

# **SysUpTime User Manual**

**Version 3.1**

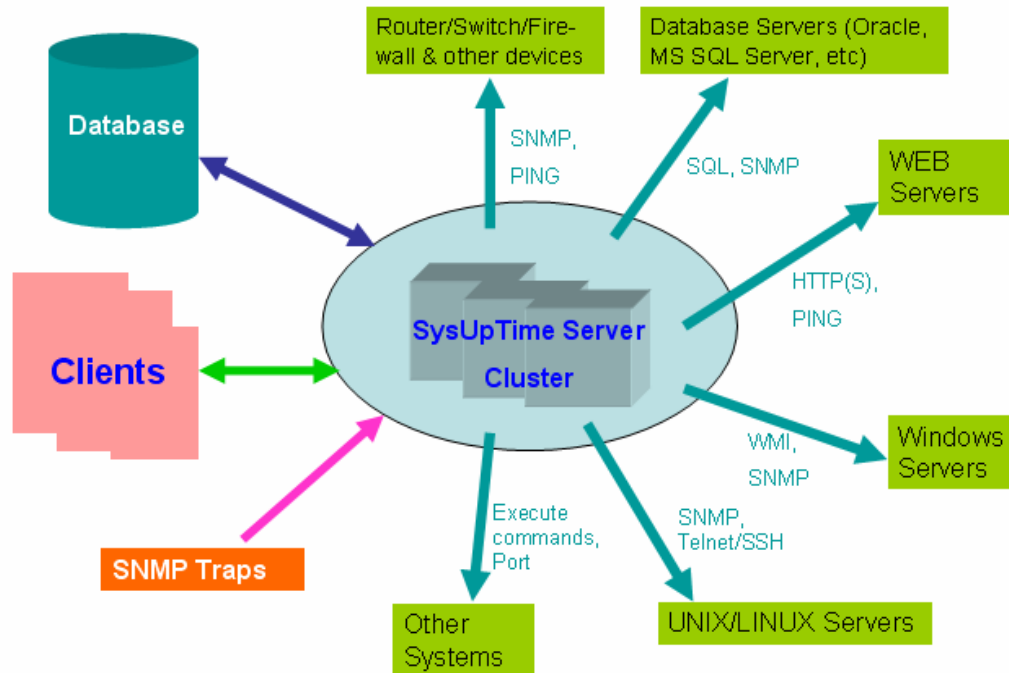
# Contents

<b>SYSUPTIME USER MANUAL</b>	<b>1</b>
<b>CONTENTS</b>	<b>2</b>
<b>CHAPTER 1. INTRODUCTION &amp; INSTALLATION</b>	<b>4</b>
<b>CHAPTER 2. USER INTERFACE</b>	<b>6</b>
LOGIN WINDOW	6
MAIN WINDOW	7
MENU	8
NETWORK EXPLORER WINDOW	10
NETWORK TOPOLOGY WINDOW	11
PROPERTIES WINDOW	16
<b>CHAPTER 3. USER AND VIEW MANAGEMENT</b>	<b>17</b>
USER MANAGEMENT	17
CHANGE PASSWORD	17
USER PERMISSIONS	18
MANAGE ORGANIZATION	18
CREATE CUSTOMER VIEW	19
<b>CHAPTER 4. NETWORK DISCOVERY</b>	<b>21</b>
START DISCOVERY	22
STOP DISCOVERY	26
PERIODICAL DISCOVERY	26
PARTIAL REDISCOVERY	26
DISCOVERY REPORT	26
VLAN MANAGER	27
DEVICE MANAGER	27
<b>CHAPTER 5. EVENT SYSTEM</b>	<b>29</b>
TRAP RECEIVER SERVER	29
ALARM BROWSER	30
<b>CHAPTER 6. PERFORMANCE MANAGEMENT</b>	<b>34</b>
ADD A NEW MONITOR	35
Common Form Values	36
Monitor Types	44
<input type="checkbox"/> DNS Monitor	44
<input type="checkbox"/> Database Query Monitor	44
<input type="checkbox"/> Directory Monitor	45
<input type="checkbox"/> E-Mail Monitor	46
<input type="checkbox"/> Monitor MS Exchange Server	49
<input type="checkbox"/> Command Executor Monitor	50
<input type="checkbox"/> File Monitor	52
<input type="checkbox"/> FTP Monitor	53
<input type="checkbox"/> Log File Monitor	54
<input type="checkbox"/> LDAP Monitor	55
<input type="checkbox"/> Ping Monitor	56
<input type="checkbox"/> SNMP Monitor	57
<input type="checkbox"/> Port Monitor	63
<input type="checkbox"/> URL Sequence	63

❑ Radius Monitor	64
❑ Telnet and SSH Monitors	64
❑ WMI Monitor	65
❑ Windows Event Log Monitor	66
MONITORS SNAPSHOT	67
CHANGE DEFAULT VALUES OF MONITORS	67
MANAGE MONITORS	68
BULK ADD MONITORS	69
PERFORMANCE GRAPH	69
CONTENT MATCH	71
MANAGE SNMP MATH EXPRESSIONS	75
<b>CHAPTER 7. REPORT</b>	<b>76</b>
QUICK REPORT	76
SCHEDULED REPORT	78
<b>CHAPTER 8. MIB BROWSER</b>	<b>79</b>
MENU	79
TOOLBAR	86
MIB TREE PANE	87
RESULT PANE	88
KEYBOARD SHORTCUTS	89
<b>CHAPTER 9. CONFIGURATION</b>	<b>90</b>
CHECK MAP NODE STATUS	90
PERFORMANCE CONFIGURATION	90
SMTP SERVER CONFIGURATION	91
ALARM CONFIGURATION	92
General	92
Event	93
Alarm Deduplication	97
Trap Clearing	98
Alarm Escalation	99
SNMPv3 Params	99
DATABASE DATA	100
<b>CHAPTER 10. TOOLS</b>	<b>101</b>
IMPORT HP OPENVIEW EVENTS ( <i>TRAPD.CONF</i> )	101

# Chapter 1. Introduction & Installation

SysUpTime network monitor is a powerful agentless network/systems management product. It provides users out-of-box capabilities to efficiently and proactively manage any network of any size. It consists of three major components: server, database, and client. All three of them can be installed on the same machine or different machines.



*Figure: Overview of SysUpTime Network Monitor*

SysUpTime's server clustering technology allows two or more servers that are interconnected to form a unified virtual computing resource.

Clustering servers increases the availability of a system by ensuring that if a server becomes unavailable because of failure or planned downtime, another server in the cluster can assume the workload, ensuring that the monitoring service is uninterrupted. Clustering also enhances scalability by automatically distributing workloads across all the available servers.

A SysUpTime client can connect to all SysUpTime servers in the cluster at the same time.

## System Requirements

- ❑ Windows 2003 Server, Windows XP SP1 or later, or Windows 2000. Or Redhat Linux 9.0 or later versions.
- ❑ 200 MB of disk space. More is required if you need to store performance and SNMP trap data.
- ❑ 256 MB of RAM required. 512 MB or more recommended.

On windows, you need to log in as a system administrator in order to install SysUpTime server. If you just need to install SysUpTime client, you do not have to log in as an administrator. SysUpTime server will run as a Windows service that automatically starts up when Windows is booted. By default, the SysUpTime service is run under the *Local System account*, which has no privileges on other machines. During the installation, you must specify an administrator account for the SysUpTime service if

- ❑ You will create monitors that access remote Windows machine.
- ❑ Or you will configure actions (reboot, kill process, etc) that access remote Windows machine.

On Linux, you need to log in as root in order to install and run SysUpTime Server. After installation, SysUpTime server is installed as Windows Service on Windows platform. The server will be automatically started when Windows is booted.

On Linux:

- Download the `sysuptime.sh` from our website.
- Login as *root* user.
- Do “`chmod +x sysuptime.sh`” to assign the executable permission to it.
- Run `sysuptime.sh`
- To start server, execute `$INSTALL_DIR/server/bin/runserver.sh`

If you have a firewall between SysUpTime server and client, then the ports between 61098 and 61107 (both inclusive) need to be open.

---

### Note:

The default database is Firebird. If you already have Firebird installed on Windows and it is being used by other applications, you have to reinstall Firebird after SysUpTime is uninstalled. And if you install Firebird again after SysUpTime server is installed, SysUpTime server may not be able to run properly.

---

## Chapter 2. User Interface

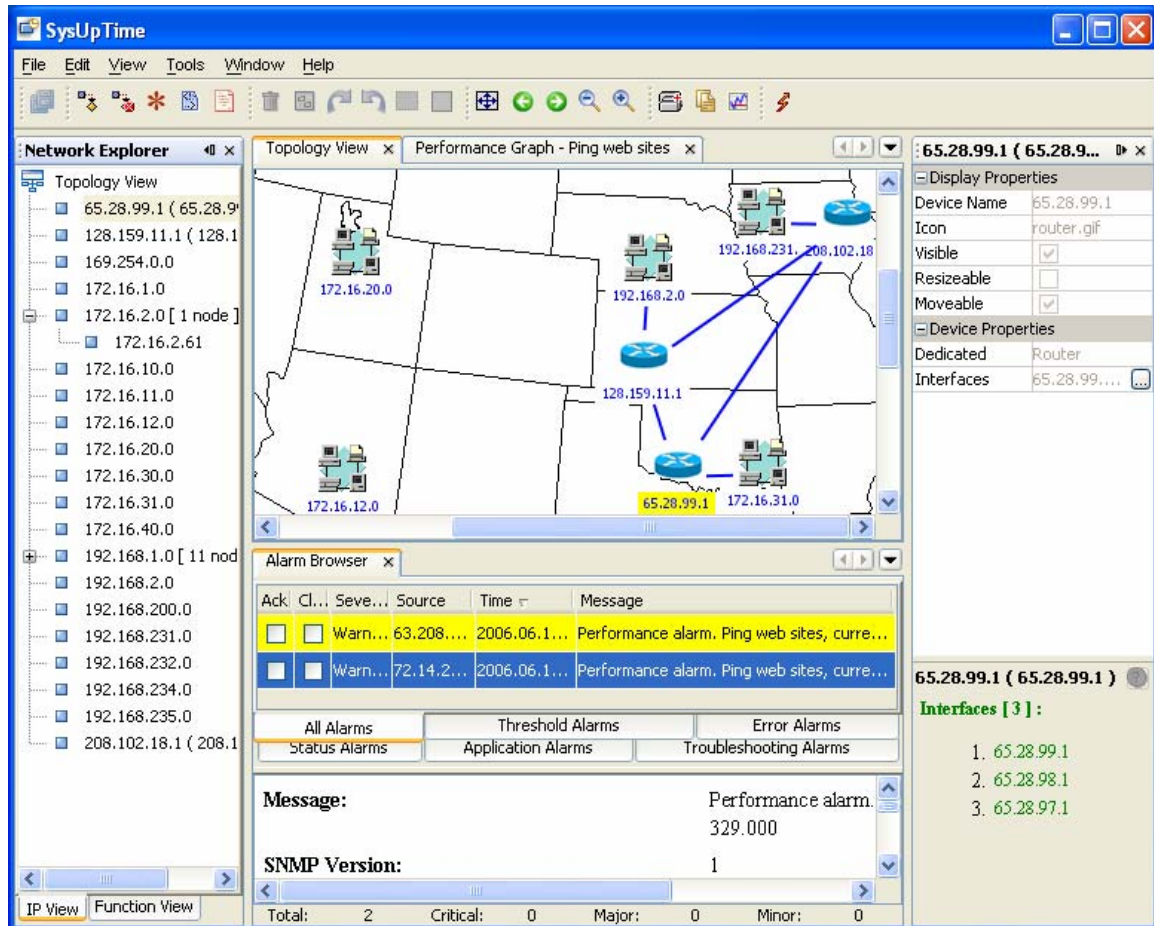
### Login window

When SysUpTime client starts up, it prompts user to enter user name and password. There is a default account with user name 'admin' and password 'admin'. It is recommended to change this default account to enhance security. The value of the server field is the host name or IP address of the SysUpTime server. A user can manage accounts after logging in if his account has enough privilege.

In a clustered environment, the server's value must be empty, otherwise the client only connects to a specific server instead of all available SysUpTime servers in the cluster.



## Main Window



Main window consists of five major components:

- ❑ Menu
- ❑ Toolbar
- ❑ Network Explorer
- ❑ Network Topology View
- ❑ Node Properties

You can move windows to different locations. For instance, the alarm browser window is located beside network topology window when it is opened. You can click its tab and hold the mouse to move it under topology window, so that you can see the incoming traps without switching.

## Menu

### □ File Menu:

- **Save:** Save current map. Only valid in edit mode.
- **Node List:** Display all the nodes in a table.
- **Export Node List:** Export nodes to a CSV file.
- **Export Current Map:** Export current map to a JPG file
- **Export All Maps:** Export all the maps to JPG files
- **Exit:** Exit client

### □ Edit Menu

- **Undo:** Undo previous map editing operation. Deleting a subnet node or modifying the properties of a node are not undoable.
- **Redo:** Redo previous map editing operation.
- **Delete Map Object:** Delete selected map object
- **Hide Map Object:** Hide selected map object. The hidden objects can be shown again by clicking “Show All Map Objects” menu item.
- **Show All Map Objects:** Show all the available map objects of current map.
- **Merge Two Nodes:** Merge two selected map objects into one object. For example, for a computer with two network interfaces but without SNMP agent, automatic discovery will treat it as two different nodes. In this case, you can use merge function to merge them into one node.
- **Background Image:** Insert or remove a background image for top level map.
- **Find Node:** Find a node based on its name, IP address, MAC address or other properties. If the node is found in the maps, it will be highlighted.

### □ View Menu

- **Switch to Edit Mode**

When client starts up, it is in view only mode. That means user can not edit map. If user has enough permission, then he or she can switch to edit mode to change maps. The menu is changed to “Switch to View Mode” when the client is in edit mode.

- **Rearrange Map**

Map can be automatically rearranged. After map rearranged, you will be prompted to save the changes when leaving current map or switching to view mode.

- **Forward/Backward**

These two menu items are for navigating between maps.

Forward: Go to the next map.

Backward: Go to the previous map.

- **Zoom in/Zoom out**

These two menu items let you change the magnification of maps.

- **Restore**

Restore the current map to its original size.

- **Tools Menu**

Menu items will be described in later chapters.

- **Window Menu**

It allows users to open network explorer and properties windows.

- **Help Menu**

“Apply license” menu item can be used to apply a new license file. Only administrators can apply license.

## Network Explorer Window

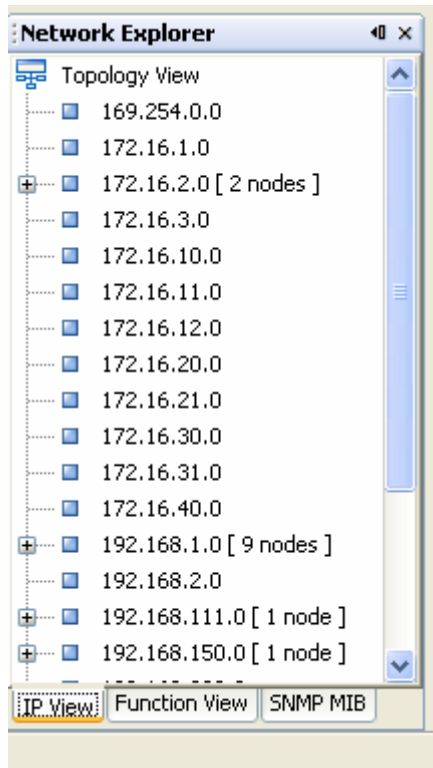


Figure: IP View Pane

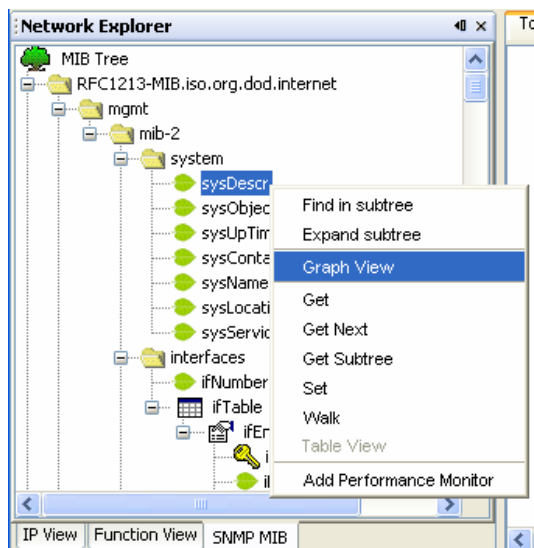


Figure: SNMP MIB Pane

### □ IP view

In this tab, nodes are sorted based on their IP addresses.

If a node has multiple IP addresses, then each IP address will be represented as a node in the IP tree.

### □ Function View

Nodes are sorted based on their functions.

If a node serves multiple functions, then each function will be represented as a node in the function tree.

### □ SNMP MIB

Display MIB trees and provide easy ways to do SNMP operations. Select a topology map node, and then right click on a MIB tree node and you can select operations like MIB table view, graph view, adding performance monitor etc.

The graph function can plot a real time graph for the selected MIB instance.

“Add Performance Monitor” menu allows you to quickly add an SNMP monitor.

This functionality is not available in the free edition.

## Network Topology Window

### □ Device Panel and Topology Map

Device panel is only available in edit mode. It provides icons that can be dragged to topology map. Icons represent network devices or links. If you right click on an icon and click on the “More Icons” menu, more icons will show up.

During network discovery, each discovered node will be assigned an appropriate icon. The type of icon is determined by the device’s value of *SysModel* property. If no matching icon is found, then a generic icon is used. For example, if a node is

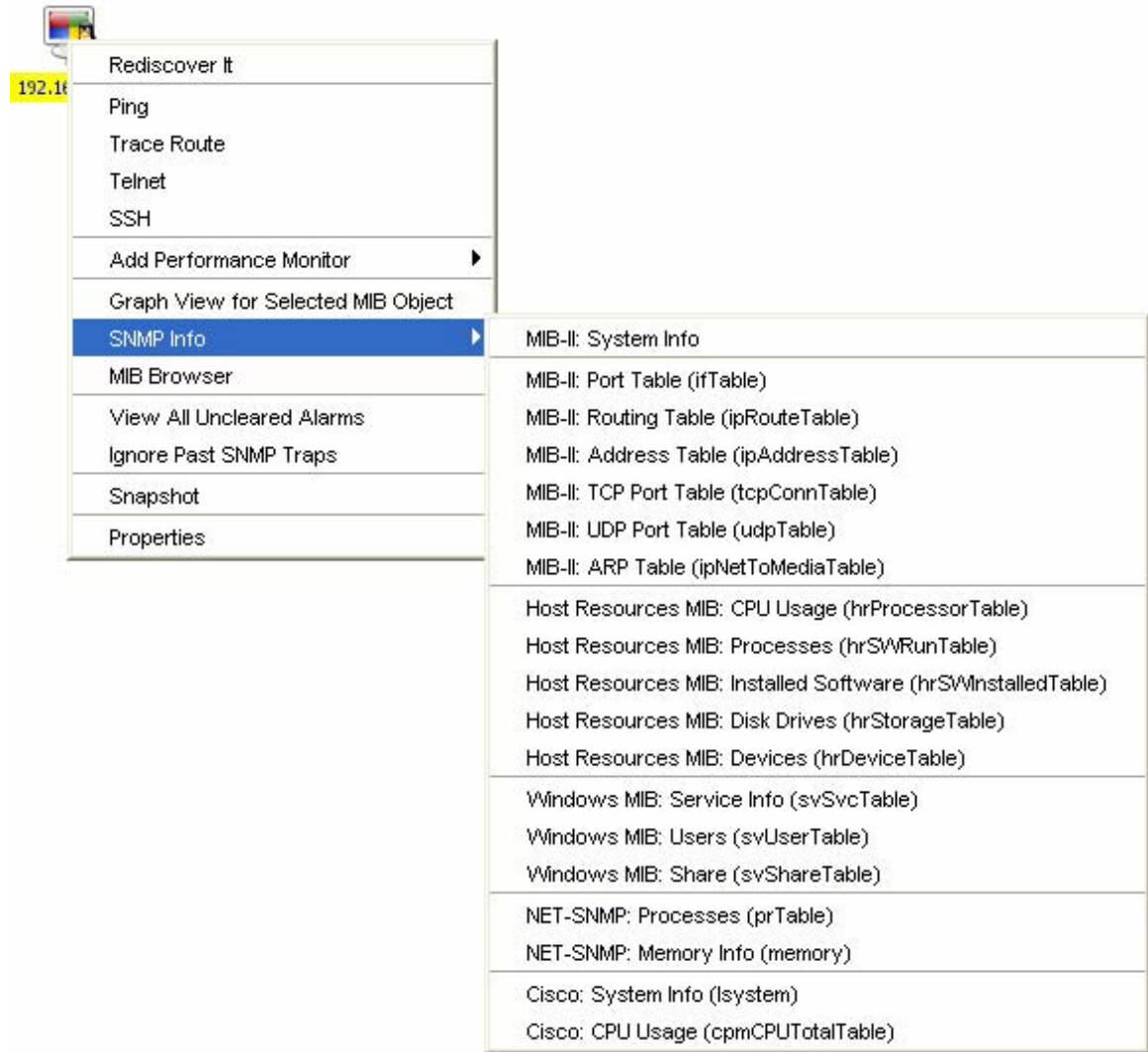
a Windows 2000 machine, a *win2000* () icon is assigned to it. So users can tell the device type easily.

Users can add more icons or modify existing ones themselves. All icons are store in the following directory:

*\$INSTALL\_DIR\SysUpTime\server\image\topology*

The sub directories denote the device types. For instance, ...*\topology\server* directory contains all the icons for servers. If you want to add a new icon, say, Mac OS X, you can add a file named *osx.gif* (or other image file types such as *jpg*). The new icons will take effect after next network discovery is finished.

