



MANAGED NETWORK SERVICES

Sify Beacon™

JAN 2023

General			
Description	This document will serve as the product description for Sify's in-house NMS Tool - Beacon™.		
Version	7.0		
Document Owner	Rahul Nair	Saurabh Kumar Acharya	Melvin Varghese
Approved By	Suresh Gummaraju		
Effective Date	1 st January 2023		

Sify's In-house NMS: Beacon™

Beacon™ is one such tool, which is born out of Sify's quest of continued adoption of industry-standard practices and tools. It is Sify's in-house developed, comprehensive network management solution (NMS). Beacon™ provides an expertise driven approach that combines best-in-class network management software with process know-how and training.

1.1. Architecture

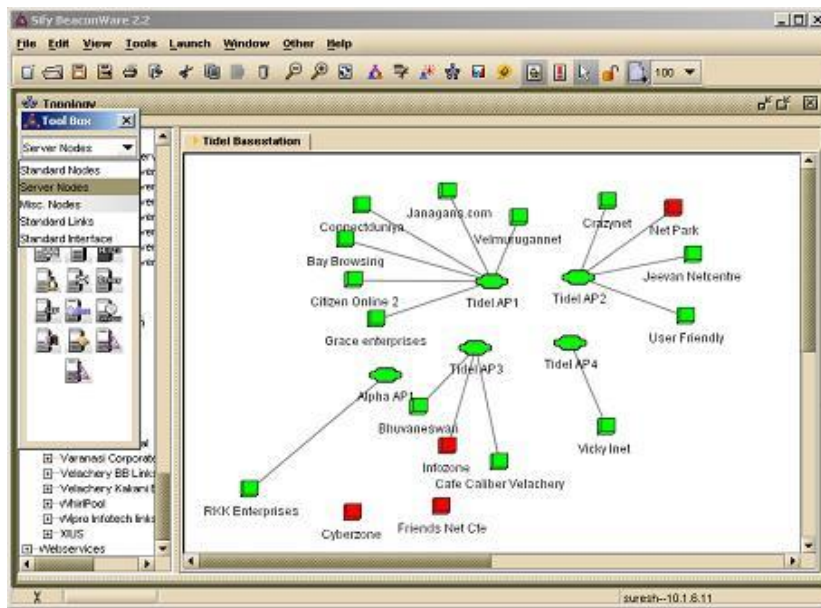
The NMS consists of the following modules:

- NMS Station
- NMS Data Poller
- NMS Database
- NMS Client
- NMS Web Server

The NMS Station is an NMS server, which acts as the nerve center for the entire network management system. It houses the database also. NMS Data Pollers, installed at various optimal points of the network, are responsible for checking the health and performance of a set of devices, links and applications and reporting this back to the NMS Station. The decision to install the number of Pollers is a function of the number of devices being monitored and the reachability of the devices from the central location. NMS clients will enable remote access to the NMS server for configuration, administration and for monitoring real time the state of the network. The Client part of the software can be installed at each of the locations and is used to view the state of the network.

1.2. Auto-Discovery

Once installed, NMS will setup your network map. It will automatically discover all network devices, links, and associated interfaces. These are then mapped diagrammatically as a topology. The discovery can be for a range of IPs or for specific IP addresses. The discovery mechanism does an SNMP walk and ping sweep of the entire network. The utility also classifies the discovered devices and application according to name and type. This utility comes of great use when configuring a complex network for monitoring. This facility of Auto-discovery can be used to map out all the devices to be monitored in the network without any effort. Auto-discovery process also grabs the details of the various ports of the devices and the details linked to the same.



1.3. Topology Maps

Multiple topologies consisting of resources and their linkages can be setup in the system for reducing the visual complexity of the network. A background image can also be setup to provide a geographical basis for the network map. Drill down topology is possible. Herein the top-level topology can be mapped out and then hyper linked to the detailed topology, which forms the downstream part of the network. This results in easy manageability. Visual alerts can be seen on these graphical views so that topologies having error conditions stand out to the network manager. A single device can belong to multiple topologies thus clearly indicating to the manager how degradation in its performance affects different sets of resource groups.

