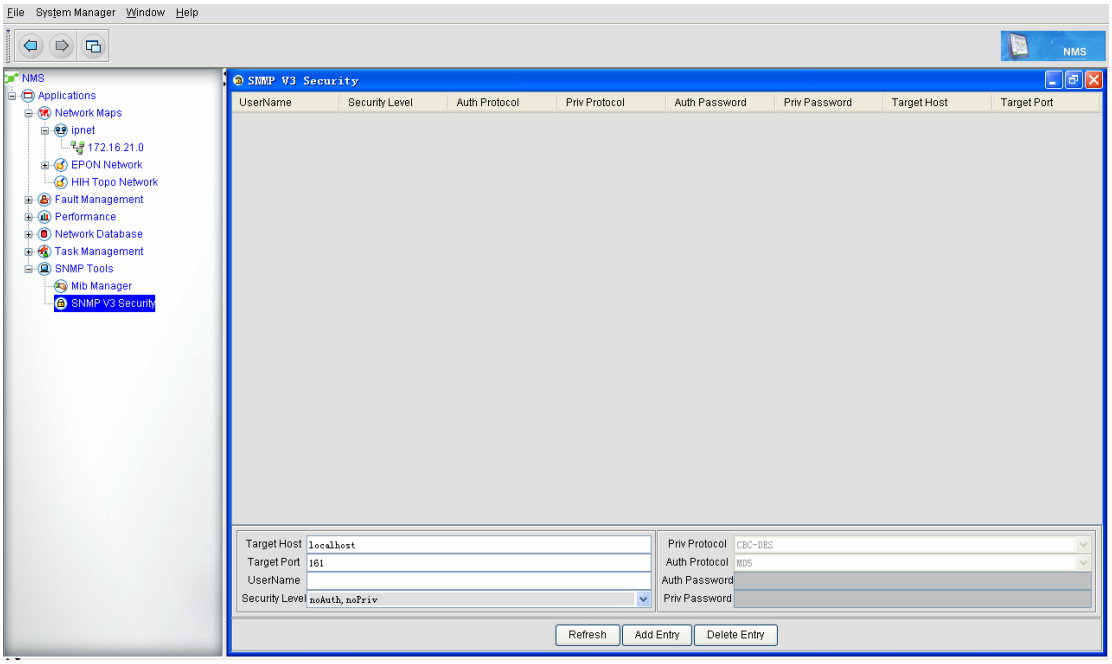


11.2 SNMPv3 Security

SNMPv3 has three important services: ID checkup, ID encryption and ID access control.Each SNMP entity includes a SNMP engine.The SNMP engine has the following functions: Sending and receiving information, ID checkup, data encryption and de-encryption, and access control.Multiple applications, which are set by the SNMP engine, consist of a SNMP entity.NMS supports the SNMPv3 protocol.

11.2.1 Adding the Protocol Information

Click **SNMPv3 security** to open the following window:



The options in the above-mentioned figure are described below:

- Destination host: it stands for the IP address of a managed device.
- Destination port: it stands for the SNMPv3 port.
- Username: It is used to set the to-be-verified username.
- Security level: there are two security settings: Auth (authentication) and Priv (privacy). The two security settings consist of three options: "noAuth, noPriv", "Auth, noPriv" and "Auth, Priv".

  Auth: it means authentication. After you select it, you shall select the related protocol (MD5 and SHA) in the **Authorized protocol** dropdown box.Enter the password in the **Authorized password** box.

  Priv: It stands for privacy, corresponding to the **Priv password** box.If you select this option, you shall enter the password in the **Priv password** box.

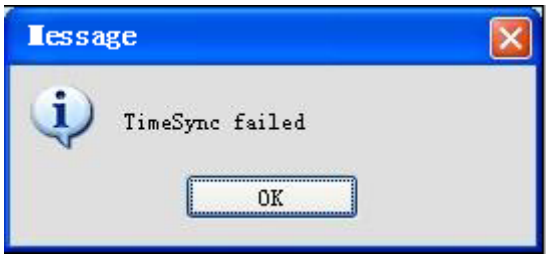
  noAuth,noPriv: it means not to require authentication, authorization and encryption.

  Auth,noPriv: it means to require authentication and authorization, but not encryption.

