MANAGING NETWORKS CONTAINING DUMB DEVICES WITH INTELLIGENT AGENTS

By

David Kenneth Barnes
Nova Southeastern University
dkbarnes@Huizenga.nova.edu
The Wayne Huizenga Graduate School of Business & Entrepreneurship
Fort Lauderdale, Florida 33315

Today there are new challenges facing network managers of heterogeneous networks. A heterogeneous network may be computing devices manufactured by various companies that are connected and potentially able to communicate with each other. Today, we have new intelligent devices mixed with old dumb devices making up vast communications networks. Network administrators need to communicate with all the devices that make up the network to monitor their status. Device failures can be very disruptive and very expensive due to the stopping of user or business productivity. These networks may be local (LAN) or spread out across a continent (WAN). The unpredictable nature and dynamism of network devices require that new ways be found to monitor the condition and performance of the total network. This must be done well in advance of any device failures.

Introduction

This section provides an overview of network management and describes the major challenges created by the growth and expansion of the Internet.

Background

It is the goal of network management to establish, integrate, and provide all the needed resources to the communication network. It is also very important that network service objectives are met within a reasonable cost. The objectives of network management are efficient use of resources, Provide network security, minimization of down time, monitor and manage the constantly changing communications, technology and services. This must be done while reducing the cost of network operations. The evolution and revolution of networks and their management systems over the years has resulted in a variety of network management issues. Key among these issues is:

- A multiplicity of device manufacturers. In networking, there has always been a various array of equipment vendors and manufactures. The deregulation of the telecommunications industry in 1984, has open the way for a rise in the number of telecommunications equipment vendors and manufacturers.
- Variability of management applications and inconsistent forms of databases.

MANAGING NETWORKS CONTAINING DUMB DEVICES WITH INTELLIGENT AGENTS

- Each network management system (NMS) was often designed for a particular function. Often applications designed by various manufactures produced the same or similar results. In the telecommunications industry, the early NMS had their own supporting databases and user interfaces. There was very little, automated exchange of information between different NMS applications. The first attempts to manage a network were first done by the use of cables. This was the physical connecting of devices using cables. This was true ,whether the devices were a switch device or repeater device that was part of a segment, or routing devices that made up LANS. These databases were often locally managed, which, being dependent on manual interventions, resulted in performance inconsistencies.

Problem Statement

The issues mentioned above, coupled with those related to the explosive growth of the Internet and the resulting integration issues, have created the following network management challenges:

- Dynamism. The structure of both networks and NMSs has been changing dramatically and the complexity has been increasing. For networks, the main reasons for these developments are the incompatibility of multi-vendor equipment and the dynamic changes in network topology due to the proliferation of wireless links. With the increasing complexity of the underlying networks, the demand for more sophisticated network management functionality has grown.
- Multiple standards. The data communications community generally adopted simple network management protocol (SNMP), while the telecommunications community generally adopted the telecommunications management network (TMN) concept and the common management information protocol (CMIP).
- Interoperability. Both SNMP and CMIP are based on platform-centric manager-agent paradigms, each with its own information model, as described in the following section. The critical network management interoperability issues result from dissimilar network management information models and manager-agent communications protocols.(n2)
- Distribution. For the reasons described above, the traditional centralized or hierarchical architectures for network management are no longer adequate. Although both have their relative merits, they both suffer from scalability problems as the network size or the number of management applications increases. Distributed network management has the advantages of NMS location-independence, better scalability, distribution of network/resource load, and reliability. However, this creates additional challenges—for example, network security.
- Network security. As the NMS controls the network and its management data, its security scheme is extremely important. With network management becoming increasingly distributed and network management standards evolving toward openness, security becomes even more critical.

- Cost. In the past, large operators of networks could afford to spend huge amounts of money on maintaining their networks. The costs were passed on to the customers, who had few choices. In the age of the Internet-based economy and fierce competition for customers' dollars cost control is a primary focus of even the biggest operators.

Outline

The main thrust of this paper is to show how intelligent agents can be utilized in the management of networks containing dumb devices by use of RMON and intelligent agents. The next section briefly describes the current approaches to network management and points out their shortcomings. The following section describes the agent-based approach to network management. It provides a brief tutorial on intelligent agents, RMON and their standards. A subsequent section provides a comparative analysis of the approaches to network management and highlights how the agent-based approach addresses the shortcomings identified earlier. The final section concludes the paper and points out future work.