1.4. Fault Management

At any point of time the complete network can be viewed through the Topology Browser. The status of all the network elements and links are displayed on the network map itself enabling the network administrator to easily identify problem areas and take steps to solve them.

NMS has a sophisticated Fault Management system designed to ensure high network availability and minimize outage. Each device on the network can be assigned thresholds, which define the standards for normal operation. Data Pollers strategically positioned at various points of the network continuously monitor these devices on the parameters defined. If any of the parameters exceed a threshold, an alert is generated.

Further for easy usability the Event Viewer, which is a dynamic log of all activities in the network, is linked to the Topology. Thus, when viewing a topology the Event Viewer for that topology at the bottom of the screen gives online status of the network. Also, when while in the event viewer, the user can automatically move the specific device in the specific topology by choosing the option on right click. The Event Viewer also provides quick short cuts to Quick Status, Instant Poll, Locating Duplicates, and Ping etc. for access maneuverability. Apart from this, it also offers an option to Detect Links from the associated device, which is useful for plotting and discovering the network.

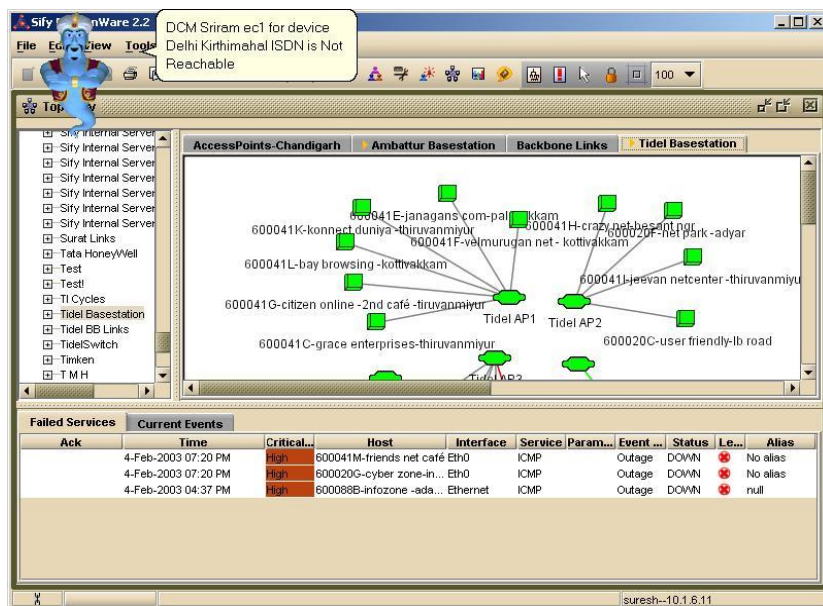
1.5. Trouble Ticketing

All alerts can be automatically recorded in the form of a trouble ticket and the ticket can be assigned to the appropriate team to work on. When an alert is shown in the NMS the monitoring operator can either manually raise a trouble ticket in one click on the monitoring client or the NMS can be configured to raise trouble tickets for each exception reported. The trouble ticket system can be configured to send e-mails to a pre-defined list and follows an auto-escalation mechanism in case problem resolution time frames exceed pre-set limits.

1.6. SNMP Traps

NMS now supports SNMP traps. SNMP (simple network management protocol) has a facility by which the SNMP agent in the device itself sends across a message to the manager (NMS) whenever some predefined event occurs. This facility helps reduce the polling frequency as the event gets notified the moment it occurs.

Link Up / Down traps are the most useful of all the SNMP traps. Herein the router sends across a trap to the NMS as soon as one the link goes down. As a result, NMS will immediately alert on any link outage.



1.7. Alerts and Escalation

Alerts are graded in terms of seriousness and appropriate action is taken to inform the network administrator of the problem. Alerts are available in different modes viz.

