The Financial Impact of Voice over IP on the Administrative and Management Systems of the North West Provincial Government, South Africa.

BRIGETTE W. G. PETERSEN

The Financial Impact of Voice over IP on the Administrative and Management Systems of the North West Provincial Government, South Africa.

By

Mrs Brigette Wownita Guzelda Petersen

submitted in part fulfillment of the requirements for the degree of

MASTERS OF BUSINESS ADMINISTRATION

(General Management)

In the Graduate School of Business and Government Leadership

in the

Faculty of Commerce and Administration

at the

UNIVERSITY OF NORTH-WEST

SUPERVISOR: PROF. S.D. EYONO OBONO

April 2003

Declaration

I do hereby declare that this work, hereby submitted, has not been previously submitted to any university nor published, that the work is original, my own in design and execution and that all the material contained herein is dually acknowledged.

Signed: ....

Dedication

This work is dedicated to my mother, Mrs Claire Abrahams, who inspires me – to this day - through her unselfish love and complete dedication to her family. Thank you, Mom!

Acknowledgements

This work would not have been possible, were it not for the support of a number of people who acted in one way or another. It is thus with sincere appreciation that I thank the following groups of people:

1. The management and staff in the Department of Finance at the NWPG, specifically the Accountant Generals' office and the IT Directorate.
2. The Deputy Director of Networks, IT Directorate - Mr Come Laubscher and Mr Eloff Scholtz for your assistance with the bulk of the study material.
3. The management and staff of Lesedi Corporate Technology Pty(Ltd) for all your support throughout the period of study.
4. The management and staff of the Graduate School for Business and Government Leadership, University of North – West, Mafikeng.
5. Mr Graham Vorster, Duxbury Networking, Johannesburg.
6. Ms Brenda Selota, Ms Vicky Olivier, Ms Charmaine Reynecke – who helped with secretarial work.
7. Ms Maureen Ledibane from the Faculty of English, University of North – West for editing the entire manuscript.
8. My good friend Ms Lina Karangwa for your support throughout the period of study.
9. My sons Lamont, Kyle and Devon for their encouragement throughout the period of study.

A special word of thanks to Mr Dudley Petersen, who assisted with some of the technical aspects of the research. More importantly, for your encouragement and support throughout the period of study, thank you!

A special word of appreciation is most definitely reserved for my supervisor Prof. Eyono Obono, Associate Professor in the Department of Information Systems at the University of North – West, a thousand thank you's.

ABSTRACT

Study Context

Government is continuously faced with the challenge of cutting cost – be it infrastructure, operating, etc. Technology as a business tool is very evident in large organizations today. More and more companies see the value of transporting voice over IP networks to reduce telephone and facsimile costs and to set the stage for advanced multimedia applications. Voice over Internet Protocol (VoIP) is a type of technology that provides the platform for simplification of systems through IP/Convergence (transporting voice, data and video over an IP based network) and thus is a good alternative to cut costs. This study investigates whether VoIP is efficient and effective, specifically focusing on the impact of VoIP on the administrative and management systems in terms of Network efficiency, Simplification and Cost reduction in government.

Objectives

The objective of this study is to establish network capabilities and efficiencies in relation to VoIP, the impact of VoIP on the current administrative and management systems run over these networks, and what impact this has on overall service delivery of the NWPG. The study also aims at establishing the cost intent of the convergence between VoIP telephony and traditional telephony. Finally, the study aims at establishing the significance of the cost reduction factor of implementing a VoIP Solution in the NWPG.

Design

This study is mainly intrusive because the bulk of the research is through participant observation. The North-West Provincial Governments' network (Westnet) formed the infrastructure base for this study. Network redesign may be considered as an option dependant on the outcomes. The main method of data collection of the study is participant observation through which data was compiled on network traffic, bandwidth usage, and network design/layout of Westnet. Because of the theoretical and technical nature of the study, it must achieve a synergy between these spheres to be practically viable to implement VoIP. Remember, for this research to become a blue print for implementation of VoIP, it must achieve this synergy.

