Nimsoft for Network Monitoring

A Nimsoft Service Level Management Solution White Paper
Nimsoft for Network Monitoring

Table of Contents

Nimsoft for Network Monitoring – Solution Summary .............................................................. 3

Solution Overview .............................................................................................................................. 3

Nimsoft for Network Monitoring – Specialized Probes ................................................................. 3

Network and Application Connectivity Probe ................................................................................ 3
  Connectivity Monitoring – Broad Device and Services Support ..................................................... 3
  Connectivity Response Time Measurement – Network Latency Monitoring ................................... 4
  Connectivity Device Configuration – Drag-And-Drop List Setup .................................................. 4
  Connectivity Path Configuration – Building Device Relationships with Traceroute ....................... 4
  Connectivity Failures – Root Cause Analysis .............................................................................. 5
  Connectivity Probe – Flexible Deployment .................................................................................... 5
  Connectivity Probe – Flexible, Reliable Notification .................................................................... 5
  Connectivity Probe – “Profile-based” Polling Configuration .......................................................... 5

Interface Traffic Probe .................................................................................................................... 5
  Interface Auto-Discovery .............................................................................................................. 5
  Interface Status and Bandwidth Calculation .................................................................................. 6

SNMP Poller and Trap Listener Probes .......................................................................................... 7
  SNMP MIB Poller and Browser ...................................................................................................... 7
  SNMP Trap Receiver ...................................................................................................................... 7
  SNMP Trap Sniffer .......................................................................................................................... 7

Nimsoft for Network Monitoring – Specialized Gateways ............................................................ 7
  Third-party Network Management System SNMP Gateway ........................................................... 7
  Syslog Gateway ............................................................................................................................. 7

Nimsoft for Network Monitoring – Real time Alarm Console ......................................................... 8

Nimsoft for Network Monitoring – Performance Trend Reporting ............................................... 9

Nimsoft for Network Monitoring – SLA Creation, Monitoring and Reporting ............................... 10

About Nimsoft ................................................................................................................................ 10
Nimsoft for Network Monitoring

Nimsoft for Network Monitoring – Solution Summary

The Nimsoft for Network Monitoring solution verifies network connectivity to devices and application services revealing accessibility and network latency. The solution auto-discovers network interfaces, monitors interface traffic and calculates bandwidth utilization. Interface variables are polled for status data and the solution receives unsolicited SNMP traps. Syslog monitoring is supported for non-SNMP devices. Status data is analyzed and displayed in graphical alarm consoles, performance reports and SLA reports.

Solution Overview

The Nimsoft for Network Monitoring solution provides complete network visibility to assure that the highest levels of business service quality are achieved. Having 360° network visibility is critical to today’s network driven business and anything less can have costly bottom line implications.

Nimsoft for Network Monitoring Primary Features

- Monitors access and response time to all network devices, application and service ports
- Monitors interface traffic for bandwidth utilization and error status
- Monitors SNMP enabled devices with polling and trap reception
- Monitors device Syslogs
- Graphical alarm console, performance and SLA reporting

The Nimsoft for Network Monitoring solution detects, isolates and accelerates resolution of:

- Broken network and application connectivity links
- Excessive network latency
- Network device degradation and failure
- Network interface degradation and failure
- Excessive bandwidth utilization
Nimsoft for Network Monitoring – Specialized Probes

The Nimsoft for Network Monitoring solution is comprised of a set of specialized probes and gateways, which provide automated and GUI driven access to device status information. All solution probes have their own graphic interface to facilitate Administrative and Operations activities.

Network and Application Connectivity Probe

To assure business continuity, the Nimsoft for Network Monitoring solution provides a robust network and application connectivity monitoring function. This ensures that end-users and business consumers have access to business critical network devices, services and applications.

Connectivity Monitoring – Broad Device and Services Support

The solution includes connectivity monitoring for network devices such as routers, switches, servers, applications, printers and practically any other device. A specialized probe uses the ping command (ICMP ECHO) to verify network connectivity between the host where the probe resides and the targeted remote system. The probe will also test connectivity to TCP based services such as telnet, http, etc., or any other application with a designated service port.
Connectivity Response Time Measurement – Network Latency Monitoring

Through the process of connectivity monitoring, the network connectivity probe will record response times to and from network devices, services and applications to aid in pinpointing areas of excessive network latency. Network connectivity status reports and round trip performance trend reports are available. Report data can be leveraged for SLA creation, monitoring and reporting.

Connectivity Device Configuration – Drag-And-Drop List Setup

To simplify setup of network devices requiring connectivity monitoring, the probe supports a drag and drop IP list feature, for example a /etc/hosts file can be dropped into the probe GUI for automatic device population. The probe's GUI also offers an intuitive interface for manually adding new devices, applications and services. At any point during the configuration of new devices and services, it is possible to test connectivity by selecting the GUI-driven connectivity 'status' test button. The results of this test will appear in a pop up window (as depicted in the figure above). All devices and services will be listed with a color-coded connectivity status icon in the left most column.

