BUILDING YOUR NETWORK MANAGEMENT TOOLSET

Maintaining highly available networks begins with having the right products and practices in place.

Executive Summary

Public- and private-sector organizations of all sizes are increasingly dependent on their networks to meet their operational imperatives. At the same time, these networks, pressed to handle proliferating demand for resources while connecting an intricate matrix of infrastructure and user variables, are growing increasingly complex.

Likewise, user expectations have reached new heights. Employees take network availability for granted, expecting to connect seamlessly to network-optimized applications and services at any time, from anywhere. Meeting stakeholder expectations in distributed network environments can be challenging even when a user base is small, based in a central location and relatively stationary.

Table of Contents

Today, however, more IT teams are serving mobile users, who often are armed with multiple devices, as well as workers operating in remote offices and other facilities situated farther from the core data center, putting added stress on network processing.

Justifiably or not, network specialists are finding themselves held responsible not only for network availability and performance, but also for the performance of any network-delivered IT resource, including data, voice and video applications; virtual desktops; and even cloud services.

What can IT shops do to ensure that their networks and expertise can rise to the challenge? Understanding network management best practices, as well as the tools, technology platforms and managed services that are available to help, is a good place to start.

Simple Network Management Protocol

From its relatively humble beginnings in the late 1980s, when the Internet Engineering Task Force tapped it as an interim solution for handling expanding Internet and other attached network traffic, the Simple Network Management Protocol (SNMP) has grown to become the management and monitoring muscle behind wired and wireless IP networks.

Network management systems (NMSs) incorporate SNMP to monitor and control the array of managed devices that collectively make networks hum. Via centralized consoles that provide both big-picture and deep-dive visibility into network operations, NMS software enables administrators to manage any device, from switches and routers to servers, desktop PCs, notebooks, printers, firewalls, backup devices and storage systems.

Some NMS platforms are designed to handle all the primary network management areas: fault, configuration, performance, security and accounting management. Others are best-of-breed point solutions or handle some combination of these management functions.

IT teams, particularly those that manage large distributed networks with thousands of devices, can't keep networks running and secure without this level of visibility and control. Operational performance depends on having a unified view of the continuous stream of information on all network activity so they can maintain high performance levels and isolate and analyze any issue, from minor anomalies to serious congestion capable of bringing down an entire network. From NMS dashboards, adminstrators can monitor various devices, quickly pinpoint malfunctions, perform preventive maintenance and fine-tune overall network and application performance.

Network Optimization Benefits Checklist

- ✓ Decreases operating and management costs
- ✓ Reduces application latency to remote end users
- ✓ Creates multiple pathways to ensure application availability
- ✓ Centralizes the network environment
- ✓ Maximizes bandwidth utilization
- ✓ Postpones wide area network (WAN) bandwidth upgrades
- ✓ Improves disaster recovery preparedness by speeding WAN backups and data replication

SNMP at Work

To do its job, SNMP employs managers, agents, virtual databases housing network device data (called management information bases or MIBs) and managed objects, each with its own object identifier (OID). In this manager/agent model, the NMS manager exchanges information with individual agents residing on managed devices throughout the network. The majority of devices on the market today incorporate SNMP agents.

Not suprisingly, network administrators prefer a "single pane of glass" approach to managing their networks, rather than having to use separate NMSs for traditional device management and mobile device management, for instance, or to monitor devices manufactured by multiple vendors. Some NMS platforms provide the integration capabilities to handle multivendor components through a single interface. But depending on their network environment, IT departments may need to run multiple NMSs.

In network-managed system environments, an NMS manager can monitor and control any device running SNMP agent software. Agents also behave proactively, sending information on common component malfunctions or IT-specified variables to the NMS when they discover a device issue. Issues that trigger agents to automatically send messages include insufficient CPU resources and memory, buffer failures or high temperature readings caused by malfunctioning fans.

A manager and agent exchange information using MIBs. A manager stores a common MIB with information on all the resources it manages, while an agent incorporates its own MIB, which it references so it can send requested or predefined status information to managers.

Built on an object-oriented model for dynamic information retrieval, an agent MIB contains the device's managed object definitions, hierarchy of variables and their specific access privileges. It references each managed object through a unique OID, which ties to specific device characteristics and enables the manager to understand the intent of messages sent by agents.

