Challenges of Implementing Network Management Solution

Umesh Hodeghatta Rao
Associate Professor, Xavier Institute of Management, Bhubaneswar
e-mail: umesh@ximb.ac.in

Abstract

A network administrator's efficiency to manage a network decreases as the network becomes more complex and heterogeneous. Managing large, heterogeneous networks created a crisis for many organizations. The network management tools and solutions available are not only expensive but also difficult to install, configure, administer, and maintain. This paper discusses the tools and solutions available for network management, challenges involved in implementing network management solutions and also a simple solution for a pro-active network management solution is proposed. This solution was tested by implementing in a large enterprise. With the implementation, the stakeholders were able to achieve higher efficiency and able to do proactive network management.

Keywords: *Network management, HPOV, NMS, SNMP*

1. Introduction

In the early 1980's, organizations realized the benefits and productivity gains created by networking technology. Many companies began to expand their existing networks as soon as new technology was introduced. Without realizing the pain of managing an unplanned network, organizations had created a complex, heterogeneous network in the organization. There was a tremendous expansion of network deployment throughout the world. Each new network technology, whether it was ATM or Frame relay or Ethernet or VPN or ISDN, required a new set of experts to manage day-to-day network operations. Managing large, heterogeneous networks created a crisis for many organizations and an urgent need for an automated network management solution was felt essential.

As Goers and et al., (2000), stated, activities such as network planning, designing, performance tuning and capacity modeling are required from the business standpoint, base lining network performance, historical usage analysis, SLA reporting and performance management are required from the service management standpoint so as activities such as monitoring, administering network, provisioning and inventory management are required from operations and maintenance standpoint. Network operators have to perform these activities constantly either manually or with the help of network management tools. Since managing enterprise network manually is tedious, time consuming and error prone, network managers heavily rely on the tools to support their daily activities. Either one network management tool must support all the above activities or multiple tools can be integrated to provide these services. In general, network management is a service that assists human network managers in monitoring, troubleshooting and maintaining networks.

Network management is a process of monitoring and controlling the network to ensure that it is operational, works and provides value to the network administrator and its users. ISO has classified the network management activities under five functional areas. They are Fault

DOI : 10.5121/ijdps.2011.2506

management, Configuration management, Performance management, Account management and Security management (FCAPS) (Sidnie Feit, 1995).

Network management architecture consists of a centralized manager and a set of relationships with end stations called managed devices which consist of computer systems and other network devices. Central Network Management Station can poll end devices (managed objects) to check the values of variables related to each of the management functions, which can be either automatic or user-initiated, but agents in the managed devices respond to all polls. All managed devices store their information in a database called Managed Information base (MIB) and run agent software that enable them to communicate with the manager station to support the management functions (FCAPS). Agent software modules first compile information about the managed devices in which they reside, then store this information in a management database, and finally provide (proactively or reactively) to the Network Management Station (NMS) via a network management protocol either SNMP or CMIP.

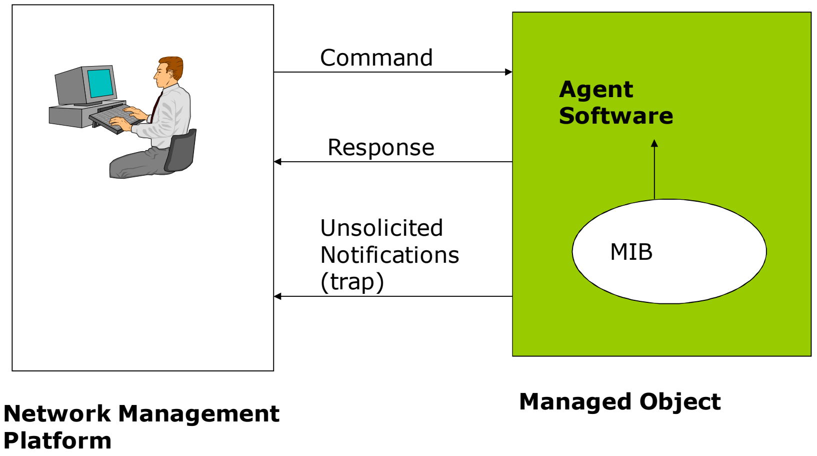

Figure 1: Basic Network Management Architecture

Fault and Problem Management

Network faults can cause downtime, network degradation and hence affect the performance of the network users. The goal of fault management is to detect, log, notify users of the problem and remotely fix the problems to keep the network running effectively. Fault management involves determining faults in the network and isolating the problem. Once the problem is identified, it has to be resolved and the solution tested and deployed on all or just the fault systems (Sidnie Feit, 1995).

