The Integrated Energy and Communication Systems Architecture

Volume IV: Technical Analysis

Appendix B:
Network Management Technologies

EPRI Project Manager

Joe Hughes

Cosponsor

Electricity Innovation Institute Consortium for Electric Infrastructure to Support a Digital Society (CEIDS)

EPRI • 3412 Hillview Avenue, Palo Alto, California 94304 • PO Box 10412, Palo Alto, California 94303 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATIONS THAT PREPARED THIS DOCUMENT

General Electric Company led by GE Global Research (Prime Contractor)

Significant Contributions made by
- **EnerNex Corporation**
- **Hypertek**
- **Lucent Technologies (Partner)**
- **Systems Integration Specialists Company, Inc.**
- **Utility Consulting International (Partner)**

ORDERING INFORMATION

Requests for copies of this report should be directed to EPRI Orders and Conferences, 1355 Willow Way, Suite 278, Concord, CA 94520. Toll-free number: 800.313.3774, press 2, or internally x5379; voice: 925.609.9169; fax: 925.609.1310.

Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc. EPRI. ELECTRIFY THE WORLD is a service mark of the Electric Power Research Institute, Inc. All other trademarks are the property of their respective owners.

Copyright © 2002, 2003, 2004 Electric Power Research Institute, Inc. All rights reserved.

CITATIONS

This document describes research sponsored by EPRI and Electricity Innovation Institute.

The publication is a corporate document that should be cited in the literature in the following manner:

THE INTEGRATED ENERGY AND COMMUNICATION SYSTEMS ARCHITECTURE, EPRI, Palo Alto, CA and Electricity Innovation Institute, Palo Alto, CA: 2003 {Product ID Number

Appendix B – Network Management Technologies

This appendix provides a survey on some of the network management technologies discussed in Volume. IV, Section 3. The attached references, specifically [Manii 00] and [Raou 02}, have been used in putting together this appendix.

1.1 ISO

OSI network management, developed by ISO [ISO], is a comprehensive network management standard covering the seven layers of the OSI network reference model. Common Management Information Protocol (CMIP) is based on the ITU-T X.700 recommendations [ITU X720, X721], along with extensions for TMN [ITU M3010] via the M.3000 series and technology or interface specific standards such as ITU-T G.774 for SDH. CMIP has built-in services, Common Management Information Service (CMIS), that specifies the basic services for various functions.

CMIP's advantages compared to SNMP [RFC 1157, 1441-1452, 2570-2580] include: (i) CMIP uses transport protocols that provide packet delivery assurance, while SNMP uses UDP which provides no guarantee of data delivery, (ii) CMIP is truly object oriented and includes the concepts of containment and inheritance, whereby the status of a global object is reflected in less global elements. In SNMP inheritance is not provided, and finally, (iii) CMIP includes event filtering by either the managed entity or management system.

The additional CMIP functionality comes at the expense of software complexity. The CMIP/CMIS stack is larges and can be of an issue on ordinary workstations or small devices. The protocol in the past has only been supported on larger systems where the investment could be justified. In general, the direction of the industry has been increasingly towards SNMP, even in the public network management space.

The OSI functional model includes:

- **Performance Management** - The task of performance management involves measurements of various metrics for network performance, analysis of the measurements to determine normal levels, and determination of appropriate threshold values to ensure required level of performance for each service. Examples of performance metrics include network throughput, user response times, and line utilization. Management entities continually monitor values of the performance metrics. An alert is generated and sent to the network management system when a threshold is exceeded.
- **Configuration Management** - Configuration management involves maintaining an inventory of the network and system configuration information. This information is used to assure inter-operability and problem detection. Examples of configuration information include device/system OS name and version, types and capacity of interfaces, types and version of the protocol stacks, type and version of network management SW, etc.

- **Accounting Management -** Accounting management keeps track of usage per account, and ensures resources are available according to the account requirements.
- **Fault Management -** Fault management detects, fixes, logs, and reports network problems. Fault management involves determining symptoms through monitoring and measurements , and isolating the problem.
- **Security Management -** Security management is to control access to network resources according to security guidelines. Security manager partitions network resources into authorized and unauthorized areas. Users are provided access rights to one or more areas. Security managers identify sensitive network resources (including systems, files, and other entities) and determine accessibility of users and the resources. Security manager monitors access points to sensitive network resources and log inappropriate access.

1.2 ITU (SG IV, TMN)

The ITU Telecommunications Management Network (TMN) [ITU M3010] consists of five layers: the Element Layer (EL), Element Management Layer (EML), Network Management Layer (NML), Service Management Layer (SML) and Business Management Layer (BML), as shown in Figure 1.

The first three layers are applicable to the management of a physical network. The NML provides the network manager with a unified view of the network under one management domain. This layer will operate through the EML, which provides the groupings of similar Network Elements (NEs). The lowest management layer, EL, performs basic management of the network equipment. The Service Management Layer provides for monitoring of services and statistics gathering functions. It includes customer-facing elements and interacts with the network management layer. Above the Service Management Layer is the Business Management Layer, responsible for business agreements between service providers. In addition, it allows for interfacing with other operators at the service and network management layers.

