Technical Specification for Network Management Software

Sr. No	Features Description
1	**Core Monitoring Capabilities**
1.1	The Network Management software must be able to monitor: (a) Routers (b) Switches (c) Firewalls (d) Wireless devices (e) Servers (e) Other SNMP-enabled devices
1.2	Should automatically provide real-time, in-depth network performance statistics after discovery/configuration of devices, including but not limited to, (a) CPU load (b) Memory utilization (c) Interface utilization (d) packet loss
1.3	Should show statistics like interface bandwidth, current traffic in bps, total bytes received/transmitted etc.
1.4	Should be able to discover and troubleshoot network paths hop-by-hop for both on premises and cloud environment for specific TCP connections
1.5	Should display information including alerting for major routing protocols (BGP, OSPF, RIP, EIGRP) with options to view and search routing tables including VRFs, changes in default routes and flapping routes, router topology and neighbor statuses
1.6	Should help with multicast traffic information monitoring, alerting including topology information, multicast information, route information, multicast errors etc.
1.7	Should display device status and interface status by different colors to represent warning and critical status
1.8	Should monitor hardware health for popular vendors like Cisco, DELL, F5, Juniper, HP etc. and should allow alerting and reporting on hardware health monitoring
1.9	Should show both Realtime details and historical details in form of charts with option to choose the time periods
1.10	Should be able to discover and monitor both IPv4 and IPv6 devices
1.11	Should have options to poll using SNMP v1, v2c and v3 and WMI
1.12	Should have options to configure polling intervals as needed
1.13	Should have options to specify data retention periods
1.14	Should have the option to determine device availability using SNMP only
2	**Network Discovery**
2.1	The Network Management software must be able to discover devices in the network with SNMP and ICMP capabilities automatically, on input of, (a) IP address ranges (b) subnets (c) individual IP addresses (d) Active Directory
2.2	Should not add devices with multiple IP addresses as duplicate nodes but should list all known IP addresses for the node
2.3	Should allow interface filtering on discovery results to exclude virtual interfaces and access ports and select interfaces based on pattern matching
2.4	Should have option to automate and schedule discovery process

2.5	Should be able to automatically imports discovered devices
2.6	Should prompt in web console on discovery of new devices in network
2.7	Should use discovered information for creating topology maps
3	**Graphical User Interface and Customization**
3.1	The Network Management software must provide a high-quality graphical user interface with asynchronous view refreshing
3.2	This web console should be accessible centrally or remotely
3.3	The web console should allow multiple users to log in at the same time
3.4	It should have load-balancing options available if too many user's login at same time
3.5	It should allow customization by having options to add/remove sections in web pages as necessary
3.6	It Should provide a unified view of alerts, traps, events, syslog messages in a single page
3.7	It should give a single unified view of multicast information, route information and device information for a device.
3.8	It should quickly highlight devices with issues, based on different properties like response time, cpu load, memory usage, high interface usage etc.
3.9	It should allow creation of custom dashboards and restrict views for users based on devices or interfaces, i.e. it should have role-based access
3.10	It should log user actions and events in the web console for audit purposes and they should be available for alerting and reporting
3.11	It should allow interactive charting for node, interface, volume charts etc.
3.12	It Should provide a dynamic dashboard that allows in-depth visibility and correlates disparate historical data points across different part of the infrastructure. The result should be exportable with a tabular format
3.13	It should allow export of any web page in console to PDF format
3.14	It should integrate with Active Directory for user login purposes
3.15	It should be easy to use and intuitive with drill-down features
4	**Advanced Reporting**
4.1	The Network Management software must provide current and historical out-of-the-box reports for various statistics monitored
4.2	Should be able to generate / create the report via the web console
4.3	Should be able to generate statistical reports that can be used as reference for future planning or troubleshooting
4.4	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns etc.
4.5	Should allow advanced customization by providing options to enter custom queries to query the database directly
4.6	Should have options to save the customized reports permanently and have them accessible in web console
4.7	Should allow reports to be sent out on schedule as daily, weekly, monthly reports

4.8	Should allow emailing of dashboards created in web console
4.9	should be able to configure both charts and tables into a single report.
4.10	Should have options to import/exports reported created by other users
4.11	Should support multiple formats such as pdf, HTML and CSV
5	**Advanced Alerting**
5.1	The Network Management software must be able to manage and display events/alerts in the web console
5.2	The alerts and events information should be logged into the database for future reference
5.3	The alerting mechanism should allow complex conditions and condition groups to be specified for narrowing down the alert condition
5.4	It should allow custom queries to be entered to create rules against the database
5.5	It should allow creation of new alerts from scratch and also customizable threshold limits
5.6	It should allow creation of alerts based on sustained states
5.7	Should have various actions that can be taken, including but not limited to, sending out emails, forwarding SNMP traps, running executables, sending SMS text alerts, playing sound, emailing a web page etc.
5.8	Should have support for variables in alert email message to make the content more self-explanatory
5.9	Should have the ability to dynamically baseline statistics and automatically set Warning and Critical threshold
5.10	Should allow alerts suppression during scheduled maintenance
6	**Grouping**
6.1	The Network Management software must allow grouping of devices by various properties -- by department, by location, by name and by other properties gathered
6.2	Should also allow adding members to groups on-the-fly by specifying a property which can dynamically change values, like volumes reaching low free space
6.3	Should be able to define dependencies and relationships between connected devices and interfaces to avoid false-positive email alerts in case of outage.
7	**Network Maps**
7.1	The Network Management software must be able to represent the network pictorially and display performance details of devices in real time
7.2	Should allow customization of background, icons etc. and should allow multiple network maps to be nested with drill-down capabilities
7.3	Should be able to display not just the device status on the map but also status of any other detail obtained through custom MIB polling
7.4	Should have the capability to display the status of nodes or an aggregated group of nodes over dynamically updated street data.

