www.cenresinpub.org
ISSN 2277-0097

DESIGN AND MODELLING OF STRATEGIC INFORMATION SYSTEM

[1]Okpeki U. Kazeem and [2]Adebari F. Adebayo
[1]Department of Electrical/Electronics/Computer Engineering, Delta State University,
[2]Department of Computer Engineering, Yaba College of Technology, Yaba Lagos.
email:omakazeem@yahoo.com

ABSTRACT
In this paper the design, modelling and management of information system is presented. It takes into consideration the basic component that makes an effective management information system. Many of information system use in many organizations today are very large, inefficient, expensive to maintain and to a very large extent do not meet the real needs of the organization. New applications have been added and new technology deployed without thought given to the system functionality, performance, reliability and security. With this strategy today's systems will benefits from the advancement made in system engineering and complexity management.
Keyword: *Entrepreneurial activity, data gathering, data processing, pooling,* sharing.

INTRODUCTION
Management information system is a communication process in which data are recorded and processed for operational purposes. The problems are isolated for higher level decision making and information is fed back to top management to reflect the progress or lack of progress made in achieving major objectives. The use of information systems is an entrepreneurial activity. Information systems greatly increase the opportunities that are available. In order to have good information system, attention has to be given to data gathering, data processing and information dissemination. The entire process ends up in a continuous cycle in any environment. The fundamentals of information networking are the notions of information processing, pooling, sharing, transfer and dissemination, as well as cooperation, standardization and coordination among network nodes. In view that data must be available before it can be used (or processed), transferred or exchange among network nodes. In light of the above in planning, attention were focused on the following data processing activities.

a) Data collection
b) Data entry
c) Data validation
d) Data assembly or aggregation
e) Data storage
f) Data analysis
g) Data transfer
h) Information dissemination
i) Information use
j) System management and coordination

For effective and consistent transfers and management of information within the organization, a standard networks that meets the underlisted requirements must be put in place. Convergence, deterministic paths, deterministic failover, scalable in size and throughput, centralized storage, 20/80 rule, multiprotocol support and multicast support.

With this, data and information relevant to the operation of the organization or establishment will be properly managed. Let's look at each of the requirements listed above individually.

Convergence
Convergence is the act of layer 2 switches and layer 3 switches adapting to network changes by using mechanisms in the protocols of both layers. The change in the network could be a broken link, a failed router or failed bridge. Regardless, if the network change happens intentionally or unexpectedly, the network must have intrinsic capabilities to adapt to the change quickly. This capability gives the network scalability as well as minimal downtime during disruptions.

Deterministic paths
The largest component of guaranteeing consistency of information flow is a logical topology that forces traffic to flow over a set of links in a predictable way. Deterministic paths results in consistent network performance and help to minimize troubleshooting efforts.

Scalable size and throughput
Networks often simultaneously grow in number of users and individual users demand as the organization expands. This means that the network design must handle an increased number of connections and more bandwidth over the networks internal links of the organization.

Centralized storage
The centralized approach to files and application management within an organization requires that all users have adequate access to the resources, instead of a user accessing a mainframe from a remote terminal, a user now access a server or a cluster of servers from his desktop.

20/80 rule
In the past, it was assumed that 80 percent at traffic originated on a network remained on the network. This means that bandwidth within a network or workgroup LAN is large and the bandwidth to connect with other networks or workgroups could be small. But with the flexibility of modern organization networks and centralized storage, this rule has completely reversed.

Multiprotocol support
The organization network must support other legacy protocols.

Multicast support
Multicasting is a mechanism by which a source sends traffic destined for a group of hosts. This concept of one – some is greatly reducing the occurrence of unnecessary traffic on the organization network and increase the reliability and response of new multimedia teleconferencing applications.

LITERATURE REVIEW

The early 1980s saw tremendous expansion in the area of network deployment. As companies realized the cost benefits and productivity gains created by network technology, they began to add networks and expand existing networks almost as rapidly as new network technologies and products were introduced. By the mid-1980s, certain companies were experiencing growing pains from deploying many different (and sometimes incompatible) network technologies. The problems associated with network expansion affect both day-to-day network operation management and strategic network growth planning. Each new network technology requires its own set of experts. In the early 1980s, the staffing requirements alone for managing large, heterogeneous networks created a crisis for many organizations. An urgent need arose for automated network management (including what is typically called network capacity planning) integrated across diverse environments.