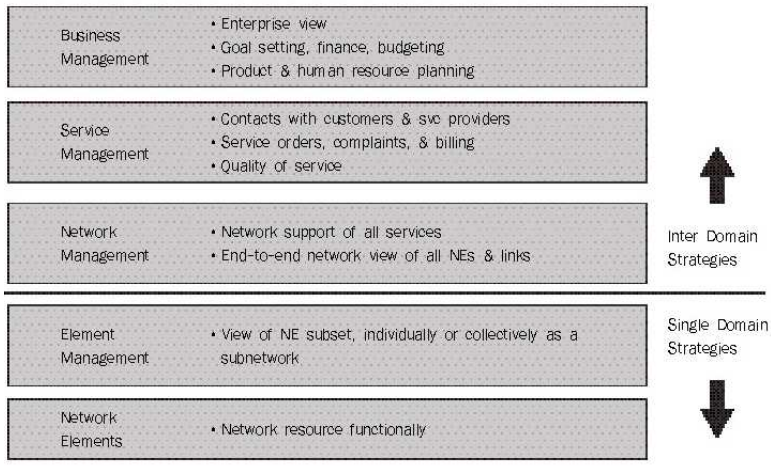

Figure 1: The TMN Framework.

TMN consists of an architecture to interconnect the various provider Operation Support Systems (OSSs) and equipment from different vendors. It also allows for the exchange of management information between different provider TMNs. The functional architecture provides for the logical allocation of functionality, while the physical architecture defines the actual interfaces and physical components. The information architecture defines the manager-agent and managed object concepts, through which, concepts such as object request brokers are introduced to insulate applications from network elements. The Common Object Request Broker Architecture (CORBA) [CORBA] and web-based management are examples.

Each interface in the TMN management architecture, namely M1 to M5, has certain characteristics and provides for different management capabilities: M1 and M2 are interfaces between a private network management system and either a Customer Premise Equipment (CPE) or a private network. M3 is the interface between private and public networks. M4 defines SNMP or CMIP management connection to a public switching systems. Finally, M5 interface connects one TMN to another for carrier-to-carrier information exchange.

1.3 IETF (SNMP, RMON)

The IETF Internet-Standard Management Framework [RFC 1441, 2570, 2571] consists of the following:

MIB - Definitions of network management objects known as Management Information Base (MIB) objects [RFC 1212,1450,1451,1907]. The management information is represented as a collection of managed objects that form a virtual information store known as the MIB. A MIB object might be a traffic/error counter, or descriptive information such as version of software running on the device, or protocol-specific information such as a routing path to a destination. MIB object define the management information maintained by a managed device.

SMI - A Data Definition Language, known as SMI (Structure of Management Information) [RFC 1155, 1442,2578] that defines the data types, an object model, and rules for writing and revising management information. MIB objects are specified in this data definition language.

SNMP - A protocol, SNMP (Simple Network Management Protocol) [RFC 1157, 1445,2570-2573], for conveying information and commands between a managing entity and an agent executing on behalf of that entity within a managed network device. SNMPv2 was a major step towards a more distributed paradigm of network management. It introduced the concept of intermediary manager [RFC 1451], which can be considered to be a "middle manager". The managing entity communicates directly with the intermediary managers and exchange command information. The intermediary managers then handle data exchange with agents. The intermediary managers assume some of the data processing from the managing entity and are capable of performing simple tasks such as periodic status pulling from agents without the intervention from the managing entity. SNMP provides varying degrees of security and security features depending on the version being used. SNMPv1 provides a weak form of security called the community-

based security model. SNMPv3 has a comprehensive security model, providing approaches for encrypting the SNMP message, replay detection/ protection, and anti-spoofing mechanisms.

RMON - RMON (Remote MONitoring) [RFC 1757] is a step towards management distribution. RMON used the concept of monitors (or probes), which are network monitoring devices. The task of a monitor is to track the network traffic at its local region and report anomalies, in the form of alarms, to its managing entity. By defining alarm types and alarm thresholds, the managing entity is able to offload some data gathering and decision-making, e.g. event filtering, to the monitors. Furthermore, monitors can also perform some data preprocessing before forwarding them to the managing entity. The RMON specification is primarily a definition of a MIB. The effect, however, is to define standard network-monitoring functions and interfaces for communicating between SNMP-based managing entity and remote monitors.

1.4 IEEE

The IEEE standards for management of Local and Metropolitan Area Networks (LAN & MAN) are concerned with physical and data link layers [IEEE]. CMIP and SNMP protocols both use the IEEE standards for the lower layers.

1.5 Web-based Network Management

A number of web-based network management solutions have been proposed and built. The main problems Web-based network management tries to address are: platform heterogeneity, lack of management console accessibility, and high cost of management platform deployment and maintenance [Mart 98, Thom 98, Ju 01]. Traditional network management solutions are platform-dependent, with proprietary management consoles, and varying user interfaces for each management platform. Web technology addresses these problems by providing ubiquitous management consoles in the form of standard web browsers.

Proprietary network management platforms are expensive and difficult to maintain. Web technology solves this issue by promoting HTML and Java-based platforms, providing a seamless Graphic User Interface (GUI) accessible everywhere. Other problems with traditional network management techniques that are being addressed by web-based techniques include: use of decentralized network management processing platforms, and reduced use of polling.

The degree to which web technology is used in network management varies from use of web browsers and access to the traditional management platform (simply web-extensions of their current network management systems), to full web-based management systems.

One of the common and possibly simplest approaches to use web technology into network management is the use of management gateways between Web browsers and the devices managed by traditional NM agents such as SNMP or CMIP. The management gateway converts HTTP requests to SNMP/CMIP requests to be sent to the SNMP/CMIP managed agents, and on the reverse direction translates the response into web documents. The advantage of this approach is the ability to use existing NM agents and only enhance

the NM console. However, the disadvantage is in the fact that the gateway may become a bottleneck in a large network and traffic engineering of gateways is needed.

