Features and benefits

- Gain total control over your network.
- Know what it is doing and where the trouble spots are.
- Call your users to inform them of a serious problem before they call you!
- Reduce costs and increase network up-time by being able to manage your network more efficiently.
- Better serve your users by being able to provide the exact information they ask for.
- Network monitoring and network management made easy!

Step one: visualize your network.

- The best way of truly understanding how a network functions is to use a network management application that can display a graphical representation of your network.
- Steer clear of management applications that only allow you to monitor network health via lists of detected hardware in your network. These applications only focus on individual devices and do not take the important network relationships into account (further explained in step two).
- Building your network maps as accurately as possible will improve the error tracking process and the speed of solving network problems. It will also help you to locate the trouble spots, and will help you to decide where to add new hardware to introduce fault-tolerance.
Step two: setup alerting and logging.

Before setting up an effective alerting mechanism, consider the following:

- To check the status of a network device, the device must be able to respond to status requests of a management station. Only manageable equipment will respond to polling. If possible, the amount of unmanageable equipment should be limited, as it will create black spots.

- Not all network equipment is of equal importance. Backbone ATM switches are usually much more important - in terms of impact for continuity in case of failure - than for example a terminal server or printer.

  - In general, network managers want to be informed about major network events such as a power failure of a backbone switch or a crash of the corporate mail-server. A non-functioning printer is less important and can wait - especially when alerting is performed via a pager or mobile phone during the weekends.

- Network managers should only be alerted once about the same failure. The management application should be able to evaluate the event stream to pinpoint the root cause of the failure and prevent superfluous and incorrect alerting.

- To provide this level of alerting, use a management application that allows you to assign different priority levels to different types of equipment and one that also includes a suitable error control feature to provide the intelligent alerting.

- A often-encountered negative side-effect of intelligent alerting is that sometimes not only incorrect and superfluous, but also less important events will be hidden. Less important events are events that do not require immediate action but are nevertheless important since they can indicate potential problems. So, pay also attention to these events, enable logging and check them regularly.

Step three: collect historic information for baselining and trending purposes.

- Baselining is a broad term for any analysis method that compares changes in actual data against a baseline. The most common use of baselining is as a tool in performance management for trending analysis - comparing a performance metric to a historical value to find a trend that can be used to estimate future performance or needs. A second use of baselining is for monitoring network health (watching for changes in problem indicators), which is a proactive form of fault management.

- Before you can define thresholds for proactive network problem detection, it is essential to know the normal behavior (baselines) of your network. Determine which information to collect from every different type of device to get a clear picture of its typical behavior.
Keep in mind that the collected data is also to be used later to determine threshold values!

- Collecting historic data also allows you to trace back why and when a problem occurred in the past, and why and when it may happen again in the future!
- Historic information combined with well-defined threshold monitoring are essentials that help you to discover potential problems before they actually occur.

Step four: set up threshold monitoring.

- In general, you can rely on two different approaches to monitor network health, or specifically to monitor the individual devices that form the network.
- Health monitoring by polling usually requires a management application that can read individual SNMP MIB fields of a network device, and can also check these values against known baseline values to determine if there is a potential problem. You can also rely on the trap mechanism, however polling is preferable. If network connectivity is lost, polling will reveal this failure. While a device does send traps when experiencing problems there is no guarantee that a trap will be delivered to the monitoring station in case of serious network troubles.
- The network traffic generated by polling is limited. Depending on your needs you can define polling periods ranging from 1 minute to 1 hour. For example: 1000 threshold data reads based on a 10 minutes time period will result in 2000/600 = 4 frames per second! - Even a 9k6 dial-up line can be used!
- When you start defining thresholds, first concentrate on thresholds that will monitor known problems. If a server is frequently suffering from hanging processes, define a threshold that detects 100% CPU utilization within - for example - a 15 minutes time-period. Define specific thresholds for every different type of equipment and activate them by default. Define thresholds to monitor all or at least the most important - services of the monitored equipment.
- For a file server for example - define thresholds that keep track of free disk space, disk failures, server temperature and network interface error rates, for uninterruptible power supplies define thresholds to trigger power failures and monitor output power load.

Step five: define real-time graphing.

- While collected historic data can tell you how your network will behave and what can be expected of it in terms of performance and reliability, real-time statistics are important for allowing you to perform detailed in-depth analysis.
- To better serve your users you also need real-time tables and graphs, which allow you to immediately respond to basic user requests.
Monitor one allows you to create and save shooters (SNMP request definition-files) to show real-time tables, graphs or Meters. To view these statistics, you only need to execute the appropriate shooter.

- Define essential real-time graphs and tables, and keep them at hand for immediate assistance in case you need them. Before building a new shooter, always ask yourself what type of user question it can help you giving the answer.
- Define shooters that help you answer the most frequently asked questions. Use standards: for every SNMP enabled device, define - for example - at least definition files to retrieve the mib-2 system and ifEntry tables. For routers add also definition files to read the ipRouteEntry table and to graphically display the traffic/load per interface. For application servers create files to show CPU utilization, user sessions, disk usage, buffer usage etc.

