IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

COMPUTER NETWORK MANAGEMENT AND ADMINISTRATION INTERNATIONAL TRADE AND UNPARALLELED TECHNOLOGICAL INNOVATIONS

Dr. Vinod Ambohore
Assist. Professor, Dept. of Commerce and Management, Siddharth Library and Information Science College, Padegaon, Aurangabad

Abstract:

The paper concludes that Computer network management has catalyzed the need to accelerate public sector reforms in developing countries and the need to set up correctly-working institutions. The current Computer network management and administration movement reveals unprecedented levels of exchange felled by levels of consumer demand never previously known, carrying a potential for growth and prosperity transcending any that the world had ever recorded. Computer Network Management and Administration refers to the subject of managing 'computer networks'. Network Management and Administration Services helps company system administrator to manage a network. Wide variety of software and hardware products are existing in IT industry.

Keywords: developing societies, Emerging-market, decision-makers, journals and books.

Introduction

1) Introduction During the twentieth century, the key computer technology has been information gathering, processing and distribution 2). PC´s and workstations interconnected are substituting mainframes. Computer networks and distributed processingmanagement systems are growing importance and, indeed, have become critical in the business world. Within a given organization, the trend is toward larger, more complex networks supporting more applications and most users. As these networks grow in scale, two facts become painfully evident 5). For the last ten years many organizations have implemented computer networks. Technological evolution is permitting the distributed systems implementation based on client/server architecture associated with efficacy and low costs 7) The computer network and its associated resources and distributed applications become indispensable to the organization. More things can go wrong, disabling the network, a portion of the network, or degrading performance to an unacceptable level.A need of efficient operation, free of faults, has appeared with the importance of networks for the organizations 3). The computer networks are compounded of differentplatforms of hardware and software: several protocols, resources and services. A large computer network cannot be put together and managed by human effort alone. The complexity of such system requires automated computer network management tools to monitors and manage the resources utilization.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

2) Computer Network Management

Definitions of computer network management 1). The ISO´s one says that "Computer Network Management has mechanisms to monitors, control and coordinate OSI environment´s resources for theinformation exchange between these resources". It involves the areas of: i) fault: The facilities that enable the detection, isolation, and correction of abnormal operation. ii) configuration: The facilities that exercise control over, identify, collect data from, and provide data. iii) account: The facilities that enable charges to the established for the use of managed objects and costs to be identified for the use of those managed objects. iv) performance: The facilities needed to evaluate the behavior of managed objects and the effectiveness of communication activities. v) security: The facilities that address those aspects of OSI security essential to operate OSI network management correctly and to protect managed objects.

In function of the distributed nature of the managed resources, network management is a distributed application based on concepts like objects, agents, managers, management information base MIB and protocols. Network devices, called objects,contain information about themselves. For example, every device has been configured with some selection of parameters. A device has a current status that indicates whether it is in healthy running condition. Devices often keep internal statistics that count incoming and outgoing traffic and various observed errors 8. It is convenient to think of the configuration, status, and statistical information in a device as forming a "database". In reality, information may be stored at a device as a combination of switch settings, hardware counters, in-memory variables, in-memory tables, or files.

This logical database of network management information is called a Management Information Base MIB. We don't really care about the internal, physical form of this data. But we are very interested in being able to access this data. Agent software is installed in each device. An agent receives incoming messages from a manager. These messages request reads or writes of the device's data. The agent carries out the request and sends back responses. An agent does not always have to wait to be asked for information. When a serious problem arises or a significant event occurs, the agent sends a notification message called a trap to one or more managers. Manager software at a management station sends request messages (polling) to agents and receives responses and spontaneous trap messages from agents. What protocol carries this message? UDP is the preferred choice, but any transport protocol is acceptable. To a network management system, we need one or more applications that enable an end user to control the manager software and view network information. To complete the Network Management, the ISO´s and ITU-T´s standards are based on the CMIP (Common Management Information Protocol) protocol and the Internet Activity Board are based on Simplecomputer Network Management Protocol 6). Because of the complexity of OSI systems, CMIP is not very easy to be implemented and will not be treated at this paper. "Support for SNMP" actually is a shorthand for the fact that hubs, bridges, routers, multiplexors, switches, or whatever canbe managed, conform to the Internet-Standard Management Framework. This framework is easy to implement, is powerful, and opens up like a big umbrella to take more and more technologies

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

under its protection. SNMP is described by the RFC1157 May, 1990: i) Defines the messages that can be exchanged between a management station and a system to read or update variable values. Ii) Defines trap (alarm) messages that are sent by a system whose status is changing in a serious way.iii) Deals with the nitty-gritty details of message formats and communications protocol specification.