Connectivity Path Configuration – Building Device Relationships with Traceroute

The network connectivity probe provides a trace route function to determine and diagnose connectivity paths. A simple push of the button will list the network hops required to reach a destination device. This facility is extremely useful for building network and application dependency paths and tree structure, which can then be leveraged for identifying the root cause of connectivity failures and identifying impacted devices. The probe's GUI supports a drag and drop function, whereby it is possible to drag and drop trace route results into the probe's GUI to automatically build ping poll path dependencies. Common network elements resulting from multiple trace routes will be overlaid on top of existing path definitions. This will create a proper path and network tree structure with shared routes and separate network segments branching out accordingly.

Connectivity Failures – Root Cause Analysis

For determining the root cause of network and application connectivity failures, the connectivity probe will reference the network tree resulting from the trace route functionality. Once the root cause of a connectivity failure is determined, the connectivity probe will automatically suppress ping fail alerts for devices and applications beyond the broken network link. Only the alert for the root cause device will display in the Nimsoft Alarm Console. To facilitate problem diagnosis and path validation, the network connectivity probe provides a graphic interface containing a listing of all connectivity paths that are being monitored. Additionally, where path connectivity is broken, the probe will indicate root cause and symptom devices with color-coded status indicators. An example screen shot which depicts this functionality is listed above.

Connectivity Probe – Flexible Deployment

The Nimsoft for Network Monitoring solution offers extremely flexible deployment options to ensure connectivity testing is being performed to and from applications and network devices that warrant close scrutiny. Unlike other market offerings, which only support centralized polling from a management server, the lightweight network connectivity probe can be deployed strategically throughout the business infrastructure. For example, in a distributed application environment, the network connectivity probe can be deployed directly on application servers and configured to test connectivity to the end-users who need access to those business critical servers. Conversely, it is possible to deploy the network connectivity probe directly on end-user workstations to monitor for connectivity to the applications servers that the user-community need access to. Businesses with branch offices may consider deploying the network connectivity probe on edge devices to monitor link connectivity between the IT data center and the branch offices.
Connectivity Probe – Flexible, Reliable Notification

The Nimsoft for Network Monitoring solution provides flexible and reliable alert notification and data transport options. In cases where the network link between the probe and Nimsoft management console is disabled, the probe will buffer alert and performance data locally until a failed network connection has been resolved. More interesting, the connectivity probe supports cellular communications for off-network alert notification and performance data transmission. This feature will remove reliance upon a potentially broken network for data transport.

Connectivity Probe – “Profile-based” Polling Configuration

Understanding that each network device may require unique polling and alert generation requirements, the Nimsoft for Network Monitoring solution supports flexible “profile-based” monitoring configuration. Every probe within the Nimsoft for Network Monitoring solution can have multiple profiles, each having their own monitoring definitions. Profiles will define unique polling intervals, alert severities for problem conditions, unique alerts messages, and more. Each profile contained within the probe can be comprised of single or multiple polled devices.

Network connectivity and round-trip performance trend reports are available. The probe will record connectivity test results and round-trip sample data for availability and performance trend reports.

Interface Traffic Probe

Due to the complexity and rapid expansion of network intensive applications that are being deployed across today’s business infrastructures, there is a need to understand the capacity of circuits and traffic flow across critical network interfaces.

Interface Auto-Discovery

The Nimsoft for Network Monitoring solution will auto-discover all device interfaces. Once discovered, the solution will monitor interface traffic and perform bandwidth utilization calculations. Additionally, each device interface will be scrutinized for error conditions that may degrade data throughput performance.

Interface Status and Bandwidth Calculation

A specialized probe utilizes SNMP to measure and report on inbound, outbound and aggregate bandwidth utilization. MIB objects are queried and analyzed both in real time and over time for alert generation and bandwidth utilization trend reporting. The probe may be configured to monitor the network interfaces on PCs, Windows and Unix Servers, routers, switches, and other SNMP enabled devices. The probe monitors and reports on the following interface parameters:

- "Dead" lines (no traffic)
- Discarded packets
- Error packets
- Queue length
- Interface status
- Average traffic in/out
- Average errors in/out
To minimize management traffic on the network, the interface traffic probe can be placed strategically throughout the network in locations that are in close proximity to the managed devices.

The solution provides “profile-based” monitoring where each interface can be configured to poll unique data variables at defined polling intervals, alert severities and messages are also defined per profile.

### SNMP Poller and Trap Listener Probes

#### SNMP MIB Poller and Browser

The Nimsoft for Network Monitoring solution provides a specialized probe that can poll any standard or proprietary MIB object from any SNMP compliant device. MIB objects can be monitored for threshold violations and alerts can be generated where necessary. Additionally the polled MIB data can be archived for trend reporting and also leveraged for SLA creation, monitoring and reporting. The probe offers a flexible interface for configuring unique MIB object poll requirements and also comes equipped with a MIB browser.