Right click on a node, depending on whether it is SNMP enabled, the following popup menu will show up:



<b>To Parent Map</b>	Jump to parent map.
<b>Rediscover It</b>	Rediscover this node.
<b>Ping/Trace Route/Telnet/SSH</b>	Use Ping/Trace Route, Telnet or SSH to check node status.
<b>Add Performance Monitor</b>	Add a new monitor for this node
<b>Graph View for Selected MIB Object</b>	Plot graph for selected MIB object of the SNMP MIB pane.
<b>SNMP Info</b>	If node supports SNMP, it will query SNMP agent to get values and show them in a new dialog window. This menu can be customized by modifying the <i>\$INSTALL_DIR/client/config/snmpinfo.conf</i> config file. You can add or remove menu items.
<b>MIB Browser</b>	Launch MIB browser window.
<b>Ignore Past SNMP Traps</b>	If node has uncleared traps and the alarm browser is open, node's color is red. You can use this menu item to change it back to normal color.
<b>View All Uncleared Alarms</b>	View all the uncleared traps of this node in the past 24 hours.
<b>Snapshot</b>	Launch a new window to display information about this node and its monitors.
<b>Properties</b>	Launch a properties window.

## □ **Editing Map**

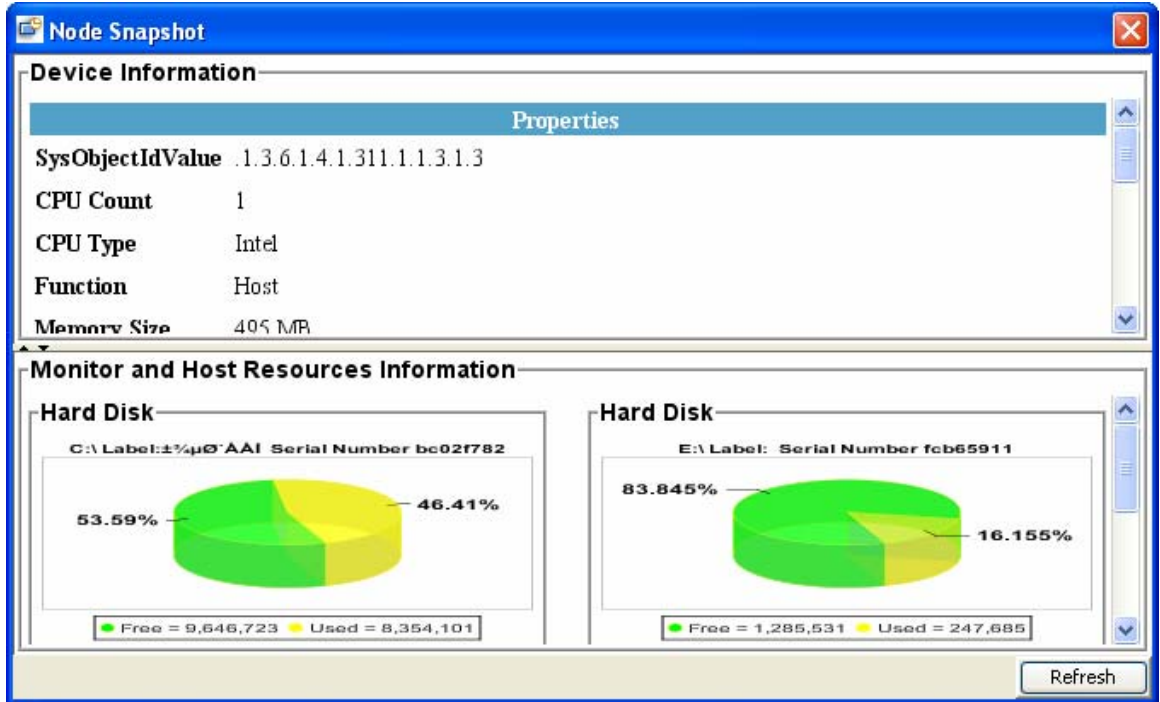
For users with enough privilege, they can switch to edit mode to modify maps.

To add a new device to the current map, you just need to drag the icon from device panel to the map. When adding a new node, system will prompt user to enter some parameters and it then automatically does a discovery against the new node. If the node is not reachable, system will prompt user to discard it or not. If the map is subnet, the newly added node will be automatically connected to subnet.

If the map is top level map, you can drag a link to connect it with another device. After a link is created, you can set its properties, and set the interfaces this link is associated with. When the end interfaces of a link are not configured, the link is red, and the link positions will not be preserved even after save unless it is correctly configured. Its color will be changed to blue after interfaces are properly configured. If a node has only one interface, it will be automatically assigned to the link. If a node has more than one interfaces, user needs to pick one of them and assign it to the link. If a node has no unoccupied interface, then you need to add one for it.

## ❑ Node Snapshot

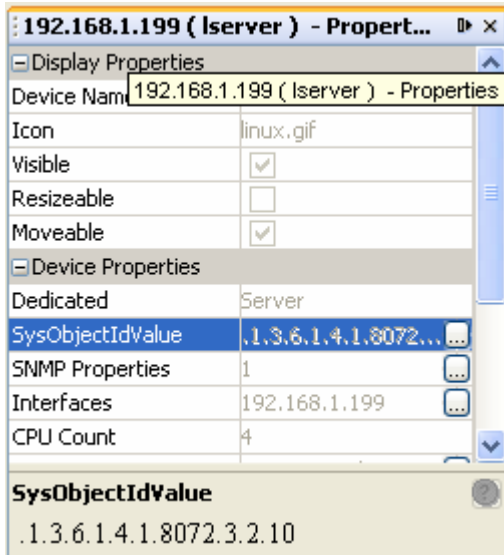
Node snapshot lets users take a quick look at the status of the selected node.



The upper panel displays properties of the node. The lower panel displays monitor and host information. The type of chart of a monitor can be configured in the "Add Monitors" dialog.

Pressing "Refresh" button will update the monitor and host information.

## Properties Window



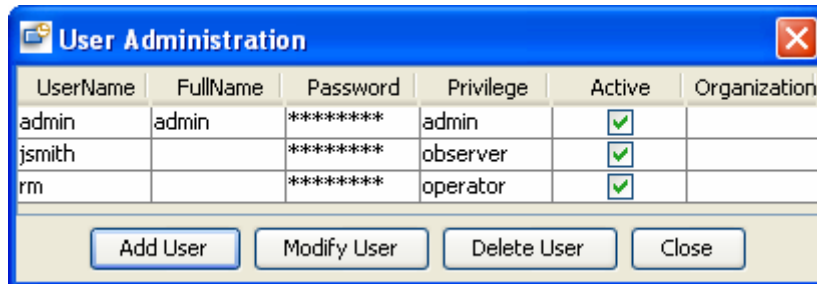
Properties window displays the properties of selected node. In view mode, properties are grayed out and can not be modified. The user needs to switch to edit mode in order to change the properties of nodes.

Network explorer window has to be open, otherwise properties window will not be updated.

If in edit mode, user can edit some fields directly to change the node's properties.

## Chapter 3. User and View Management

### User Management



Each user is assigned one of the three privileges: admin, operator and observer. By default, admin privilege has all the permissions and observer group has minimum permissions. You can change their privileges in the “User Permissions” window.

Each user is associated with zero or more organizations, which are tied to different topology views.

User name must start with a letter or digit. And ‘@’ is not allowed in user names. The maximum length of user name is 20 characters. Number of allowed users depend on the license type.

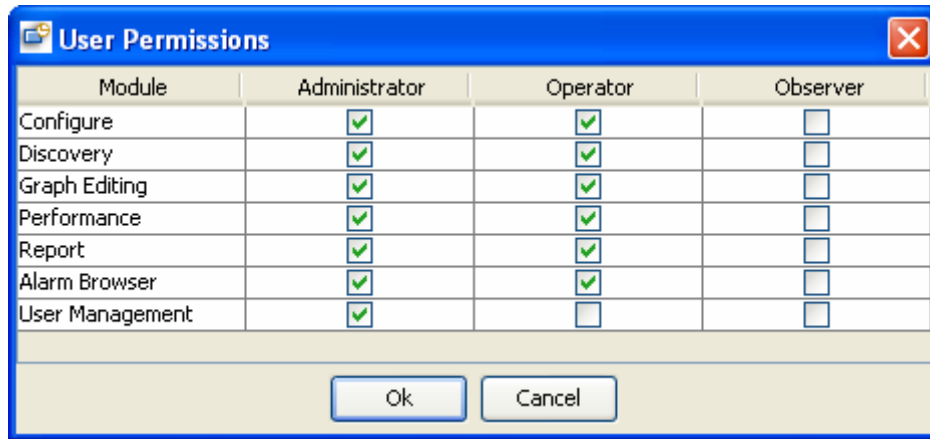
You can suspend a user by clicking the checkmark of the “Active” column.

After SysUpTime is installed, a default user “admin” with password “admin” is created. You should change its password to a secure one to enhance security.

### Change Password

Change current user’s own password.

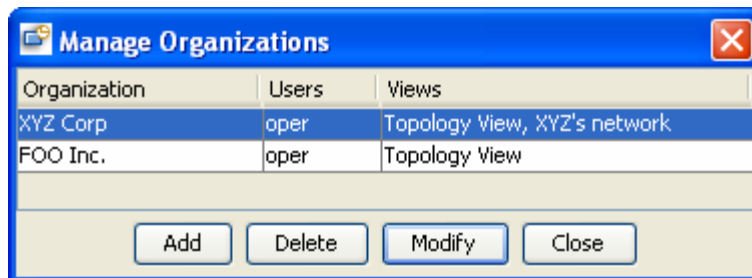
## User Permissions



This window is used to assign permissions to different groups. By definition, administrator group has all privileges, and observer group has read-only privileges.

For trap module, although observer group does not have privilege to change a trap's properties, it still can view all the traps.

## Manage Organization



An organization can have one or more users, and it can be associated with one or more network views. A user can only open the views assigned to his organization.

## Create Customer View

The screenshot shows the 'Create Customer View' dialog box. At the top, there are two text input fields: 'View Name' containing 'XYZ's Network' and 'Visible to Organizations' containing 'XYZ Corp.', with an 'Edit' button to the right. Below these are three main sections: 'Optional', 'Properties', and 'Selected'. The 'Optional' section contains a list of IP addresses: 172.16.2.61, 192.168.1.1 (LINUX), 192.168.1.238 (YXKJ-4F...), and 192.168.1.254. The 'Properties' section is a table with columns 'Name' and 'Value'. The 'Selected' section contains a list of IP addresses: 192.168.1.190 (7F67DC...), 192.168.1.198 (SERVER), 192.168.1.199 (lserver), and 192.168.1.235. Between the 'Optional' and 'Selected' sections are two buttons: '>>' and '<<'. At the bottom, there is a 'Filter' section with an 'Apply Filter' checkbox, a 'Type' dropdown menu set to 'All Types', a 'Device Name' text input field, and an 'IP Address Range' text input field with an 'Examples' button. On the right side of the dialog are 'Ok' and 'Cancel' buttons.

*Figure: Create a new customer view*

Customer views can be used to create user-defined maps. It lets you create your own set of devices based on device type, location, or other selection criteria. Each customer view can be associated with an organization, so users who are not in the right organizations can not access the customer view. Administrators have access to all the customer views.

Topology view is the global view and contains all the nodes. Nodes in the customer views are the same as those in the topology view. If you edit the properties for a node in the topology view, the node in other views will change as well. However, if you delete a node from a customer view, it will not be deleted from topology view.

Customer views, unlike subnet map, can be rearranged and background image can be inserted after switching to edit mode.

Customer view can be opened through “File/Open View” menu.

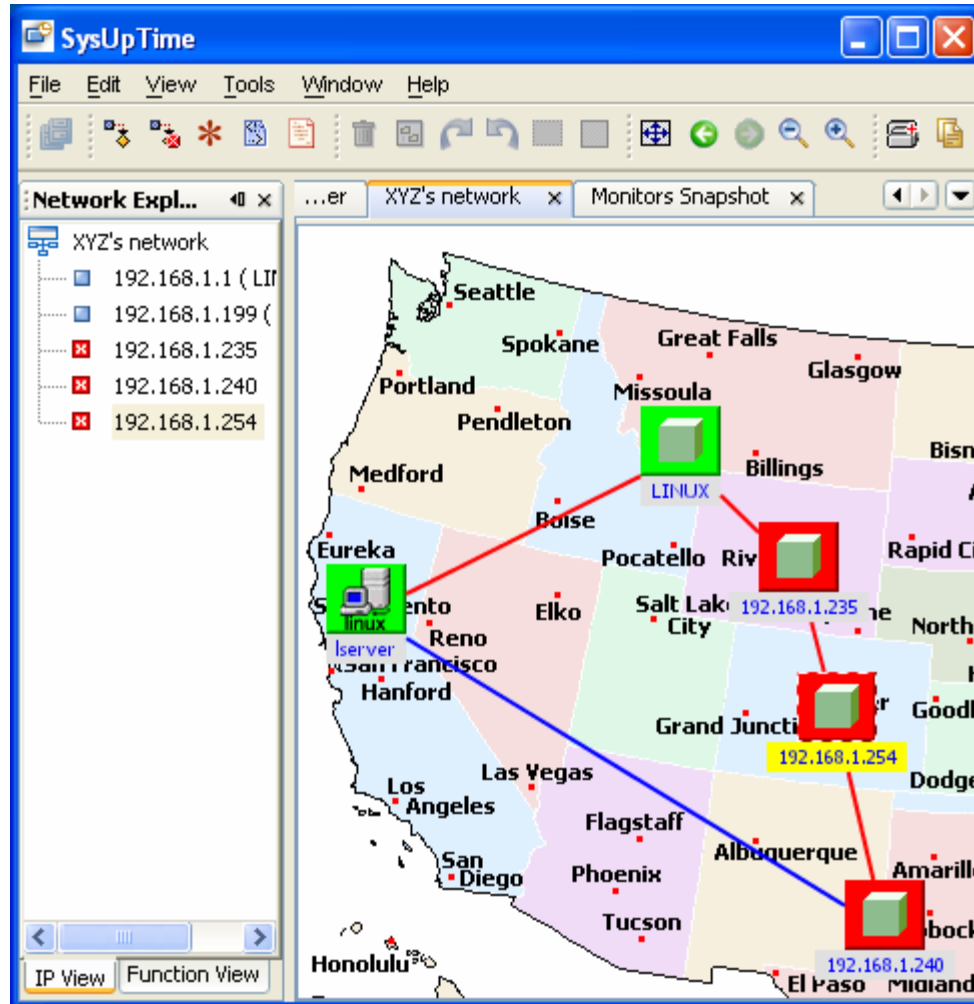


Figure: A customer view with five nodes

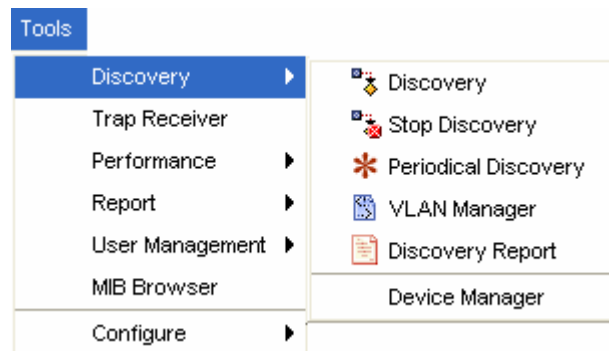
## Chapter 4. Network Discovery

Network discovery is an important step for network management. An accurate topology map is vital for identifying network problems.

Major features of SysUpTime's discovery module:

- Support for layer 3 and layer 2 discovery.
- Accuracy.
- CIM (Common Information Model) based object model.
- Support for multiple protocols including SNMPv1/v2c/v3, PING, Netbios, HTTP, etc.
- Unique mediation layer technology ensures unlimited extensibility. New device support can be easily added by user.
- Periodical discovery.
- Automatically merge topology of a new discovery with the old one.  
Manually added/hidden nodes will be preserved in new topology.

The menu of network discovery is shown below:



## Start Discovery

Discovery Options

Seed: 192.168.1.1

Is Private IP Only:

Max Public IP Hops: 0

Timeout: 1.0 seconds

Number of Threads: 31

Ignore Non-SNMP-enabled Devices:

Clean Discovery:

Detect Network Services:  Edit

SNMP Agent Properties

IP Address	Read Community	Version	User Name
192.168.1.199	*****	1	
192.168.1.197		3	afas

Discovery Filters

IP Range	sysName	sysDescr	Device Types	Mode
			...	IGNORE
192.168.1.0				MUST

Buttons: Add, Delete, Modify, Add, Delete, Import, Ok, Cancel

This dialog is for specifying discovery settings. The settings will be stored in database so next time the user does not have to reenter them. If periodical discovery is enabled, it will use the settings as well.

- **Seed**

The starting point of discovery. If no seed is specified, the default gateway will be used.

If the seed IP address is not reachable, SysUpTime will ask user to continue discovery or not. If yes, the first IP address of the subnet will be used as seed.

- **Is Private IP Only**

If selected, discovery will be limited to private IP addresses. All public IP addresses will be ignored.

- **Max Public IP hops**

If the previous option is not selected, discovery will continue until all available IP addresses are scanned. It may take too long and cause security problems. So we need to limit the scope of discovery.

- **Timeout**

Timeout value for PING and SNMP queries in seconds. The minimum value is one second. Smaller timeout value can speed up discovery, but it may skip some unresponsive nodes.

- **Number of Threads**

Number of threads for discovery. More threads can speed up discovery process but it may add too much network traffic.

- **Ignore non SNMP enabled devices**

If selected, all nodes without active SNMP agent or correct SNMP community names will be ignored.

- **Clean Discovery**

If selected, previous discovery results and manually modified maps will be discarded.

If not selected, SysUpTime will try to merge the new discovery result with the old maps. All manually added/hidden nodes will be preserved. For instance, if you hide a node, this node will be still invisible even if it is discovered again. However, for manually deleted nodes, they will show up again if they are discovered.

- **Detect Network Services**

If selected, network services such as FTP, HTTP and others will be detected if they are active on the nodes being discovered.

- **SNMP Agent Properties**

If SNMP agents to be discovered are SNMPv3 agents or SNMPv1/v2c agents with non-default community names ('public'), then you need to add their properties so that their SNMP values will be discovered.

- **Discovery Filters**

If you don't want to discover everything in your networks, then filter is a great tool to limit discovery scope. Or if there are some subnets that cannot be automatically discovered, you can set filters to force discovery engine to discover them.

Filter can be set by the following conditions:

- **IP Range or IP address**

Four formats are supported:

- Subnet Format

IP range ends with '\*.\*' or '.0'. For instance, "192.168.1.\*" or "192.168.1.0" mean all the IPs between 192.168.1.1 and 192.168.1.254.

- Partial Subnet Format: Two IPs in the same subnet, separated by '-'.

For example, "192.168.1.10 - 192.168.1.100" means all the IPs between 192.168.1.10 and 192.168.1.100, inclusive.

- CIDR Format

For example, "192.168.1.0/24" means all the IPs between 192.168.1.1 and 192.168.1.254; "192.168.1.0/25" means IPs between 192.168.1.0 and 192.168.1.127.

- Individual IP: A single IP address.

- **sysName**

Value of SNMP MIB-II sysName.

'\*' and '?' are allowed for wildcard match. '\*' matches an arbitrary string of characters, and the string can be empty. '?' matches any single character.

For instance, "\*" matches all system names; "test\*" matches any string starting with "test"; "te?t" matches "test", "te1t", or other strings with similar pattern.

❑ **sysDescr**

Value of SNMP MIB-II sysDescr  
'\*' and '?' are allowed for wildcard match.

❑ **Device Types**

User can select one or more system types. System type is determined by the value of sysObjectID. There is a list of predefined mapping of sysObjectID's value to device type. And new mapping can be configured through "Tools/Discovery/Device Manager" menu.

❑ **Mode**

➤ *IGNORE*

Ignore all the nodes meeting the criteria.

➤ *MUST*

Discovery engine must discover all the nodes meeting the criteria.

If there are any conflicts between *IGNORE* and *MUST* mode, *MUST* will take precedence. If filter settings conflict with other discovery settings, filter settings take precedence.

❑ **Import filter button**

Import 'MUST' discovered IP or IP range list from a text file. File format: each IP or IP range take one line.

Here is an example:

<b>IP Range</b>	<b>sysName</b>	<b>sysDescr</b>	<b>Device Types</b>	<b>Mode</b>
192.168.1.0				MUST
172.16.1.0	Windows*		Host, Server	IGNORE
192.168.2.10 – 192.168.2.150				IGNORE
192.168.3.1				IGNORE

Discovery engine will discover all nodes except hosts or servers whose IPs are:

1. between 172.16.1.1 and 172.16.1.254 and
2. between 192.168.2.10 and 192.168.2.150 and
3. 192.168.3.1

The discovery should explicitly discover the 192.168.1.0 subnet.

## **Stop Discovery**

Stop network discovery. However, network topology may not be accurate if discovery is stopped in the middle.

## **Periodical Discovery**

Discovery can be scheduled to occur periodically. Periodical discovery will reuse settings of last discovery. If no manual discovery is done, periodical discovery will use default settings. Periodical discovery starts at 00:00.

## **Partial Rediscovery**

If a subnet or node's properties have changed and the changes do not affect others, you can use partial rediscovery to update a subnet or node instead of launching a full-scale rediscovery.

