ABSTRACT

Today's computer networks have high usage and provide sophisticated applications. As a consequence, the issues of their uptime and optimal operation are critical. The networks support an assortment of applications and frequently use several networking protocols. Furthermore, their topology is complex as a result of interconnections and the networking equipment is typically provided by different vendors. A management system is a necessity in such environments and contemporary network management systems need to take into account all these factors in implementing an effective solution.

INTRODUCTION

This paper presents the design of a simple application layer protocol, the framework of which permits the implementation of management functions in providing the integrated management of measurement entities distributed over interconnected networks. High performance passive monitors examine all traffic on their individual network segments and obtain relevant information necessary to provide LAN statistics to one or more Management Nodes. This transfer of information and other management functions is effected through the use of the communication protocol in question. To complete the network management scenario, the Management Node may further process the received information and present it through a user interface.

An overview of the evolution of network management products and their role is presented. Next, the five broad functional areas of management recommended by the ISO are outlined. Specifications related to the LAN and monitoring devices are reviewed and trade-offs deliberated upon, for the model. A brief mention of the monitor design and management node software functions is provided to outline the requirements they place on the management protocol design. Following this, the Monitor Management Service environment is outlined; communication facilities specified and services listed. Finally, the Monitor Management Protocol is presented; usage assumed from other Application and Presentation Layer services are reviewed and protocol elements defined.

EVOLUTION AND ROLE OF NETWORK MANAGEMENT

The purpose served by network management tools has been constantly changing. Initially, relatively few tools were required to determine the performance of various LAN environments. Usage was restricted to the comparison of elementary parameters such as packet rate, utilization and bandwidth and setting benchmarks [1, 4]. They were experimental tools in a research environment and helped enable the development of new LAN standards with improved performances.

Later, with the commercialization and increasing complexity of networks, management tools were used to diagnose bottlenecks in individual LANs [2, 3]. Network management was disjoint with different tools testing different parameters on different network elements with varying extents of coverage.

Today, LANs have grown to form an integral part of computer systems vis-a-vis distributed computing. Networks are large and interconnected demanding new levels of network management. Each LAN in a large environment typically supports several protocols provided by different vendors, each supporting a host of different applications. Equipment comprising a network typically comes from several different vendors. A look at any large network reveals a diverse mixture of network management products resulting in a very disjoint base of information. As a result, techniques have been developed to integrate network management products over multiple networks. The ISO has developed standards for the management of separate networking resources. Specifications of the new standard are complete, in that it encompasses all aspects of the generalized term "management", from the fundamental issues such as Accounting through Network Security.

The OSI Management Architecture defines five main facilities to support the users' need for network management [5]. These facilities are defined to allow a modular approach to the design of management functions. Functions from more than one management facility may be used to provide a management service desired by the user. The facilities are as follows: Fault Management, Configuration and Name Management, Performance Management, Accounting Management and Security Management.

The procedures that constitute each functional management facility are implemented by management functions using management protocol elements. Statistical data for these functions are provided by the network monitors. Thus, monitoring is essential to managing a network as it indirectly provides the network manager with relevant data.

INTEGRATED NETWORK MANAGEMENT ENVIRONMENT AND MODEL

Fig. 1 illustrates a typical internet composed of LANs. The interconnected LAN environment has certain characteristics that should be recognized by designers of network management products.

Characteristics

LANs have characteristics, both inherent and specified by usage [6], that are noteworthy from the point of view of Measurement Management implementation. The inherent characteristics include: a relatively small geographic extent, a bandwidth greater than 1 Mbps, multi-access nature and broadcast communication. Characteristics dependent on usage include: several protocols from different vendors co-existing on the same LAN, ownership and management of network stations being distributed among several groups, and the dynamic availability of stations or services on the LAN.
Bridges allow the individual LANs to be transparently connected and filter local traffic. The characteristics of bridged LANs are extended over those of individual LAN segments. Specifically, bridged LANs span a greater geographic area, support more users and provide greater aggregate bandwidth. The number of protocols on a bridged LAN is the sum of the protocols on its individual LAN segments. Since bridges filter local traffic localizing it to LAN segments, monitors need to be placed on each LAN segment in order to provide a global view on an internetwork [6, 7].

The monitoring entity local to a LAN may monitor the network using one of two techniques:
1. Active monitoring wherein the monitor injects packets at specified intervals and records statistics based on these and other packets,
2. Passive monitoring wherein the monitor collects and processes all packets on the network as they arrive [8].

Active monitoring introduces overhead and is slower because of the dual tasks of packet injection and collection.

