TRENDS AND ISSUES IN NETWORK MANAGEMENT

Dragomir D. Dimitrijević
Consultant
Belgrade, Yugoslavia

Ilija Đekić
Institute for
Small and Medium Sized Enterprises
Belgrade, Yugoslavia

I INTRODUCTION

In this paper we present issues and trends in network management [3,7,12,17]. The material presented here is an overview of theoretical a practical experience gained in various project over the years. In today's increasingly competitive telecommunication services business, quality of a network management system is the most important aspect of a telecommunication system. The ongoing deregulation in the US and Europe, increases competition and need lower operating cost. The need for lower operating cost causes reengineering and massive downsizing in telecommunication services companies. To preserve and preferably improve quality of service, a highly automated network management system is a must.

Today's communication networks are a complex mixture of heterogeneous hardware, protocols, network management standards, and network management applications. Even worse, many vendors that claim compliance with standards, are far from being compliant. A network management application developer may have big problems to manage a network with equipment falsely pronounced compliant. An interesting study of non-compliance with SNMP may be found in [15].

Future of network management standards is uncertain and that makes decision about its choice difficult to make. It is clear that even when (or more likely if) one of the standards win, there will be too many incompatible systems around to deal with.

A network management system developer faces many design decisions that may have tremendous impact on the final product. They range from choice of system's basic constituent parts (e.g., protocols, databases, and graphical user interface) to high-level business management layer applications (e.g., customer care and billing systems). This paper addresses some of the design issues a network management system designer has to deal with.

II NETWORK MANAGEMENT CONCEPTS

II.1 NETWORK MONITORING

II.1.1 Architecture

The purpose of network monitoring is acquisition of information about the state of networks in order to make most of network resource. This information may be:

- Static information that changes slowly such as network topology;
- Dynamic information that shows current state and activity in a network;
- Statistical data that is derived from dynamic information shows network behavior in longer periods such is an hour.

Network elements, such as base stations in mobile telephone networks, generate in real-time information about their state. This information is stored in the Management Information base (MIB). Monitoring agents use this information to generate statistical information.

Control applications distributed across the network use the information stored in the MIB to undertake an appropriate control action. Communication and cooperation between control application is achieved using the following architectures:

The client/server architecture, shown in Figure 1, is an older architecture typical for systems where the number and type of control terminals and applications are defined and do not change a lot in time. A typical example is network management of Local Area networks (LAN). Such a system consists of one or more servers that contain information about the network. Control applications/terminals distributed across the network may access the servers. The information is obtained from servers directly and control commands are this approach heavily depends on the physical organization of the MIB. Any change in the MIB requires changes in the client software. Security of information directly depends on servers' security that is the only obstacle to potential intruders.

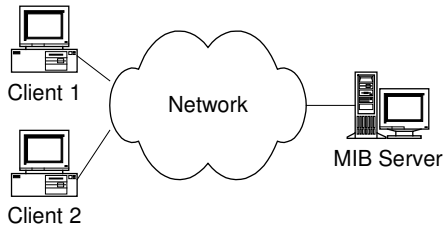

Figure 1: Client/Server Architecture

The three-tier architecture, shown in Figure 2, has gained popularity with the increased use of the Internet. The

increasingly large number of network control/management applications migrates to the Internet. This increased the network security risk. The number and type of network management/control applications as well as the structure of the MIB are dynamically changed. The three-tier architecture is a better choice for such an environment.

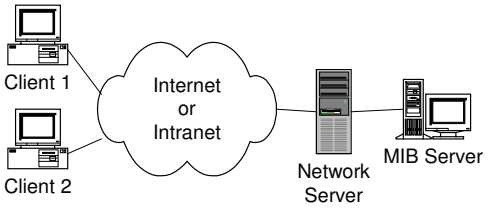

Figure 2: Three-Tier Architecture

Unlike in the client/server architecture where clients access the MIB directly, using the complete knowledge about its physical and informational structure, the three-tier architecture introduces an intermediate network (web) server. This server is a mediator between clients and the MIB. In such a way, the server takes the burden and eventual absorbs changes in the system. The application software remains intact.