SNMP Speaks, Network Admins Listen

The simplicity credited to SNMP is largely due to the small number of command types it uses to allow managers and agents to communicate. This simplicity has assured its nearly ubiquitous adoption as a network management protocol. Today, SNMP relies on seven basic messages, sent as information packets called protocol data units (PDUs), to enable manager/agent communications. To standardize messages, all PDUs are organized under the following construct:

- **IP Header:** specifies the IPv4 address of a packet's source, as well as the IPv4 address of its intermediate or final destination; for the new IPv6 protocol, the header field includes the 128-bit IPv6 address that identifies the source of the packet, as well as that of its destination
- **User Datagram Protocol (UDP) Header:** provides port numbers for the PDU source and destination
- **Version:** identifies the version of SNMP an agent supports (SNMPv1 uses an integer with a 0 value, while SNMPv2's integer has a value of 1. An NMS relies on its MIB database to ensure it communicates with agents using the appropriate SNMP version.)
- **Community:** authenticates a manager and its access rights before allowing agent access
- **PDU Type:** specifies the type of PDU
- **Request ID:** associates requests with responses
- **Error Status:** indicates an error and its type
- **Error Index:** associates an error with an object variable
- **Variable Bindings:** ties an object to its values

SNMP's seven PDUs dictate the actions that managers and agents take:

GetRequest: A manager sends a GetRequest command when it wants an agent to send back values for one or more variables. The agent responds with the current values.

GetNextRequest: A manager sends an agent the GetNextRequest command when it wants to discover available variables and their values. The agent uses the OID contained in the PDU and retrieves and sends the values of objects whose OIDs are sequentially adjacent.

GetBulkRequest: An optimized version of GetNextRequest, this command is used to ask the agent for multiple iterations of GetNextRequest. Using this PDU, the agent can run through its entire MIB and respond with multiple variable bindings.

Trap: This command is an unsolicited message sent by an agent to notify a manager about a significant event in the agent's device. Within the Trap PDU, the agent sends OID data and variable bindings.

InformRequest: This PDU is used for both manager-to-manager and agent-to-manager communications. A manager can be configured to send an InformRequest message to managers on other NMS workstations in the network (alerting them to a trap notification from an agent, for example) and confirm delivery through an acknowledgement receipt.

SetRequest: A manager issues this command to request that an agent change the value of one or more variables. The agent makes the requested changes and returns the new values.

Response: This acknowledgement message, along with one or more variable bindings, is sent by the SNMP agent in response to a GetRequest, SetRequest, GetNextRequest, GetBulkRequest or InformRequest.

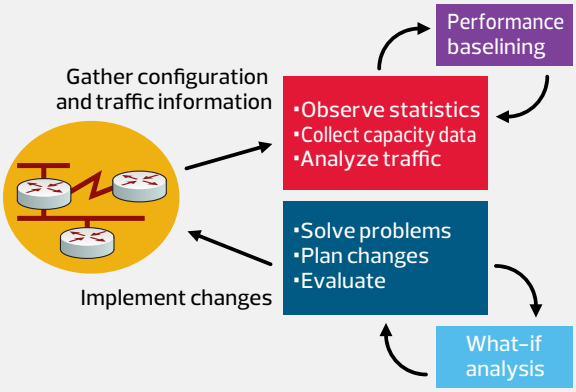
Performance & Capacity Management

High-availability networks are high-performance networks. Performance management best practices focus on ensuring consistent network performance and availability. Using performance management technologies, IT staff can ensure fast response, quality and consistency in their service delivery. Performance management goes hand in hand with capacity planning, as network performance problems are closely linked to capacity.

Capacity and Performance Management Processes

Network administrators who capture network baseline data are better able to address capacity issues, which helps them upgrade networks before performance degrades. Better still, they can use the baselines to conduct trending and "what-if" analysis.

With trending, administrators can review capacity and performance baselines for trends that shed light on requirements for potential network upgrades. What-if analysis, meanwhile, is key to effective configuration change management, as it allows IT staff to test the impact of any network changes before taking action.



