SLAC-PUB--5913

DE93 004003

Network Management, Status & Directions

R. L. A. Cottrell and T. C. Streater

Stanford Linear Accelerator Center, Stanford University, Stanford, CA 94309

ABSTRACT

It has been said that the "network is the system". This implies providing levels of service, reliability, predictability and availability that are commensurate with or better than those that individual computers provide today. To provide this requires integrated network management for interconnected networks of heterogeneous devices covering both the local campus and across the world and spanning many administrative domains. This talk will review the status of existing tools to address management for networks. It draws on experience from both within and outside the HEP community.

Introduction

Complete books have been written and week long conferences have been held on network management. This short paper will try to provide a flavor of where we are today in some of the major areas that are of interest to High Energy Physics and a hint of where things are going.

What's so Difficult about Network Management?

It has been said that *The Network is the System* in today's distributed computing environment. This analogy to the old central systems is useful, however there are important differences which make management more complex. In comparison to matured and bounded mainframes with a single operating system and physical backplane, networks have a widely distributed and easily extendable "physical backplane" which is constantly being modified by people with widely varying responsibilities and skills. In addition the network supports multiple protocols, applications, and consists of equipment from multiple vendors.

Ideally what we want is **intelligent**, automated network management with an end state that the network needs no human management. Using a network should be like using a power line in which connectivity is simple (plug in), uninteresting, there on demand, and you pay as you go with a predictable cost. We would like a network that manages itself, failing that, one that users can manage and failing that, one that specialists can manage. Unfortunately today's networks are not yet manageable by highly trained individuals.

What is Network Management?

Network management entails managing the delivery of an agreed upon service level to the user. The major functional areas that feed into the service level and the importance ranking ascribed by a recent survey[1] are:

1. Fault: alarm reporting, logging, isolation, trouble-ticketing;
2. Configuration: inventory of resources to be managed;

* Work supported by D[illegible]ent of Energy, contract DE AC03-76SF00515.

Presented at the 10th International Conference on Computing in High Energy Physics (CHEP 92), Annecy, France, September 21-25, 1992

3.Performance: monitoring, setting, maintaining and adjusting thresholds to ensure the network meets design criteria and business purposes;

4.Security: ensure integrity of corporations data;

5.Accounting: measures for charging and/or allocating services delivered.

Of these, fault management, specifically the alarm reporting and logging facilities, was clearly the most critical in the opinion of the survey respondents.

A major tool to address network management is the Network Management Station (NMS). This provides the ability to monitor and control network elements (agents) through access to their Management Information Bases (MIBs) via a management protocol such as the Simple Network Management Protocol[2] (SNMP).

Where are we Today?

Today's NMS is, potentially, a very powerful tool. In the ideal world it would solve all the above problems and integrate with corporate databases and applications and be intuitive and easy to use.

An NMS, today, provides several functions. Typically, it can generate a symbolic map of the network, with coloured icons representing the various network components and their states (green = up, red = down, etc.). It provides fault detection synchronously or asynchronously, by polling or by receiving unsolicited messages (traps) from remote network monitors. It may provide a means of doing network node discovery, of displaying, modifying, graphing, and storing the network data that the station can access. Currently, however, NMSs do not integrate well with other databases and applications, they are difficult to use, many of the MIBs are proprietary, each one often being supported by only one vendor, and many devices (especially older one) are not even monitorable. As a result many network operations centers today require multiple vendor specific NMSs and highly skilled network managers.

What is Still Needed?

- **Data management**: We need to let an NMS do what it does best, namely monitoring the network, and leave other facets to other packages. We need to correlate (and in some cases modify) information in corporate databases such as employee information, property control, cable plants, and a Geographical Information System (GIS), with devices in the NMS database. This requires a decentralized view of the data with clearly published interfaces so that data can be used from multiple separately managed data sources.
- **Presentation:** At the same time as providing a geographical view of the network, we also need multiple customizable views providing various logical views with the ability to zoom in on these views. In addition to the real time needs, customizable reporting is required. We need to be able to specify easily what to collect and with what frequency. We then need to be able to extract, process and display it in a familiar format for example by feeding it to a familiar analysis, graphics or spreadsheet package, and possibly deliver it to the relevant people (e.g. for accounting or billing purposes).
- **Integration with Other Tools:** Besides integration with databases, many NMSs need improvement in the integration of other network diagnostic tools such as `nslookup`, `netstat`, `traceroute`, and `etherfind`. A big step in this direction will be to provide standard Application Program Interfaces (API).

