Volume 12, Number 2
February 1991
ISSN 0270-7284

SNA Perspective

The single source, objective monthly newsletter covering IBM's Systems Network Architecture

NetView and OSI Management

SNA users are grappling with managing devices not only on SNA networks but also on multivendor networks. IBM has made a strategic commitment to enhance NetView to manage SNA, OSI, and TCP/IP networks. During 1990, several NetView features were introduced for just this purpose. However, the NetView architecture differs significantly from the OSI management architecture.

Because OSI management standards have been developing recently, SNA users need to keep current on their status in order to plan when and how to incorporate OSI network management in their networks. This article notes the progress at and since the recent OSI management committee meetings, reviews the OSI management standards components, structure, and terminology, makes note of emerging OSI standards work in layer management, and examines several issues of concern with regard to NetView's ability to provide OSI management.

(continued on page 2)

Taming the Wild LAN: Systems Management

Most SNA networks today interface with local area networks. Managing these networks is a challenge. LAN management is maturing and enlarging its focus. Moving past its traditional concern with physical facilities LAN management is expanding to include the attached systems. Workgroup systems—the desktop computers and servers—are being considered an integral part of the distributed management environment. Systems management, including management of these attached systems, is an increasingly important aspect of LAN management.

This article defines the manager-agent model of OSI and TCP/IP network management, describes the functions of the systems agent, and identifies some LAN systems management products. Further, because NetView has a different way of looking at management topology from the OSI model used by most LANs, the OSI manager-agent model is compared to NetView's.

(continued on page 9)

In This Issue:

(Continued from page 1)

OSI Standards Progress

OSI management standards made substantial progress after network management committee meetings of the ISO/TC97/SC21 in Seoul, Korea in the summer of 1990. Progress was significant in three areas—progression through the adoption process itself, stabilization, and completeness.

Progression

Many of the standards moved to the second stage, or draft international standard (DIS) status. At this stage, the initial draft proposal (DP) has received approval from all member countries. When a specification reaches DIS status it is considered to be technically stable. Therefore, many vendors will begin developing products once specifications reach this stage. Elevation to full-fledged international standard (IS) status requires only editorial revisions for accuracy and consistency with other documents and a final vote of members. Substantial progress was made in all areas of the OSI management standards work. Hopefully, this progress is bringing closer the time for real OSI-compliant management products.

Stabilization

Revisions were made to achieve more consistency between different parts of the management standards family. Some specifications were reorganized in order to reflect a cleaner architecture. This work illustrates the maturity of the specifications; deeper understanding is leading to a more coherent architecture which will provide long-term stability in the OSI management area.

Completeness

New specifications were added to fill out the complement of functions. These new specifications are currently at the beginning DP stage, but they are expected to advance to DIS status quickly, perhaps by the summer of 1991.

The OSI Management Family

The family of OSI management standards has grown to keep pace with the requirements of managing a heterogeneous environment. Management functions are grouped into:

- systems management
- layer management

Systems management has received the most attention, but now the layer management functions are also taking form.

OSI systems management is defined by the set of standards shown in Figure 1. Those parts near the top are more abstract; the remainder contain more detailed specifications which are derived from those near the top.

The basic management architecture is outlined in IS 7498-4. This addendum to the basic seven-layer open systems interconnection (OSI) reference model description defines management requirements and their relationship to the OSI architecture, and serves as a basis for developing detailed specifications. The five basic functional areas are:

- fault
- configuration
- performance
- accounting
- security

The Systems Management Overview (IS 10040) elaborates on the basic definitions. This document defines the manager-agent architecture and the use of hierarchical management domains.

The Structure of Management Information (DIS 10165) is a multipart standard that defines the way management information is organized. All managed resources are represented as *objects* that have certain attributes, operations, and notifications. Part 1 introduces the object oriented approach to modeling resources and covers operations on