Interventions

Case studies, modeling experiments and other relevant documentation of the NWPG were used for data extraction in conjunction with participant observation (used to gauge network traffic data, current utilization of bandwidth, etc.) over a 4-month period. Financial data was obtained from both the IT Chief Directorate and the Department of Finance over the same period to gauge the cost of the current network infrastructure and the current expenditure. Diagrams were developed and/or adapted during the course of the study to enhance and clarify various Information Communication Technology (ICT) concepts related to VoIP.

TABLE OF CONTENTS

List of Tables

List of Network Diagrams

List of Figures

Appendix A

Appendix B

Appendix C

CHAPTER 1

ORIENTATION

1.1 INTRODUCTION

The public telephone network and its equipment are taken for granted in most parts of the world. Availability of a telephone and access to a low-cost, high-quality worldwide network is considered to be essential in modern society (telephones are even expected to work when the power is off). Anything that would jeopardize this is usually treated with suspicion (Ryan, 1999: 3).

There is however, a paradigm shift beginning to occur since more and more communications are in digital form and transported via packet networks such as IP, ATM cells, and Frame Relay frames. Since data traffic is growing much faster than telephone traffic, there has been considerable interest in transporting voice over data networks (as opposed to the more traditional data over voice networks), otherwise known as Voice over Internet Protocol (VoIP) (Ryan, 1999: 3).

Frost & Sullivan and other research firms have estimated that the compound annual growth rate for IP-enabled telephone equipment was 132% over the period from 1997 to 2002. It was expected that VoIP would be deployed by 70% of the fortune 1000 companies by the year 2000 (Ryan, 1999: 9). According to Frost & Sullivan, both these projections has been surpassed by at least 2.5% and 4% respectively.

More and more companies see the value of transporting voice over IP networks in terms of reduction of telephone and facsimile costs and as an infrastructure for advanced multimedia applications. Providing high quality telephony over IP networks is one of the key steps in the convergence of voice, fax, video, and data communications services. Voice over IP has now been proven feasible; the race is on to adopt standards, design terminals and gateways, and begin the rollout of services on a global scale (Bull, 2002: 2, 3).

Before we discuss Voice over IP (VoIP) any further, it is probably advisable to explain briefly what it is. Voice over IP is a very broad subject, however, its core is to transport speech signals in an acceptable way from sender to destination over an IP network. An Internet Protocol (IP) network is a computer network that uses the IP protocol suite to transmit information. The definition of `acceptable' depends on the particular situation we are dealing with.

1.2 STATEMENT OF THE PROBLEM

Government is faced with the challenge of cutting costs. There are many different costs incurred by government on a day-to-day basis: operating costs, administrative costs, information technology costs, to mention but a few.

Considering the fact that the e-government concept has taken root and that the budget allocation 2003 for developing the Information Technology (IT) infrastructure has substantially increased, it is clear that government is gearing itself to address the digital divide which exists in South Africa (Kuscus, 2003: 11, 14). In order to achieve the technology objectives mentioned above, the existing ICT resources should be expanded and/or merged.

Currently the North West Provincial Government (NWPG) uses different types of communication devices: telephone, internet, fax and cellular. Some of the drawbacks of using such an array of devices are compatibility and cost which are discussed in detail in chapter 5. This study investigates whether VoIP is the most effective alternative to address these drawbacks. The administrative and management systems of the NWPG will be the focus of the study. A comprehensive discussion on the rationale and the definition of the problem will be covered in Chapter 3 of this research study.

1.3 CLARIFICATION OF CONCEPTS

We need to understand the following issues: Terms of Reference, Elements of the Business Environment, the OSI and TCP/IP Reference Models and the Convergence of Systems such as IP Telephony and traditional telephony.

