بسم الله الرحمن الرحيم

Sudan University of Science & Technology

College of Post Graduate Studies

MSc Program in Computer Science

Towards optimum security operation centre with fair bandwidth allocation

A Research Submitted in Partial fulfilment for the Requirements of M.SC in computer science

(Information security)

Prepared by: **Hind Abdullah Osman**

Supervised by: **Dr.Abuagla Babiker Mohamed**

July 2015

بسم الله الرحمن الرحيم

قال تعالى

قُلْ هُوَ اللَّهُ أَحَدٌ (١) اللَّهُ الصَّمَدُ (٢) لَمْ يَلِدْ وَلَمْ يُولَدْ (٣) وَلَمْ يَكُنْ لَهُ كُفُوًا أَحَدٌ (٤)

"صدق الله العظيم"

Acknowledgement

And also thank all those who helped to complete this search and gave us a helping us to extend a helping hand and provided us with the necessary for the completion of this research information and singled out: administrators Dr.Abuagla Babiker Mohamed and thank them all.

Abstract

Confidential and reliable information delivery is considered as one of the essential requirements that must be available in every area of life. The effective design as well as the implementation of efficient tools for bandwidth monitoring and control helps a lot in achieving the above mention availability requirements. The focus of this research mainly into two parts. The first part is to do an extensive survey on the effective design approaches for Security operation centre (SOC) in addition to investigating the suitable alternatives for different enterprise networks according to the nature of the owner (i.e. SOC for Bank is totally different for SOC for university campus). This part deals with knowledge of the basic steps that must be followed to design secret operations centres via personal interviews (questionnaire interview) which has been collected from a number of institutions that have computer networks. The second part concentrates on bandwidth management specifically the usage control so as to target the security threats that attacks the internet link which directly affect the availability specifically and deteriorate the performance as general. This part aims to maintain fair allocation of bandwidth not only among users only but also among the branches of the enterprise network. Survey results shows the optimal design of security operation centre according to the organizational needs, as well as set of recommendations for securing the data centres in more details according the experience transfer via the interviews. Moreover the results of the implementation of the fair allocation of bandwidth, proofs the effective utilization of bandwidth, fair allocation, and prevention from

the attackers that aim to overwhelm the internet link with huge traffic that may leads to performance degradation.

المستخلص

تعتبر سرية المعلومات والموثوقية في توصيلها واحدة من المتطلبات الأساسية التي يجب أن تتوفر في كل مجال من مجالات الحياة. التصميم الفعال وكذلك كيفية تنفيذ أدوات فعالة لرصد ومراقبة سعة الانترنت يساعد كثيرا في تحقيق متطلبات السرية. وينقسم هذا البحث أساسا إلى قسمين. القسم الأول هو ان نقوم بعمل استبيان من خلاله تم التوصل الي معلومات لكيفية تصميم مركز سرية عمليات بصورة فعالة لمختلف المؤسسات علي سبيل المثال جامعة او بنك او اي نوع اخر من المؤسسات. ، يتناول هذا القسم معرفة الخطوات الأساسية التي يجب اتباعها لتصميم مراكز العمليات السرية عن طريق المقابلات الشخصية (مقابلة الاستبيان) التي تم جمعها من عدد من المؤسسات التي لديها شبكات الكمبيوتر. ويتناول القسم الثاني القدرة على إدارة السعة الكلية للشبكة على وجه التحديد و مراقبة الاستخدام وذلك لاستهداف التهديدات الأمنية التي تهاجم وصلة الإنترنت لتؤثر بشكل مباشر على الاتاحية لسعة الشبكة تحديدا وتدهور الأداء على النحو العام. ويهدف هذا القسم ايضا إلى توزيع عادل للحفاظ على السعة االمتاحة ليس فقط بين المستخدمين فحسب، بل أيضا بين فروع شبكة المؤسسة. نتائج الاستبيان تظهر التصميم الأمثل لمركز العمليات الأمنية وفقا لاحتياجات المؤسسة ، فضلا عن مجموعة من التوصيات لتأمين مراكز البيانات. وعلاوة على ذلك نتائج تنفيذ التوزيع العادل لسعة الانترنت ، تبرهن الاستخدام الفعال لسعة الانترنت الكلية، وتوزيع عادل، والوقاية من المهاجمين التي تهدف ألي الاطغاء علي وصلة الانترنت مع الحركة الضخمة التي قد تؤدي إلي تدهور الأداء.

Contents

List of table

List of figures

List of Term

Term	Term Description
SOC	SECURITY OPERATIONS CENTRES
AIMD	ADDITIVE INCREASE AND MULTIPLICATIVE DECREASE
BEB	BINARY EXPONENTIAL BACK
ECN	EXPLICIT CONGESTION NOTIICATION
ICT	INFORMATION COMMUNICATION TECHNOLOGY
ICE	INFORMATION COMMUNICATION
ICC	INFORMATION COMMUNICATION CENTRES
MR	MULTI ROUTER TRAFFIC GRAPHER
NAC	NETWORK ACCESS CONTROL
P2P	PEER TO PEER
QOS	QUALITY OF SERVICE
IPFM	IP FLOW METER
TC COMMAND	TRAFFIC CONTROL
C SHARP	PROGRAMMING LANGUAGE
LAN	LOCAL AREA NETWORK
HTTP	HYPER TEXT TRANSFER PROTOCOL
NETFLOW	A NETWORK PROTOCOL DEVELOPED BY CISCO FOR THE COLLECTION AND MONITORING OF NETWORK TRAFFIC FLOW
IFTOP	A COMMAND-LINE SYSTEM MONITOR TOOL
PFTOP	IS A SMALL, CURSES-BASED UTILITY FOR REAL-TIME

	DISPLAY OF ACTIVE STATES AND RULE STATISTICS FOR THE PACKET FILTER FOR OPENBSD
PINGSTING	IS AN APPLICATION THAT MONITORS NETWORKS FOR ICMP ECHO
TCPSPY	IS AN ADMINISTRATORS' TOOL THAT LOGS INFORMATION ABOUT SELECTED INCOMING AND OUTGOING TCP/IP CONNECTIONS
NOMAD	NOTTINGHAM ONLINE MAPS AND DATA AND ITS TOOL FOR MONITORING NETWORKS AND ANALYSIS
FLOWSCAN	A NETWORK TRAFFIC FLOW REPORTING AND VISUALIZATION TOOL
MRTG	MULTI ROUTER TRAFFIC GRAPIER AND ITS TOOL FOR MONITORING NETWORKS AND ANALYSIS
NTOP	IT IS A TOOL THAT SHOWS THE NETWORK USAGE, IS BASED ON CAPTURES AND IT HAS BEEN WRITTEN IN A PORTABLE WAY IN ORDER TO VIRTUALLY RUN ON EVERY UNIX PLATFORM.
WIRESHARK	IS AN OPEN SOURCE TOOL FOR PROFILING NETWORK TRAFFIC AND ANALYSING PACKETS
ANGRY IP	ANGRY IP IS A VERY LIGHTWEIGHT PROGRAM THAT ALLOWS YOU TO QUICKLY SCAN A RANGE OF IP ADDRESSES
NMAP	NETWORKED MESSAGING APPLICATION PROTOCOL AND ITS TOOL FOR MONITORING NETWORKS AND ANALYSIS

PRTG	PASSEL ROUTER TRAFFIC GRAPHER AND ITS TOOL FOR MONITORING NETWORKS AND ANALYSIS
IPFIX	INTERNET PROTOCOL FLOW INFORMATION EXPORT
PSAMP	PUGET SOUND ASSESSMENT AND MONITORING PROGRAM
EPON	ETHERNET PASSIVE OPTICAL NETWORKS
DBA	DYNAMIC BANDWIDTH ALLOCATION
P-EPON	PENETRATED-EPON
OPNET	OPTIMIZED NETWORK ENGINEERING TOOL
OLSR	OPTIMIZED LINK STATE ROUTING
CISCO	COMPUTER INFORMATION SYSTEM COMPANY
IP VOICE	VOICE APPLICATIONS PROVIDED OVER THE INTERNET
VPN	VIRTUAL PRIVATE NETWORK
MPLS	MULTI-PROTOCOL LABEL SWITCHING
IT	INFORMATION TECHNOLOGY
SAN	STORAGE AREA NETWORK
VM-LEVEL	VIRTUAL MACHINE LEVEL
MYSQL	OPEN SOURCE DATABASE SOFTWARE
AIMD	ADDITIVE INCREASE AND MULTIPLICATIVE DECREASE
ECN	EXPLICIT CONGESTION NOTIFICATION.
OMNET++	EXTENSIBLE, MODULAR, COMPONENT-BASED C++
TCP	TRANSMISSION CONTROL PROTOCOL
UCON	USAGE CONTROL MODEL
IPTRAF	IS A CONSOLE-BASED NETWORK MONITORING PROGRAM FOR LINUX THAT DISPLAYS INFORMATION ABOUT IP TRAFFIC

SFLOW	A MULTI-VENDOR SAMPLING TECHNOLOGY EMBEDDED WITHIN SWITCHES AND ROUTERS. IT PROVIDES THE ABILITY TO CONTINUOUSLY MONITOR APPLICATION
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
SNMP	SIMPLE NETWORK MANAGEMENT PROTOCOL
WINPCAP	WINDOWS PACKET CAPTURE PACKAGE

Table of Hypothesis

Hypothesis	Description
First Hypothesis	Most of organizations have not a secret operation centres
Second Hypothesis	Most of organizations have computer centre (cc) or Information Communication Technology Centre (ICT)
Third Hypothesis	Most of organizations have not using any mechanisms or policies or operation and have not control techniques?
Fourth Hypothesis	Most of organizations suffer from the problem of hacking
Fifth Hypothesis	Most of organizations have use firewall to protection their centres and using anti viruses??
Six Hypothesis	Most of organizations existence Trojan Hours viruses and have most organizations using Kaspersky the main anti-virus
Seventh Hypothesis	Do Most of organizations have a security log file and have method to analyse log file?

Chapter 1: Introduction

Chapter 1

Introduction

1.1Background

Security is becoming more and more established in the corporate structure it is no longer acceptable for security to be a resultant function of an IT department. To address this challenge, organizations are investing in the development of Security Operations Centres (SOCs) to present increased security and rapid response to events throughout their networks. Building an SOC can be task although the improved points of SOC use are very much network-specific, there are a quantity of major gears that every organization must include people, process, and technology [1].

The purpose of security operation centre is responsible for monitoring, detecting, and separating incidents and the group of the organization's security produce, network devices, end-user devices, and systems network monitoring is the collection of helpful information from a variety of parts f the network so that the network can be manage and embarrassed using the collected information[2].

Network monitoring is deal with collection function of network organization. Network monitoring applications are formed to collect data for network management application[3].

Most of the network devices are placed in far-off location. These devices do not regularly have openly connected terminals so that network management application cannot monitor their statuses easily. Thus, network monitoring

techniques are developed to allow network management applications to test the states of their network devices. As more and more network devices are used to build better-quality networks, network monitoring techniques are expanded to monitoring networks as a whole Bandwidth Monitor monitors bandwidth usage during PC it's installed on[4].

The software display real-time download and upload speeds in graphical and, wood bandwidth usages, and present day by day, weekly and monthly bandwidth usage reports. Bandwidth Monitor monitors all network links on a computer, such as LAN network relationship, Internet network connection, and VPN connection[5].

Bandwidth control from manage links enable our business to benefit by getting [6]:

- Better information - we can improved understand your bandwidth usage with full bandwidth management tools.
- Faster application speed - bandwidth management can allocate bandwidth to key critical applications enabling better performance**.**
- Reduce unwanted traffic - we can isolate P2P users or bandwidth hogs on your network so that you control the quality of performance seen across your data connections**.**
- More bandwidth - we can achieve up to 35 times the throughput with bandwidth management services.

Benefits of a Bandwidth Monitor Understanding bandwidth and resource consumption is the key to better network management:[6]

- Avoid bandwidth and server performance bottlenecks

- Find out what applications or what servers are using up your bandwidth
- Deliver better quality of service to your users by being proactive
- Reduce costs by buying bandwidth and hardware according to actual load.

The flowing figure [1.1] show Amount of bandwidth used in week one of Trinity term 2005 to 2010

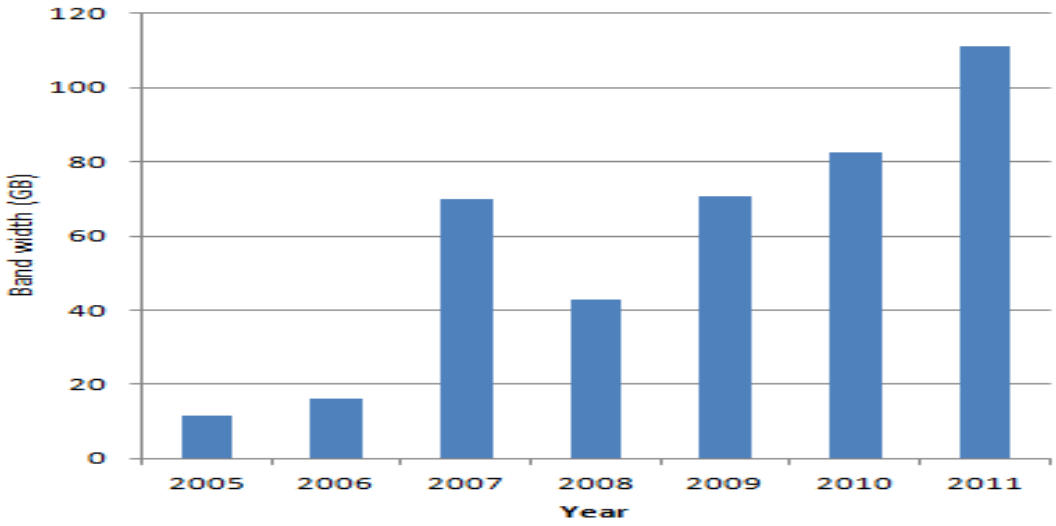


Figure 1.1: Amount of bandwidth used in week one of Trinity term 2005 to 2011

1.1.1 The basic goals for network monitoring

1.1.1.1 Performance monitoring

There are three important issues in performance monitoring. Performance monitoring information is usually used to plan future network expansion and place recent network usage problems. And the time frame of performance monitoring must be long enough to start a network behaviour model. And choose what to determine is important. There are too many measurable things in a network. But the list of items to be measured should be meaningful and cost effective.

1.1.1.2 Fault monitoring

Fault monitoring deals with measuring the fault in the network. Fault monitoring deals with different layers of the network. When a problem happen, it is key in to know which layer is have problem. And fault monitoring requires establishing a usual attribute of the network in an extended period of time. The focus here is divided into two regarding the fault, firstly is by designing a reliable SOC to avoid faults, secondly, by maintain internet traffic control to avoid congestion which is considered indirectly logical fault in the link

1.1.1.3 Account monitoring

Account monitoring deals with how users use the network. The network keeps a record of what devices of the network are used by users and how often they are used. This type of information is used for bill user for network usage, and for predicts expectations network usage.

1.2 Problem Statement

The well design of security operation centres is challenging task due to the dynamic nature of attackers as well as the different security levels which are required by network owners according to their business sensitivity .Before the construction of the security operations centres, organizations need to take some time to plan. Often this plan represents core stage, which focuses not only on the process of surveys, following standards, but also on experience transfer through interviews and meetings which related to experts .Spending some time at this stage of planning will benefit in the long term.

It is a fact that the users always require a very high availability, quality of service, very high speed internet access to satisfy their application's needs. On the other hand in most of the cases the Internet link has a limited bandwidth due to the budget constraints.

To maintain availability as one of the essential security requirements, the usage of the users may be classified into normal and abnormal usage. Leaving the internet link without control and due to the existence of heavy usage for either the user or the overall accumulation of traffic form the subnet will lead to lack of availability as well as slowness of the internet for normal users.

1.3 Research Goal

The objectives of this research are as follows:

- To propose an effective design of Security Operation Centre (SOC) which balance between cost and business security level?

- To perform continuous availability monitor and control according to the usage of user/subnet. So as to enhance the availability as one of the security requirements.
- Developing an algorithm that maintains the fair allocation of bandwidth. And control usage user/subnet for the purpose of enhanced the link utilization with useful traffic.

The overall outcomes is to come up with optimum design for the security operation centre (SOC) as well as to reduce the congestion while at the same time maximize the link utilization, further more it aims also to reduce the cost of upgrading the link.

1.4 Importance of Research

Security operation centres is very import ant because it enables the monitoring of all data in addition to filtering the find and control, and log data to see all dangers threats to be exposed.

Also the importance of this is to distribute the Internet among all colleges in the university building fairly and useful applications

The important of management the bandwidths very use full to availability to use the internet link and enhance the network performance. Network monitoring is a difficult and demanding task that is a vital part of a Network Administrators job. Network Administrators are constantly striving to maintain smooth operation of their networks. If a network were to be down even for a little period of time output within a company would decline, and in the case of public service department the ability to provide essential services would be compromised[7]. In order to be

proactive rather than reactive, administrators need to monitor traffic group and performance throughout the network and verify that security do not occur within the network.

1.5 Research Methodology

The methodology of this research begins by making Interview questionnaire to some computer organization authorities. Then the collected data has been analyzed to achieve the goal of optimum design of (SOC). Moreover the second part is to obtain the availability as one of the essential security requirements.

1.6 Thesis Layout

This thesis consists of five chapters, followed by list references and appendixes.

Chapter 2: explains the concepts of security operation centres and explains the concepts of traffic monitoring, traffic control, bandwidth management, traffic congestion and …etc., and finally the previous studies, moreover, it explores the detail of every study and highlights the advantages and disadvantages.

Chapter 3: Contains the security operation centres research methodology and how to write algorithms.

Chapter 4: includes data collection, analysis, results, discussion as well as the interpretation.

Chapter 5: presents the important findings, recommendations and suggestion based on the study.

Chapter 2: Background Literature Review

Chapter 2

Background and Literature Review

2.1 Introduction

This chapter has been divided into three Sections. The first Section discusses the background about security operation centres. The second Section discusses the general introduction to the network monitoring, analysis, control and Tools using traffic monitoring and analysis. The third section is previous study.

