Application MIBs for Network Operation Centers Collaborative Management

Alex Bordetsky
Naval Postgraduate School
abordets@nps.navy.mil

Daniel Dolk
Naval Postgraduate School
drdolk@nps.navy.mil

George Zolla
Naval Postgraduate School
gazolla@nps.navy.mil

ABSTRACT

At present there is very little coordination between Network Operation Centers (NOC) across organizational domains or across the Internet. Our goal is to create a model to facilitate this process. We introduce the concept of Application MIBs and Knowledge Management Gateway for structuring knowledge management across multiple NOCs. SNMP Network Element (NE) Management Information Base (MIB) agents are used to gather network information and application MIBs are used as a metric for a Mission-Policy-Metrics-{Sense-Analyze-Adapt} feedback loop that is used to analyze the effectiveness of network operations. We believe that the combination of collaborative technology, enhanced application MIBs, and multiple agents that execute the relationships of the adaptation loop will create a desirable knowledge management architecture for Knowledge Management Gateways. This architecture will not only enhance NOC efficiency but could also lead to prioritization of network applications and the creation of a multiple level NOC collaborative environment.

1. INTRODUCTION

The ultimate goal of our research is to create a model that will facilitate Network Operation Fusion (collaborative management) of multiple Network Operations Centers (NOCs) across the Internet.

In this paper, a conceptual model will be built for a single knowledge management gateway that will ultimately collaborate with other knowledge management gateways. We will use the combination of collaborative technology (Bordetsky 2000, Bordetsky & Mark 2000), NOC SNMP Management Information Base (MIB) agents, and an adaptive multiple agent architecture to create a transparent knowledge management space supporting the Mission-Policy-Metrics-Sensor feedback model. Application MIBs will be discussed in detail to demonstrate their potential in supporting this model.

2. ROLE OF NOCs

2.1 Motivation for NOCs

The NOC collects, integrates, and displays data measurements taken from the underlying network. NOCs are well-established components in telecommunications grids as indicated by the Network Management Layer in the telecommunications management network (TMN) hierarchy (Fig 1). Typically, however, their focus tends to be towards the lower levels of operational support, specifically operations involving network elements and network element management. While this level of functionality is necessary, it is not sufficient to meet the higher-level requirements of service and business management encapsulated in the two top layers in Figure 1. The need for NOCs with broader scope and more robust knowledge management capabilities has become more pointed in recent years. A confluence of factors has contributed to the emergence of business-oriented operations centers, particularly in the area of wireless communications and the transportation arena (Perkins & McGennis 1997).

Advances in database technology. A major driver of contemporary sensor technology is the software agent. Agents can go where "no man has gone before", namely in the bowels of a network device itself. An agent can monitor, filter, and even calibrate the network in which it's placed. The use of agents in the Internet is perhaps the most striking example of this capability. It also underscores the refinement of granularity which accompanies advances in sensor technology. One of the major impacts of finer grained sensors is a commensurate increase in the amount of data which is collected. This requires better tools for storing, filtering, and analyzing large amounts of data efficiently. The emergence of database technology in the form of very large data warehouses, on line analytical processing (OLAP) and data mining, coupled with the ability to disseminate information and analysis from these tools rapidly and widely via the Internet, addresses this need in ways that have not been possible before. Aligning the data warehouse structures with quality-driven performance metrics provides a solid foundation for decision support capabilities necessary to network operations centers (Dolk 2000).

2.2 A Conceptual Process Model for NOCs

The confluence of factors mentioned above has conspired to make the development of NOCs not only feasible, but also necessary, for their successful management at many different levels. To extend the functionality of NOCs to accommodate service and business knowledge management, we must first develop a generalized conceptual process model for NOCs and trace the implications of this model, with particular attention to the knowledge management domain. We do this by combining a simplified military command and control decision-making process with a standard management control system.

Operations centers have been prevalent in the military, probably from the inception of warfare. Command and control centers are designed to manage the very complex activity of warfare, which involves coordinating usually vast numbers of humans and machines in such a way as to maximize the chances of a successful outcome. The military command and control center allows commanding officers to monitor the battlefield and deploy force structure changes in near real time. Sensors, both human and nonhuman, provide streams of information, which must be filtered, interpreted, and transformed into decision choices. The emergence of choices may, in turn, engender requests for more information from the sensors to elucidate the desirability of certain options. Once a decision is made, the sensors provide feedback on the effects that the decision is having on the battlefield, and the process continues iteratively.