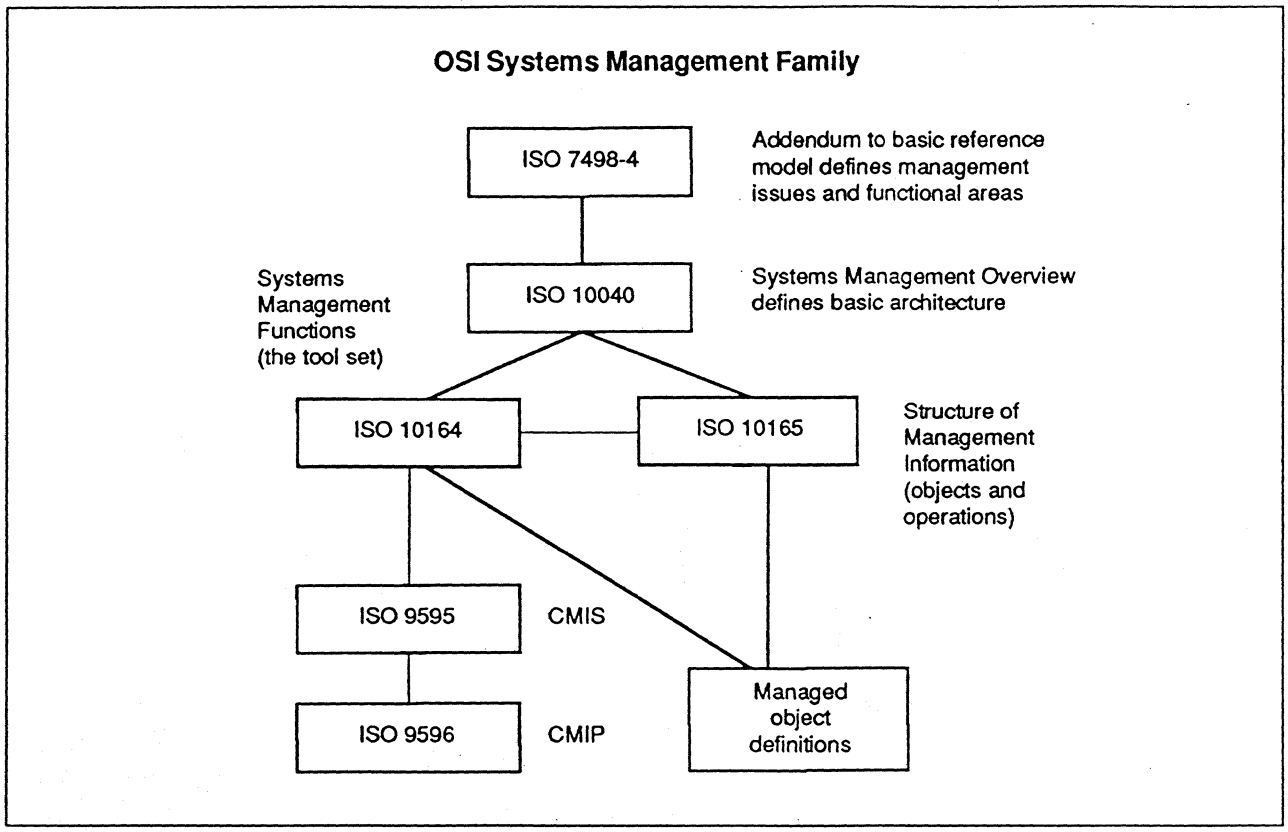


Figure 1

objects and the inheritance of properties from other objects. Part 2 defines object classes, attributes, and notifications for an initial family of managed objects. Part 4 provides guidelines for defining and creating new objects ad templates are provided for notational and descriptional consistency. Note that Part 3 was merged with Part 4 and the committee decided that renumbering would be more confusing.

The systems management functions are the actual tool set for building management applications. Each function covers a certain area such as object management or workload monitoring. Applications can be constructed that use the appropriate systems management functions to carry out their tasks.

Structure of Management Information

The Structure of Management Information (DIS 10165) was fairly stable before the Seoul meetings. The major focus was the resolution of inheritance. Inheritance allows a new object to have properties of the object from which it was derived—its super class. This is one of the attractive aspects of object-oriented approaches since new objects are easily created. For example, an object such as "system" can be defined with generic attributes. Other objects such as "server," "end-system," "router," and so forth can be derived from the super class object "system" and then refined to model their unique properties.

One of the outstanding issues was whether a new object could inherit properties from more than one super class. Before Seoul, the committee had decided to restrict inheritance to a single object. However, multiple inheritance was again included in the specifications. Multiple inheritance, or *allomorphism*, allows a newly created object to inherit properties, behaviors, and notifications for more than one super class. This will allow the creation of new objects that can still be recognized by management applications with no prior knowledge of their existence.

Managed Object Classes

The second part of DIS 10165 defines a set of managed objects that will be the generic objects to be further specialized for particular needs. The managed object *top* is the root of the inheritance tree and every other managed object class is derived from it. The next level of managed object classes derived directly from *top* includes discriminators, systems, logs, log records, access control information objects, and accounting meters. Others will be added as needs are identified. These basic objects will be further refined into more specialized subclasses as more needs are identified and met.

Discriminators are used to apply criteria to the selection of particular managed objects, events, and so forth. Discriminators include a discriminator construct that makes assertions about attribute equality, presence, matching, etc. These assertions can be connected with the boolean operators—and, or, not—to create more complex selection criteria.

Systems identify either end systems or intermediate systems within the OSI environment. All the resources of a system are inherited and contained within the system object.

Logs contain management information that is captured and used for subsequent analysis.

Log records are those objects contained in a log. These records have been further refined into specific examples such as an event report record, attribute change record, security violation record, and so forth.

Access control information objects are used to provide information about what management information is to be protected and the particular access control policies that are to be applied in determining access to this information.

Accounting meters are used to monitor the use of resources within an open environment.

Attributes

Specific attributes have also been defined that can be applied to a wide range of managed objects. Important attributes are counters, relative distinguished names, gauges, thresholds, and tide marks.

Counters are used to monitor events associated with a particular managed resource. They are always incremented by one and wrap around to zero when the maximum value is reached. Counters may, for example, track the number of messages sent or received.

Relative distinguished names are the attribute associated with each object that provides a unique identification of each instance of a managed object class. Every managed object must have this attribute.

Gauges are similar to counters except the value can move in either direction and can change by increments larger than one. Gauges are assigned maximum and minimum values; if a value exceeds them in either direction, it is set to the maximum or minimum. An example of a gauge might be utilization of a communications link.

Thresholds are associated with counters or gauges and can be used to trigger notifications when a counter value is exceeded. Counter-thresholds are associated with counters (see Figure 2). Gauge-thresholds have two values; a minimum value or a maximum value limit threshold can trigger an appropriate event notification.

Tide marks measure the highest and lowest values of a gauge during a measurement interval. For example, tide marks could give the maximum and minimum utilizations of a communications link (see Figure 3).

Each attribute has a unique identifier code. These generic attributes have been refined for specific purposes. For example, the counter has been extended to model messages received, protocol errors, connection failures, and so forth. Each counter has an associated threshold that can be used to trigger specific events.

