

Overview of Network Management

Addicam.V.Sanjay

Abstract

Overview of Network Management 2

This paper attempts to present an overview of Network Management. This paper will attempt to address the issues like what is Network Management, what is it made up of and where is it used. The paper will deal with the various standards used in Network Management. The paper will also look into the various tools and systems available for Network Management. It will also look into the drawbacks of existing Network Management methods. The author will also suggest ways in which the limitations of the current Network Management methods can be overcome. The paper will also look into the future of Network Management.

What is Network Management???

Network management means different things to different people. In some cases, it involves a solitary network consultant monitoring network activity with a protocol analyzer. In other cases, network management involves a distributed database, auto polling of network devices, and high-end workstations generating real-time graphical views of network topology changes and traffic. In general, network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks. (Cisco, 2002)

What are the various aspects of Network Management???

Network Management involves three main divisions. They are

1. Network Provisioning.
2. Network Operations.
3. Network Maintenance.

What is Network Provisioning???

Network Provisioning involves planning of the network. In you work place, this involves, planning about the type of servers to use through out the network. (The servers may be Windows 2000 servers or Novell servers or Linux servers or some thing else.) It involves decisions on the type of physical connection to use. (The physical connection may be Ethernet, fiber access, coaxial etc). It involves decision about company wide wireless access or wireless access only to executives. It involves decision about the type of network security package to by deployed.

In other words, Network provisioning is all about planning and designing a network.

What is Network Operations???

Network Operations involves the day to day handling of the various operations of a network. All these operations are handled from a central Network Operations Center (NOC).

The day-to-day operations of a Network are

1. **Fault Management:** This involves detecting and correcting the faults in a network. For example, in a network, some one might have accidentally plugged in a non-official DHCP server. This DHCP server may be giving out all sorts of erroneous IP addresses, which might be incompatible with the existing network setup. This has the potential to bring the entire network down. Fault management involves tracking down the root cause of this fault and its location. This translates to finding out, in the vast corporate network, the office or the cube, in which the delinquent DHCP server is present. This also involves the resources needed in shutting down the concerned DHCP server.
2. **Configuration Management.** Configuring Management involves configuration of the network. This may involve the Sub netting of a particular Segment of the network with some IP address. This may involve adding the email address of a new employee to the company email list. This may also involve a company wide policy about the way in which email addresses are assigned. For example one company may have a policy where a new employee john doe might get an email address john.doe@company.com. Another company may have a policy where the employee may get an email address doe.john@company.com.

Configuration management also involves keeping track of any major change of software in the future and planning for it. For example a company might decide to move from windows me to windows xp operating system. Configuration management is responsible for planning for this move and migrating the computers from one operating system to another, without the computers losing their individual unique configuration data.

3. **Security Management:** Security Management is responsible for protecting the network from the threats of Viruses, Hackers etc. Security Management is responsible for monitoring the various fixes available for different viruses and incorporating these fixes into the network. Security Management is also responsible for creating firewalls and proxy servers and protecting the corporate network from attacks.

They are also responsible for monitoring the network for objectionable material access (pornographic) and stopping these accesses. The Security Management division is also not responsible for the access to applications. Let us assume that there is software, which is used to store the current salaries of all the employee's. The security Management division is not responsible for granting and managing access to this software.

4. **Performance Management:** Performance Management data, as the name suggests, is responsible for measuring the performance of the network. A company may have a corporate network dial up facility to encourage telecommuting. The performance team is responsible for measuring the average dial up speed to the corporate network from different cities. They are responsible for identify network

bottlenecks at different points and correct. Dial up speed measurement is just one aspect. Performance management team is responsible for measuring the network utilization, average response time in a certain segment, the classification of data flowing in the networks, network patterns (example 80% of the data flowing in the network is html requests for www.cnn.com, www.msnbc.com etc. 20% of the data flowing is to the company bug reporting web site). These traffic statistics is can be used to predict future network growth and plan for it.