The basic process model we adopt for NOCs is a command and control model leavened with a standard management control feedback loop familiar to the accounting domain. Figure 2 shows a Mission-Policy-Metrics-{Sense-Analyze-Adapt} feedback structure, which we claim is relevant to the NOC environment as well. The top-level process of this process is to identify and articulate the mission, which is clearly a strategic activity. The next level in this process is to identify and specify various policies by which the mission is to be realized. One of the by products of articulating the mission and associated policies is the generation of a set of feasible performance metrics which allow decision makers to measure how well the organization is executing the stated mission. Each metric must be associated with one or more sensors that collect relevant data, which can be used in the computation of that metric. The computation of the metric and the comparison of those metrics with the mission objectives satisfying policy constraints comprise the analysis stage of this process. Analysis may require the use of models to calculate the metrics themselves and compare them to the objectives, as well as to identify alternative paths of action to adapt, or respond, to the current environment. The Sense-Analyze-Adapt structure is a persistent loop, which occurs continuously at the operational level, however, the adaptation stage may also result in a more critical change to the overall mission, associated policies, and/or to the metrics that are deemed necessary and sufficient.

Although developed from a military command and control perspective, we claim this process model is relevant to NOCs as well. The NOC serves as a critical interface between the organizations, in our case any company for whom wireless technology constitutes a substantial part of its infrastructure, and its environment. We note that the persistent, adaptive feedback loop is driven by the fusion of data from agents embedded within the network. This describes the current state of the art in NOCs, which we mentioned previously, focuses primarily on low-level network elements. With this conceptual model, we can now delve into more detail concerning the requirements for collaborative technology NOCs that can give us feedback on for each of the different network elements as well as feedback on network applications.

3. KNOWLEDGE MANAGEMENT ACROSS NOCS

3.1 Integrated Service Level Management

NOC services embrace a wide range of functionality; however we can identify four meaningful high level categories of service for the purposes of our discussion: fault management, configuration management, performance management, and accounting / security management. Fault management is largely concerned with root cause analysis involving remote identification and correction of real time network problems. Remote fault management monitors the health of the network infrastructure, components, subsystems, and interfaces. Configuration management facilitates the remote configuration of network software, interfaces and service capabilities as a network expands. Performance management involves analysis of performance trends and network problems so that preemptive action can be taken to assure network viability. Performance reporting is driven by decision-making requirements as set forth by senior management in concert with the technical team. Accounting and security management involves customer billing and the maintenance of network security. Table 1 shows more specific functionality for each of these categories.

The described integrated services as they evolve will heavily rely on multiple decision support functions across different carrier (platform) NOCs. So far little is known about how to provide network management knowledge transfer between different platform NOCs and how to organize knowledge management at these sites.

3.2 Modeling Integration and Knowledge Management Across Platform NOCs

The NOC management functions delineated in Table 1, a Wireless Grid containing several NOCs, clearly illustrate that integration is accomplished by adding **remote monitoring** options to the subset of actions within the Fault and Configuration Management functions. The remaining functionality is largely similar to the typical list of management tasks supported by commercial network management systems such as HP Open View, Aprisma Spectrum, and Tivoli.

This “conventional wisdom” about NOC functionality is obviously not sufficient for the integrated seamless management of applications across different wireless NOCs. The “conventional wisdom” is based upon a static hierarchy of Simple Network Management Protocol (SNMP) descriptions of managed network elements, called Management Information Bases (MIBs) (Sebastian, Dolk & Kuchen 2001). In spite of its universal character, the hierarchy of NE MIBs doesn’t provide for the dynamics of a seamless Quality-of-Service (QoS) management process across the NOCs to satisfy ad hoc application processing requirements. The challenge is to combine knowledge about Network Element (NE) management within each platform NOC domain with the dynamics of applications management across different NOCs. In this case NOCs become managed elements of a NOC grid.

From the system dynamics perspective the substance of each NOC process is contained in knowledge management about NEs and course of action selection. Network operation crews powered by network management systems currently conduct such activities. So far, however, little has been explored about how to represent the NOCs as knowledge management entities and how to build the control processes across different NOCs. In order to address this problem, we suggest expanding the concept of the SNMP MIB to the level of the NOC. Specifically, in the center of our knowledge management model is a knowledge management gateway that enables translation of NE MIBs at the individual NOC level into a higher level MIB that represents management knowledge flow through the NOC. Such an extension makes management across multiple NOC NE layers transparent to the management agents that have SNMP MIB interfaces and therefore can be used for designing a knowledge management gateway (Fig. 4).

3.3 Knowledge Management Models for NOCs

We now address the issue of what the knowledge management models for individual NOCs look like. Table 1 provides a summary of the five platforms mentioned earlier with respect to mobility, location, access, interfaces, and knowledge sources. We use this table as the basis for constructing conceptual models for knowledge management for each of these subnets.