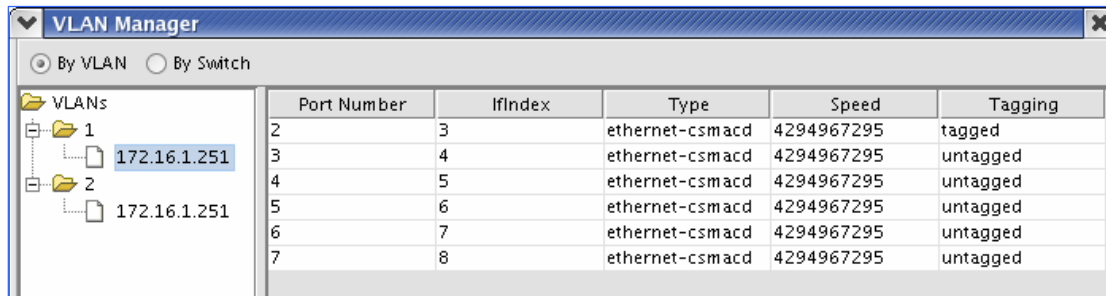
To invoke a partial rediscovery, right click on a node or subnet and select "*Rediscover It*" menu.

## **Discovery Report**

It shows a summary of the last network discovery.

## VLAN Manager

It shows properties of VLANs found in discovery. Items found can be ordered by VLAN ID or by switch.

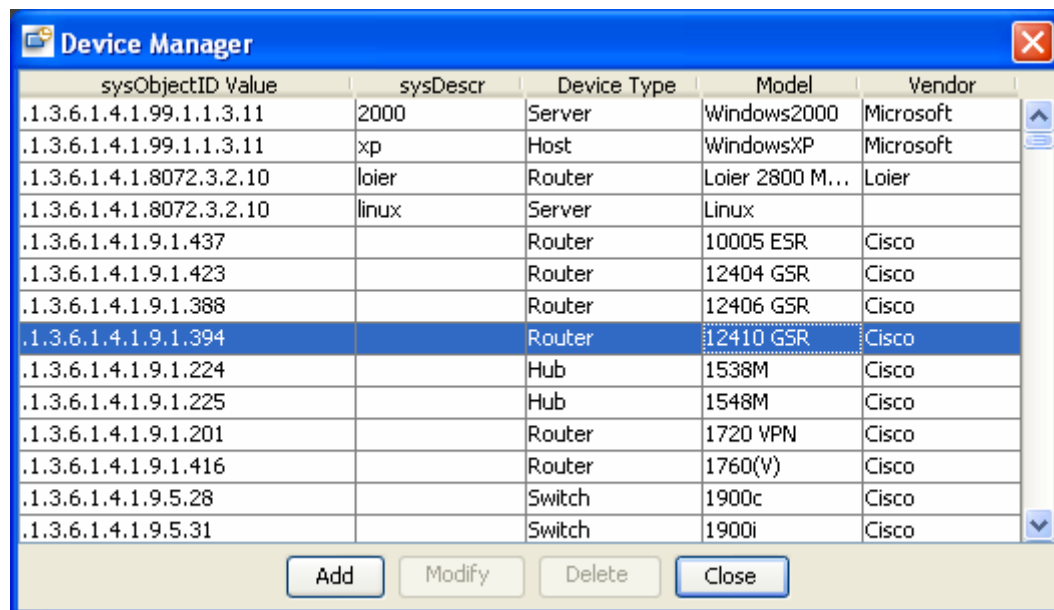


The screenshot shows the 'VLAN Manager' window. On the left, there is a tree view under 'VLANs' with two folders, '1' and '2', each containing a file named '172.16.1.251'. On the right, a table displays the properties of these VLANs.

Port Number	IfIndex	Type	Speed	Tagging
2	3	ethernet-csmacd	4294967295	tagged
3	4	ethernet-csmacd	4294967295	untagged
4	5	ethernet-csmacd	4294967295	untagged
5	6	ethernet-csmacd	4294967295	untagged
6	7	ethernet-csmacd	4294967295	untagged
7	8	ethernet-csmacd	4294967295	untagged

## Device Manager

SysUpTime supports thousands of devices and applications. It also provides excellent extensibility so that users can easily add new device support through device manager. One requirement is new device must support SNMP. If a device is supported, its properties, including device type, model, and other information will be identified during network discovery.

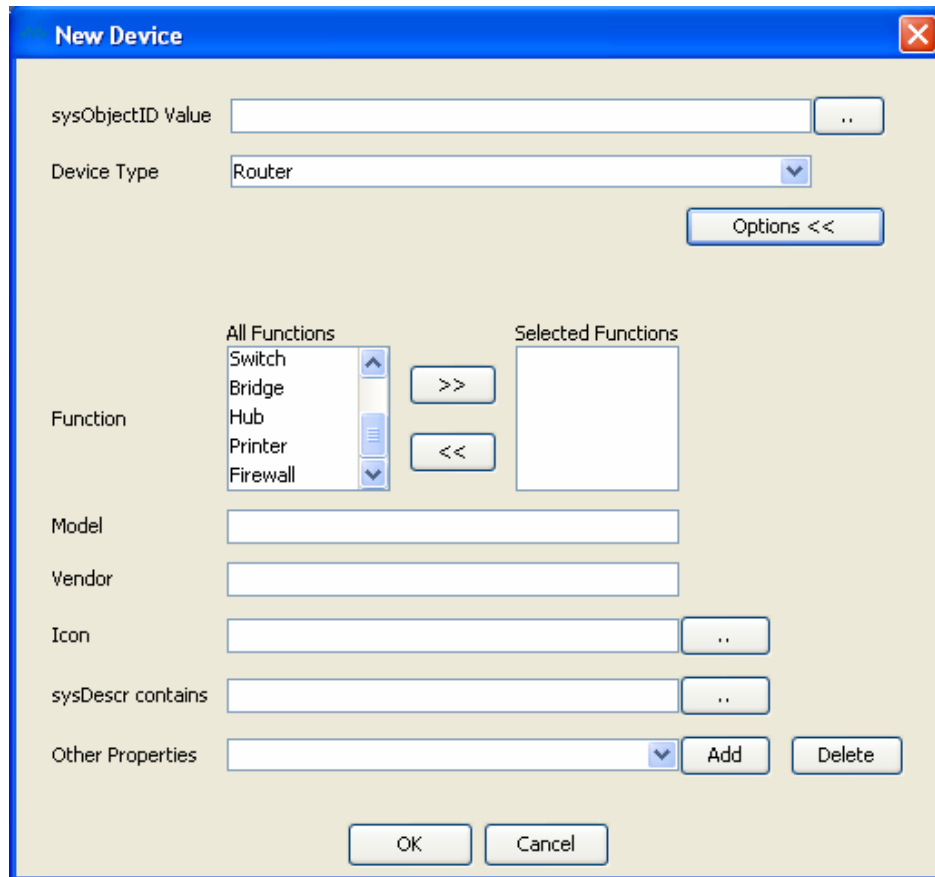


The screenshot shows the 'Device Manager' window with a table of discovered devices. The table has columns for sysObjectID Value, sysDescr, Device Type, Model, and Vendor. The row for '12410 GSR' is highlighted.

sysObjectID Value	sysDescr	Device Type	Model	Vendor
.1.3.6.1.4.1.99.1.1.3.11	2000	Server	Windows2000	Microsoft
.1.3.6.1.4.1.99.1.1.3.11	xp	Host	WindowsXP	Microsoft
.1.3.6.1.4.1.8072.3.2.10	loier	Router	Loier 2800 M...	Loier
.1.3.6.1.4.1.8072.3.2.10	linux	Server	Linux	
.1.3.6.1.4.1.9.1.437		Router	10005 ESR	Cisco
.1.3.6.1.4.1.9.1.423		Router	12404 GSR	Cisco
.1.3.6.1.4.1.9.1.388		Router	12406 GSR	Cisco
.1.3.6.1.4.1.9.1.394		Router	12410 GSR	Cisco
.1.3.6.1.4.1.9.1.224		Hub	1538M	Cisco
.1.3.6.1.4.1.9.1.225		Hub	1548M	Cisco
.1.3.6.1.4.1.9.1.201		Router	1720 VPN	Cisco
.1.3.6.1.4.1.9.1.416		Router	1760(V)	Cisco
.1.3.6.1.4.1.9.5.28		Switch	1900c	Cisco
.1.3.6.1.4.1.9.5.31		Switch	1900i	Cisco

Buttons: Add, Modify, Delete, Close

The built-in devices cannot be modified or deleted. However, users can add a device with the same sysObjectID value to overwrite the existing settings.



The sysObjectID value is required and it will be used as a key to identify devices during network discovery.

sysDescr contains: Enter keyword that sysDescr (SNMP MIB-II object) includes. This field is necessary if two different devices with the same sysObjectID values but different sysDescr values.

Other Properties: User can enter custom properties of new devices. Each property has an OID, which will be used to query SNMP agent to get its value.

## Chapter 5. Event System

SysUpTime's event system is a powerful tool for processing SNMPv1/v2c/v3 traps/informs and internally generated performance events.

Event system consists of three major components: database tables for storing events, trap receiver server on the server side, and alarm browser window on the client side.

### Trap Receiver Server

By default, trap receiver server will be automatically started when SysUpTime server starts up. However, if you do not need trap receiver, you can disable it. To disable trap receiver, edit

*\$INSTALL\_DIR/server/server/default/conf/server.properties* and change to *trapReceiver=no*.

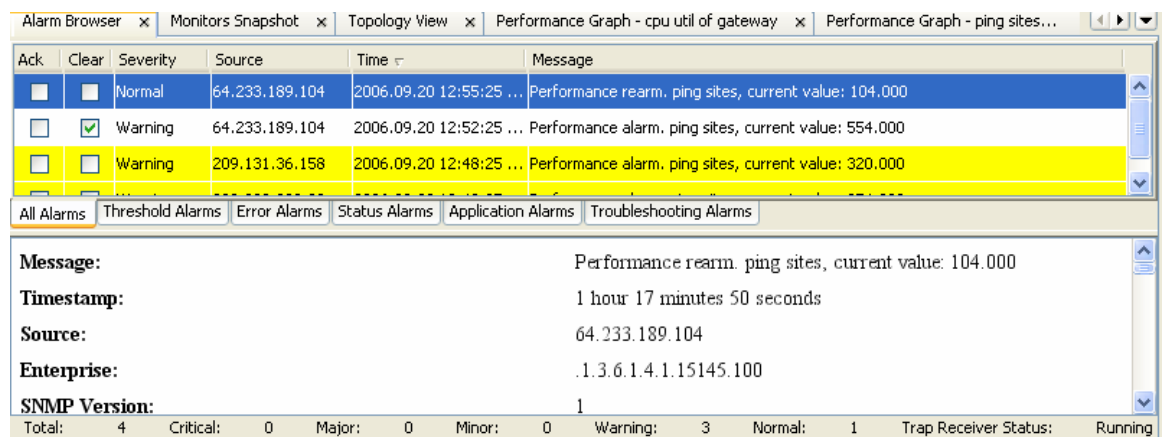
The default port number of trap receiver is 162. On some platforms, this port may already be occupied by some other application, then trap receiver can not be started unless you stop the application that takes port 162 first. If SysUpTime server is running on Linux/UNIX, it must have root privilege in order to start trap receiver at port 162.

In a clustered environment, there can be more than one trap receiver servers. In this case, SysUpTime client connects to all trap receiver servers and display all the received traps.

## Alarm Browser

On the SysUpTime client side, alarm browser is not opened the first time you start SysUpTime client. Click “Tools/Alarm Browser/Open Alarm Browser” menu to open it. If the alarm browser is open when you exit client, its state is preserved and it will be opened next time you start client. By default, alarm browser window can hold up to 1,500 traps. If number of alarms exceed this number, oldest ones will be removed.

Depending on the configuration, incoming alarms are stored in database or discarded. You can use alarm browser window to view historical alarm data. SysUpTime can be configured to periodically delete old alarms.



Alarm browser is divided into two panels. The upper panel shows summaries of alarms. The lower one shows details of selected alarm. The status bar on the bottom shows the current status of alarm browser.

The following popup menu will show up if right clicking on a row. The menu items there have the same effects as those under Tools/Alarm Browser.

Source	Time
64.233.161.99	2005.10.12 11:07:23 GMT+0...
64.233.161.99	2005.10.12 11:04:28 GMT+0...
64.233.161.99	IT+0...
64.233.161.99	IT+0...

- Set Filters
- Reset Filters
- Display Historical Traps
- Clear Selected Rows
- Change Severity
- Send Email
- Delete
- Hide
- Hide All
- Ping
- Trace Route

Menu Items of Alarm Browser Window:

<b>Open Alarm Browser</b>	Open alarm browser window. If alarm browser window is already open, it will be brought to the front.
<b>Close Alarm Browser</b>	Close alarm browser window. The trap receiver on the server side is not affected and continues to process incoming alarms.
<b>Start Trap Receiver Service</b>	Start trap receiver for receiving SNMP traps.
<b>Stop Trap Receiver Service</b>	Stop trap receiver.
<b>Set Filters</b>	Set filters to reduce alarms on the screen.
<b>Reset Filters</b>	Reset all filters and revert back to the default states.
<b>Display Historical Alarms</b>	Load historical alarms from database and show them. If number of traps are over 1,500, only the first 1,500 traps are retrieved.
<b>Clear Selected Rows</b>	Clear selected one or more alarms. User will be prompt to enter comment. Comment will be added to detail panel if clearing succeeded. Other clients can see the change immediately.
<b>Change Severity</b>	Change the severity of selected alarm both on the client side and database. Other clients can see the change immediately.
<b>Send Email</b>	Send selected alarm via email. SMTP server needs to be configured beforehand.
<b>Delete</b>	Permanently delete selected alarm both on the client side and database. Other clients can see the change immediately.
<b>Hide</b>	Hide selected rows. It does not affect alarms in the database and other client will not be affected.
<b>Hide All</b>	Hide all the traps. It does not affect alarms in the database and other client will not be affected.
<b>Ping</b>	Ping the alarm originator to see if it is reachable.
<b>Trace Route</b>	Trace route the alarm originator.

There are five levels of severity: normal, warning, minor, major, and critical. And their corresponding colors are:

<b>Alarm Severity</b>	<b>Color</b>
<b>Normal</b>	white
<b>Warning</b>	yellow
<b>Minor</b>	orange
<b>Major</b>	pink
<b>Critical</b>	red

Incoming alarms are sorted into five predefined categories depending on the event configuration: Threshold, Error, Status, Application, Troubleshooting alarms. If an incoming alarm is not configured, then it does not belong to any categories and will be placed in the “All Alarms” tab. An alarm needs to be configured through “Tools/Configure/Alarm /Event” to set its category. New categories can be added in event configuration.

In the upper panel of the alarm browser window, by default, the alarms are in chronological order with the most recent alarm at the top of the list. You can sort alarms by clicking the table header. The table columns are listed below:

<b>Ack</b>	<p>It indicates whether the trap is acknowledged or not. Acknowledging a trap means somebody is working on the network issue but this issue has not been resolved yet.</p> <p>Click the check mark of <i>Ack</i> column to acknowledge the trap. You will be prompted to enter comment. The comment will be seen in the detail panel.</p> <p>When one client acknowledges a trap, the trap status is changed to acknowledged in other active clients.</p>
<b>Clear</b>	<p>It indicates whether the trap is cleared or not. Cleared trap means the network issue has been completely resolved. When a trap is cleared, the color is changed to white.</p> <p>Click the check mark of <i>Clear</i> column to clear the trap. You will be prompted to enter comment. The comment will be seen in the detail panel.</p> <p>When one client clears a trap, the trap status is changed to cleared in other active clients.</p>
<b>Severity</b>	Trap’s severity.
<b>Source</b>	The IP address of the trap sender.
<b>Time</b>	The time when the trap was received.
<b>Message</b>	Brief description of the trap.

Other functionality, such as trap de-duplication, event configuration, trap clearing, and alarm escalation will be described in the configuration chapter.

## Chapter 6. Performance Management

It is important to measure network and systems performance in order to manage it. SysUpTime's performance management warns you proactively of potential problems in the managed environment. Performance management monitors network performance variables to ensure that it is maintained at an acceptable level. Network throughput, user response time, and line utilization are good examples of variables that are monitored.

SysUpTime periodically collect and monitor performance variables. When a performance threshold is exceeded, an alarm is posted in the alarm browser window and its associated actions will be performed. There are two different ways to manage threshold in SysUpTime:

- Self-learning Dynamic Statistical Baseline (based on historical data)

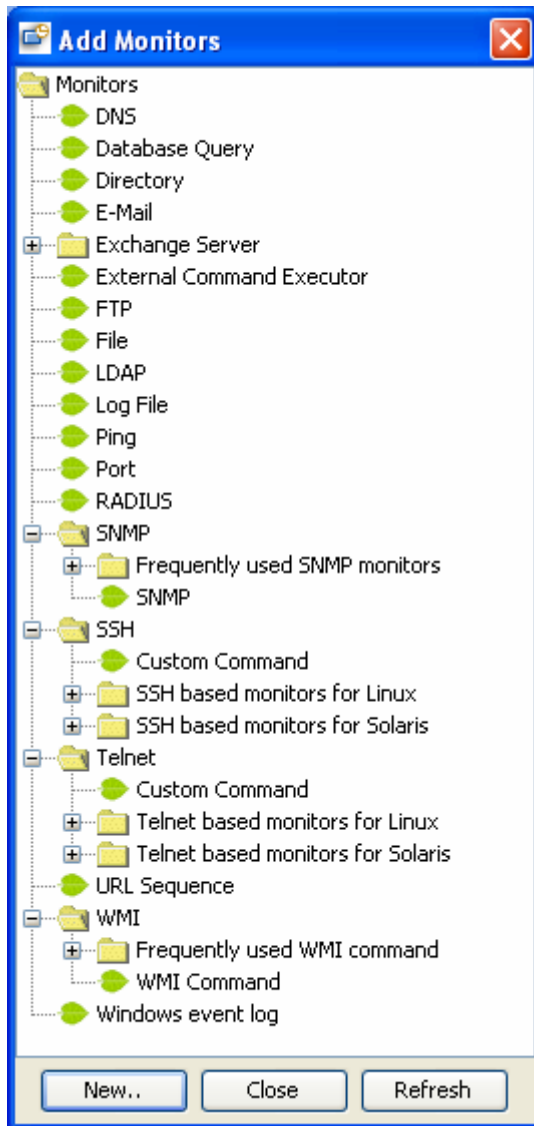
SysUpTime continuously examines what has happened in the past, learns from it, and creates a dynamic baseline of "normal" performance data. In operation, SysUpTime then computes and looks for deviations from those normal parameters. The automated self-learning baseline approach eliminates time-consuming manual threshold administration by automatically generating dynamic thresholds for thousands of monitors.

- Multi-level Fixed Thresholds

It allows user to set multiple thresholds (based on time) with each threshold corresponding to an alarm severity level. Each threshold can be associated with a time frame. For instance, for weekdays, we can set a threshold of 80 with severity level of major, 75 with severity of minor; and for weekends, we can set a threshold of 60 with severity level of major, 55 with severity of minor.

Take for another example that you have configured your system to alert you if your router's interface utilization reaches 80 percent. But, what if your router has been running at a 79 percent for all week? If your system is not configured to send you an alarm below 80 percent, you will not even notice this potentially dangerous anomaly in your router till trouble actually strikes. A proactive stance would be to not let such a situation arise. You can set multiple thresholds for alarms, one at the critical point and another before that when the load reaches, say 10 percent before the critical point.

## Add a New Monitor



This window lists available monitor types. Press “New” button to create a new monitor.