SNMP specifies for managing:

i) All sorts of equipment - bridges, repeaters, ASCII terminals. ii) Many types of interface technology - Point-to-Point, DS1, DS3, X.25, Frame Relay, Ethernet, Token -Ring, FDDI, and others. Iii) Popular proprietary protocols such as DECnet, Phase IV, and AppleTalk.

The simplicity of version one of SNMP contributed to its rapid implementation and acceptance. However, version one had some serious shortcomings. There was no reliable method of authenticating the source of network management messages. There was no way to secure the contents of network messages from network eavesdroppers. In April of 1993, SNMP version 2 was put onto the standards track. Version two addressed the authentication and security of management messages. It also contained useful protocol enhancements and improved the administrative framework for the maturing protocol suite. But version two has been criticized because of its complexity: it uses far greater system resources than version 1). The SNMP community has used an evolutionary approach to standardize what information should be kept in a device's MIB: i) Define groups of clearly useful parameters. ii) After several months of field experience, fine-tune these groups. Throw away parameters that are not useful. Add new ones that are needed. iii) Set up committees of industry experts to define MIB variables for special technologies, such as bridges or Token-Ring interfaces. Iv) Add vendor-specific extensions that cover special features of a vendor's products.

To get this level of flexibility, management information is structured as a tree, so that new branches can sprout wherever they are needed. SNMP was originally developed to satisfy an immediate requirement to manage TCP/IP communications on the Internet. The first MIB, now called MIB-I, concentrated on information specific to TCP/IP. Sample variables from the originals MIB included: • A system description • The number of networking interfaces • The IP address associated with each network interface • Counts of the numbers of incoming and outgoing datagrams

Information about active table of TCP connections

After deployment in the field, the basic definitions were clarified and many new definitions were added. The results were published in RFC1213: MIB-II. MIB-II has proved to be a robust basis for TCP Management. At the time of writing, there were still network devices deployed that had not been upgraded from MIB-I to MIB-II. Life being what is, this probably will persist for some time. However, the good news is that, since MIB-II is compatible with MIB-I, management stations can work with agents that support either MIB.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

3) BasedPractical Recommendations on the Example of Computer Network Management at PortableTo customize a network management tool, this work based on the example of Portable's network management.

4)Suggests the division between areas, looking at: i) topology - faults, ii) servers and links - performance iii) utilization of resources - account iv) control of distributed resources - configuration v) control of access - security

The fault-monitoring system should assist in isolating and diagnosing the fault. Examples of tests that a fault-monitoring system should have at its command include a i) connectivity test ii) data integrity test iii) protocol integrity test iv) data saturation test v) connection saturation test vi) response-time test vii) loopback test viii) function test ix) diagnostic test. The most important Network Performance Indicators should be present in performance reports: i) Availability ii) Accuracy iii) Response Time iv) Throughput v) Utilization

Examples of resources that may be subject to accounting include the following:i) computer hardwareii) communications facilities iii) software and systems.

Management of Services

Configuration information describes: The nature and status of devices, specification of the resources, attributes of the resources.

Computer network security address three requirements: Secrecy:information accessible only for reading by authorized parties, integrity: assets can be modified only by authorized parties, availability: assets are available to authorized parties

Conclusions and suggestion

The arrival of Pcs, workstations, LANs, and servers changed the shape of networks forever. Customers began to buy systems from different vendors. Computer Network Management tools appeared to solve the chaotic situation of different platforms talking with each other at the same time. There is a widely implemented protocol, SNMP, for network equipment's of all types. To monitore a computer network by a manager station, it is necessary to buy a management software and customize it taking care on each parameter of the devices, depending on the information needed: of fault, of configuration, of performance, of security, of account.

Bibliography:

1. Duarte, Fátima de Lima Procópio Duarte, Simulação e Análise do Benchmark TPC-C, Dissertação de MestradoapresentadaaoDepartamento de Ciência da Computação da Universidade Federal de Minas Gerais, Brasil, Janeiro de 1996.

2.Brisa, Gerenciamento de Redes - Uma Abordagem de SistemasAbertos, Makron Books, Brasil, 1993.

3. Stallings, Willian, SNMP SNMPv2 and RMON, Addison-Wesley Publishing Company, 1996

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

4.Feit,

5.Teixeira, Suzana de Queiroz Ramos e Oliveira, Mauro, Disponibilização do Conhecimento no Gerenciamento de Redes de Computadores, artigo, Brasil, XXIII SeminárioIntegrado de Hardware e Software, Agosto 1996.

6. GRC, Gerenciamento da Rede Municipal de Informáticaatravés do ISM, Prodabel, Brasil, Fevereiro de 1997.

7.Tanembaum, Andrew S., Computer Netwoks, Prentice Hall International Inc., USA, 1989.

8. Case, J., Fedor, M. Schoffstall, M. Davin, J., Network Management Protocol-SNMP, May 1990.