We use influence diagrams to structure the knowledge management models. The influence diagram technique alone is good for structuring static Choice-Goal relationships, but lacks the means to represent the dynamics of knowledge transfer within the NOC. Thus, we integrate the influence diagrams with the conceptual model for control center adaptive DS functionality shown in Figure 2, which adds the necessary dynamic dimension into the Knowledge Management model for platform NOC.

The diagrams represent two types of knowledge spaces: the space of individual NOC functional metrics and knowledge space of adaptive decision support loop that NOCs share along the timeline of ad hoc application processing. For the sake of simplicity we define rules very generally as Rules = {production rules (IF-Then-Else), Cases (frames), Policies}. How can we manage the knowledge flow across two spaces? One possible answer is to develop the NOC knowledge management gateway, which would be capable of associating the spatially distributed functional rules with the rules of decision-making dynamics. The idea of gateway intelligent agent-brokers dates back to the early work of (Genesereth & Ketchpel 1994).

4. MANAGING ACROSS THE NOCs: KNOWLEDGE MANAGEMENT GATEWAY

The NOC adaptive management process described in Figure 2 presents a natural foundation for structuring knowledge management across multiple NOCs. The dynamic process of Mission-Policy-Metrics-{Sense-Analyze-Adapt} could be executed by the set of intelligent agents of each category (Fig 4) combined in the NOC knowledge management gateway.

The SNMP variables comprising NE MIBs define the individual NOC functional knowledge space. On the other hand the agents providing Mission-Policy-Metrics-{Sense-Analyze-Adapt} feedback loop should talk to the individual NOCs as nodes of the knowledge sharing network. In accordance with this model, Mission Agent or Performance Metrics Agent would read the NOC MIB providing "big picture" information to the controlling NOC level about each sub network configuration, availability, etc. This would automatically add to the huge tree of SNMP MIBs identifiers in which the lower level variables such as those reflecting traffic at each NE, routing table entries, etc are already populated by the "traditional" network management system's agents. By sharing the same SNMP MIB tree for NOCs and NEs, the gateway agents are capable of associating their results with network management agents and crews at the individual NOC level. This in turn enables both data mining operations between two levels and building associations for seamless QoS application processing across the grid.

In an ideal world, the solution proposed above would be complete, however, in reality we still need instantaneous access to the NOC crews and their expertise to remedy real time problems arising from configuration management, fault monitoring, and traffic management. In terms of the knowledge gateway model presented in Figure 4, this would require collaborative transactions to provide values for the missing SNMP variable values in the NOC MIB. The combination of collaborative technology (Bordetsky 2000, Bordetsky & Mark 2000), NOC SNMP MIBs, and adaptive multiple agent architecture creates a transparent knowledge management space supporting the Mission-Policy-Metrics-{Sense-Analyze-Adapt} process. The agents' navigation of the knowledge management space based on the SNMP MIB trees could be further automated by the implementation of emerging policy-based language technology (Stone, Lundy & Xie 2001). By using the policy-based language, the agents could translate the NOC MIB requirements directly into action variables for NE MIBs.

5. APPLICATION MIBs

A Management Information Base (MIB) is a Simple Network Management Protocol (SNMP) specification containing definitions of management information so that networked systems can be remotely monitored, configured and controlled (Perkins & McGennis 1997). They are used extensively in Network Elements (NE) such as routers and hubs. This information is sent to network management applications that are used by NOC personnel. These agents act as Daemons on NE that respond to requests for information from the network management application. NE MIBs equate to the top level of Figure 4.

Application MIBs provide information from network applications such as DBMS and Web servers. They are shown near the bottom of Figure 4. Application MIBs could conceptually be used as the Metrics in the Mission-Policy-Metrics-{Sense-Analyze-Adapt} feedback structure discussed earlier. Where the NE MIBs provide information on network statistics, application MIBs can provide information on how well the applications are functioning. In the following paragraphs we will discuss in some detail what information is provided by application MIBs and how they could be used to contribute to an upper level NOC MIB.

5.1 Application MIB Taxonomy

Application MIBs are part of the Global Structure (Tree) of SNMP Management Information Base (MIB) Variables (Fig 3). MIBs are identified using a unique Object Identifier (OID) value. The permanent assignment of an OID value, or identity, to an item is called a registration. A rooted tree is often used to illustrate the number s in sequences that correspond to OID values (Perkins & McGennis 1997).

All application MIBs start at the 1.3.6.1 level which corresponds to ISO.ORG.DOD.Internet. Two sublevels: management (1.3.6.1.2) and private (1.3.6.1.4) contain application MIBs that are of interest to our discussion. The management level deals with general areas of network management. The private level deals with specific instances of corporate application MIBs. In the private level anyone can ask for an enterprise number.