## Common Form Values

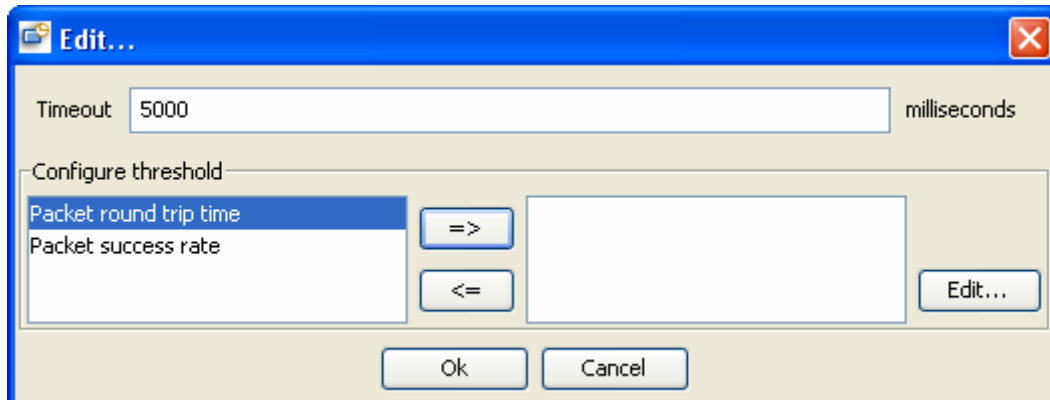
The following figure is the first screen of creating a new PING monitor:

The screenshot shows a dialog box titled "New...Ping" with a close button in the top right corner. The dialog box contains the following fields and controls:

- Host name:
- Monitor name (1-50 chars):
- Polling interval:
- Decrease polling interval by:    times when threshold is crossed
- Threshold settings:
- Actions:
- Depends on:
- Group:
- Snapshot settings (optional):
- Save run results to database
- Test run
- 
-

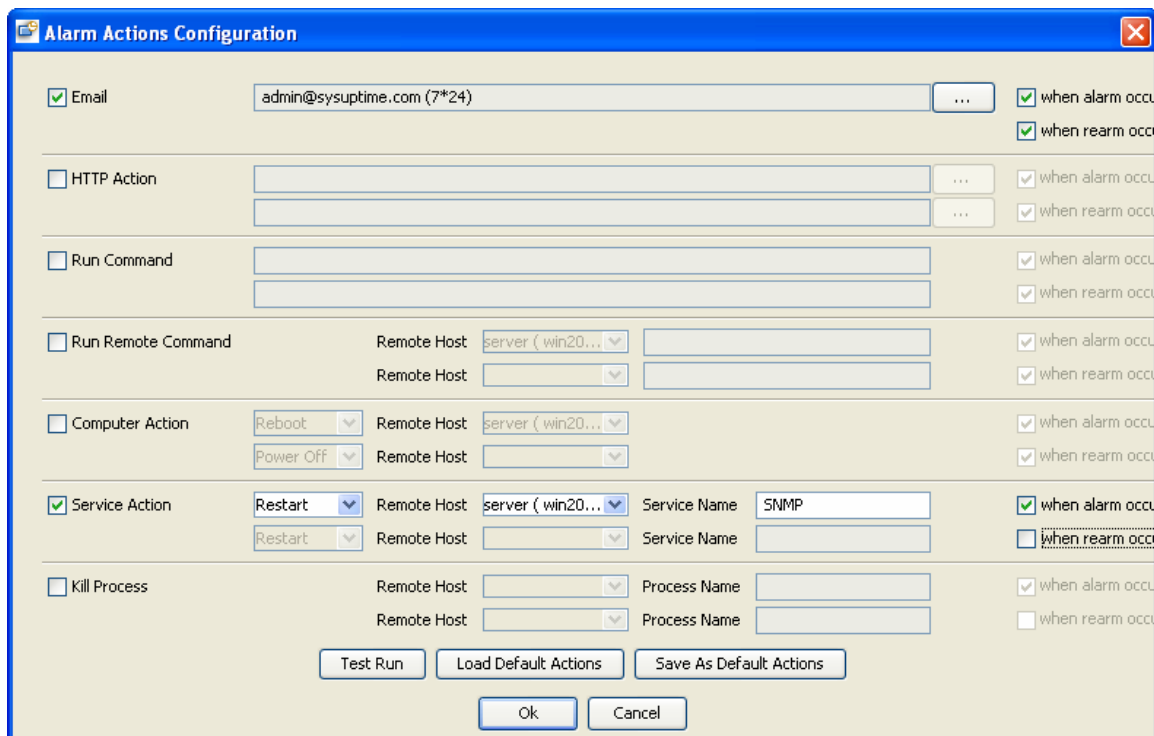
<b>Host Name</b>	Specify the host name or IP address of the network node to be monitored. If user enters an IP address, system will try to resolve it to a DNS name and use DNS name internally.  Some monitors allow multiple host names separated by comma or semicolon.
<b>Monitor Name</b>	A meaningful name for this monitor.
<b>Polling interval</b>	The interval between pollings.
<b>Decrease polling interval by <math>x</math> times</b>	The default value is 1, which means polling interval stays constant. For instance, if the value is 5 and the polling interval is 10 minutes. When the threshold is exceeded, the polling interval will be changed to 2 minutes. The polling interval will go back to normal when rearm occurs.
<b>Threshold settings</b>	User needs to press “Configure” button to set up threshold.
<b>Actions</b>	Configure actions for this monitor only. Actions will be triggered when an event (alarm or rearm) occurs. You can use “Tools/Configure/Alarm/Event/Performance monitor” to configure global actions for all performance monitor.
<b>Depends on</b>	If this monitor depends on another one, it cannot run until the other monitor’s state meets the specified condition. For example, if it depends on monitor A, and the “Depends condition” is “Ok”, then it can run only if monitor A’s performance threshold is not exceeded.  Multiple levels of dependency is supported. That is, monitor A can depend on monitor B, and monitor B can depend on monitor C.  A monitor can have only one monitor depending on itself.
<b>Group</b>	A monitor can belong to a group. If later this group is deleted, all monitors in it will be removed.
<b>Snapshot properties</b>	Optional. Chart properties of this monitor in snapshot. Press “Configure” button to configure it.
<b>Save run results to database</b>	Specify whether to save data in database. Data can be used later for reporting, trending, graphing, etc.
<b>Test run</b>	Specify whether to do a test run, which can help determine if all monitor settings are correct.
<b>Advanced options</b>	By default, a monitor will start immediately and run 7X24 for unlimited times. You can change all those options.

## Edit Metrics:



This screen lets you configure threshold and other parameters specific to this metric. Press “=>” button to configure threshold for selected metric. After configuring metric is finished, it will be placed to the right panel. It can be edited again by pressing the “Edit...” button.

## Actions



Actions will be triggered when an event (alarm or rearm) occurs. The following actions are supported:

- **Email**  
Send emails based on different time frame
- **HTTP Action**  
Post to a web site using either GET or POST methods. Form data can be specified for POST method.
- **Run Command**  
Execute a SysUpTime server side command. You can embed token *\$ip* in the command. Token *\$ip* is the IP address of the host being monitored. This is a sample command that uses *\$ip*:  
*ping \$ip*
- **Run Remote Command**  
Use SSH/Telnet/RPC to login and then execute a command on remote computer, including Windows and Linux/UNIX machines. You can embed token *\$ip* in the command. Token *\$ip* is the IP address of the host being monitored.
- **Computer Action**  
Reboot/Power off a remote computer, including Windows and Linux/UNIX machines.
- **Service Action**  
Start/Stop/Restart a service on a remote computer, including Windows and Linux/UNIX machines.
- **Kill Process Action**  
Kill a running process on a remote computer, including Windows and Linux/UNIX machines.

Authentication is usually required if you need to access remote machine. The following dialog is for entering user/password information. Protocol field is for specifying the protocol that will be used for communicating with the server. The supported protocols are SSH/Telnet/Windows RPC. Windows RPC should be selected if the remote machine is a Windows machine. Windows RPC is not available if the SysUpTime server runs on Linux.



**Buttons:**

<b>Test Run</b>	Perform a test run. The selected actions will be performed. For instance, if one of the selected action is rebooting a machine, SysUpTime server will try to reboot it. This way can test if there are any incorrect parameters in action settings.
<b>Save As Default Actions</b>	Save the current actions to database, which can be used later so you don't have to enter the same action next time.
<b>Load Default Actions</b>	Load the default actions (saved beforehand) from database.

## Configure Threshold:

**Packet round trip time**

Enable threshold

Threshold

Fixed ▼ Severity: Warning

Fixed threshold: Generate alarm if result > 200 milliseconds Adva

Statistical threshold: Generate alarm if result Above times of standard d

Baseline Interval Days Adva

Generate alarm if 1 times of threshold violation occur.

Rearm

Fixed ▼

Fixed threshold: Generate rearm if result <= 200 milliseconds Adva

Statistical threshold: Generate rearm if result Within or below times of standard d

Ok Cancel

This screen is for configuring alarm and rearm threshold.

### Enable threshold:

By default, threshold checking is enabled. If disabled, monitor will only collect data.

## Threshold:

### ❑ Fixed Threshold

Threshold is fixed. You need to know what is normal and what is out of range first in order to set fixed threshold.

Press “Advanced” button to configure different fixed thresholds with different severity level for time ranges. For example, if your web server’s traffic varies dramatically on weekdays and weekend. You can set a threshold for weekdays, and another threshold for weekend.

### ❑ Adaptive Statistical Threshold

It uses dynamic rolling baseline to manage threshold. Baseline data is collected over a period of time, and baseline data is constantly updated as new data is collected. Threshold is automatically set based upon standard deviations of collected baseline data, or the average value of the past data. No alarm will be raised if minimum set of baseline data has not been collected.

The duration of the baseline period should be sufficiently long to span a similar variety of operating modes as will likely occur in the future.

Baseline interval is the length of time over which one set of data that will be baselined is collected.

The threshold is measured by number of standard deviations. If the collected data follows a Normal distribution, a range covered by one standard deviation includes about 68% of the total data; a range of two standard deviations about 95% of the total data; and of three standard deviations about 99.7% of the total data. For example, suppose a baseline value for a Ping monitor's round-trip time is 10 seconds and the standard deviation is 2 seconds. If the threshold is three times the standard deviation, then the monitor will remain in a good condition as long as it is round-trip time does not exceed 16 seconds. This can be represented as a formula of:

*if(round-trip > (baseline + (multiplier \* stddev)) then threshold is exceeded*

Substituting the numbers from the example above gives:

*if(round-trip > (10 + (3 \* 2)) then threshold is exceeded*

For instance, we plan to use statistical threshold to monitor a business web site. We create a URL sequence monitor with polling period of 5 minutes and set its threshold to be 3 standard deviations. We assume the web traffic patterns are similar on a weekly basis. So we set the baseline interval to 7 days. By default, the minimum set of baseline data is 5, and the maximum set of data is 10. We choose to use the default values. After monitor is started, it collects data for 35 days (because the minimum set of data is 5 and the baseline interval is 7 days), and then starts to computer statistical values and checks for threshold violation. If system collects data at 10:00 AM on Monday, system will use the previously collected sets of Monday 10:00 AM performance data to compute standard deviations and check if threshold is exceeded. If threshold is not exceeded, this new data will be added to baseline data and used later for computing statistical values. So baseline data is constantly updated and can always adapt to current situations.

Press “Advanced” button to configure boundaries for baseline data. Sometimes it is necessary to set boundaries for baseline data to ensure that baseline data is normal.

### **Rearm Threshold:**

Configure threshold for rearm event, that is, clearing alarm event. The rearm indicates that the monitored object has returned to a normal state. When rearm conditions are satisfied, a rearm event will be posted to alarm browser window and it can automatically clear corresponding threshold alarm.

## Monitor Types

### □ DNS Monitor

The DNS monitor checks a domain name server. It verifies that the DNS server can respond to requests and domain name can be correctly resolved.

#### Metrics Configuration:

<b>Host name to be resolved</b>	Enter a host name, such as “www.google.com”. This name will be passed to DNS server to be resolved to an IP address.
<b>Resolving host result</b>	Optional. Enter one or more IP addresses corresponding to the host name, separated by semicolon.

#### Threshold Configuration:

<b>Round trip time</b>	The response time of DNS query
------------------------	--------------------------------

### □ Database Query Monitor

Send SQL queries to Database server and measure response time and/or check content of response. Major database servers such as Oracle, MS SQL Server, Sybase, DB2, MySQL, and PostgreSQL are supported.

#### Metrics Configuration:

<b>Database name</b>	Name of the database.
<b>SQL statement</b>	An SQL statement to be used for query.

#### Threshold Configuration:

<b>Record rows</b>	Number of rows returned from SQL query.
<b>Content match</b>	Check the result of the SQL query.
<b>Result column 1</b>	Check the first column of the result of the SQL query.
<b>Result column 2</b>	Check the second column of the result of the SQL query.

## □ Directory Monitor

The Directory monitor watches an entire directory and reports on the total number of files in the directory, the total amount of disk space used, and the time (in minutes) since any file in the directory was modified. This information is useful if you have limited disk space, you want to monitor the number of files written to a specific directory, or you want to know the activity level in a certain directory.

### Metrics Configuration:

<b>Directory path</b>	Enter the directory that you want to monitor. The directory is relative to the SysUpTime server. To monitor a directory on a remote machine in a Windows NT/2000 network, enter the UNC name for that directory. For example: \\192.168.1.100\sharedDir.
<b>Check subdirectories</b>	If checked, subdirectories will be counted.
<b>Check for directory changes</b>	This option affects all the threshold metrics. If checking failed, an error will be raised.  Three modes: <ul style="list-style-type: none"> <li>▪ No checking SysUpTime does not check for directory changes.</li> <li>▪ Compare to last contents SysUpTime compare the directory with the previous results.</li> <li>▪ Compare to first contents SysUpTime compare the directory with the first results.</li> </ul>
<b>Check metrics</b>	It doesn't matter if the mode of "Check for directory changes" is "No checking".  Three options: <ul style="list-style-type: none"> <li>▪ File name When checking for directory changes, only file names are considered.</li> <li>▪ File name and size When checking for directory changes, only file names and their sizes are considered.</li> <li>▪ File name, size and modified time When checking for directory changes, only file</li> </ul>

	names, their sizes and modification time are considered.
--	--

**Threshold Configuration:**

<b>Number of files</b>	Check if the number of files in the monitored directory exceeds a given number.
<b>Directory age</b>	Check if the age of the monitored directory exceeds a given number of minutes.
<b>Total size of the directory</b>	Check if the total size of the directory exceeds a certain number of bytes.

□ **E-Mail Monitor**

The E-Mail monitor checks an email Server via the network. It verifies that the email server is accepting requests, and also verifies that a message can be sent and retrieved. It does this by sending a standard email message using SMTP and then retrieving that same message via a POP3 user account. Each message that SysUpTime sends includes a unique key which it checks to insure that it does not retrieve the wrong message and return a false OK reading. If SysUpTime is unable to complete the entire loop it generates an error message.

## Metrics Configuration:

<b>Action</b>	<p>Select the action the E-Mail Monitor should take with respect to the mail server. The <i>Send &amp; receive</i> option will allow you to send a test message to an SMTP server and then receive it back from the POP3 or IMAP4 server to make sure the mail server is up and running. Use the <i>Receive only</i> option to check the incoming POP3 or IMAP4 email servers for a message that was sent previously. This check is done by matching the content of the previously sent message. The <i>Send only</i> option checks that the receiving email server has accepted the message.</p> <p><b>Note:</b></p> <p>If the <i>Receive only</i> option is selected, you should use this monitor for a dedicated email account that is NOT being accessed by any other email client. If another email client attempts to retrieve email messages from the account that the E-Mail Monitor is monitoring in <i>Receive only</i> mode, the monitor and the other mail client may lock each other out of the account such that neither is able to retrieve the messages.</p>
Send E-Mail configuration	
<b>SMTP server</b>	Enter the hostname of the SMTP server to which the test mail message should be sent (for example, smtp.foo.com).
<b>User name/ Password</b>	User name and password if SMTP server requires authentication.
<b>From</b>	The email address to which the test message is sent from.
<b>To</b>	The email address to which the test message should be sent.
<b>Subject</b>	The subject of the test email message.
<b>Body</b>	The body of the test email message.
<b>Attachment</b>	The full path name of a file to add as an attachment to the test email message.
<b>Encoding</b>	Encoding of the email body. The default is Cp1252 (Latin).
<b>Timeout</b>	Timeout value for sending the test message.

Receive E-Mail configuration	
<b>Protocol</b>	The protocol used for receiving emails, either POP3 or IMAP4.
<b>Mark deleted</b>	If checked, fetched messages will be deleted on the server side.
<b>Server</b>	The host name or IP address of POP3 or IMAP4 server
<b>User name/ Password</b>	User name and password if server requires authentication.
<b>Timeout</b>	Timeout value for receiving the test message.
<b>Delay</b>	For “Send and receive” mode only, SysUpTime waits after message has been sent and then starts fetching the email.

#### Threshold Configuration:

<b>Send time</b>	The time used for sending out the email. It is not valid for “Receive only” action.
<b>Receive time</b>	The time used for receiving emails. It is not valid for “Send only” action.
<b>Round trip time</b>	The time used for sending and receiving emails.
<b>Receive content match</b>	Check content of the received emails. It is not valid for “Send only” action.

## □ Monitor MS Exchange Server

If you want to check the SMTP/POP3/IMAP4 functionality of Exchange server, you can create Email monitors. For example, you can create an Email “Send and Receive” monitor to check if a user can send out an email via SMTP and receive the email via POP3 or IMAP4.

For Exchange server with version earlier than Exchange server 2000, you can create SNMP monitors to check metrics of it. For Exchange server 2000 and later versions, you can create Exchange server monitors to monitor critical Exchange services and performance counters (Information Store, mailboxes, SMTP service, etc.).

### Metrics Configuration:

<b>Remote host</b>	Enter information about Exchange server.
<b>Timeout</b>	Timeout value for connecting to the Exchange server.
<b>Instances</b>	The instances to check.

### Threshold Configuration:

<b>Match result</b>	The query result.
---------------------	-------------------

## ❑ Command Executor Monitor

Run command on the server side and compare the output against threshold.

### Metrics Configuration:

<b>Encrypt the command</b>	If checked, command to be executed will be encrypted. This is necessary if commands contain sensitive data such as passwords. The command is not editable if this option is checked.
<b>Timeout</b>	Timeout value for executing the command.

### Threshold Configuration:

<b>Response time</b>	The time used for executing the command.
<b>Content match</b>	Check the result of the command.

Here is an example of content match for command “ping www.google.com”. On windows, the command line output is listed below:

*“ Pinging www.l.google.com [64.233.161.147] with 32 bytes of data:*

*Reply from 64.233.161.147: bytes=32 time=490ms TTL=233*

*Reply from 64.233.161.147: bytes=32 time=470ms TTL=232*

*Reply from 64.233.161.147: bytes=32 time=476ms TTL=232*

*Reply from 64.233.161.147: bytes=32 time=477ms TTL=233*

*Ping statistics for 64.233.161.147:*

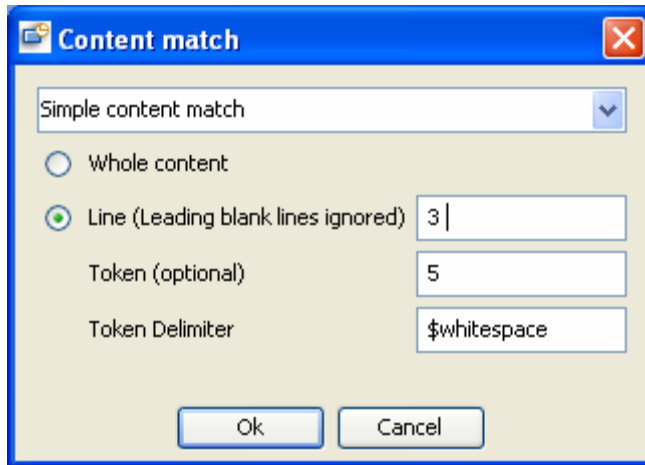
*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

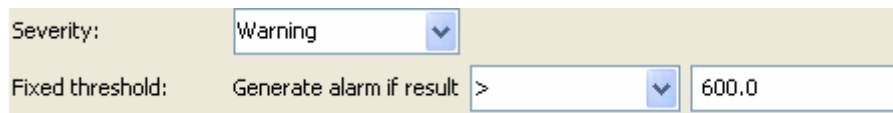
*Minimum = 470ms, Maximum = 490ms, Average = 478ms*

*“*

There is an empty line in the beginning of the result but it will be ignored (All the leading blank lines are ignored). If we want to check the response time from the first “*Reply from*” line, we can set:



And in the threshold configuration screen:



Although the token fetched is “*time=490ms*” which contains both letters and digits, it will be converted to digit and check against threshold (600.0) in this case.

## □ File Monitor

The file Monitor reads a specified file. In addition to checking the size and age of a file, the file monitor can help you verify that the contents of files, either by matching the contents for a piece of text, or by checking to see if the contents of the file ever changes.

### Metrics Configuration:

<b>File path</b>	Enter the fully qualified name of the file to be monitored. For example, c:\docs\doc1.doc.
<b>No error if file not found</b>	If checked, no alarm will be raised when the file being monitor does not exist.
<b>File encoding</b>	The encoding of the file if it is a text file.
<b>Check for content changes</b>	If checking failed, an error alarm will be raised.  Three modes: <ul style="list-style-type: none"><li>▪ No checking SysUpTime does not check for content changes</li><li>▪ Compare to last contents Compare the contents to the last one.</li><li>▪ Compare to saved contents Compare the contents to the saved contents. If the saved contents change after monitor starts, the change will not be honored.</li></ul>

### Threshold Configuration:

<b>Content match</b>	Check the content of the file.
<b>File size</b>	Check the size of the file.
<b>Status</b>	Check if error occurs.

## □ FTP Monitor

The FTP monitor attempts to log into an FTP server and retrieve a specified file. A successful file retrieval assures you that your FTP server is functioning properly.

In addition to retrieving specific files, the FTP monitor can help you verify that the contents of files, either by matching the contents for a piece of text, or by checking to see if the contents of the file ever changes compared to a reserve copy of the file.

### Metrics Configuration:

<b>Remote host</b>	The host name or IP address of the FTP server.
<b>File path</b>	The file name to retrieve, for example <i>/pub/readme.txt</i>
<b>File encoding</b>	The encoding of the file if it is a text file.
<b>Check for content changes</b>	If checking failed, an error alarm will be raised.  Three modes: <ul style="list-style-type: none"><li>▪ No content checking SysUpTime does not check for content changes.</li><li>▪ Compare to last contents Compare the contents to the last one.</li><li>▪ Compare to saved contents Compare the contents to the saved contents. If the saved contents change after monitor starts, the change will not be honored.</li></ul>

### Threshold Configuration:

<b>File content match</b>	Check the content of the received file.
<b>File size</b>	Check the size of the received file.
<b>Round trip time</b>	Check the round trip time of receiving a file.

## □ Log File Monitor

The log file monitor watches for specific entries added to a log file by looking for entries containing a text phrase or a regular expression.