NETWORK MANAGEMENT

Network management becomes more essential as networks increase in size with organisation. The recommended network management solution must help manage this growth. Beyond monitoring current network behaviour and configuration, network management tools must assist in identifying potential problem areas or elements that might limit future growth.

Network Management Architecture

Most network management architectures use the same basic structure and set of relationships. End stations (managed devices) such as computer systems and other network devices, run software that enables them to send alerts when they recognize problems (for example, when one or more user-determined thresholds are exceeded). Upon receiving these alerts, management entities are programmed to react by executing actions such as operator notification, event logging, system shutdown, and automatic attempts at system repair. Management entities also can poll end stations to check the values of certain variables. Polling can be automatic or user-initiated, but agents in the managed devices respond to all polls. Agents are software modules that first compile information about the managed devices in which they reside, then store this information in a management database, and finally provide it (proactively or reactively) to management entities within network management systems (NMSs)via a network management protocol. Well-known network management protocols include the Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP). Management proxies are entities that provide management information on behalf

of other entities. Figure1 depicts a typical network management architecture.

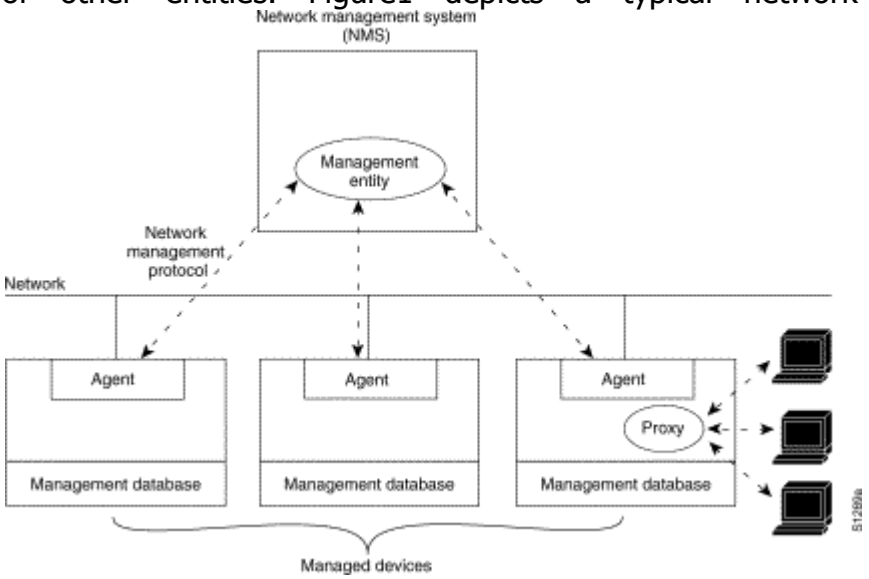

Figure 1: A typical network management architecture maintains many relationships.

ISO Network Management Model

The ISO has contributed a great deal to network standardization. Their network management model is the primary means for understanding the major functions of network management systems. This model consists of five conceptual areas:

- Performance management
- Configuration management
- Accounting management
- Fault management
- Security management

Performance Management

The goal of performance management is to measure and make available various aspects of network performance so that internetwork performance can be maintained at an acceptable level within the organization. Examples of performance variables that might be provided include network throughput, user response times, and line utilization.

Performance management involves three main steps. First, performance data is gathered on variables of interest to network administrators. Second, the data is analyzed to determine normal (baseline) levels. Finally, appropriate performance thresholds are determined for each important variable so that exceeding these thresholds indicates a network problem worthy of attention. Management entities continually monitor performance variables. When a performance threshold is exceeded, an alert is generated and sent to the network management system. Each of the steps just described are part of the process to set up a reactive system. When performance becomes unacceptable because of an exceeded user-defined threshold, the system reacts by sending a message. Performance management also permits proactive methods.

Configuration Management

The goal of configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and

software elements can be tracked and managed.Each network device has a variety of version information associated with it. Configuration management subsystems store this information in a database for easy access. When a problem occurs, this database can be searched for clues that may help solve the problem.