  Auth,Priv: it means to require authentication, authorization and encryption.
- Priv protocol: it means to support the encrypted protocol information.This option is not available for you to enter values.
- Authorized protocol: It has two options: SHA and MD5.
- Authorized password: If you choose **Auth** for **Security level**, you need to enter a value here.
- Priv password: If you choose **Priv** for **Security level**, you need to enter a value here.

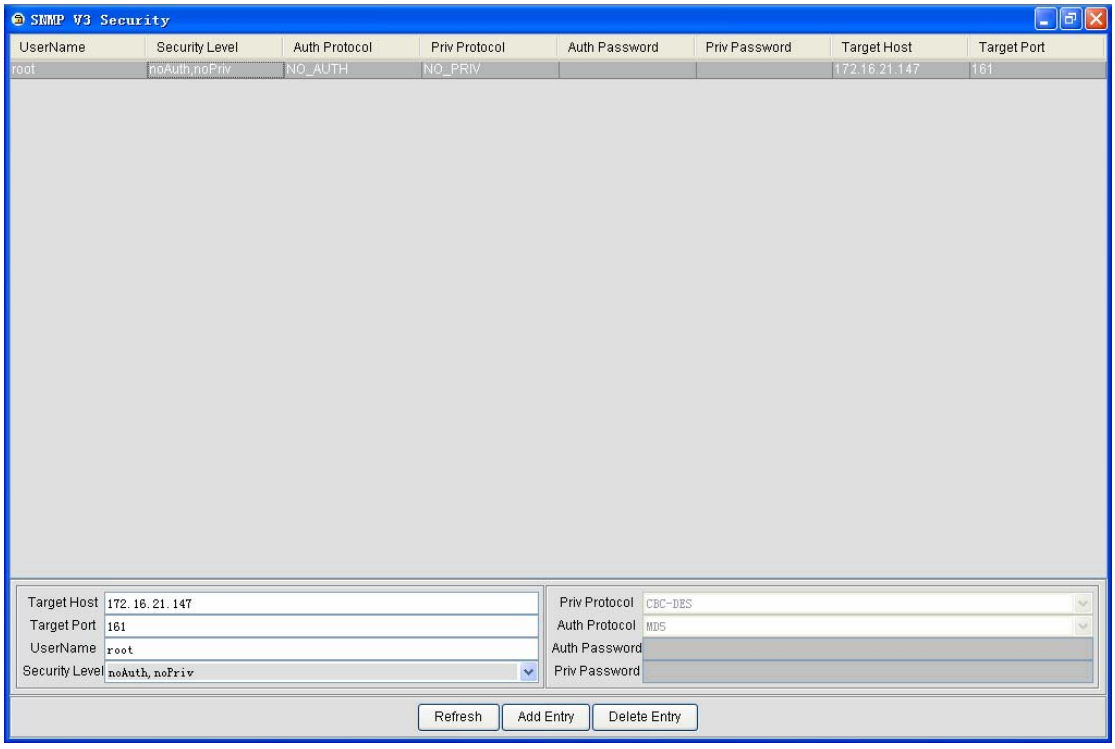
After you enter the corresponding data and click **Add entry**, the entered data will be added.If

the data is successfully added, the data will be shown on the above-mentioned table.If the data fails to be added, an alarm message will appear, as shown in the following two figures:



11.2.2 Changing the Protocol Information

Click a row in the table to show the related data at the bottom area.See the following figure:



After modifying some data, click **Update**. These data will be updated.

11.2.3 Canceling the Protocol Information

To cancel data, select a row in the table and then click **Cancel entry**.There is no notification when you cancel data, so please be cautious when you conduct this operation.

Appendix 1 Operation Problems about NMS Server

Q1: The NMS server cannot be run

A: In general, after the NMS server is installed the system will automatically upload services and start the NMS server.However, in some special cases, the NMS server cannot be started or the NMS server fails to be connected after the client is started.We list out all the reasons one by one and help users to use this NMS server better:

1) Overdue license

If the license overdued during server startup, it means that the trial version is overdue and the NMS server therefore cannot be started. To solve this problem, you shall start the **NmsReg.exe** program in the **Installation -> Bin** directory and then enter the sequence ID and the corresponding license file according to requirements. It is OK after the NMS server is rebooted.

2) Chinese characters exist in the installation path

If there are Chinese characters in the installation path, the third-party Apache software cannot work normally. It is OK if the installation path has no Chinese characters.

