Many libraries began automating in the 1970s; however, it was not until the early 1990s that there was an explosion in the deployment of networks. Initially, the networks were limited to staff workstations and patron access catalogs accessing an integrated library system, but with the growth of the Internet, including remote access to library servers from outside libraries and access out from libraries to electronic resources, the management of networks became quite complex.

While library staff and patrons will usually report network problems after they occur, a library should seek to identify potential problems before they affect users on the network. Network management software does that not only by sending out reactive alerts as soon as a problem has been detected, but also by providing warnings about potential network problems before they affect staff and patrons.

**Network Management Software Components**

There are five components of network management. The first four—which deal with performance, faults, accounting, and configuration issues—can often be purchased as part of a bundled suite of products. The fifth—security management—usually is not bundled with the others.

**Performance management** has as its objective the measurement of various aspects of network performance so that performance can be maintained at a planned level. The measures may include network throughput, user response times, and line utilization. It is not only necessary to measure, but to analyze the measurements to determine normal or baseline levels so that remedial action may be taken when performance is not acceptable. Performance measurement may also include network simulation to project how network growth may affect performance so that potential problems can be avoided.

**Fault management** is used to detect, log, notify administrators, and automatically fix—to the extent possible—network problems. It involves determining symptoms, isolating the problem, fixing the problem, and then testing the solution on all parts of the network. Fault management is often the first component of network management to be implemented because it contributes most directly to network up-time.
**Accounting management** seeks to measure network utilization so that usage quotas, if needed, can be set and changes in usage patterns can be projected. By creating reports about network use and performance over time, it is possible to predict future network needs and to budget for them. It is also a useful tool for determining how much bandwidth an ISP (Internet Service Provider) is actually delivering. Accounting management is often bundled with performance management.

**Configuration management** seeks to monitor network and system configuration information so that the effects on network operations of hardware and software can be tracked and managed. This is not as simple as it appears because differences in operating systems, Ethernet interfaces, and other system software will impact differently on a network. When a problem occurs, the configuration database can be searched for clues that may point to the source of the problem.

**Security management** controls access to network resources according to locally determined guidelines so that the network cannot be compromised and sensitive information cannot be accessed by those who lack authorization. The software can monitor users logging on and can refuse access to those who are not authenticated or limit what they may do. Security management has become a high priority for most libraries. Libraries are therefore, replacing earlier generation firewalls with tools that encompass all areas of security, including policies, firewalls, security scans, intrusion detection, virus detection, filtering, and physical security.

**Network Management Architecture**

The most common network architecture deploys software to managed devices, including servers and network devices, so that a network server will be alerted when problems are recognized. Upon receiving these alerts, network management software reacts by executing actions that may range from event logging and operator notification to automatic attempts at repair and system shutdown. Alternately, software on the network server can poll servers and network devices to check their status. The polling can be automatic or operator-initiated.

**Network Management Protocols**

The most widely used network management protocols are the Simple Network Management Protocol (SNMP), the Common Management Information Protocol (CMIP), the Remote Monitoring (RMON) network management protocol, and Web-Based Enterprise Management ((WBEM)). Before making a choice of network management protocol, it is necessary to determine what protocol each existing piece of equipment (servers, routers, switches) supports.

**SNMP - Simple Network Management Protocol**
SNMP was developed by the Internet Engineering Task Force (IETF) in the mid-1980s. It provides standard, simplified, and extensible management of LAN-based networking products such as bridges, routers, and wiring concentrators. It is a communication specification that defines how management information is exchanged. There are several versions. When all of the managed devices and software from different vendors conform to the same version or compatible versions of SNMP, they can be managed by a single network management tool.

SNMP is well suited to network monitoring and capacity planning, but it is not very good for troubleshooting. It also has minimal security capabilities.

**CMIP – Common Management Information Protocol**

CMIP is similar to SNMP and was developed to address the latter’s shortcomings, especially with regard to security and the reporting of unusual network conditions. However, it takes substantially more system resources than SNMP, is more difficult to install and maintain, and requires use of the ISO protocol stack (X.700-96), an international standard that is far less well known than the ubiquitous TCP/IP standard. It is implemented around the world, but has not been popular in the United States.

The best feature of CMIP is that events can be triggered automatically when a specific condition is identified. For example, when a computer cannot reach a server for a predetermined number of times, an automatic notification to a network manager can be triggered. With SNMP, the notification would have to be made by the user.