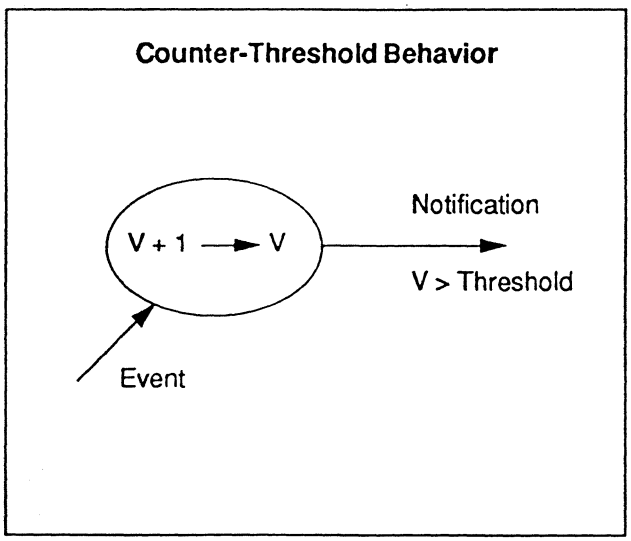


Figure 2

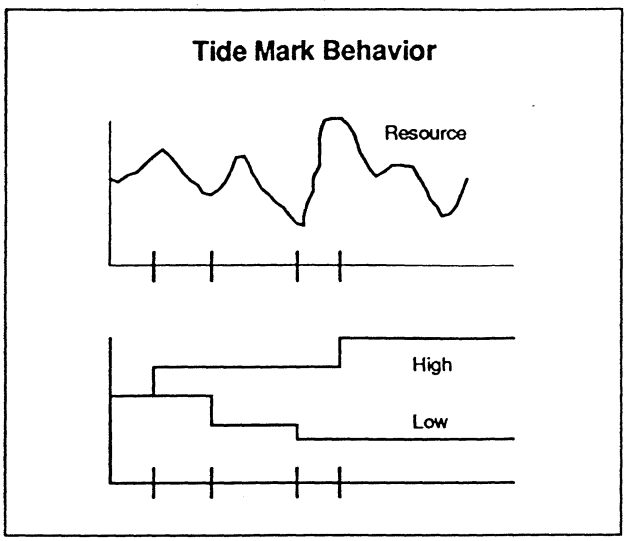


Figure 3

At this time, there are many attributes defined:

- sixty-one related to different notifications
- nine for state management
- ten for relationships
- twenty-three miscellaneous ones such as start time

Systems Management Functions

The current complement of systems management functions have been reorganized slightly, improved, and made more consistent. In addition, new systems management functions were added to make a more complete tool set for building management applications. Table 1 shows the complement of systems management functions that are currently defined. Note that some of the newest functions have not yet been assigned part numbers within the ISO 10164 specification. Part 1 through Part 7 are at DIS status; the remainder are still in the DP stage.

Event Reporting

Part 5 was modified so that only an event forwarding discriminator is used. This discriminator determines which notifications are actually passed from an agent to a manager. There is now no filtering and selection of incoming management requests. That function has been removed from Part 5 and assigned to the access control function, Part 9.

Access Control

Part 9, the access control function, is a new addition that provides an architecture and a description of objects that are used to enforce access control policies. The two parts to the new access control function control the creation of associations and access for management operations. Association control is used to allow only authorized management applications to establish associations with each other. Management operations control is used for each management operation to determine whether the requesting application is allowed to perform that operation with the specified object(s).

Test Management

Test management replaces the confidence testing and diagnostic function from the previous work and provides a general purpose scheme for remote testing and diagnostics. Included in the initial repertoire are the ability to create test objects, to set up test conditions and environments (including taking equipment out of service), and then to restore the operational environment upon completion of the test.

Systems Management Functions

Part	Function
1	Object
2	State
3	Relationships
4	Alarm reporting
5	Event reporting
6	Log control
7	Security alarms
8	Security audit
9	Access control
10	Accounting meter
11	Work load monitor
m	Measurement summarization
?	Test management

Table 1

Test classes are an additional part that was originally part of the confidence and diagnostic testing function. It is used to define different categories of testing. At the present time, testing processes include internal resources, data integrity, protocol integrity, and capacity testing. Further additions to test classes are expected as new requirements are identified.

Accounting Meters

Accounting meters are used to monitor resource usage in an open environment. Each accounting meter is associated with the particular managed object and attribute values that are to be monitored. Accounting meters are also equipped with thresholds so that event notifications can be triggered under certain conditions.

The Tool Set

The structure of the systems management functions as shown in Figure 4 can be clustered around three basic services: object management, event management, and log control. These three services are used by most of the other systems management functions. Newer functions will undoubtedly be defined and will use preexisting functions whenever possible to support their activities.

As part of the procedure for establishing an association between two management applications, the functional units are negotiated. Functional units select which of the systems management functions from which support will be required for the two applications to carry out their management activities.

Layer Management Standards

Layer management specifications have begun to appear as committee drafts (CD—the new term that replaces DPs for new ISO standards). Preliminary work for the network and transport layers and 802.3 LANs was issued in December of 1990.

Each specification defines the managed objects that are required to support management functions. The CSMA/CD layer management approach is shown in Figure 5. The basic architecture will be the same for all layer management functions: the layer management entity "sits beside" the layer it manages. A management application interfaces to the layer manager. The management application can obtain operational information or affect layer behavior through the layer manager.

The media access control (MAC) layer has a set of statistics that are provided by counters. Counters are either mandatory, recommended, or optional. Examples of mandatory counters are number of transmitted frames, number of collisions, and number of received frames.