3) MySql has been installed before

Our installation program includes a third-party **MySql** database.If you have previously installed the MySql database, the NMS server cannot be started.The solution is to find the **my.ini** file in the C disk and then delete it.

4) Improper operating system and language version

At present, the NMS server supports the following platforms: Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista and Windows 7.

5) Port 9090 is occupied

The running of this NMS server needs to start port 9090. If port 9090 is occupied, the NMS server cannot be started.In this case, you need to use **netstat –ao** in the command line of the operating system to check whether a process occupies port 9090. If a process occupies port 9090, you need to shut down the ID of this process.

6) The NIC is not activated and the license cannot be authenticated

Our authentication mechanism is bound to the NIC. If the NIC of the NMS server is not activated or the NIC is not connected, the license cannot be authenticated.Before starting the NMS server, make sure that the host on which the NMS server is installed has activated its NIC.

7) Check whether the server was normally shut down last time

If there are **Mysqlm**, **rmi register**, and **apache** in the process list, it indicates that the server was shut down abnormally. The system therefore cannot be started normally. To solve this problem, you need delete the **MySql.exe** process, the **rmiregistry.exe** process, the **apache.exe** process and the **java.exe** process in **Windows task manager** and then restart the server.

8) The current user has no write permission towards the installation path

Run **/bin/startPostgreSQL.bat** in the DOS window. If the following information appears,

check whether the current user has the write permission to the installation directory.

Q2: Why cannot the traps be received?

It has the following reasons:

1) The trap host is not set and its IP address is not the IP address of the current network management host.

In this case, you need to check whether the **Trap host** option is set during the configuration of the command line and set the IP address of the trap host to be IP address of the current network management host.

2) Port 162 is occupied.

You can use the **netstat –ao** command to check whether port 162 of the current network management host is occupied by other process.If it is occupied by other process, you shall shut down the network management software (NMS) and then release port 162 and then restart NMS.

3) The firewall of the NMS server blocks port 162.

If port 162 is not occupied by other process but the trap message cannot still be received, check whether the firewall of the NMS server blocks the trap message of port 162.If the firewall blocks the trap message, you need to close the firewakk and then restart NMS.

4) Check whether there are 3 switches in the command.

解答：You shall add **trap host x.x.x.x community authentication snmp configuration** in the command line during the command line configuration.

Q3: The hand-in-hand topology cannot be discovered.

To find the EPON hand-in-hand topology, you shall set the standard SNMP options and the trap and then other related requirements.Do as follows:

1) Use the **epon ip-address** command to ser the device.

In the hand-in-hand topology, two OLTs connect the same ONU through their PON ports. The PON port of the current active OLT needs to record the IP address of the OLT on which the peer PON port locates. During the shift of the PON ports, OLT needs to know which IP address shall be written into the ONU's information.Before discovering the hand-in-hand topology, OLT must set **epon ip-address x.x.x.x**.

2) After PON port shift, ONU needs to record the IP address of the peer OLT.

In the hand-in-hand topology discovery, the PON port of the OLT on which the current online ONU locates needs to record the address and index of the PON port of another OLT.The premise to record this information is that ONU has been registered on two PON ports. In general, after ONU is registered, you shall switch the current ONU over on another PON port and then switch it back. In this way, the ONU information will be recorded on two PON ports of two OLTs.

Q4: A device cannot be discovered or its type cannot be identified.

All device types can be detected and their models can be displayed in normal case if you click **Real-time management -> Topology discovery**. But in special cases, the devices cannot be discovered or the device types are incorrect even though the devices are discovered. The possible reasons are listed below:

1) Check whether this device's SNMP attribute is set.

During discovery settings, the SNMP community of a device should be set. If device discovery fails, you need to confirm whether the device has contained the SNMP community settings.

2) Check whether the community used during discovery is the same as that of the device.

When you conduct the discovery settings on the NMS terminal, guarantee the community of the NMS terminal and that of the device terminal are same.

3) Check whether a device can be reached.

When device discovery fails, you should test whether the device can be detected. You can ping it or conduct SNMP operations on it. If the two operations can be done successfully, the device is reachable.

4) The network condition is poor or the device response times out.