Under management, there is only one sub level: mib-2 applications (1.3.6.1.2). It contains numerous MIBs with two of particular interest: rdbmsMIB and wwwMIB.

Under the private level (1.3.6.1.4) there is only one sub category, enterprises (1.3.6.1.4.1). This is the area mentioned above where anyone can ask for a MIB OID. Under the enterprise level there are many sublevels for private vendors. Two vendors of note are: Oracle (1.3.6.1.4.1.111) and Microsoft (1.3.6.1.4.1.311).

5.2 Application MIB objects

Application MIBS have numerous objects that respond to requests from network management software. Several objects of interest will be discussed below. First the generalized MIBs:

The rdbmsMIB (1.3.6.1.2.1.39) is a Relational Database Management (RDMS) information base. Some interesting sub levels include:

rdbmsSrvInfoHandleRequests (1.3.6.1.2.1.39.1.6.1.10) – The total number of requests made to the server on inbound associations. This is intended to encapsulate high level semantic operations between clients and servers.

rdbmsSrvInfoRequestRecvs (1.3.6.1.2.1.39.1.6.1.11) – The number of receive operations made processing any requests or inbound associations.

rdbmsSrvInfoHighwaterInboundAssociations (1.3.6.1.2.1.39.1.6.1.13) – The greatest number of inbound associations that actually have been simultaneously open to this server since startup.

rdbmsSrvInfoMainboundAssociations (1.3.6.1.2.1.39.1.6.1.14) – The greatest number of associations that can be simultaneously open with this server.

The wwwMIB (1.3.6.1.2.1.65) is a Web server information base. Its objects show information on transactions such as in request and out requests. Some interesting sublevels include:

wwwService (1.3.6.1.2.1.65.1.1.1.1.2) – Textual description of the web service including at least the vendor and version number of the application.

wwwServiceName (1.3.6.1.2.1.65.1.1.1.1.5) – The fully qualified domain name which this service is known. This object must contain the virtual host name if the service is realized for a virtual host.

wwwServiceOperStatus (1.3.6.1.2.1.65.1.1.1.1.8) – Indicates the operational status of the WWW service.

wwwSummaryTable (1.3.6.1.2.1.65.1.2.1) – The table providing overview statistics for the WWW services on this system.

wwwSummaryRequestInTable (1.3.6.1.2.1.65.1.2.2) – The table providing detailed statistics for requests received by WWW services on this system.

wwwSummaryRequestOutTable (1.3.6.1.2.1.65.1.2.3) - The table providing detailed statistics for requests generated by the services on this system.

The vendor specific application MIBs provide much more detailed information than the generalized MIBS. Some examples:

The Oracle MIB structure is particularly rich. It contains a tremendous number of MIBs that describe in detail the performance of the particular DBMS. Some specific MIBS of interest:

oraDedicatedSrvEstablishedConnections (1.3.6.1.4.1.111.5.1.2.1.2) – Indicates how many incoming connection requests have been accepted by the dedicated server.

oraDedicatedSrvRejectedConnections (1.3.6.1.4.1.111.5.1.2.1.3) – Indicates how many incoming connection requests have been rejected by the dedicated server.

oraSIDTable (1.3.6.1.4.1.111.5.1.5) – The system identifier (SID) specifies the Oracle SID of the database server.

oraSIDCurrentConnectedClients (1.3.6.1.4.1.111.5.1.5) – Indicates the total number of currently connected clients.

The Microsoft MIB enterprise level is interesting because it contains information about the workstation or server operating system and several Microsoft applications including SQL Server (1.3.1.6.1.4.1.311.1.1.3.1.1), FTP servers, and the Internet Information System HTTP server. Some specific MIBS of interest:

Operating System MIBs

performance (1.3.1.6.1.4.1.311.1.1.3.1.1) – Top of a hierarchical tree that gives numerous operating systems MIBs that include network connection information as well as FTP and HTTP statistics.

Selected MIBs for the Microsoft SQL Server:

mssqlSrvVersion (1.3.1.6.1.4.1.311.1.4.1.1.1.1.3) – The version of installed SQL Server

mssqlSrvState (1.3.1.6.1.4.1.311.1.4.1.1.1.1.5) – Identifies the current state of the SQL Servers as Unknown, Running, Paused, and Stopped.

mssqlSrvInfoServerName ((1.3.1.6.1.4.1.311.1.4.1.2.1.1) – The name of the local SQL Server.

mssqlSrvStartupTime (1.3.1.6.1.4.1.311.1.4.1.1.2.1.2) – The date and time at which the current running SQL Server process was started.

mssqlSrvInfoNetworkReads (1.3.1.6.1.4.1.311.1.4.1.1.2.1.13) – The number of tabular data stream (TDS) packets read from the network since SQL Server was started.

mssqlSrvInfoNetworkWrite (1.3.1.6.1.4.1.311.1.4.1.1.2.1.14) – The number of tabular data stream (TDS) packets written to the network since SQL Server was started.