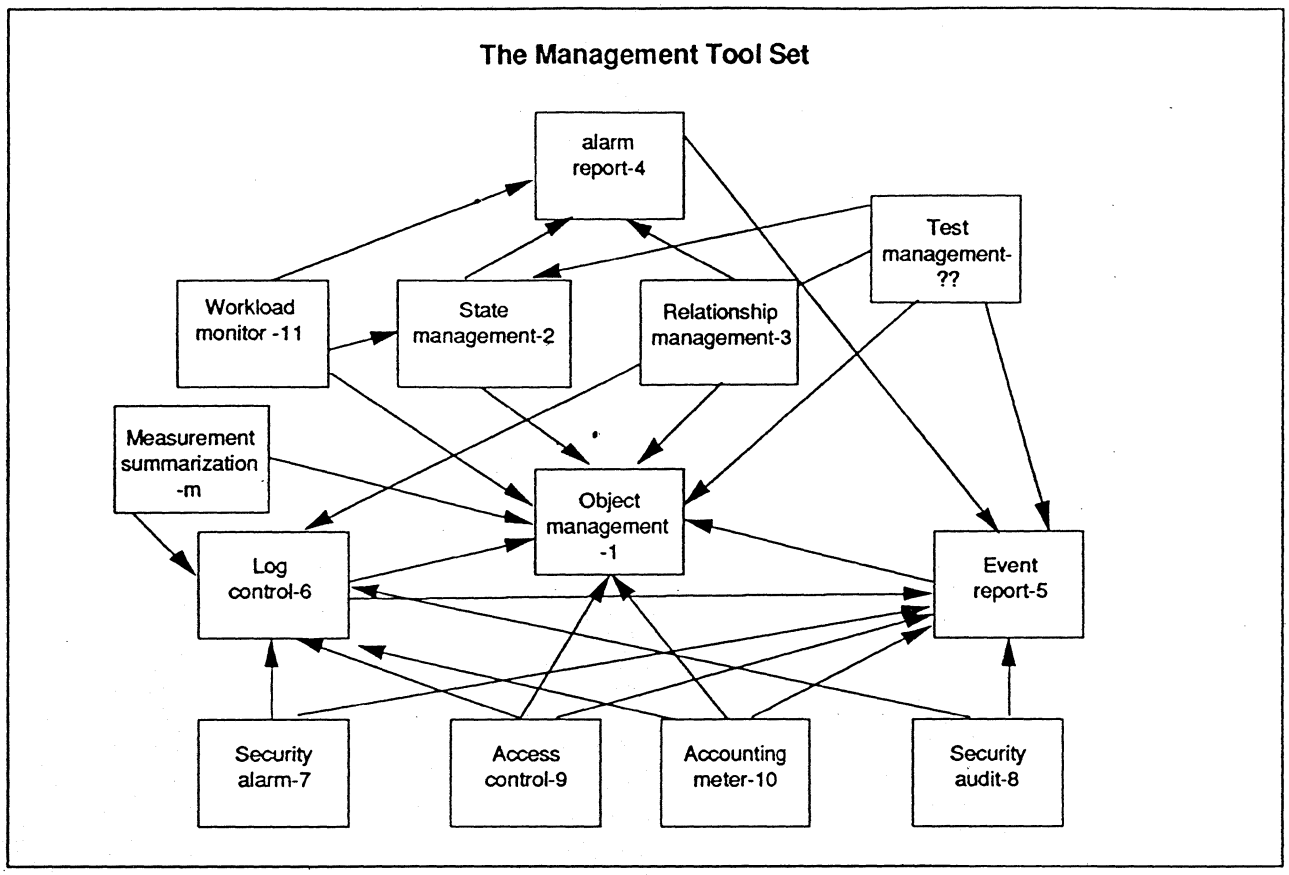


Figure 4

Recommended counters include the number of deferred transmissions (if the bus was busy) and the number of octets received. Optional counters measure such things as the number of multicast or broadcast frames sent or received.

Control functions are also included so the MAC operations can be managed. A management application can perform actions through the MAC layer manager such as initializing the MAC (mandatory), adding a group address, enabling/disabling transmit or receive functions, and modifying the MAC address.

The network and transport layer managed objects are considerably more complicated because they deal with protocol machines (X.25, the connectionless protocol, CLNP, etc.), connections, addresses, and interfaces to the neighboring layers.

Other Developments

Another encouraging development is that new OSI specifications are incorporating management requirements and definitions as they are developed. A particular case in point is the development of ISO 10589, the IS-IS routing exchange protocol. Intermediate systems, such as routers, will use the IS-IS protocol for exchanging routing information within a given routing domain. An extension to the specification uses the guidelines set forth in the Structure of Management Information and defines the required managed object classes and attributes that will be necessary for managing an Intermediate System in an open routing environment. This is one of the first cases of management specifications being included with a protocol specification. Further developments are expected to follow as new specifications are completed.