Configuration Management

Configuration management function is responsible for remote management of network devices. The goal of configuration management is to monitor configuration information of a device, so that the impact on network operation of various versions of hardware and software elements can be tracked and managed. Example of configuration management elements include: Operating system, Ethernet interface type and version, TCP/IP stack version, SNMP version, etc.. All these configuration management information are stored in a database for easy access. When a problem occurs, this configuration database can be searched for clues that may help in solving the problem. Some of the configurations such as, interface operational status, routing table forwarding information etc, can be configured remotely (Sidnie Feit, 1995).

Performance Management

Function of the performance management is to measure the performance of network components such as hardware, software and media. The goal of performance management is to measure various aspects of performance parameters pertaining to network performance and maintain the network at an acceptable level of performance. Examples of performance measurements include network throughput, percentage of utilization, error rates, user response times and line utilization. Performance management involves setting performance threshold parameters such as interface traffic, TCP connections, number of packets transmitted and received, etc., so that exceeding these thresholds indicates a network problem worthy of attention or investigation. Performance management can be both reactive and proactive. When performance becomes unacceptable, the system reacts by sending a message. In case of proactive management, network simulation can be used to project the network traffic pattern and its growth resulting in appropriate measures being implemented (Sidnie Feit, 1995).

Security Management

The goal of security management is to control the access to network resources according to organizational guidelines so that the network cannot be damaged intentionally or unintentionally. The goal is also to protect sensitive information from being accessed by those without appropriate authorization. A security management system should monitor users logging onto a network resource and prevent access to those who enter without appropriate access codes. Security management system can also work by partitioning network resources as authorized and unauthorized areas. For example, access to human resources data for other departments is inappropriate and hence can be restricted to only that department (Sidnie Feit, 1995).

Account Management

The goal of inventory management/account management is to understand the behavior of the network by having an inventory of users, network devices, bandwidth utilization and analyzing these data to provide insight into current usage patterns. Based on this analysis, usage quotas can be set to individual users or groups. Optimal access points can be reached after several iterations and some correction. Once optimal point is reached, ongoing measurement would yield information related to billing and to assessment of fair and optimal utilization of the resources (Sidnie Feit, 1995).

The OSI management protocol is Common Management Information Protocol (CMIP), and has built-in services called Common Management Information Services (CMIS), that specifies the basic services needed to perform the functions specified above (FCAPS). It is the most comprehensive protocol which addresses all seven layers of OSI Reference Model. Because of the complexity, memory and performance limitations, CMIP protocol is not widely used for managing data communication networks (LAN/WAN). The Internet Engineering Task Force (IETF) proposed a new protocol SNMP (Simple Network Management Protocol) to support the network management functions of ISO, namely – fault management, configuration management, performance management, security management and account management. In contrast to CMIP, SNMP is truly simple, as the name indicates. It started as an industry standard and has since become very much a standard specifications of IETF (Subramanian, 2000).

This paper discusses the challenges involved in implementing the network management solution using commercially available NMS tools and possible solution to implement the same. The solution was implemented in more than one enterprise with strength of more than 1000 full time employees and geographically spread across, with at least three branch offices. All the branch offices were connected through WAN.

2. Background

Managing corporate networks is becoming harder and harder due to the complexity and heterogeneity. The most common and serious problems of a network are the connectivity failures or fault management. The intermittent problem that could also occur as a result of traffic and traffic overload causes delays and packet losses in the network which results in performance degradation.

According to Mani (2000), some of the major challenges in managing networks include staying abreast of the rapid advancement in technology, keeping constant touch with trade magazines, knowledge of vendor product updates and current technology information; analyzing problems with intuition and skill; anticipating customer demands for the network usage; diagnosing problems and outages in a non-disruptive manner; scalability and expanding network issues; keeping the network topology as simple as possible to reduce network administrative overheads; gathering statistics to present to the senior management.