The Monitor one functions

Graphical network topology map

- Monitor one lets you create an intuitive multi-level hierarchical network topology map that closely matches your actual network. The maps can be made easier to understand and more attractive by adding geographical maps or floor plans as backgrounds.
- The maps are accessible via the console or via a web browser
- Status information for each device is displayed on the map.
- SnipMons appear as small images just below a device icon on the map. They collect important statistics or performance data from a device through SNMP. They are updated in real-time and are especially useful for having important or critical device information always directly at hand (CPU or interface utilization, Allocated disk space etc).
- The network topology can be discovered semi-automatically. IP address ranges can be defined and scanned for existing nodes. The discovered IP nodes be added to the network maps.
- The maximum number of IP nodes that can be added to the topology map depends on the purchased license type. (L-type = max = 5000)
The monitor one hierarchical multi-level network map. The graphical network map uses colours and icons to indicate network status at a glance. The Map makes it easy to view the IP subnets and the IP hosts. Click the image to enlarge.

**Uptime monitoring**

- Monitor one performs ICMP pings to check up/down status for IP enabled devices.
- If ICMP cannot be used because of a firewall blocking this protocol, Monitor one can also use SNMP data collected from a device to verify up/down status.
- The polling interval for the status checks is configurable per device (10..90 seconds)
- Monitor one performs duplicate alarm suppression. In Monitor one terminology called: "Error control"

Error control (EC) is a powerful feature that helps you quickly locate a problem, prevents superfluous alerting and incorrect interpretation of a problem. Click the image to enlarge.
SNMP monitoring / Network performance monitoring / Network traffic and bandwidth monitoring

- SNMP polling (CPU utilization, traffic load etc) is supported by using Shooters, (request definitions)

- The Shooter feature allows you define which MIB values (SNMP OID's) to query, how to process the retrieved responses and how to display these values. New shooters can be build with just a few mouse-clicks. Shooter definitions are stored in the database and can be executed to poll whatever MIB values.

- For real-time monitoring, retrieved values can be shown in Tables, Graphs (3D), Pies and Meters. The Graphs and Meters are highly customizable (Bar, Area, Line, 3D graphs and old style VDO.

- Monitor one supports SNMPv1 + SNMPv2

- Monitor one allows you to define an alternative port for SNMP polling (not only port 161)

A real-time Graph that shows the load on a switchport. The portnumber is chosen at runtime. Click the image to enlarge.

Besides Graphs, Monitor one can also show real-time SNMP information in Pies, Meters and Tables. Monitor one makes it easy to collect any SNMP information available and display it in the most suitable way. Click the image for more screenshots.

SNMP trap receiver

- Monitor one provides a trap listener with an overload protection system and intelligent filtering capabilities.

  Traps can be filtered/blocked by user defined logic.
Syslog listener/server

- Monitor one provides a Syslog receiver with overload protection system and filtering capabilities.

TFTP listener/server

- Many devices like routers and terminal-servers can use a TFTP server to load their program images. Usually a separate server is used to provide this functionality. This is not a very cost effective solution. Monitor one provides a TFTP server to eliminate the need of a separate server.

Threshold monitoring

- Threshold monitoring with Monitor one is done through the use of "Threshold Shooters". The powerful Shooter mechanism provides the possibility to compare collected SNMP data with user defined threshold values. Monitor one can be configured to send out alerts when values exceed these thresholds. With Threshold Shooters you can easily monitor the interface status of thousands of router- or switch ports, CPU utilization of servers, Free disk-space on servers, power loss on UPS systems etc...
Trending

- For superior trending and long term analysis capabilities, Monitor one can act as a "front end" for RRD. RRD is the Acronym for Round Robin Database.
- Data can be manipulated into reports by exporting it to CSV files that can be imported in a spreadsheet or in a database for further processing.
Monitor one provides a MIB browser and a MIB compiler

The default MIB tree contains about 7000 nodes (OID's) from the most frequently used rfc MIB files.

New MIB files can be added to the MIB tree by using the Monitor one MIB compiler

The MIB tree can be used to build new shooters

A snapshot of the Monitor one MIB tree. This window is the main window for creating and modifying Shooters. Click the image to enlarge.

Event logging

- Event details are stored to the so called Monitor one "Logbook". The logbook content can be accessed by using the Monitor one logbook viewer or can easily be exported to a CSV file for use in a spreadsheet or database.

Alerting

- Monitor one can send alerts for the following events: Status events ('No response, 'Responding again', 'Status unknown'), Threshold events ('Threshold exceeded', 'Under threshold value'), Trap received events, Sensitivity events, Syslog message received events.

- Alerting can be accomplished by any of the following methods: Audible alerting (beeping or speech), Visual alerting (flashing lights), alerting by email, alerting via SMS, pager or cell phone. Alerts can also trigger the execution of a program or script.

- In order to prevent superfluous alerting, the decision whether or not to alert is determined by the so called "Alerter". The alerting scheme is highly customizable and the decision is based on the priority level of the device causing the alert and the event severity.
Extensive Monitoring

- Extensive monitoring is a powerful feature that is able to scan enterprise networks for bad interfaces, auto-sensing problems on switch-ports, poor performing WAN links etc.