- **User Interface:** Today's NMSs have a Graphical User Interface (GUI) which is complex to use with many levels of menus and pop-up boxes etc. to traverse. They require considerable training and network expertise to use.
- **Distributed Management:** To manage a large network, we need to be able to distribute the managements tasks to multiple autonomous groups while still being able to provide a unified view of the whole. This will require many levels of access to interworking NMSs that divide up the management tasks, with appropriate access permissions.It may be necessary to designate a master server, which can float depending on priorities and availability.
- **Expert Systems:** Typically, the NMS can accept traps or generate them itself, when an exceptional condition is noted. The NMS can do a good job of collecting the SNMP traps and firing off scripts each time, but if all the script does is send a mail item, then someone's mail box is going to fill up very quickly. Often one component failure can result in a blizzard of alerts from cascading faults, many of which are irrelevant. Some heuristics are needed here to perform triage, decide what should be done, by-pass simple problems, and call for help if necessary. The area of automating alert processing is still in its infancy for network management. Substantial benefits should be realized when the work processes are modified or redesigned, and rule based expert systems with automatic learning are applied to them.
- **Extending Network Management to Enterprise Management:** Network components are only one of the items that can fail and prevent access to information. We also need to monitor and manage hosts, applications, and other hardware such as environmental control systems, phone switches, modem banks etc., which can either cause the failures or provide information to help discover potential problems earlier. Some NMS packages now monitor the host MIB information. An Internet Engineering Task Force (IETF) working group expects to provide a PC MIB in the next 6-9 months. However, very few hosts are manageable from the NMS. Nine manufacturers of Uninterruptible Power Systems (UPS) recently agreed to work on an SNMP MIB. There are some proprietary systems for environment monitoring, but these need to be made more open and integrated into the total picture. Many mission critical applications are already instrumented and monitored. However, again this instrumentation and monitoring is proprietary and needs to be standardized and integrated.

What's Coming

- **Remote Monitoring (RMON) MIB[5]:** Essentially, this combines the best and most important items from various Enterprise MIBs, and forms a standard out of them. The importance of this lies in the fact that now NMS vendors can once again code to a standard MIB whose semantics are known to the NMS. Thus proper support can be provided, and rather than merely providing variables which instrument TCP/IP and SNMP itself, there are those which give us information about the network itself, which is where most problems tend to come from. The existence of RMON will help move NMS development forward again. The RMON MIB will expand as time passes. Currently it has nine different sections for segment statistics, history information, host table, host top N, traffic matrix, alarms, packet filter, packet capture, and event logging.
- **SNMP-II:** The Simple Management Protocol[3] (SMP) which has been proposed to the IETF, addresses several shortcomings of SNMP including the lack of: a bulk file transfer; adequate security features; support for alternative transport mechanisms such as AppleTalk; NMS to NMS communications; and of an event-polling mechanism to help foresee system breakdowns. Also the Open Systems Interconnection's (OSI) Common Manage-

ment Information Protocol[4] (CMIP) will be coming to market in the next year. OSF/DME (see below) will support both SNMP and CMIP and several major vendors have lined up to support of CMIP.

- **Distributed Management Environment[6] (DME):** This is a first attempt to define open, vendor-neutral Application Program Interfaces (APIs) for accessing a common management platform. When it becomes available in 1993 it will provide an object oriented approach to network management which hides the minute differences between vendor devices. Objects represent a network or system resource such as a router or bridge that needs to be managed. Thus a vendor will provide a DME router object that contains not only a standard MIB but also software routines (i.e. methods) to perform management functions such as downloading software, running diagnostics etc. DME objects can also contain instructions on how to display their information or draw the object's icon. The SNMP/SMP premise that agents are small and simple with a more powerful NMS, may be at variance with the more symmetric DME approach that shares more of the management throughout the network.

Conclusions

To manage an enterprise we need standards, cooperation among multiple vendors from multiple disciplines to drive and adhere to the standards. To get this we, as users, must work with vendors to tell them what our needs are and to push them towards standards based solutions that are interoperable. In the meantime we need to take an evolutionary approach of small, safe steps to managing the networks, then the hosts and finally the applications. At the same time, legacy systems will not disappear overnight and any management system will need to manage both the old and the new.

Acknowledgments

We would like to acknowledge Connie Logg for her help with editing the paper, Ted Sopher of LBL, Jeff Hodges of Stanford University, and Mike Collins of NERSC for detailed discussion on their network management systems, Jim Browne of IBM who provided information on Netview/6000, and the SLAC Network Group.

References

1. Adams, E., *Global Commonality in User Requirements*, **Integrated Network management II, ISBN: 0 444 89028 9**, 1991.
2. Case, J., Fedor, M., Schoffstall, M., and Davin J. *Simple Network Management Protocol*, **Internet RFC 1157**, 1990
3. Case, J., McCloghrie, K., Rose, M., and Waldbusser, S. *Introduction to the Simple Management Protocol Framework*, **Internet Working Draft**, 1992.
4. ISO/IEC 9595 and 9596, *Open Systems Interconnection - Common Management Information Service Definition and Protocol Specification*, 1990.
5. Waldbusser, S. *Remote network monitoring Management Information Base*. **Internet RFC 1271**, 1991
6. Open Software Foundation. *Request for Technology, Distributed Management Environment.* OSF, 11 Cambridge Center, Cambridge, MA, 1990.

DATE
FILMED
01/21/93