SOURCE: Cisco Systems

Both disciplines, meanwhile, depend on the organization's network manageability objectives. To achieve these objectives, IT teams must understand the capabilities of their NMS platform and all related network management tools. This ensures that they're able to handle capacity changes, gain visibility into network components that can affect performance and make improvements to shore up weaknesses within the infrastructure.

A number of capacity-related elements influence network performance. If there's not enough capacity to achieve throughput, service quality deteriorates. When this occurs, data applications may have trouble loading. And if they do load, they may perform operations slowly. Voice applications, such as voice over IP, may deliver poor call quality, and video applications may lag due to high latency.

Network elements that administrators need to consider in their capacity planning and performance optimization efforts include:

CPU: To function, every managed device needs adequate CPU resources. Insufficient CPU on a single device increases latency as data piles up in the queue and can even cause enough congestion to bring down the network.

Input/output (I/O): If SNMP devices don't have the I/O required to handle network traffic volume, they drop packets. As they try to resend the packets they've dropped, traffic jams increase, exacerbating performance problems.

Memory: Without sufficient memory, devices may fail to handle some or all of their required operations. Failure at the device level can slow network performance or result in downtime.

Interface and bandwidth: These dictate the volume of data a network can send simultaneously over a connection. Limited bandwidth causes queue pileups. Although IT staff can tune transmit queues to prioritize data, a significant backlog affects an interface's ability to transmit even higher-priority data.

Queuing, jitter and latency: IT shops must balance queues to ensure they're properly sized. If they're too large, data sits longer before it is transmitted; if they're too small, packets are dropped. Although delays caused by drops and retransmission may be tolerable for some data applications, they aren't acceptable for video and voice applications. CPU and memory resources also impact queuing.

Jitter is caused by variations in the arrival rate of packets. Although larger interpacket gaps don't significantly affect data applications, they do cause noticeable quality degradation in streamed applications such as video and voice.

Latency (the normal processing time between the receipt and forwarding of a packet) differs based on the packet type. With sufficient resources, modern data switches and routers have very low latency. Devices that compress and convert analog voice packets usually have higher latency due to the work they perform before forwarding. Constrained capacity and similar resource issues increase latency across the network.

Speed and distance: The distributed nature of the 21st century workforce — situated in satellite facilities, home offices and remote sites far removed from core data centers — can affect application-access speeds. A data network's standard packet-forwarding speed is about 100 miles per millisecond. If an employee is trying to access an on-premises application from halfway around the world, he or she could experience delayed response.

Application characteristics: Applications that aren't optimized for network environments typically don't scale well and, thus, don't meet performance requirements. If an application's architecture causes it to send more data than needed to the client side, the application might not perform well in some Transport Control Protocol/Internet Protocol network environments, particularly wide area networks (WANs). Application keep-alives, which check that links between two devices are operating, also affect capacity and performance.

Service-level Agreement Options

Today's complex, distributed networks are dynamic entities, connecting ever-shifting combinations of components. Ensuring high network availability and performance for present needs and future upgrades requires comprehensive capacity planning.

IT professionals naturally strive to deliver the best performance possible, but if they're operating under severe resource constraints, they can't always plan capacity effectively. Nevertheless, service best practices dictate that they be accountable for delivering defined services within an agreed-upon period.

To set expectations for service delivery, IT leaders should work with user groups and business units to establish service-level agreements (SLAs) based on the service, staff resources, support requirements and network capacity. If their budget and other resources are overly limited, they can request that departments benefiting from higher service quality finance the service. Another option is for IT departments to consider requests for new services or faster service delivery levels on a case-by-case basis, depending on their resources.

Measurement and Reporting

Effective performance and capacity management demands that IT organizations continuously collect data from across the network infrastructure for regular review and analysis. As part of the process, they should first collect the necessary data — for example, network throughput and CPU, buffer, memory, media and link utilization — to establish a network baseline. This baseline serves as a benchmark to measure whether proposed changes and upgrades meet uptime and performance needs.