**RMON – Remote MONitoring network management protocol**

RMON, which has been preferred over CMIP in the United States since shortly after it’s publication in 1996 by the Internet Engineering Task Force (IETF), allows network information to be gathered at a single workstation. It collects a much wider range of data than SNMP—including current statistics, historical statistics, and alarms when current statistics deviate from thresholds established by historical statistics—and is easier to install and maintain than CMIP. However, for it to work, network devices, such as hubs and switches, must be designed to support it.

**WBEM – Web Based Enterprise Management protocol**

WBEM was developed to unify the management of distributed computing environments. Distributed computing consists of multiple autonomous computers that communicate through a network. WBEM includes the Common Information Model (CIM), a set of definitions of management information for systems, networks, applications and services.

Detailed technical information about each of the foregoing can be found by “Googling” the names or acronyms of these protocols.

**Network Management Products**
There are hundreds of network management products and scores of network management suites. None of the suites is a complete solution for a library that wants to implement all aspects of network management because most of them do not include a product for one or more of the components of network management, and none handles all aspects of network management equally well.

Hewlett-Packard’s Network Management Center (“Google” the name as the URL changes regularly), IBM’s Tivoli NetView (http://www-01.ibm.com/software/tivoli/products/netview/) as of the fourth quarter of 2009, but may change as IBM is redesigning its massive Web site) and Sun’s SunNet Manager (www.sun.com/software) are among the comprehensive network management suites offered by computer manufacturers. They tend to be strongest in performance, fault, and accounting management; and weakest in security management. Configuration management is done particularly well by Hewlett-Packard.

One of the most extensive network management suites offered by a communications company is Alcatel-Lucent’s VitalSuite (www.alcatel-lucent.com). The suite covers every aspect of network management except security management.

Performance management products are the most mature, and the only ones for which there have been a number of published evaluations. The consistently highest rated are ProactiveNet BSM (www.proactivenet.com) and Computer Associates’ CA Network Management (www.ca.com/us/virtual-management-solutions.aspx).

There appear to be no recently published ratings of fault management and accounting management products. It is, therefore, necessary to search on these terms to identify products and read the descriptions to narrow down the choices.

Configuration management is a weak area in most network management suites. The most widely used configuration management product for network components is SolarWinds’ Configuration Manager (www.solarwinds.com/products). The products can be used to remotely configure routers, switches, firewalls, and wireless access points.

Security management products have gotten a great deal of attention in the past five years. McAfee (www.mcafee.com), the largest company in the computer security field, offers McAfee Total Protection Small Business for organizations with fewer than 100 clients and McAfee Total Protection Enterprise for organizations with 100 or more clients. Total Protection is widely used as a complement to the products of computer manufacturers and network hardware and software manufacturers.

Check Point (www.checkpoint.com), the leader in firewalls, has a security management suite called Check Point Express that addresses all aspects of network security.

Network management products are expensive, ranging in price from several thousand dollars to tens-of-thousands of dollars. For example, the minimum price for the most widely used network management suites is $12,500.

For libraries that cannot afford the commercial network management products, there are
open source options. The Carnegie Mellon University and University of California at Davis developed net-SNMP for handling that protocol. Product development is now supported by a coalition of users. As of the fourth quarter of 2009, the URL was www.net-snmp.org. The toolkit lets users receive data such as network latency, device availability, and throughput, and can set the software to perform some corrections automatically. It is available for free download, but there is no support other than that provided by volunteers who respond to questions asked on the user mail list.

Another widely used open source network management product is Spiceworks (www.spiceworks.com). It is available for free download, but support is limited to exchanges among users.

Two other open source products are supported by commercial firms. They are Zenoss Core (www.zenoss.com/product/network-monitoring) and GroundWork Monitor(www.groundworkopensource.com/products). The cost of training and support can add several thousand dollars to the free open source software.

**Network Management Services**

Many libraries lack staff with the expertise to implement and utilize network management technology. They are, therefore, increasingly turning to network management companies, among the Network Diagnostic Clinic (www.netdiag.com) and NUVO (www.nuvo.com). These companies remotely perform all of the applications a library might perform in-house. Routine applications are undertaken by moderately paid staff, but highly experienced staff are available as needed. While each company offers emergency problem resolution, more typically they undertake a network audit to establish the baselines and then configure a server that is loaded with the appropriate software. They will, if requested, remotely monitor network components and undertake such remedial action as may be necessary. Each of these companies utilizes a combination of products that is far more extensive than that offered by any single vendor of network management products.

Outsourcing network management does have a drawback: it often costs libraries more than they would spend on in-house network management. However, the higher cost does translate into a more consistent level of service and avoids the effects of a possible high turnover in skilled technicians.

Final version prepared November 23, 2009