### Metrics Configuration:

<b>File path</b>	Enter the fully qualified name of the file to be monitored. For example, c:\docs\doc1.doc.
<b>No error if file not found</b>	If checked, no alarm will be raised when the file being monitor does not exist.
<b>File encoding</b>	The encoding of the file if it is a text file.
<b>Check from beginning</b>	<p>If checking failed, an error alarm will be raised.</p> <p>This setting controls what SysUpTime will look for and how much of the target file will be checked each time that the monitor is run. Three modes:</p> <ul style="list-style-type: none"> <li>▪ Never Check only newly added records, starting at the time that the monitor was created (not when the file was created). This is the default behavior.</li> <li>▪ First time only Check the whole file once when the monitor is first created, then only for new records on each subsequent monitor run. Use this option to check a file that already had entries before the monitor was created or started.</li> <li>▪ Always Always check the contents of the whole file.</li> </ul>

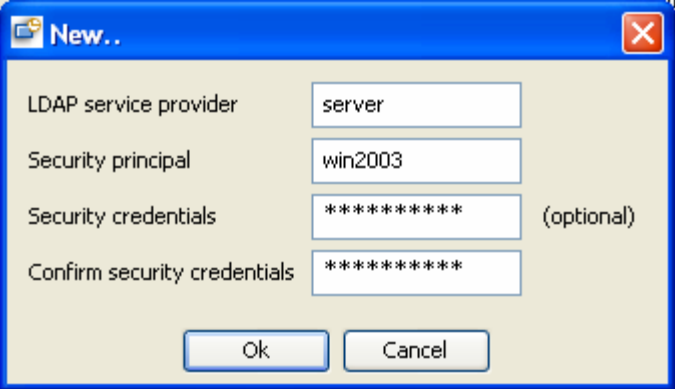
### Threshold Configuration:

<b>Content match</b>	Check the content of the file.
<b>Size</b>	Check the size of the file.

❑ **LDAP Monitor**

The LDAP monitor verifies that a Lightweight Directory Access Protocol (LDAP) server is working correctly by connecting to it and performing a "simple" authentication. Optionally, it can check the result for expected content.

**Metrics Configuration:**

<p><b>Remote host</b></p>	<p>LDAP server data.</p>  <ul style="list-style-type: none"> <li>▪ <b>LDAP service provider</b> Host name or IP address of LDAP server, or a URL string such as <i>ldap://server:389</i></li> <li>▪ <b>Security principal</b> User name.</li> <li>▪ <b>Security credentials</b> Password.</li> </ul>
<p><b>Object Query</b></p>	<p>Use this box to enter an object query to look at a LDAP object other than the default user dn object. For example, enter the mail object to check for an e-mail address associated with the dn object entered above. You must enter a valid object query in this text box if you are using a LDAP filter.</p>
<p><b>LDAP filter</b></p>	<p>Enter an LDAP filter in this text box in order to perform a search using a filter criteria. The LDAP filter syntax is a logical expression in prefix notation meaning that logical operator appears before its arguments. For example, the item <i>sn=Smith</i> means that the <i>sn</i> attribute must exist with the attribute value equal to <i>Smith</i>. Multiple items can be included in the filter string by enclosing them in parentheses, such as <i>(sn=Smith)</i> and combined using logical operators such as the <i>&amp;</i> (the conjunction operator) to create logical expressions. For example the filter syntax <i>(&amp; (sn=Smith) (mail=*))</i> requests LDAP entries that have both a <i>sn</i> attribute of <i>Smith</i> and a <i>mail</i> attribute.</p> <p>More information about LDAP filter syntax can be found at <a href="http://www.ietf.org/rfc/rfc2254.txt">http://www.ietf.org/rfc/rfc2254.txt</a> and also at <a href="http://java.sun.com/products/jndi/tutorial/basics/directory/filter.html">http://java.sun.com/products/jndi/tutorial/basics/directory/filter.html</a></p>
<p><b>Search</b></p>	<p>Three modes:</p>

<b>scope</b>	<ul style="list-style-type: none"> <li>▪ <b>The named object:</b> Search the named object.</li> <li>▪ <b>One level of the named context:</b> Search one level of the named context.</li> <li>▪ <b>Subtree at the named context:</b> Search the entire subtree rooted at the named object.</li> </ul>
<b>Return Attributes</b>	Specifies the attributes that will be returned as part of the search. Empty value indicates that all attributes will be returned.

**Threshold Configuration:**

<b>Content match</b>	Check the content of the received file.
<b>Round trip time</b>	Check the round trip time of LDAP query.

□ **Ping Monitor**

Ping monitor sends ICMP PING requests to check the status of network nodes.

**Metrics Configuration:**

<b>Timeout</b>	Timeout value for PING requests, in milliseconds.
----------------	---

**Threshold Configuration:**

<b>Packet round trip time</b>	The round trip time of the PING request.
<b>Packet success rate</b>	For each run, monitor sends three PING requests and calculate the success rate. The delay between PING requests is one second.

## ❑ SNMP Monitor

SysUpTime provides comprehensive SNMP monitoring capacities. The SNMP monitor issues SNMPv1/v2c/v3 requests to retrieve the values from SNMP agents and check against preset threshold values.

Requirements for using the SNMP monitor include:

- SNMP agents must be deployed and running on the servers and devices that you want to monitor
- The SNMP agents must be supplied with the necessary Management Information Bases (MIBs) and configured to read those MIBs/
- You need to know the Object ID's (OIDs) of the parameters you want to monitor.

### Metrics Configuration:

<b>OID/Expression name</b>	Enter SNMP OID or math expression, which specify which value should be retrieved from the SNMP agent.  See the following OID/Expression section for more details.
<b>Port number</b>	The port number of SNMP agent.
<b>Community</b>	The community string of SNMP agent. The default value is “public”. If its value is empty, the default value will be used instead.
<b>Timeout</b>	Timeout value for PING requests, in milliseconds.
<b>Retries</b>	Number of retries for SNMP requests after requests fail.
<b>Version</b>	The SNMP version number of SNMP agent.

Threshold includes comparison of numeric value and content match. For instance, you can create a monitor with numeric threshold to check interface utilization of a node, or a monitor with content match threshold to check whether the SNMP *sysDescr* string has been changed to another value.

### SNMP OID/Expression

If OID ends with “.s” (such as 1.3.6.1.2.1.25.4.2.1.2.s), it means all the values under this subtree (1.3.6.1.2.1.25.4.2.1.2) will be retrieved, and the values will be treated as string data type and concatenated into a string separated by new line character.

If OID ends with “.d” (such as 1.3.6.1.2.1.25.4.2.1.2.d ), it means all the values (must be numeric) under this subtree (1.3.6.1.2.1.25.4.2.1.2) will be retrieved, and the sum of the values will be calculated and returned.

If OID ends with “.”, it means it is a tabular object whose index needs to be supplied. If you have this type of OID in an expression, you will be prompted to enter its index value.

Variable Name	Variable OID
ifInOctets	.1.3.6.1.2.1.2.2.1.10.
ifOutOctets	.1.3.6.1.2.1.2.2.1.16.
ifSpeed	.1.3.6.1.2.1.2.2.1.5.

Each expression has a name, expression body and description. Expression name can only start with a letter. Expression can have one or more variables, with each variable corresponding to an SNMP OID. After querying SNMP agent, the variables will be replaced with the values corresponding to their OIDs. And then those variables will be fed into the expression to calculate the final value of the expression.

The following functions are supported in expression:

<ul style="list-style-type: none"> <li>▪ <i>double abs(double a)</i> Returns the absolute value of a double value.</li> <li>▪ <i>float abs(float a)</i> Returns the absolute value of a float value.</li> <li>▪ <i>int abs(int a)</i> Returns the absolute value of an int value.</li> <li>▪ <i>long abs(long a)</i> Returns the absolute value of a long value.</li> <li>▪ <i>double acos(double a)</i> Returns the arc cosine of an angle, in the range of 0.0 through pi.</li> <li>▪ <i>double asin(double a)</i> Returns the arc sine of an angle, in the range of -pi/2 through pi/2.</li> <li>▪ <i>double atan(double a)</i> Returns the arc tangent of an angle, in the range of -pi/2 through pi/2.</li> <li>▪ <i>double atan2(double y, double x)</i> Converts rectangular coordinates (x, y) to polar (r, theta).</li> <li>▪ <i>double ceil(double a)</i> Returns the smallest (closest to negative infinity) double value that is not less than the argument and is equal to a mathematical integer.</li> <li>▪ <i>double cos(double a)</i> Returns the trigonometric cosine of an angle.</li> <li>▪ <i>double exp(double a)</i> Returns Euler's number e raised to the power of a double value.</li> <li>▪ <i>double floor(double a)</i> Returns the largest (closest to positive infinity) double value that is not greater than the argument and is equal to a mathematical integer.</li> <li>▪ <i>double log(double a)</i> Returns the natural logarithm (base e) of a double value.</li> </ul>	<ul style="list-style-type: none"> <li>▪ <i>double max(double a, double b)</i> Returns the greater of two double values.</li> <li>▪ <i>float max(float a, float b)</i> Returns the greater of two float values.</li> <li>▪ <i>int max(int a, int b)</i> Returns the greater of two int values.</li> <li>▪ <i>long max(long a, long b)</i> Returns the greater of two long values.</li> <li>▪ <i>double min(double a, double b)</i> Returns the smaller of two double values.</li> <li>▪ <i>float min(float a, float b)</i> Returns the smaller of two float values.</li> <li>▪ <i>int min(int a, int b)</i> Returns the smaller of two int values.</li> <li>▪ <i>long min(long a, long b)</i> Returns the smaller of two long values.</li> <li>▪ <i>double pow(double a, double b)</i> Returns the value of the first argument raised to the power of the second argument.</li> <li>▪ <i>double random()</i> Returns a double value with a positive sign, greater than or equal to 0.0 and less than 1.0.</li> <li>▪ <i>double rint(double a)</i> Returns the double value that is closest in value to the argument and is equal to a mathematical integer.</li> <li>▪ <i>long round(double a)</i> Returns the closest long to the argument.</li> <li>▪ <i>int round(float a)</i> Returns the closest int to the argument.</li> <li>▪ <i>double sin(double a)</i> Returns the trigonometric sine of an angle.</li> <li>▪ <i>double sqrt(double a)</i> Returns the correctly rounded positive square root of a double value.</li> <li>▪ <i>double tan(double a)</i> Returns the trigonometric tangent of an angle.</li> </ul>
--	--

For example, we can use max function to calculate the interface utilization for full-duplex point-to-point media:

$$\text{max}(ifInOctets, ifOutOctets) * 8 / ifSpeed * 100$$

SNMP monitor can query agent using an OID or expression. You can choose one from a list of predefined expressions, or create a new expression. For example, *ifutil* is defined as:

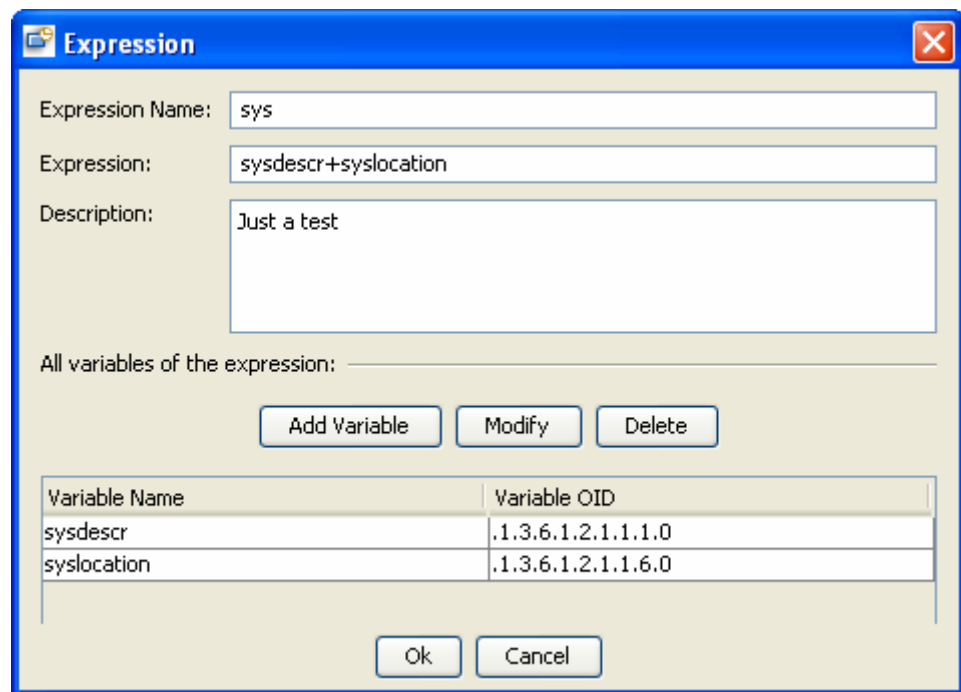
$$(ifInOctets + ifOutOctets) * 8 / ifSpeed * 100$$

*ifInOctest*, *ifOutOctets* and *ifSpeed* are tabular objects whose OID ends with “.” in the expression, so you need to supply an index for them.

Expression also supports string values. If values of variables are string type, their values are concatenated in this way:

- If they are scalar objects (only one value for each variable), there values are concatenated into value1<>value2<>... (“<>” is the delimiter). The order of values are determined by the order of variables in the variable list.

Here is an example:



This example concatenates sysDescr and sysLocation variables. A sample result is:

```
Linux lserver 2.6.9-5.0.3.ELsmp #1 SMP i686<>Unknown<>
```

- If they are tabular objects, values are concatenated line by line, with columns separated by ‘<>’. For instance, if we have two variables and their values are  
“A  
B  
C”  
and

“1  
2  
3”

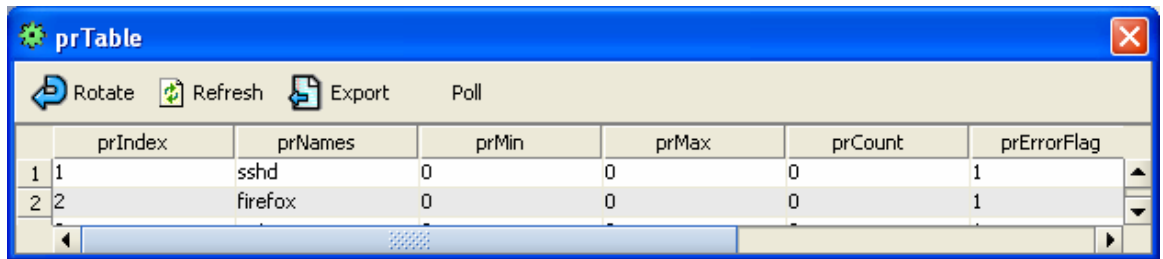
The final result is

“A<>1<>  
B<>2<>  
C<>3<>”

A real world example is an expression for checking the running status of a process on Linux. If the default NET-SNMP agent is running, you can configure its `snmpd.conf` file to let it report the status of processes. For example, we want to monitor the `sshd` process, so we add a line to the `snmpd.conf`:

```
proc sshd
```

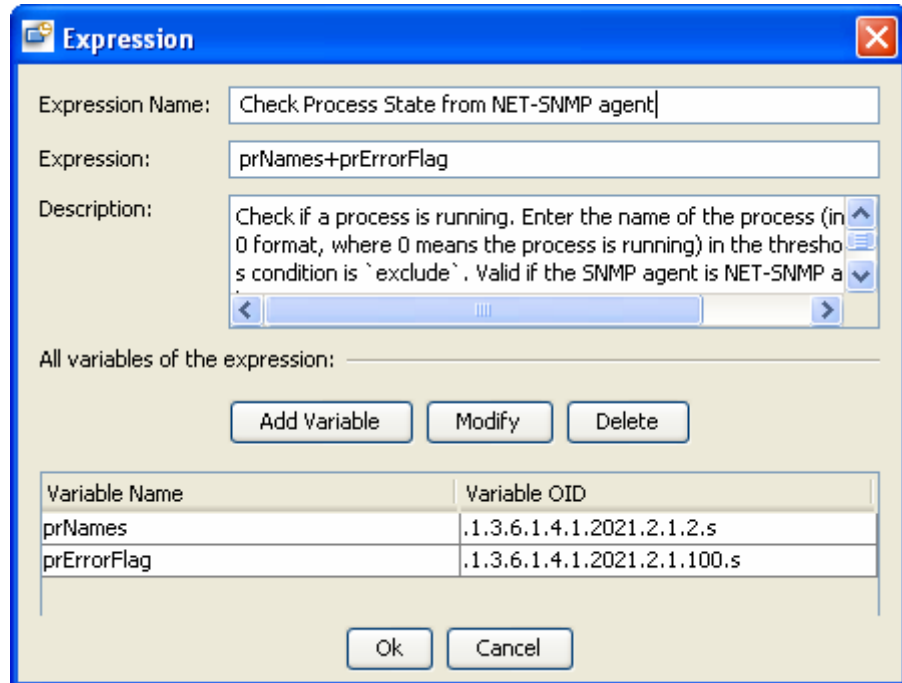
Then the *prTable* should report `sshd`'s running status, as shown below:



	prIndex	prNames	prMin	prMax	prCount	prErrorFlag
1	1	sshd	0	0	0	1
2	2	firefox	0	0	0	1

To monitor if a process is OK, we need to check both “*prNames*” and “*prErrorFlag*” columns to make sure that the process’ name is there and its *prErrorFlag*’s value is 0 (no error).

We create the following expression:



The OIDs of *prNames* and *prErrorFlag* end with “.s” because we need to get all the values under the subtrees.

A sample result is:

```
sshd<>0<>
firefox<>0<>
gvim<>0<>
```

In the threshold screen, we set the condition to be “exclude” and the threshold value is “sshd<>0<>”. Then if sshd process is down, the value will be changed to “sshd<>1<>” and an alarm will be raised.

**Note:**

The order of the result is not determined by the expression in this case. That is, the result would be the same if you changed the expression from “*prNames + prErrorFlag*” to “*prErrorFlag + prNames*”. The order is determined by the variable order in the “Variable Name” table. If you moved *prErrorFlag* to be the first variable, the result would be “0<>sshd<>”.

## SNMP Counter Objects

All SNMP counter data types are converted to rate. For instance, in the aforementioned *ifutil* expression, *ifInOctets* and *ifOutOctets* are counters, the values of them in the expression will be their rates, that is

$$ifInOctest = ( ifInOctest(t2) - ifInOctest (t1) ) / (t2 - t1)$$

$$ifOutOctest = ( ifOutOctest(t2) - ifOutOctest (t1) ) / (t2 - t1)$$

where t2 and t1 are the time of two pollings. Rate can not be computed if there is only one value. So the first value of an expression with counter variables will be always unavailable.

In SNMP agent, SNMP counter value will be reset if it reaches its maximum value. SysUpTime can handle a single counter wrap properly. If two counter wraps occur between two polling data, the result will be wrong. So you need to set a proper polling interval if SNMP counter is involved. The maximum value of a 32 bit counter is 4,294,967,296. For the *ifInOctets* counter, it will reach maximum value and reset in about 6 minutes if the link speed is 100Mbps, and about 30 seconds if the link speed is 1Gbps.

## □ Port Monitor

Port monitor verifies that a connection can be made to a network port and measures the length of time it takes to make the connection. Optionally, it can look for a string of text to be returned or send a string of text once the connection is made.

### Metrics Configuration:

<b>Port</b>	Port number to connect to.
<b>Timeout</b>	Timeout value for network connection, in milliseconds.
<b>Send String</b>	String to be send. It can be one line or multiple lines. New line characters will be preserved if present.

### Threshold Configuration:

<b>Port content match</b>	Check the content of response.
<b>Port response time</b>	Check the response time.

## □ URL Sequence

Send one or more HTTP/HTTPS requests to web servers. It can be used to monitor the performance and availability of web servers, and performance of multi-step web transactions (banking, shopping carts, etc.).

Functionality includes:

- Availability check
- Performance check
- Content verification
- POST URL Monitoring (Form submission)
- Password protected sites
- Follow Redirection

## □ **Radius Monitor**

The Radius monitor checks that a RADIUS server is working correctly by sending an authentication request and checking the result.

### **Metrics Configuration:**

<b>Remote host</b>	Select or create a host to be monitored.
<b>Secret phrase</b>	The secret phrase used to encrypt all requests to this RADIUS server
<b>Retries</b>	Number of retries after queries fail.
<b>Timeout</b>	Connection timeout value.

### **Threshold Configuration:**

<b>Content match</b>	Check the result.
<b>Round trip time</b>	Check the response time.

## □ **Telnet and SSH Monitors**

Use Telnet or SSH to connect to remote Linux/UNIX server and issue commands and check the results against thresholds. The more secure version of SSH, SSH2, is supported. Telnet/SSH monitors are powerful tools to monitor the detailed status of servers. For instance, they are commonly used to monitor the CPU, memory, process information of Linux/UNIX servers.

### **Metrics Configuration:**

<b>Remote host</b>	Select or create a host to be monitored.
<b>Command</b>	The command to be issued after connected to the host.

**Threshold Configuration:**

<b>Content match</b>	Check the result of the command.
<b>Response time</b>	Check the response time.

□ **WMI Monitor**

The WMI monitor is used to monitor the status of Windows machines. WMI monitors are powerful tools to monitor the detailed status of Windows machines. For instance, they are commonly used to monitor the CPU, memory, process information of Windows servers.

**Metrics Configuration:**

<b>Remote host</b>	Select or create a host to be monitored.
<b>Script path</b>	<p>The absolute path of the WMI script to be executed. The script must take one, three or four arguments:</p> <ul style="list-style-type: none"> <li>▪ One argument: Host name. No authentication is required.</li> <li>▪ Three arguments: Host name, user name and password.</li> <li>▪ Four arguments: Host name, user name, password, and Windows domain name.</li> </ul> <p>The return value of the script will be used for checking against threshold.</p>
<b>Timeout</b>	Timeout value for executing the WMI script.

**Threshold Configuration:**

<b>Content match</b>	Check the result of the command.
<b>Response time</b>	Check the response time.

## □ Windows Event Log Monitor

The Windows Event Log monitor watches Windows Event Logs (System, Application, Security or others) for newly added entries. It can scan Windows Event logs on local or remote computers and look for specific Event Sources, Categories, and Event IDs as well as for patterns in the Description of the Event.

The Windows Event Log Monitor examines only log entries made after the time that the monitor is created. Each time the monitor runs thereafter, it examines only those entries added since the last time it ran. You can choose to filter out messages that are not important.