Current Approaches to Network Management

This section describes existing strategies for network management and discusses their shortcomings.

Agent/Manager Paradigm

It is possible (in fact, likely) that a specific management system may function as a manager for some applications and as an agent for other applications. The agent/manager paradigm is similar to the client/server paradigm except for some subtle differences. Usually, the manager is analogous to the client, and the agent, to the server.

The agent initiates a reporting action, so it acts as a client. The manager reacts to the agent's action,

So it behaves like a server. Swapping of roles is not part of the traditional client-server model.

A manager is a software program that can query agents, receive responses from agents, and send directives to agents. An agent is a software program (often residing on the managed entity) that responds to manager requests and performs management functions on managed entities (communication resources capable of being monitored and controlled). A management information base (MIB) is a conceptual representation of information related to a managed entity and how users can access it.

The agent acts as an interpreter of information resources contained in the MIB, providing filtering of the information and informing the manager about autonomous events that occurred. Communication between agent and manager is performed as a set of requests, responses, and autonomous messages as defined by specific standards (for example, SNMP and CMIP).

MANAGING NETWORKS CONTAINING DUMB DEVICES WITH INTELLIGENT AGENTS

SNMP

SNMP was issued in 1988 by the Internet Activities Board (IAB) and was soon adapted as a simple tool for managing bridges and routers in transmission control protocol (TCP)/Internet protocol (IP) networks. (N3) It is based on the manager-agent paradigm.

SNMP runs over user datagram protocol (UDP) and relies on polling to collect management data. The manager has all the management intelligence (for example, for filtering data). SNMP version 1 (SNMPv1) has five messages, or protocol data units (PDUs), restricts the maximum size of messages, and provides only simple security based on community name and password. SNMPv2, issued in 1993, includes two additional PDUs: GetBulkRequest to allow one SNMP message to access multiple objects in a MIB and InformRequest to allow manager-to-manager communication, as shown in Figure 2. SNMPv2 was also meant to include several security features: access control (read-write permissions for specific MIB views), authentication, and message encryption. However, agreement could not be reached on the security protocols to use. Consequently, several versions of SNMPv2 were issued with or without these security features. SNMPv3, issued in 1998, included user-based security and view-based access control models. A detailed account of the evolution of SNMP is given by Stallings. (n4)

The fact that SNMP relies on polling to collect management data creates a scalability problem as the number of managed elements increases. Furthermore, a very large amount of operational data is sent to the manager, which must be monitored and processed, making bandwidth a critical factor and increasing computational load on the manager. Several techniques have been used to resolve these problems including trap-directed polling, management by delegation, and agent extensibility protocol (AgentX). In trap-directed polling, agents can be instructed to inform the manager of specified events, thus freeing the manager from continuous polling. In management by delegation, (n5) the agents are enhanced to perform certain functions (for example, event filtering and event correlation) to free the manager from performing these tasks. In AgentX, (n6) a hierarchy of agents is created: a master agent communicates with several subagents using the AgentX protocol. Only the master agent communicates with the manager, and its MIB logically has all the information contained in the MIBs of the subagents registered with the master agent.

Even with these enhancements, the centralized architecture of SNMP, although simple to implement and use does not meet the requirements of large distributed systems.

Intelligent Agents

The term agent is highly overused. (n17-n20) On one hand, we have systems like SNMP or CMIP agents that are nothing more than servers providing data to their clients—management applications. On the other side of the spectrum, there are expert systems with huge knowledge bases, which are also considered agents due to their intelligent behavior.

MANAGING NETWORKS CONTAINING DUMB DEVICES WITH INTELLIGENT AGENTS

In this paper, an agent is defined to be a computational entity that acts on behalf of others, is autonomous, is both proactive and reactive, and exhibits a certain degree of ability to learn, cooperate, and move. Just as one delegates to a human agent certain tasks such as booking a trip, selling a house, or gathering sensitive information, a client delegates to a computational agent certain tasks that are to be achieved without, or with a minimum of, his further involvement. After receiving the details of the task, the agent acts autonomously following certain algorithms. Even network segments containing "dumb" devices, can be monitored and topologized through the use of probes, agents and RMON.

