Network Management

- Network management is the process of controlling a complex data network to maximize its efficiency and productivity
- The overall goal of network management is to help with the complexity of a data network and to ensure that data can go across it with maximum efficiency and transparency to the users

Network Management

Requirements

Example of approach

- Controlling strategic assets
- Controlling complexity
- Improving service
- Balancing various needs: performance, availability, security, cost
- Reducing downtime
- Controlling costs

Network Management

- The International Organization for Standardization (ISO) Network Management Forum divided network management into five functional areas:
  - Fault Management
  - Configuration Management
  - Security Management
  - Performance Management
  - Accounting Management

Fault Management

- Is the process of locating problems, or faults, on the data network
- It involves the following steps:
  - Detect the fault
  - Determine exactly where the fault is
  - Isolate the rest of the network from the failure so that it can continue to function
  - Reconfigure or modify the network in such a way as to minimize the impact
  - Repair or replace the failed components

  - Tests: connectivity, data integrity, response-time, ….

Configuration Management

- The configuration of certain network devices controls the behavior of the data network
- Configuration management is the process of finding and setting up (configuring) these critical devices
- Involves following steps:
  - Installation of new hardware/software
  - Tracking changes in control configuration
  - Who, what and why? - network topology
  - Revert/undo changes
  - Change management
  - Configuration audit
  - Does it do what was intended

Security Management

- Is the process of controlling access to information on the data network
- Provides a way to monitor access points and records information on a periodic basis
- Provides audit trails and sounds alarms for security breaches
- Several security measures are provided:
  - Security services: generating, distributing, storing of encryption keys for services
  - Exception alarm generation, detection of problems
  - Uniform access control to resources
  - Backups, data security
  - Security logging

Performance Management

- Involves measuring the performance of the network hardware, software, and media
- Examples of measured activities are:
  - What is the level of capacity utilization?
  - Is there excessive traffic?
  - Has throughput been reduced to unacceptable levels?
  - Are there bottlenecks?
  - Is response time increasing?
  - What is the error rates?
  - Indicators: availability, response time, accuracy ← service
    throughput, utilization ← efficiency

Accounting Management

- Involves tracking individual's utilization and grouping of network resources to ensure that users have sufficient resources
- Involves granting or removing permission for access to the network
- Identifying consumers and suppliers of network resources - users and groups
- Mapping network resources consumption to customer identity
- Billing

Network Management Protocols

- A simple protocol defines common data formats and parameters and allows for easy retrieval of information
- A complex protocol adds some change capability and security
- An advanced protocol remotely executes network management tasks, is independent of the network protocol layer
- Managed objects: functions provided by the network
- Element Management Systems (EMS): managing a specific portion of the network (may manage async lines, multiplexers, routers)
- Managers of Manager Systems (MoM): integrate together information from several EMS

Network Management

Standards

- Internet approach: Simple Network Management Protocol (SNMP, secure SNMP, SNMP v2)
- OSI approach: CMIP - common management information protocol, CMIS - common management information service (user interface)

We concentrate on SNMP

Network Management

Proprietary solutions

- The world of Microsoft PC software:
  Windows NT + several (or hundreds) of PCs with Windows 95 (98??)

- Solution: Microsoft SMS software:
  full control over workstations (Windows95) from central NT server
  software configuration, updates, full inventory

- NT world - incorporates SNMP mechanisms

Network Management Protocols

- So where is technology today?
  - The most common protocols are:
    - SNMP (Simple Network Management Protocol)
    - SNMPv2 (SNMP version 2)
    - CMIS/CMIP (Common Management Information Services/Common Management Information Protocol)

Network Management Protocols

- SNMP is beyond the simple protocol with adequate monitoring capabilities and some change capabilities
- SNMPv2 greatly enhances the SNMP feature set
- CMIS/CMIP approaches the advanced tool, but implementation issues have limited its use

SNMP

- At the end of the 80's, a solution was chosen called the Internet-standard Network Management Framework.
- This was a set of three documents defining:
  - A set of rules for describing management information
  - An initial set of managed objects
  - A protocol used to exchange management information
- Comprised of agents and managers
  - •Agent - process running on each managed node collecting information about the device it is running on.
  - •Manager - process running on a management workstation that requests information about devices on the network.

SNMP

- The SNMP protocol was a mere 36 pages within these documents
- The framework could be extended by defining new managed objects, but changes to the description rules or the protocol weren't allowed.
- Today, there are literally hundreds of SNMP-capable products and thousands of managed object definitions.

SNMP

- The work on SNMP security was completed in early 1992
- The security features introduced authentication, authorization, and privacy
- Unfortunately, this required a changed in the SNMP protocol which became SNMPv2

SNMP

- A group was formed and their efforts were complete in early 1993
- There are 12 documents describing SNMPv2
- There are 3 basic commands that are used with SNMP:
  - Get
  - Set
  - Get Next

SNMP

- Authorization and authentication relies on a SNMP community string
- The community string(s) can be read-only or read-write
- The default community strings are:
  - public (read-only)
  - private (read-write)
- Community strings are case sensitive

Advantages of using SNMP

- Standardized
- universally supported
- extendible
- portable
- allows distributed management access
- lightweight protocol

SNMP

- There are two approaches for the management system to obtain information from SNMP
  - Traps
  - Polling

Trap

- Traps are unrequested event reports that are sent to a management system by an SNMP agent process
- When a trappable event occurs, a trap message is generated by the agent and is sent to a trap destination (a specific, configured network address)
- Many events can be configured to signal a trap, like a network cable fault, failing NIC or Hard Drive, a “General Protection Fault”, or a power supply failure
- Traps can also be throttled -- You can limit the number of traps sent per second from the agent
- Traps have a priority associated with them -- Critical, Major, Minor, Warning, Marginal, Informational, Normal, Unknown