#### SNMP Trap Receiver

Network devices, such as routers, switches, servers and printers, which are SNMP enabled, can be configured to report a variety of error-conditions in the form of SNMP ‘traps.’ Traps are automatically forwarded to a designated server – typically a network management server.
The Nimsoft for Network Monitoring solution comes equipped with a specialized SNMP trap receiver probe. It will listen to port 162 (default, but is re-configurable) and any incoming SNMP traps will be converted to Nimsoft formatted events. The formatted events will then be analyzed for alert generation or archived for trend reporting. The trap receiver probe offers an intuitive GUI to convert the SNMP traps to user-friendly alert messages. Out-of-the-box support is available for COMPAQ Insight Manager and Dell Open Manage traps.

**SNMP Trap Sniffer**

The SNMP trap receiver probe (described above) also provides a real-time trap ‘sniffer’ function. The probe watches the network in promiscuous mode to see all SNMP traps on the network wire. The probe’s graphic user interface displays all traps in an active scrolling list as they are detected. Pressing the ‘start’ button in the probe’s interface easily activates the sniffer function. A green diode indicates that “sniffing” is in progress. Individual traps that are “sniffed” can be selected and quickly added into the Nimsoft event monitoring system. Each trap that is selected through the probe’s graphic interface will have its own monitoring profile automatically defined. The monitoring profile dictates how SNMP traps should be processed when they arrive in the Nimsoft system. SNMP event messages can be restructured and event counts, alert thresholds, and alert severity can also be defined.

**Nimsoft for Network Monitoring – Specialized Gateways**

**Third-party Network Management System SNMP Gateway**

The Nimsoft for Network Monitoring solution provides an SNMP Gateway that will transform Nimsoft alarm messages to SNMP trap messages that are readable by any SNMP based event manager. Predefined SNMP Gateway solutions are available for HP OpenView Network Node Manager, CA Unicenter-TNG and BMC Patrol Enterprise Manager (PEM).

**Syslog Gateway**

Device Syslogs are a critical source of network status information. This is especially true for non-SNMP enabled devices. The Nimsoft for Network Monitoring Syslog Gateway acts as a gateway from the Syslog “world” into Nimsoft. Most network-devices, such as routers, switches, firewalls, UNIX servers, etc., report events using SNMP as well as using the well-known Syslog format. The Syslog Gateway will listen to port 514/udp when running in a receive mode. All incoming Syslog messages will be acted upon using the defined receive mode:

- Generate Nimsoft Alarm
- Generate SYSLOG-IN (for post-processing) messages
- Log to file

The Syslog Gateway also includes a graphical Syslog viewer to view messages as they occur.
Nimsoft for Network Monitoring – Real time Alarm Console

The Nimsoft for Network Monitoring solution offers a web-based Nimsoft Alarm Console. The Nimsoft Alarm Console can be applied to create and customize user specific network monitoring “dashboards.” Alarm dashboards can show up-to-the-minute status of critical network links, bandwidth utilization, network latency, response times and other critical network issues. Below is a small sampling of network specific Nimsoft Alarm Console features:

- Network and application alerts can be viewed in realtime
- Network device auto-layout and drag and drop host lists for device auto-population
- Layered views for application drill down through to underlying network devices and interfaces
- Configurable Operations drop-down menu lists – this functionality can provide point-and-click context sensitive access to third-party diagnostic tools
Nimsoft for Network Monitoring – Performance Trend Reporting

Nimsoft for Network Monitoring solution offers a robust performance reporting solution that will allow businesses to track and trend network availability and performance parameters such as network interface utilization, error rates, connectivity failures, latency and any other technical items from a Service Level perspective. All network availability and performance data collected by the Nimsoft for Network Monitoring probes can be utilized for Quality of Service and Performance report generation.
Nimsoft for Network Monitoring – SLA Creation, Monitoring and Reporting

The Nimsoft for Network Monitoring Solution offers a robust SLA creation, monitoring and reporting solution. Quality of Service and performance data collected by the Nimsoft for Network Monitoring probes can be leveraged to calculate and report on service level compliance and breaches. All SLA and performance reports are viewable in HTML format via web-browser.
About Nimsoft

Nimsoft provides integrated, modern IT management solutions for more than 1000 enterprise and service provider customers globally, including 1&1, CDW, SoftLayer, Sur La Table, TriNet, and Virgin America. The company’s Nimsoft Unified Manager is an industry-leading solution which helps organizations easily monitor and manage IT services in increasingly complex business environments. Nimsoft products integrate with existing solutions at any point from the data center to the cloud. For more information, visit www.nimsoft.com.