

Evaluation Guide for SNMPc v7.0

Introduction

Thank you for downloading the SNMPc evaluation, in order to allow you to evaluate the product quickly and easily we have prepared this short guide. The purpose of this evaluation guide is not to describe every feature that SNMPc has to offer, rather to demonstrate some of the key functionality that some of the existing 100,000 SNMPc users have cited as the most useful.

During your evaluation period, please contact us at support@snmp.co.uk with any questions or comments that you may have.

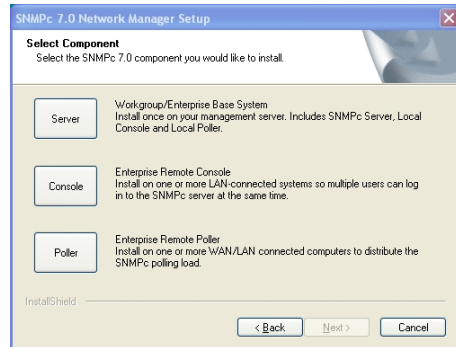
Prerequisites

The evaluation software comprises time limited versions of SNMPc Enterprise and the Remote Access Extension module. More information on the different versions of SNMPc can be found at <http://www.snmp.co.uk/snmpc/index.htm>. This guide assumes that you have at least one SNMP enabled device on your network (preferably a router or a switch) and that you know the IP address of this and your PC.

Installation

When installing the evaluation you will be presented with a choice of the installable SNMPc components. If this is the first time you are installing the evaluation you must select the *Server* option.

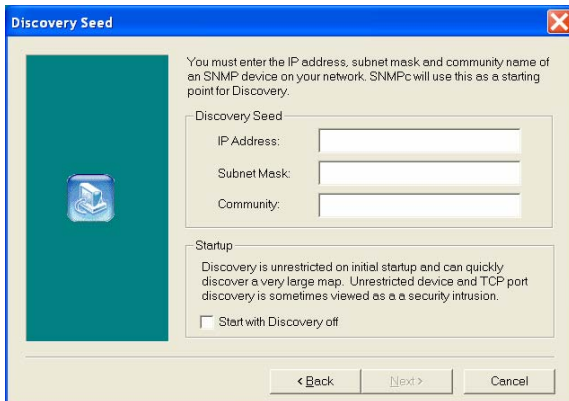
SNMPc Enterprise is a distributed management system. You can subsequently install Remote Consoles or Polling agents on other machines and connect to the central SNMPc server. JAVA consoles are also supported in this evaluation version.



You will then be prompted to configure the network auto-discovery. The Discovery Seed is the starting point for the network discovery. The seed should ideally be the IP address of your local SNMP enabled Router.

After entering the IP address and subnet mask you should enter the SNMP read community for the Router. The default community string for most devices is *public*. The community string is case sensitive.

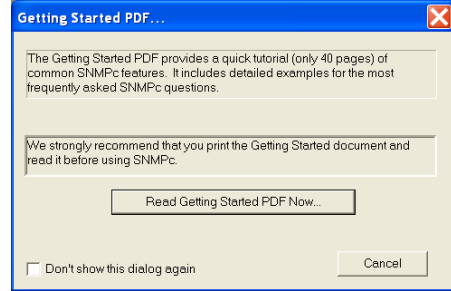
A check box option is provided to disable the network discovery on startup



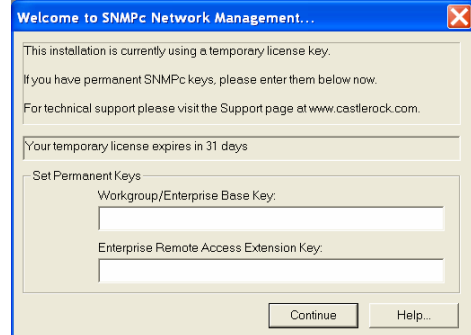
When SNMPc has been installed restart your machine and SNMPc will start automatically. As default SNMPc will be running in application mode. You can subsequently configure SNMPc to run as a Windows service. In the Windows notification area you should see the yellow SNMPc icon.