Selected MIBs for the Microsoft FTP Server:

totalBytesSentHighWord (1.3.1.6.1.4.1.311.1.7.2.1.1) – This is the high 32-bits of the total number of BYTES sent by the FTP Server.

currentConnections (1.3.1.6.1.4.1.311.1.7.2.1.13) – This is the current number of connections to the FTP Server.

maxConnections (1.3.1.6.1.4.1.311.1.7.2.1.14) – This is the maximum number of connections to the FTP Server.

Selected MIBs for the Microsoft IIS Web server:

totalBytesHighWord (1.3.1.6.1.4.1.311.1.7.3.1.1) - This is the high 32-bits of the total number of BYTES sent by the HTTP Server.

totalFilesSent (1.3.1.6.1.4.1.311.1.7.3.1.5) – This is the total number of files sent by this HTTP Server.

currentAnonymousUsers (1.3.1.6.1.4.1.311.1.7.3.1.7) – This is the total number of anonymous users currently connected to the HTTP Server.

maxAnonymousUsers (1.3.1.6.1.4.1.311.1.7.3.1.11) – This is the maximum number of anonymous users simultaneously connected to the HTTP Server.

maxConnections (1.3.1.6.1.4.1.311.1.7.3.1.13) – This is the current number of connections connected to the HTTP Server.

5.3 Future Research for Application MIBs

Application MIBs are ideally suited for intra and inter NOC measurements. Within the single NOC architecture application MIBs can evaluate it the internal network is providing sufficient bandwidth for the clients and servers. They can also be an exception tool to measure whether applications are functionally efficiently within a Knowledge Management Gateway or even across multiple Knowledge Management Gateways. If we used the Navy/Marine Corps Intranet (NMCI) as an example, we could determine if NMCI servers are running optimally within the Intranet.

At present, there are only a few application MIBs and those create only IO (Sensing) objects. We need to develop MIBs that cover additional types of applications and MIBs that can be used to create logs for developing knowledge and learning.

Additional MIBs need to be developed for more vendor specific Web servers. Only one was found. Additional types of application MIBs need to be created for applications such as streaming video, mail servers, additional DBMSs and virtual reality sites.

Application MIBs concentrate on IO information. Logs are needed to develop long-term views of how applications are functioning on the network so that modifications can be made to enhance overall performance.

When application MIBs are enhanced as discussed above they will be able to give us an accurate overview of network operations that can be used as metrics for intra or inter Knowledge Management Gateway Mission-Policy-Metrics-{Sense-Analyze-Adapt} management cycles (Fig 2).

6. CONCLUSIONS

We believe that the combination of collaborative technology, additional enhanced application MIBs, and multiple agents that execute the relationships of the adaptation loop will create a desirable knowledge management architecture for Knowledge Management Gateways. This architecture will not only enhance NOC efficiency but could also lead to prioritization of network applications and create a multiple level NOC collaborative environment. The described approach is currently under testing for developing a command and control wireless operations fusion test bed.

6. REFERENCES

1. Bordetsky, A. Adaptive QoS Management via Multiple Collaborative Agents, Ch.4 in: *Agent Technology for Communications Infrastructure,* Wiley, 2000.

2. Bordetsky, A. and Mark, G. (2000), Memory Based Feedback Controls to Support Groupware Coordination. *Information Systems Research,* Vol. 11, 4, 2000, 366-385.

3. Dolk, D. Integrated modeling environments in the data warehouse era. *European Journal of Operations Research,* 122, 2 (April 2000), 199-218.

4. Genesereth, M.R. and Ketchpel, S.P. Software Agents, C*ommunications of ACM*, 37, 7, 1994, pp. 48-53.

5. Libicki, M. Who Runs What in the Global Information Grid: Ways to Share Local and Global Responsibility, RAND Corporation, 2000.

6. Perkins, D. and McGennis E. Understanding SNMP MIBs, Prentice Hall, 1997

7. Sebastian, H-J, Dolk, D, Kuchen, R. Operations centre for logistics. *Proceedings of the 34th Hawaii International Conference on Systems Science*; Kihei, Hawaii, January 7-10, 2001.