- Message Popup
- Text-to-Speech voice alerter
- Playing a voice file
- SMS or E-mail

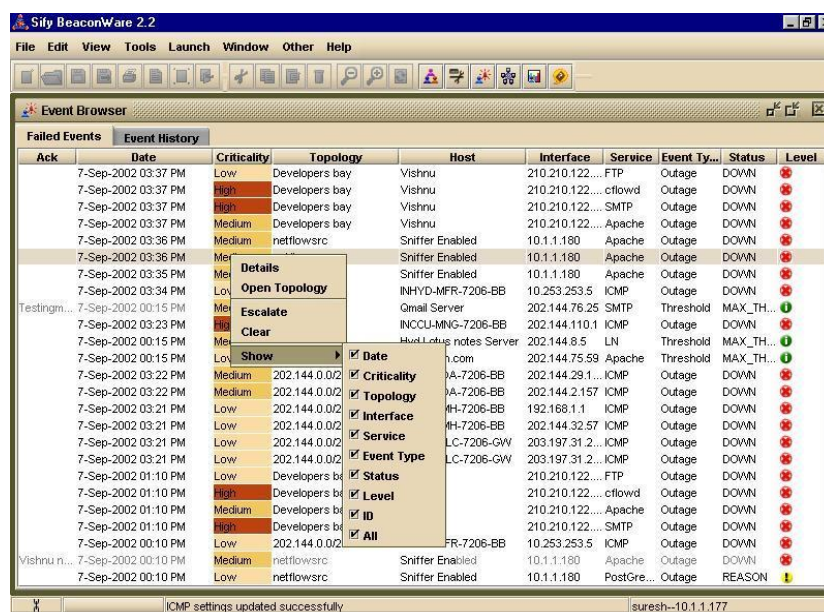
In case, the problem is serious and not resolved within a specified time frame, NMS will intelligently escalate the alert to the next level in the escalation hierarchy using email and SMS. Escalation charts

can be setup for each network device or service indicating the escalation hierarchy. The escalation hierarchy is completely customizable - different escalation charts can be specified for different types of alerts –for intimating an outage or threshold exception for each device or application. NMS also monitors the connection of Poller(s) and intimates the same to the user.

NMS offers the option of creating, using, and assigning multiple Escalation Charts and assigning them to network devices or services as required. Further the charts offer the flexibility to incorporate the days of week with time when the escalation is to be disabled along with facility to mute escalations on specific days (like public holidays) of the year.

1.8. Event Viewer

An Event Viewer is provided for viewing the detailed events logged. Alert details, severity of problem and the status is displayed in the event browser along with details of different information that the system records dynamically.



Events can be filtered based on the seriousness of the event - so that only the events relevant to the user are displayed. For each event about an outage or a threshold violation, there is a corresponding event generated when the normalcy is achieved. The user has the option of viewing only the failed devices at that point of time. A drill down facility is supported where users can always find out more about an event by double clicking on it.

Users can now directly do the following from the Event Viewer:

- Escalate
- Open Topology containing a specific device.
- Create trouble tickets.
- Manage view of event viewer
- Acknowledge an event, which will carry the user's name (login name) and time of acknowledgement, which is useful in multi-user environment.

By default, the Event Viewer has two tabs:

- **Current Events:** It shows events as they occur which includes threshold exceptions and outages.
- **Failed Services:** It shows the events linked to outages, as they are more critical than other events.

1.9. Performance Management

NMS helps you to improve performance of your network by presenting real time and historic information about your network. The performance metrics measured can be used as elements of service level reporting. NMS aids capacity planning too - network devices and links that are approaching peak capacity utilization will be indicated in the reports enabling you to add capacity before problems arise. Performance reports enable proactive troubleshooting of your network by helping you isolate faulty devices.

NMS helps you monitor performances across any of the parameters that are supported by the SNMP agents of the device. In a typical deployment the relevant parameters are identified from the list (made available by the vendors) and these are then enabled with lower and upper thresholds defined.

1.10. Comprehensive Reporting

Reports are presented in an easy-to-understand graphical format with the ability to customize the report based on date interval, type of graph (bar, area, line), legends, colors, and information to be plotted. Report customizations can be stored and retrieved for future use. NMS's flexible reporting system provides real time and historic information useful for network monitoring and management. Detailed availability reports are provided to help monitor your service level agreement fulfillment. To enable planning for future network growth, detailed outage reports are provided. The report system enables network managers to comprehensively monitor network devices on an hourly, daily, monthly, or even yearly basis on the following parameters:

- CPU Utilization
- Memory Utilization
- Traffic In
- Traffic Out
- Errors In
- Errors Out
- Response Time

NMS Report system provides detailed network link reports including availability reports, performance reports and traffic reports. This would help the user understand the utilization of bandwidth across the network.