Using their skills, agents proactively try to attain the goal defined by the assigned task. They can acquire their skills by being told (education) or through expertise (observation). Agents react to changes in the available data by modifying their plans. They acquire and modify their knowledge in response to experience and exchange of information. They also communicate to share their knowledge and collaborate in attaining their goals. Agents may have to be mobile to achieve their goals.

RMON Standards

RMON was developed to enhance the monitoring capabilities defined in the original mib-2 MIB.(n2) RMON provides standard methods to control the operation of and collect statistics from a generic network-monitoring device—an "RMON probe." This generic probe is assumed to have one or more promiscuous interfaces through which network segments can be monitored. The RMON standard has been developed in phases. The first phase (RMON-I)(n2) provided MIBs and definitions that primarily dealt with monitoring network traffic at the second layer (the logical link layer) of the Open Systems Interconnection (OSI) reference model.

The main focus was Ethernet, with an extension to support token-ring networks.(n52) the second phase of RMON development culminated in the RMON-II(n51) specification. RMON-II provided support for monitoring statistics at the third OSI layer and above, as well as other extensions.

Comparative Analysis

In the "Problem Statement" section, a number of the challenges of managing complex networks, which must be handled by network managers and designers of network management systems, were described. In the following sections, the ability to address these issues through solutions based on agents and probes is contrasted with the ability—or, in many instances, the inability—to deal with the problems without such technology.

Dynamism

Dynamism is handled by agent-based systems in a natural way, because an agent platform provides for a controlled agent life cycle. Agents can be added to the system at will. They can join the agent society through registration mechanisms, which are an integral part of the platform. A device can make itself known to the rest of the network through its agent, so that network discovery is automatic.

Similarly, services can be created on-line and added to the offerings through directory services or brokers of various levels of sophistication. The meta-level facilities are used to dynamically discover supported communication parameters such as language, protocol, and ontology.

Multiple Standards
At the highest level, agents use a uniform communication means. Any other standard can be applied at the content level. There is no other technology that allows for such a degree of flexibility in network management.

Interoperability
Ontology is a branch of metaphysics that deals with the nature of being and reality. The meta-level layer for exchanging data about communication acts allows for coherent exchange of data at the content level. Each side of the communication link knows exactly what kind of data to expect and what is their meaning . This allows for machine-to-machine understanding in which data are processed automatically without prior arrangements. Ontologies provide a means not only for structuring data, but also for describing relationships and rules governing the data, as well as processing algorithms. It is too early to predict how ontologies will be handled in the context of network management, but one probable scenario is that they will not be subjected to lengthy standardization processes. There already exist public repositories of ontologies. (n46) In the future, there might be commercial sites as well. Nevertheless, even if ontology were to be standardized, it would be much easier to agree upon due to its relatively small size.

Security
Agent-based systems allow for security schemes at several layers, as explained in a previous section. Every other network management technology provides security mechanisms, because security is considered a critical aspect of managing networks. Implementing a security scheme is controversial as could be seen following the evolution of SNMP, which, only in its third version, provides for a security scheme.(n4)

Both SNMP and CMIP standards mandate security schemes that have to be implemented at the design and deployment phases. Agent-based computing is a convenient paradigm to enforce security because, in contrast to mere objects, agents decide at run time whether a received request will be fulfilled.

User Experience
Web-based management simplifies access to network management functionality and data using popular Web browsers as front ends.

Deployment is also simplified, because most workstations already have a browser. The reporting side uses a Web server, which is also familiar to many network managers. Other technologies described in this paper do not make any assumptions as to the presentation of network management data. Agent-based systems stand out, because in their most sophisticated versions, they deliver plug-and-play networks.

MANAGING NETWORKS CONTAINING DUMB DEVICES WITH INTELLIGENT AGENTS

A special kind of agent—an interface agent—can be used for user profiling. One application is customization of workspaces for network managers, which may improve productivity. This kind of agent can also be used for profiling network users, thus improving the quality of service.

Rapid Software Delivery

Of all the approaches discussed in this paper, new architectures built on top of SNMP and CMIP standards are the most expensive to design, implement, deploy, and maintain. Modifications require numerous changes to the configuration data as well as off-line time. To accommodate new advances in standardization, software components have to be recompiled and linked again .