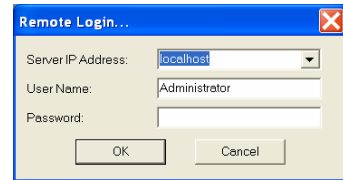
When the SNMPc local console starts you will be prompted to view the Getting Started guide. It is *highly* recommended that you print the guide out and read it during your evaluation period. The guide contains step by step instructions on configuring SNMPc for common tasks such as generating email alerts when devices fail. The Getting Started guide can also be accessed via the *Help* menu.



You are then prompted to enter a license key. No license key is required initially. If you decide to purchase the software you will be provided with a key which will remove the time restriction from the software. All maps and recorded data will be preserved.



You can log in using the default User Name of *Administrator* with no password. Individual users can subsequently be created with differing usernames, passwords and security levels. SNMPc can also be configured so that individual users are presented with their own unique views of the network. This is a useful feature for MSP's and large Enterprise networks.



Unless you selected for the automatic network discovery to be disabled during the install process, on startup SNMPc will discover the network and populate the map with icons. After a short period you will see a screen similar to the following.

Selection Window

Trend Reporting tab

Add Device

Manual Map Editing Toolbar

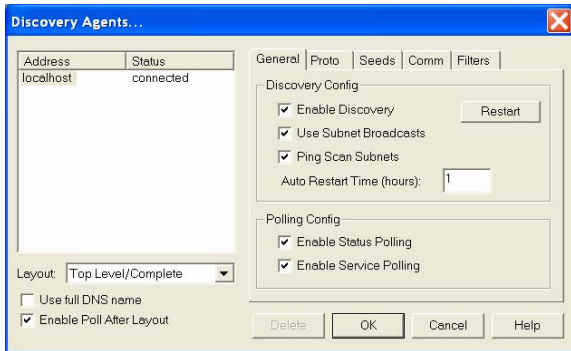
Submap Icon

Event Log

Severity	Date	Time	Device	Message
Normal	04/28/2003	14:44:27	WLAN	Device Responding to Poll
Normal	04/28/2003	14:46:14	www.castlerock.com	Device Responding to Poll
Normal	04/28/2003	14:46:25	www.castlerock.com	Web Service Up
Normal	04/28/2003	14:53:58	cisco	Device Responding to Poll
Normal	04/28/2003	14:54:42	T1 Connection	Device Responding to Poll

The network discovery engine will discover many of the devices in your network. Sometimes though for network auditing it is desirable to be able to force SNMPc to check every IP address within your network.

By selecting *Discovery Agents* from the *Config* menu and checking *Ping Scan Subnets* SNMPc will poll all possible IP addresses within your network range. If you choose to use this feature it is highly recommended that you limit the network search by using *Filters* and that once completed, the *Ping Scan Subnets* feature is disabled.



A complete description of the network-discovery options are contained in the *Getting Started* guide from page 31 onwards. There are also articles on configuring the Network Discovery in the SNMPc Knowledge base. The Knowledge base can be accessed from the *Support* page on the Castle Rock Computing web site (www.castlerock.com)

Configuring the Map


SNMPc arranges devices in a hierarchical layout. Routers are displayed on the top level map with SNMP and TCP/IP devices displayed in IP based submaps. Icons are colored based on their status. Green icons represent devices that are responding to polling requests; red icons are devices that have failed to respond.


Submaps are represented by icons with a hexagon background shape. You can enter a submap by double-clicking on it. Icons can be moved or dragged between maps using the mouse. A detailed description of map editing is covered in the *Getting Started* guide from page 11.