In order to support the monitoring of all LAN traffic, packet processing has to be completed within the minimum packet time, demanding a very high level of performance from the monitors. The management entity local to a LAN may simply gather all data from the network itself as described above. Alternatively, each element on the LAN may be provided with monitoring software and/or hardware. Each network element is required to report monitored information to its local management device using a protocol. The local devices in turn need to use a second protocol to transfer monitored data to a station dedicated to integrated management. This, however, is difficult to implement in multi-vendor, multi-protocol type environments and is obviously also expensive. In the case of heavily loaded LANs or very high performance monitors, the option of using a separate net dedicated to transmit monitored data becomes necessary.

**Chosen Environment**

In an environment consisting of inter-connected networks, each individual segment of the internet requires a Local Monitoring Entity (LME) to provide statistics associated with that segment. This calls for a distributed set of local monitoring systems. The development of an Integrated Network Management System (INMS) using distributed local monitors requires work in three areas:
1. Design of the Local Monitoring System (Monitoring Device) hardware and software,
2. Design of the protocol to support the communication.
3. Design of System Management Entity (Management Node) software to support the user interface and management functions.

**SPECIFICATION OF THE LOCAL MONITORING ENTITIES AND THE MANAGEMENT NODE**

In order to get a clear picture of the requirements imposed by the INMS on the Monitor Management Protocol (MMP), it is necessary to analyze the operation of the LME and System Management Entity (SME) and their interaction.

The operation of the LMEs and MNs and their interaction imposes certain restrictions on the design of the MMP that supports their communication and also gives some insight into the requirements that it must meet. A brief review of their operation is provided to get a clear picture of these requirements.

**Local Monitoring Entity**

Two basic LME design goals are:
1. the Local Monitoring Device should collect all valid packets regardless of their traffic rate,
2. it should process the necessary information required to make a meaningful presentation of statistics.

The high level of performance makes it necessary to distribute part of the data processing to the SME [6, 7].

The LME comprises the following elements: one or two 10 Mbps 802.3 interfaces, a microprocessor, buffer memory and specialized learning hardware that provides the high level of performance [6]. The processing of each packet is supported by the following counters:

- General counters for byte and packet count of single destination (SD) and multicast (MC) packets and error count,
- Type Field Traffic counter matrix that categorizes each SD packet based on its type field and packet size.
The MMP provides the following service: the user at the Management Node (SME) specifies a set of LMEs to the Monitor Management Service Provider for an internet monitoring operation. Each LME is contacted by the SME. Each LME verifies its ability to participate in the activity and acknowledges it to the SME. The LMEs providing acknowledgements are sent command files specifying all parameters related to the operation [9]. It includes counter resetting, sample time interval and report time interval specifications, threshold setting for alarm events and resource allotments for optional user specified data analysis. The MM Service Provider at each LME receives the command in the form of a service element. Each LME then carries out the operation returning unsolicited statistics at user specified intervals. This time interval is the "report interval". The counters kept by the LMEs are cumulative allowing them to collect statistics without the SME being associated. When association is established, the information available at the LME will reflect the status of the LAN over the period of disassociation. The user has the facility to start and stop each monitoring operation.

To allow the operation described above, the MMP must perform the following functions:

- establish an association between the SME and one or more LMEs for the purpose of collecting traffic statistics,
- place a command file at each LME associated with the monitoring operation,
- transfer traffic related statistics from the individual LMEs associated with the operation,
- terminate an association on completion of a monitoring operation.

The MM Service provides this capability by means of five communications facilities:

- The Establishment facility produces an association and an initial MM environment when the user invokes the MM Service.
- The Commitment facility enables the SME to provide each LME with a command file enabling it to start the monitoring operation.
- The Data Transfer facility ensures the transfer of SME commands to the LMEs and measurement statistics from the LMEs to the SME.
- The Status Check facility enables the user to determine the state of an LME e.g. whether a particular LME is associated for the current monitoring operation.
- The Termination Facility enables the user to terminate the association. The establishment and termination facilities allow the specification of different sets of LMEs for different monitoring operations.

Table 1 shows a list of the MM Services that are designed for the purpose of implementing the above five functions.

<table>
<thead>
<tr>
<th>Facility</th>
<th>Service</th>
<th>Service Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishment</td>
<td>OPEN</td>
<td>Confirmed</td>
</tr>
<tr>
<td>Commitment</td>
<td>EXECUTE</td>
<td>Confirmed</td>
</tr>
<tr>
<td>Data Transfer</td>
<td>LOAD</td>
<td>Confirmed</td>
</tr>
<tr>
<td></td>
<td>TRANSFER</td>
<td>Confirmed</td>
</tr>
<tr>
<td>Status Check</td>
<td>STATUS</td>
<td>Confirmed</td>
</tr>
<tr>
<td></td>
<td>STOP</td>
<td>Non-confirmed</td>
</tr>
<tr>
<td>Termination</td>
<td>FINISH</td>
<td>Confirmed</td>
</tr>
</tbody>
</table>

Table 1: MM Services
A confirmed service consists of a request, an indication, a response, and a confirm. Non-confirmed services consist of only a request and an indication \([10, 11]\). An example of the service primitives for the service OPEN is:

\[
\begin{align*}
\text{MM-OPEN.request} & \quad \text{(S-AOQ)} \\
\text{MM-OPEN.indication} & \quad \text{(S-AOI)} \\
\text{MM-OPEN.response} & \quad \text{(S-AOR)} \\
\text{MM-OPEN.confirm} & \quad \text{(S-AOC)}
\end{align*}
\]

The service OPEN is a confirmed service because the monitors, being remote peers, must agree to establish a connection. Therefore the primitives request, indication, response and confirm are used.