Clients and the server communicate by exchanging commands and responses in a form of objects. The interface between clients and servers, i.e., the form of objects that are exchanged, is defined via the Interface Definition Language (IDL). A client sends to a server an object that describes the request and its parameters. The server accesses the MIB knowing its exact physical structure and implementation. The requested information is packaged in a form of an object with a format expected by the client. Such an object is returned to the client as a response.

The Object Management Group (OMG) defines the syntax of IDL. This specification is in conjunction with the Common Object Request Broker Architecture (CORBA).

An IDL specification is compiled with an IDL compiler and translated to a high-level programming language stub. This stub is further used as a framework for software that implements interfaces. Objects in the interface receive a unique identifier used to recognize objects in the network and take appropriate actions.

Distributed network management systems that use the described paradigm are robust and easily adopt physical and logical changes in the system. A well-defined interface promotes code portability and development by independent software development groups.

II.1.2 Performance Monitoring

Network performance monitoring is necessary to achieve successful control and optimal network performance. A correct choice of network performance indicators is important. Some of typical performance indicators are:

- Response time;
- Availability of network resources;
- Mean time between failures
- Mean time to recovery;
- Accuracy;
- Throughput;
- Utilization.

II.1.3 Fault Monitoring

Fault monitoring enables fault detection in as short period as possible after faults occur. Network elements inform constantly network control center about their statuses. This information, called alarms, is shown in an operator's console using a color-coded scheme that depends on alarm's priority/severity. An alarm contains information about alarm's source, severity, time of occurrence, etc.

A single fault in a network may cause multiple alarms that may come from multiple network elements as a domino effect. A procedure called root cause analysis has to detect the actual cause of problems. The ultimate goal is to automatically generate a trouble ticket with a complete diagnosis and dispatch a repair crew. Due complexity and network heterogeneity, this problem has not been solved. Only proprietary trouble-ticketing procedures exist for proprietary equipment.

II.1.4 User Accounts Monitoring

The purpose of user accounts monitoring is to collect data on usage of particular network resources by particular users. The type and the purpose of the information vary. Information may be used to (re) configure the network in order to improve its performance or for billing purposes.

II.2 NETWORK CONTROL

II.2.1 Configuration Control

The purpose configuration control is the defining of network configuration that satisfies prescribed criteria such as performance and cost. It also includes the defining of future network monitoring parameters and corresponding corrective actions in case the defined monitoring parameters change. Due course of time, it is possible that network performance deteriorate (e.g., due increased number of users and network load). In that case, the network has to be reconfigured.

II.2.2 Security Control

The purpose of security control is protection of network integrity as well as protection of users from intentional or unintentional intruders. In particular, mobile networks are vulnerable and often a target of malicious users. Commercial scanners are available that allow eavesdropping and mitigation of users.

III TECHNOLOGY OVERVIEW

III.1 NETWORK MANAGEMENT PROTOCOLS

III.1.1 SNMP

The Simple Network Management Protocol (SNMP) is a network management protocol [5,6,8,10,11,13,15] based on Transport Control Protocol / Internet Protocol (TCP/IP) [2,4,]. It was developed in late seventies and early eighties. Primarily, it has been developed to maintain and search network's Management Information Base (MIB) as well as for reception, search, and filtering of alarms generated by network elements. The information stored in the network's MIB defines the state of the network. The SNMP contains a small set of instructions for search (Get/Get Next) and change (Set) of values in the network's MIB. The SNMPv2 is an enhanced version with more efficient communications and security.

SNMP++ is a C++ Application Programming Interface (API). It was developed by Hewlett-Packard (HP) [9]. At present time, it appears to be a de facto API for SNMP based network management applications. Libraries for UNIX as well as MS-Windows are available which increases portability of software. In the MS-Windows environment, the SNMP++ relies on the WinSNMP library, which is a de facto standard in that environment. There are indications that the SNMP++ will be translated to Java which should lead to a truly portable developed code.

The main advantage of SNMP is its wide acceptance in practice. The main drawback is its simple functionality, which requires complex application software.

III.1.2 TMN

The Telecommunication Management Network (TMN) [1,8,18] is a network management protocol based on the Open Systems Interconnection (OSI) [14] standards. The TMN consists of two parts:

- The Common Management Information Protocol (CMIP) is a protocol that defines message formats and the corresponding procedures. The CMOT is a version of CMIP that uses the TCP/IP.