In this case, click **Real-time management -> Discovery configuration -> Regular -> Initialized parameter** to set a relatively big value for SNMP timeout time and retry times.

5) The device type is not supported by the NMS server.

A device type cannot be detected correctly, but all SNMP configurations are correct.In this

case, you need to check whether the current NMS server supports the device type. You need to communicate with related testers and rearchers. Generally speaking, the latest released device types may not be supported by the NMS server.

6) If ONU type cannot be identified, check vendor ID and model ID.

Before ONU discovery, check whether the ONU version is compatible with the NMS server's version (both are NMS versions, neutral versions, or customized versions).

7) The EPON device cannot be discovered, or the EPON device is not displayed in the EPON network tree node after the EPON device is discovered.

In this case, the most possible reason is that the PON card of the current EPON device is not started or the type of the PON card cannot be identified by NMS.You should conduct the SNMP operations to check whether the current PON card can be identified on the device layer.The OID of the SNMP table is 1.3.6.1.4.1.3320.3.6.10 (bdcardTable). For the SNMP operations, see figure 2.Check whether the **bdcardDescr** option in the SNMP table contains the type of the corresponding PON card.If it contains the type of the corresponding PON card, the device can be identified; if not, the correspinf card cannot be discovered.

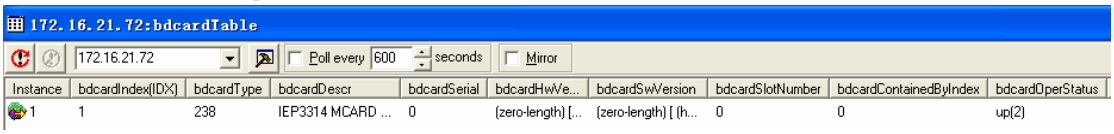


Figure 2: SNMP operations of the PON card's type

Q5: The settings cannot be distributed through the NMS window.

Do as follows:

1) Check whether the device type is normal.

Ping or telnet a device to check whether it is reachable.Then perform the SNMP operations to check whether the device responses.

2) Check whether a device can be reached.

Conduct the SNMP operations.

3) Check whether the write community is set on NMS.

Check whether the community of the device, which is accessed currently be the NMS, has the write permission.

4) Other reasons exist, such as the device itself is abnormal.

If all above-mentioned options have no problems, try to distribute the same settings on the device terminal through the telnet or console mode and see whether it can be done successfully.If it is done successfully, the **snmp set** operation of the device terminal has problem. If it fails, the

device itself is abnormal. In this case, please contact related technicials or researchers.

Q6: The client cannot log onto the server.

Because NMS server is in C/S mode, you need to start the NMS server and the server at the client terminal. The NMS window then appears.If the NMS window does not appear, do as follows:

1) Check whether the server is normally started.

Check whether the NMS server is successfully started by clicking **Start log** at the right bottom corner of the NMS server.What’s more, you can check the log files in the **logs** directory of the installation path to see whether the NMS server is normally started.

2) Check whether the login password is correct.

If the server is normally started but cannot be logged, please check the username and the password are right.

3) Check whether the IP address of the server is correct.

When logging on to the client, click **Advanced** and check whether the IP address and port of the server, which you enter on the cureent client, are the same as those of the real server.

4) Check whether the communication between the client and the server is normal.

If the server cannot be connected, ping on the client the corresponding port of the server to see whether the port can be connected.

5) Check whether the firewall of the server is enabled.

If the server cannot be connected, it is possible that the firewall of the server blocks the current communication. So you should check this case.

Q7: The NMS window has no response.

A client is successfully enabled, but after an operation or just after a while the client's window has no response if you click this window. The possible reasons are shown below:

1) Uncertain window exists in the backstage.

In many cases, you open a lot of windows and do related configurations at the same time. The current window may cover the dialog box of the NMS window.In this case, press **ALT** and **TAB** at the same time to switch over to the dialog box of the NMS window.

2) The network is slow or CPU is busy.

Due to heavy load, the window of the NMS client may not response to the cursor’s or keyboard’s operations.In this case, you'd better wait for a minute.If there is no response for a long time, you can close the NMS client and restart it.If the NMS client cannot be connected, you need to restart the NMS server.It is noted that you store the logs about abnormities and send these logs to our technicians for problem locating and resolving.The storage address of the client’s logs is the **clientlog** folder under the installation path, while that of the server’s logs is the **logs** folder under the installation path.