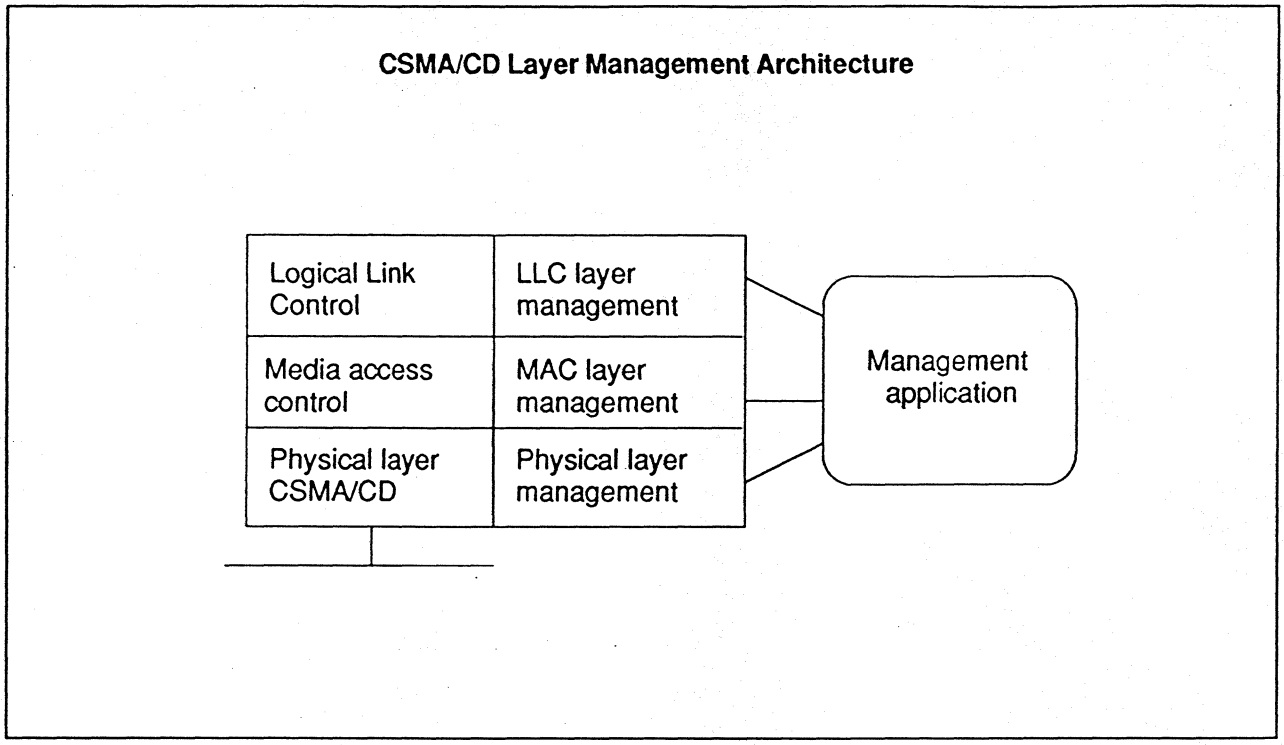


Figure 5

OSI Network Management Forum

The OSI Network Management Forum, an independent consortium of vendors building OSI network management products, has undertaken the task of being closer to the bottom of the hierarchy of specifications. This vendor consortium has taken responsibility for translating the higher level specifications of the OSI standards into the particular and specific details that will be necessary to build OSI-compliant management products. Is the ball in its court? The Network Management Forum released its first library of managed objects in June 1990. This first library is very sparse and is a long way from providing the necessary information to realize products.

For example, although there are seventy defined objects, many relate to records that are captured in logs. Logging information for later analysis is certainly important, but there is a need for many more objects that model real elements in real networks. There are very few objects in these seventy that relate to actual network elements such as a LAN bridge, protocol entity, circuit, and system. Further definitions must be supplied to ensure interpretability. For example, attribute value ranges, notifications, and other information must be treated in the same manner by each equipment vendor.

In contrast, the SNMP management information base (MIB) now contains almost three hundred managed object definitions and variables. The OSI Network Management Forum still has substantial work to do if it is to meet its goal of demonstrating interoperable management products by the end of 1991.

And NetView?

These developments continue to raise user questions about the role of NetView. IBM has indicated that NetView will evolve to a multiprotocol platform that will manage SNA, OSI, and TCP/IP elements through a single, consistent interface. While this is a worthy goal, it seems there are still many unanswered questions. Among them:

Where is the shared database that management applications need? The Repository from AD/Cycle has been considered a likely candidate for this role; however, no definite commitments have been made.

How will a single interface work? Managing current SNA devices that are not designed for the emerging environment will be difficult. Both OSI and TCP/IP use an object-oriented approach that is very different from the SNA network management vector transport (NMVT). Will there be a mass of conversion software hidden under the interface?

How will the NetView interface be changed? It must certainly be enhanced to incorporate a more sophisticated information model if applications are going to be easy to write.

What about resource utilization? NetView has a bad reputation for excess consumption of expensive mainframe cycles. Processing more complex data structures and management operations will not reduce the loading.

Conclusions

Substantial progress has been made recently in the OSI management standards. As the framework solidifies there should be an increasing rate of progress. The needed details for building real, manageable products are closer to stability. Many vendors are already designing the required management agents and instrumentation so their products can participate in a multivendor environment.

NetView still remains a question mark. IBM needs to make clear its intentions and its timetable if it wants to keep NetView at the top of the management hierarchy. Many other platforms will be able to manage multiple protocol suites and they appear to be ahead of NetView in terms of availability and capability. NetView may be relegated to the subsidiary role of SNA manager while other platforms manage the rest of the multivendor enterprise. On the other hand, IBM has surprised the industry in the past with dramatic leaps. The coming year will be interesting to watch. ■

(Continued from page 1)

Why Systems Management?

System management is an essential element of any LAN management plan for the following reasons:

- Applications are the ultimate source of traffic and congestion on networks and thus affect network behavior and performance
- Many workgroup environments have grown without much direction. Administrators have difficulty maintaining current inventories of systems and their resources
- Administrators spend a great amount of effort troubleshooting user problems, many of which are due to improperly configured software
- The integration of workgroups and the corporate MIS environments requires stronger control and more consistency in procedures, applications, and management. Client-server computing throughout the enterprise demands closer coordination of all the elements

NetView Architecture: Where Does It Fit?

NetView has its own architecture which does not yet converge with the OSI management framework, although there are similarities. Both use an indirect management approach whereby a central manger issues directives to components which actually manage network elements.

The NetView Focal Point is analogous to a manager within the OSI architecture: it receives the management information, acts on it, and issues directives to an Entry Point. The Entry Point in turn directly controls devices such as cluster controllers, switches, Token-Ring gateways, and so forth. OSI management has a more clearly defined hierarchy which allows an agent-manager combination which can be used to manage a specific domain.

NetView is evolving in this direction as the Token-Ring LAN Network Manager is integrated into the NetView environment. The major differences are the lack of an integrated database to support

NetView applications and an object-oriented approach to management information. Without these elements, it will be difficult to position NetView as a major multivendor management platform.