Accounting Management

The goal of accounting management is to measure network-utilization parameters so that individual or group uses on the network can be regulated appropriately. Such regulation minimizes network problems (because network resources can be apportioned based on resource capacities) and maximizes the fairness of network access across all users.

As with performance management, the first step toward appropriate accounting management is to measure utilization of all important network resources. Analysis of the results provides insight into current usage patterns, and usage quotas can be set at this point. Some correction, of course, will be required to reach optimal access practices. From this point, ongoing measurement of resource use can yield billing information, as well as information used to assess continued fair and optimal resource utilization.

Fault Management

The goal of fault management is to detect, log, notify users of, and (to the extent possible) automatically fix network problems to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements. Fault management involves first determining symptoms and isolating the problem. Then the problem is fixed, and the solution is tested on all important subsystems. Finally, the detection and resolution of the problem is recorded.

Security Management

The goal of security management is to control access to network resources according to local guidelines so that the network cannot be sabotaged (intentionally or unintentionally) and sensitive information cannot be accessed by those without appropriate authorization. A security management subsystem, for example, can monitor users logging on to a network resource, refusing access to those who enter inappropriate access codes.

Security management subsystems work by partitioning network resources into authorized and unauthorized areas. Security management subsystems perform several functions. They identify sensitive network resources (including systems, files, and other entities) and determine mappings between sensitive network resources and user sets. They also monitor access points to sensitive network resources and log inappropriate access to sensitive network resources.

Simple Network Management Protocol

The SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

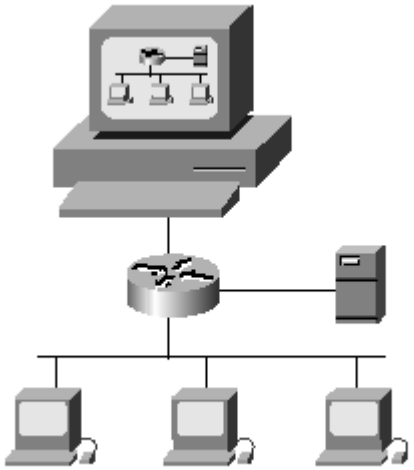

Figure 2SNMP Facilitates the Exchange of Network Information Between Devices

An SNMP managed network consists of three key components: managed devices, agents, and NMSs. A managed device is a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers, access servers, switches, bridges, hubs, computer hosts, and printers. An agent is an NMS software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network. Figure 3 illustrates the relationship between these three components.