Cost

Costs are incurred while addressing all issues discussed in this section and elsewhere in the document. As argued in this paper, agent-based systems are characterized by advantages in all solutions relevant to network management. Therefore, employing agents will result in lower expenses.

Conclusions

I have described the current approaches to network management, pointed out their shortcomings, and explained how intelligent agents can be utilized to address these shortcomings. I have shown how intelligent agents can effectively deal with issues of dynamism, interoperability, and distribution, and I have contrasted the effectiveness of intelligent-agent-based solutions to network management with the way traditional network management methods deal with such issues.

References

(n1.) P. Kalyanasundaram and A. S. Sethi, “Interoperability Issues in Heterogeneous Network Management,” J. of Network and Systems

(n2.)W. Stallings, SNMP, SNMPv2, SNMPv3, and RMON 1 and 2--Practical Network Management, 3rd ed., Addison-Wesley,

Reading, Mass., 1999. Management, Vol. 2, No. 2, June 1994, pp. 169-193.

(n3.) J. Case, M. Fedor, M. Schoffstall, and J. Davin, “A Simple Network Management Protocol (SNMP),” IETF RFC 1157, May 1990,
http://www.ietf.org/rfc/rfc1157.txt

(n4.) W. Stallings, “SNMPv3: A Security Enhancement for SNMP,” IEEE Commun. Surveys, Sept. 1998,
http://www.comsoc.org/pubs/surveys

(n5.) G. Goldszmidt and Y. Yemini, “Delegated Agents for Network Management,” IEEE Commun. Mag., Vol. 36, No. 3, Mar. 1998, pp.
66-70.

(n6.) M. Daniele, B. Wijnen, and D. Francisco, “Agent Extensibility (AgentX) Protocol,” IETF RFC 2257, Version 1, Jan. 1998,
http://www.ietf.org/rfc/rfc2257.txt

MANAGING NETWORKS CONTAINING DUMB DEVICES WITH INTELLIGENT AGENTS

(n7.) International Organization for Standardization, "Common Management Information Service Element (CMISE)," ISO Rec. 9595, Nov.
1998.
(n8.) International Organization for Standardization, "Common Management Information Protocol (CMIP)," ISO Rec. 9596, Nov. 1998.
(n9.) International Telecommunication Union, "Guidelines for the Definition of Managed Objects," ITU-T Rec. X.722, Jan. 1992,
http://www.itu.int

(n10.) Object Management Group, "CORBA-Based Telecommunication Network Management System," OMG White Paper, May 1996,

ftp://ftp.omg.org/pub/docs/telecom/ 96-07-01.pdf
(n11.) http://www.omg.org/
(n12.) Joint Inter-Domain Management Group, Inter-Domain Management: Specification Translation, X/Open Company Ltd., Reading,
Berkshire, U.K., 1997.
(n13.) http://www.rapidlogic.com/tech/white_papers.html
(n14.) http://www.agranat.com/emweb/
(n15.) http://www.w3.org/MarkUp/
(n16.) http://www.w3.org/XML/
(n17.) Unmasking Intelligent Agents, special issue of Intelligent Systems and their Applications, Vol. 14, No. 2, IEEE Press, Piscataway, N.J.,
Jan./Feb. 1999.
(n18.) W. Brenner, R. Zarnekow, and H. Wittig, Intelligent Software Agents, Springer-Verlag, New York, 1998.
(n19.) N. R. Jennings and M. J. Wooldridge, AgentTechnology, Springer-Verlag, New York, 1998.
(n20.) J. M. Bradshaw, Software Agents, MIT Press, Cambridge, Mass., 1997.
(n28.) http://www.fipa.org/
(n29.) Foundation for Intelligent Physical Agents, "FIPA '97 Specification Part 2: Agent Communication Language," Version 2.0, Oct. 1998,
http://www.fipa.org/spec/FIPA97.html
(n30.) Foundation for Intelligent Physical Agents, "FIPA '97 Specification Part 1: Agent Management," Version 2.0, Oct. 1998,
http://www.fipa.org/spec/FIPA97.html
(n31.) C. J. Petrie, "Agent-Based Engineering, the Web, and Intelligence," IEEE Expert, Vol. 11, No. 6, Dec. 1996, pp. 24-29.
(n32.) M. Barbuceanu and M. S. Fox, "COOL: A Language for Describing Coordination in Multi-Agent Systems," Proc. 1st Intl. Conf. on

Multi-Agent Systems (ICMAS '95), San Francisco, Calif., June 12-14, 1995, pp. 17-24.