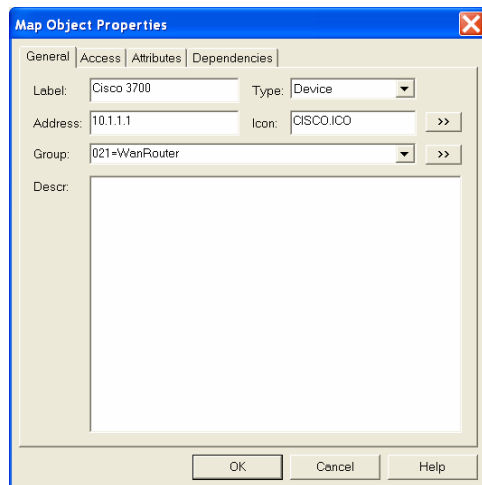
The manual map editing tool bar allows you to individually add devices or submaps. It also allows you to create links between devices or networks. To manually add a device you need to know the address of the device and whether it is SNMP enabled.

Examples of how to manually add devices to the map:


SNMP Router which will open a Telnet session when double-clicked.

Select the 'Add device' icon.  When prompted enter the device *Label* and choose the *Icon* that you wish to use. Set the *Address* to the Routers IP Address. If the Router is using SNMP v1 with a community string of 'public' (most routers will) no changes will need to be made on the *Access* Tab. From the *Attributes* tab change the 'EXEC Program' field from auto.exe to telnet.exe \$a. Select *OK* to add the device to the map.

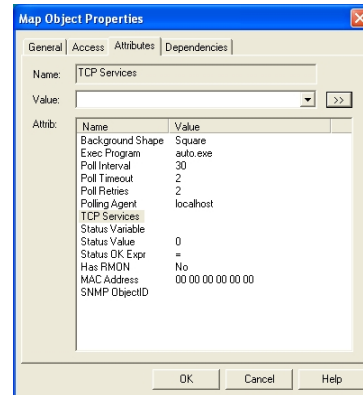
The icon will be placed on the top left of the map. You can create links to other devices or networks by selecting both icons while holding the CTRL key. When both icons are highlighted, use the *Insert Link* icon  to create the connection.



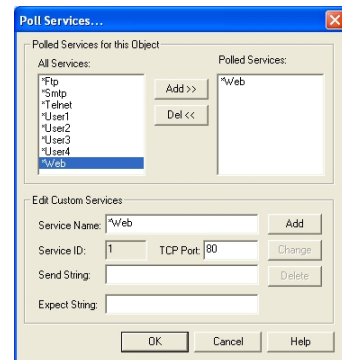
Non SNMP enabled Website which will connect using Internet Explorer when double-clicked

Select the 'Add device' icon.  When prompted choose the device *Label* and *Icon* that you wish to use. Set the *Address* to the web URL (i.e. www.castlerock.com).

Usually SNMP is not enabled on a website server so select the *Access* tab and change the *Read Access Mode* to ICMP Ping. Finally select the *Attributes* Tab and change the *EXEC Program* to *iexplore.exe \$a*. To enable Web service polling highlight *TCP Services* and select *HTTP* from the pull down menu.



For more advanced TCP service polling options double-click *TCP Services* to display the *Poll Services...* window. Using the Send and Expect Strings you can configure SNMPc to monitor the health of an application. More information is available from the SNMPc Knowledge base.



Exec Program Summary

The *Exec Program* field tells SNMPc which program to run when the icon is double-clicked. It is very simple using this field to add support for third party applications.

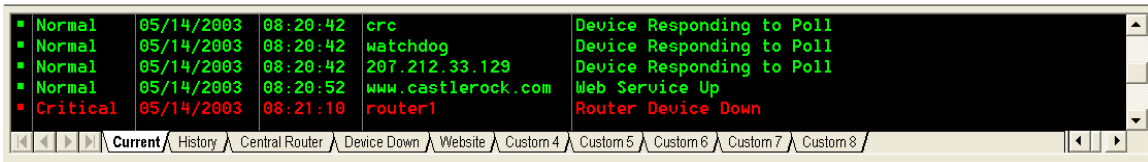
Networking manufacturers such as Cisco, Nortel and Lucent now support web based GUI's for device management. By selecting an icon and editing the *Properties* so that *EXEC Program* is set to *iexplore.exe \$a* SNMPc will browse to that device when double-clicked. Netscape users should set the *Exec Program* field to *'netscp.exe \$a'*.