Another web-based approach is to use web-embedded servers and apply web technology to all managed devices. Each managed device is a miniature web server, capable of accepting HTTP request and constructing HTML/XML presentation of device data. Because of the self-contained nature of web-embedded servers, there is no requirement for additional management support. A network manager can interact with a web-embedded device via a standard web browser. The problem with this approach is that web-embedded servers are not deployable on devices with limited resources and processing power. Furthermore, there are many existing network devices which have traditional NM agents.

The above two types of web NM approaches are the most adopted solutions in the network management domain today. In both cases, preliminary processing of device data, formulation of status report, and GUI presentation are handled by separate entities other than network managers.

The most involved web-based NM approach is to use web technology as the core technology in the design of new network management platforms, with its own management protocol, data model, and architecture. Two main proposed full web-based management approaches are Web Based Enterprise Management (WBEM) [WBEM]and Java Management eXtensions (JMX) [JMX]. Both JMX and WBEM are to establish new technology as the standard for future network. WBEM and the JMX technology do not attempt to replace existing network management systems, rather to provide a framework for unification.

1.1.1 WBEM

WBEM [WBEM], under the control of the Distributed Management Task Force (DMTF), is based on a new object model, a new management protocol on top of HTTP as the network management platform. WBEM proposed the way for the encoding of the Common Information Model (DMTF CIM) schema in XML. The DMTF CIM is an object-oriented information model, providing a conceptual framework within which any management data may be modeled. Allowing DMTF CIM information to be represented in the form of XML brings the benefits of XML and its related technologies to management information, which uses the DMTF CIM meta-model.

The XML encoding specification defines XML elements, written in Document Type Definition (DTD), is used to represent DMTF CIM classes and instances. The encoded XML message could be encapsulated within HTTP. Further, WBEM defines a mapping of DMTF CIM operations onto HTTP that allows implementations of DMTF CIM to operate in a standardized manner.

1.1.2 JMX

JMX [JMX], formerly Java Management API (JMAPI) proposes that the managed objects will be Java-OS based and RMI will be used for communication. Java Management Extension (JMX) is a new addition to the Java platform that promises a

scalable, low-implementation cost, and legacy-compatible solution to the problems associated with enterprise network management. There are various features of the Java platform that make it a good candidate for the implementation of complex network management solutions, including platform and OS independence, networking, and dynamic adaptability. The ability to dynamically and securely load classes across the network can be leveraged by network management software. For example, a Java-based EMS can support new devices or services by "loading" its support module across a network, and software modules that implement network management intelligence can be dynamically upgraded on demand. However, the issue of performance with Java remains an area of concerns for the developers.

JMX is an effort to create a set of specifications that will describe architecture, API, and a set of distributed services for network management using the Java programming language. The goal of JMX is to define only the interfaces that make up the systems within the JMX architecture, but not to dictate implementations and policies. The JMX specification defines the interface for basic services as a registry (*Mbean Server*) for *Mbeans* (JavaBeans for management). These services enable agents to manage their own resources and let managers forward information back and forth between agents and management applications.

In the JMX architecture, both services and devices are treated as managed objects. The components, *Mbeans*, can be added and removed as needs evolve. Appropriate protocol adapters can provide a recognizable object to the Browser or JMX manager whose specification is under way. JMX depends greatly on Java. In order to be instrumented in accordance with the JMX, a resource must be fully written in the Java programming language or just offer a Java technology-based wrapper. Java Virtual Machine is a basic requirement for the management application. This heavy technology dependency on Java results in less generality. Figure 2, from www.java.com, shows the various components of JMX.

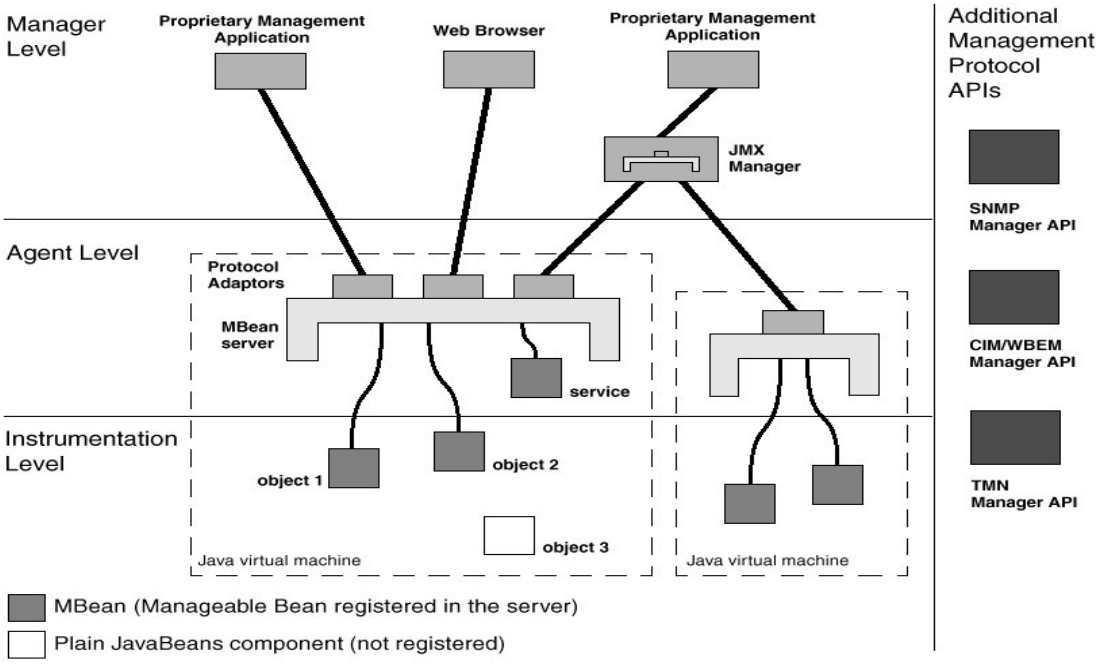

Figure 2. JMX Components

1.6 Distributed Object Computing for NM

Distributed Object Computing (DOC) uses Object-Oriented methodology to construct distributed applications. It supports a distributed network management architecture and integration with existing heterogeneous network management solutions.