Administrators also should be vigilant in their network oversight to identify potential problem areas before they

affect performance. To aid these efforts, they should establish and measure against key performance indicator (KPI) metrics such as:

- **Network availability:** the time a system or application is available to users
- **Network response time:** the time traffic takes to travel from point to point
- **Accuracy:** packet-forwarding success rate versus total packet rate
- **Utilization:** usage of a resource versus its maximum operational capacity
- **Capacity:** throughput rate

The best approach to performance monitoring is to collect data and report on conditions in real time. This enables IT departments to address potential problems proactively rather than reactively, after serious damage may have already occurred. If a malfunction that couldn't have been anticipated does occur, real-time reporting data can alert IT managers so they can take immediate action. They also can analyze trends in data to identify ongoing performance issues.

Practicing baselining and trending enables network teams to address capacity problems proactively by upgrading networks before performance is impaired. Network management systems typically provide the ability to run scripts that collect capacity data on such resource variables as link, CPU, memory and buffer utilization, as well as ping performance, queue depth, broadcast volume and frame-relay congestion.

In addition, using their network baseline, administrators can choose more complex variables to measure, such as polling interval effectiveness and the overhead incurred from specific network management functions, and analyze collected data for trending purposes.

Quality of Service Management

QoS management tools help network administrators address queue delay, packet drops and bandwidth problems. QoS management practices call for the IT group to establish traffic classes and prioritize them accordingly. Traffic classification, often based on SLAs, prioritizes critical or more resource-intensive applications and segments less critical classes so they don't impact higher priority classes.

To effectively classify traffic, IT departments must understand their basic network utilization, specific application resource requirements and their organization's application priorities. IT personnel can then test different traffic classes as they travel over links and make necessary adjustments to achieve acceptable traffic-specific performance.

Fault Management

Network availability has long been a priority for IT administrators, but performance has joined uptime as a high-priority management issue. Because network degradation can influence productivity as much as an actual outage, fault management technology adoption is widespread.

These tools are designed to detect network problems, log the pertinent information, notify users and take remedial action if possible. The traps that agents use to capture problem data and alert management stations are invaluable to fault detection.

Management systems also detect faults through standard SNMP polling and syslog messages. If a management system polls a device to check resource utilization, for example, and its associated value exceeds the standard threshold, the agent generates an event.

However, because the IT team must address faults quickly, standard SNMP polling intervals of five, 10 or even 20 minutes aren't always effective. Issues that occur immediately after an SNMP status poll will go unnoticed until the subsequent poll. Serious faults can cause significant network degradation — or worse — in mere minutes.

Fault Management Best Practices

For some network components, IT departments should consider leveraging SNMP agents' remote monitoring (RMON) capabilities. IT personnel can better keep abreast of issues by using RMON alarms and event groups on select devices to track suspected problem points in data streams, eliminating the need for SNMP polling.

Best practices for fault management, not surprisingly, include this level of proactive fault analysis. A self-monitoring device, configured to monitor rising and falling thresholds, compares a sample of a variable (such as CPU, memory and link utilization or I/O drops) against defined thresholds.

If a value falls outside the threshold operating range, the agent generates an exception alarm. Administrators typically restrict the use of RMON alarms to critical devices so they won't waste time taking extraordinary measures in situations that don't require drastic action.

To leverage this kind of proactive analysis, administrators need to determine which thresholds to set for which devices, a time-intensive process. The good news is that they can apply the network baseline data they've already captured for performance management activities as the foundation for this fault detection method, saving them significant time and resources.

Device Management

To effectively manage a network environment, IT teams need to be aware of everything the network encompasses. That requires understanding its configuration, based both on current resource demands and the upgrades it will likely require to meet future needs, as well as all network components, their interrelationships and their relationships to end users. From a device management standpoint, administrators should know what devices they have and need to manage, which devices should handle which functions, and all users involved.

Armed with this knowledge, they're better positioned to meet service delivery requirements. First, they're equipped to deploy the right device portfolio to meet operational and organizational needs. Plus, they can maximize finite staff resources by speeding repairs, maintenance and upgrades, thereby allocating more resources to focus on performance and security improvements.

This knowledge depends largely on their ability to inventory all hardware and software assets on the network and dynamically track any changes. A complete inventory documents hardware types, vendors and resource requirements; software types, vendors and versions; and device locations and their IP addresses.

Just getting a handle on the software the devices run is a major step forward for many organizations. It enables them to practice software version control: By reducing multiple versions of the same software, they reduce support costs, limit interoperability problems and streamline upgrades. Standardizing software for like devices, meanwhile, eases deployment and upgrades, while reducing support and maintenance tasks for the entire network.