Common applications such as the WEB browser, Telnet or MIB tool can also be accessed by right clicking on the icon and selecting the appropriate option from the *Tools* menu.

Alerting

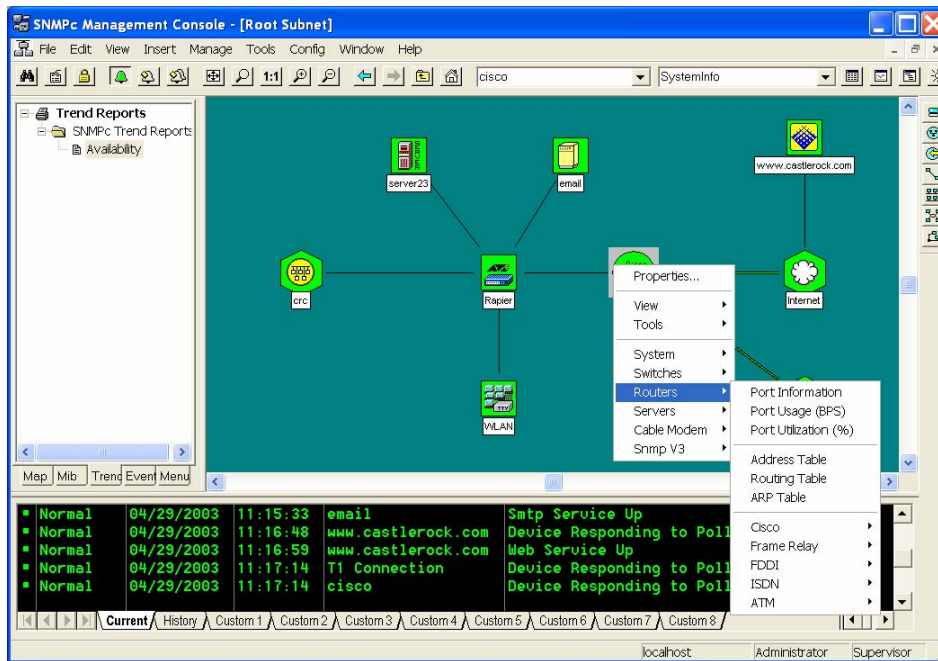
The ability to receive alert notifications before they become user affecting problems is key to moving from fire fighting a network to managing a network. SNMPc is a proactive network management system which can receive and process SNMP alarms from any device regardless of manufacturer. It can also poll any SNMP variable and compare the results against pre-defined thresholds. The inbuilt automatic baselining system monitors polled statistics and generates alerts if unusual data patterns are seen

All network events and alarms are displayed in the Event Log Tool. You can configure the *Custom* tabs to display only events relating to a particular submap or device type. SNMPc also features a 'real language' alarming system which takes complex SNMP alarms and converts them into readily understandable sentences. This aids problem resolution times. All event messages can be customized via a simple GUI so SNMPc can be configured to deliver instructions tailored to the network environment.



When events are received SNMPc can provide a range of notifications including email/cell phone messages, WAV sounds or forwarding alarms to other management systems. A step-by-step guide to generating an email alert when a device fails is contained on page 26 of the *Getting Started* guide.

Device Management



To access the device menu shown above, right-click on an icon. The menu system is organized by device type for easier selection. SNMPc is designed to manage devices regardless of vendor. The only prerequisite is that the device must be SNMP enabled. For example to manage a Windows 2000 Sever you must first have installed the Microsoft SNMP agent.