DOC provides distribution of services and applications transparently by separating object distribution complexity from network management functionality. Another advantage of this separation of concerns is the ability to provide multiple management communication protocols accessed via a generalized Abstract Programming Interface (API), supporting interoperability of heterogeneous network management protocols, such as SNMP and CMIP. In addition, DOC provides distributed development platform for implementation of unified, and reusable services and applications.

Current DOC in network management is oriented around the Object Request Broker (ORB) concept. ORB facilitates communication between local and remote objects in a way that free the application from low-level infrastructure and communication concerns. The two major adaptation of DOC to network management are: Common Object Request Broker Architecture (CORBA) [CORBA, OMG99] and Distributed COM (DCOM) [Roge 02].

DOC has been used to design distributed network management systems. Example is the standardization work done by Telecommunication Information Network Architecture Consortium (TINA-C) [Proz 97] and Joint Inter Domain Management (JIDM). Their proposed frameworks provide transparent remote services invocation using DOC support. Thus, the management processing and services do not need to be located at centralized

locations in the network, but rather distributed across remote locations. This feature allows management tasks to be delegated, by region or by functional areas, to intermediate entities, making managers no longer the center of all management decision making. DOC is also used to augment existing network management infrastructures with distributed capability.

CORBA [OMG 99] is a well-received technology for developing integrated network management architectures with object distribution [ITU M3120, ITU Q8221, DSLF TR041, ATMF 02]. The success of CORBA can be attributed to the fact that CORBA has well-established supporting environment for run-time object distribution and a set of support services. Thus, CORBA is useful as integration tools for heterogeneous network management domains, and extending deployed network management architectures.

Issues that limit DOC's deployment is that it uses static object distribution. Furthermore, DOC requires dedicated and heavy run-time support, which may not always be feasible on every device in the network.

1.7 Policy-based Network Management

Policy-based network management [Casa 00, Dobs 89, Lupu 99, Moff 93, RFC 3084, 2748, 3483] has been primarily used as representation of information in security management. In policy-based network management, policies are defined as rules that govern the states and behaviors of the network elements. The management system needs to translate the management objectives to syntactical and verifiable rules governing the function and status of the network, the translation of these rules to mechanical and device-dependent rules and configurations. Further, it needs to manage distribution and enforcement of these configurations by management entities. The reference model of policy-based network management consists of Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs). PDP's perform the translation and distribution of policies, while PEPs handle the enforcement. The benefit of policy-based network management is that it promotes the automation of establishing management level objectives over wide-range of network devices.

Resource Allocation Protocol [RFC 2748] is a query and response protocol that is used to exchange policy information between a policy server (PDP) and its clients (PEPs). One example of a policy client is a router that must exercise policy-based admission control. Some proposals push the mundane policy decision tasks from the PDPs to the PEPs. This represents a novel attempt at empowering agents with more management capabilities, moving policy-based network management towards a more distributed intelligence design.

1.8 Intelligent Agents

An intelligent agent is an independent entity capable of performing complex actions and resolving issues on its own. The use of intelligent agents removes the need for dedicated manager entities, as intelligent agents can perform the network management tasks in a distributed fashion, via inter-agent communications [Chei 98, Koch 01]. However, The application of intelligent agents to network management is still at its infancy. It is believed that intelligent agents are the future of network management, since there are significant advantages in using intelligent agents for network management. First,

intelligent agents provide scalable solutions. Hierarchies of intelligent agents could each assume a small task in its local environment and coordinate their efforts globally to achieve some common goal, such as keeping overall network utilization at close to maximum. Second, distributed processing and decision-making removes bottlenecks and increases reliability as compared with centralized network management systems. Third, the intelligent agents are self-configuring and self-managing. Such a system would largely ease the burden of network management routines that a network administrator has to currently struggle with.

Wooldridge and Jennings [Wool 95] defined three intelligent agent architectures: (i) deliberative agents, (ii) reactive agents, and (iii) hybrid agents. Deliberative agents are based on a representation of the management information and management rules. A deliberative agent runs processes using these information to generate overall intelligent actions. Reactive agents do not require complex representation of knowledge. They operate based on environmental observations. Thus, reactive agents are more responsive than deliberative agents due to the lack of any reasoning mechanism. Reactive agents could be applied to traffic monitoring, fault diagnosis, congestion control, and admission control, because these management functions do not have or require perfect representation of a world model. Furthermore, they require rapid responses and actions, which the reactive agents are capable of. Hybrid agents are a mix of both deliberative and reactive agents. A hybrid agent has rules for planning, and decision making, but it can also react to events without complex reasoning. Hybrid agents have been proposed for fault diagnosis. Due to the size and complexity of hybrid agents, they may not be easily usable within any environment.

Aside from technological difficulties with widespread use of intelligent agents, issues remain to be resolved in the area of network management. These include security aspects involved with allowing many intelligent agents autonomously operate within a network, the performance and cost implications of many agents communicating in a mesh-networking environment, and finally availability of agent-agent communication protocols.