2.1.1 Background of security operation centres

In this section define the basic concepts of the security operation centres objectives, and responsibilities. Defining these core items will make sure its endurance and help avoid conflict with other company wide functions. To begin, create a SOC that formally documents

Each of the following items

- Mission
- Charter
- Objectives
- Responsibilities
- Operational Hours

2.1.2 Determine the Processes

The number of processes and procedures for a SOC is firm by its scope, how many armies are offered, the number of clients supported, and the number of different

technologies in use. An established global SOC environment may have tens or even hundreds of procedures. At a least, the basic procedures that are necessary for maintaining the SOC are:

- Monitoring procedure.
- Notification procedure (email, mobile, home, chat, etc.).
- Notification and escalation processes.
- Transition of daily SOC services.
- Shift logging procedures.
- Incident logging procedures.
- Compliance monitoring procedure.
- Report development procedure.
- Dashboard creation procedure.
- Incident investigation procedures (malware, etc.).

2.1.3 SOC tools and technology needs, including

- Managing Asset Information
- Finding Vulnerabilities
- Detecting Threats
- Monitoring for Suspicious Behaviour
- Utilizing SIEM Event Correlation
- Saving Time in Deployment

2.2 Background of traffic control and network monitoring

In this section define the basic concepts of traffic control, bandwidth management, and quality of Service. These three concepts are related but distinct.

2.2.1 Traffic

The project aims to build a security operation centres in this system must be build system for monitoring, analysing, and managing or controlling the network traffic to avoid the congestion and give the fairness by another meaning this project proposes a simple load balancing approach to optimize use of LAN links in the simulation and build system to collect event in the servers and analyses them and the expected outcome from the proposed system is to have the following characteristics:

- Provide higher link utilization with useful applications.
- Fairness, when offered traffic load must be cut back in this adaptive approach, it is important to do so fairly.

Robustness, when used to describe software or computer systems, robust can describe one or more of several qualities a system that does not break down easily or is not wholly affected by a single application failure, a system that either recovers quickly from or holds up well under exceptional circumstances, a system that is not wholly affected by a bug in one aspect of it, a system that comes with a wide range of capabilities.

- Simplicity.
- Low cost.
- Smart and adaptive control.

The key components of this scheme are: monitoring algorithm, analysing

Algorithm, decision function, and increase/decrease algorithms, as show below on figure [2.1]:

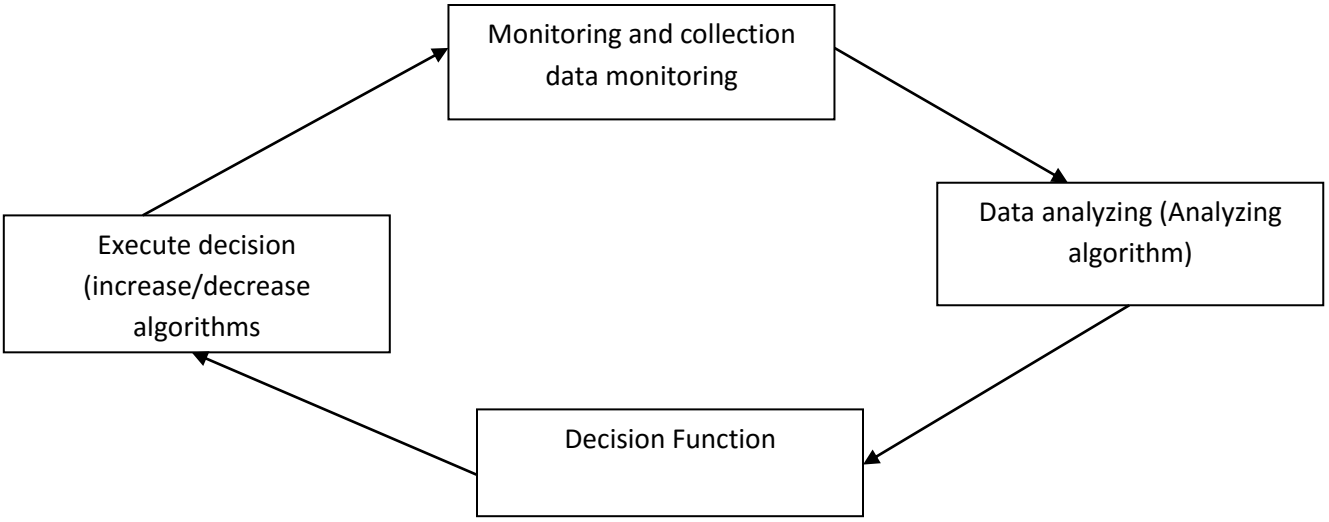


Figure 2.1: component of the soc

2.3 Historical background of Internet traffic control

In this section define the basic concepts of traffic control, bandwidth management, and quality of Service. These three conceptions are related but distinct.

2.3.1 Network Capacity planning

Network planning is determining how much bandwidth the network actually needs.

2.3.2 The Benefits of Capacity Planning

1. Budgeting

Capacity planning outlines the personnel and equipment your small business will need in order to maintain current operations and reach goals.

2. Scalability

Scalability is the process of planning for expansion.

3. Dynamic Change

The process of capacity planning collects a significant amount of data on how your company currently operates. One of the ways in which you can stay competitive in the marketplace is to use that capacity data to make changes to your organization to keep up with your competition. For example, if your prime competitor expanded its customer service staff by 20 present, then your capacity planning information can let you know exactly what you would need it terms of money, facilities and personnel to keep up with the competition's level of support.

The following figure [2.2] shows Capacity Planning Methodology

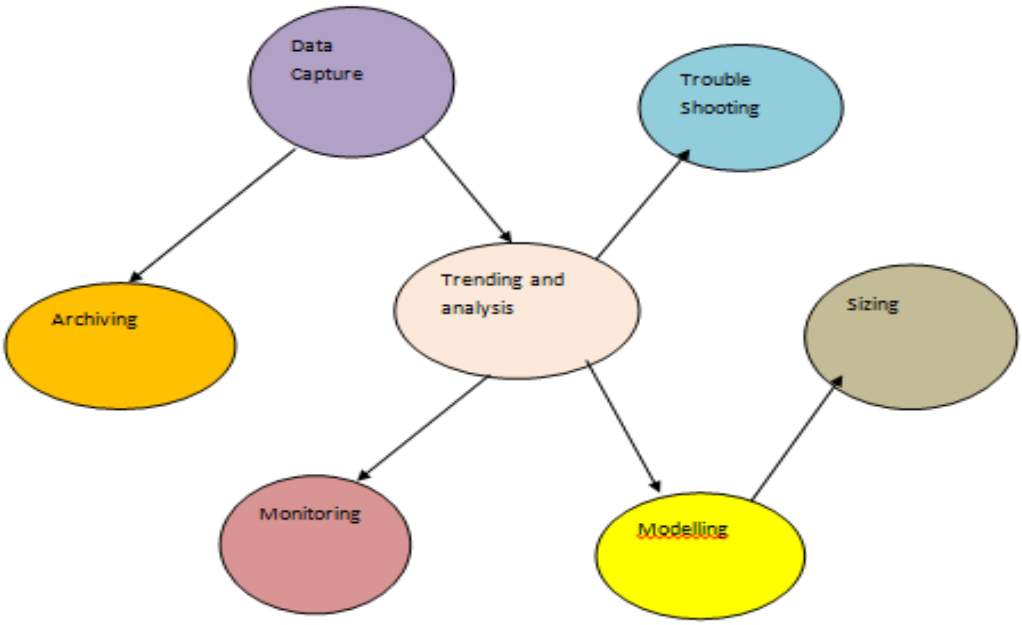


Figure 2 .2: Capacity Planning Methodology

2.3.3 Traffic Congestion

Congestion is said to occur in the network when the resource demands exceed the capacity and packets are lost due to too much queuing in the network. During congestion, the network throughput may drop to zero and the path delay may become very high. A congestion control scheme helps the network to recover from the congestion state[8].

A congestion avoidance scheme allows a network to operate in the region of low delay and high throughput. The problem of congestion control is more difficult to handle in networks with connectionless protocols than in those with connection-oriented protocols. In connection-oriented networks, resources in the network are reserved in advance during connection setup. Thus, one easy way to control congestion is to prevent new connections from starting up if congestion is sends [9, 10].

2.3.4 Traffic Monitoring

The term network monitoring describes a range of techniques by which it is sought to observe and quantify exactly what is happening in the network, both on the microcosmic and macrocosmic time scales. Data gathered using these techniques provides an essential input towards:

• Performance tuning: identifying and reducing bottlenecks, balancing resource use, improving QOS and optimizing global performance.

• Troubleshooting: identifying, diagnosing and rectifying faults.

• Planning: predicting the scale and nature of necessary additional resources.

• Development and design of new technologies: Understanding of current operations and trends motivates and directs the development of new technologies.

• Characterization of activity to provide data for modelling and simulation in design and research.

• Understanding and controlling complexity: to understand the interaction between components of the network and to confirm that functioning, innovation, and new technologies perform as predicted and required. The introduction of persistent HTTP connections, for instance, was found in some cases to reduce overall performance.

• Identification and correction of pathological behaviour.

The mechanisms employed to gather data from the network are classier as passive or active, although both may be used in conjunction [11].

2.3.5 Traffic analysis

Network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network. Traffic monitoring and analysis is essential in order to more effectively troubleshoot and resolve issues when they occur, so as to not bring network services to a stand still for extended periods of time. Numerous tools are available to help administrators with the monitoring and analysis of network traffic[7].

2.3.6 Bandwidth Management

Bandwidth is a term used in much of the telecommunications industry as a measure, usually expressed in bits per second, of the rate at which information moves from one electronic device to another.

Without proactive management of bandwidth, network capacity fills with viruses and inappropriate traffic, problems cannot be diagnosed and the connection becomes ineffective.

Managing bandwidth improves the performance of an internet connection by removing unnecessary traffic: "improving bandwidth management is probably the easiest way for universities to improve the quantity and quality of their bandwidth for educational purposes". Bandwidth is like a pipe, it doesn't matter how big the pipe is, if the traffic in the pipe is not managed it will clog up with unwanted traffic and be hijacked by viruses, spam, peer-to-peer file-sharing traffic and problems on the network will not be accurately diagnosed. Bandwidth management requires three activities: Policy, Monitoring and Implementation. If any one of these is activities is missing then the management of bandwidth is significantly compromised. The activities inform and reinforce each other it is not enough to right-size the bandwidth. In order to properly manage this scarce resource, IT departments need a complementary budget for supporting infrastructure and staff. In particular, adequate budget will be needed to enforce policies and to use technology smartly [12].

2.3.7 Traffic Control

Traffic control is an agreement between a source and a destination to limit the flow of packets without taking into account the load on the network. The purpose of traffic control is to ensure that a packet arriving at a destination will find a buffer there.

Without any control, the source may send packets at a pace too fast for the destination. This may cause buffer overflow at the destination leading to packet losses, retransmissions, and degraded performance. A flow control scheme protects the destination from being flooded by the source [13].

2.3.8 Usage control

The term usage control is a generalization of access control to cover obligations, conditions, continuity (on going controls) and mutability. Traditionally, access control has dealt only with authorization decisions on a subject's access to target resources. Obligations are requirements that have to be fulfilled by the subject for allowing access. Conditions are subject and object-independent environmental requirements that have to be satisfied for access. In today's highly dynamic, distributed environment, obligations and conditions are also crucial decision factors for richer and finer controls on usage of digital resources. Traditional authorization decisions are generally made at the time of request but typically do not recognize ongoing controls for relatively long-lived access or for immediate revocation. Moreover, mutability issues that deal with updates on related subject or object attributes as a consequence of access have not been systematically studied[14].

2.4 Overview of tools network monitoring and Control

2.4.1 Introduction

The network monitoring directory contains software which allows a system administrator to monitor a network for the purposes of security, billing, and analysis (both online and offline).

Network analysis is the process of capturing network traffic and inspecting it closely to deter mine what is occurrence on the network. Network analyser decodes, or dissects the data packets of common protocols and displays the network traffic in human-readable format. Network analysis is also recognized

by several other names: traffic analysis, protocol analysis, packet sniffing, packet analysis, and eavesdropping to name a few.

Network analysis tools enable diagnosis of problems or allow exploration of all hardware on a computer network.

Network traffic control is the process of managing, prioritizing, controlling or reducing the network traffic, particularly Internet bandwidth, e.g. by the network scheduler.

It is used by network administrators, to reduce congestion, latency and packet loss. This is part of bandwidth management. In order to use these tools effectively, it is necessary to measure the network traffic to determine the causes of network congestion and attack those problems specifically.

Network traffic measurement is the process of measuring the amount and type of traffic on a particular network. This is especially important with regard to effective bandwidth management.

2.5Network Traffic Measurement Tools

2.5.1 DNSPerf

DNSPerf measures Authoritative Domain Name services and is designed

Simulate network conditions by self-pacing the query load.

2.5.2ResPerf

It is designed specifically to simulate Caching Domain Name services. To test a caching server, ResPerf systematically Increases the query rate and monitors the response rate.

2.5.3 DHCPerf

DHCP performance testing provides a means of predicting server behaviour under load and verifying server performance. The most important elements in a DHCP performance test tool are:

- Accuracy the tool's results should correlate strongly with the server's "real-world" Performance.
- Reproducibility Successive testing runs with the tool should produce strongly similar results.
- Simplicity Good results should not be dependent upon configuration options, and the tool should be easy to use and understand.

2.5.4 PRTG

PRTG is an indispensable network traffic logger that makes life for network administrators much easier. In addition to measuring network traffic, PRTG also monitors the availability and performance of network devices, checks the quality of VoIP connections, monitors CPU and RAM usage, etc. Each PRTG license includes various remote probes which allow you to monitor multiple locations with just one installation of the monitoring software.

2.5.5 MRTG

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network links. MRTG generates HTML pages containing PNG images which provide a LIVE visual representation of this traffic.

MRTG consists of a Perl script which uses SNMP to read the traffic counters of your routers and a fast C program which logs the traffic data and creates beautiful graphs representing the traffic on the monitored network connection. These graphs

are embedded into web pages which can be viewed from any modern Web-browser.

MRTG is not limited to monitoring traffic, though. It is possible to

Monitor any SNMP variable you choose. You can even use an external program to gather the data which should be monitored via MRTG. People are using MRTG, to monitor things such as System Load, Login Sessions, Modem availability and more. MRTG even allows you to accumulate two or more data sources into a single graph

2.4.6 Network Monitoring and analysing Tools

2.4.6.1 NETFLOW

Net flow is another option for bandwidth usage analysis. Net flow is a standard means of traffic accounting supported by many routers and firewalls. You need a Net flow collector running on a host inside your network to collect the data. Pf Sense can export Net flow data to the collector using the pfflowd package, or soft flowed.

2.4.6.2 SFlow

SFlow is a multi-vendor sampling technology embedded within switches and routers. It provides the ability to continuously monitor application level traffic flows at wire speed on all interfaces simultaneously.

The SFlow Agent is a software process that runs as part of the network management software within a device. It combines interface counters and flow samples into SFlow datagram that are sent across the network to SFlow Collector. Packet sampling is typically performed by the switching routing ASICs, providing

wire-speed performance. The state of the forwarding routing table entries associated with each sampled packet is also recorded.

The SFlow Agent does very little processing. It simply packages data into SFlow Data grams that are immediately sent on the network. Immediate forwarding of data minimizes memory and CPU requirements associated with the SFlow Agent.

2.4.6.3 SARG

SARG is an open source tool that allows you to analyses the squid log files and generates beautiful reports in HTML format with information's about users, IP addresses, top accessed sites, total bandwidth usage, elapsed time, downloads, access denied websites, daily reports, weekly reports and monthly reports.

The SARG is very handy tool to view how much internet bandwidth is utilized by individual machines on the network and can watch on which websites the network's users are accessing.

2.4.6.4 Ping sting

Ping sting is an application that monitors networks for ICMP Echo Requests and attempts to determine what application generated the ICMP packets.

2.4.6.5 Nagios

Nagios is a system and network monitoring application. It watches hosts and services that you specify, alerting you when things go bad and when they get better.

Nagios was originally designed to run under Linux, although it should work under most other uncles as well.

Nagios was designed as a rock solid framework for monitoring, scheduling and alerting. Nagios contains some very powerful features, harnessing them is not only a matter of understanding how Nagios works, but also how the system you're monitoring also works. This is an important realization. Nagios can't automatically teach you about complex systems, but it will be a valuable tool to help you in your journey.

2.4.6.6 Nomad

Nomad is a network mapping program designed to automatically discover a local network, using SNMP to identify network devices and work out how they are physically connected together. The network is then presented as a topology diagram with simple integrated monitoring. Changes in the network are reflected in the diagram which continuously updates, and you can customize your own views of the network map with various views and filters.

2.4.6.7 NTop

Ntop is a tool that shows the network usage, similar to what the popular top UNIX command does. Ntop is based on capture and it has been written in a portable way in order to virtually run on every UNIX platform.

2.4.6.8Wire Shark

Has established itself as the premier packet analyser. It can capture packets of standard Ethernet, PPP and VPN interfaces. I have used it many times to identify people running heavy reports bringing servers down to a crawl.

Wire Shark requires installation of Windows Packet Capture package (WINPCAP).WinPcap allows for other software to 'listen' secretly to the information coming and going through the network card on the computer. I found

it better to install the latest WinPcap first, rather than versions included with the programs.

2.4.6.9 Angry IP

Angry IP is a very lightweight program that allows you to quickly scan a range of IP addresses. It provides less information and options than Nmap, but shows open ports and highlights which addresses are active.

2.4.6.10 IPTraf

IPTraf is a menu driven utility that allows you to monitor your TCP network. Information such as ICMP, OSPF, TCP and UDP counts can be displayed easily. Interfaces can be monitored. Monitor connectivity and traffic with ease.

IPTraf cannot create the configuration file. The most likely cause of this is that you didn't properly install the program, and the necessary directory /var/local/iptraf does not exist. Can also be generated if you have a disk problem or if you have too many files open.

2.4.6.11 IPFM

IPFM is a bandwidth analysis tool. It counts how much data was send and received by specified hosts through an Internet link.

IPFM collects data (statistics) in RAM. The DUMP keyword specifies the interval at which to create log files. The log files thus show cumulative results.

2.6 Categories Network Monitoring and analysing Tools

In this section explain the categories of network Monitoring and analysing according to flow, SNMP and Full Packet Capturing as in following table:

Table 2.1: Categories Network Monitoring and analysing Tools

	Flow	SNMP	Full Packet Capturing	Measuring tools
Net Flow	Flow traffic			
MRTG		MRTG		
PRTG		PRTG		
wire Shark			wire Shark	
IPFM				
SARG		SARG		
Ping sting				Ping sting
NTop	NTop			
Angry IP		Angry IP		
IPTraf			IPTraf	

2.7 Network Usage Control Tools

2.7.1 NAC

Network Access Control (NAC) is a complete standards-based, multi-vendor interoperable pre-connect and post-connect Network Access Control solution for wired and wireless LAN and VPN users. Using Extreme Networks NAC Gateway appliances and/or NAC Gateway Virtual Appliance with Net Sight NAC management configuration and reporting software, IT administrators can deploy a leading-edge NAC solution to ensure only the right users have access to the right information from the right place at the right time including time of day, location, authentication types, device and OS type, and end system and user groups.