Management functions may be performed explicitly by human operators, but in such cases, most management functions will be performed from a limited number of remote locations. As today's organizations are heavily dependent on a network of computing for their day-to-day transactions and work, there is a great demand for network and system administrators to make sure that the network runs very smoothly, without any hitches and interruptions. The network administrator's job is to maintain the IT infrastructure of the company and to fix any problems that may arise in it whatsoever (www.buzzle.com).

A survey of more than 350 managers conducted by Communication week (Jerry Fitzgerald, 2005) identified following skills for managing networks (network administrators):

Very important skills: Network design, Project management, Knowledge of TCP/IP and routing technologies.

Moderately important skills: Capacity planning, Knowledge of web technologies, Knowledge of windows, UNIX and Novell Netware.

Less important skills: Knowledge of asynchronous transfer mode, Knowledge of frame relay, Knowledge of integrated services digital network and dominos.

4. Current Problem

The key challenge for network managers is to maximize the productivity benefits of the network without significantly increasing the cost of network ownership. The total cost of network ownership includes the cost of support staff to train, implement, operate, and administer the network apart from capital equipment cost and annual maintenance costs. There are plethora of network management tools and solutions available in the market to keep up with the changing business need from networks, and to help organizations in managing their increasingly complex and critical network systems. Some examples include HP Open View, Ciscoworks, CA Unicenter, IBM Tivoli, and Novell ZENwork. All of them use the centralized architecture and SNMP protocol to manage the network. Network management tools have advanced to span heterogeneous networks, protocols and equipment in a complex communications environment of voice, video and data. Most of the products accomplish this by being out of the box, with little or no customization.

HP OpenView (openview.hp.com) is the most widely deployed NMS framework targeted at large, heterogeneous IT environments. The NNM map requires a lot of administrative overhead both the NNM map and message browser are very old-fashioned, the OVO agents are a pain to work with and also they often die down and result in restarting the system quite frequently. The OVO agent install process isn't very smooth. The overall solution is complex to implement and the price makes it less suited for smaller organizations.

If the network is a predominantly Cisco-based network, and needs to be managed with the least amount of effort, then CiscoWorks (CW) is the recommended tool. It does not recognize all the non-Cisco devices and its response is extremely slow. It is based on a proprietary CDP (Cisco Discovery Protocol) protocol and unless one has knowledge of CDP, it is hard to troubleshoot and administer the product.

CA Unicenter (www.ca.com) Network and Systems Management enables customers to ensure the availability and performance of mission-critical services by providing an integrated view of events and notifications of their entire IT infrastructure within the business processes and services. As applications span platforms and servers, the network is the thread that links application components together. The functioning and responsiveness of a network is critical to application availability and performance. This product is expensive and meant only for large enterprises. It requires deep understanding of the technology and protocols, thus making the tool complex.

SolarWinds Orion Network Performance Monitoring tool is also most widely used SNMP based network management product. Easy to install, it has friendly user interface but the function is limited to only Fault Management. In order to support full functionality, it has to be integrated with various other products from the same company, which may turn out to be expensive for an enterprise. In order to unlock and understand all the features, the tool needs further customization.

Nagois (www.nagois.org) is a Linux based Open Source tool which is most widely used today. Though the basic installation is simple and easy to install but most of the tool configuration has to be done manually. The user interface is not user friendly and requires not only networking skills but also Linux administrator skills. The Web GUI, complexity of the tool, does not make a real world IT NMS solution. However, it is an Open source tool and hence available for free.

These commercial products are not only expensive but also tend to be difficult to install, configure, administer, and maintain. Also the solution is expensive. Though the network management products and solutions have been available for many years, it is observed that, due to their high cost and complexity:

- Many companies have failed to deploy
- Many companies have deployed partial solution with a low-end monitoring systems

- Many companies have not deployed any formal monitoring technology
- Many companies have abandoned the attempt to deploy them

5. Solution

Most of the organizations are stuck with reactive mode due to the complexities of using the existing network management tools. At the same time, business users are more service-focused and less particular about the underlying technology. Organizations demand reliable network maintenance support services that help to get their job done. In spite of using the latest gigabit network hardware, enterprises are plagued with intermittent bandwidth issues, performance issues, and complaints from users of slow network response.