7.5	Should be able to automatically connect devices by means of topology information gathered during discovery, like Cisco Discovery Protocol or Link Layer Discovery Protocol
7.6	Should be able to view multicast topology using upstream and downstream device list information
7.7	Should be able to display devices location on the geographical level and down to street level
7.8	Should have the ability to show the link utilization as a 'weather map'
8	**Multi-vendor Support**
8.1	The Network Management software must not be vendor-specific
8.2	The discovered devices should be detected as that of a specific vendor and categorized automatically
9	**Extensibility**
9.1	The Network Management software must allow gathering of custom properties from SNMP-enabled devices by specifying the OID of the properties
9.2	Should be able to fetch properties from devices without need to import device MIBs into MIB database
9.3	Should be able to get real-time values, charts and also alerts on these custom properties
9.4	Should have APIs available to programmatically import/export nodes and do similar functionality
10	**Application Aware Network Performance Monitoring**
10.1	The Network Management software must be able to provide Network Response Time (NRT) and Application Response time (ART) for critical applications
10.2	Should be able to identify and classify ~1200 applications out of the box
10.3	Should have the ability to display aggregate volume metrics per application / node
10.4	Should have the ability to create custom HTTP applications
10.5	Should be able to contextually provide QoE data for nodes in Node Details sub view
11	**Additional Components**
11.1	The Network Management Software Should have utilities to view the database, to stop and start application services
11.2	Should have options to receive, display and alert on syslog messages and traps from devices
11.3	Should have wireless reporting option to display wireless thin and autonomous access points and their associated clients
11.4	Should have customized mobile views of console for administrators' immediate viewing
11.5	Should be able to monitor invidual member switches, power stack and data stack rings in Cisco switch stacks
11.6	Should be able to report on technologies like Cisco UCS, Energy wise feature

11.7	Should be able to report on virtualized Cisco Nexus 1000V switches, VSAN, Fiber Channel switches like Cisco MDS, Brocade, McData devices
11.8	Should be able to monitor cloud-based Meraki wireless infrastructure
11.9	Should be able to monitor entire VMware and Hyper-V virtual infrastructure, including Virtual Centers, Datacenters and ESX clusters, and automatically track VM performance
11.10	*Should be able to monitor individual components in F5 BIG-IP load balancing environment*
11.11	*Should be able to monitor individual components in Cisco ASA firewall, including but not limited to, connection count, site to site and remote access VPN tunnels, interface identity and utilization, high availability status and configuration synchronization status.*
12	**Integration**
12.1	The Network Management software must be able to integrate with modules serving other monitoring purposes and provide a single-pane-of-glass view
12.2	Should allow integration with third-party applications at user-interface layer, through message exchanges and also through APIs
12.3	Should be able to integrate with ServiceNow, with the ability to automatically create incidents and synchronize the acknowledgement of incidents bidirectionally
13	**Enterprise Scalability**
13.1	The Network Management software must be able to accommodate network growth through addition of load-balancing applications
13.2	Load-balancing engines should handle interruptions in the connection between the engines and the main application
13.3	Should allow information from multiple instances of application to be consolidated into a single view
13.4	Should support multiple deployment options: (a) Centralized deployment (b) Distributed deployment (c) Hybrid deployment With a centralized operations console view, alert acknowledgement and reporting interface
14	**High Availability**
14.1	The Network Management Software Should have options for ensuring high-availability of application, with/without use of failover products
15	**Deployment**
15.1	The Network Management Software Should be deployable within one hour and should not require consultants for deployment, implementation, configuration or customization
15.2	Should support agentless deployment
15.3	Should include optional agent for Windows, Linux (Intel and ARM)

16	Frequency of Updates
16.1	New features to be added to product versions frequently, preferably twice every year or more
16.2	Should notify availability of new versions in the web console
17	**Product Support**
17.1	Should provide 24x7 support
17.2	Active support through forums and community would be a welcome feature

Note: Network Management software required for 250 Elements.

1. **Dr. Muhammad Asif Habib**
   (Associate Professor) Dept. of Computer science

   (Convener Technical Committee)

2. **Mr. Waqar Ahmad**
   (Assistant Professor) Dept. of Computer science

   (Member Technical Committee)

3. **Mr. Abid Hussain**
   (Network Administrator) Dept. of IT

   (Member Technical Committee)