One of SNMPc's great strengths is its ability to deliver meaningful statistics from raw SNMP data. Octets of data are automatically converted into link utilization or data transferred in bits per second (bps). Disks are monitored in terms of percentage disk space used/free rather than size and number of allocation units.

In addition to the device type menus the *System* menu provides information on network latency and device/application availability. The *SNMP V3* menu provides additional support for devices which implement the secure network management protocol SNMP V3.

Common Menu Selections

Link Utilization

Menu Selection

Switches or Routers/Port Utilization (%)

Index	Descr	InUtil	OutUtil	TotalUtil	ErrorsPercent
1	Serial0	98.163	1.819	99.983	0
2	Ethernet0	0.370	15.302	15.673	0
3	Serial1	0	0	0	0
4	Null0	0	0	0	0

Network Round Trip Delay, Device Availability (%)

Menu Selection

System/Service Stats

(Multiple Devices Selected)

Node	RESP-MS AVG	FAIL% AVG	POLL	WEB	FTP	SMTP	TELNET
email	0	0	UP	UP	unk	UP	unk
cisco	24	0	UP	unk	unk	unk	unk
Repier	9	0	UP	unk	unk	unk	unk
www.castlerock.com	12	0	UP	UP	unk	unk	unk
WLAN	0	0	UP	unk	unk	unk	DOWN
server23	24	0	UP	unk	unk	unk	unk
Firewall	10	0	UP	UP	unk	UP	unk

Server Disk Capacity

Menu Selection

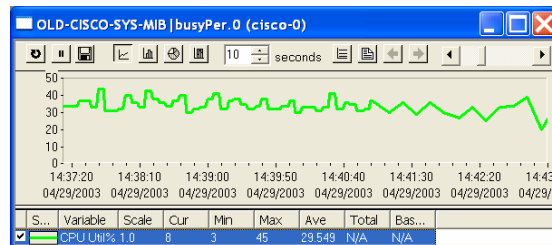
Servers/Disk Drives

StorageIndex	1	2	3
StorageType	hrStorageFixedDisk	hrStorageRemovableDi	hrStor
StorageDescr	C:\	D:\	E:\
BytesTotal	39.983G	0	0
BytesFree	27.132G	0	0
BytesUsed	12.850G	0	0
PercentFree	67.860	0	0
PercentUsed	32.139	0	0

Graph of Cisco CPU

Menu Selection

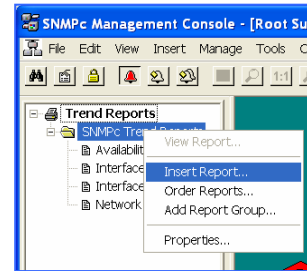
Routers/Cisco/Graph CPU Utilization



All Statistics can be graphed in different formats or viewed in a table. Statistics can also be stored for long term analysis using the trend reporting functionality.

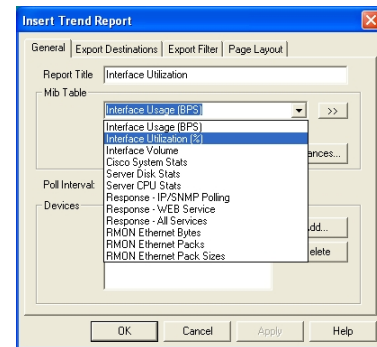
Long Term Statistical Gathering

To create a trend report first highlight the device you want to record the statistics from. Select the *Trend* tab on the bottom of the selection tool (the left-hand pane of the main window). Right-click on the folder named *SNMPC Trend Reports* and select *Insert Report*.



Give your Trend Report a *Report Title*.

SNMPC can record statistics on any SNMP variable but some of the most common reports are available in a drop down list under '*MIB table*'.