The System Agent

The manager-agent architecture requires an *agent* in each managed system. The agent manages system resources under the direction of a remote management system. As viewed from a management perspective, resources include:

- the protocol suite(s) used for communication
- memory
- peripherals
- access control information (passwords, etc.)
- applications
- the operating system
- operational information such as CPU utilization, communicating partners, and system faults

Manager-agent communications use a management protocol to exchange information and instructions. Current systems management products use proprietary protocols. The growing influence of TCP/IP's simple network management protocol (SNMP) makes it very likely that the next product generation will be SNMP-based. The OSI common management information protocol (CMIP), the emerging international standard, will become a factor after the standards stabilize. CMIP will find its earliest popularity, however, in manager-manager communications. See the sidebar on CMIP and NetView.

Agent Operations

An agent carries out instructions issued by a manager, as shown in Figure 6. Operations include:

- Reporting requested operational information
- Changing system behavior such as reinitializing or deactivating software
- Reporting events such as interface failures, lack of buffers, and communication problems.

System agents are intimately related to the specific operating environment. For example, a UNIX platform can easily add an agent as a daemon while a DOS system would use the more complicated terminate and stay resident (TSR) approach. Access to operating system information is necessary in order to carry out the agent's responsibilities. More sophisticated management schemes will also include a mechanism for the agent to directly influence the operating system.

Software versus Hardware Agents

Early implementations of agents were software-based. Manager-agent communications could be interrupted by incorrect installation or user errors. Hardware-based agents that reside on network adapter boards are beginning to appear. They place the agent directly in the communications path and guarantee better remote management control. *SNA Perspective* expects these advantages of hardware agents will generate demand and encourage more vendors to offer them.

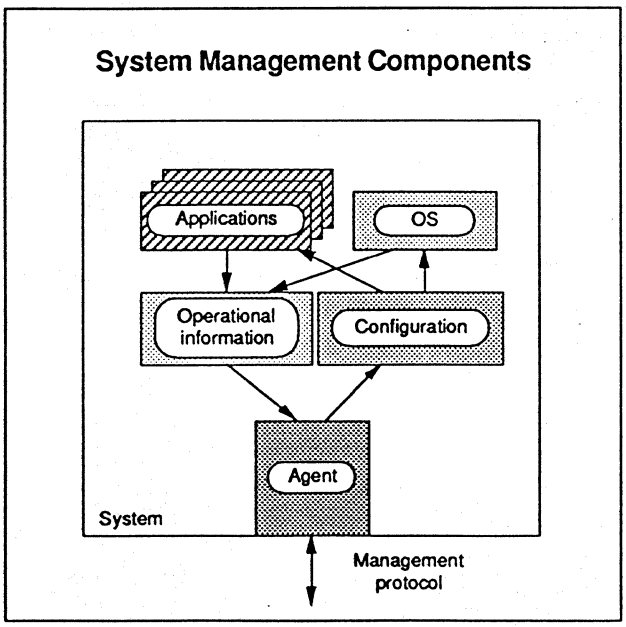


Figure 6

Remote Operation

One of the first uses for an agent is remote operation. With this capability a system administrator can exercise some degree of control across the network. The expertise of a small technical staff can be leveraged to the maximum by allowing them to work with systems from a single site. Personally visiting each system that needs attention is very expensive, especially given the shortage of experienced network management personnel.

With a remote operation capability, a system administrator with the appropriate privileges can take over the keyboard and capture the screen of a remote system on the network. Once remote operation is activated, the administrator can work with a user or perform other tasks alone. For example, troubleshooting is simplified because a remote administrator can monitor a user's actions and demonstrate corrective actions. The administrator can delve into system information when the problem is more stubborn.

One remote operation capability, included in several products, is a "chat window" that enables the user and the administrator to carry on a separate dialogue that does not interfere with any procedures and operations that are being carried out.

Configuration Management and Software Distribution

Configuration problems consume a great deal of any system administrator's time and attention. Many so-called network problems can actually be traced to configuration errors, using incompatible versions of the same application software, or failing to follow the correct procedures. These problems will be compounded in the future because the growing dissemination of desktop technology will involve users who are less sophisticated.

Manually installing software on hundreds of systems is a potential source of problems because of inconsistent information, procedures followed incorrectly, and so forth. Distributing and installing software throughout the network from a central

CMIP and NetView

NetView is currently the most sophisticated, mature, broad-spectrum network management system available. However, although optimized to support large SNA systems, it faces limitations when adapted to manage TCP/IP, OSI, or other non-SNA networks.

From the TCP/IP world, SNMP has less feature/function breadth and system size capability, though it is continually being enhanced by the Internet Engineering Task Force. CMIP is comparable to NetView in breadth of architecture and capability. Because of its recent development, it does not have the real world experience of NetView but, on the other hand, it has the added advantage of being an open rather than a proprietary solution.

SNA Perspective believes that IBM is in the process of changing NetView from the inside out to comply with the OSI CMIP standard. For example, a hint of this was given in fall 1990 when LU 6.2 support was added to NetView and its new management services unit is not NMVT based. Also, in April 1990, IBM described a plan to use an adapted form of CMIP over SNA sessions to manage SNA nodes, though delivery of this enhancement is probably still over a year away.

Moving NetView closer to OSI management standards will provide several benefits:

- Enhanced NetView capability to manage OSI networks
- Enhanced NetView focal point–to–CMIP manager interactions
- Familiar NetView interfaces and leverage of existing investment in NetView staff training and experience ■

point will reduce these problems substantially. System management agents can be used to support this function.

File transfer is the easiest part of software distribution. Standard file transfer can be employed to deliver new software to any system. However, once the software has arrived it must be installed and integrated into each system environment.

Software may be configured before distribution when many systems have an identical configuration. In this case, it is simply transferred and placed in the appropriate directories. In the more likely scenario today, configurations are more variable and the installation will require different steps for each system or system type. In either case, remote operations capabilities will probably be used to complete the process and ensure that the installation was successful.