(n33.) Y. Shoham, "Agent- Oriented Programming," Artificial Intelligence, Vol. 60, No. 1, Mar. 1993, pp. 51-92.

MANAGING NETWORKS CONTAINING DUMB DEVICES WITH INTELLIGENT AGENTS

(n34.) D. Kinny, M. Georgeff, and A. Rao, "A Methodology and Modeling Technique for Systems of BDI Agents," Proc. 7th European

Workshop on Modeling Autonomous Agents in a Multi-Agent World, Eindhoven, The Netherlands, Jan. 22-25, 1996, pp. 56-71.

(n35.) S. A. DeLoach, "Multiagent Systems Engineering: A Methodology and Language for Designing Agent Systems," Agent-Oriented

Information Systems Conf. (AOIS '99), Seattle, Wash., May 1, 1999, and Heidelberg, Germany, June 14-15, 1999.

(n36.) M. Elammari and W. Lalonde, "An Agent-Oriented Methodology: High-Level View and Intermediate Models," Agent-Oriented

Information Systems Conf. (AOIS '99), Seattle, Wash., May 1, 1999, and Heidelberg, Germany, June 14-15, 1999.

(n37.) M. Wooldridge, N. R. Jennings, and D. Kinny, "Methodology for Agent-Oriented Analysis and Design," Proc. 3rd Intl. Conf. on

Autonomous Agents, Seattle, Wash., May 1-5, 1999, pp. 69-76.

(n39.) B. Hayes-Roth, "A Blackboard Architecture for Control," Artificial Intelligence, Vol. 26, No. 3, July 1985, pp. 251-321.

(n40.) K. Taveter, "Business Rules' Approach to the Modeling, Design, and Implementation of Agent- Oriented Information Systems,"

Agent-Oriented Information Systems Conf. (AOIS '99), Seattle, Wash., May 1, 1999, and Heidelberg, Germany, June 14-15, 1999.

(n41.) http://www.oasis-open.org/cover/dmtf-cim.html

(n42.) http://www.w3.org/TR/PR-rdf-syntax/

(n43.) http://wave.eecs.wsu.edu/CKRMI/OML.html

(n44.) B. N. Grosof and Y. Labrou, "An Approach to Using XML and a Rule-Based Content Language with an Agent Communication Language," Intl. Joint Conf. on Artificial Intelligence (IJCAI '99) Workshop on Agent Communication Languages, Stockholm, Sweden, Aug.1, 1999.

(n45.) J. D. Case and D. B. Levi, "SNMP Script Language," IETF Internet Draft, Oct. 1993, http://ftp.sunet.se/ftp/pub/network/monitoring/

btng/draft-levi-snmp-script-language-00.txt

(n46.) http://ontolingua.stanford.edu/frame-editor

(n47.) http://www.lucent-inferno.com/

(n48.) http://java.sun.com/products/jini/index.html

(n49.) http://www.upnp.org/

n50) S. Waldbusser, "Remote Network Monitoring Management Information Base," RFC 1757, IETF, Feb. 1995, http://www.ietf.org

MANAGING NETWORKS CONTAINING DUMB DEVICES WITH INTELLIGENT AGENTS

(n51.) D. Perkins, RMON: Remote Monitoring of SNMP-Managed LANs, Prentice Hall, Upper Saddle River, N.J., 1998.

(n52.) S. Waldbusser, "Token Ring Extensions to the Remote Network Monitoring MIB," RFC 1513, IETF, Sept. 1993,

http://www.ietf.org

By David K. Barnes

David Kenneth Barnes is a member of technical staff in NetworkCare Professional Services at Lucent Technologies in Marlboro, Massachusetts and an Adjunct Research Professor in the Systems and Computer Engineering Department at Boston University in Boston, Massachusetts. He received a M.B.A. degree from Rivier College, Nashua, New Hampshire concentrating in information systems. He is a PhD candidate in Business and Information Technology, at Nova Southeastern University, Fort Lauderdale, Florida. Mr. Barnes was formerly associated with Eastman Kodak, Nortel Networks, and Sun Microsystems Inc. His work has focused on network management, computer based education, and Consonance Theory.