- The Common Management information Service (CMIS) is an interface, which defines services provided by the TMN.

The X Management Protocol (XMP) defines the API for management of communication services provided by CMIP and SNMP.

CMIP API (Red, Green, and Blue) is a C++ interface defined by the Network Management Forum (NMF) and the X-Open.

The TMN is defined as a hierarchical structure shown in Figure 3. The highest layer deals with the overall management of the entire network and the corresponding business model. The layer below manages and controls services provided by the network. The following two layers manage the network and its elements. At the lowest layer are the managed network elements.

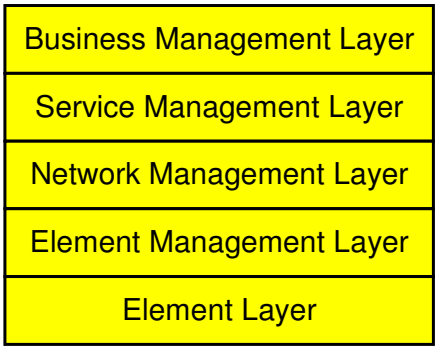

Figure 3: The TMN Hierarchy

The advantage of TMN is that it supports the Open System Interconnection (OSI) referent model. The TMN is advocated by Bellcore [1] and the European Technical Standards Institute (ETSI). A drawback of TMN is its complexity.

III.2 DATABASES

Databases are constituent part of network management systems [16] and in this section we describe database technologies.

III.2.1 RELATIONAL DATABASES

Relational databases are a well-established technology. It is based on Structured Query Language (SQL) which is a more or less standardized language for database manipulation. Although the syntax of SQL is standardized, the behavior of databases of different vendors is far from being standardized.

Majority of databases uses the relational database model. There is a wealth of database development tools.

There are three database categories:

- High-end databases like Oracle, Sybase, and Informix are the most expensive databases used for most demanding applications.

- Mid-range databases like Microsoft SQL have acceptable performance and lower price.

- Low-end databases like Microsoft Access and Paradox have acceptable performance for low-end applications but are not used for serious network management applications.

The advantage of relational databases is their widespread use and maturity. A drawback is the discrepancy with the modern object oriented software development technology.

III.2.2 OBJECT ORIENTED DATABASES

Object oriented databases are a relatively new technology developed to overcome discrepancy between relational

databases and object oriented software development technology. ODMG-93 is the current standard.

The stated advantage of object oriented databases is their ability to store objects, handle inheritance, and object-level locking. Although there is a big push in the telecommunication industry (especially in the USA) to migrate toward object oriented databases, this is still an immature technology. Also the migration path is a thorny one.

III.2.3 OBJECT-RELATIONAL DATABASES

The object relational database technology is a trade-off between relational and object oriented databases. In essence it is a slew of software development tools, which create software development framework directly from a relational database schema. As a result, software developer starts with a number of C++ or Java classes (objects) which represent information in the database in an object oriented fashion.

III.3 GRAPHICAL USER INTERFACE (GUI)

III.3.1 OSF/X-MOTIF

This graphical user interface standard has been developed for UNIX operating system. Its advantage is that developers of telecommunications equipment as well as large telecommunications companies support it. Its drawback is a high cost of development tools as well as workstations and servers.

III.3.2 MS-WINDOWS

MS-Windows environment is less widely used in professional network management systems. It has started to gain grounds with wide introduction of 32 bit multi-threading versions of this operating system. The advantages of this environment are inexpensive development tools and workstations and servers.

III.3.3 HTML/JAVA

With extensive growth of the Internet, graphical user interface based on Hyper-Text Markup language (HTML) forms and Java programming language has gained a lot of popularity. Although the struggle for supremacy between software industry giants has caused a number of interoperability problems, one might say that the Java concept promotes true software portability on the source code level. Development tools are inexpensive and often free. Wealth of the developed underlying API expedites software development process. It is very likely that this concept will be the primary choice for development of network management systems.