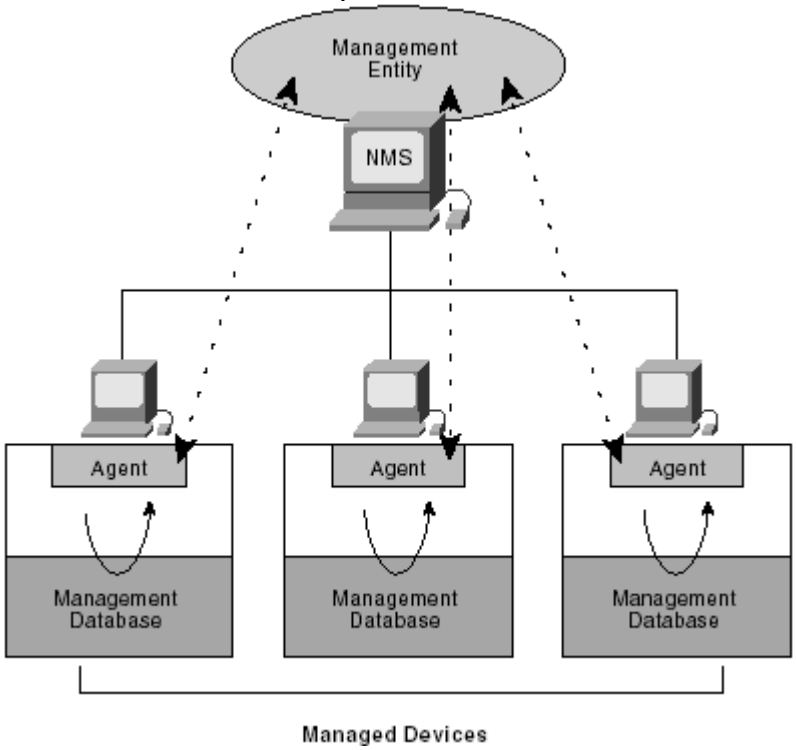

Figure 3:An SNMP Managed Network Consists of Managed Devices, Agents, and NMSs

SNMP Basic Commands

Managed devices are monitored and controlled using four basic SNMP commands: read, write, trap, and traversal operations. The read command is used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices. The write command is used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices. The trap command is used by managed devices to asynchronously report events to the NMS. When certain types of events occur, a managed device sends a trap to the NMS. Traversal operations are used by the NMS to determine which variables a managed device supports and to sequentially gather information in variable tables, such as a routing table.

Management Information Base

A Management Information Base (MIB) is a collection of information that is organized hierarchically. MIBs are accessed using a network-management protocol such as SNMP. They comprised of managed objects and are identified by object identifiers. A managed object (sometimes called an MIB object,) is one of any number of specific characteristics of a managed device. Managed objects comprised of one or more object instances, which are essentially variables. Two types of managed objects exist: scalar and tabular. Scalar objects define a single object instance. Tabular objects define multiple related object instances that are grouped together in MIB tables. An object identifier (or object ID) uniquely identifies a managed object in the MIB hierarchy. The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. Figure 6 illustrates the MIB tree. The top-level MIB object IDs belong to different standards organizations, while lower-level object IDs are allocated by associated organizations. Vendors define private branches that include managed objects for their own products. MIBs that have not been standardized typically are positioned in the experimental branch. The managed object at Input can be uniquely identified either by the object name.

SNMP and Data Representation

SNMP must account for and adjust to incompatibilities between managed devices. Different computers use different data-representation techniques, which can compromise the ability of SNMP to exchange information between managed devices. SNMP uses a subset of Abstract Syntax Notation One (ASN.1) to accommodate communication between diverse systems.

