Present and Desired Network Management to Cope with the Expected Expansion, NM-AIST Study Case.

Shadrack Stephen Madila, George Sizya Germinous, Sarah Nyanjara Magoti
ICT department, Moshi University College of Co-operative and Business Studies
P. o. box 474 Moshi, Tanzania

Abstract

The network management as defined by the International Standards Organization (ISO) has five functional areas of network management. In this work we explore all functional areas for the present and desired network management to cope with the expected expansions. We provide recommendations on each functional area to increase the overall effectiveness of current and future management tools and practices for the NM-AIST (Nelson Mandela African Institute of Science and Technology) network. The design guidelines for future implementation of network management tools are also explored.

ABBREVIATIONS

- *NMS – Network Management System.*
- *ISO–International Standards Organization*
- *SNMP – Simple Network Management Protocol.*
- *MIB – Management Information Base.*
- *SLA- Service Level Agreement*
- *CORBA – Common Object Request Broker Architecture and*
- *RMON- Remote Monitoring.*
- *IOS – Internetworking Operating System.*
- *IDS – Intrusion Detection System.*
- *IPS – Intrusion Prevention System.*
- *NM-AIST- Nelson Mandela African Institute of Science and Technology*

Introduction

The ISO network management model's five functional areas include [1]:-

I. Fault Management for detection, isolation, notification, and correction of faults encountered in the network.
II. Configuration Management for configuration aspects of network devices, reconfiguration and documentation.
III. Performance Management for monitoring and measuring various aspects of performance such as capacity, traffic, throughput and response time so that overall performance can be maintained at an acceptable level.
IV. Security Management for controlled access to network devices and corporate resources by authorized individuals.
V. Accounting Management for controlled usage of network resources.

The following figure outlines a reference architecture that should be a minimal solution for managing a data network. This architecture includes a Call Manager server for managing Voice over Internet Protocol (VoIP); it also shows how to integrate the Call Manager server into the NMS topology.

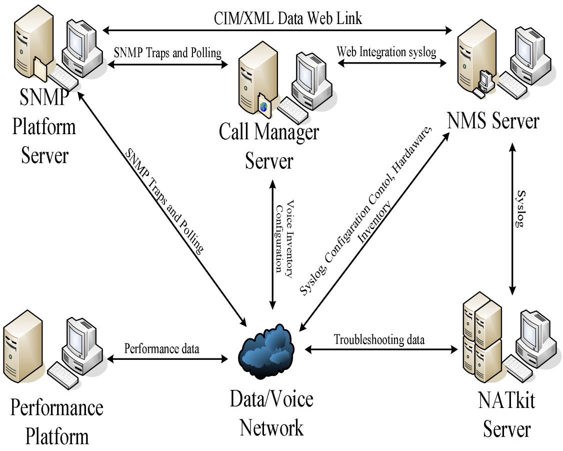

Fig. 1: Reference Architecture for NMS The network management architecture

The network management architecture include the following :-

I. Simple Network Management Protocol (SNMP) platform for fault management.
II. Performance monitoring platform for long term performance management and trending.
III. Server for configuration management, syslog collection, and hardware and software inventory management (documentation).

Some SNMP platforms can directly share data with the server using Common Information Model/eXtensible Markup Language (CIM/XML) methods. CIM is a common data model of an implementation neutral schema for describing overall management information in a network/enterprise environment.

XML is a markup language used for representing structured data in textual form. XML is similar in concept to HTML, but whereas HTML is used to convey graphical information about a document, XML is used to represent structured data in a document.

Fault Management

The goal of fault management is to detect, isolate, notify users of, and (to the extent possible) automatically fix network problems to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements.

Network Management Platforms

Network management platform deployed manages an infrastructure that consists of multivendor network elements. The platform receives and processes events from network elements in the network [1]. Commonly available functions in a standard management platform include:-

I. Network discovery
II. Topology mapping of network elements
III. Event handler
IV. Performance data collector
V. Management data browser

Network management platforms can be viewed as the main console for network operations in detecting faults in the infrastructure. The ability to detect problems quickly in any network is critical. Network operations personnel can rely on a graphical network map to display the operational status of critical network elements such as routers and switches.