IV INDUSTRY PLAYERS

Major players in the US telecommunications industry are Regional Bell Operating Companies (RBOC) and Inter-Exchange Carriers (IXC). Since the introduction of the Telecommunications Bill, differences between them gradually diminish. Their networks have large number of Network Elements (NE). Also they have large number of legacy network management systems which must be upgraded to TMN. Fault and performance management is typically provided by Network Monitoring and Analysis (NMA), one of Operations Systems (OS). OSs and NEs communicate via Transaction Language One (TL1). Provisioning is typically provided by Trunk Integrated Record Keeping System (TIRKS), which is primarily for interoffice and digital facilities, and Facilities Assignment and Control System (FACS), which is primarily for end-user Plain Old Telephone Service (POTS) type circuits. In order to easily provision upgraded networks, TIRKS and FACS must be upgraded. Either complete system must be purchased or proprietary network management systems must be developed. Usually, centralized control over the entire network is performed from a single Network Operations Center (NOC). There is a need for a high degree of automation prompted by downsizing and increased competition due to the Telecommunications Bill.

Post, Telephone, and Telegraph (PTT) are the major telecommunications players in Europe. They are subject to regulations by the European Union (EU) and by individual state governments. European public utilities are required to purchase equipment to established European Telecommunication Standardization Institute (ETSI) standards. With the ongoing deregulation in Europe, differences between RBOCs and PTTs will diminish.

With ongoing deregulation of telecommunications industry, Independent Operating Companies (IOC) and Competitive Access Providers (CAP) have become significant players in the telecommunications industry. They have large number of embedded, less intelligent NEs. They do not have large base of homogeneous operations systems. Therefore the primary need is functionality, not compatibility of equipment. Network management systems for IOC/CAP networks must provide centralized management during early deployment, and evolve into distributed multi-user systems.

Private networks are the most heterogeneous part of the telecommunications industry. They are much smaller than telephone networks. Their size and geographic topology is extremely variable Need for network management is also variable. Private networks are engineered to be optimized for a particular use. Thus, they tend to maximize the use of features of the particular network technology. This requires network management systems that is tightly coupled to the NEs and will result in network management systems being developed by the same vendor as NEs. This will result in a hierarchical NM strategy where an integrated network management system communicates with NE vendor network management systems.

V EXAMPLES OF NETWORK MANAGEMENT APPLICATIONS

V.1 REAL-TIME TROUBLE-TICKETING AND DISPATCHING

When a failure in a network occur, multiple alarms are generated by multiple network elements. A root cause

analysis procedure identifies the actual cause of problem. Then, a trouble-ticket has to be issued. Ideally, a trouble-ticket should contain a detailed description of a failure with instructions to a repair crew. The trouble-ticket should be sent to the repair crew that is most qualified for the job. The system may be linked with the spare parts ordering system so that the overall system is aware of availability of spare parts needed for repair. To increase utilization of resources across wide geographic areas, mobile crews may be located via GPS, and the closest crew may be dispatched. Currently, the technology is still far from such a complete solution, predominantly due network heterogeneity and unavailability of a sufficiently general root cause analysis procedure.

V.2 CUSTOMER CARE SYSTEM

In the increasingly competitive telecommunication services business (e.g., Internet Services Providers), quality of Customer Care System (CCS) is often a decisive factor in selection of a telecommunication services provider.

Staff of a CCS center consists of telephone operators that accept customers' telephone calls (complaints, service requests, etc.) and generate service orders (e.g., repairs), and service crews that execute service orders.

Events that take place since a customer calls for the first time are as follows:

1. A customer calls a CCS center, explains the problem, and tells its personal information.

2. Based on the obtained information, an operator selects one of the problem categories from a list of problems defined in the system.

3. Based on the selected problem category and availability of repair crews qualified for the problem, a service order is generated and a service crew is scheduled for a first possible appointment;

4. After the service order is completed, it is closed and annotated by the crew.

The system allows a number of functions that further enhance the quality of service such as:

- Automated repair crew notification via a pager or e-mail;

- Statistical (historical) analysis of service orders (customer satisfaction, number and type of repairs, etc.).

- Dial-up access to the service orders database that allows service crews to get service orders for the day from home, thus saving the trip to the CCS center; This facility also allows crews to annotate service orders from customers' site.

V.3 ADVANCED BILLING SERVICES

With the Internet gaining popularity on a daily basis, communications services providers develop new services to their users that are available over the Internet. One of basic services is access to billing information about users' accounts. Typically, such a system has a three-tier architecture described in this paper. The network access server provides access to the Internet and verifies user access rights. It also generates responses to users in HTML format. The server is connected via Intranet with a database server that contains billing information.