2.7.2 Squid

Squid is caching proxy server, which improves the bandwidth and the response time by caching the recently requested web pages. Now a day's many servers in the world are configured with squid in order to provide high delivery speeds to the clients. Configuring the squid in transparent mode, special configuration is not required on the client side. All the requests originaltigniting from client and going to internet on port 80 are automatically redirected by proxy. Depending on the requirement we need to configure the squid as transparent or non-transparent proxy. This lab aims to enable readers implement a Proxy server in the network so that other users of the LAN can leverage the functionalities of accessing internet through proxy.

2.7.3 TC command

Traffic control is the name given to the sets of queuing systems and mechanisms by which packets are received and transmitted on a router. This includes deciding

which (and whether) packets to accept at what rate on the input of an interface and determining which packets to transmit in what order at what rate on the output of an interface.

2.7.4 IP TABLE

IP tables is a generic table structure that defines rules and commands as part of the net filter framework that facilitates Network Address Translation (NAT), packet filtering, and packet mangling in the Linux 2.4 and later operating systems. NAT is the process of converting an Internet Protocol address (IP address) into another IP address. Packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. Packet mangling is the ability to alter or modify packets before and/or after routing.[24]

2.8 Previous Studies

In reference [9] they compare the idea of congestion avoidance with that of flow control and congestion control. A number of possible another for congestion avoidance have been recognized. From these a few they are certain for study. In particular, they wanted the scheme to be globally efficient, fair, dynamic, convergent, robust, distributed, configuration self-determining, etc. They model the network and the user policy for congestion averting as a feedback control system. The key components of a generic congestion avoidance scheme are: congestion detection, congestion feedback, feedback selector, signal filter, decision function, and in- crease/decrease algorithms. The congestion avoidance research was done using an arrangement of analytic model and simulation techniques.

They are able to design the scheme to get the following objectives: efficiency, fairness, convergence, responsiveness, source bound. However, No Reverse Traffic, No Acknowledgment Withholding.

In reference [15] they demonstrate the potentials of a new network monitoring architecture named HISTORY (High Speed Network Monitoring and Analysis). The basis of this approach is a high-speed monitoring probe allowing to process up to one gigabit per second on a standard PC. The complete architecture relies on standardized protocols such as IPFIX and PSAMP for transmission of monitoring data between the monitoring elements and successive traffic analysis. Especially the employed statistical methodologies allow the usage of History for various applications in network security such as intrusion detection and trace back. In this paper they introduce two tools developed in History for high- speed network monitoring (Vermont) and analysis (Nasty). The advantages of HISTORY: cooperative autonomous entities with distributed functioning, Emergent behaviour through adaptive self-organization, Operation in high-speed networks while utilizing standard PC components, Wide application range from accounting up to traffic engineering, intrusion detection and trace back, but it is Expensive, Complex.

In reference [16] they propose a novel QoS management scheme based on per class degradation. Its performance has been compared with the previous proposed adaptation algorithm. They are able to design a new scheme generally performs better since it provides better fairness and faster calculation, whereas the previous algorithm, based on per flow, can utilize the system bandwidth more efficiently. It also provides computation simplicity and executes faster, which is important to the admission control component. However, per flow method can use the system resources more efficiently than the per class method. Simulation experiments also

indicate that the adaptive multimedia framework outperforms the non-adaptive approach in terms of lower handoff dropping probability and call blocking probability while still maintaining acceptable QoS to the end users.

In reference [17]propose several novel architectural enhancements for Ethernet passive optical networks (EPON), which will help increase the viability of optical access over a broader range of subscriber access scenarios. Specifically, they propose a two-stage EPON architecture that allows more end-users to share an optical line terminal link, and enables longer access reach/distances(beyondtheusual25km distance).In addition, a new dynamic bandwidth allocation(DBA) algorithm is proposed to effectively allocate bandwidths between end users .This DBA algorithm can support differentiated services in a network with heterogeneous traffic. They conduct detailed simulation experiments to study the performance and validate the effectiveness of the proposed architecture and algorithms. They reviewed the overall architectures and bandwidth allocation algorithms of emerging EPON designs and proposed a novel two-stage enhancement, penetrated-EPON (P-EPON). This scheme utilizes an intermediate state to help increase universality and boost distance and coverage within the access domains. A comprehensive DBA algorithm for P-EPON is also tabled and its throughput-delay performance studied using simulation techniques for various realistic network set- tings. Overall, these finidings help validate the effectiveness of the proposed architecture and its new DBA algorithms.

In reference [18] they develop QoS versions of the OLSR (Optimized Link State Routing) protocol, which is a “pro-active” Ad-Hoc routing protocol. They introduce heuristics that allow OLSR to find the maximum bandwidth path, show through simulation and proof that these heuristics do improve OLSR in the bandwidth QoS aspect; they also analyse the performance of the QoS routing

protocols in OPNET, observe the achievement obtained, and the cost paid. The results show that the QoS versions of the OLSR routing protocol do improve the available bandwidth of the routes computed. However, it added cost; the additional overhead also has a negative impact on the network in End-to-End Delay and Packet Delivery Ratio, especially in the high speed movement scenarios.

In reference [12] Previous IP networks sent data that (mostly) tolerated delay, new applications have new QOS requirements (IP voice is sensitive to latency, jitter, packet drops IP video is sensitive to latency, packet drops).

QOS can be applied incrementally, but is much easier to manage if applied as a standard.

The network grew in size and complexity, mirroring the growth of the company, two things happened: Better QOS technologies were needed, and it became a great time to partner with the Cisco development organizations.

However: Lab traffic with QOS needs: Labs are not trusted traffic sources, but may need QOS, IP voice over VPN: Home office users starting to need QoS over the Internet, QOS over MPLS VPN: Service providers handle and bill for varying classes of service differently, Call admission control: Gatekeeper handling of oversubscription needs to know the network topology, Desktop trusted edge: Cisco IT is migrating trusted edge to desktop to support desktop videoconferencing, Storage networking: Cisco IT is beginning to put very high volume SAN traffic across the LAN, and is studying how best to use QOS to support SAN and other traffic needs during congestion.

In reference [19], they are propose Data-centre administrators perform traffic management tasks (e.g., performance monitoring, server load balancing, and traffic

engineering) to optimize network performance for diverse application. Increasingly, traffic management functionality is moving from the switches to the end hosts, which have more computational resources and better visibility into application behaviour. However, traffic management is complicated by the various interfaces for monitoring and controlling hosts and switches, and the scalability challenge of collecting and analysing measurement data across the data centre. They present a scalable and programmable platform for joint Host Network (HONE) traffic management. HONE's programming environment gives a simple, integrated, and logically-centralized view of the data centre for denting measurement, analysis, and control tasks across hosts and switches. Programmers can think globally and rely on HONE to distribute the program for local execution and scalable aggregation of data across hosts and switches. HONE success- fully balances the inherent tension between ease-of-use and performance. they evaluate HONE by implementing several canonical traffic management applications, measuring its efficiency with micro benchmarks ,and demonstrating its scalability with larger-scale experiments on Amazon EC2.However, VM-level monitoring and migration, and preventing the host agents and the controller from becoming overloaded not found in this study.

In reference [13]their work focus on the development of an application to combat the challenges facing easy flow of data transmission problems in network design as organization network evolves. Here PHP Script, Apache Server and My SQL are the development tools used. Using bandwidth management to allocate bandwidth to applications or users during peak times can prevent traffic congestion on the network. When bandwidth is bought and controlled, data's and communications are transferred around easily. Networks make it very easy for users that need to send information at a fast pace. This work presents a testable

application that combat the challenges facing easy flow of data transmission problems in network design as organization network evolves. Further work improvement on the system is recommended to assist large scale organizations in the management and control of their computer networks bandwidth.

In reference[20], their aims at designing a congestion and priority solution for Ethernet congestion management. follow the popular approach that uses a cooperation of an Additive Increase and Multiplicative Decrease (AIMD) based rate limiter and Explicit Congestion Notification (ECN) active queue management to combat congestions in Ethernet, the plan considers differentiated AIMD settings for rate limiters to achieve congestion control differentiation for traffic of different priorities. We show that while the operations of AIMD and ECN are independent, by using different AIMD settings, they can achieve differentiated control of bandwidth utilization. They develop a control theoretic analytical model to study the effectiveness of their proposed method. Moreover, they implement their proposed method in OMNET++ simulator to conduct simulation experiments. Their analytical and simulation results both indicate the effectiveness of bandwidth ratio differentiation. Thus a higher system performance with low overhead can be achieved. However, results show that the bandwidth is generally governed by the rate limiter at Layer-2 as the rate limiter at Layer-2 reacts faster than that at Layer- This suggests that the targeted differentiated congestion control remains effective when the network carries TCP traffic.

In reference [17], they describe the architecture and implementation of a scalable network traffic monitoring and analysis system. The gigabit interface on the monitoring system was configured to capture network traffic and the Multi Router Traffic Grapier (MRTG) and Webalizer produces graphical and detailed traffic analysis. This system is in use at the Obafemi Awolowo University, Ile-Ife,

Nigeria; they describe how this system can be replicated in another environment. They have presented the development of a scalable network traffic monitoring and analysis system. The system is capable of monitoring and analyzing network traffic for both the Intranet and the Internet traffic, the design employ free open source programs such as IP Traffic, MRTG and Nebulizer, and scripts written in Perl language. The system monitors network traffic passively, this implies that it is non-intrusive and monitors network traffic always, using the loss data storage technique to store the data as web pages. Graphical over- views of the traffic monitored were existing using MRTG, while detailed analyses of the traffic and proxy log analysis were presented using Webalizer. A user can view the results of the monitoring system using a web browser. They have described the hardware and software required to setup the system and how it can be replicated on any network. Using the system we were able to monitor the internal and external network, the scalability feature of the system, makes it attractive to both re- searchers and network managers. The output graph generated by the system provides details of the network dynamics and insight into problems that could lead to congestion and poor network performance. But is not focus on intrusion finding monitoring module and pre-emptive intrusion control.

In reference [18] they address the problem of real-time update of access control policies in the context of a database system. Access control policies, governing access to the data objects, are specie in the form of policy objects. The data objects and policy objects are accessed and mode led through transactions. They consider an environment in which deferent kind of transactions execute concurrently some of which may be procedure update transactions. They propose algorithms for the concurrent and real-time update of security policies. The algorithms deferent on

the basis of the concurrency provided and the semantic knowledge used. A lot of work still remains to be done.

On the Automated Analysis of Safety in Usage Control: a New Decidability Result.

Chapter 3: Methodology

Chapter 3
Methodology

3.1 Introduction

This chapter presents the methodology to be adopted in continuing this research procedure, operational framework, assumptions and limitations.

3.2 Research Design and Procedure

Four main phases describe the research procedure: problem identification, finding new approach, prototype implementation and validation.

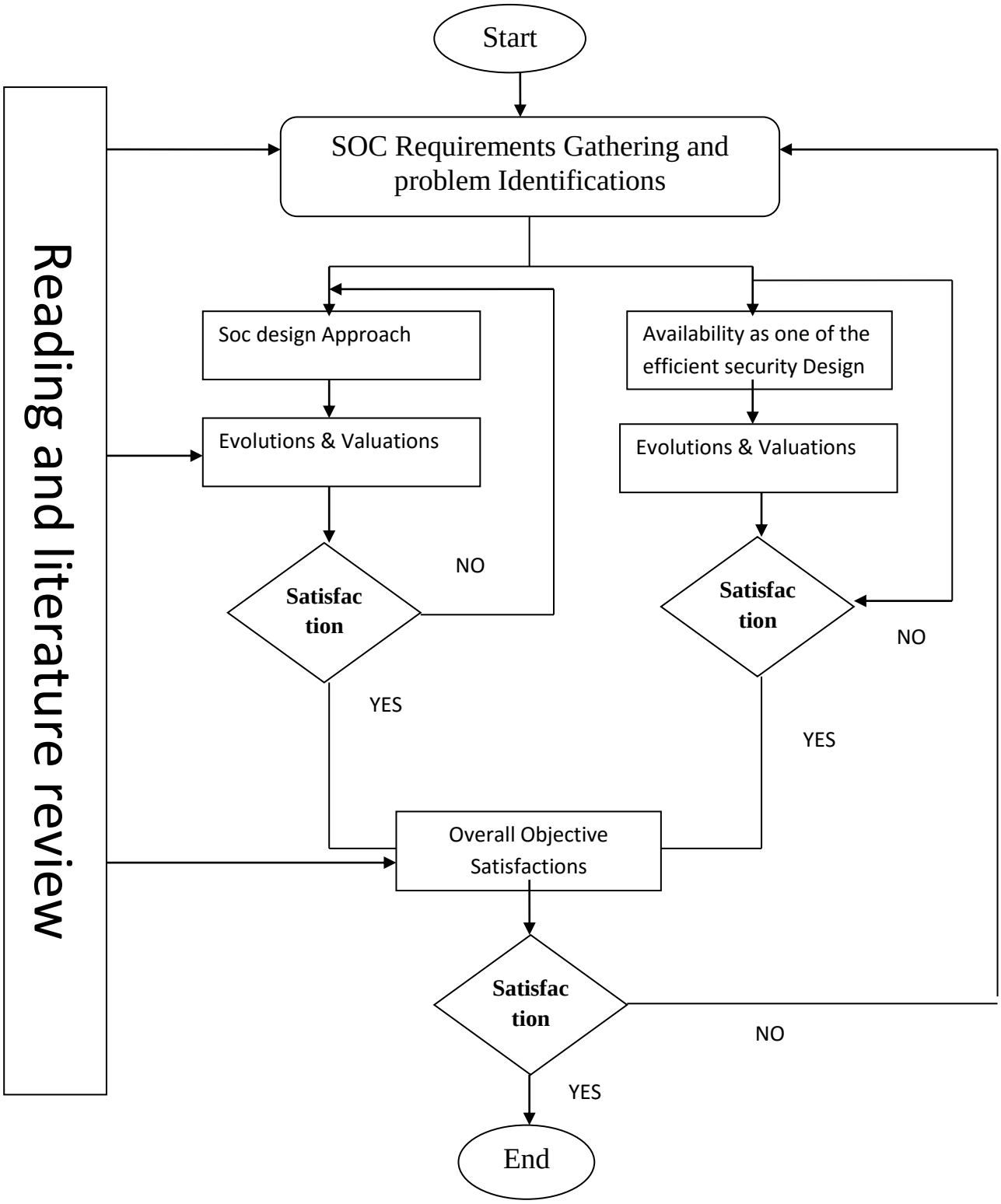


Figure 3.1 Research Design and Procedure

3.3 Security Operation Centre Methodology

To design security operation centres content five steps must be applied anthers steps explain this steps:

Event generation responsible of generation event with using type of event like Sensors the most well-known type of sensors are IDS's, be they host based or network.

- Data collection responsible to collection data using some methods to applied this type like in this project using interview questioners to collection data.
- Stores in data base responsible to save all data in the database using SQL servers or oracle data base in this project using accesses database.
- Data analysis responsible to analysis all data found in data base using some tools like MRTG in this project after collection data using spss software to analysis all data.
- Data operation responsible of reaction after any problem using alert or any action to solve the problem using in network the result of this project how to design optimal security operation centres.

The figure below shows the security operation design methodology according to genera l concept of soc

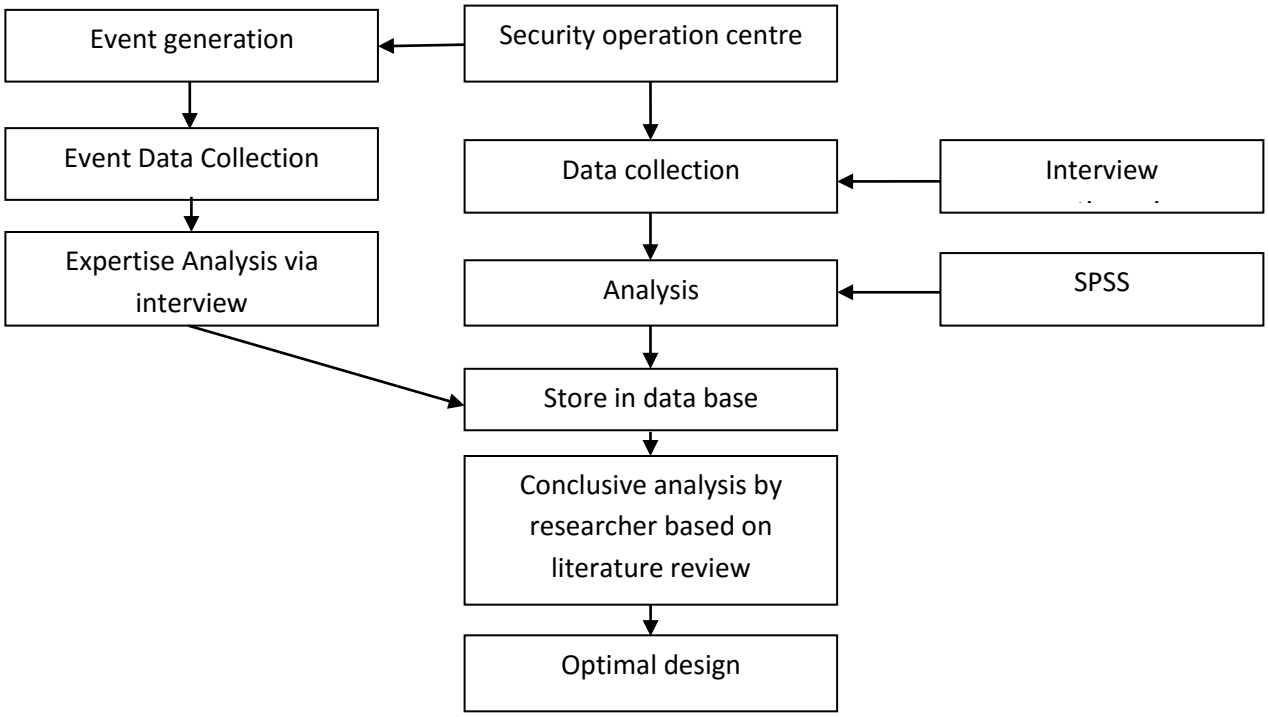


Figure 3.2 security operation centre design methodology

As can be seen from the above figure it explains all the steps which are related to the design of security operation centres according to interview questionnaire.