### Metrics Configuration:

<b>Remote host</b>	Select or create a host to be monitored.
<b>Timeout</b>	Timeout value.
<b>Log name</b>	Select all or one of Application, Security, System or user-defined log.
<b>Type</b>	Event severity.
<b>Source</b>	Event source.
<b>Category</b>	Event category.
<b>Event ID</b>	Event ID
<b>User</b>	Value of the user field of the event.
<b>Computer</b>	Value of the computer field of the event.

### Threshold Configuration:

<b>Content match</b>	Check the result of the event query.
<b>Response time</b>	Check the response time.
<b>Match count</b>	The total number of retrieved events.

## Monitors Snapshot

Monitors snapshot gives a snapshot of the current state of all the active monitors. The results can be automatically refreshed periodically.



## Change Default Values of Monitors

The default values, such as timeout and port, come from an XML located at `$INSTALL_DIR/server/server/default/conf/client-monitor.xml`. You can use any text editors to change default values or add new monitor types.

Example 1: Add a new Ping monitor whose timeout value is 30 seconds

```
<ServiceCommunity name="PING">
  <ServiceFamily name="PING">
    <Service name="PING" tooltip="tooltip_ping">
      <Metrics name="PING" protocol="PING" length="190" height="30">
        <Parameter name="timeout" input="JTextField"
          validation="com.yxkj.mainframe.performance.PositiveIntValidator"
          unit="MILLISECONDS">
          5000</Parameter>
        <ConfigThreshold name="PACKET_RTT" unit="MILLISECONDS"/>
        <ConfigThreshold name="PACKET_SUCCESS_RATE"/>
      </Metrics>
    </Service>
    <!--NEW -->
    <Service name="PING" tooltip="tooltip_ping">
      <Metrics name="PING" protocol="PING" length="190" height="30">
        <Parameter name="timeout" input="JTextField"
          validation="com.yxkj.mainframe.performance.PositiveIntValidator"
          unit="MILLISECONDS">
          30000</Parameter>
        <ConfigThreshold name="PACKET_RTT" unit="MILLISECONDS"/>
        <ConfigThreshold name="PACKET_SUCCESS_RATE"/>
      </Metrics>
    </Service>
  </ServiceFamily>
</ServiceCommunity>
```

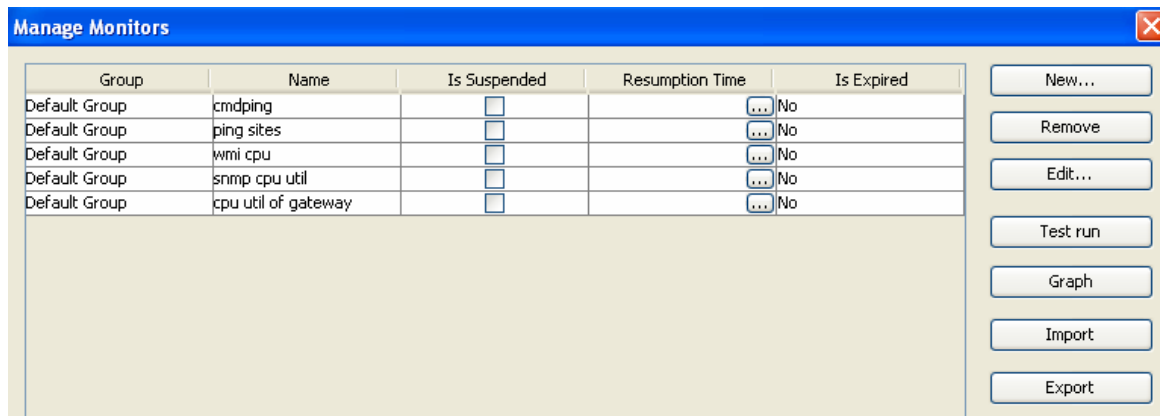
## Example 2: Add a new Telnet monitor for Linux

This new monitor uses “*ps aux | wc | awk '{print \$1}'*” command to check the number of processes running on Linux machine.

```
<Service name="TELNET_PROCESSES_LINUX" isHostDisabled="true" tooltip="tooltip_telnet_linux_process" >
  <Metrics name="TELNET" protocol="TELNET" length="190" height="30">
    <Parameter name="remote_host" input="JComboBox"
      validation="com.yxkj.mainframe.performance.NonNullValidator"/>
    <Parameter name="command" input="JTextField"
      tooltip="tooltip_command"
      validation="com.yxkj.mainframe.performance.NonNullValidator">
      ps aux | wc | awk '{print $1}'
    </Parameter>
    <ConfigThreshold name="TELNET_CONTENT_MATCH" isFixedOnly="true" isMulti="true"
      condition="exclude"/>
  </Metrics>
</Service>
```

After you change the client-monitor.xml, you can press “Refresh” button in the “Add Monitors” dialog to reload it.

## Manage Monitors



Buttons are listed below:

<b>New</b>	Create a new monitor.
<b>Remove</b>	Select one or more rows and remove them. You need to hold down CTRL key and select multiple rows.
<b>Edit</b>	Select a row and edit it.
<b>Test run</b>	Select a row and do test run.
<b>Graph</b>	Plot performance graph for selected monitor.
<b>Import</b>	Import monitors from an XML file.
<b>Export</b>	Export selected one or more monitors to an

XML file.
-----------

You can click on the checkmark of the “*Is Suspended*” column to suspend a monitor. You will be prompted to enter monitor resumption time. If you do not want to resume this monitor at a later time, you can just disable resumption.

## Bulk Add Monitors

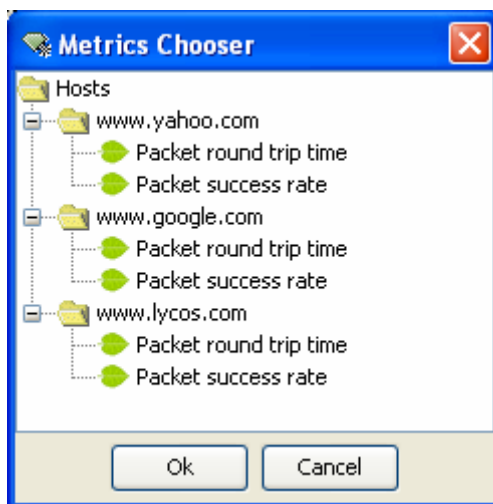
The export/import buttons on the “Manage Monitors” dialog can be used to bulk add monitors. This is a typical way:

1. Create a sample monitor.
2. Export it to an XML file.
3. Use your favorite text editor to open the XML file. Each “Monitor” section represents a monitor. Copy the “Monitor” section and change the monitor name and other parameters to create a new monitor. The monitor name must be unique.
4. Import the XML file.

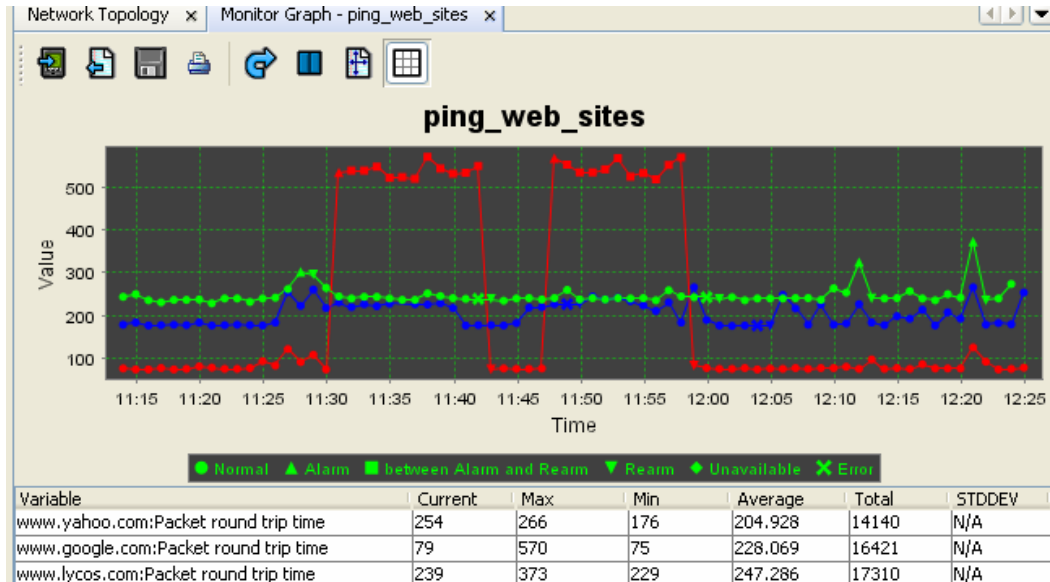
## Performance Graph

Performance graph can help you view the current and historical values of a monitor in a graph.

If the monitor has multiple metrics, you will be prompted with the following dialog window:



You can choose one of them, or hold down CTRL key and select multiple metrics. All the selected metrics will be plotted in the same graph.



To zoom into an area, move the mouse pointer to the area you wish to select, click on the left mouse button, and hold it down to select the rectangle. To go back to the original state, right mouse click on the graph and select “Auto Range/Both Axes” menu.

To maximize the graph, you can double click its tab, and double click again to restore to its original size.

### Graph Legends:

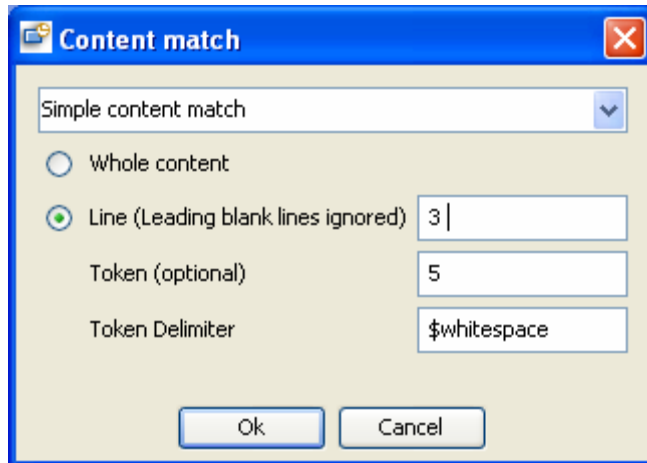
<b>Normal</b>	Normal data.
<b>Alarm</b>	Alarm occurs.
<b>Between Alarm and Rearm</b>	Alarm has not been cleared.
<b>Rearm</b>	Rearm event occurs. Status goes back to normal.
<b>Unavailable</b>	Data temporarily unavailable. But no error occurs.
<b>Error</b>	Error such as timeout occurs.
<b>Threshold</b>	Threshold bar

Besides showing current values in graph, you can press the “Import” button on the graph’s toolbar to import and plot historical data.

## Content Match

For monitors such as HTTP, SNMP, Telnet and Port, you can check the contents of the results. You can check if a phrase is contained in the whole result, or in a particular line and column, or compare the numerical value of a phrase with a threshold value.

Regular expression is supported. For instance, you can use “site[1-9]” to match “site1”, “site2”, ..., “site9”.



There are three types of content match:

### 1. Simple Content Match

- Whole content

Check whole content.

- Line

Line number. The default value ‘-1’ means checking the whole content. All the leading blank lines are ignored.

- Token

Token number. The default value ‘-1’ means checking the whole line.

- Token Delimiter

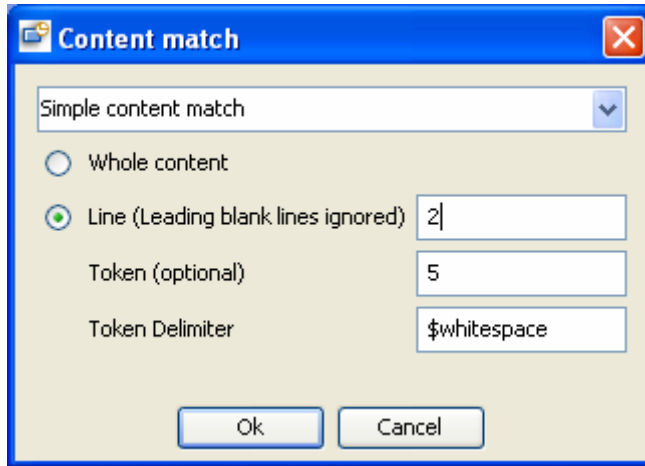
Token delimiter, required if token number is not ‘-1’. The default value ‘\$whitespace’ means white space.

Example:

For the following result:

*Pinging nt-e.gxn.net [195.147.246.32] with 32 bytes of data:  
Reply from 195.147.246.32: bytes=32 time=357ms TTL=107*

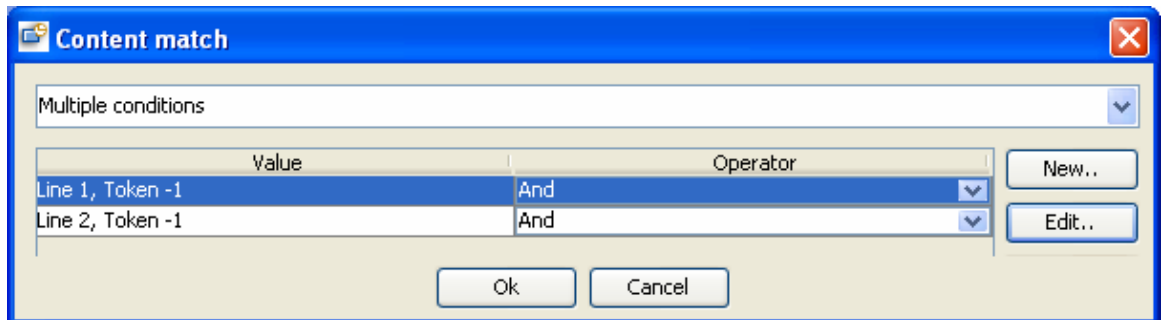
If we want to check the value of time, we can use the following values:



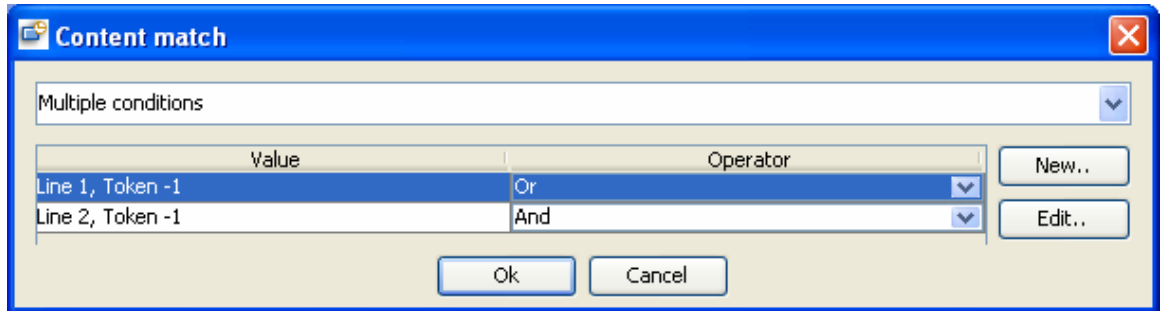
The token value is “*time=357ms*” . If the threshold is to compare it with a numerical value, this token will be automatically converted to 357.

## 2. Multiple Conditions

Multiple conditions can be specified. For instance, if you want to check if line 1 of the result contains ‘foo1’ and line 2 contains “foo2”, then you can set the conditions like this:



Or if you want to check if line 1 of the result contains ‘foo1’ or line 2 contains “foo2”, then you can set the conditions like this:



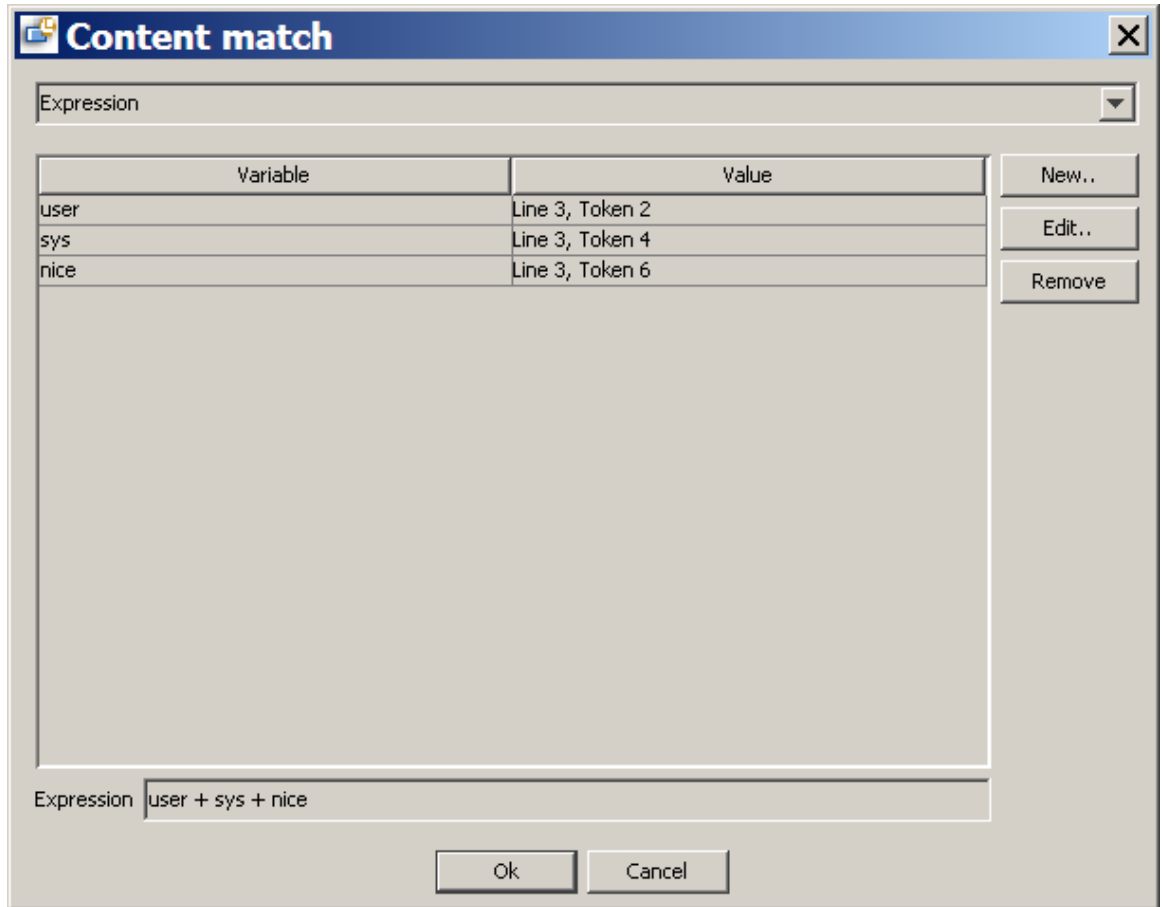
Because thresholds are already specified in conditions, there is no need to configure the threshold value in the final screen of the monitor configuration.

### 3. Expression

Sometimes, we need to use a math expression to calculate the final value of some data. For instance, one way to calculate user CPU usage on Linux is to issue this command “top -n 1 | head -3”. The following is a sample output:

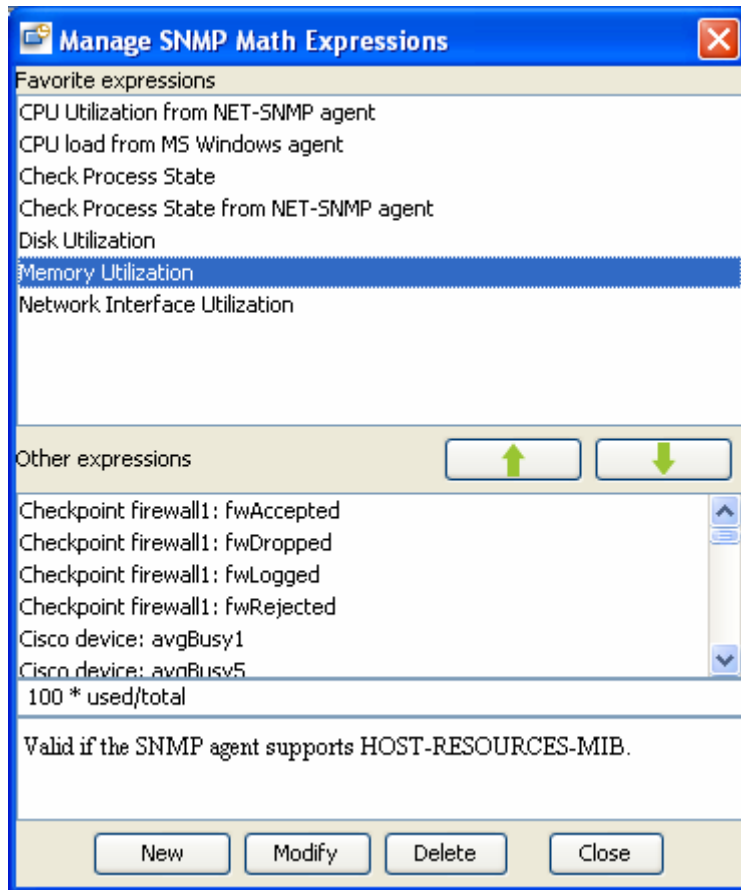
```
top - 15:20:13 up 7:17, 21 users, load average: 0.51, 0.41, 0.47
Tasks: 208 total, 1 running, 207 sleeping, 0 stopped, 0 zombie
Cpu(s): 7.8% us, 1.8% sy, 0.1% ni, 89.4% id, 0.7% wa, 0.0% hi, 0.3% si
```

The CPU usage is  $7.8 + 1.8 + 0.1 = 9.7$ , which is based on the values of the second, forth and sixth tokens on the third line. This screen shows an expression that calculates the result of “*user + sys + nice*”:



“user” value is taken from the second token of line 3, “sys” value from the fourth token of line 3, and “nice” value from sixth token of line 3.