5. Accounting Management: This is used to allocate resources of network to different groups. Metrics are used to measure the resources allocated to different groups. For example Group A has been given 40 routers, Group B has been given 20 routers. These resources are tracked, measured and accounted for by the Accounting department.

What is Network Maintenance???

Network Maintenance is the group responsible for the maintenance and installation of corporate networks. This is the team, which is responsible for laying of the coaxial cable all across the corporate network. This is the team, which periodically services the printers and zerox machines in a big corporation. This is the team, which actually implements, the plans designed by the network provisioning team. These teams are responsible for the periodic update of software's in some legacy systems.

This team works closely with the help desk team. When you call up the help desk at office and report that your computer is not working. A representative of the Network maintenance group will turn up at your desk and resolve the

problem. This team usually is made up of specialists, who have Microsoft accreditations or CISCO Networking certificates.

What are the current Network Management standards???

1. CMIP:

CMIP is Common Management Information Protocol. This protocol was constructed with the OSI stack in mind. There have been numerous problems with the implementation of CMIP, so it was never implemented. CMIP is an object-oriented protocol with a greater control of the network. CMIP has 11 types of command to acquire various types of statistics from the network.

The Advantages of CMIP:

- a. CMIP can be used to control network systems in a manner, which is far more superior to its nearest competitor, SNMP.
- b. CMIP was built on its nearest competitor SNMP (another network management standard, which is explained later). Hence it overcomes many of the problems, which are present in SNMP. Problems like security management devices that support authorization, access control and security logs.
- c. Not only governments, but also large corporations funded CMIP.

Disadvantages of CMIP:

- a. CMIP is 10 times more resource intensive than its nearest competitor, which is SNMP.
- b. CMIP is a very complex protocol, which is very difficult to program and control.

2. SNMP:

SNMP is Simple Networking Management protocol. This protocol was supposed to be a temporary fix before CMIP was implemented. CMIP was never implemented and SNMP became the most popular Network Management Protocol. SNMP has a very simple, and straightforward architecture. It has around 5 commands to control the various network elements.

There have been many versions of SNMP. SNMPv1 was the earliest version of SNMP. It proved to be very popular. It also was vulnerable, in the sense that it had no security. To improve upon this situation SNMPv2 was created. SNMPv2 turned out to be too very complex and not compatible with SNMPv1. Because of this SNMPv2 was not implemented. SNMPv3 is the latest version, which has corrected all the security flaws of SNMPv1. It is also backward compatible with all the previous versions of SNMP. SNMPv3 has proved to be very popular and is widely implemented.

Advantages of SNMP:

- a. It is in very wide use today. So you find a number of products related to SNMP.
- b. SNMP is a very simple protocol. Hence it is very easy to extend this protocol with enhancements. The design of SNMP is very simple.

Disadvantages of SNMP:

- a. SNMP is not a particularly efficient protocol. There is a number of useless information and the information in some of the directives is oversized. Because of this Network bandwidth is wasted.

3. TMN: Telecommunication Management Network is a standard proposed by the International Telecommunications Union-Telecommunications (ITU-T) in 1986. This standard was created to address the interoperability of multi vendor equipment used by service providers and to define standard interfaces between service provider operations. (Subramanian , 2000)
4. IEEE: This is Network Management standard which is supported by IEEE (Institute of Electrical and Electronic Engineers). This standard works with the OSI architecture in mind. This standard addresses the address management of LANs and MANs. This standard works with the physical and data link layer of the OSI model.
5. WBEM: WBEM is Web Based Enterprise Management. This is a standard, which plans to manage network systems across multi vendor environments. The unique selling point of the web based enterprise management helps in taking away the dependency from one centralized management console. This standard is compatible with all the existing network management standards like SNMP, CMIP etc. This standard is being promoted by DMTF (Distributed Management Task Force, Inc).