8. Stone, G., Lundy, B., and Xie, G. Network Policy Languages: A Survey and New Approach, *IEEE Network*, January/February, 2001, pp.10-21

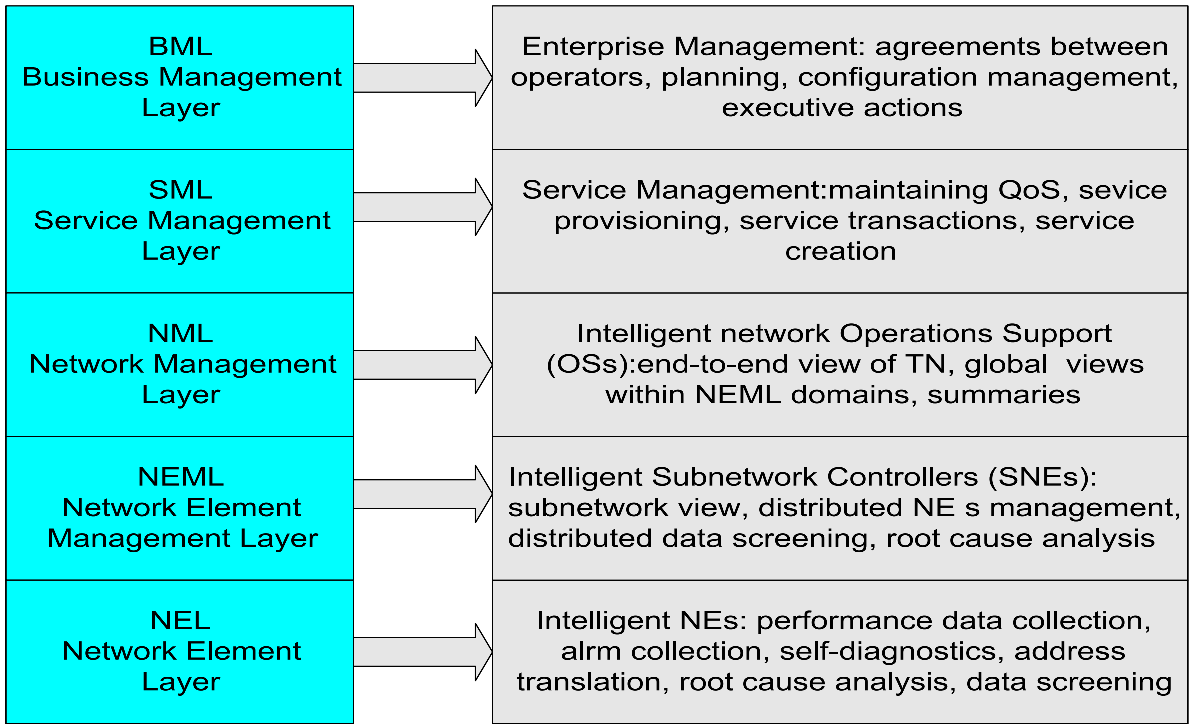


Figure 1: TMN Intelligent Management Architecture