Given the pace of change in larger networks, IT departments need automated software for inventory management and broader device management functions. NMS vendors often either provide inventory capabilities in their platforms or integrate with third-party network inventory software.

Among key inventory management capabilities are device discovery features, which automate the discovery of all network-managed devices and their associated interfaces and peripherals. Discovery jobs can target individual or multiple IP addresses.

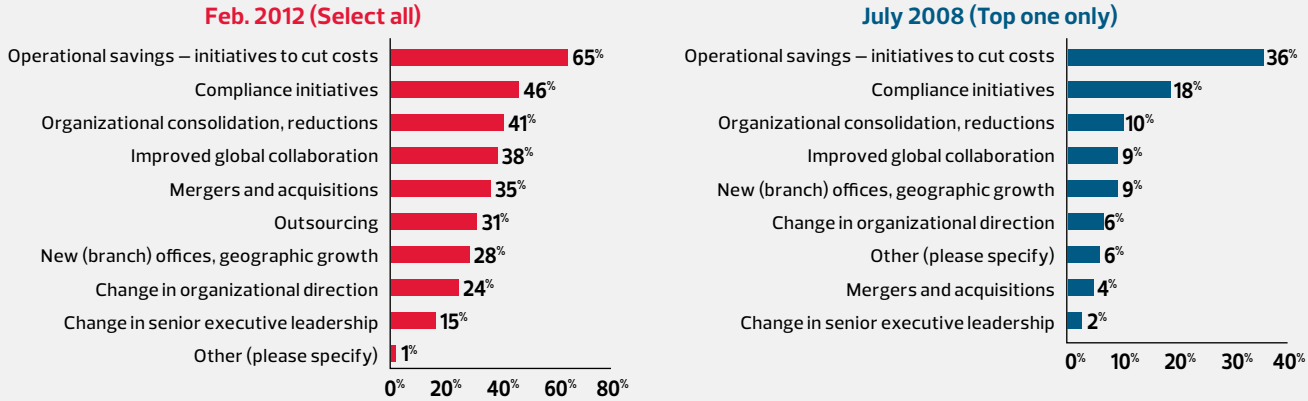
All inventory information is stored in a network inventory system database, if available. These databases have sophisticated capabilities, including the ability to synchronize inventory data with NMS databases and to track modifications in preparation for the next inventory run.

Inventory management systems offer unified, real-time views of the entire network inventory. Using centralized inventory data, the IT department can change device capabilities for group devices based on department or other user-defined group data, customize device settings, easily add or remove devices from a group and perform related management tasks.

Good device inventory management also enables IT organizations to maintain a streamlined network configuration and a high level of functionality. If IT managers don't know what devices are on the network or the software that each device is running, they're at risk for noncompliance with licensing agreements, higher security threat levels due to increased vulnerability, and wasteful support expenditures. Further, if they're relying on outdated or underutilized device hardware and running multiple or incompatible software versions, they can't maximize network performance and availability.

Organizational Initiatives That Drive Network Management Efforts

In separate network "megatrend" surveys conducted by the research firm Enterprise Management Associates in 2008 and 2012, the same organizational initiatives topped respondents' lists of network management drivers. The leading drivers — network management's "Four C's" — continue to be operational cost containment, compliance, organizational consolidations and improved global collaboration.



SOURCE: *Network Management 2012: Megatrends in Technology, Organization and Process*, Enterprise Management Association (EMA)

Security

Along with networking's continuous advances come new security threats, which multiply seemingly by the day. The dynamic nature of attacks demands dynamic multipoint security solutions.

Network management systems, with their monitoring capabilities and unified views into infrastructure dynamics, give IT organizations a powerful weapon for fighting cyberthreats. To secure today's distributed networks, IT teams also must develop defense-in-depth strategies that combine network-enforced security technologies with best practices.

The following products should be part of every IT organization's network security toolset:

Intrusion detection and prevention systems: IDS and IPS tools help IT staff identify and protect their wired and wireless networks against several security threat types. These technologies, like several other categories of network security tools, are being deployed with greater frequency as networks grow in size and complexity. Annual IPS revenues are expected to more than double between 2012 and 2017 (from $1.21 billion to $2.44 billion) according to estimates from the research and analysis firm Frost & Sullivan.