A user provides its password and accesses information about current charges and/or billing history. It is also possible to obtain other information such as telephone calls history that contains a list of called numbers and duration of calls.

It is also possible to provide such services to users without access to the Internet. In such a case, user commands are restricted to a standard touch tone 12-button dial and/or simple spoken commands such as numbers 0-9, "yes", and "no". The response is in a form of synthesized speech.

Users may elect to receive invoices over e-mail and receive credit from the communication services provider.

It is possible to send invoices in a preformatted electronic form that users may later use for their own accounting purposes.

Users may have an option to pay their bills over the Internet. This service would expedite flow of money and eliminate paperwork completely.

VI CONCLUDIONS

In this paper we presented issues and trends in network management. Quality of a network management system is a crucial element of a communication system and may be a decisive difference in today's increasingly competitive telecommunication services business. By no means we intended to be exhaustive. The paper is a compilation of experience gained in various projects. Issues range from low-level design decisions such as selection of a database to design of high-level Business Management Layer applications.

REFERENCES

[1] -. Generic Requirements for Operations Based on the *Telecommunications Management Network (TMN) Architecture, Bellcore Generic Requirements*, GR-2869-CORE, Issue 1, October 1995.

[2] U. Black, *TCP/IP and Related Protocols*, McGraw Hill, 1992.

[3] -, *Principles for a Telecommunications Management Network*, CCITT Recommendation M.3010, October 1992.

[4] S. Feit, *TCP/IP: Architecture, Protocols, and Implementation*, McGraw-Hill.

[5] S. Feit, SNMP: *A Guide to Network Management*, McGraw-Hill, 1994.

[6] S. J. Harnedy, *Total SNMP: Exploring the Simple Network Management Protocol*, CBM Books, 1994.

[7] Leinwand, and K. Fang, *Network Management: A Practical Perspective*, Addison-Wesley, 1993.

[8] S. Mazumdar, S. Brady, D. W. Levine, "Design of Protocol Independent Management Agent to Support SNMP and CMIP Queries," Third International Symposium on Integrated Network Management, April, 1993.

[9] P. E. Mellquist, *SNMP++: An Object Oriented Approach For Network Management Programming Using C++*, Revision 2.1, Hewlett-Packard, January 1995.

[10] M. E. Miller, *Managing Internetworks with SNMP: The definitive Guide to the Simple Network management Protocol (SNMP) and SNMP Version 2*, M & T Books, 1993.

[11] M. T. Rose, *The Simple Book: An Introduction to Management of TCP/IP-based Networks*, Prentice-Hall, 1990.

[12] M. T. Rose, *The Simple Book: An Introduction to Internet Management*, Prentice-Hall, 1993.

[13] M. T. Rose and K. Z. McCloghrie, *How to Manage Your Network Using SNMP: The Network Management Practicum*, Prentice-Hall, 1990.

[14] S. Scoggins and A. Tang, *Open Networking with OSI*, Prentice-Hall, 1992.

[15] W. Stallings, *SNMP, SNMPv2, and CMIP:The Practical Guide to Network Management Standards*, Addison-Wesley, 1993.

[16] F. Stamatelopoulos, N. Roussopoulos, B. Maglaris, "Using a DBMS for Hierarchical Netrwork Management," Engineer Conference, NETWORLD+INTEROP '95, Las Vegas, March 1995.

[17] K. Terplan, and J. Hungtington-Lee, *Applications for Distributed Systems Management*, Van Nostrand Reinhold, 1994.

[18] Yoda, K, Yata, and N. Fujii, "Object Oriented TMN Based Operations System Development Platdorm," ICC/SUPERCOM, 1994.

Credit: Work on this manuscript was partially supported by Mobtel.

Abstract: In this paper we present issues and trends in network management. Due ongoing deregulation in the US and Europe, telecommunications services business has become increasingly competitive. Downsizing in staff has prompted the need for reengineering and improved efficiency. In such a competitive environment, quality of a network management system may be a decisive factor. In this paper we discuss some of the issues a network management system designer/developer has to deal with.

TRENDS AND ISSUES IN NETWORK MANAGEMENT

Dragomir D. Dimitrijević and Ilija Đekić