Common Report Selections:

Interface Usage (BPS)

Records the data transmitted and received on an interface. The data is measured in bits per second (bps). This is the same measurement that network interfaces are rated by. (56Kbps WAN Link, 100Mbps LAN)

Interface Utilization (%)

Displays data transmitted as a percentage of the total available bandwidth. This report can record statistics on both LAN and WAN interfaces. This report also records the total errors seen on the interface as a percentage of the overall traffic transmitted. Many customers configure SNMPC to generate an alert when traffic rises above 80% of the available link capacity. This alerts them to large data transfers and possible network slowdowns.

Server Disk Stats

Records disk related statistics including total disk capacity and percentage disk space used/free. As with all statistics recorded by SNMPc the system can be configured to automatically generate an alert if disk capacity breaches a preset threshold.

Server CPU Stats

The server CPU utilization expressed as a percentage. By setting a threshold for above 90% Utilization you can be alerted to potential server hangs.

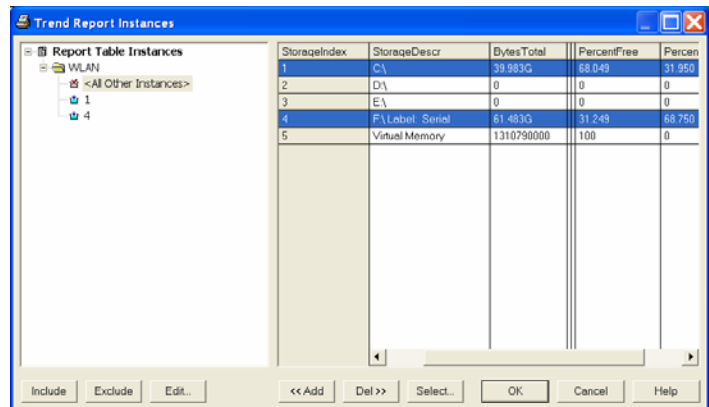
Response - IP/SNMP Polling

Records device or application availability as a percentage. This is useful for SLA reporting. The time taken for a packet to be transmitted between SNMPc and the device is also recorded as a measure of network latency. Using the distributed polling functionality of SNMPc Enterprise the network latency can be measured from strategic points in the network.

If you wish to configure threshold alerts on your Trend Report, choose a subset of interfaces to be recorded or define names for the individual instances you should select the *Instances* button.

By highlighting an instance and choosing *Add* you can select what information will be recorded. If you *Add* individual instances you would normally *Exclude* '<All other Instances>.'

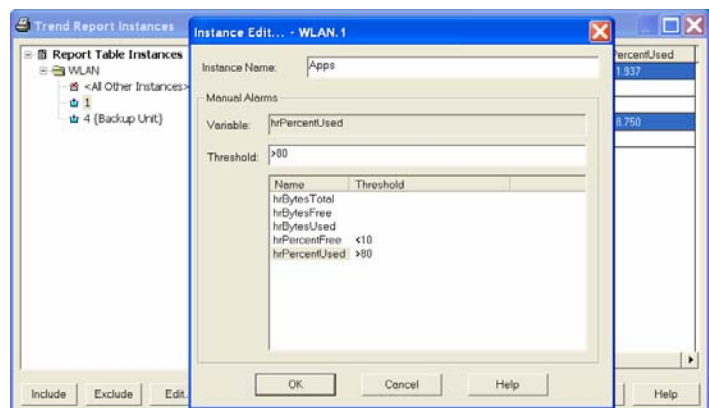
In the pictured Disk Space report we have selected two hard disks to record information on and *Exclude*'d '<All Other Instances>.'



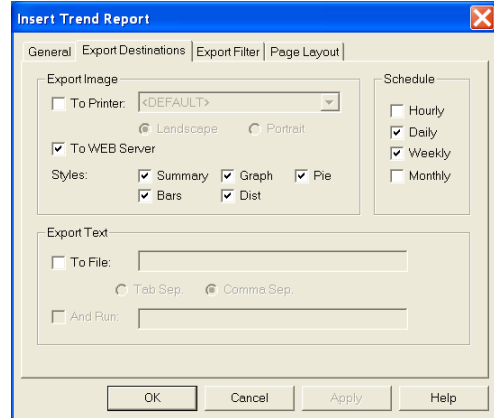
The *Edit* button allows you to define thresholds and the names that will be used in the final report.