Network management solutions should overcome the cost and complexity concerns that have kept organizations from implementing them by a simple GUI, rapid and easy implementation, reduced overall investment, strong industry standards basis, operational model with data center management experience, simple licensing, technology to support Internet-enabled technology, a single interface for 24 x 7 control.

The basic steps of defining a deployment strategy, for proactive network management solution, is to start with the fault management activities and then slowly move to performance management, then configuration management and finally to reach the goal of proactive network management (Umesh H and Sanjay M, 2010).

It is imperative to refine the configurations until network management station fully reflects the entire enterprise network topology. The following table (table 1) describes minimum parameters to be monitored for fault, performance and configuration:

Table 1: Sample Network Management Parameters

Fault Management	**Object Identifier**	**Example**
Contact and location change (any change should trigger n alarm)	iso.internet.internet.internet.mgmt.mib-2.system.sysLocation (1.3.6.1.2.1.1.6.)	SNMPv2-MIB::sysLocation.0 -IT lab - floor 5 – Conference Room
System Up Time (The time system was last re-initialized)	iso.internet.internet.internet.mgmt.mib-2.system.sysUpTime (1.3.6.1.2.1.1.3.)	(CISCO Router) DISMAN-EVENT-MIB::sysUpTimeInstance: 96:23:13:02.14
Interface added or deleted (number of interfaces on the system)	iso.internet.internet.internet.mgmt.mib-2.interfaces.ifNumber(1.3.6.1.2.1.2.1.)	IF-MIB::ifNumber.0::16
Interface Administrative Status (desired state of the interface)	iso.internet.internet.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus - (1.3.6.1.2.1.2.2.1.7.)	
Interface Operating Status (Operational status of the interface)	iso.internet.internet.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus - (1.3.6.1.2.1.2.2.1.8.)	
Link address change, Network mask change (any changes to IP address)	iso.internet.internet.internet.mgmt.mib-	

	2.ip.ipAddrTable.ipAddrEntry.ipAdEntAddr - (1.3.6.1.2.1.4.20.1.1.) iso.internet.internet.internet.mgmt.mib - 2.ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask - (1.3.6.1.2.1.4.20.1.3.)	

Performance Management Parameters	**Object Identifier**
Total Packets (octets) received on an interface (The total number of octets received on the interface)	iso.internet.internet.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets - (1.3.6.1.2.1.2.2.1.10.)
Total Packets (octets) transmitted on an interface (The total number of octets transmitted out of the interface)	iso.internet.internet.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets (1.3.6.1.2.1.2.2.1.16.)
Interface Errors (input) (The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol)	iso.internet.internet.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInErrors = (1.3.6.1.2.1.2.2.1.14.)
Interface Link speed (An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth)	iso.internet.internet.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifSpeed (1.3.6.1.2.1.2.2.1.5.)
Interface Average Packet Size (The size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface)	iso.internet.internet.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifMtu (1.3.6.1.2.1.2.2.1.4.)
TCP segments received (The total number of segments received, including those received in error)	iso.internet.internet.internet.mgmt.mib-2.tcp.tcpInSegs = (1.3.6.1.2.1.6.10.)
TCP segments transmitted (The total number of segments sent, including those on current connections)	iso.internet.internet.internet.mgmt.mib-2.tcp.tcpOutSegs = (1.3.6.1.2.1.6.11)

Other Parameters	**Object Identifier**
IP Addresses	iso.internet.internet.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry.ipAdEntAddr= (1.3.6.1.2.1.4.20.1.1.)
TTL Value (The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol)	iso.internet.internet.internet.mgmt.mib-2.ip.ipDefaultTTL (1.3.6.1.2.1.4.2.)