Trap Receivers

- Traps are received by a management application.
- Management applications can handle the trap in a few ways:
  - Poll the agent that sent the trap for more information about the event, and the status of the rest of the machine.
  - Log the reception of the trap.
  - Completely ignore the trap.
- Management applications can be set up to send off an e-mail, call a voice mail and leave a message, or send an alpha-numeric page to the network administrator's pager that says:

Your PDC just Blue-Screened at 03:46AM. Have a nice day. :)

SNMP Traps

- When an event happens on a network device a trap is sent to the network management system
- A trap will contain:
  - Network device name
  - Time the event happened
  - Type of event

SNMP Traps

- Resources are required on the network device to generate a trap
- When a lot of events occur,the network bandwidth may be tied up with traps
  - Thresholds can be used to help
- Because the network device has a limited view, it is possible the management system has already received the information and the trap is redundant

SNMP Polling

- The network management system periodically queries the network device for information
- The advantage is the network management system is in control and knows the "big picture"
- The disadvantage is the amount of delay from when an event occurs to when it's noticed
  - Short interval, network bandwidth is wasted
  - Long interval, response to events is too slow

SNMP Traps/Polling

- When an event occurs, the network device generates a simple trap
- The management system then polls the network device to get the necessary information
- The management system also does low frequency polling as a backup to the trap

SNMP MIBS

- Management Information Base (MIB) is a collection of related managed objects
- Used to define what information you can get back from the network device
- There are standard and enterprise specific MIBS

SNMP MIBS

- Types of MIB Modules
  - Standard: These are the standard MIBS currently designed to capture the core aspects of the particular technology
  - Experimental: Temporary and if achieves standardization then it is placed in the standard module
  - Enterprise-specific: Vendor specific MIBS that provide additional management capabilities for those features that require it

SNMP MIB Tools

- A MIB compiler
- A MIB browser
- A MIB alias tool
- A MIB query tool

CIMS/CIMP

- The OSI framework is an object-oriented paradigm
  - Objects have attributes, generate events, and perform actions
  - Objects are scoped by numerous hierarchies for the purpose of inheritance or containment
- Although the OSI model “sounds neat”, it is much more complicated and is not very common

Network Management Protocols

- These protocols do not state how to accomplish the goals of network management
- They give methods to monitor and configure network devices
- The challenge to analyze the information in an effective manner rests with software engineers who write network management applications

Network Management Platform

- Historically, network management revolved around multiple systems, each managing one specific set of components on the data network
- Restrictions of money, physical space, and technical expertise led to the desire to have the components managed by a single system that would show their interconnections on a network map

Network Management Platform

- A network management platform is a software package that provides the basic functionality of network management for different network components
- The goal for the platform is to provide generic functionality for managing a variety of network devices

Network Management Platform

- Basic features for any platform to include are:
  - Graphical User Interface (GUI)
  - Network Map
  - Database Management System (DBMS)
  - Standard Method to Query Devices
  - Customizable Menu System
  - Event Log

Network Management Platform

- Additional features for a platform include:
  - Graphing Tools
  - Application Programming Interface (API)
  - System Security

Network Management Platform

- Management Platforms that exist today
  - Sun's SunNet Manager
  - HP's OpenView
  - IBM's Netview for AIX
  - Cabletron's Spectrum

Network Management Architectures

- The Network Management Platform can use various architectures to provide functionality
- The 3 most common are:
  - Centralized
  - Hierarchical
  - Distributed

Centralized Architecture

- The Network Management Platform resides on a single computer system
- For full redundancy, the computer system is backed up by another system
- Can allow access and forward events to other consoles on network

Centralized Architecture

- Used for:
  - All network alerts & events
  - All network information
  - Access all management applications

Centralized Architecture

- Pros:
  - Single location to view events & alerts
  - Single place to access network management applications and information
  - Security is easier to maintain

Centralized Architecture

- Cons:
  - Single system is not redundant or fault tolerant
  - As network elements are added, may be difficult or expensive to scale system to handle load
  - Having to query all devices from a single location

Hierarchical Architecture

- Uses multiple computer systems
  - One system acting as the central server
  - Other systems working as clients
- Central server requires backups for redundancy

Hierarchical Architecture

- Key features:
  - Not dependent on a single system
  - Distribution of network management tasks
  - Network monitoring distributed throughout network
  - Centralized information storage

Hierarchical Architecture

- Pros:
  - Multiple systems to manage the network
- Cons:
  - Information gathering is more difficult and time consuming
  - The list of managed devices managed by each client needs to be predetermined and manually configured

Distributed Architecture

- Combines the centralized and hierarchical architectures
- Uses multiple peer network management systems
  - Each peer can have a complete database
  - Each peer can perform various tasks and report back to a central system

Distributed Architecture

- Contains advantages from central & hierarchical architectures
  - Single location for all network information, alerts & events
  - Single location to access all management applications
  - Not dependent on a single system
  - Distribution of network management tasks
  - Distribution of network monitoring throughout the network

Network Management Applications

- Goals
  - Effectively manage a specific set of devices
  - Avoid functionality overlap with the platform
  - Integrate with a platform through the API and menu system
  - Reside on multiple platforms
- Applications do not share information

Network Management Applications

- Applications that exist today
  - BayNetworks' Optivity
  - Cisco's CiscoWorks
  - 3Com's Transcend

Choosing a Network Management System

- Built from two major components: the Platform and Applications
- A practical approach follows these steps:
  - Perform device inventory
  - Prioritize the functional areas of network management
  - Survey network management applications
  - Choose the network management platform

Other Topics

- Sniffers
- RMON
- Network Statistics

Network Statistics

- Baseline
- Trouble shooting
- Capacity planning for the future
- Reports