3.4 Bandwidth Management Methodology

In this section explain the concept of management bandwidth control and compression between without faire distributed bandwidth and faire distributed.

3.4.1 The importance of Internet traffic Control

In computer networks, bandwidth is used for data transfer rate, the amount of data that can be carried from one point to another in a given time period (usually a second). Network bandwidth is usually expressed in bits per second (bps); modern networks typically have speeds measured in the millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second,

or Gbps). The below figures concerned distributed the bandwidth but not fair to all users is very important.

The below figure show distributed internet link without fair distributed

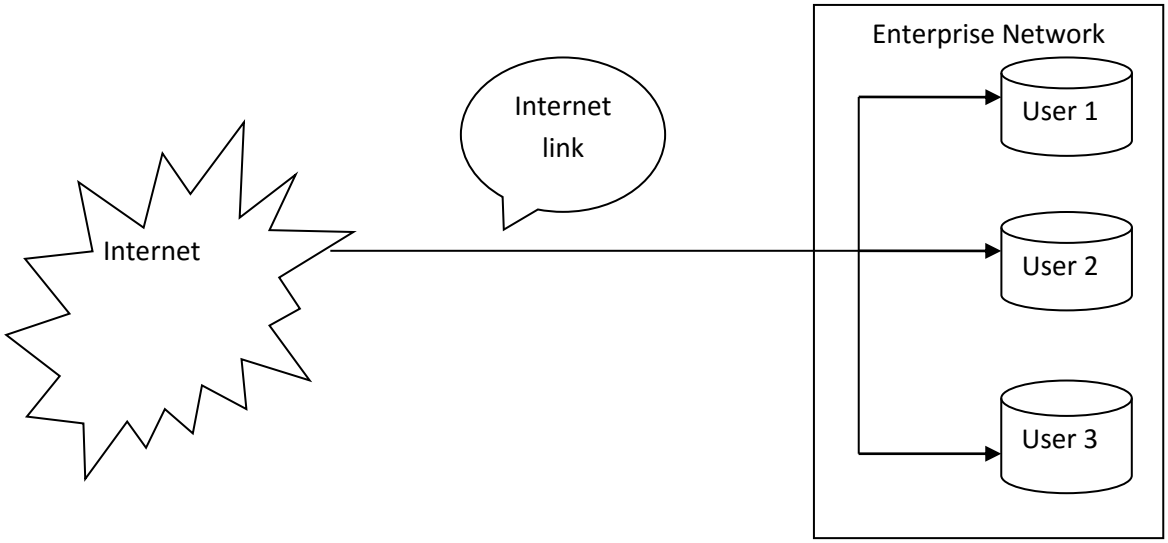


Figure 3.3 without fair distributed internet link

This figure concerned the worst scenarios when the student final capacity is not fairly distributed the internet link in all users of the network this type of scenarios is very poor because it reduce the availability of internet link and degrade the performance the network. According to the normal usage.

3.4.2 Bandwidth management according to distributed capacity

Fair usage policy is a policy used by Internet service providers for the distribution of capacity for each user to prevent users from infringing on the specific capacity and when this limit, the speed drops to a low speed exceed. The illustration below

Show distribution of capacity to each section of the university and every official of the department for distribution capacity for each user within the division and punish anyone who exceed her capacity, was applied both the faculty distributed

bandwidth algorithm and department distributed bandwidth algorithm specialized distribution capacity on this form andappear that third more effective because it fair distribution faire distributed in addition to most of the existing users.

The below figure show distributed internet link with fair distributed

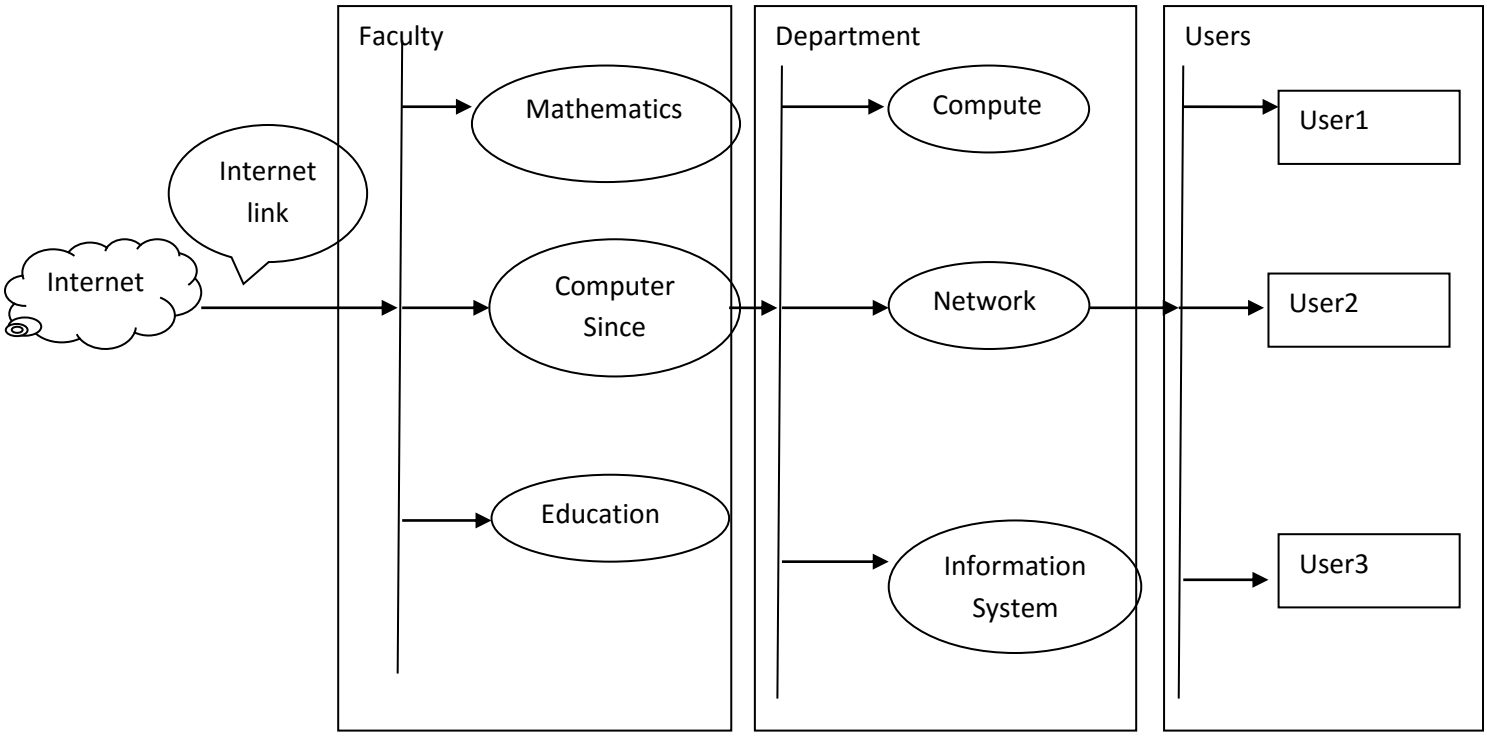


Figure 3.4 fair distributed internet link

3.5.1 Bandwidth monitoring and control

This section proposes a distributed bandwidth monitoring and control. The management of the link bandwidth is divided into four separated algorithms, the first one manage the bandwidth in a utilize centre link the second one manage faculty level, that is to say the algorithm always monitor the overall internet link utilization and accordingly if the link is over utilized, a fair bandwidth allocation to the faculty will be enforced, that means the faculty which over consume its expected bandwidth will be regulated (bandwidth throttling). Similarly the second called department distributed algorithm which works according to the link utilization of the campus in addition to the link of the faculty so as to determine the over consumption in the user level instead of faculty level and regulate the usage of the abnormal user directly. By implementing the tow algorithms concurrently, the internet link will be healthy and the usage will be fair among the faculties and users as well.

Figure [3:3] and figure [3:4] represents the college regulation algorithm and the user deregulation algorithm respectively in four hierarchical levels. The first, second and third algorithm design to faire distributed bandwidth.

Faire distributed bandwidth is very use full or very important to all levels of users in network and create high performance to network and easy to access internet link. The both Second and third Algorithms in depended the min max algorithm to create faire distrusted bandwidths the below steps concerned second algorithm.

- Enter total capacity using Keyport
- Enter any user capacity using Keyport
- Test of the all capacity less than the total capacity or not
- If not less after that decrees any capacity by 1 and result

  The below figure show the distributed bandwidth for all faculty of university

  Sum all capacity of users

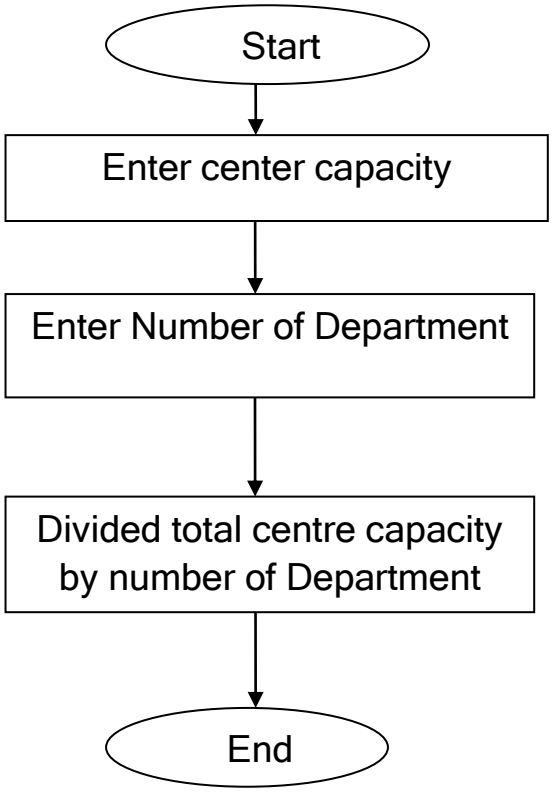


Figure 3.5 Centre distributed bandwidth algorithm

The below steps concerned Faculty distributed algorithm Enter any user capacity using keyboard

- Enter total capacity using keyboard
- Sum all capacity of users
- Test of the all capacity less than the total capacity or not
- If not less after divide any capacity by 2 and resume

The below figure show the distributed bandwidth for all users in faculty of university

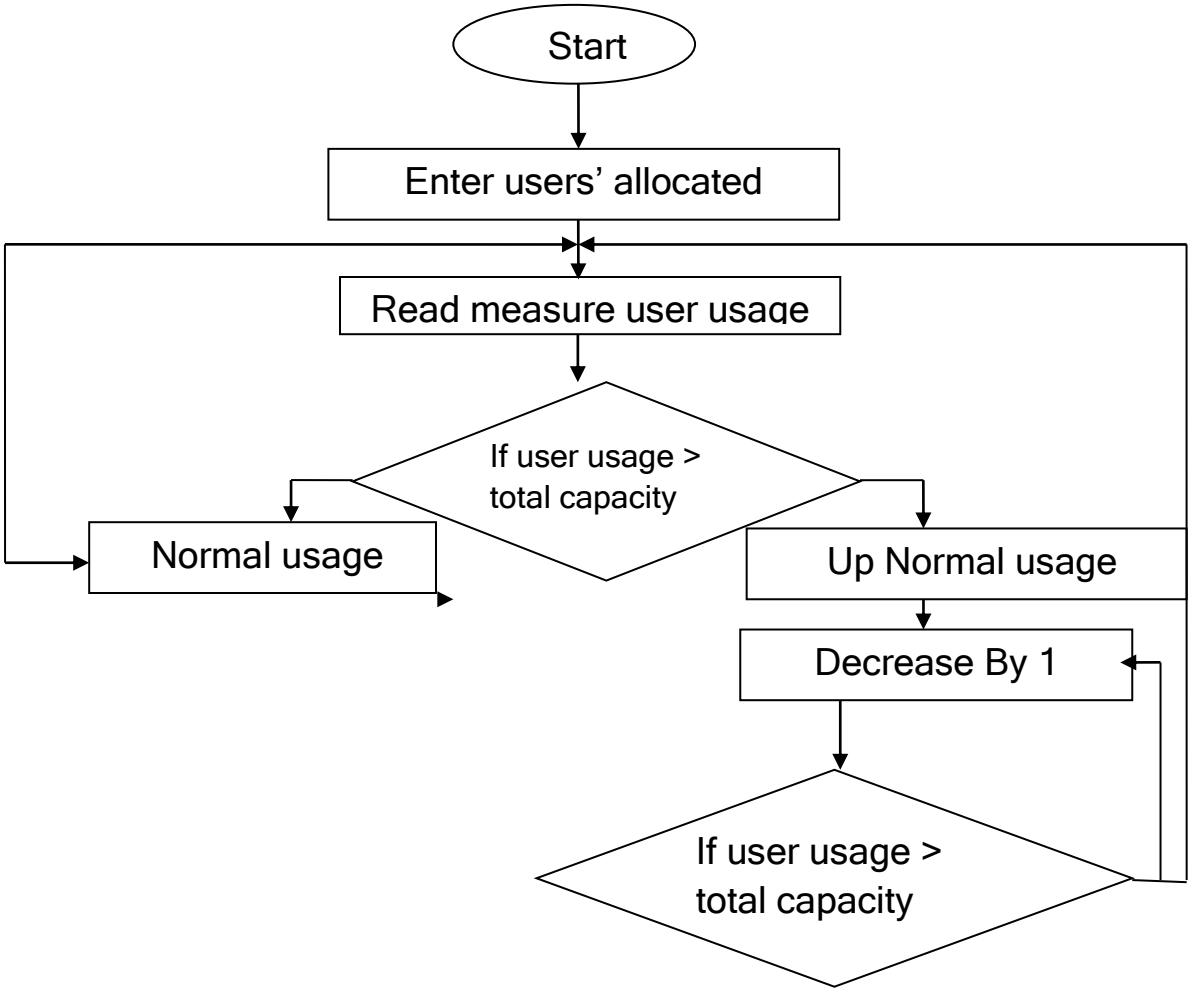


Figure 3.6 Department distributed bandwidth algorithm

The below steps concerned Faculty distributed algorithm Enter any user capacity using keyboard

- Enter total capacity using keyboard
- Sum all capacity of users
- Test of the all capacity less than the total capacity or not
- If not less after divide any capacity by 2 and resume

The below figure show the distributed bandwidth for all users in faculty of university

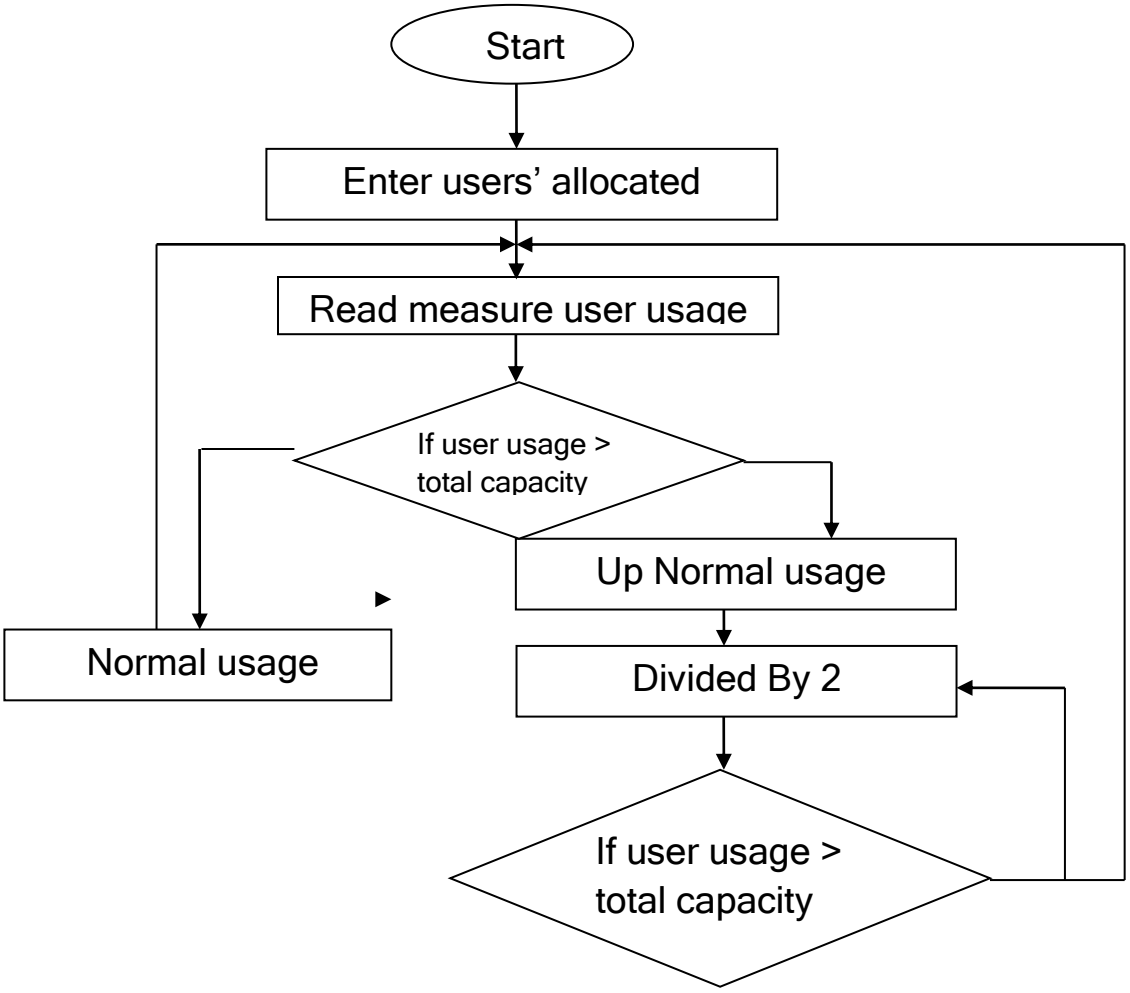


Figure 3.7 Faculty distributed bandwidth algorithm

The Department distributed bandwidth algorithm is more efficient than faculty distributed bandwidth algorithm because to use large capacity of bandwidth by users and distributed capacity large number of users.

The four algorithm called user bandwidth monitoring control measures the usage of any users in the network, and then helps him/her to perform self-based regulation by adapting his/her usage according to the expected usage. This algorithm displays to users their corresponding usage. Moreover it calculates the total of capacity in daily or weekly basis. The below steps explain how the proposed algorithm calculate the total capacity of individual users.