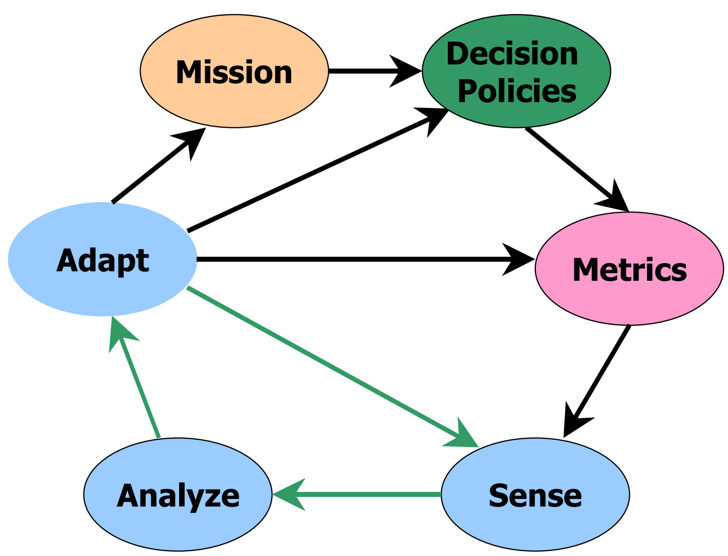
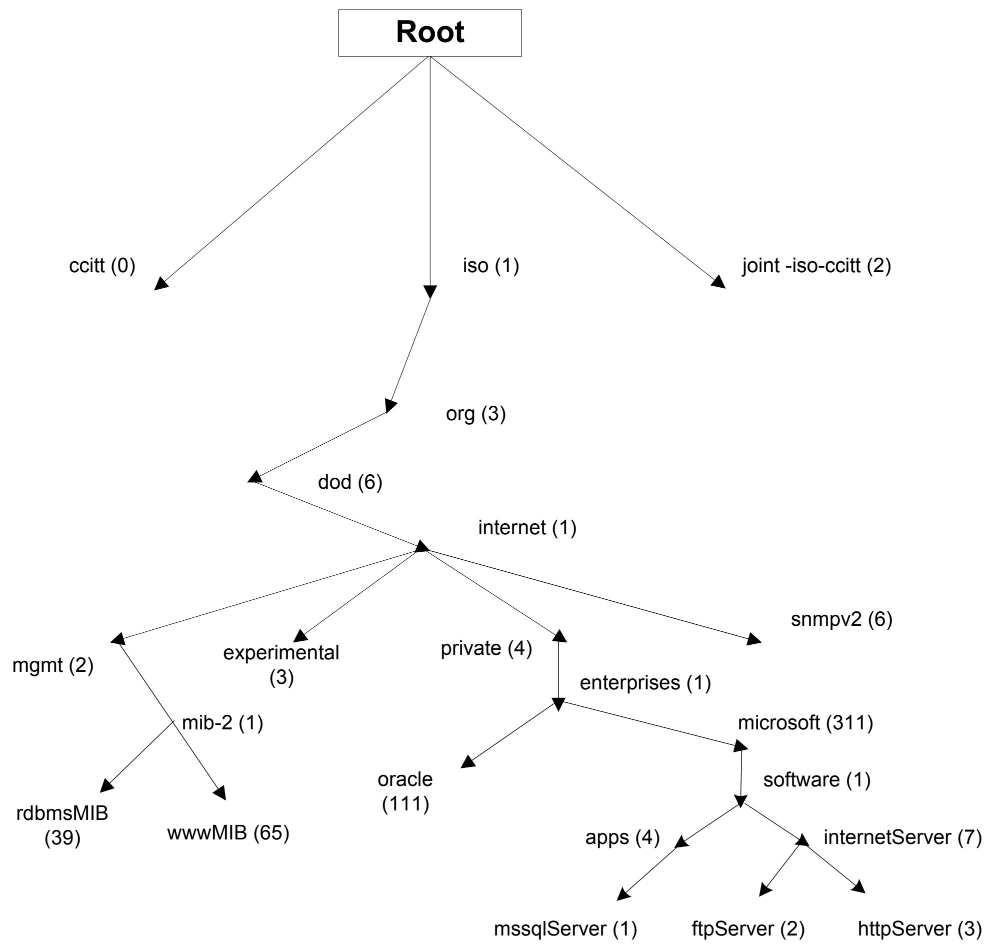


Figure 2. Conceptual Model for NOC Processes



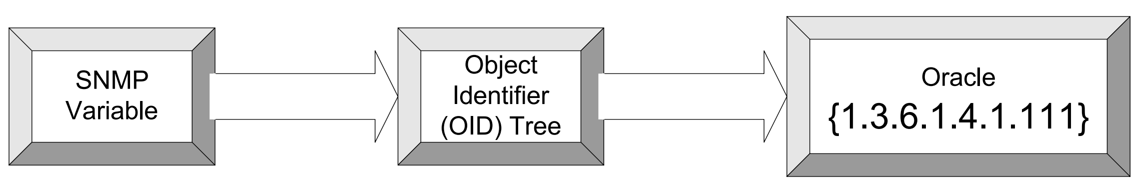


Figure 3. Global Structure (Tree) of SNMP Management Information Base (MIB) Variables