Q8:During the removal of the PON port, the plug or insertion operation cannot be done simultaneously or rapidly, or the devices cannot be fully displayed or deleted.

In some cases, you may remove a PON card on a slot to another slot of the local machine.The NMS has to process ONUs and PON cards one by one and, if the number of related PON cards and ONUs is large, NMS needs to take a lot of time. So if you want to remove one PON card and then another one, the interval should be at least several minutes.

Q9: If you start multiple servers and at the same time access devices or conduct operations to the devices, the read and access or the settings will time out.

The response of SNMP packet on a device is a single-process one, so only one SNMP request can be answered at a time.So when you conduct SNMP operations to a device, you should avoid starting multiple NMS servers at the same time.

Q10: During device discovery, you may discover a device in the IP network but cannot discover it in the EPON network all the time.

The reason may be that it times out when SNMP obtains related MIBs or that the PON card is not inserted when this device is detected.To advoid this case, you should first detect the device in the IP network topology, delete it from the IP network topology and then rediscover it in **Discovery Management**.(If the network is good and the device is not busy, this case will not occur; otherwise, packet loss occurs or the SNMP request times out)

Q11: The device's status on the topology cannot be updated

In most cases, the real-time update of the device's status or line's status on the NMS window depends on the trap message, which is transmitted from a device. Furthermore, when a trap message is sent and its IP address is not designated, the IP address of the trap message is an address, which is in the same network segment with the trap host's address.If the IP address of the trap message, which is transmitted by a device, is not the IP address of the device when NMS detects it, NMS may regard that this device is not discovered after receiving the trap message and therefore cannot update the real-time status.

Q12 How to backup the NMS database regularly?

Considering the complexity of the real network and historical data backup, NMS provides the function of regular database backup. For details, see the database backup function at the **Task Management -> Task Configuration** directory.

Q13: The configured tasks fail to run.

The running of a configured task relates to a lot of function configurations. If a problem occurs in any function configuration, the configured task cannot be run normally.

1) The Telnet authentication information is not set for a device.

During execution of configured task, the administrator needs to conduct related settings to the device through Telnet. Hence, you have to conduct the Telnet authentication on the device.

2) The task operation times out due to network congestion and heavily loaded CPU.

You have to wait for a few minutes and then reset and run it.

3) The third-party TFTP server cannot access the IP layer of the device.

On failing to execute a configured task, you have to confirm whether the communication between TFTP server and device is normal.

4) The device gets offline or the configuration information of the device is changed (add or delete ONUs).

Before setting ONU, you should check whether the current ONU is online.If the device is offline or disconnected for some reason, the settings and its distribution must fail.

5) When the NMS server is used as the operation source or destination, you should check whether the occupation of the TFTP port causes the TFTP

server to be started unsuccessfully.

In this case, you should check whether the TFTP port of the current NMS host is used by the current NMS.

Q14: Check whether the version of the installed server is consistent with that of the client.

The interconnection and startup of the server and the client may fail because the version of the client is inconsistent with that of the client.

Q15: Qestions about performance collection

1) **During the collection of historical performance, the server cannot display related data unless it has run for a long time.**

The system sets the historical performance collection interval to 5 minutes. After starting the server, you have to wait for at least 10 minutes and then the system shows the curve.

2) **Make sure that the RMON configuration has been done on the port on which the performance collection or historical collection is conducted.**

The performance data collection of an Ethernet port is realized through the RMON performance collection, so you must conduct the ROMN configuration before historical performance collection.

Q16: How to save the configurations?

After you have done related configurations on a device through the NMS, you have to save these configurations on the device by right clicking **Save configuration**.

Q17: Why can the boders of a button on the window not be displayed?