1.3.1 TERMS OF REFERENCE

- ***LAN and WAN***. A Local Area Network (LAN) is simply a number of computers running specialized communication software that are joined through an external data path (Wave Technology, 1998: 9). A Wide Area Network (WAN) expands this basic LAN model by linking LANs and allowing them to communicate with each other. Traditionally a LAN becomes a WAN when it cross a public right-of-way, requiring public a public carrier for data transmission (Wave Technology, 1998: 10).
- ***Star Topology***. Topology means study of geometric properties unaffected by changes of shape or size (Branford, 1989: 816). Star/hub networks connect the peripheral devices via point-to-point links to a central location. Star topologies provide architectural flexibility but can require more cable than traditional bus or ring topologies (Wave Technology, 1998: 48).
- ***UTP.*** Unshielded Twisted Pair (UTP) is a set of twisted pair within a plastic sheath. The most common use for this type of cable is telephone wire. Different types or categories of UTP cabling are suitable for different speed communication (Wave Technology, 1998: 38).
- ***UTP Cat5 Cable.*** Unshielded Twisted Pair Category 5 cable is UTP cable containing four pairs of copper wire capable of transmission of up to 100Mbps. Cat5 UTP is used for most network cabling schemes because it offers reduced noise levels and better speeds than the other categories (Wave Technology, 1998: 38, 39).
- ***Fiber Backbone.*** Fiber Optic cable is comprised of light-conducting glass on plastic fibers surrounded by protective cladding and durable outer sheath. Data rates from 100Mbps to over 2Gbps are supported at

distances of 2 to 25Km. It is reliable and secure and supports extremely high bandwidth (Wave Technology, 1998: 43). Backbone means spine or main support of structure (Branford, 1989: 49).

- ***Hub.*** A hub is a simple connection device which allows multiple devices to be connected to a single central point (Thomson, 2001: 586).
- ***Switch.*** The term switch tends to take in a wide range of device capabilities. In its simplest implementation, a switch is similar to a hub but electronically isolates each of the connected devices. Many switches also have routing capabilities (Thomson, 2001: 586).
- ***Router.*** Routers control communication between subnetworks. When data is being sent to another subnetwork, the system directs the data to the router. The router determines the path the data should take and sends the data along to the next router in the path. This continues until the data reaches its final destination (Thomson, 2001: 587).
- ***Gateways.*** Gateways provide a communication path between otherwise incompatible systems. They may provide full content conversion between two environments, such as ASCII to EBCDIC, and could be active at all layers for the OSI Model (Wave Technology, 1998: 146, 147). The OSI Model is discussed in detail in Chapter 2.
- ***Netcache.*** Netcache is a network device which simplifies data management and content delivery. Netcache appliances provide a secure architecture and advances security features to help protect sensitive information and network operations from intruders inside and outside your network. Netcache appliances enable a host of next-generation network services and applications such as remote access to business applications, on-line training, executive video broadcasts, and large-scale video-on-demand services. They reduce network latency to enhance productivity and the overall web experience for e-commerce customers, intranet users, and external suppliers and partners (Network Appliance, 2002: www.netapp.com).

- ***Collaborative white-boarding.*** Collaborative white-boarding is a form of document conferencing and performs the same purpose that a physical white would in a meeting/boardroom environment (Youngburg, 1999: 3).

1.3.2 ELEMENTS OF THE BUSINESS ENVIRONMENT

In a business environment there are different elements such as technology, productivity, management, etc. which influences the achievement of a particular businesses objectives. Some of the elements of the business environment are tangible and others intangible, however, dependent on the nature of the element, one would have to adapt to it or risk underachieving or worse, failure (Cento *et al*, 2001: 33, 34).

A tangible element of the business environment is new technology. It does not necessarily smother old technology, but sometimes stimulate its growth through development. Technological innovation originates in research and development by universities, business and government and results in new machinery, equipment and products as well as new processes, methods and even approaches to management. Technology has grown in leaps and bounds over the past 50 years and this growth should be embraced. If it is not embraced, the digital divide will grow to such an extent that it cannot be bridged (van Rensburg, 2001: 21).

An intangible element of the business environment is change. "The rate of change often has a greater effect on the environment than the direction of the change" (van Rensburg, 2001:19). The duty of management is to monitor the change to enable the organization to adopt itself and attain its objectives.