Performance Management derivations:

1. Percent of bandwidth utilization on an interface

$$\frac{(\text{received byte rate} + \text{transmitted byte rate}) * 8}{\text{Interface link speed}} \quad \text{X } 100$$

2. Absolute traffic on an interface

(Received byte + transmitted byte)

3. Percentage of error packets (in)

$$\frac{\text{Input error rate}}{\text{Total packets received}} \quad \text{X } 100$$

4. Input Utilization = $\dfrac{\blacktriangle\text{ifInOctets X 8 X 100}}{(\text{number of seconds in } \blacktriangle) \text{ x ifSpeed}}$

5. Output Utilization = $\dfrac{\blacktriangle\text{ifOutOctets X 8 X 100}}{(\text{number of seconds in } \blacktriangle) \text{ x ifSpeed}}$

6. Interface Throughput = Total packets received/Total Packets sent X 100

▲ = change

6. Conclusion

As the network becomes larger and complex, it is harder and harder to manage due to the complexity and heterogeneity. The most common and serious problems of a network are the connectivity failures or fault management. Network management solutions should be simple to implement and cost effective. They should have a simple GUI, rapid and easy implementation and should reduce overall investment. Network managers and administrators should be able to effectively use the tool to perform network monitoring, performance management and configure devices remotely from one central point to manage network devices in multiple sites. In this paper, one such network management solution implemented using HP Open View is discussed. This implementation resulted in reduced downtime of network devices, higher performance of networks and finally faster, more predictable response times due to proactive network management. The implementation was smooth and appreciated by all the stakeholders.

References

1. Aiko Pras, Jurgen Schonwalder, Mark Burgess, Oliver Festor, Gregorio Martinez Perez, and Burkhard Stiller, "Key Research Challenges in Network Management", IEEE Communication Magazine, October 2007

2. Kristian Hjort-Madsen, "Enterprise Architecture Implementation and Management: A case study on Interoperability", Proceedings of the 39th Hawaii International Conference on Systems Sciences, 2006

3. Jim Metzler Ashton, "The Changing Role of the Network Adminsitrator", Metzler & Assocaites, Lpswitch.com, 2010

4. Michael L Lewis, United States Patents and Trademark, Patent No. US 7274677B1

5. S.F.Bush and S. Kalyanaraman," Management of Active and Programable networks", Journal of Networks and Systems Management, Vol. 14, No.1, pp 1-5, March 2006

6. Alok Gupta, Dale O Stahl, and Andrew B Whinston, "The Economics of network management", Communications of ACM, Vol 42, No.9, September 1999

7. Umesh H Rao and S Mohapatra, "Deploying Network Management Solutions in Enterprises", IEEE Proceedings, International Conference on Networked Computing (INC) 2010

8. Ciprian Popoviciu, Petre Dini, "IPV6 as a practical solution to Networm Management Challenges", Proceedings of the International Multi-Conference on Computing in the Global Information Technology (ICCGI'06), 2006

9. "Making the Best of a Difficult Situation", Communication Week, 2006

10. Asta Dogra, "Tope 10 jobs in Demand", http://www.buzzle.com/articles/top10-jobs-in-demand.html, July 2010

11. Jerry Fitzgerald and Alan Dennis, "Business Data Communication Network", Eighth edition, Wiley-India, 2009

12. Dr. Sidnei Feit, "SNMP: A Guide to Network Management", McGraw-Hill International Edition, 1995

13. Mo Li and Kumbesan Sandrasegaran, "Network Management Challenges for Next Generation Networks", IEEE Conference on local computer Networks, 2005;

14. Case, J., Fedor M., Schffstall, M., Davin, J., " A Simple Network Management Protocol", RFC 1157, May 1990

15. Leinwand, A., Fang, K., "Network Management: A Practical Perspective", Addison Wesley, 1993

16. Manifred, R. Siegl, Georg Trausmuth., "Hierarchical network management: a concept and its prototype in SNMPV2", 6th Joint European Networking Conference, February 1996, Volume 28, Issue 4, p441-452

17. Goers, William C., Brenner, Michael R., "Implementing a Management System Architecture", Bell Labs Technical Journal, Oct-Dec 2000, Vol. 5, Issue 4, p31-43

18. Mohesen Kahani, H.W., Peter, “Decentralized Approaches for Network management”, ACM SIGCOMM
19. Paolo Bellavista, Antonio Corradi., and Cesare Stenfanelli., “An Integrated Management Environment for Network Resources and Services”, IEEE Journal of Communications, Vol 18, No 5, May 2000
20. Ankur Gupta, “Network Management: Current Trends and Future Perspectives”, Journal of Network and Systems Management, Vol 14, No4, December 2006
21. White Paper Cisco systems; www.cisco.com