Software distribution will be automated so that applications monitor and track the distribution and installation process. Such applications will also build a configuration database for the workgroup that the administrator can use for other purposes as well. Applications could track outdated versions of software and delete them, forcing the user to obtain the correct version. Further, when two systems have a problem interfacing, the administrator can access configuration information for both.

Application Management

Ultimately, systems management will require managing the applications executing within that system. There are several aspects to application management. One aspect is to ensure that the application is well-matched to the system and to the network resources that are supporting it. For instance, more sophisticated configuration procedures would ensure that an application doing bulk transfer would have enough buffering to support high bandwidth communication across the network. Further, it would select network options such as packet size and flow control windows to optimize high-volume transfers. Balancing all these factors optimizes use of network and system resources.

Another important aspect of application management is managing applications from a remote management platform. For instance, the network may become congested because of failures or unexpectedly high traffic loads. Using information about a particular workgroup or enterprise environment, the system administrator can change application behavior with remote management tools. Low priority applications could be suspended, thus removing their traffic from the network and giving the essential applications the resources they need.

Political Pitfalls

One of the initial attractions to workgroup users of LANs was the relative freedom from organizational or corporate MIS constraints. As LANs are integrated into the corporate environment, appropriate organization-wide controls and more centralized management of these distributed workgroups is becoming increasingly necessary. The free and effective interchange of corporate information is impeded when users employ incompatible applications with different protocols, data formats, and so forth. Bringing consistency to the LAN environment will require administrative control of each local system environment.

Workgroups that value their independence from the MIS culture will resist giving up some of that freedom for the good of the entire organization and to meet organization-wide information interchange goals. Introduction of systems management tools will have to be carefully considered in order to minimize the political side effects of such a change in the distributed computing environments.

Privacy and Security

Security and privacy are major considerations in introducing remote systems management. When an outsider can take control of a local system, there is potential for abuse. Users will be concerned about privacy issues; the idea of a system administrator with the capability to read private files and electronic messages without the user's specific knowledge can be very upsetting. Recent lawsuits by employees on this very subject underline the

significance of this concern. These particular issues transcend the technical issues and require organizational focus and policies.

Products

Initial products indicate the immaturity of systems management approaches on LANs. Although complete functionality is still at least a year away, some products illustrate the possibilities. A quick review of features is given in Table 2.

AT&T has developed its StarGroup management products for Intel-based UNIX systems. A system administrator can take control, distribute software, manage the configuration and help a user troubleshoot problems. Additional features allow a system administrator to assign new users, determine the application mix, and receive indications of resource utilization.

Farallon Systems has had Timbuktu on the market for some time. Timbuktu is a Macintosh-based remote management tool that works within a graphic interface environment (in fact, it is the only product that does this at this time). System administrators can use Timbuktu to troubleshoot and configure remote systems. Timbuktu is being enhanced to increase its capabilities.

Hewlett-Packard has systems management products for its UNIX systems that run under its OpenView platform. A system administrators can deliver software, configure systems, and work with users. New products are being introduced at a rapid rate. OpenView is also moving beyond SNMP, integrating Novell networks with systems management products from Network Computing, Inc.

IBM has the Distributed Console Access Facility (DCAF) which allows a system administrator on a PS/2 to control OS/2 and DOS systems across an

Some LAN Systems Management Products and Features

Product / Features	AT&T StarGroup	IBM DCAF	HP OpenView	Farallon Timbuktu
Remote operation	Yes	Yes	Yes	Yes
Chat windows	Yes	No	Yes	Yes
Trouble shooting	Yes	Yes	Yes	Yes
Software distribution	Yes	No	Yes	No
Configuration management	Yes	Some	Yes	Yes
Application management	Some	No	No	No

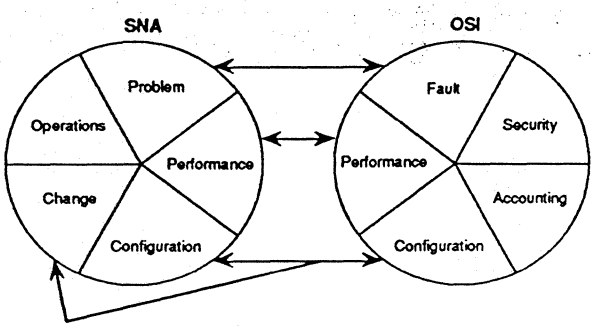
Table 2

SNA network on a LAN. DCAF is nothing more than an LU 6.2-based remote operations package at this point. No software distribution or application management tools are available. DCAF may be an interim product that will be replaced by Station Master after its release in late 1991. Station Master will be a CMIP-based systems agent implementing the heterogeneous LAN management (HLM) specifications developed jointly by IBM and 3Com. The recent IEEE adoption of HLM will make it an important element in the LAN management picture.

SystemView is IBM's strategy for management of systems and networks which was announced in September 1990. SystemView currently includes NetView and some existing management products renamed to fall under the SystemView umbrella. Future LAN systems management products will also likely fit into the SystemView strategy.