Network management platform such as HP OpenView can perform a discovery of network devices. Different colors on the graphical elements represent the current operational status of network devices. Network devices can be configured to send notifications, called SNMP traps, to network management platforms. Upon receiving the notifications, the graphical element representing the network device changes to a different color depending on the severity of the notification received. These notifications are placed in a log file. It is particularly important that the most current Management Information Base (MIB) files be loaded on the SNMP platform to ensure that the various alerts from devices are interpreted correctly.

A number of network management platforms are capable of managing multiple geographically distributed sites. This is accomplished by exchanging management data between management consoles at remote sites with a management station at the main site. The main advantage of a distributed architecture is that it reduces management traffic, thus providing a more effective usage of bandwidth.

A recent enhancement to management platforms is the ability to remotely manage the network elements using a web interface [1]. This enhancement eliminates the need for special client software on individual user stations to access a management platform.

A typical enterprise is comprised of different network elements. However, each device normally requires vendor specific element management systems in order to effectively manage the network elements. Therefore, duplicate management stations may be polling network elements for the same information. The data collected by different systems is stored in separate databases, creating administration overhead for users. These limitations prompt the adoption of standards such as Common Object Request Broker Architecture (CORBA) to facilitate the exchange of management data between management platforms and element management systems.

CORBA specifies a system that provides interoperability between objects in a heterogeneous, distributed environment and in a manner that is transparent to the programmer.

Fault Detection and Notification

The purpose of fault management is to detect, isolate, notify, and correct faults encountered in the network. Network devices are capable of alerting management stations when a fault occurs on the systems. An effective fault management system consists of several subsystems. Fault detection is accomplished when the devices send SNMP trap messages, SNMP polling, remote monitoring (RMON) thresholds, and syslog messages. Upon receipt of alerts corrective actions can be taken. A periodic review of configured traps ensures effective fault detection in the network.

The current NM-AIST network does not have any Fault Management mechanism installed, yet. But fault detecting device is a proposed solution and this will serve well the purpose to monitor the faults as they occur on the network, detect, isolate, and notify the users of the network and for some simple issues, automatically fix them.

This is a necessity because the NM-AIST network is growing and is likely to grow to the extent when it will be impossible to manually find the fault devices and fix them.

Furthermore, Fault detection and monitoring of network elements can be expanded from the device level to the protocol and interface levels. For a network environment, fault monitoring can include Virtual Local Area Network (VLAN), asynchronous transfer mode (ATM), fault indications on physical interfaces, and so forth. Protocol-level fault management implementation is available using an element management system such as the **CiscoWorks2000 Campus Manager**.

As the network grows, an event management system that is capable of correlating different network events (syslog, trap, log files) may be considered. This architecture behind an event management system is comparable to a Manager of Managers (MOM) system. This allows personnel in the network operations center (NOC) to be proactive and effective in detecting and diagnosing network issues. Event prioritization and suppression allow network operation personnel to focus on critical network events.

Configuration Management

The goal of configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

Configuration Standards

Naming conventions for network devices, starting from device name to individual interface should be planned and implemented as part of the configuration standard. A well defined naming convention provides personnel with the ability to provide accurate information when troubleshooting network problems. The naming convention for devices can use geographical location, building name, floor, and so forth. For the interface naming convention, it can include the segment to which a port is connected, name of connecting hub, and so forth. On serial interfaces, it should include actual bandwidth, local data link connection identifier (DLCI) number (if Frame Relay), destination, and the circuit ID or information provided by the carrier.

Configuration File Management

Additional of new configuration commands on existing network devices requires verifying the commands for integrity before actual implementation takes place. An improperly configured network device can have a disastrous effect on network connectivity and performance. Configuration command parameters must be checked to avoid mismatches or incompatibility issues.

So far, in the NM-AIST networking environment; the configurations for the devices are done using only the built in software that comes with the devices; for instance the **Internetworking Operating System (Cisco IOS)** that comes with **Cisco devices.** And they are performed remotely using the terminal programs using either *telnet* or *ssh* protocols for remote access of the devices. The changes made on the routers and switches can be tracked using the features built in the IOS but this is limited only to manage the configurations on the devices.

The dynamic listing of all the devices in the network, and the software versions in the various devices are not supported at all in the current NM-AIST network.

For the expected expansion in the network management; the **inventory management** and the **software management** mechanisms are to be implemented and they are of great necessity as detailed in the following paragraphs.

Inventory Management

The discovery function of most network management platforms is intended to provide a dynamic listing of devices found in the network. Discovery engines such as those implemented in network management platforms should be utilized for such purposes.