- Enter the total internet link capacity
- measure the user's usage
- Extract percentage so explain the usage of capacity for any user in the networks

  The below figure (3-8) shows the algorithm

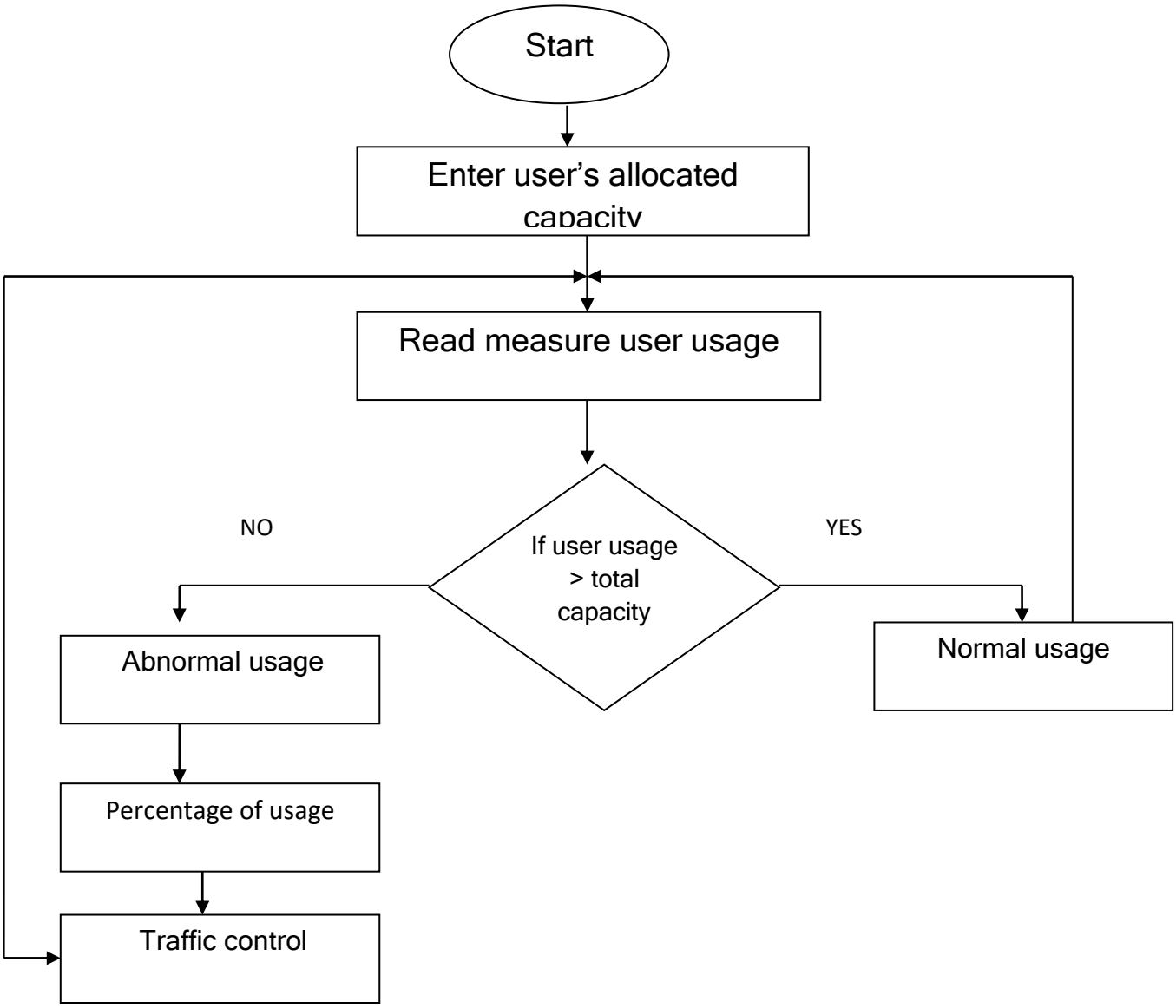


Figure 3.8 users bandwidth monitoring

Chapter 4: System Implementation and Result

Chapter 4

System Implementation and Result

4.1 Introduction:

This chapter explain the analysis data according to interview questionnaire using SPSS software to analysis this data and introduce result .this result explained how to build security operation Centre applied. Others this chapter explained how to management bandwidth.

4.2 Security Operation Centres Design Result, Analysis and Discussion

In this section the details of the questionnaire question by question will be explored, to see the complete version of the questionnaire please refers to appendix.

4.2.1 Analysis and Discussion of q0:

According to the two questions in the interview questionnaire which is ((Do you have a secret operation centres (soc**)**?)). The researcher makes this question to validate the first research hypothesis which is ((Most of Organizations have not a secret operation centres **(**soc**)?**

The table below includes the percentages of existence of SOC according to the interview questionnaire.

Table (4.1) percentages of existence SOC

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	1	10.0	10.0	10.0
	No	9	90.0	90.0	100.0
	Total	10	100.0	100.0	

From table (4.1) appear that (90%) from the ICS administrators have not security operation centres. These results agree with the first research hypothesis. Figure (4.1) illustrates the analyses and the result of q0.

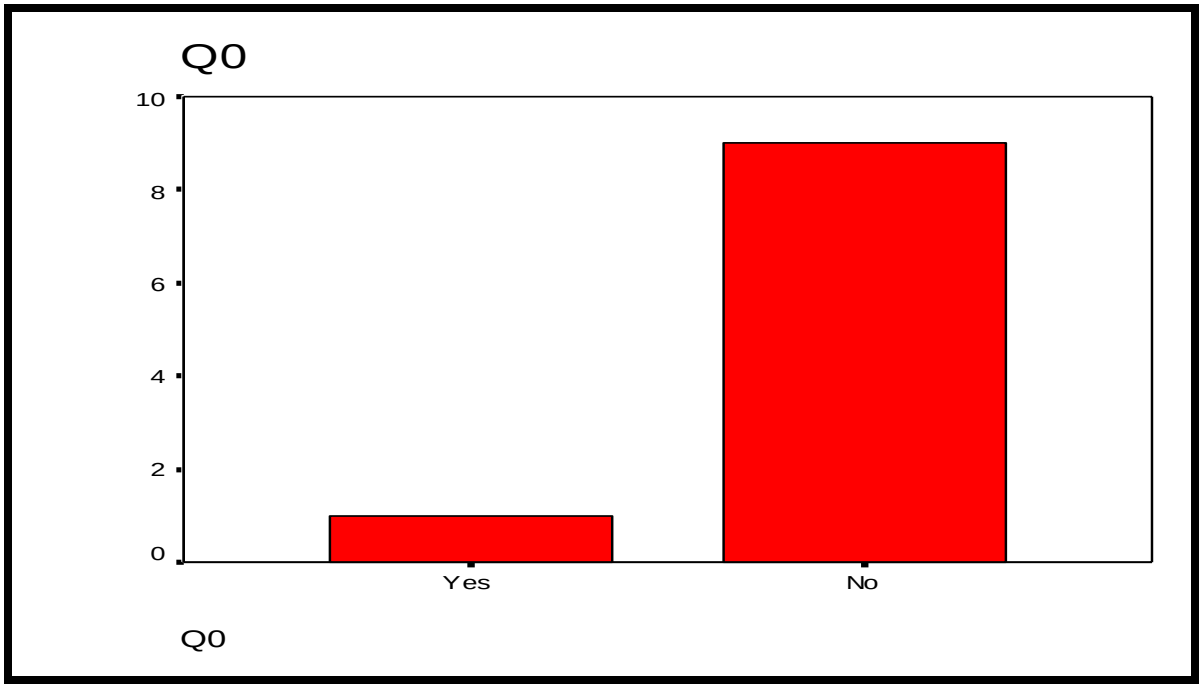


Figure (4.1) levels of existence Of SOC

4.2.2 Analysis and Discussion of q1:

According to the first question in the interview questionnaire which is ((Do you have Computer Centres (CC) or Information Communication Centres (ICT)?)). The researcher makes this question to validate the second research hypothesis which is **((**Most of Organizations have computer centre (cc) or Information Communication Technology Centre (ICT).

The percentages of existence Of ICC according to the interview questionnaire Will be included in the below table.

Table (4.2) percentages of existence Of ICC according to the interview questionnaire

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	9	90.0	90.0	90.0
	No	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

From table (4.2) appear that (90%) from the ICT administrators have security centres. These results agree with the first research hypothesis. Figure (4.1)illustrates the analyses and the result of q1.

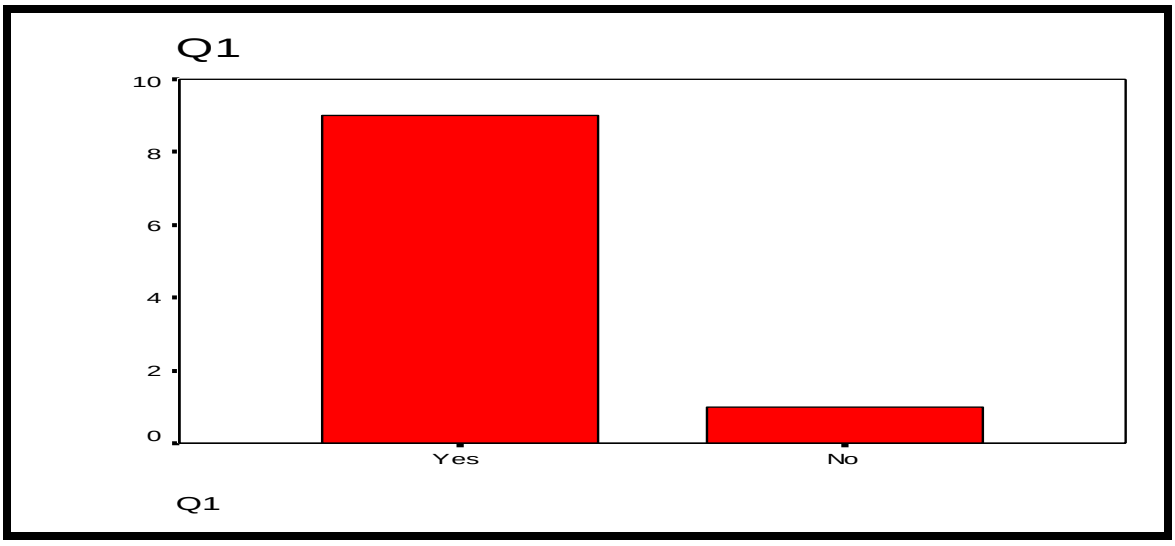


Figure (4.2) ICC levels according to the interview questionnaire

4.2.3 Analysis and Discussion of q2 and q3:

According to the two questions in the interview questionnaire which is **((**What are the mechanisms or policies or operations to achieve the secret?)). The researcher makes this question to validate the third research hypothesis which is **((**Most of Organizations have not using any mechanisms or policies or operations and have not a control techniques?)).

The below table content the percentages of using mechanisms or policies according to the interview questionnaire.

Table (4.3) percentages of using mechanisms or policies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Active directory	4	40.0	40.0	40.0
	username/ password	6	60.0	60.0	100.0
	Total	10	100.0	100.0	

From table (4.3) appear that (62%) from these results agree with the second research hypothesis. Figure (4.3) illustrates the analyses and the result ofq2 and q3.

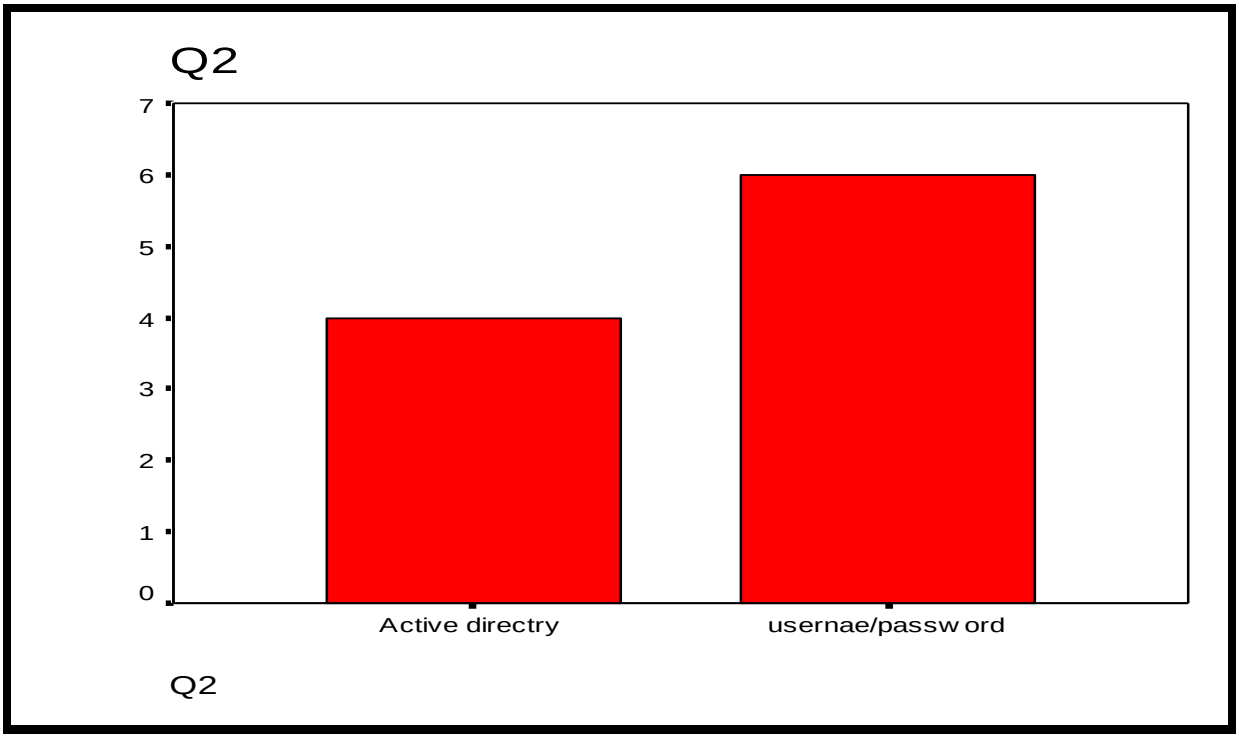


Figure (4.3) levels of using mechanisms or policies

4.2.4 Analysis and Discussion of q4-6:

According to questions four to six in the interview questionnaire which is ((What are the types of attacks or threats?)). The researcher makes this question to validate the fourth research hypothesis which is ((Most of Organizations suffer from the problem of hacking & viruses??

The table blow includes the percentages of existence of Problem according to the interview questionnaire.

Table (4.4) percentages of existence of Problem

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	viruses	4	40.0	40.0	40.0
	spam	2	20.0	20.0	60.0
	Hacking	4	40.0	40.0	100.0
	Total	10	100.0	100.0	

From table (4.4) appear that (60%) from thee suffer the problem of hacking & viruses in your centres. These results agree with the forth research hypothesis. Figure (4.4) illustrate the analyses and the result ofq4-6.

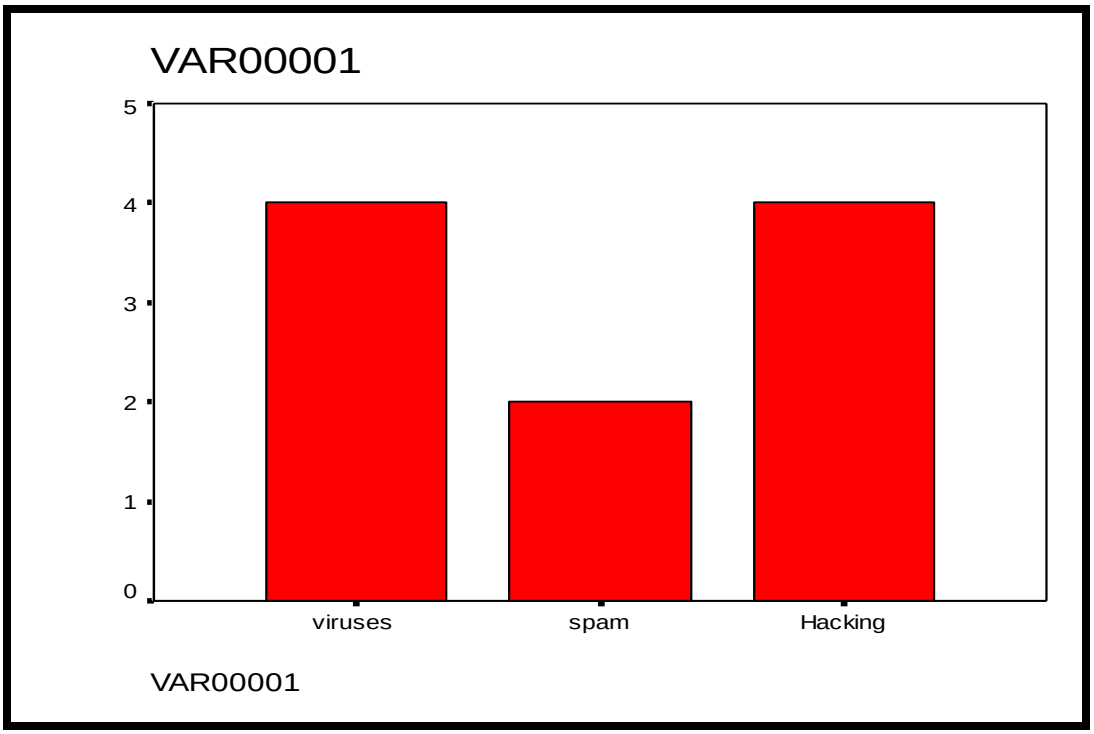


Figure (4.4) levels of existence of Problem

4.2.5 Analysis and Discussion of q7:

According to the seven question in the interview questionnaire which is ((. What are the methods used to protect your centres?)). The researcher makes this question to validate the fifth research hypothesis which is **((**Most of Organizations have use firewall to protection their centres and using anti viruses??

Table (4.5) include the percentages of the method using to protect the cc according to the interview questionnaire.

Table (4.5) percentages of the method using to protect the computer centres

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Firewall	5	50.0	50.0	50.0
	Antivirus	3	30.0	30.0	80.0
	Access list	1	10.0	10.0	90.0
	Anti Spam	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

From table (4.5) appear that (50%) from thee centres using firewall to protection your centres. These results agree with the third research hypothesis. Figure (4.5) illustrates the analyses and the result of q7.