Some of the special reports (apart from standard value vs. time plots) are:

- **Top N Reports** (which gives the top “N” number of devices which are of a particular state or profile where N is defined by the user)

- Location Specific Reports giving reports for specific locations.
- Topology wise reports for reports on specified topologies
- Reports with filters for Business Hours (which would then discount parameter values for off-office hours)
- Reports with filter for specific device type in topology, location

NMS also offers service-monitoring reports. Availability and response time reports are provided for FTP, HTTP, DNS, LDAP, IMAP, POP3, SMTP and generic TCP services. It also has the inbuilt intelligence to monitor the following database servers with ease: Oracle, PostgreSQL, SQL Server, MySQL, and DB2.

The report engine is also linked to a Reports Newsletter Engine which enables users to set pre-defined reports to be e-mailed at pre-defined times (e.g., every Monday morning). The reports also provide an option to export data in standard format to integrate with third party products or to get raw data on the network performance. The reports are web based; hence they can be viewed from any machine in the network.

1.11. SLA tracker

This module enables to configure and track SLA adherence of devices. Any violation will be reported, and reports will be generated in a graphical and tabular format.

1.12. Administration

Multiple levels of users can be setup based on roles they play. Hence access can be restricted based on the responsibilities of the person. As a result, the personnel who are responsible for say the Chennai part of the network can see events / alerts and performance graphs along with the status of only the Chennai network devices.

The entire setup, use and administration of NMS is GUI based with simple menu driven functions. NMS has a backup facility in-built into the system enabling the Network Administrator to easily backup the crucial information about network performance that NMS collects.

1.13. SNMP support

NMS can monitor any device or application that is SNMP enabled.

- Support for snmpget, snmpset, snmpwalk, snmpbulkget, snmpbulkwalk, snmptraps and snmptable
- Support for stable SNMP v1, v2c & v3
- Extensive library of MIB's maintained at backend to support a vast number of devices.
- Support for updating MIB library with new MIBs.

1.14. Port monitoring

Sify NMS can monitor and report availability and performance of any TCP port. This is a good feature where a customized application listening on a TCP port can be monitored. Reports on the port response time will also be available.

1.15. Secure

All data that is transferred from the Poller to the station for processing is 3 DES encrypted. This feature is of great use when the NMS polling device has been deployed at the customer site and the station is installed at Sify.

1.16. Data Persistence

In the event of a network cut between the Poller and the station, then all polled data is persisted at the Poller end and then sent to the station when the connectivity is back on again.

1.17. Simple

Sify NMS comes as a single package. You do not need to install separate packages and plug-ins for any additional monitoring requirements. The entire Sify NMS is highly configurable with no extra licensing requirements, provides ease of administration.

1.18. Scalability

Resource utilization intensive data collection process can be spread across multiple machines located anywhere on the reachable network. This not only lends to scalability but also contributes to failover and load balancing. Strategic positioning of these data collection engines also lends to multiple views of the network performance and end-to-end connectivity issues.

1.19. Monitoring Parameters

Sify NMS can monitor the following parameters.

Mandatory

- ICMP Latency
- ICMP Packet loss
- SNMP Cisco Link Reliability
- SNMP Interface Input Errors
- SNMP Interface output Errors
- SNMP Interface Output Traffic - Threshold can be configured.
- SNMP Interface Input Traffic - Threshold can be configured.

Optional

- SNMP Cisco Used Memory Pool - Threshold can be configured.
- SNMP Cisco Free Memory Pool - Threshold can be configured.
- SNMP CPU 1-minute Average Utilization - Threshold can be configured.
- SNMP CPU 5-minute Average Utilization - Threshold can be configured.
- SNMP Cisco-TempInlet

SNMP Cisco-TempOutlet