An inventory database provides detailed configuration information on network devices such as models of hardware, installed modules, software versions e.t.c. The up to date listing of network devices collected by the discovery process can be used as a master list to collect inventory information using **SNMP** or **scripting**.

Software Management

Successful upgrade software on network devices requires a detailed analysis of the requirements such as memory. The upgrade window to complete device maintenance is fairly limited for some organizations. In a large network environment like the expected NM-AIST with limited expensive resources, it is recommended to schedule and automate software upgrades after business hours.

Changes to software in network devices should be tracked to assist in the analysis phase when software maintenance is required. With an upgrade history report readily available, the person performing the upgrade can minimize the risk of loading incompatible software into network devices.

Performance Management

Service level agreements (SLA) are written between a service provider and their customers on the expected performance level of network services. The SLA consists of metrics agreed upon between the provider and its customers e.g. capacity, Traffic, throughput and response time.

Various interface statistics can be collected from network devices to measure the performance level. These statistics can be included as metrics in the SLA. At the device level, performance metrics can include CPU utilization, buffer allocation (big buffer, medium buffer, misses, hit ratio), and memory allocation.

There is no mechanism that is running currently in the NM-AIS network to for performance management. There is, however a proposal to purchase and deploy **Riverbed Bandwidth manager** that is meant to measure the network performance, to limit the bandwidth usage and monitor the performance of the other installed applications on the network.

In addition to this Bandwidth Manager to perform all those management tasks; SNMP will still play an important role in monitoring, measuring and reporting the performance of the devices and applications on the network as discussed below.

Performance Monitoring, Measurement, and Reporting

Different performance metrics at the interface, device, and protocol levels should be collected on a regular basis using SNMP. The polling engine in a network management system can be utilized for data collection purposes. Most network management systems are capable of collecting, storing, and presenting polled data. The response time can be measured between the source and the destination or for each hop along the path. SNMP traps can be configured to alert management consoles if the response time exceeds the predefined thresholds.

Performance Analysis and Tuning

In many networks user traffic increases rapidly and places a higher demand on network resources. Network managers typically have a limited view on the types of traffic running in the network. Two technologies for that matter, **RMON probes** and **NetFlow**, all from Cisco, provide the ability to collect traffic profiles.

Data gathered on network devices are exported to a collector. The collector performs functions such as reducing the volume of data (filtering and aggregation), hierarchical data storage, and file system management.

Security Management

The goal of security management is to control access to network resources according to predefined policies so that the network cannot be sabotaged (intentionally or unintentionally). A security management subsystem can monitor users logging on to a network resource, refusing access to those who enter inappropriate access codes.

A good security management implementation starts with sound security policies and procedures in place. It is important to use a platform with minimum configuration standard for all routers and switches that follow industry best practices for security performance.

The Security mechanism that are implemented on the NM-AIST network presently include the configured Firewall on the routers, the Access control lists to filter the communications in and out the network. And there are plans to change the network management strategy from the workgroup to a domain system of managing the network. This will ensure central management of users and devices on the domain by the use of the Active Directory services.

Some more features can be deployed in order to manage the increased users and devices in the NM-AIST network that is expected to grow over the years. This includes some mechanisms for **detecting** and **preventing** intrusions on the network (i.e. **IDS** and **IPS – Intrusion Detection System** and **Intrusion Prevention System**), some mechanisms for Authentication, Authorization and Accounting should be implemented as well. The server for this purpose that is generally referred to as AAA Server should be configured to serve the functions discussed below.

Authentication

Authentication is the process of identifying users, which includes login and password dialog, challenge and response, and messaging support. Authentication is the way a user is identified prior to being allowed access to the router or switch. There is a fundamental relationship between authentication and authorization. The more authorization privileges a user receives, the stronger the authentication should be.

Authorization

Authorization provides remote access control, including one time the user for each service that requests authorization and authorization. It is an act of permitting access to a resource based on authentication information in the AAA Model.

Accounting

Accounting allows for the collecting and sending of security information used for billing, auditing, and reporting, such as user identities, start and stop times, and executed commands. Accounting enables network managers to track the services that users are accessing as well as the amount of network resources they are consuming. Accounting provides auditing and logging functionalities to the security model.