WBEM plans to have a web Server in all the monitored devices like Gateways, Hubs, Routers etc. These Web Servers will be acting as Management agents and controlling the device. The web servers can be controlled and managed by any given Web browser. Microsoft has a scheme called Common Information Model (CIM). This model helps in integrating the existing standards like CIM and SNMP.

6. JMX: Java Management Extension is a management standard which is similar to WBEM. This standard also aims to be a distributed management console, which is compatible with existing network management standards and works with multi vendor environment. This standard was proposed and is being promoted by SUN.

What are the different Network tools, which are available???

Network Tools are tools, which are used to test some aspect of a given network.

Here are some of the popular network tools and their functionality

1. Ping: This is the most popular tool in the networking community. This tool is used to test the connectivity between two systems. This tool is also used to calculate the average response time between two systems.
2. Trace route: This is a tool, which is used to find out the route taken by a packet. Let us assume that there are two systems A and B, separated by a huge network. A packet travels from A and B. Trace route helps in finding the route taken by the packet from A to B.
3. If config : A computer may have interfaces(connections) to multiple networks. This command helps in finding the various details of an interface. Details like IP address, MTU etc
4. Protocol Analyzer: A protocol Analyzer is a tool, which captures packets going on the wire, and analyzes them into various protocols. Netmon, Sniffer, Lan Analyzer etc are some of the common commercial network protocol analyzers.

5. **Packet Generators:** Packet Generators are tools, which are used to fabricate various types of packets and put them in a network. For example, a Packet generator can generate a PING packet and put it on the wire. These packet generators are very good in testing a network. Eg; SmartBits is a commercial Packet Generator.
6. **MIB-Browser:** This a tool, which is used to issue SNMP, commands to the network. Mg-Soft, Silver creek are some of the popular, commercial software.

There are many other Network Tools. These tools can be classified according to the following category

1. The functionality of the tool. The tool may be used to test the security of a link or to monitor traffic on a link or to act as a network manager etc.
2. The Resource or the component monitored or managed by the tool. The tool may be used on bridges or on LAN's or on WAN's etc.
3. The mechanism or the Network Management standard, used by the tool in monitoring the network.
4. The operating system or operating Environment of the tool.
5. The method in which the tool can be acquired. A tool may be freely available or the tool may be a commercial software product.

What is a Network Management System?

A network Management system (NMS) is an automated system tool that helps networking personnel performs their function efficiently. (Subramanian, 2000)

A network Management system has the following five associated components

1. **Hardware:** This is the Machine on which the network management system works. This may be a SunSparc Work station or an Intel Pentium processor or a Hewlett-Packard HP 9000 workstation.
2. **Operating System:** This is the operating system used by the Network Management system. Operating system like Linux, Windows, Unix etc.
3. **Core Application Service:** This is the part of the Network Management System, which is visible to the user. This is the part of the NMS, which displays the network being monitored, and the status of the various network components.
4. **Common SNMP services:** This is the SNMP manager part of the Network Management System. This is responsible for the complete processing of various types of SNMP related functions. This part is also responsible for handling various SNMP version (SNMPv1, SNMPv2 etc) messages.
5. **Vendor-Specific NMS services:** This is the component, which is customized to suit the needs of one particular vendor. Every vendor may have some proprietary MIBs (Management Information Base) or some particular configuration setting. These components are handled by the Vendor-Specific NMS services.

Some of the commercial Network Management Systems are Hewlett-Packard's Open View Network Node Manager, Cabletron's Spectrum Platform etc.

What are the shortcomings of the current Network Management practices???

1. **Improper Statistics collection:** Let us assume that the some executive wants to know the average response time of the network. At this point of time, it involves, sending out ping or ICMP echo packets to all the systems in the network. The ping or echo packets can calculate the individual response time. Taking the addition of all the response times and dividing it by the number of network systems calculates the average network response time.