1.9 ATM Network Management

A reference model for management of ATM networks is the ATM Forum network management framework, which is based on the five ISO functional areas: configuration, performance, fault, accounting and security management. Both private and public network management are included within this model, which provides for management at the User-Network-Interface (UNI) via the Integrated Local Management Interface (ILMI) [ATMF 96] and SNMP [RFC 1695, ATMF 98], end-to-end circuit management, and "total" management of ATM networks and services. This management model is contained within the ITU TMN also. The ATM Forum has focused on the M3 and M4 [ATMF 99a, ATMF 99b, ATMF 99d] interfaces as standards and MIBs for M1 and M2 were developed external to the Forum.

Public service provider can provide Customer-Network-Management (CNM) capability over the M3 interface so that the network administrator of the private network may have visibility into the public ATM service performance [ATMF 94].

ATM layer management consists of those network management actions, which take place at the ATM cell level and below. These actions may be divided into three categories: alarm surveillance and connection performance monitoring via Operations, Administration and Maintenance (OAM) flows and management of valid/invalid Virtual Path/Circuit Identifiers via the ATM cell header. The ATMF has also extended the RMON paradigm to ATM to define an "ATM RMON" or AMON to provide ATM Layer statistics including cell counts, call setups and traffic matrices. An ATM RMON MIB [ATM 97] has been defined. AMON is also built upon RMON-2 for higher layer functions.

There has been growing realization of the importance of all aspects of management and provisioning in running an ATM network. This is reflected in the wide variety of management platforms available for service providers as well as for enterprise users. In the latter space, combinations of SNMP, ILMI, RMON and Web-based techniques all play a part. SNMP can be used to manage both the network elements and the services themselves. This is evidenced by ongoing work within the ION working group of IETF.

1.10 Access Network Management

1.1.3 Asymmetric Digital Subscriber Line (ADSL) Access networks

The ADSL service provider and/or the ISPs need to manage the end-to-end system at various logical layers as defined in the TMN model described above [DSLF TR022, TR005, TR030, TR035, TR046]. At the Element Layer of TMN, only an ADSL Line MIB has been standardized [RFC 2662] and any additional instrumentation relies on vendor-specific MIBs. The ultimate goal is to combine the relevant elements of these proprietary MIBs into a standard (ADSL) subnetwork MIB. There is also a proposal to combine the Element Network Layer (ENL) and Network Management Layer (NML) functionality in the ADSL space so that the vendors can provide the necessary functionality to allow the service provider to manage the ADSL access network as a single entity. This proposed enhanced NML would then interface with the provider's existing SML.

Regarding the classic the ISO functions: fault, configuration, accounting, performance and security, a set of ADSL Forum Network Operations Reference Model (NORM) documents, have outlined the top-level requirements. For Element Layer management, G.997.1, developed by ITU-T and ADSL, defines the various parameters that may be managed between ATU-C and ATU-R. It also introduces the concept of an ADSL Line and ADSL ATM Path, the former connecting the digital outputs of the respective ADSL modems, while the latter extends from the ATM interfaces at the ATU-C (i.e. DSLAM side) and ATU-R (i.e. the ADSL modem side). The ADSL Line MIB then takes the concepts defined within G.997.1 and outlines an actual SNMP MIB.

For service management, more advanced systems support "flow-through-provisioning", either across the ADSL components of a network or even including an ATM core network. These are functions that occur at the Service Management Layer of TMN architecture. One major complexity with flow-through provisioning is whether a single entity controls all the devices along the end-to-end service path, which is usually not the case. For example, the ILEC (Incumbent Local Exchange Carrier) may be responsible for

the access network (DSLAMs) and the ISP is responsible for the core aggregation function.

1.1.4 Cable Modem (CM) Access networks

The network management requirements to support a DOCSIS (Data Over Cable Service Interface Specification) are defined [DOCS OSSI] document released by CableLabs. The basic network management specification details how SNMP should be used to manage CMs and CMTSes (Cable Modem Terminal Servers) and the relevant IETF RFCs and MIBs. [RFC 2665, 269, 2863, 2933, 3083]. SNMPv3 has been selected as the communication protocol for management of data-over-cable device. Also, since many existing management systems may not be capable to support SNMPv3 agents, support of SNMPv1 and SNMPv2 is also required for DOCSIS compliant CMs and CMTSes for backward compatibility reasons. Other highlights include:

- The specification of Subscriber Account Management Interface for the CMs so as to enable operators and interested parties to define, design and develop Operations and Business Support System (OBSS) for the commercial deployment of different classes of services over cable networks with accompanying usage-based billing of services. To facilitate processing of the Subscriber Usage Billing Records by a large number of diverse billing and mediation systems, an XML format is proposed for DOCSIS Cable Data Systems Subscriber Usage Billing Records [IPDR 02].
- For security management, the DOCSIS OSSIS provides the requirements [RFC 2786], guidelines and examples related to the Digital Certificate management process and policy. The DOCSIS Root Certificate Authority (CA) issues two kinds of digital certificates. One is the Manufacturer CA Certificate embedded in the DOCSIS compliant CMs and verified by the CMTS in order to authenticate the CM during initialization and provisioning. The other is the Manufacturer Code Verification Certificate used to ensure secure software downloading (upgrade) to the CMs in the future.**Wireless Network Management**

A major part of wireless networks is wired, and the management is similar to the wired network. However, there are management issues that become either specific to the use of wireless access points or mobile devices, which make wireless network management different from wired, network management. The specific issues are listed below:

- Discovery and security of access points
- Geographical coverage and the number of mobiles supported by each access point.
- Performance and fault management of the access points.
- Privacy and security – Wired Equivalence Privacy (WEP) of 802.11b promises privacy and confidentiality as good as wired network. Issues still exist.
- Device and user identification.
- Virus protection for virus's entered through the mobile devices.
- Network management through mobile devices.