Accounting Management

Accounting management is the process used to measure network utilization parameters so that individual or group users on the network can be regulated appropriately for the purposes of accounting or charge back. Similar to performance management, the first step toward appropriate accounting management is to measure the utilization of all important network resources.

Presently; Accounting Management is not in place at all in the NM-AIST network for controlled use of resources. There are plans to utilize the Bandwidth Manager (*Riverbed*) that is yet to be purchased and deployed on the network. Extensive accounting and billing systems are of great importance to cope with the expected expansion of the network.

A usage based accounting and billing system is an essential part of any service level agreement (SLA). It provides both a practical way of defining obligations under an SLA and clear consequences for behavior outside the terms of the SLA.

NetFlow Activation and Data Collection Strategy

NetFlow (network flow) is an input side measurement technology that allows for capturing the data required for network planning, monitoring, and accounting applications. NetFlow should be deployed on edge/aggregation router interfaces for service providers or WAN access router interfaces for Enterprise customers.

Recommendations are made for a carefully planned NetFlow deployment with NetFlow services activated on the strategically located routers. NetFlow can be deployed incrementally (interface by interface) and strategically (on well chosen routers), rather than deploying NetFlow on every router on the network. Carefully determinations on key routers and key interfaces where NetFlow should be activated based on the network traffic flow patterns, network topology and architecture.

The key deployment considerations include:-

I. NetFlow services should be utilized as an edge metering and access list performance acceleration tool and should not be activated on *hot* core/backbone routers or routers running at very high CPU utilization rates.

II. Understand application driven data collection requirements. Accounting applications may only require originating and terminating router flow information whereas monitoring applications may require a more comprehensive (data intensive) end to end view.

III. Understand the impact of network topology and routing policy on flow collection strategy. For example, it is advisable to avoid collecting duplicate flows by activating NetFlow on key aggregation routers where traffic originates or terminates and not on backbone routers or intermediate routers, which would provide duplicate views of the same, flow information.

IV. Service providers in the transit carrier business (carrying traffic neither originating nor terminating on their network) may utilize NetFlow Export data for measuring transit traffic usage of network resources for accounting and billing purposes.

Configuration of IP Accounting

IP accounting provides basic IP accounting functions. By enabling IP accounting, users can see the number of bytes and packets switched through on a source and destination IP address basis. Only transit IP traffic is measured and only on an outbound basis. Traffic generated by the software or terminating in the software is not included in the accounting statistics. To maintain accurate accounting, the configuration maintains the accounting databases.

IP accounting configuration also provides information that identifies IP traffic that fails IP access lists. Identifying IP source addresses that violate IP access lists signals possible attempts to breach security. The data also helps in identifying how the IP access list configurations should be verified. Users can then display the number of bytes and packets from a single source that attempted to breach security against the access list for the source destination pair. By default, IP accounting displays the number of packets that have passed access lists and were routed.

Conclusion

Network Management Systems are essential in any network deployed. In this work, the significance of each functional area of the ISO's network management model in the management of the entire network has been detailed giving the specifics for a present and desired network management for the Nelson Mandela African Institute of Science and Technology as the case study. In order to cope with the expected expansion of Mandela; the proposed solutions are inevitable.

New features of management platforms like the ability to remotely manage the network elements using a web interface are very essential and eliminate the need for special client software on individual user stations to access a management platform.

The adoption of standards such as Common Object Request Broker Architecture (CORBA) to facilitate the exchange of management data between management platforms and element management systems is significant especially when the enterprise is comprised of heterogeneous network element for interoperability.

The expected expansion of the network should among other things be able to support the desired applications that are intended to support the communications and other academic related issues. These include such applications as Video Conferencing, Voice over IP, and include other services for File transfer (FTP), Mail services and web services from local servers for improved performance, security, management and accountability.

References

[1] http://www.cisco.com/network Management best practice

[2] TANENBAUM, A.S.: *Computer Networks,* Fourth Edition, New Jersey - USA: Prentice Hall, 2003.

[3] LEE, T.T. and LIEW, S.C.: *Principles of Broadband Switching and Networking*, New Jersey – USA: John Wiley & Sons Inc., 2010.

[4] CCNA Discovery 4: Designing and Supporting Computer Networks: Cisco Systems, Inc., 2007.

[5] LAMMLE, T.: *Cisco Certified Network Associate Study Guide*, Sixth Edition, Indianapolis, Indiana – USA: Wiley Publishing, Inc., 2007.