THE MONITOR MANAGEMENT PROTOCOL AND ARCHITECTURE

The MM Service is provided by the Monitor Management Protocol machines residing on the SME and LMEs. The MMPMs fit into the Application Layer of the ISO Reference Model. Both, the MMP Machine on the SME (S-MMPM) and an MMP machine on an associated LME (L-MMPM) use the services of the Presentation Layer of the OSI Reference Model both directly and through the Association Control Service Entity (ASCE). Both depend on File Transfer Access and Management (FTAM) which in turn invokes the ACSE and Presentation Layer services \([9]\). Figure 4 shows the architecture of the MM Protocol.

The MM Service functions used for the transfer of data and control information between the protocol machines are implemented by procedures. The procedures are defined in terms of:

- the interactions between the S-MMPM and one or more L-MMPMs through the exchange of MM Protocol Elements.
- the interactions between an S-MMPM and an MM Service user through exchange of MM Service primitives
- the interactions between an L-MMPM and an MM Service application through exchange of MM Service primitives
- the interactions between an MMPM and the providers of the ACSE, FTAM and Presentation services through exchange of ACSE, FTAM and Presentation Service primitives

Table 2 shows a list of the protocol elements and the protocol functions to which each one belongs. Table 3 gives an example of the OPEN service for the ESTABLISHMENT function implemented by a procedure defined in terms of MM services and primitives.

### Table 2. MM Protocol Elements

<table>
<thead>
<tr>
<th>Function</th>
<th>Abbreviation</th>
<th>Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishment</td>
<td>AOQ</td>
<td>MM-OPEN.req</td>
</tr>
<tr>
<td></td>
<td>AOR</td>
<td>MM-OPEN.resp</td>
</tr>
<tr>
<td>Termination</td>
<td>AFQ</td>
<td>MM-FINISH.req</td>
</tr>
<tr>
<td></td>
<td>AFR</td>
<td>MM-FINISH.resp</td>
</tr>
<tr>
<td>Data Transfer</td>
<td>FLQ</td>
<td>MM-LOAD.req</td>
</tr>
<tr>
<td></td>
<td>FLR</td>
<td>MM-LOAD.resp</td>
</tr>
<tr>
<td></td>
<td>FTQ</td>
<td>MM-TXFER.req</td>
</tr>
<tr>
<td></td>
<td>FTR</td>
<td>MM-TXFER.resp</td>
</tr>
<tr>
<td>Commitment</td>
<td>FXQ</td>
<td>MM-EXEC.req</td>
</tr>
<tr>
<td></td>
<td>FXR</td>
<td>MM-EXEC.resp</td>
</tr>
<tr>
<td></td>
<td>PRQ</td>
<td>MM-START.req</td>
</tr>
<tr>
<td>Status Checking</td>
<td>PSQ</td>
<td>MM-STATUS.req</td>
</tr>
<tr>
<td></td>
<td>PSR</td>
<td>MM-STATUS.resp</td>
</tr>
<tr>
<td></td>
<td>ASR</td>
<td>MM-STOP.req</td>
</tr>
</tbody>
</table>

### Table 3. An MM Procedure for Association Establishment

<table>
<thead>
<tr>
<th>Step</th>
<th>Machine</th>
<th>Event</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>S-MMPM</td>
<td>S-MMPM accepts S-OPQ</td>
<td>Send P-OPQ</td>
</tr>
<tr>
<td>2.</td>
<td>L-MMPM</td>
<td>L-MMPM accepts P-OPQ</td>
<td>Issue: S-OPQ</td>
</tr>
<tr>
<td>3.</td>
<td>L-MMPM</td>
<td>S-OPR carries result=&quot;success&quot;</td>
<td>Send P-OPR with result=&quot;success&quot;</td>
</tr>
<tr>
<td>4.</td>
<td>S-MMPM</td>
<td>P-OPR carries result=&quot;success&quot;</td>
<td>Issue S-OPC with result=&quot;success&quot;</td>
</tr>
</tbody>
</table>

CONCLUSION

At the time of writing this paper, work was being done in determining the usage of ACSE, FTAM and Presentation Service primitives and in designing a mapping machine to translate MM Service elements to the appropriate lower level service elements based on their usage.

REFERENCES