In the pictured example we have highlighted instance number '1' and then selected the *Edit* button. The instance has been named and two thresholds have been configured.

One alert will be generated when disk usage goes above 80% capacity and one when disk space falls below 10%. Using SNMPc's event filters you could then create different actions for each event. When the disk space is 80% full SNMP could send an email to the support team. If disk space falls below 10% a page could be sent to your cell phone or pager.



Select OK until you return to the Insert Trend Report configuration screen. Then choose the *Export Destinations* tab. Here you can control how your report is generated. SNMPc Enterprise can automatically produce scheduled hourly, daily, weekly, and monthly reports. Report formats include graph, pie, bar chart, distribution, and summary (table). You can also choose how the data is exported. Reports can be automatically sent to a printer, web server or saved to disk. Using ODBC you can also export recorded data to third party databases.

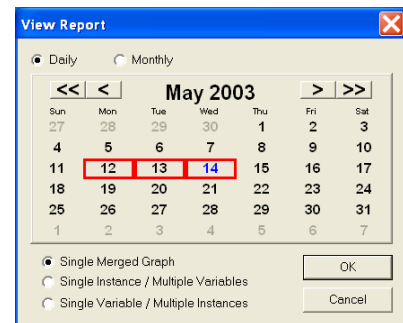


From the *Page Layout* tab you can choose layout options such as axis labels and the position of the Legend.

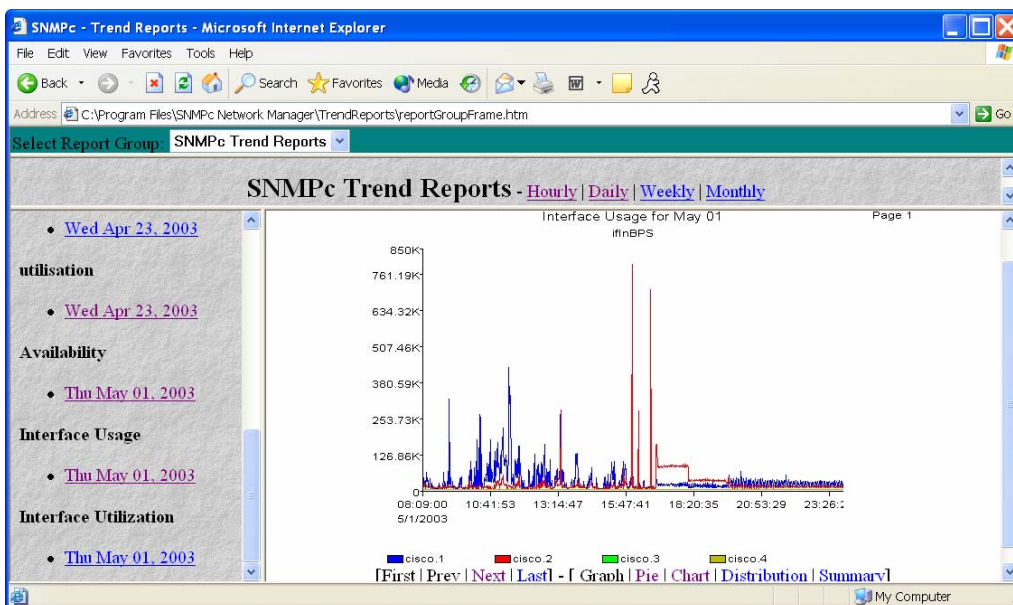
Select *OK* to save your settings and begin the data collection process.

At any time, trend reports can be viewed by right-clicking on the report name in the Trend selection tool and selecting *View Report*. The date range and format of report that you wish to see can then be selected.