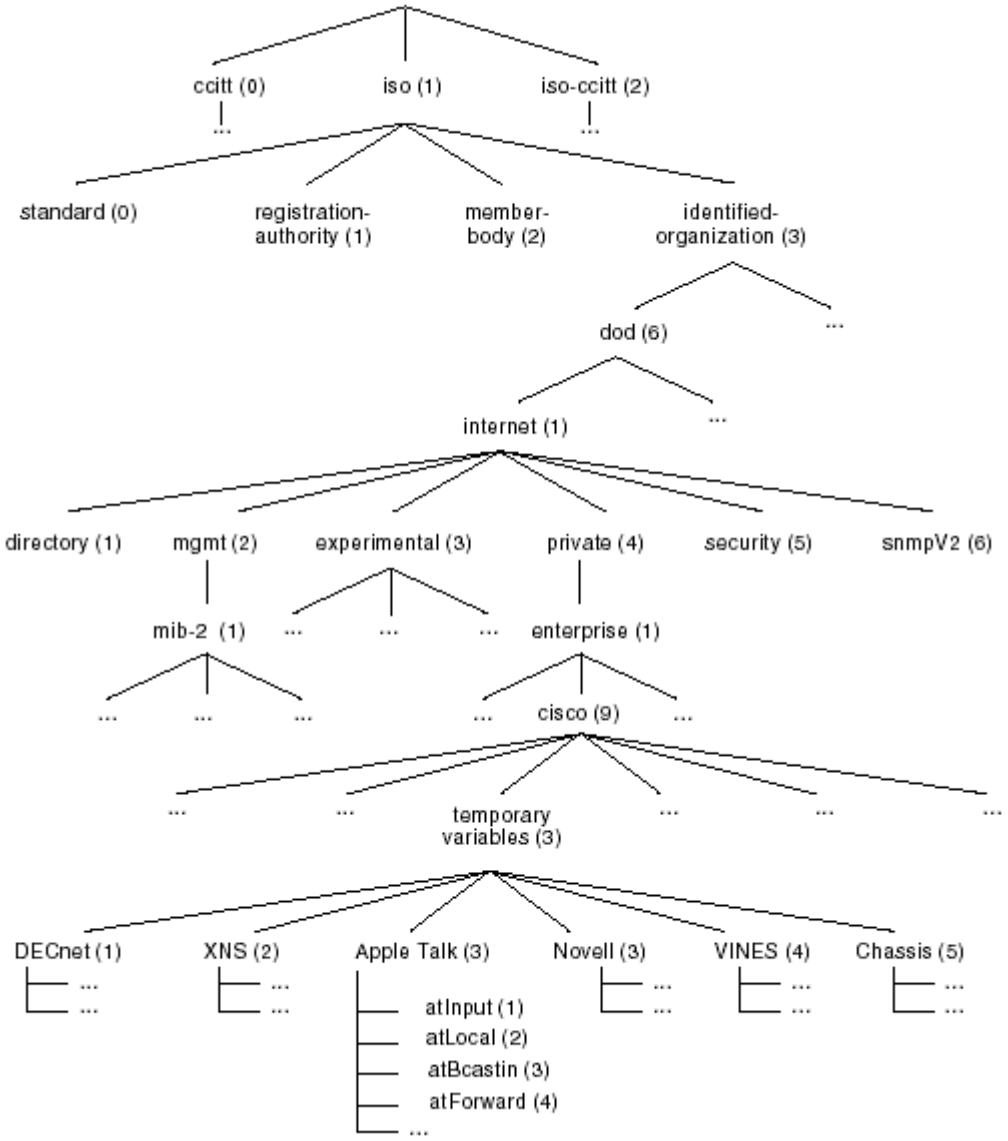

Figure 4:The MIB Tree Illustrates the Various Hierarchies Assigned by Different Organizations

SNMP Management

SNMP is a distributed-management protocol. A system can operate exclusively as either an NMS or an agent, or it can perform the functions of both. When a system operates as both an NMS and an agent, another NMS might require that the system query managed devices and provide a summary of the information learned, or that it report locally stored management information.

SNMP Security

SNMP lacks any authentication capabilities, which results in vulnerability to a variety of security threats. These include masquerading, modification of information, message sequence and timing modifications, and disclosure. Masquerading consists of an unauthorized entity attempting to perform management operations by assuming the identity of an authorized management entity. Modification of information involves an unauthorized entity attempting to alter a message generated by an authorized entity so

that the message results in unauthorized accounting management or configuration management operations. Message sequence and timing modifications occur when an unauthorized entity reorders, delays, or copies and later replays a message generated by an authorized entity. Disclosure results when an unauthorized entity extracts values stored in managed objects, or learns of events by monitoring exchanges between managers and agents. Because SNMP does not implement authentication, many vendors do not implement Set operations, thereby reducing SNMP to a monitoring facility.

Design Methodology

A proactive approach toward network management is essential for an effective design. This means monitoring the network before problems occur. Network statistics must be gathered and documented as a baseline of the current status of the network. As part of the baseline, segment utilization must be included, router CPU utilization, and response time tests. Then we can define acceptable service goals for the network.

A proactive network management strategies is developed using the following steps:

- Determine network service goals.
- Define metrics for measuring whether the goals have been met.
- Define processes for data collection and reporting.
- Implement network management systems.
- Collect performance data and record trends.
- Analyze results and write reports.
- Locate network irregularities and bottlenecks.
- Plan and implement network improvements.
- Review and adjust metrics and processes, if necessary.
- Document changes.

The figure below shows the block diagram of how the design of the system is interrelated.