Both IDS and IPS solutions detect threat activity in the form of malware, spyware, viruses, worms and other attack types, as well as threats posed by policy violations. IDS tools passively monitor and detect suspicious activity; IPS tools perform active, in-line monitoring and can prevent attacks by known and unknown sources. Both tool types can identify and classify attack types.

Anti-malware: Anti-malware network tools help administrators identify, block and remove malware. They enable the IT department to tailor its anti-malware policies to identify known and unknown malware sources, for example, or surveil specific users and groups.

Malware is always on the lookout for network vulnerabilities — in security defenses, operating systems, browsers, applications and popular targets such as Adobe Flash, Acrobat and Reader — that they can exploit to fully access a victim's network. Best practices call for a multipronged defense that might also include IP blacklisting, data loss prevention (DLP) tools, anti-virus and anti-spyware software, web browsing policies, egress filtering, and outbound-traffic proxies.

Mobile device management: MDM software bolsters network security through remote monitoring and control of security configurations, policy enforcement and patch pushes to mobile devices. Further, these systems can remotely lock lost, stolen or compromised mobile devices and, if needed, wipe all stored data.

Network access control: NAC products enforce security policy by granting only security policy–compliant devices access to network assets. They handle access authentication and authorization functions and can even control the data that specific users access, based on their ability to recognize users, their devices and their network roles.

Next-generation firewalls: This technology expands on traditional stateful inspection to provide next-generation network security services, including application visibility and control and web security essentials. Next-generation firewalls also improve on standard firewall capabilities through application-awareness features.

Authentication and authorization: Traditional directory-based services, such as Active Directory, authenticate users and grant access based on authorization rules. Newer identity-based security technologies manage authentication and authorization through such methods as digital certificates and public key infrastructure solutions. Additional security is provided by the SNMP protocol itself. The most recent version, SNMPv3, provides authentication, authorization and encryption capabilities lacking in the previous two versions.

Configuration Change Management

To achieve higher availability and performance, IT teams must be capable of making necessary modifications while minimizing disruptions to the network and the people who depend on it. Improvement objectives may require them to upgrade hardware and software, swap out underperforming and damaged components, remove underutilized devices, streamline configuration traffic flows or overhaul the entire infrastructure.

In some cases, relatively minor changes can improve uptime and performance without having any affect on network availability. In other cases, improvement objectives require major modifications throughout a configuration. Those with the resources to establish a redundant network infrastructure can perform changes without a significant disruption, but many smaller organizations don't have the resources to create a high level of redundancy.

To minimize downtime during major overhauls, IT leaders must take a disciplined approach to configuration change management, leveraging best practices and technologies that automate well-defined processes. Because the stakes are so high, the goal should be to successfully implement changes on the first attempt.

The complex, interdependent nature of distributed network configurations and the people they connect makes the impact of infrastructure hardware and software changes difficult to predict. Given the ramifications, IT departments shouldn't

undertake configuration changes without careful planning, thorough documentation and proven change back-out procedures.

Configuration change management processes and technologies are designed to plan, track, test and document network changes. Network service transition efforts require thorough analysis and change control to ensure changes are effective and don't negatively affect end users. Further, IT teams should have safeguards in place so they can automatically roll back changes and return to the current configuration or a previous working configuration.

To gauge the effects and outcome of any planned network changes, it's important to conduct a "what-if" analysis. IT personnel can segment proposed changes into risk categories so they can invest more resources in testing the most critical infrastructure change impacts. They can analyze what-if scenarios using simulation modeling software or set up a test system that replicates the production environment. The latter approach, optimally performed in a lab environment to isolate it from the network, is the more comprehensive option.

Using traffic generators in the lab, network administrators can test the planned configuration, including any new software, hardware and other changes. To fully test the new configuration, they can generate different types of traffic, such as encrypted, compressed or SNMP, and review device resource requirements. These requirements relate to utilization across such areas as queuing, CPU, memory, backplane and buffers and should be tested under normal conditions, as well as under stress scenarios such as during device restarts and route convergence.