MAX: THE COMPLETE NETWORK MANAGER

Introduction

The whole gamut of network management involves monitoring of network resources for the purpose of maintaining high quality of service (QoS) levels, improving performance, documentation and reporting, detecting latent anomalies, and troubleshooting actual problems. Basic management tasks include data backup, security provision, user training, and policies development, among others.

The international quality standards body ISO constructed a network management model that plots the key functions of network management systems. The model defines the following 5 areas:

- Fault management. Detection and logging of anomalies, notification of users regarding network events and alarms, and auto-fixing of network problems to maintain smooth network operations.
- Configuration management. Monitoring of network and systems configuration information to keep track of the affects of software and hardware elements.
- Accounting management. Measurement of network utilization so that individual or group use of network resources can be monitored and regulated.
- Performance management. Monitoring and measurement of network variables such as throughput, user response time, and line utilization.
- Security management. Control over access to all network resources.

MAX Network Manager

MAX delivers an integrated solution that provides an end-to-end infrastructure management system, which in turn administers to heterogeneous and often complex IT environments. Through the proactive management of your IT Infrastructure MAX ensures your business availability consistently, helps you cut down operation costs and still scale up your business as it grows, and ultimately improves your ROI. MAX ensures early anomaly detection, preemptive information delivery to designated IT personnel (to address problems before they actually happen), and timely events/alarms notifications (to reduce the mean time to repair or MTTR).

The integrated network management solution in MAX enables you to:

- Measure the performance and availability of varied network devices from different vendors and based on various networking technologies. MAX also auto-discovers the

topology of your IP-based network, and systematically correlates the topological relationships between and among the network resources.

- Monitor the bandwidth utilization of your WAN interfaces, providing insight to the bandwidth requirements of your mission-critical applications.

- Monitor the traffic distribution in your network using RMON or Cisco NetFlow technologies.

- Monitor your service levels, even your vendor-committed SLAs to ensure that your business is not at risk.

- Monitor user acceptance of your network services from multiple locations at the same time using simulation requests sent by MAX, thus providing you insight into the expected response time of your business services. Also supports monitoring of network response time using Cisco Proxy Ping technologies and MPLS/VPN network environments.

- Alert your network engineers and perform time-based alarms escalation to IT managers (up to the highest level) whenever a fault happens or a probable future fault is detected based on historical and current performance trends. Also supports integration with self-remedy applications that ensure timely auto-fixes to problems as they are detected—thus reducing the MTTR—and the prevention of the future problems itself.

- Use a fully Web-enabled graphical interface that can be accessed from any location at any time all the time.

- Manage large networks using the distributed architecture of MAX, which can provide customizable maps and sub-maps for your infrastructure environment.

- Generate top-to-bottom graphic reports to provide a single view of the infrastructure resources.

MAX, using customized external scripts and OSS integration, can also be configured to perform remote desktop and configuration management, software installation and licensing management, network asset management, help desk service, performance and protocol analysis, resource and bandwidth management, capacity planning, and simulation. The following are among the key features of MAX's network management module:

- Network Device Management. MAX provides the ability to proactively monitor, and carry out fault and performance management on varied network devices from different vendors and based on various networking technologies. Where anomalies or faults occur, MAX readily alerts the designated IT personnel, at the same time informing them of any future business interruption. MAX's extensive out-of-the-box reporting tools also provide you with the ability to plan and manage networks based on their capacity requirements.

- Bandwidth Management. MAX provides the ability to monitor network interfaces and measure their health status. Monitoring the WAN bandwidth provides valuable insight into network resources usage, and provides detailed analysis of the network services catering to your business requirements.

- Cisco NetFlow-based Traffic Management. NetFlow technology, an integral part of Cisco IOS software, collects and measures data as it enters specific routers or switch interfaces. By analyzing NetFlow data, MAX's network management engine, among others, can identify the cause of congestion, determine the type of service (ToS) for

each user and application, and identify the source and destination network for your NetFlow-based traffic.

- RMON-based Traffic Management. MAX communicates to the RMON probe to obtain the status of the probe itself, and the RMON groups 12, 14 and 16 classes of information. This way, MAX provides you with detailed information on the availability of the RMON probe and the protocol distribution, among other vital data derived from using RMON technology.

- Service Level Management. Setting SLAs in MAX allows you to achieve proactive service level management functions, e.g., alerting users or the administrator prior to the actual breach of the SLA. MAX implements SLA as a compliance statistics of the condition, and most of the online real-time reports apply to SLA statistics. Alarms and events may be set for an SLA resource if you intend to be informed through alarms, events, or event notifications when the SLA compliance percentage falls below a certain percentage. Additionally, threshold alarms can be set for an SLA resource with various severity levels for the SLA compliance percentage, just as thresholds can be set for other resources in MAX.

- Event Notification. MAX provides customizable events and alerts notification via email, pager or short messaging service (SMS), or by executing batch files, generating SNMP traps, and invoking workstation beeps, with the flexibility to integrate with existing user systems.

- Distributed Architecture for unlimited scalability. MAX is designed and engineered based on a distributed architecture, making it highly resilient and scalable, catering to enterprises that extend across various territories and are geographically dispersed.

- User Experience. As a Web-based system, using MAX is best described as easy, intuitive and user-friendly. Whether you are looking to set up the initial system, define threshold alarms, or view a wide array of performance and event reports, these tasks are easily accomplished through an easy-to-use Web interface—no complicated, proprietary client software is involved—thus allowing you to quickly deploy and implement MAX, greatly shortening your learning curve and maximizing user experience and satisfaction.

- Capacity Planning. MAX offers different types of reports to assist in analyzing the network resources, their users and the volume of usage, among others—elements crucial in performing capacity planning for proactive management of the infrastructure.

- OSS Integration. MAX supports multi-vendor equipment and IT infrastructures based on disparate platforms, and provides for the flawless integration with applications and utilities using Open Source Software. These utilities work and communicate with MAX to invoke user-configurable scripts that allow them to execute several fault resolution actions, such as putting a device into maintenance mode, connecting to a 24-hour help desk, and automatically opening trouble tickets.