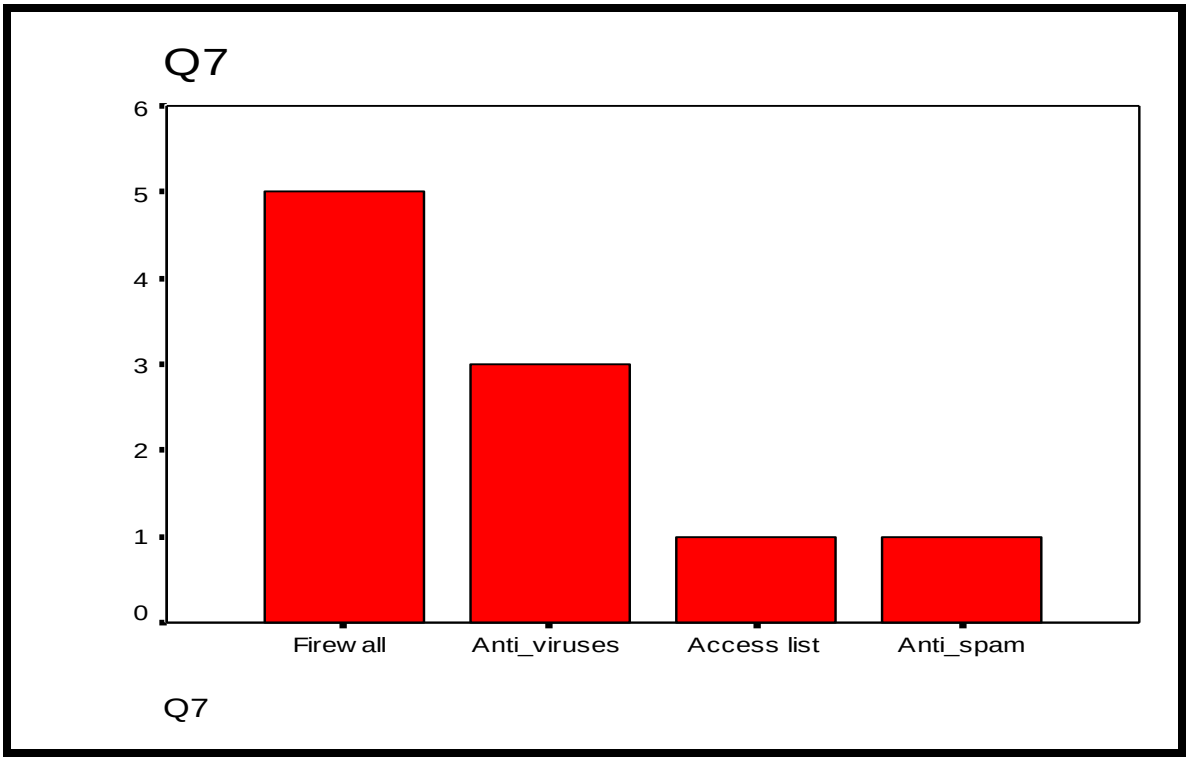


Figure (4.5) levels of method using the protect your computer centre

4.2.6 Analysis and Discussion of q13:

According to the thirteenth question in the interview questionnaire which is ((Do you have control techniques?)). The researcher makes this question to validate the above third research hypothesis.

The table blow includes the percentages of existence control techniques according to the interview questionnaire.

Table (4.6) percentages of existence control techniques

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	5	62.5	62.5	62.5
	No	3	37.5	37.5	100.0
	Total	8	100.0	100.0	

From table (4.6) appear that (62%) from the have control techniques. These results disagree with the third research hypothesis. Figure (4.6) illustrates the analyses and the result of q13.

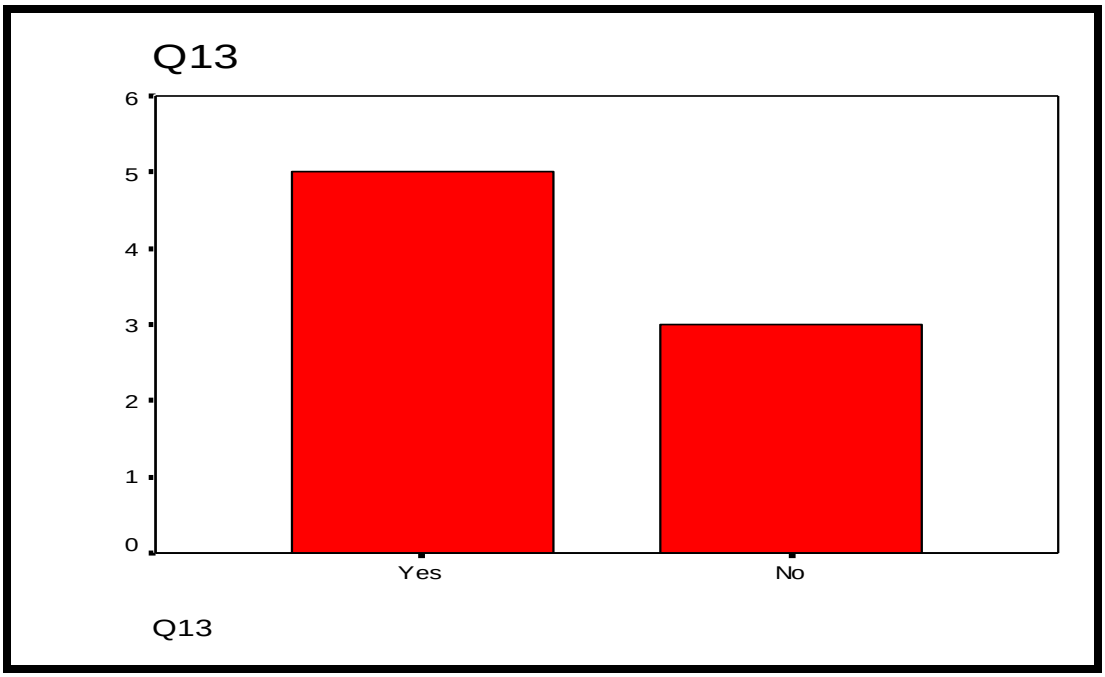


Figure (4.6) levels of existence control Techniques

4.2.7 Analysis and Discussion of q14:

According to the questions number fourteen in the interview questionnaire which is **((**What are the types of viruses you have?)). The researcher makes this question to validate the sex research hypothesis which is **((**Most of Organizations existence Trojan hour's viruses and have Most organization using Kaspersky the main ant viruses.

The table below includes the percentages of type of Viruses according to the interview questionnaire

Table (4.7) percentages of type of
Viruses according to the interview questionnaire

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Trojans hours	6	60.0	60.0	60.0
	Worms	4	40.0	40.0	100.0
	Total	10	100.0	100.0	

From table (4.7) appear that (62%) from the have control techniques. These results disagree with the third research hypothesis. Figure (4.7) illustrates the analyses and the result of q13.

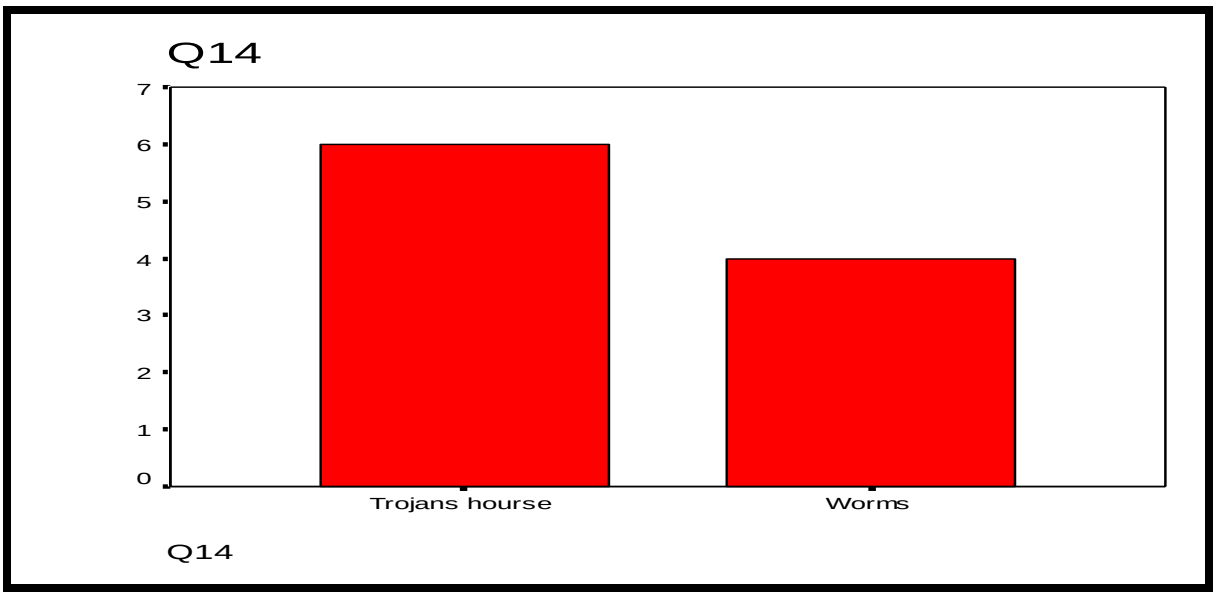


Figure (4.7): Types of viruses According to the interview questionnaire.

4.2.8 Analysis and Discussion of q15:

According to the fifteen questions in the interview questionnaire which is ((What are the types of antivirus software that you used?)). The researcher makes this question to validate the sex research hypothesis.

The table below include the percentages of existence of Ant viruses according to the interview questionnaire

Table (4.8) percentages of existence of
Ant viruses according to the interview questionnaire

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Kaspersky	5	50.0	50.0	50.0
	Nod32	3	30.0	30.0	80.0
	Eset	1	10.0	10.0	90.0
	A vast	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

From table (4.8) appear that (50%) from using Kaspersky the main Ant viruses these results agree with the second research hypothesis. Figure (4.8) illustrates the analyses and the result of q15. Type of ant viruses.

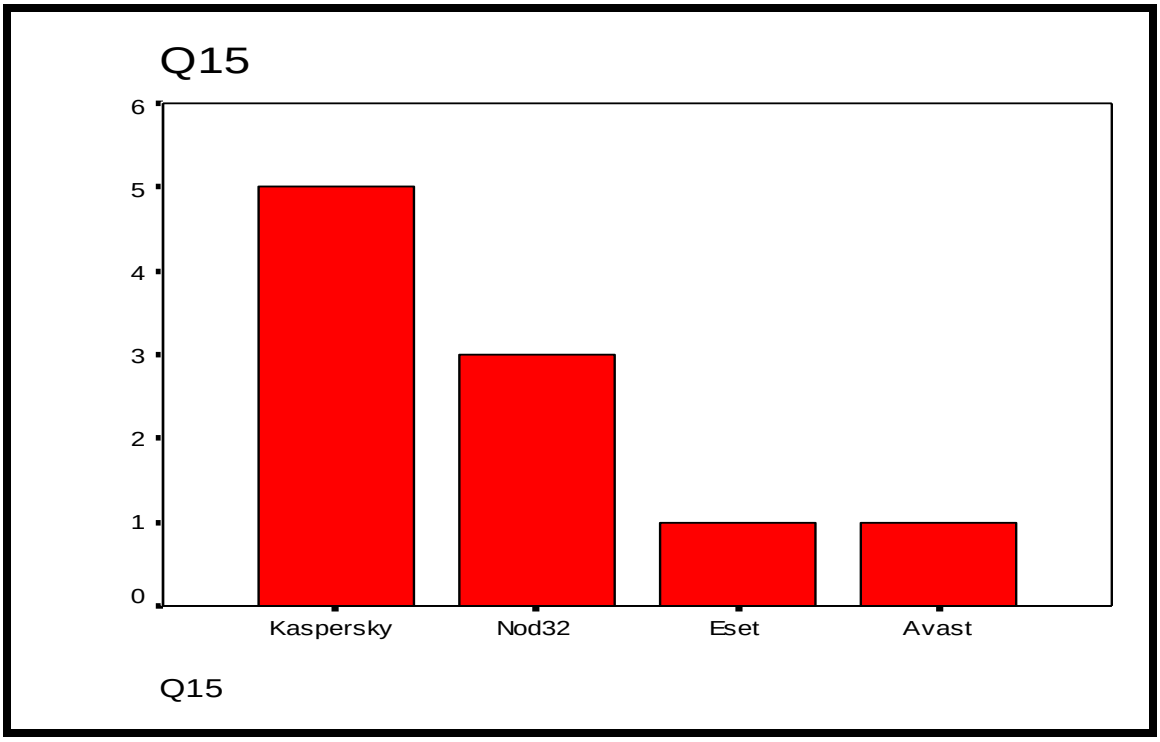


Figure (4.8) levels of existence of ant viruses

4.2.9. Analysis and Discussion of q17:

According to the seventeenth question in the interview questionnaire which is ((Do you have a security log file?)). The researcher makes this question to validate the fifth research hypothesis which is **((**Do Most of Organizations have a security log file and have method to analyse log file?)).

The table blow includes percentages of existence of Security log file according to the interview questionnaire.

Table (4.9) percentages of existence of Security log file

	Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid Yes	10	100.0	100.0	100.0

From table (4.9) appear that (100%) from have security log file. These results agree with the second research hypothesis. Figure (4.9) illustrates the analyses and the result of q17.

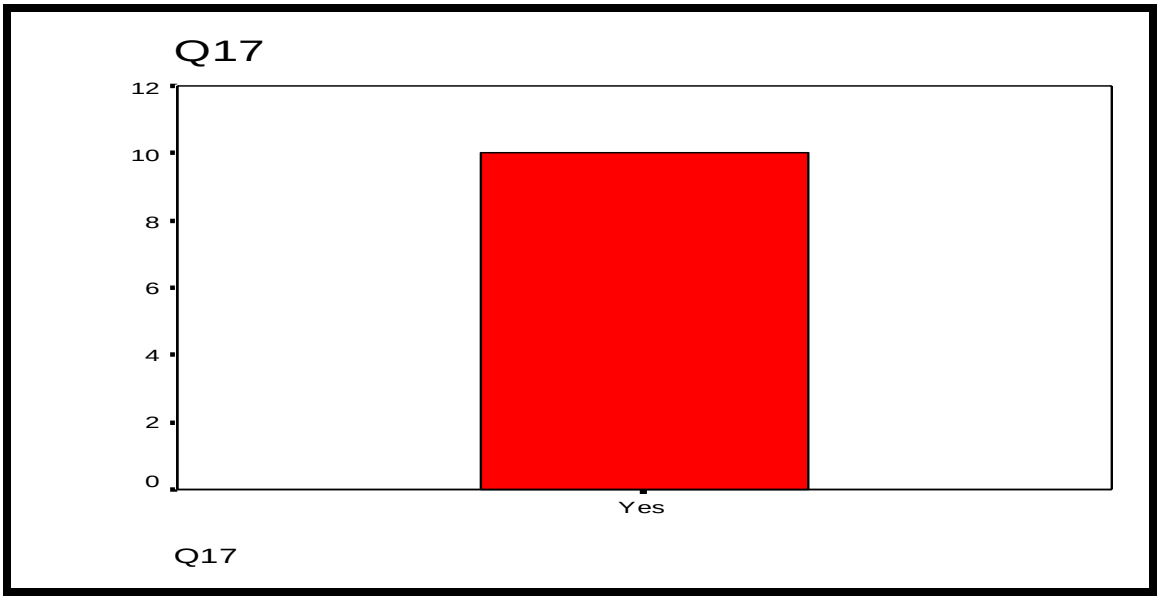


Figure (4.9) levels of existence of security Log file

4.2.10 Analysis and Discussion of q18:

According to the Eighteenth questions in the interview questionnaire which is **((**What are the methods used to analyses the content of the Log file?)). The researcher makes this question to validate the fifth research hypothesis in the above.

The table below includes the percentages of type of the Method according to the interview questionnaire.

Table (4.10) percentages of type of the Method

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	software in side firewall	1	10.0	10.0	10.0
	just reading	7	70.0	70.0	80.0
	software analyze	1	10.0	10.0	90.0
	With SEIM	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

From table (4.10) appear that (70%) just reading the log file. These results disagree with the third research hypothesis. Figure (4.10) illustrates the analyses and the result of q13.

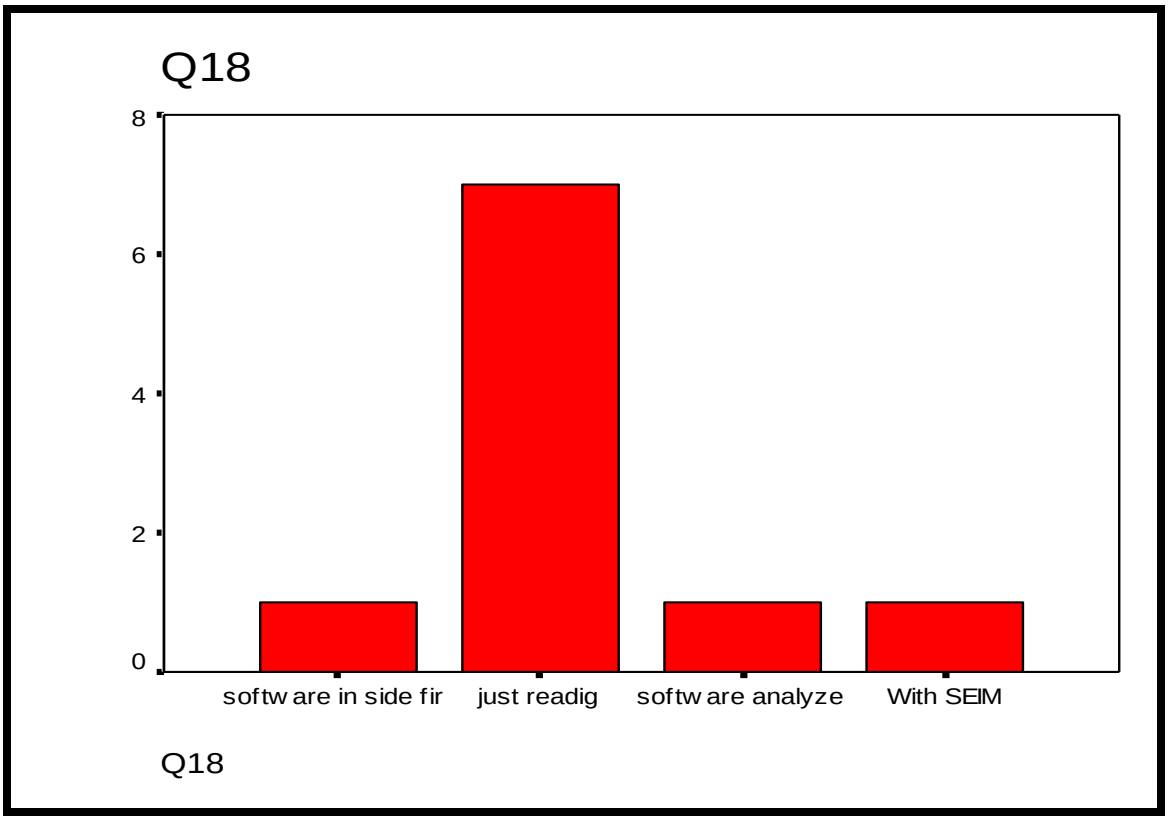


Figure (4.10) levels of methods using to Analyses log file

4.2.11 Result presentation, Analysis and Discussion:

In addition to hypothesis above themes of result of the ICC administrator see that determined security tools that can apply to enhance the security of centres like

- Well prepare data centres.
- Enhance security policies.
- Good protection from viruses and hackers.