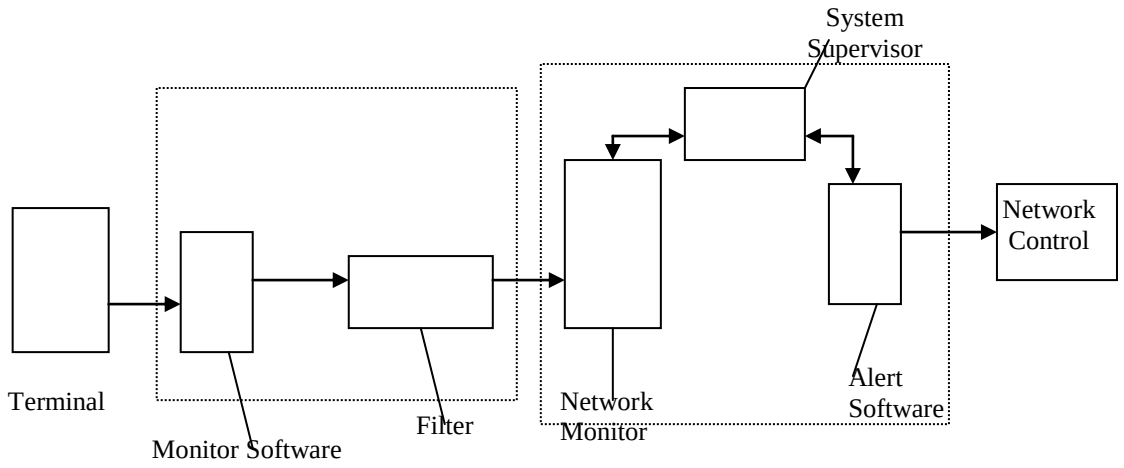

Figure 5: Strategic information System model

Figure 5 shows the model for the implementation of strategic management information system.

- The **terminal** is the device used for obtaining or entering data on a network that.

- **Monitor software** is a software that tracks all or selected part of network traffic. It examines packets and gathers information about packet types, errors, and packets traffic to and from each terminal.
- **Filter** is a device that route packets between internal and external hosts, but does it selectively. It allow or block certain types of packets in a way that reflects a site's own security policy
- **Alert Software** informs the administrator whenever there is any problem on the network. It also shows where the problem is located.
- **Network Controller:** System **Management** Server provides Help Desk and diagnostics utilities which allow control and monitoring of remote clients directly. The diagnostics utilities allow the administrator to view the client's current configuration. The Help Desk utilities provide direct access to a remote client.

Network management includes many responsibilities, one of the most important being network performance management. The administrator monitors network performance for bottlenecks and to see how performance can be improved. Monitoring performance also aids in planning and forecasting future network need..

CONCLUSION

Information technology combines technology with the creation and use of information systems. A management information system (MIS) is a computer system or group of systems which collects and presents management information for a business organisation thus servicing the organisation's need for co-ordination and control at strategic, tactical and operational levels. A MIS is different from a transaction processing system which processes routine operational data - orders, payslips, invoices, stock issues. A transaction processing system often produces management information as scheduled reports but these are scheduled - derived from operational transactional processing. A MIS in contrast supports unscheduled, on-demand reporting giving the user-manager (decision-maker) freer access to stored information without requiring the direct intervention of DP specialists. In making strategic goals operational it is vital that progress can be monitored via the management information system otherwise progress may be invisible. At the strategic management level we are interested in summary information to define current status and measure how well we are doing. This is long-term stuff usually relating to a rolling corporate plan which can be reviewed annually. We implemented tactical measures to secure strategic objectives. This means setting up allocating staff, devising reporting structures, authorising resources (budget) and emphasising certain approaches over others. We want to know in the medium term if the "tactical" are working so that fine adjustments, on the basis of variances over plan, can be made between strategic reviews. The management information system should service such tactical adjustment. All these activities will only be possible if the network is design such that it is up and running all the time. This will enhance the quality of service and increases productivity of the organization network system.

REFERENCES

Annabel Z. Dodd. "The Essential Guide to Telecommunications" 2nd Ed. Prentice Hall.

David Best &Touche Ross (1993):"Information Management and Organisational change". IEE Computing & Control journal, April Pp 50-51.

EMMAN NICHOLSON: "Protection of information in IT era", IEE Computing and Control Engineering Journal, May 1992. Pp 129-131.

ODUSOTE I. A. (1995): "Internet problems and Prospect", A paper presented at the 1995 Annual conference / AGM of the Association of Professional Women Engineers on 25th October, 1995 at the MUSON Centre, Onikan, Lagos.

Networking with Microsoft TCP/IP. New Rider

Networking Essentials – Hans-on Self Training for Supporting Local and Wide Area Networks. Microsoft Press.

www.cisco.com/warp/public/cc/cisco/mkt/enm/config/index.shtml

www.cisco.com/univercd/cc/td/doc/clckstrt/cfgmkr/cmakecd1.htm.