Viewing data over long periods of time is invaluable when capacity planning for network growth. The ability to view traffic profiles in hindsight is a powerful aid to problem resolution

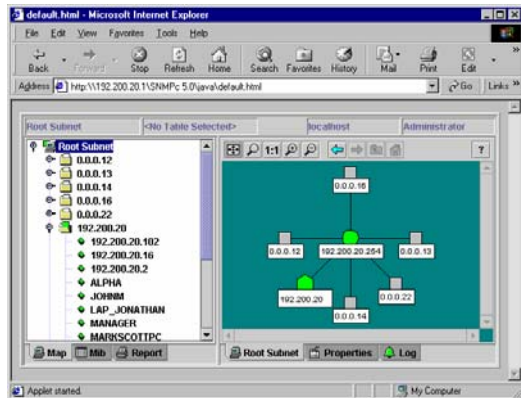


To view Html reports select the '*Web Reports.....*' option from the *Tools* menu. The web report template can only be viewed once the first report has been created.

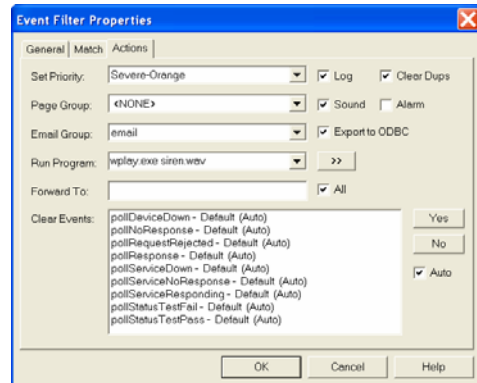


Screenshots from SNMPc

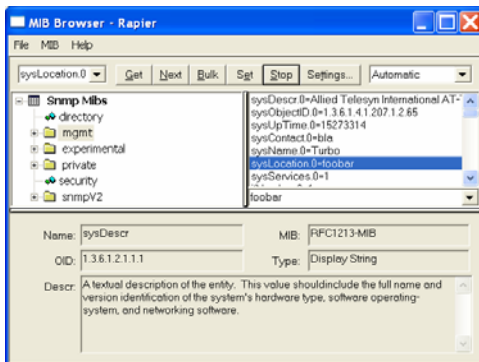
JAVA based Console



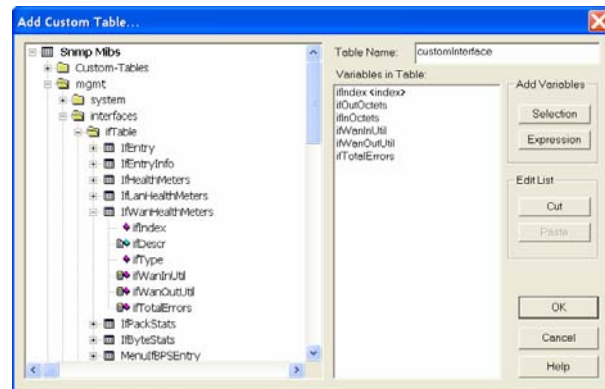
Event Filter



MIB Browser



Custom Tables



Features Summary for SNMPc

1. Monitors SNMP devices, WAN Links, Servers and Applications
2. Distributed Architecture, including JAVA Consoles and Polling Agents
3. Supports SNMP v3 for secure and efficient management
4. Automatic Generation of printed and WEB based trend reports
5. Automatic Traffic Baselining and Alarms
6. Runs as a Windows Service
7. Email/Paging Event Notification
8. TCP Application Polling
9. Live/Standby Server Support
10. Programming Interfaces
11. Custom Menus and Tables
12. OEM Version

Summary

The above guide has attempted to provide you with a very brief overview of SNMPc. Although we have only covered a small subset of SNMPc's capabilities hopefully the key benefits of SNMPc, powerful functionality combined with unparalleled ease of use have been demonstrated. If you have any questions during your evaluation please contact us at sales@snmp.couk