Some of them see that the centres must preparing the building at first and then follow security methods and polices.

4.2.12 Analysis and discussion Explain number of firewall

The below figures include the number of firewall according to interview questionnaire the to any university

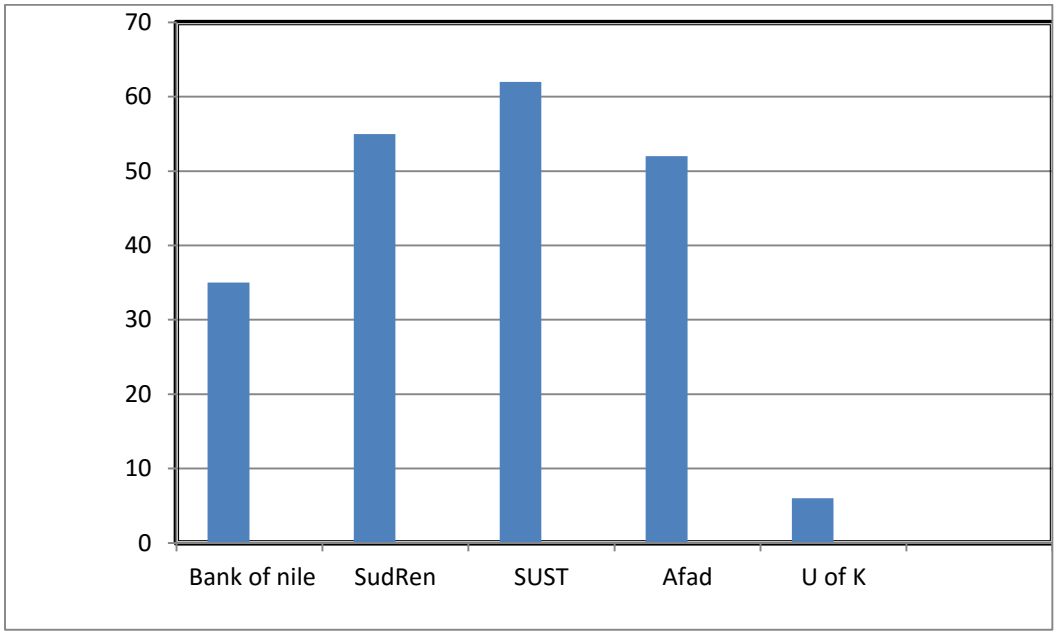


Figure (4.11) levels of numbers of routers

From the above figure numbers of firewall SUST has a big number of routers which are (65%).this result refers to more needs of routers which support the security needs .instead of that u of k has a small number of router and this result refer to there is no needs for more security policies.

4.3 Security Operation Centre Result and Design Solution

The researcher presents in the following section the result of the study in relation to the nine hypotheses of this study

1- In the case of existence of ICC All of the responders said they have ICT.

2- In the case of method, policy, controls and other tools the study proved that there are (60%) have control centres. But from the observation of the researcher found that most of these the control are protected by (ID &password).this result reflected weakness in the security polices ,because there are other strong security tolls that can be applied like(finger print ,petrol ,voice code ,and other modern tools) in addition to the wide separation of hackers and crackers.

3- Most of ICC used firewall and anti-viruses in the protection of centres. The researcher sees that some of these anti viruses were not obtained from the original source instead of free download.

4- Most of ICC faced dangers represent and in hackers and viruses'.

5- Most of ICC existence of log file, and have not analyse software .the observation of the researcher most ICC just reading the log file and not to extract reports and tray to solve the problem. But view of ICC extracts report (the finales paper explains examples of reports) but one of organization using ESIM to analyse log file this tools is very useful.

6- In case existence Trojan hour's viruses of ICC study proved (62%).the observation of researcher most ICC do not learn viruses and type of viruses and how to solve this problem.

7- The study of interview questionnaire proved (50%) from ICC using Kaspersky to main anti viruses .the research observations that is very dangers, because is not full protection all type of viruses

8- Analysis of the interview findings to a positive relationship between the amount of network components and the methods used to keep them in terms of software and physical. It is the view of observation researcher has to be a

balance between works needs and network how to provide adequate protection to them.

9- Most of the institutions, the Sudanese government does not hold the centres of confidential information because it does not hold the concept of secret information in full plus they had lost to the possibilities of the material and practical expertise in secret. secret operations is one of the main centres which must be available at each institution because its way is maintained on any component of network components from threats both internal and external in this research we are going to learn how to set up the centres of confidential information and therefore has been the work of a questionnaire interview on the way is to collect a range of information about threats and hacker and viruses that are experiencing any network and components and appropriate ways to solve them and alternative solutions and through result that have been reached it became necessary to establish a centres of confidential information with a high specification and look depending on the researcher must use all of the programs and scientific expertise, and the place is equipped with the tools and programs that are related to the confidentiality of the selection of the best control methods such as MTGR.

4.4 Optimal design

Through information gathered from the questionnaire has been reached on how to design general a secret operation centres. Design that the annexation of this design and the overall shape of the basic steps that must be followed and tried to cover all the required confidentiality requirements that must be available in the centres of secret information.

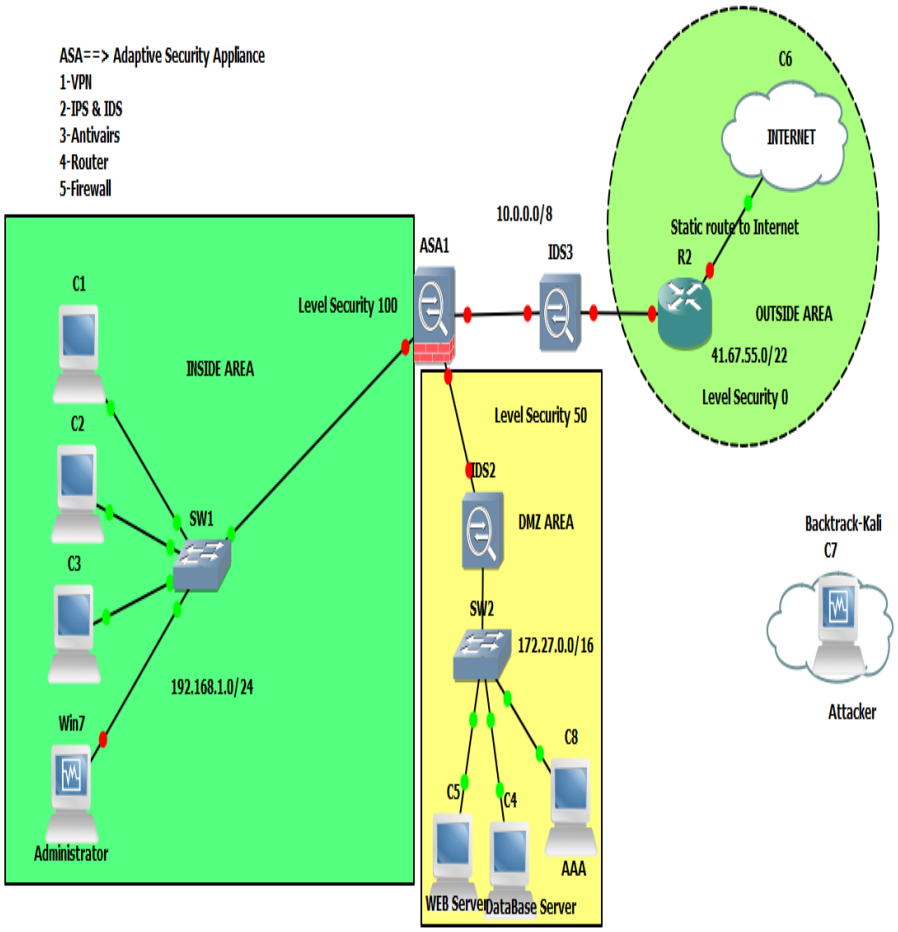
Design the security operation centres is very complex and needed many employee in different jobs and high experience because the network exhibition group of hacker, virus and threats.

The figure below illustrates the optimal design of the security operation centres using all security available to help to protection physical and logical network the below steps concerned how to design security operation centres in Sudan university of since and technology,

And figure concerned the network and how to protect by using some devices:

- To design security operation centre must be type of university and understand all concepts of network.
- Using the strong physical and logical design.
- Using all software and hardware to protect the device.
- The above design using to any tools of monitoring and controls of the data. And how to control internet link to enhance the viability of using internet enhance the performance network which indirectly prevents the campus

form traffic congestion.



Figures [4:12] security operation centres optimal design

- The above figure of security operation centres must be include the network devices to communication then another network to exchange the information to or to browsing or upload and download to internet according to pervious reasons must be the network content network administrators to management all devices in network and using strong tools to protection the network like ids (intrusions detection system).this figures concerned the levels of security this level to using to manage the security example security level =100 explain any user outside the network using level of security =100 and save in the

routers but the level security =0 explain the all interface or user inside the network this users must not allowed to the network .This design suitable for university according to interview questionnaire because all university content information security and always using the internet. Internet speed for each college management division creates a kind of Internet availability, quality and performance of the network

4.4.1. Optimal design according to the organization type:

Through information gathered from the questionnaire has been reached on how to design a secret operation centres to any organization or environment (government organization, industry organization, university environment) the following paragraph explain how to design security operations centres.

4.4.1.1 Enterprise environment or decision environment

In all institutions and all environments, information is a very valuable source, and must be protected from all risks. The three environments of choice in this research is the government, educational and industrial environment, because these environments is very influential environments in the communities and the economy and in the culture of Sudanese society, and hardly represents the basic infrastructure of the state. In this paragraph, we review some of the qualities of these environments.

4.4.1 .1.1The first educational environment

The learning environment can be divided into conventional environment and electronic environment. The conventional environment consists of traditional buildings, lectures and students in addition to the database. All of these components are fixed place thereby reducing the threats insurance. For example, a student must have a unique number to enter its exam, and only study for students sitting for the exam and who have to pay the tuition fees have been given them

numbers The recent years have seen a major shift educational environment with the development of technology.

This development has helped to add e-services to the educational environment

4.4.1 .1.2 State Environmental of more environments

environments allergic, since they must provide full security to any government institution to ensure the safety of all the assets that are the institution, and within these assets information as it is an important component of the government institutions components, as they are dealing within these institutions to exchange information between the different actors if this information is computerized it was very easy to violate them and attack to steal, modification or denial or other types of attacks. Since this information is highly sensitivity violation may lead to the death of a person or being imprisoned for a long period or lead to significant or financial loss that could lead to war between the two states, we need to secure this information full insurance, and this is it clear to unless the use of standards to make sure information security and insurance system on government establishment. It can be considered that the primary purpose of government institutions is to achieve informatics at the government.[21]

4.4.1 .1.3 Industrial Environment

The industry is to transform the raw material utilized to crafts, as any manufactured goods pass through several stages of the deportation of raw materials, storage and quality check to become suitable for use as a commodity by the consumer. Because of the abundance of technology in recent times and the importance of the use of technology in all areas, it has become important to use information technology in the industrial environment, since they must provide information correctly in all stages of manufacturing.[21]

4.5 Tools available

One of the important factors to determine the appropriate security standards is having tools that help in the measurement process, and this goes back to the decision-maker you can provide the right tools? Stimulation of these tools (Tripwire Tools), detection of network architecture tools (Nmap), r. And also the safety analysis tools as well as documents and charts on the Foundation, which helps the good knowledge of the system and calculates the costs and others. For example, If possible, use the Nmap His decision can be obtained sufficient information on the network structure and the Ports in the network and thus can use the access counter

Groups of guides or steps or decisions that may be taken in charge of the institution insurance system to design security operation centres to any environment:

First resolution: the use of physical and logical design methods.
The second resolution: follow or improve insurance policy.
Resolution III: improving existing security controls of the institution or recurrence.
Resolution IV: Adding a new security controls.
Resolution V: improving risk task and process management.
Resolution VI: develop laws to punish the attacker or modify previous laws.
Resolution VII: follow the correct legal procedures.
Resolution VIII: implementation of laws to punish the attacker.
Ninth resolution: To provide advice and increased training.
Resolution X: Use the ways and programs to monitor and analyze network.
Decision atheist ten: operates 24 X 7from central offsite locations.
Resolution XII. The use of tools and software control.
Resolution XIII: Use tools of monitoring and follow-up data.
Resolution XIV: providing tools before the implementation of decisions.
Decision XV: reduce the financial cost of implementing the right decisions at the right time.
Resolution XVI: the use of firewalls

Resolution XVII: Use policies to control the bandwidth.
Resolution XVIII: the use of global calibrated to maintain the confidentiality of the information. Resolution XX: using SIM/SIME/SEM tools

Resolution XX I :identified type of data centers or CTI OR CC

Resolution XX II: using devices IPs and IDS

After that must be determined some algorithm or policies and tools using to manage and control the bandwidth the following steps or explain this:

First policy: using dynamic bandwidth or share bandwidth

Second policy: using quota system

Third policy: using max min algorithms to distributed bandwidth

According to above decision and polices to management bandwidth to help to design security operation centre must be Classification of these environments by the appropriate decision for design security operation centres the following table explain this classification:

(Table 4.11) classified or Organization environments of soc

Organization environments	decision for design soc
Educational environment	First resolution+ Resolution VII+ Resolution XVIII+ Resolution XIII+ Resolution XVII+ third policy
State Environmental	First resolution+ Resolution III+ The second resolution+ Decision XV+ Ninth resolution+ Resolution XVI+ Resolution XX I+ Resolution XIII+ Resolution VI+ Ninth resolution + second policy
Industrial Environment	First resolution+ The second resolution+ Resolution IV+ Ninth resolution+ Resolution XII+ Resolution XIII+ Resolution XIV+ Resolution XVII+ Resolution XX + Resolution XX I+ Decision atheist ten + first policy

Through information gathered from the questionnaire has been reached on how to design a secret operation centres to any university the following.

4.6 Implementation to management bandwidth

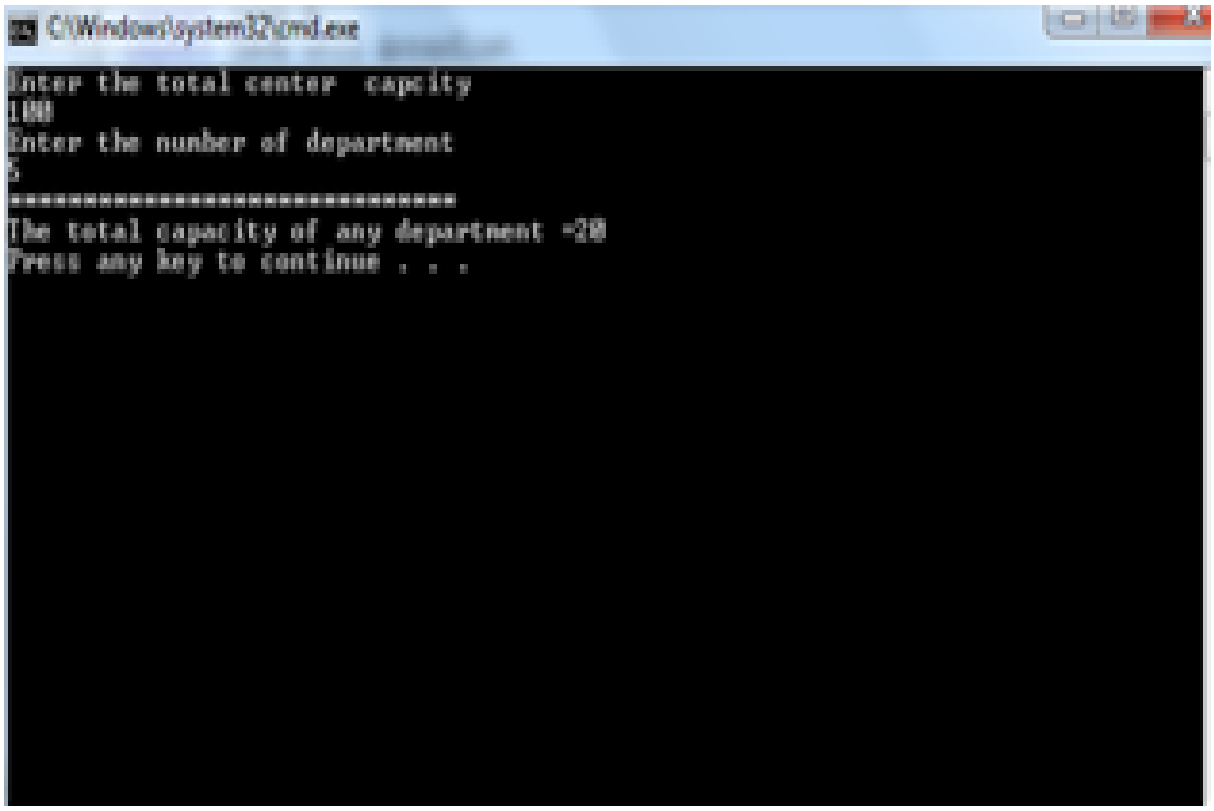
Bandwidth defined as the volume of communication between your website and other sites of your network [22]. It is clear that the more simple things that reduces the limited bandwidth. After all, what could be the service provider is doing that Is provided the frequency domain to the extent allowed by the Internet service provider, the Internet is not a good privacy to everything, it is a tangle of millions of computers connected to the network, and each party to the communication may be big or small Depending on each party equipment[23].

No matter how small or large telecommunications service provider that may ultimately determine the size of the h frequency domain available to the user in the future project on the Internet. And on the service provider that has the scope of a sufficient bandwidth to serve your purposes own, as is the rest of the customers in this will be to know the total capacity used by the user compared to the capacitive available to him in the network**.**

4.6.1 System implementation to distributed capacity

In this section explain how to management and distributed the capacity of bandwidth Using four algorithms concern in the following figures.