Conclusion

Systems management is becoming an essential element of LAN management strategies, expanding the focus of LAN management beyond the physical facilities to encompass the attached systems. Building the appropriate systems management tools will be a lengthy task since the operating systems and applications must also be engineered to work within a new paradigm, to become more manageable. Users should begin to investigate the emerging tools and plan how best to use them. ■



OSI Versus SNA Management Architectures

The correspondence between SNA and OSI functional divisions is more exact in some areas, less exact in others. Of the five areas, the clearest mapping is of OSI Fault Management with SNA Problem Management; likewise, Performance Management is identical in both the OSI and SNA frameworks. Less clear is Configuration Management, which in the ISO framework encompasses both SNA Configuration Management as well as SNA's Change Management. In the remaining two areas, OSI and SNA depart completely from each other's division of functions. SNA has no functional area corresponding to either Accounting or Security Management. These are subsumed to a degree in other SNA areas, and have their functionality provided by the associated IBM operating systems and access methods such as Multiple Virtual Storage (MVS) and Virtual Telecommunications Access Method (VTAM). ■

Architect's Corner

3270—Draw Up The Middle

by Dr. John R. Pickens

Like Joe Montana and football, IBM has architected many plays for the game of distributed computing. The LU 6.2 long bomb, the SNADS delayed hand-off, the NetBIOS/DLC streak, the IND$FILE flea flicker. But, repeatedly, IBM returns to its tried-and-true stalwart, the 3270 play-action fake and draw up the middle. (To those readers for whom the game of football connotes something other than a hundred yards, four downs, and sixty minutes, the less metaphorical characterization follows.)

Most people, myself included, continue to be surprised not only by the durability of 3270, but also by its adaptability. We often tend to think of 3270 as an "SNA" data stream—more precisely as an SNA logical unit type 2. Yet the 3270 data stream today, as well as historically, has been capable of being utilized in other protocol environments, such as TCP. Surprised? How is it possible?

First, a brief review. What is 3270, really? Originally, 3270 was a real device. But not any more. The designation "3270" is now generic—like Kleenex or crescent wrench—denoting the block-oriented terminal function that was exhibited by the original device. Now this function is implemented in many types of devices, ranging from the successor of the 3270—the 3178/9 et. al.—to emulation software running in personal computers and minicomputers.

The so-called 3270 data stream is documented in IBM document GA23-0059 3270 Data Stream Programmer's Reference. Notable in recent years is the degree to which the data stream has been added to, as a sort of universal function carrier. Besides the original basic emulation function, the data stream now has extensions to support file transfer (two types), mixed object content, graphics, and cooperative processing (SRPI). It is only a matter of time until the 3270 data stream is enhanced with functions commensurate with today's GUI environments.

3270, however is not the fundamental base for distributed and cooperative processing. That role is reserved for LU 6.2, RPC, SNADS, etc. Yet 3270 continues to be adapted to multiple underlying transport protocol environments.

Figure 7 shows the three mainstream forms taken by 3270 since its inception, plus two projected future configurations. There are other configurations, notably DFT for coax attachment and NetBIOS for early, obsoleted versions of the IBM 3270 emulation program and its gateway feature.

How is 3270 so adaptable? Layering. In all cases, the 3270 presentation services data stream is common—the same commands, orders, aid keys, structured field extensions, etc. What differs is the underlying transport layer architecture. What differs from transport environment to transport

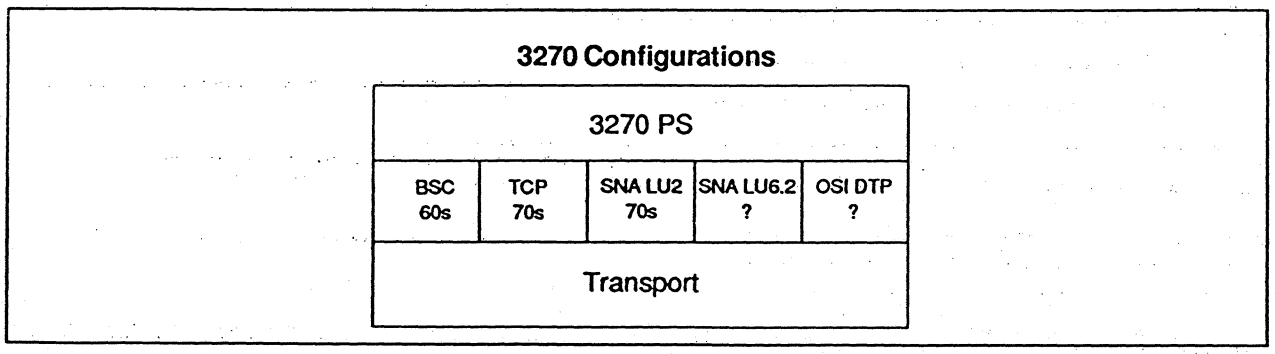


Figure 7

environment is the method for establishing sessions, negotiating facilities, handling contention functions, etc. But the basic 3270 data stream is the same.

The TCP variant of 3270 is called tn3270. This tn3270 is implemented in a variety of systems—UNIX, DOS, or OS/2 as 3270 clients; 9370, S/370, S/390 hosts (VM environment) as 3270 servers. RFC 1041 describes the mechanism for establishing TCP sessions between a 3270 end system and a host as well as how to use telnet to negotiate session options. Documentation of the data stream, however, is contained in the above referenced 3270 data stream reference.

Are more transports in 3270's future? Certainly. LU 6.2 is the most obvious candidate. I have mentioned this direction several times previously. I first heard the 3270/6.2 rumor in 1986. Yet it hasn't materialized. Certainly, inclusion of 3270 in SAA mandates LU 6.2 transport—LU 2 is not an SAA data stream. My suspicion is that it awaits release of the LU 6.2 NT 2.1 capable version of the 3174 establishment controller—probably in 1991. An LU 6.2 version of 3270 would capitalize on the expanded internetworking provided in APPN networks, break the 256 session limit, and be SAA compliant.

And an OSI version of 3270 cannot be far behind. What transport layer would be used? Possibly DTP—the OSI equivalent of LU 6.2—or perhaps the OSI session layer. Whichever method was used, the architecture layering principles would be the same: perform transport-specific session negotiation, but convey standard 3270 data stream.

At the line of scrimmage, IBM continues to call 3270 audibles in the game of distributed processing. Such strategies will continue to succeed until LU 6.2 (IBM's run-and-shoot offense) firmly takes hold. ■