## Manage SNMP Math Expressions



This window is divided into two pane: favorite expressions and others. You can select an expression and click up or down arrow button to move it between two panes.

There are some math expressions being used in SNMP monitors. You can create new expressions or edit existing ones. If an expression contains tabular objects, you need to provide index suffix for it, and then a new expression with the index suffix appended to its name will be added automatically. For example, if you use *ifutil* expression, and then you choose index to be “.2”, then a new expression named “*ifutil.2*” will be created automatically.

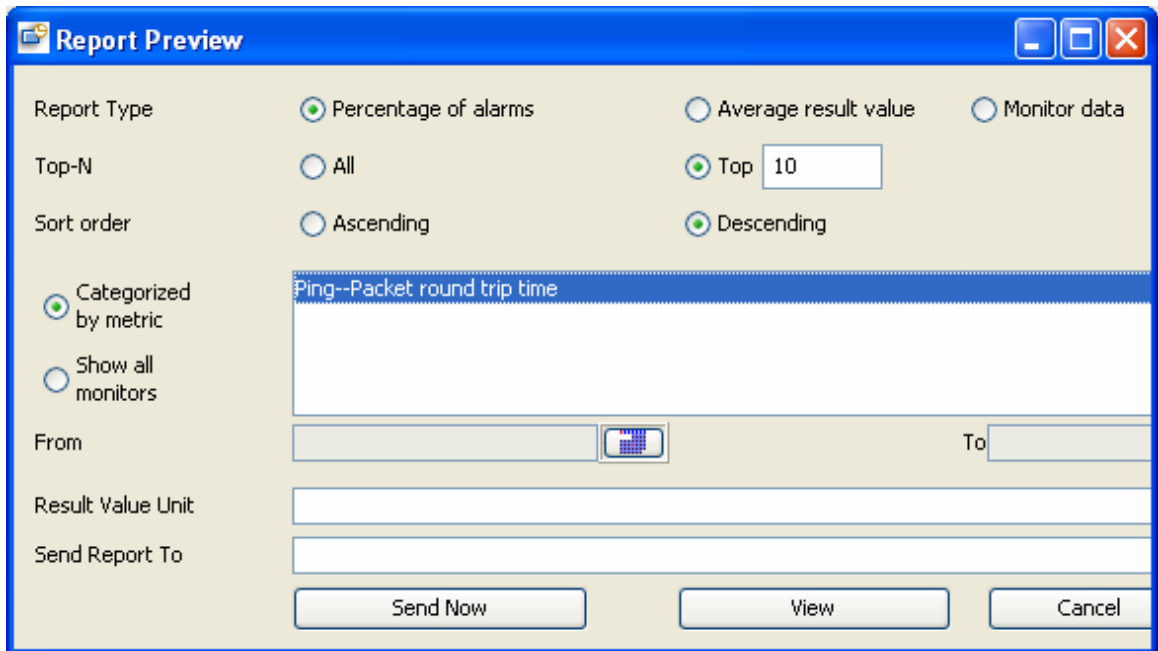
# Chapter 7. Report

## Quick Report

It allows user to take a quick look at the report of one or more monitors, or a top-N report that lists monitors sorted by alarm percentage or average values.

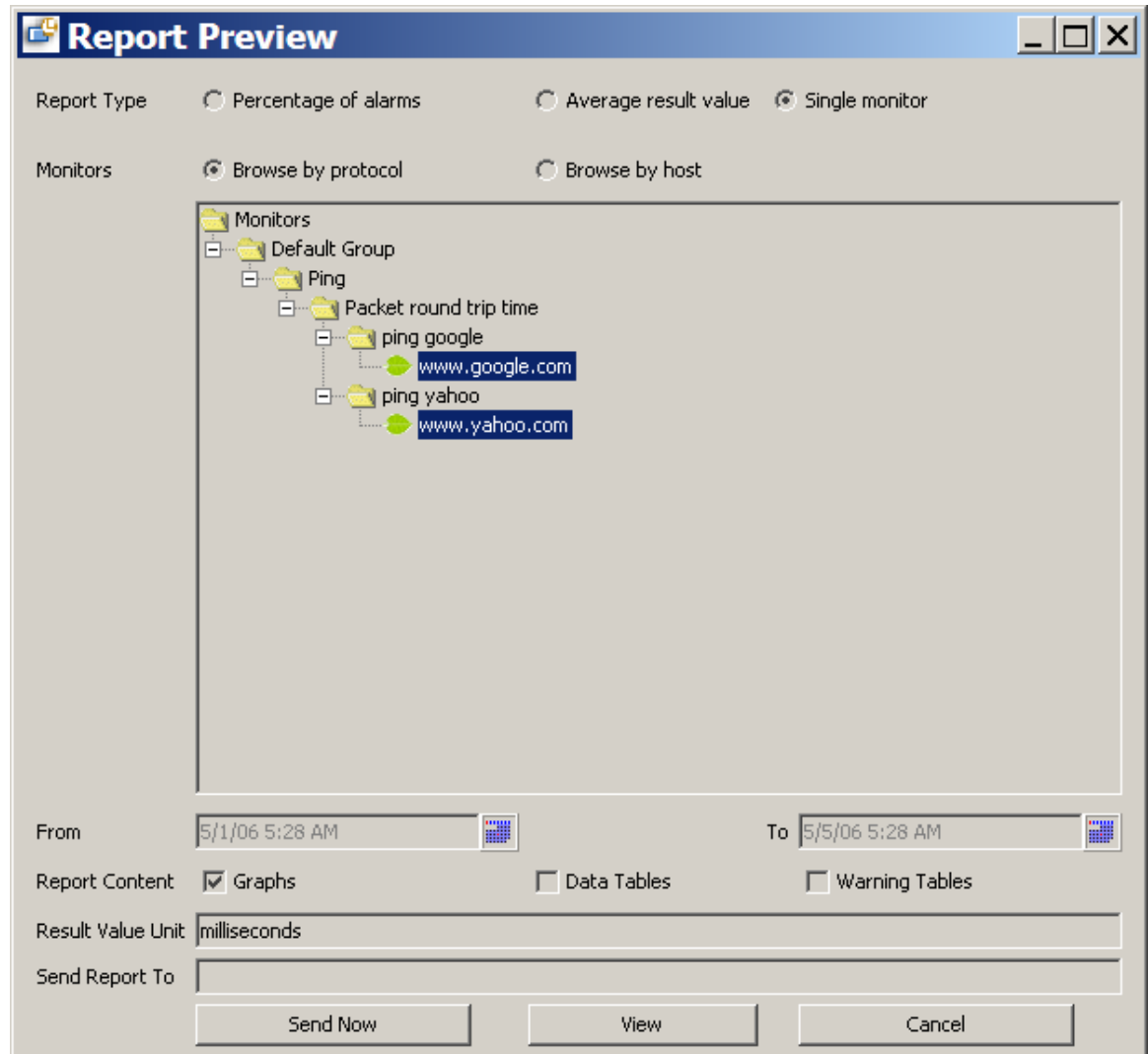
## Top-N Report

The top-N report is a powerful tool that you can use to identify problem elements. A top-N report is a tabular report that lists top N or all monitors sorted by average values or alarm percentage.



If it is categorized by metric, you can select one of the metric types. If all the monitors listed, you can hold down CTRL key and select multiple monitors.

## Monitor Data



This type of report shows the historical data of one or more monitors. You can hold down CTRL key and select multiple metrics.

### Options:

<b>Report Type</b>	Choose top-N report (percentage of alarms or average result values) or monitor data report.
<b>Filter</b>	All monitors or top-N monitors.
<b>From/To</b>	Select the time period of the report
<b>Graphs</b>	Print graph and chart.
<b>Data Tables</b>	Print a table of all collected data.
<b>Warning Tables</b>	Print a table of alarm data.

**Buttons:**

<b>Send Now</b>	Send the report to an email account. SMTP server needs to be configured beforehand.
<b>View</b>	View the report in a new window.

**Scheduled Report**

You can configure scheduled reports that will be generated periodically. If you do not need them, you can pause them or just delete them.

For each scheduled report, you need to specify a title. Report can be generated daily, weekly, monthly or daily (month to date). For weekly or monthly reports, reports will be generated at 00:00.

The generated report will be in PDF format and sent to specified email accounts. SMTP server needs to be configured beforehand.

# Chapter 8. MIB Browser

## The Browser GUI

### Menu

▶ **File menu**

▪ **Load MIB**

Launch a file dialog for picking one or multiple MIB files. You need to hold down CTRL key if you want to select multiple files.

▪ **Exit**

Exit browser.

▶ **Edit menu**

▪ **Find**

Find a node in MIB tree.

▶ **Operations menu**

▪ **Get**

Issue SNMP GET request against current agent.

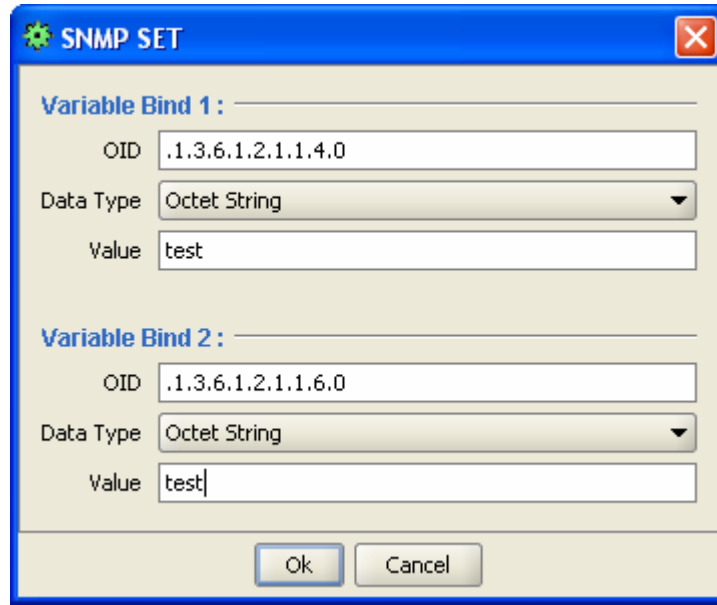
▪ **Get Next**

Issue SNMP GET-NEXT request against current agent.

▪ **Set**

Issue SNMP SET request against current agent.

The following window will show up:



Enter a new value in the "Value" field then click on "Ok" button.

To set multiple variables, you can hold down CTRL key and select multiple rows in the result pane, then choose SET operation.

---

**Note:**

1. For *BITS* data type, you need to use mathematical notation for a set of integers, that is, something like  $\{1, 3, 8\}$ .
2. The format for hexadecimal string is  $(0x[0-9A-Fa-f][0-9A-Fa-f] )+$ . For instance,  $0x12\ 0xA1\ 0x30$

---

- **Get Subtree**

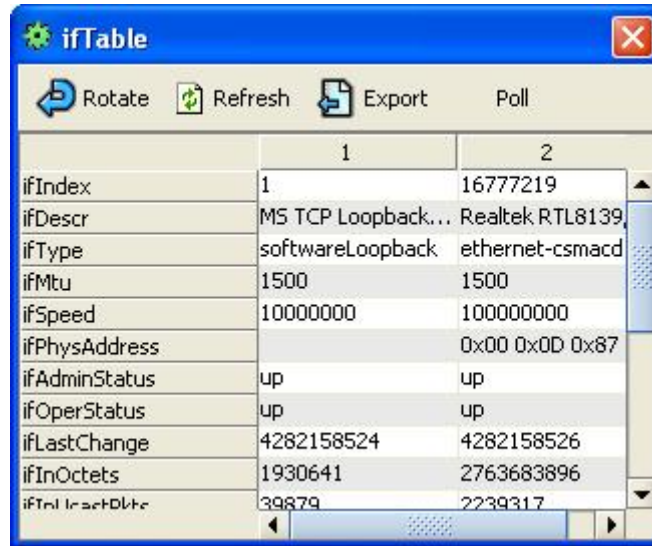
Issue SNMP GET-NEXT requests to get the whole subtree against current agent.

- **Walk**

Do SNMP walk against current agent.

- **Table View**

Open a new window to show MIB table information.



Clicking on this menu item will bring up a new table view window. But first, you need to select a tree node or its sub nodes in the left MIB tree pane.

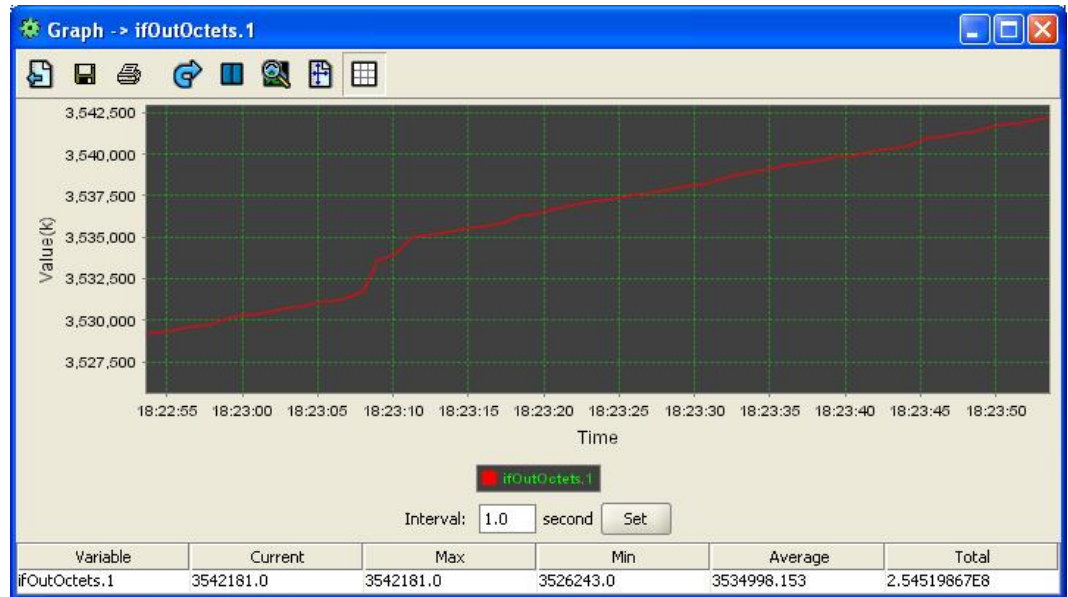
You can hold down CTRL key and select multiple tabular variables of the same table in the left MIB tree pane, then click "Table View". In this way, table view only shows the tabular variables you selected rather than the whole table.

There are four buttons on the toolbar of table view window:

<b>Rotate button</b>	Rotate table 90 degrees
<b>Refresh button</b>	Refresh table now
<b>Export</b>	Export table data to a CSV file
<b>Poll button</b>	Refresh table periodically

- **Graph**

Plot graph for selected OID.



Clicking on this menu item will bring up performance graph window. But first, [OID field](#) needs to be a numerical OID value or table column node whose instances are numerical values. For example, it can be *sysUpTime*, *ifOutOctets*, *ifOutOctets.1*, etc.

Buttons on the toolbar:

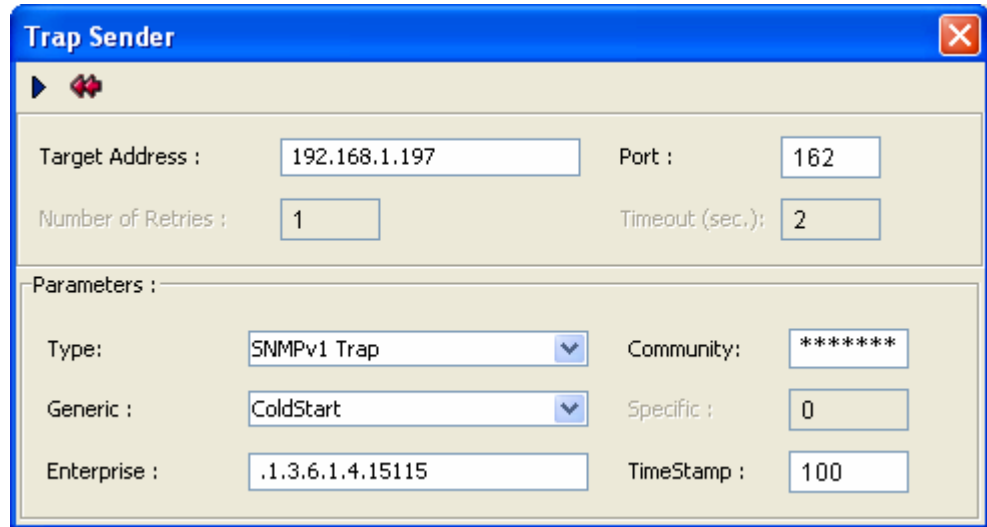
<b>Export to CSV file</b>	Export chart data to a CSV file
<b>Save</b>	Save chart data to a PNG format file
<b>Print</b>	Print out the chart
<b>Restart</b>	Restart plotting chart
<b>Pause</b>	Pause plotting chart
<b>Switch</b>	Switch between current view and global view
<b>Display trace</b>	Display trace lines
<b>Grid</b>	Display grid lines

The polling interval can be changed by clicking on the "Set" button.

#### ► Tools menu

##### ▪ Trap Sender

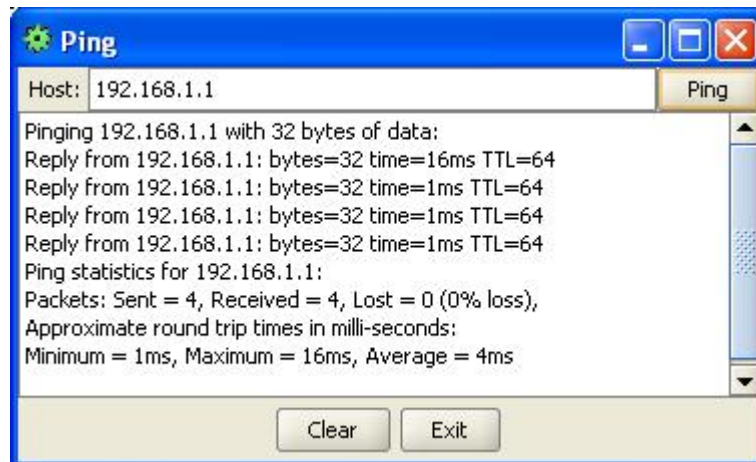
Open trap sender window:



This window allows user to send out SNMPv1/v2c traps.

- **Ping**

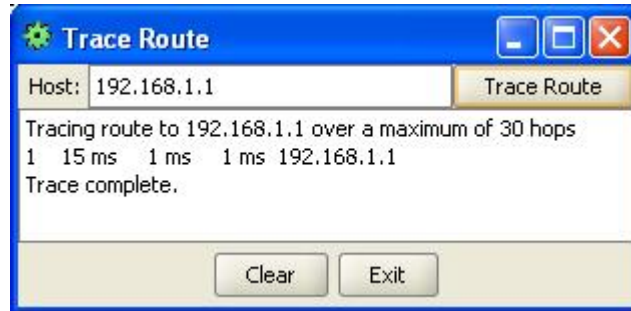
Open ping tool window:



Enter an IP address and press "Ping" button. The results will be displayed in the text area.

- **Trace Route**

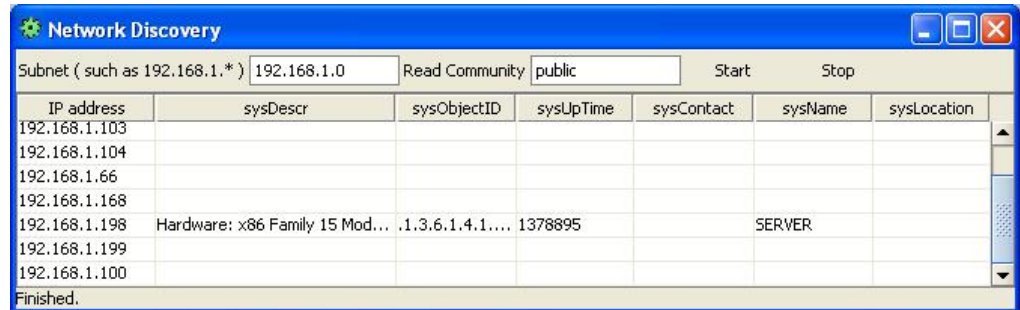
Open traceroute tool window:



Enter an IP address and press "Trace Route" button. The results will be displayed in the text area.

- **Network Discovery**

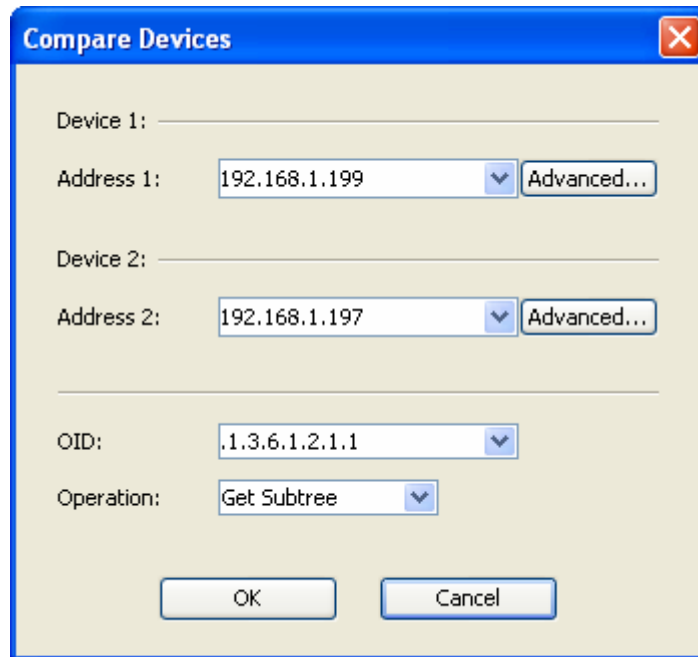
Open LAN discovery tool window:



Enter a subnet IP address such as 192.168.1.0 and then press "Start" button. It can discover all hosts in the subnet. And if SNMP agent is running on a host, its system table will be queried as well.