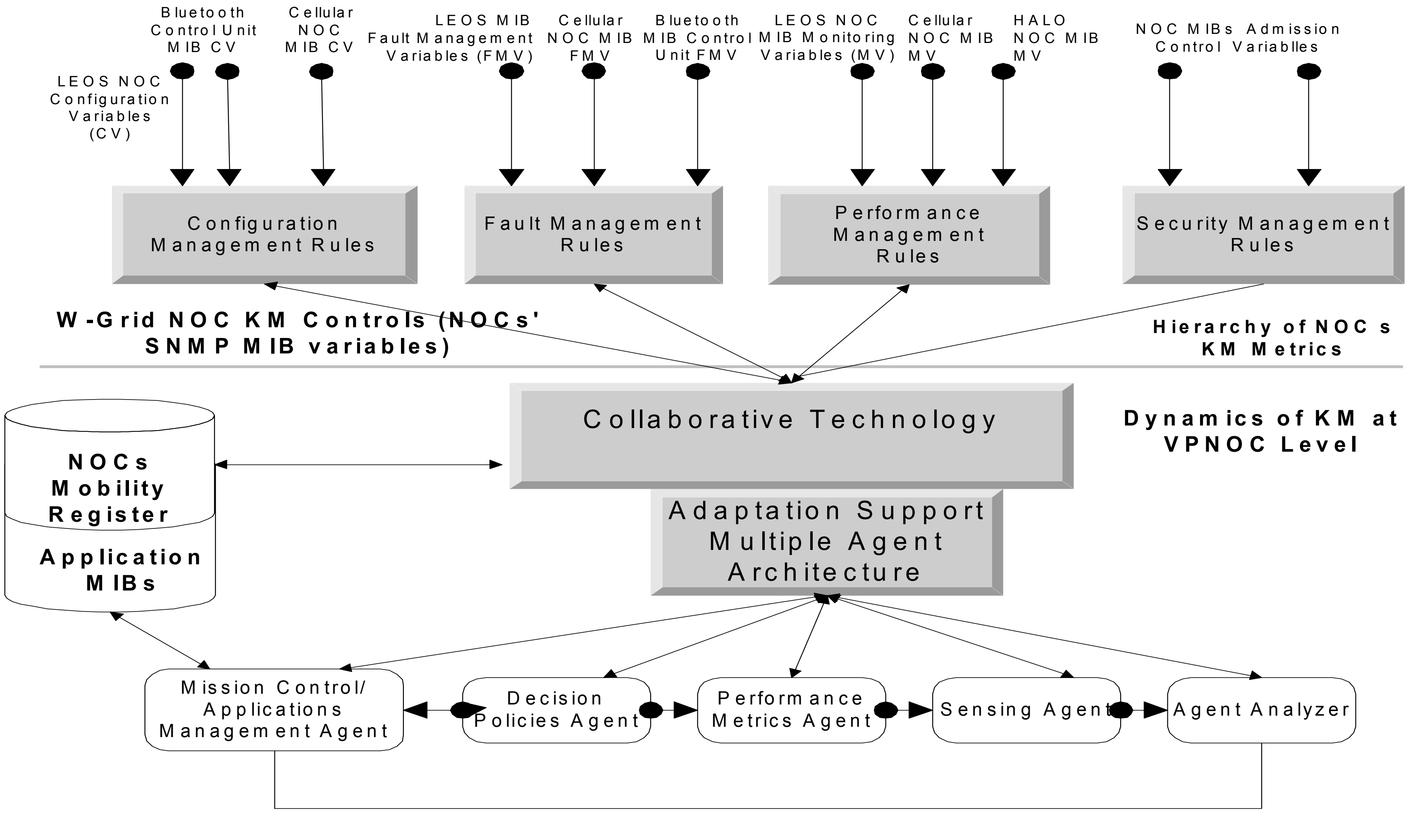


Figure 4. Solution: W-Grid Knowledge Management Gateway

	LEOS NOC (Exs: Iridium, Orbcomm, SkyBridge)	**Cellular PCS NOC (Exs: Mobile Switching Center, GSM, CDPD Services)**	**Bluetooth NOC (Exs: Arca Wavecatcher Protocol Analyzer Unit)**	**PAN NOC**	**HALO NOC**
Mobility	Fixed	Fixed	Mobile	Mobile	Mobile
Location	Terrestrial	Terrestrial	Terrestrial, Sea, Airborne	Human body	Airborne
Access	Regional (restricted)	Regional or global	Piconet, scatternet	Near-field electrostatic body-device links	Metropolitan, 40-60mi
Interfaces	Cellular NWs; Telephony NWs; GPS Constellation; Geo-synchronous satellites	Air interface (terminals); Telephony NWs (T-interface); Other wireless (M-interface); GPS (emerging)	Cellular, Telephony and Satellite NWs via PCS, Palm and other terminals	Bluetooth, Cellular, Telephony, and Satellite NWs via wearable terminals	Cellular network, T1, ATM, LAN bridges, LMDS
Knowledge Sources	Orbital configuration, performance; Transmission link levels and budget; Transponder schedule; Transponder sharing policy; Customer database	Mobile stations (terminals); Base stations (repeaters); Customer mobility mgmt: -Home location register -Visited locator register -Equipment ID register	Master-slave configuration; Flows composition (DH1-DH5); Packets integration; Piconet and scatternet routing; Terminals (printers, handhelds, telephones, etc.)	Near-field links bandwidth; Wearable PAN devices	The user terminal -MMW Antenna -MMW Transceiver -Radio Frequency unit Cell configuration Configuration of 1-15 antenna beams

Table 1. Wireless Grid NOC Knowledge Management Sources