The average response time might be an optimistic figure, but it might not be a true indicator of the network response. Some of the systems in the network may be high availability back up servers, whose response times may be not good. This problem is masked in the way in which we calculate average response time. The importance or the priority of certain devices is not considered in calculating the average response time.

Solution:

All the devices should be given a priority. This priority must be reflected in the manner in which statistics are calculated. This priority is applicable to all sorts of network calculations, calculations like network utilization, bandwidth consumption etc.

2. **Help Desk Interaction with Network Management Systems:**

Most of the corporations have the very latest Network Management tools. These tools are not always available to the Help Desk. Help Desk are the first line of contact for network problems. If the help desks do not have the latest network management tools, it will delay the response time of the help desk.

Solution: Help desk folks should have easy access to all Network management tools.

Future of Network Management!!!!

Network Management has an interesting concept called as Remote Monitoring (RMON). These are intelligent agents, which are distributed, in different corners of a network. These agents monitor and analyze various characteristics of a network. They raise an alarm to the central network manager, only when needed. RMONs have two major advantages: They help in reducing the network management traffic, which would normally flow towards the central network manager. Since RMONs are present physically in different network segments, they are better positioned to make a more accurate assessment of the Network segment's help. RMONs are going to play a very important role in the future. Network Management will move more towards RMONs in the future.

SNMPv3 is undergoing modifications to support various types of Network Management Environments. It is also undergoing changes to support Quality of Service Requirements. Quality of Service will play a very important role in the future. SNMPv3 is gearing up towards it.

Web-Based Management Systems will also become very popular in the future. WBEM and JMX, with their ability to work in a distributed environment is the right step towards the future. It takes the dependency away from one central monitoring console.

At this point of time, let us consider a network operation engineer John Doe. John is responsible for maintaining all the routers of his office. He can, presently do this with the help of SNMP. A SNMP browser is loaded on to one particular machine; John has to make use of this machine to monitor the health of the routers. If John is traveling, dependency on a single machine becomes a major inconvenience.

With web based management systems like WBEM or JMX, this dependency is removed. For example, John Doe can log into the website www.Monitormyrouters.com, from any machine, and monitor his routers. The web site can be linked to a web based enterprise management suite, which can talk either SNMP or CMIP and can publish the management results in a web-based format.

Conclusion

Network Management is a vast area with many interesting concepts. As we become more and more dependent on the Internet and the network around us for the various aspects of our life, it becomes more than imperative to have a healthy data and telecommunication network around us. Network Management is a very important aspect in maintaining, monitoring and restoring the health of a network. There are many tools and standards available to assist in managing a network.

References

(I have cited articles from these two references in my research paper.)

Cisco (2002). Network Management Basics. Retrieved June 12 2004, from the World Wide Web:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm#xtocid3

Subramanian, Mani. (2000). Network Management: Principles and practice, Addison Wesley, Massachusetts.

(I have referred these references, when researching my paper, but I did not find an opportunity to cite from the articles at these references.)

Comer, Douglas. (1997). Computer Networks and Internets, Prentice Hall, New Jersey.

Guild Soft. (2000). Network Management –Scope of a CMIP stack. Retrieved June 12 2004, from the World Wide Web:

<http://www.guildsoftindia.com/nms.htm>

Stevenson, Douglas. (1995). Network Management: What it is and what it isn't. Retrieved June 12 2004, from the world wide web:<http://netman.cit.buffalo.edu/Doc/Dstevenson/>

Stevens, Richards. (1999). TCP/IP Illustrated Volume 1: The protocols, Addison Wesley, Massachusetts.

Tabor, Daniel. (1995). Network Management Lesson 27. Retrieved June 12 2004, from the World Wide Web:

<http://www.cs.njit.edu/~cis456/protected/lesson27/single27.html>

Unknown. (????). SUMMARY: Retrieved June 12 2004, from the World

Wide Web: <http://www.geocities.com/SiliconValley/Horizon/4519/work.html>