- Integrated wireless and wired network management.
- Software delivery and updates.
- Ability to disable information transfer to mobile devices in case of security alarms.
- Mobile devices data backup and recovery.
- Scalable network management to manage multiplicity of mobile devices.

1.11 Some Additional Perspectives

In recent years, there has been a general trend of distributing network management intelligence from the managing entity (i.e. management console) to management agents [Gold 95, Mart 99, Raou 02]. Policy-based network management allows managers to partially delegate management tasks to agents in form of concrete policy settings. Web-based network management offloads the processing, presentation and display device information to web gateways or embedded web servers residing with the managed devices. Distributed object computing, such as CORBA, and Java-based network management provides the means for management task distribution in the network via the deployment of static distributed objects. Intelligent agents push distributed intelligence even further by defining autonomous agents that are capable of making complex management decisions. The role of such intelligent agents is no longer confined to either the managing entity or the agent, as the intelligent agents can adopt these roles dynamically, based on their assigned tasks or their own motivations.

References

[ATMF 94] ATM Forum, "Customer Network Management (CNM) for ATM Public Network Service," ATMF Specification af-nm-0019.000, Oct, 1994

[ATMF 96] ATM Forum, "Integrated Local Mgmt. Interface (ILMI) Ver. 4.0," ATMF Specification af-ilmi-0065.000, Sep, 1996.

[ATMF 97] ATM Forum, "ATM Remote Monitoring SNMP MIB," ATMF Specification af-nm-test-0080.000, July 1997

[ATMF 98] ATM Forum, "SNMP M4 Network Element View MIB," ATMF Specification af-nm-0095.001, July 1998

[ATMF 99a] ATM Forum, "Network Management M4 Security Requirements and Logical MIB," ATMF Specification af-nm-0103.000, Jan, 1999

[ATMF 99b] ATM Forum, "M4 Interface Requirements and Logical MIB: ATM Network View Version 2," ATMF Specification af-nm-0058.001, May, 1999

[ATMF 99c] ATM Forum, "Auto-configuration of PVCs Specification," ATMF Specification af-nm-0122.000, May 1999

[ATMF 99d] ATM Forum, "CMIP Specification for the M4 Interface: ATM Network Element View, Version 2," ATMF Specification af-nm-0027.001, July, 1999

[ATMF 00] ATM Forum, "ATM Usage Measurement Requirements," ATMF Specification af-nm-0154.000, November 2000

ATMF 01a] ATM Forum, "Requirements and Logical MIB for Management of Path and Connection Trace," ATMF Specification, af-nm-0153.000, April, 2001

[ATMF 01b] ATM Forum, "CORBA Specification for M4 Interface: Network View", ATMF Letter Ballot Document: fb-nm-0166.000, Apr 2001.

[ATMF 02] ATM Forum, "M4 Interface: ATM Network View, CORBA MIB, Version 2," ATMF Specification af-nm-0185.000, August, 2002

[ATMF 03] ATM Forum, "ATM Performance Management Bulk, Data File Structure," ATMF Specification af-nm-0194.000, April, 2003

[Bell 93] Bellcore TA-NWT-001114, Generic Requirements for Operations Interfaces Using OSI Tools: ATM/Broadband Network Management, Issue 2, October 1993.

[Bell 96] GR-2869-CORE, *Generic Requirements for Operations Based on the Telecommunications Management Network (TMN) Architectur*e, Issue 2, Bellcore, October 1996.

[Bell 94] SR-TSV-002690, *Requirements for an EML Platform Environment,* Bellcore, Issue 1, March 1994.

[Bell 96] *Network Management Layer to Element Manager Interface Descriptio*n, Bellcore, February 1996.

[Bell 00] Bellavista P., Corradi A., Stefanelli C., "An Integrated Management Environment for Network Resources and Services," IEEE Journal on Selected Areas in Communications, Vol. 18, No. 5, May 2000

[Casa 00] Casassa M., Baldwin A., Goh C., "POWER Prototype: Towards Integrated Policy-Based Management," IEEE/IFIP Network Operations and Management Symposium, 2000.

[Chei 98] Cheikhrouhou M. M., Conti P., Labetoulle J., "Intelligent Agents in Network Management: A State-of-the-art," 1998

[CORBA] CORBA www.omg.org, www.corba.org

[Dobs 89] Dobson J.E., McDermid J.A.,"A Framework for Expressing Models of Security Policy," IEEE Symposium on Security & Privacy, May 1989, Oakland, CA, 1989.

[DOCS OSSI] Data-Over-Cable Service Interface Specifications DOCSIS 2.0 - Operations Support System Interface Specification, SP-OSSIv2.0-104-030730, July 2003.

[DSLF TR005] DSL Forum "ADSL Network Element Management", DSL Forum Technical Report TR-005, March 1998.

[DSLF TR022] DSL Forum, "The Operation of ADSL-based Networks," DSL Forum Technical Report TR-022, August 1999.

[DSLF TR030] DSL Forum, "ADSL EMS to NMS Functional Requirements," DSL Forum Technical Report TR-030, Feb 2000.

[DSLF TR035] DSL Forum, "Protocol Independent Object Model for ADSL EMS-NMS Interface," DSL Forum Technical Report: TR-035, March 2000.

[DSLF TR041] DSL Forum, "CORBA Specification for ADSL EMS-NMS Interface," DSLF Technical Report TR-041, June 2001.

[DSLF TR046] DSL Forum, "Auto-Configuration Architecture & Framework", DSL Forum Technical Report, TR-046, February 2002.

[Enns 03] R. Enns, "XMLCONF Configuration Protocol", IETF Internet Draft draft-enns-xmlconf-spec-00.txt, Feb. 2003.