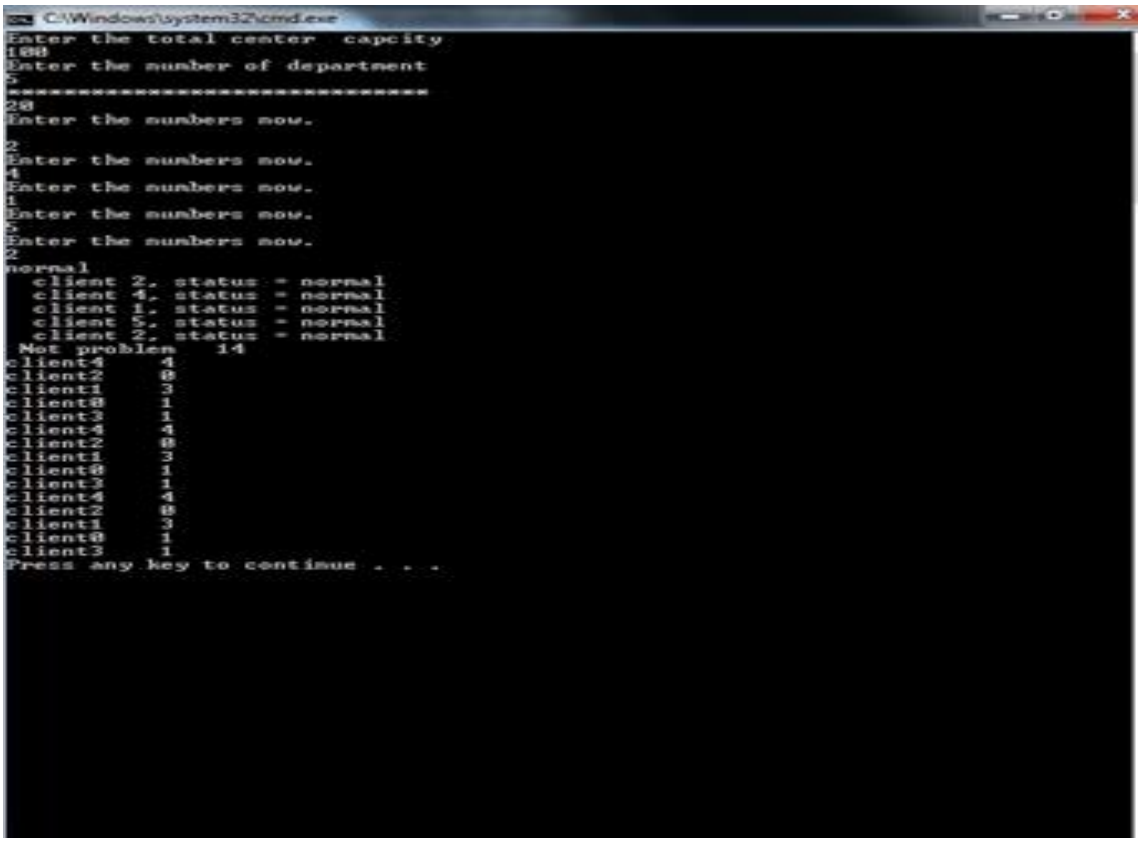
The below figures explain how the centre distributed bandwidth of any department in the university by identified the number of department divided by total of capacity.



Figures [4-13] Centre distributed capacity

In the above algorithm concerned total capacity in data centres and how distributed faire by using easy algorithm applied to distributed capacity.

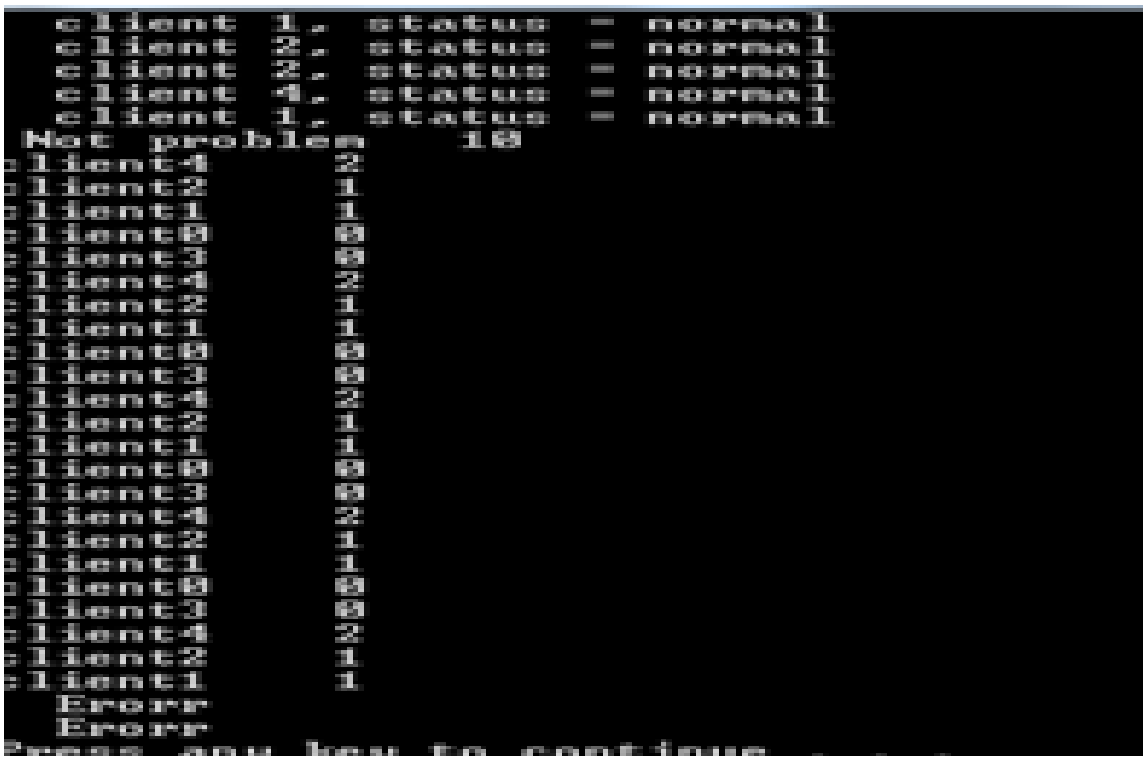
The below figures explain the Department distributed bandwidth Based on the total capacity, which was given to him by the Centre.



Figures [4.14] Department to distributed capacity

This algorithm explain how to distributed capacity bandwidth the begging calculate the total capacity of all users if the result over the total capacity after that applied algorithm the maximum algorithms to set capacity and using mathematical function (decrees by 1) this function is more efficient because failures distributed capacity bandwidth un all computer network. In this algorithm using priority because help to fair distributed.

The below figures explain the faculty distributed bandwidth depended the total capacity of department.



Figures [4.15] Faculty to distributed capacity

This algorithm explain how to distributed capacity bandwidth using the maximum algorithms to set capacity and using mathematical function (divided by 2) this function is work after sum all any faculty if the result over the total capacity of department after that applied the above algorithm. The department distributed algorithm is more efficient than faculty distributed algorithm because easier and more fair distributed.But this two algorithm is simple and essay to use to allocated capacity bandwidths.

4.6.2 Users control distributed capacity

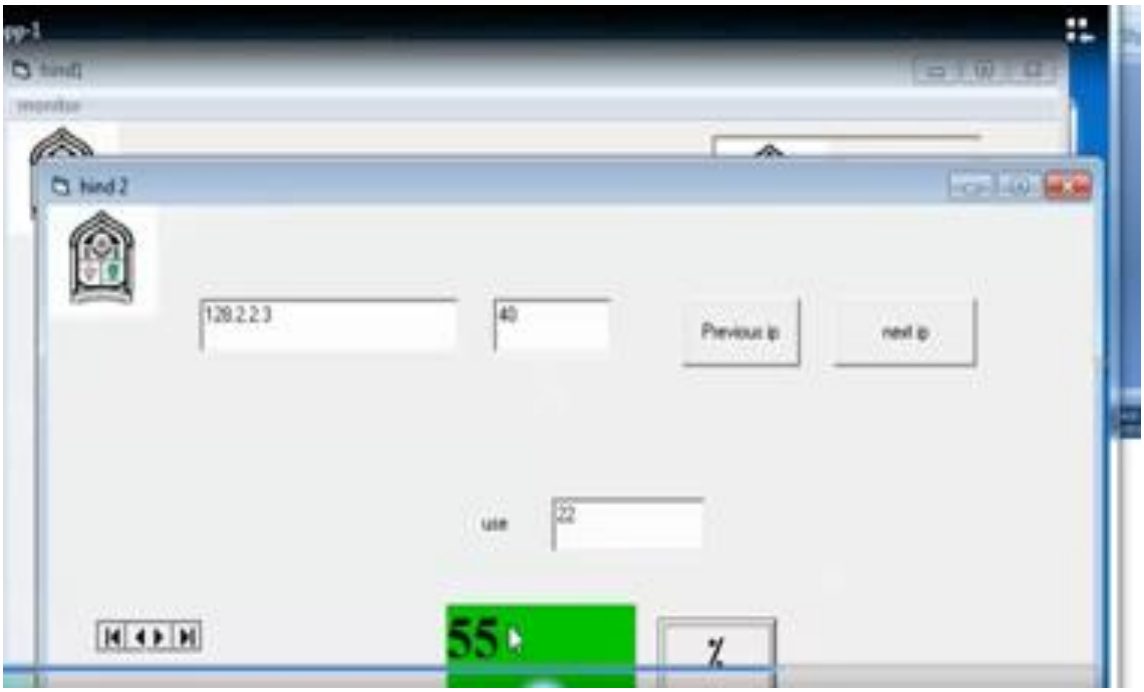
This section explain how the user in the facility of any university self control the bandwidths because to use the all bandwidth provided by administrator .the user using program to calculate capacity to use weekly or daily. This monitoring important to user management bandwidth. All figures concerned how the users in network monitored self the bandwidth because to manage the internet link capacity.

The flowing figures concern how the first step to monitoring capacity by inter IP and total capacity user.

Figures [4.16] Interface to enable the entry of IP

After the save all users in the data base using form include text to enter really user usage capacity because to calculate the percentage in total capacity.

After click the monitoring button appear form explain IP address and capacity of bandwidth and filed to inter real capacity usage. The flowing figure explain this



Figures [4.17] normal percentage of rely user usage capacity

Figures [4.18] percentage of low capacity in all capacity usage to system

The percentage 55% in green colour concern the capacity use of according to use and the totals of capacity and the green colure explain normal usage.

The below figure also concerned the percentage of relay user usage capacity

Figures [4.18] normal percentage of rely user usage capacity

The percentage 2.5% concern the capacity use of according to use and the totals of capacity and red colour explain not normal usage because don’t usage the capacity this indicator some problem.

Chapter 5: Conclusion and Recommendation

5.1 Conclusions

The focus of this project is about how can we build an optimum secret Information Centres with high internet link availability according to fair bandwidth allocation.

The design Security operation centres is very complex because of the integration and implementation of individual modules. In this thesis, using interview for data collection from different organizational, governmental, and institutional networks has been done, analyzed, and finally, a set of recommendations has been proposed for the optimum design of security operation centre. The other part of this thesis is concerning with the availability as one of the strongest security requirement via the fair bandwidth allocation among faculties, departments as well as users. In this thesis to control the bandwidth and extract the usage ratio. Thus the total link capacity of the original internet link this is distributed in an effective way. The allocation of bandwidth will be enforced according to the assumed capacity. Among the benefits of this project it turned to the director of the organization do not need to increase bandwidth at a time because of the bad use of users and other benefits such as fairness too. Moreover, the good side of this implementation is that it can help users to adapt themselves automatically by reducing traffic by the mean of self-adaptation. The outcomes of the results shows distributed and fair allocation of bandwidth consisting of three algorithms ensure the fairness control by seeking for the abnormal users. It starts by firstly punishing the faculty to control the link to

the ISP, and then secondly every faculty, punishing the departments, and finally, the department will directly punish the user.

5.2 The Recommendation of the Study

After the outputs and presenting of the result in the previous sections the researchers presents in this section recommendations of this study as in the following points:

1. Enhance and well prepared infra-structure specially building.
2. Implement modern & strong security access control.
3. Obtain the security tools from the original resources such as Anti-Viruses.
4. The ICC needs to apply special monitoring of system to decreases prevent the dangers of viruses and hackers.
5. All ICC must be using analysis software to analyses log file and explain result by report.
6. Administrators and authorities must educate the users so as increase their awareness regarding the security issues.
7. Design Centres secret operations not easy, requires a large group of employees with high expertise in all disciplines so it has to be the top choice of programs and services for the establishment of this centres and through this research was concluded that the use of all methods of protection, of the work to develop policies governing the powerful example (active directory) and excellent infrastructure for the network and the use of surveillance programs such as (VLANS) and control and monitoring programs such as (MTRG) well as the use of log file and use software to analyses such as (SEIM). If there was integration between all

these groups will be centres for information confidential high level to maintain information on the entire network and the network of both internal and external threats

8. Add to the system administration priorities such as users, teachers and students so that people can be punished with a lower priority.
9. Develop Android application for this system with some renovation to be available for regular users to monitor and manage their own Internet packets.

References

1. Daliri, S., *Feasibility of creating SOC in Agricultural Bank of Iran.* 2015.
2. Gaumnizt, W., *Controls and Safeguards.* The Phi Delta Kappan, 1939. **22**(4): p. 155-157.
3. Sim, L.O., et al., *Network resource monitoring and measurement system and method*. 2008, Google Patents.
4. Islam, A., *A. Net Framework Approach for a Network Monitoring Tool.* International Journal of Computer Applications, 2012. **55**(10).
5. Crow, B.P., et al., *IEEE 802.11 wireless local area networks.* Communications Magazine, IEEE, 1997. **35**(9): p. 116-126.
6. Mahanta, D., M. Ahmed, and U.J. Bora, *A study of Bandwidth Management in Computer Networks*. 2013, IJITEE.
7. Cecil, A., *A summary of network traffic monitoring and analysis techniques.* cit, 2012: p. 10-25.
8. Bauer, S., D.D. Clark, and W. Lehr. *The evolution of internet congestion*. 2009: TPRC.
9. Jain, R. and K. Ramakrishnan, *Congestion avoidance in computer networks with a connectionless network layer, Part I: Concepts, Goals and Methodology.* arXiv preprint cs/9809095, 1998.
10. Ahuja, V., *Routing and flow control in systems network architecture.* IBM Systems Journal, 1979. **18**(2): p. 298-314.
11. Hall, J., *Multi-layer network monitoring and analysis*. 2003, University of Cambridge.
12. Rehmus, P.G., *M.(2003) The Army's Bandwidth Bottleneck.[Electronic Version] The Congress of the United States, Congressional Budget Office, Washington DC, August. Retrieved November 19, 2003*.
13. Mahanta, D., M. Ahmed, and U.J. Bora, *A study of Bandwidth Management in Computer Networks.*
14. Sandhu, R. and J. Park, *Usage control: A vision for next generation access control*, in *Computer network security*. 2003, Springer. p. 17-31.
15. Dressler, F. and G. Carle. *History-high speed network monitoring and analysis*. in *Proceedings of 24th IEEE Conference on Computer Communications (IEEE INFOCOM 2005), Miami, FL, USA*. 2005.
16. Wang, X.G., et al., *A QoS-based bandwidth management scheme in heterogeneous wireless networks.* International Journal of Simulation Systems, Science and Technology, 2004. **5**(1-2): p. 9-17.
17. Shami, A., et al., *QoS control schemes for two-stage Ethernet passive optical access networks.* Selected Areas in Communications, IEEE Journal on, 2005. **23**(8): p. 1467-1478.
18. Ge, Y., T. Kunz, and L. Lamont. *Quality of service routing in ad-hoc networks using OLSR*. in *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*. 2003: IEEE.
19. Sun, P., et al., *Programmable Host-Network Traffic Management.*
20. Fang, S., C.H. Foh, and K.M.M. Aung, *Differentiated congestion management of data traffic for data center ethernet.* Network and Service Management, IEEE Transactions on, 2011. **8**(4): p. 322-333.
21. نهج لتحديد مقاييس أمن المعلومات
22. Abrams, M. and J. Weiss, *Malicious control system cyber security attack case study–Maroochy Water Services, Australia.* McLean, VA: The MITRE Corporation, 2008.
23. Nilsson, A. and K. Fahlberg, *A complete software development process of a general report publication service implemented using Web Services.* 2008.

بسم الله الرحمن الرحيم

Sudan University of Sciences and Technology

Master Program in Information Security

Interview Questions to gather information to the thesis titled:

((Security operations centre**))**

By :

Hind Abdulla Osman

Supervised by **.Abuagla Babiker Mohamed**

Thank you so much for agree to asset in this master research, I know that you are busy and I highly appreciate your cooperation. The following questions will help me to get a better understanding about the security operations in your centre (The information you give will be in confidential and will not be used for any other purpose).

General Information:
Name of Organization: ……..
Name of Administrator……..
Qualification: ……..

Interview Questions:
1. Do you have a Computer Centre (CC) or Information Communication Centre (ICT)?
.....
2. What are the mechanisms or policies to achieve the secret?
.....
.....
3. What are the operations that must be secret in your Centre?
.....
.....
.....

4. Mention types of threats or attacks that may affect any component of the network and the methods used to solve them?

.....
.....
.....

5. What are the threats that attack or affect the planning system and the most methods used to solve them?

.....
.....
.....

6. What are the most threats in your centres and how you resolve them?

.....
.....
.....
.

7. What are the methods used to protect your centres?

.....
.....
.....

8. What are the methods used to protect the components of the network router and others?

.....
.....
.....

9. Please describe the centre architecture and topology?

.....
.....
.....

10. Please describe the network (type, security cost, network speed, band width, type of connection, transmission media, and number of nodes, number of servers, number of computer, routers, switches, and other network devices?

.....
.....

……
.
11. In your opinion what are the steps, policies or factors required for the network architecture?
.....
.....
.....
12. What are the most problems you face in the network? How do you solve them?
.....
.....
.....
13. Do you have control techniques? With said software used to control? And what are the more types of network used? (Land schools)?
.....
.....
.....
14. What are the types of viruses you have? List some of them or the most effecting in the network
.....
.....
.....
15. What are the types of antivirus software that you used?
.....
.....
.....
16. What is the software used to analyze the problems and gaps?
.....
.....
.....
17. Do you have a security log file?

.....
.....

18. What are the methods used to analyze the content of the Log file?
.....
.....
19. What are your suggestions to develop the security strategy as general and for your centre?
.....
.....

Thank you for participating in this research
The researcher