- **Compare Devices**

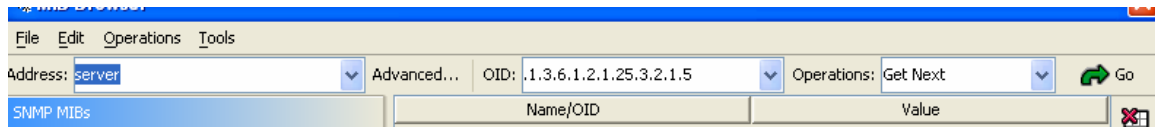
Compare the SNMP values of two devices:



If the values of them are different, the font color is changed to blue:

Name/OID	Value ( 192.168.1.199 )	Value ( 192.168.1.197 )
sysDescr.0	Linux lserver 2.6.9-5.0.3.ELs...	Windows XP (Build Number: ...
sysObjectID.0	.1.3.6.1.4.1.8072.3.2.10	.1.3.6.1.4.1.99.1.1.3.11
sysUpTime.0	2936216	2952313

## Toolbar



- ▶ **Address field**

Enter the IP address and port number of SNMP agent, in the format of "ipAddress@port" or "ipAddress:port" (IPv4 only). The "@port" or ":port" are not necessary if the port number is 161.

- ▶ **Advanced button**

Customize the properties of current SNMP agent, such as community names, SNMPv3 USM parameters, etc.

- ▶ **OID field**



Object identifier to be used for SNMP queries. This field is updated when user select a node in MIB tree or a row in the result table. You can also type new value directly in this field.

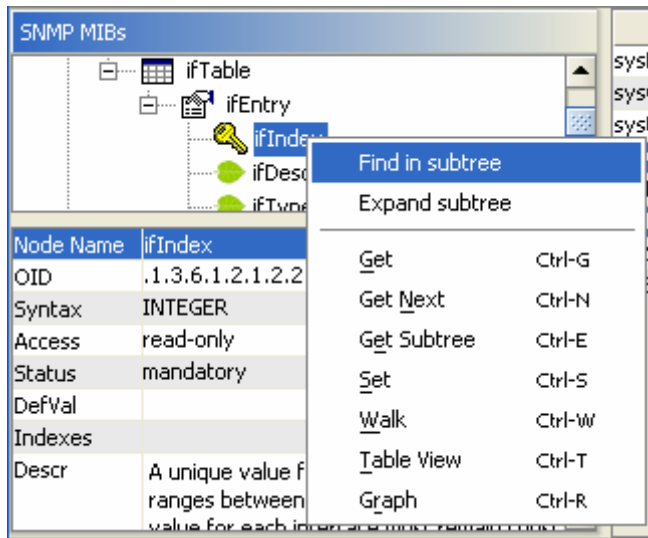
- ▶ **Operations**

Select one of the SNMP operations from the list. Operation will be performed immediately when it is selected.

- ▶ **Go button**

Press this button to perform the selected operation.

## MIB Tree Pane



It is divided into two panes: Tree pane on the top and properties pane on the bottom.

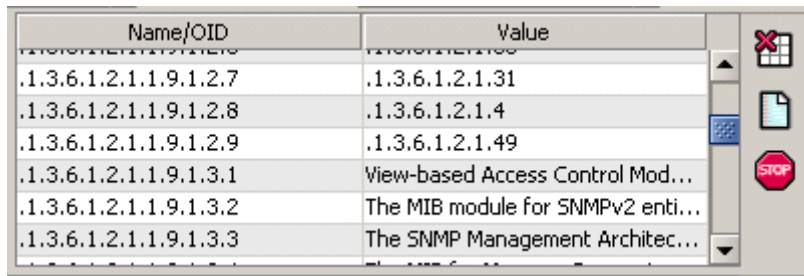
- ▶ **Tree Pane**

Display MIB trees. Right click on a node, a popup menu shows up.

- ▶ **Node Properties Pane**

Display properties of selected node. Tooltips of second column show more information.

## Result Pane



Name/OID	Value
.1.3.6.1.2.1.1.9.1.2.7	.1.3.6.1.2.1.31
.1.3.6.1.2.1.1.9.1.2.8	.1.3.6.1.2.1.4
.1.3.6.1.2.1.1.9.1.2.9	.1.3.6.1.2.1.49
.1.3.6.1.2.1.1.9.1.3.1	View-based Access Control Mod...
.1.3.6.1.2.1.1.9.1.3.2	The MIB module for SNMPv2 enti...
.1.3.6.1.2.1.1.9.1.3.3	The SNMP Management Architec...

Display the result of SNMP queries in a table.

There are three buttons on the right toolbar:

<b>Clear Table button</b>	Clear the result table
<b>Raw Data button</b>	Launch a new dialog window showing the raw results of SNMP queries
<b>Stop button</b>	Stop pending SNMP queries

## Keyboard Shortcuts

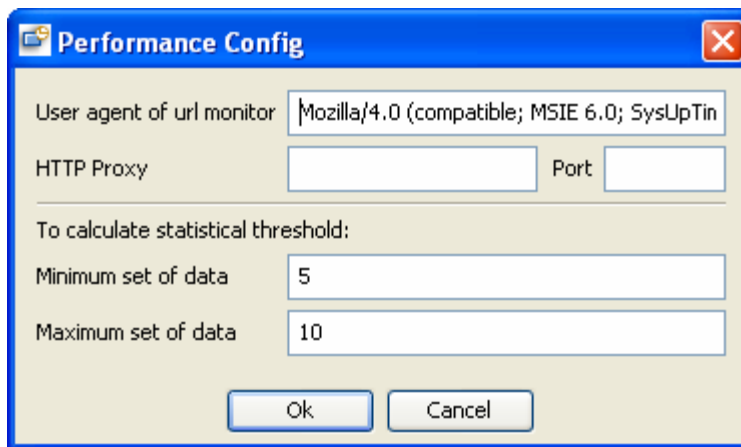
CTRL-F	Find MIB node
CTRL-G	Perform SNMP GET operation
CTRL-N	Perform SNMP GET-NEXT operation
CTRL-E	Perform Get-Subtree operation
CTRL-S	Perform SNMP SET operation
CTRL-W	Perform walk operation
CTRL-D	Compare devices
CTRL-P	Stop current operation
Enter	If Operations or Go button have focus, pressing “Enter” key will repeat last operation.
CTRL-R	Plot graph

## Chapter 9. Configuration

### Check Map Node Status

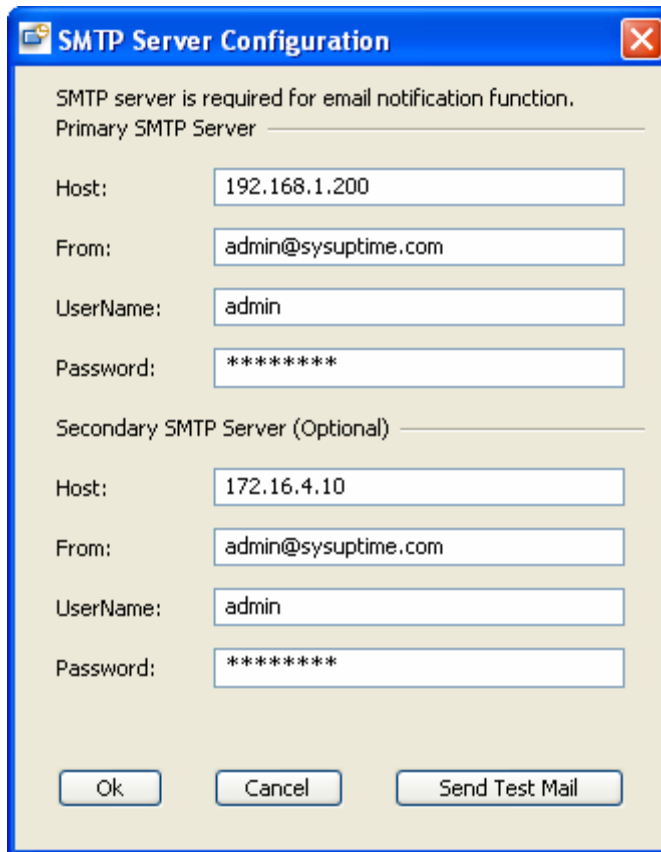
If enabled, there will be a background thread periodically ping nodes in maps. If a map node fails to respond to ping request, its color will be changed to red.

### Performance Configuration



<b>User Agent</b>	The User-Agent field of HTTP(s) requests used in URL sequence monitors
<b>HTTP Proxy</b>	The proxy settings for all URL monitors.
<b>Minimum set of data</b>	Minimum set of data required for calculating statistical values
<b>Maximum set of data</b>	Maximum set of data for calculating statistical values. If maximum is reached, the oldest set of data will be discarded.

## SMTP Server Configuration



The screenshot shows a dialog box titled "SMTP Server Configuration" with a blue title bar and a close button (X) in the top right corner. The main area has a light beige background. At the top, it says "SMTP server is required for email notification function." Below this, there are two sections: "Primary SMTP Server" and "Secondary SMTP Server (Optional)". Each section contains four text input fields: "Host", "From", "UserName", and "Password". The "Primary SMTP Server" fields contain: Host: 192.168.1.200, From: admin@sysuptime.com, UserName: admin, Password: \*\*\*\*\*. The "Secondary SMTP Server (Optional)" fields contain: Host: 172.16.4.10, From: admin@sysuptime.com, UserName: admin, Password: \*\*\*\*\*. At the bottom of the dialog, there are three buttons: "Ok", "Cancel", and "Send Test Mail".

Two SMTP servers can be configured. If primary server fails, secondary server will be used for sending emails. If only primary server is configured, then emails cannot be sent if it fails.

User name and password are required only if SMTP server requires authentication.

After you configure SMTP server, you can press "Send Test Mail" to send a test email.

## Alarm Configuration

### General

#### ❑ Trap Receiver Port

Configure the port number of trap receiver. The default value is 162. Some other applications may already take port 162, so make sure that port 162 is unoccupied otherwise trap receiver cannot be started. If SysUpTime server runs on Linux/Unix platform, make sure SysUpTime server is run in an account with root privilege.

#### ❑ Unknown Traps

Unknown traps mean that they are not defined in “Tools/Configuration/Alarm /Event” panel. You can configure whether to store the unknown traps to database and send them to SysUpTime clients.

Message format is the format of message displayed in the upper panel of alarm browser window. The allowed tokens are listed below:

<b>\$ip</b>	IP address of trap sender.
<b>\$en</b>	Enterprise value.
<b>\$oid</b>	Value of snmpTrapOid.
<b>\$ts</b>	Timestamp.
<b>\$sp</b>	Specific value of SNMPv1 trap.
<b>\$ge</b>	Generic value of SNMPv1 trap.
<b>\$#</b>	Number of variable bindings.
<b>\$vb.n</b>	<i>n</i> th variable binding. For instance, \$vb.1 means the first variable binding in the SNMP variable binding list; \$vb.2 the second variable binding.
<b>\$vb.*</b>	All variable bindings.

*Table: Allowed tokens*

Tokens can be combined. For example, “\$oid, \$vb\*” means showing snmpTrapOid and all variable bindings.

#### ❑ Trap Forwarding

- Forward trap to remote trap receiver  
If checked, traps will be forwarded to remote trap receiver. SNMPv2/v3 traps will be converted to SNMPv1 traps to preserve the IP address of original trap sender.
- Forward trap via email

Each trap will be converted to email and then forwarded to one or more email accounts. Each email account is associated with a time range. So traps can be forwarded to different email accounts based on time.

#### ❑ **Node's Color Change on Traps**

If the IP address of a received trap can be found in the network topology, then the corresponding node will turn red.

## **Event**

It is for configuring SNMP traps and internal events. Traps that are not configured are regarded as unknown traps.

Each event is identified by a unique Object ID. For SNMP traps, event ID is the same as snmpTrapOid. For instance, SNMP cold start is identified by oid .1.3.6.1.6.3.1.1.5.1.

#### ❑ **Add Enterprise**

It's used to categorize events. Each event belongs to an enterprise category. Enterprise has a unique enterprise ID, and a meaningful enterprise name. The IDs of its child events must start with the enterprise ID.

#### ❑ **Modify**

If the selected item is enterprise, clicking "Modify" button will bring up a dialog for modifying enterprise. If the selected item is an event, clicking "Modify" button will bring up a dialog for modifying event.

#### ❑ **Delete**

Delete the selected item.

## New/Modify Event Dialog:

**Modify Event**

Event Name:

Event Identifier:

Mode:

Sources:

Severity:

Forward to Trap Receiver:

Actions (Server Side):

Alarm Sound (Client Side):

Run Command (Client Side):

Message Format:

Description:

<b>Event Name</b>	Name of this event.
<b>Event Identifier</b>	Event ID, starting with enterprise ID(non-editable).
<b>Mode</b>	<ul style="list-style-type: none"> <li>• <b>Store And Display In Category:</b> Store it into database and forward it to client for displaying. You can choose a category from the list.</li> <li>• <b>Store Only:</b> Only store it into database</li> <li>• <b>Ignore:</b> This event will be discarded.</li> </ul>
<b>Sources</b>	IP addresses of the trap originator. Selecting “All Sources” means that we do not check source IP address when identifying this event.
<b>Severity</b>	<ul style="list-style-type: none"> <li>• <b>Fixed</b> One of {normal, warning, minor, major, critical}</li> <li>• <b>Based on Variable Binding</b> Severity is determined by the values of variable binding.</li> </ul>
<b>Forward to Trap Receiver</b>	Specify a remote trap receiver.
<b>Actions (Server Side)</b>	<p>Actions will be triggered on the server side when an event (alarm or rearm) occurs. The following actions are supported:</p> <ul style="list-style-type: none"> <li>• <b>Send Email</b> Send emails based on different time frame</li> <li>• <b>HTTP Action</b> Post to a web site using either GET or POST methods. Form data can be specified for POST method.  Allowed tokens such as \$ip, \$vb.1 can be used in URL. They will be converted to corresponding values.</li> <li>• <b>Run Command</b> Execute a server side command. Allowed tokens such as \$ip, \$vb.1 can be used in command. They will be converted to corresponding values.</li> <li>• <b>Run Remote Command</b> Use SSH/Telnet/RPC to login and then execute a command on remote computer, including Windows and Linux/UNIX machines. Allowed tokens such as</li> </ul>

	<p>\$ip, \$vb.1 can be used in command. They will be converted to corresponding values.</p> <ul style="list-style-type: none"> <li>• <b>Computer Action</b> Reboot/Power off a remote computer, including Windows and Linux/UNIX machines.</li> <li>• <b>Service Action</b> Start/Stop/Restart a service on a remote computer, including Windows and Linux/UNIX machines.</li> <li>• <b>Kill Process Action</b> Kill a running process on a remote computer, including Windows and Linux/UNIX machines.</li> </ul>
<b>Alarm Sound (Client Side)</b>	Play a sound on the client side upon receiving this event. The SysUpTime client must be running and connected to the server.
<b>Message Format</b>	Specify message format. See the “Allowed tokens” table for available tokens.
<b>Run Command (Client Side)</b>	Execute a command on the client side when receiving this event. The SysUpTime client must be running and connected to the server.
<b>Description</b>	Brief description of this event

## Alarm Deduplication

SysUpTime can filter out duplicate alarms. Alarm deduplication function is not enabled by default. If an alarm is considered duplicate in the specified time window, then it will be discarded.

Enable Deduplication

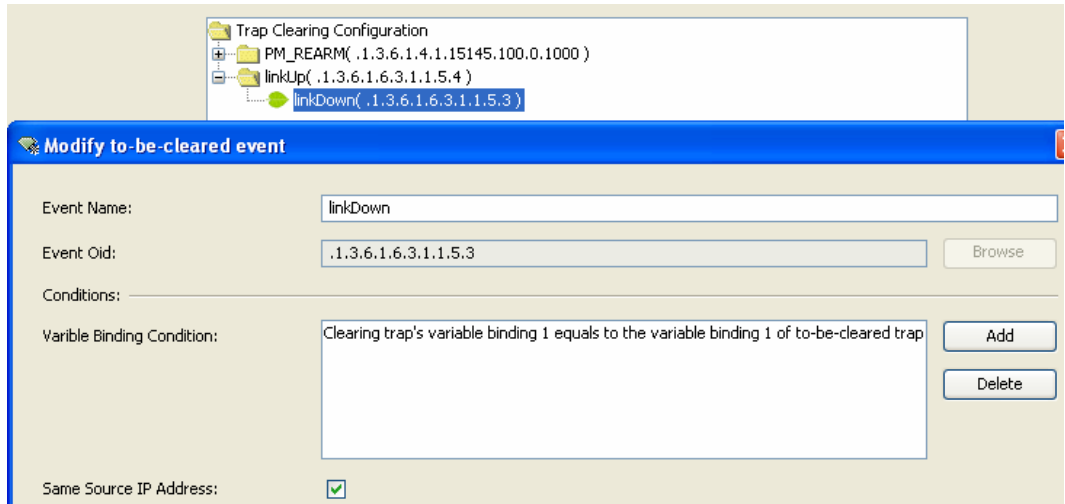
Deduplication Time Window In Second:

Name	Oid	Condition
SNMP cold start	.1.3.6.1.6.3.1.1.5.1	\$ip
SNMP warm start	.1.3.6.1.6.3.1.1.5.2	\$ip
SNMP link down	.1.3.6.1.6.3.1.1.5.3	\$ip,\$vb.1
SNMP link up	.1.3.6.1.6.3.1.1.5.4	\$ip,\$vb.1

Here is an example. In the above figure, the time window is 60 seconds. For the SNMP cold start trap, if trap sender's IP addresses are the same, then it is considered to be duplicate alarms. For instance, if an SNMP cold start trap is received at 10:00:00 AM sent from 172.16.1.90, then any new cold start traps from 172.16.1.90 received before 10:01:00 will be discarded. However, if a new cold start trap from 172.16.1.90 received at 10:01:01, it is not regarded as a duplicate trap.

## Trap Clearing

A trap can be configured to be automatically cleared by other traps.



Here is an example. In the above figure, it defines a linkDown trap can be cleared by a linkUp trap when the following conditions are satisfied:

1. linkUp trap must be received within 60 minutes after linkDown trap is received
2. The first variable binding of linkUp trap (ifIndex) must be equal to the first variable binding of linkDown trap.
3. linkUp trap must be from the same trap source IP address as the linkDown trap

Predefined PM\_REARM section is for automatically clearing internally generated threshold traps. If you do not need this function, you can delete the whole section.

## Alarm Escalation

There may be times when technical personnel are unable to respond to an alarm or simply do not see the alarm. Alarm escalation makes sure that an unanswered alarm can be rerouted to other designated locations. This reduces the risk of a major problem being ignored.

Escalation chain is supported. If an alarm is not cleared within a particular period, one person is contacted, and another person will be contacted if the alarm is still not cleared later, etc.

**Configure Alarms**

General | Event | Deduplication | Alarm Clearing | **Escalation** | SNMPv3 Params

Enable Alarm Escalation

Check trap status every  minutes

Escalation Email Configuration

Time (...)	Severity	Subject	Emails
60	Critical	Alarm not cleared within 1 hour	alarm@sysuptime.com (7*24)
120	Critical	Alarm not cleared with 2 hours	sysadmin@sysuptime.com (7*24)

Add  
Modify  
Delete

Apply

Close

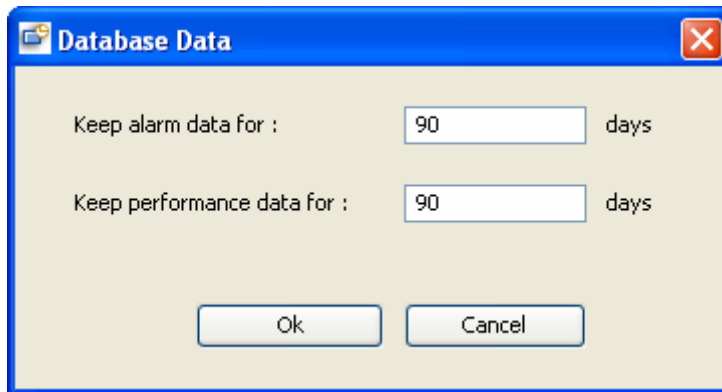
In the above example, it defines the following alarm escalation rule:

If an alarm whose severity is critical, and it is not cleared for one hour, then an escalation email will be sent to alarm@sysuptime.com. If the alarm is not cleared for two hours, an escalation email will be sent to sysadmin@sysuptime.com. You can send escalation email to different email accounts based on time.

## SNMPv3 Params

You need to add SNMPv3 trap senders' properties if you have incoming SNMPv3 traps. There is no need to configure it if there are only SNMPv1/v2c traps.

## Database Data



Keep alarm data for :  days

Keep performance data for :  days

Ok Cancel

It configures how long SNMP trap data and performance data should be kept in database.

## Chapter 10. Tools

### Import HP OpenView Events (*trapd.conf*)

This tool is located at `$INSTALL_DIR\server\bin\import_events.bat`. It is a command line tool for importing your existing HP OpenView's event configuration data into SysUpTime network monitor, so that you do not have to enter them manually.

If you execute it without arguments, the following usage will show up:

*Usage: import\_events.bat eventFileName*

The *eventFileName* is the fully qualified file name of OpenView's event configuration file (*trapd.conf*).

After data is imported into SysUpTime network monitor, you may need to restart the SysUpTime server service.