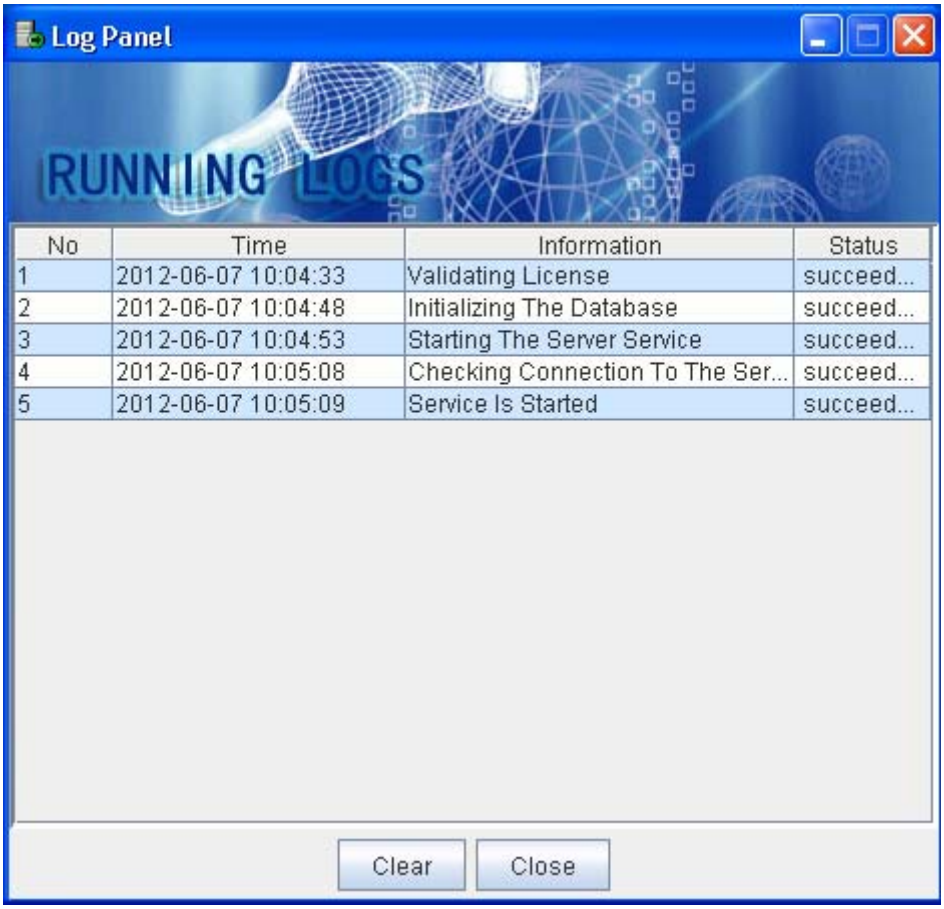
In some special cases, NMS is installed on the Windows operating system but its client's window cannot display some window components normally, such as the button, the table's head and the list.To solve this problem, you have to confirm whether the window style on the current Windows operating system is the classical one. If not, please set the window style to the classical style.

Q18: Why is Ifindex of a PON port inconsistent with the port description after NMS is closed and the device is restarted?

Each time you discover OLT and ONU, there is a unique index in the software corresponding to them. This unique index is also the system ID. The system ID may change after device reboot. In this case, the system cannot correspond to the related PON port and ONU correctly.Therefore, after device discovery, you should enter **write ifIndex** in the command line on the OLT.

Q19: After a service is enabled, the log window appears. But why is the log window then closed instantly?

Because the **mysql-d** process exists, you have to kill this process and then you can start the server. After the server is normally started, the following window appears.



Q20: Why is the icon of a switch or router a PC icon?

The possible reasons are shown below:

1. After OLT is restarted, its current settings is not saved and the SNMP related parameters in

the previous settings are discarded. The SNMP packets then cannot respond.

2. OLT is busy and the SNMP packets time out, which causes NMS to regard this device is not the SNMP device.

3. The community is entered incorrectly during NMS discovery.The community on the NMS server is not the same as that on the device.

The solution is:

You can delete the device that the PC icon corresponds to, check the configuration and the device and then rediscover this device.

Q21: In what cases device deletion and then device rediscovery should be conducted?

In the following cases, you should do as the above-mentioned:

1. All OLT configurations are deleted and then OLT is restarted.
2. PSG configuration is reset (specifying the PON port of a member again).
3. OLT is restarted without saving the **ifIndex** information.
4. The PON card is removed (the PON card is removed from one slot to another slot).

Q22: Why does it fail if you conduct device settings through the NMS window?

It has the following reasons:

1. The BIN version itself has problems and the corresponding MIB does not support.
2. The SNMP's write community on the NMS server is inconsistent with that on the device, so the settings is unsuccessful.
3. The device itself cannot be accessed or the network connection has problems.