[Gins 99a] D. Ginsburg, *ATM Solutions for Enterprise Internetworking, 2nd Edition*, Addison Wesley, 1999.

[Gins 99b] D. Ginsbury, Implementing *ADSL*, Addison Wesley, 1999.

[Gold 95] Goldszmidt G., Yemini Y., "Distributed Management by Delegation," Procs. Of the 15th International Conference on Distributed Computing Systems, June 1995

[Hege 99] Hegering H., Abeck S., Neumair B., *Integrated Management of Network Systems*, Morgan Kaufmann Publishers, Inc. 1999

[IEEE] IEEE www.ieee.org

[IETF] IETF www.ietf.org.

[IPDR 02] “Network Data Management – Usage (NDM-U) For IP-Based Services”, Version 3.1, IPDR.org, April 15, 2002.

[ISO] ISO www.iso.ch

[ITU G9971] ITU-T Draft Recommendation G.997.1, "Physical Layer Management for Digital Subscriber Line (DSL) Transceivers", October 1998.

[ITU M3010] ITU-T Recommendation M.3010: “Principles for a Telecommunications Management Network”, October 1992.

[ITU M3100] ITU-T Recommendation M.3100: “Generic Network Information Model Version 2”, March 1995.

[ITU M3120] ITU-T, SG4, Recommendation M.3120, “CORBA Generic Network and NE Level Information Model," October 2001.

[ITU Q8221] ITU-T, SG4, Recommendation Q.822.1, “CORBA-based TMN Performance Management Service”, October 2001.

[ITU X720] ITU-T Recommendation X.720, "Information Technology – Open Systems Interconnection – Structure of Management Information: Management Information Model," January 1992.

[ITU X721] ITU-T Recommendation X.721, “Information Technology - Open Systems Interconnection - Structure of Management Information - Part 2: Definition of Management Information”, February 1992.

[JMX] JMX **www.java.com**

[Ju 01] Ju H., Choi M., Hong J., "EWS-Based Management Application Interface and Integration Mechanisms for Web-Based Element Management," Journal of Network and Systems Management, Vol.9, No.1, 2001

[Knig 99] Knight G., Hazemi R., "Mobile Agent-Based Management in the INSERT Project," Journal on Network and Systems Management, Vol.7, 1999

[Koch 01] Koch F. L., Westphall C. B., "Decentralized Network Management Using Distributed Artificial Intelligence," Journal of Network and Systems Management, Vol.9, No.4, Dec. 2001

[Lang 97] Lange, D., "Java Aglets Application Programming Interface (J-AAPI)," IBM white paper, Feb. 1997. (www.trl.ibm.com/aglets/JAAPI-whitepaper.htm)

[Lupu 99] Lupu E., Sloman M., "Conflicts in Policy-Based Distributed Systems Management," IEEE Transactions on Software Engineering, Vol. 25, No. 6, Nov. 1999.

[Mani 00] Subramanian, Mani, *Network Management, Principles and Practice*, Addison Wesley, 2000.

[Mart 98] Martin-Flatin J., "Push vs. Pull in Web-Based Network Management, "Technical Report SSC/1998/002, Swiss Federal Institute of Technology Lausanne, 1998

[Mart 99] Martin-Flatin J. P., Znaty S., Hubaux J. P., "A Survey of Distributed Enterprise Network and Systems Management Paradigms," Journal of Network and Systems Management, Vol.7, No.1, 1999

[Moff 93] Moffett J., Sloman M., Policy Hierarchies for Distributed Systems Management, IEEE Journal on Selected Areas in Communication, Vol. 11, No. 9, Dec. 1993.

[Nade 03] T. D. Nadeau, *MPLS Network Management - MIBs, Tools and Techniques*, Morgan Kaufmann, 2003.

[OMG 99] The Object Management Group (OMG), "The Common Object Request Broker: Architecture and Specification", OMG Document: formal/99-10-07, Revision 2.3.1, October 1999.

[Proz 97] Prozeller P., "TINA and the Software Infrastructure of the Telecom Network of the Future," Journal on Network and System Management, Vol.5, Dec. 1997

[Raou 02] Raouf Boutaba, Jin Xiao, "Network Management: State of the Art," Communication Systems: The State of the Art (IFIP World Computer Congress), p.g.127-146, 2002.

[RFC 1155] K. McCloghrie, M. Rose, "Structure and Identification of Management Information for TCP/IP-based Internets," IETF RFC 1155, May 1990.

[RFC 1157] Schoffstall, M., Fedor, M., Davin, J. and Case, J., A Simple Network Management Protocol (SNMP), IETF RFC 1157, May, 1990

[RFC 1212] K. McCloghrie, M. Rose, "Concise MIB Definitions", IETF RFC 1212, March, 1991.

[RFC 1213] K. McCloghrie and M. Rose. Management Information Base for Network Management of TCP/IP-base Internets: MIB-II, IETF RFC 1213, and March 1991

[RFC 1215] Rose, M.T. "A Convention for Defining Traps for use with the SNMP", IETF RFC 1215, March 1991.

[RFC 1224] L. Steinberg. Techniques for Managing Asynchronously Generated Alerts, IETF RFC 1224, May, 1991

[RFC 1406] F. Baker, J. Watt, "Definitions of Managed Objects for the DS1 and E1 Interface Types", IETF RFC 1406, Jan 1993.

[RFC 1407] T. Cox, K. Tesink, "Definitions of Managed Objects for the DS3/E3 Interface Type", IETF RFC 1407, Jan 1993.

[RFC 1441] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Introduction to version 2 of the Internet-standard Network Management Framework", IETF RFC 1441, May 1993.

[RFC 1442] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1442, May 1993.

[RFC 1443] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1443, May 1993.

[RFC 1444] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1444, May 1993.

[RFC 1445] J. Davin, K. McCloghrie, "Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1445, May 1993.

[RFC 1446] J. Galvin, K. McCloghrie, "Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1446, May 1993.

[RFC 1447] K. McCloghrie, J. Galvin, "Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1447, May 1993.

[RFC 1448] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1448, May 1993.

[RFC 1449] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1449, May 1993.

[RFC 1450] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1450, May 1993.

[RFC 1451] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Manager to Manager Management Information Base", IETF RFC 1451, May, 1993.

[RFC 1452] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework", IETF RFC 1452, May 1993.

[RFC 1493] E. Decker, P. Langille, A. Rijsinghani, and K.McCloghrie., Definitions of Managed Objects for Bridges, IETF RFC 1493, July, 1993

[RFC 1573] K. McCloghrie, F. Kastenholz, "Evolution of the Interfaces Group of MIB-II", IETF RFC 1573, Jan 1994.

[RFC 1595] T. Brown, K. Tesink, "Definitions of Managed Objects for the SONET/SDH Interface Type", IETF RFC 1595, March 1994.

[RFC 1695] M. Ahmed and K. Tesink, "Definitions of Managed Objects for ATM Management, Version 8.0 using SMIv2", IETF RFC 1695, August 1994.

[RFC 1757] Waldbusser S., Remote Network Monitoring Management Information Base., IETF RFC 1757, Feb. 1995

[RFC 1901] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Introduction to Community-based SNMPv2", IETF RFC 1901, January 1996.

[RFC 1903] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1903, January 1996.

[RFC 1905] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1905, January 1996.

[RFC 1906] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1906, January 1996

[RFC 1907] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1907, January 1996.

[RFC 2011] K. McCloghrie, "Category: Standards Track SNMPv2 Management Information Base for the Internet Protocol using SMIv2", IETF RFC 2011, November 1996

[RFC 2013] K. McCloghrie, "Category: Standards Track SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2", IETF RFC 2013, November 1996

[RFC 2570] J. Case, R. Mundy, D. Partain, B. Stewart, "Introduction to Version 3 of the Internet-standard Network Management Framework", IETF RFC 2570, April 1999

[RFC 2571] Harrington, D., Presuhn, R. and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", IETF RFC 2571, April 1999.

[RFC 2572] Case, J., Harrington, D., Presuhn, R. and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", IETF RFC 2572, April 1999

[RFC 2573] Levi, D., Meyer, P. and B. Stewart, "SNMP Applications", IETF RFC 2573, April 1999.

[RFC 2574] Blumenthal, U. and B. Wijnen, "The User-Based Security Model for Version 3 of the Simple Network Management Protocol (SNMPv3)", IETF RFC 2574, April 1999

[RFC 2575] Wijnen, B., Presuhn, R. and K. McCloghrie, "View-based Access Control Model for the Simple Network Management Protocol (SNMP)", IETF RFC 2575, April 1999

[RFC 2576] R. Frye, D. Levi, S. Routhier, B. Wijnen, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard and Network Management Framework", IETF RFC 2576, March 2000.

[RFC 2578] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)", IETF RFC 2578, April 1999

[RFC 2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Textual Conventions for SMIv2", IETF RFC 2579, April 1999

[RFC 2580] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Conformance Statements for SMIv2", IETF RFC 2580, April 1999

[RFC 2662] B. Bathrick, F. Ly, "Definitions of Managed Objects for the ADSL Lines", IETF RFC 2662, August 1999.

[RFC 2665] J. Flick, J. Johnson, “Definitions of Managed Objects for the Ethernet-like Interface Types”, August 1999

[RFC 2669] M. St. Johns, “DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems”, August 1999

[RFC 2670] M. St. Johns, “Radio Frequency (RF) Interface Management Information Base for MCNS DOCSIS compliant RF interfaces”, August 1999

[RFC 2748] D. Durham, Ed. "The COPS (Common Open Policy Service) Protocol," IETF RFC 2748, Jan. 2000.

[RFC 2786] M. St. Johns, “Diffie-Helman USM Key Management Information Base and Textual Convention”, IETF RFC 2786, Aug, 1999

[RFC 2863] K. McCloghrie, F. Kastenholz, “The Interfaces Group MIB”, June 2000.

[RFC 2933] McCloghrie, K., Farinacci, D., Thaler, D., “Internet Group Management Protocol MIB”, IETF RFC 2933

[RFC 3083] R. Woundy, “Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems”, RFC 3083, March 2001.

[RFC 3084] Chan K, et al, "COPS Usage for Policy Provisioning," IETF RFC 3084, March 2001.

[RFC 3483] D. Rawlins et al, "Framework for Policy Usage Feedback for Common Open Policy Service with Policy Provisioning (COPS-PR)," March 2003.

[Roge 02] Rogerson D., Inside COM, Redmond, WA, Microsoft, 1997

[Stra 96] Straber M., Baumann J., Fohl F., "Mole – A Java Based Mobile Agent System," 10th European Conference on Object-Oriented Programming ECOOP’96. Jul. 1996

[Thom 98] Thompson J., "Web-based Enterprise Management Architecture," IEEE Communications Magazine, Mar. 1998

[WBEM] www.dmtf.org

[Wool 95] Wooldridge M., Jennings N. R., "Intelligent Agents: Theory and Practice, The Knowledge Engineering Review," Vol. 10, No.2, 1995

This page intentionally left blank.