To illustrate how adapting to change and embracing new technology has assisted a large corporation to thrive in its environment, is briefly described below:

"The benefits of voice over IP impressed executives at Kanematsu's Tokyo headquarters, and in early 1997 they decided to use the technology for as much of the company's global communications as possible", says George Emmett, assistant manager for communications at Kanematsu USA and a 21-year veteran of the company (Karve, 1999: 2).

"The company chose IP telephony over other wide area transports such as frame relay and ATM because of its relatively simple implementation", says Hiroyuki Niwano, Kanematsu USA's IS manager. "IP telephony doesn't have the limitations of frame relay's physical connection, and [IP telephony is] much easier to deploy," he says (Karve, 1999: 2).

1.3.3 REFERENCE MODELS FOR NETWORKS

Generally speaking, a network reference model is a sequence of layers with protocols active at each layer. A protocol is a set of strict rules that govern the exchange of information between network computers. For the purpose of the study, two reference models for networks will be discussed, namely; the OSI and TCP/IP Reference Models for layered design (Thomson Learning, 2001: 592).

1.3.3.1 THE OSI REFERENCE MODEL

The Open Systems Interconnection (OSI) reference model is a model with seven layers that was developed by the International Standards Organization (ISO). The model only specifies what each layer should do, without going into any detail about, for example, the protocols that should be used. First, the OSI model was carefully designed and thereafter protocols were designed to fit the model. This makes the OSI model a very general one (Thomson Learning, 2001: 449, 450)).

Figure 1.1 below was developed during the course of the research to illustrate the layered design of the OSI Model.

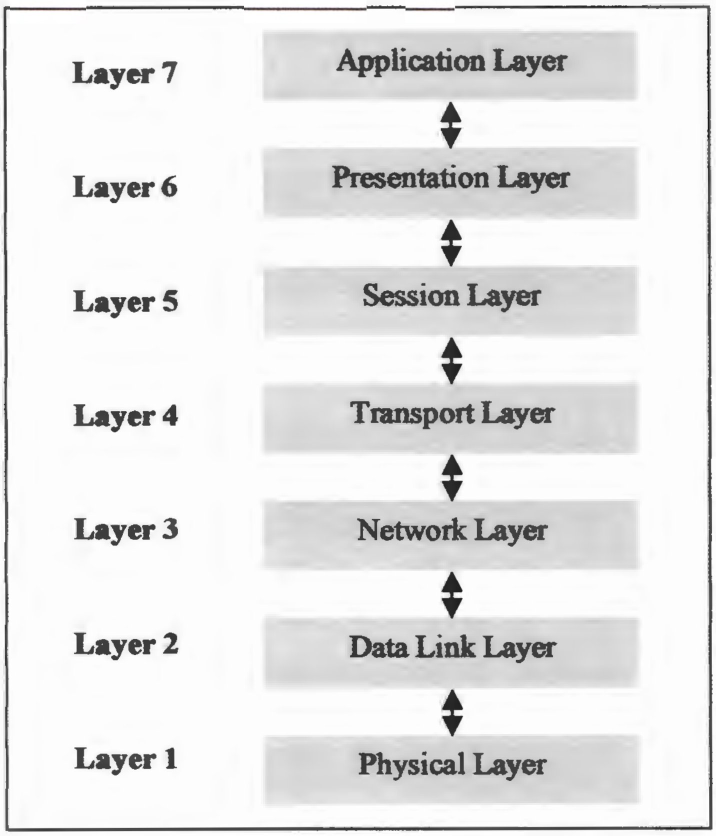


Figure 1.1: Layered Design of the OSI Reference Model

1.3.3.2 THE TCP/IP REFERENCE MODEL

The TCP/IP model was originally designed for use on the ARPANET, a US military network in the late 1960s. It is, in fact, this concept that grew out to become the Internet as we know it today. Because of its military background, there were two major requirements for the model: robustness and interoperability (Thomson Learning, 2001: 688).

Firstly, the protocols were designed to meet the requirements of the Department of Defense (DoD) and thereafter, these descriptions were provided for these protocols. These descriptions became the reference model. The TCP/IP model has become very popular and more widely used than the OSI model (Husman, 2001: 76).

Figure 1.2 below, was developed whilst conducting the research, to depict the TCP/IP layered design.

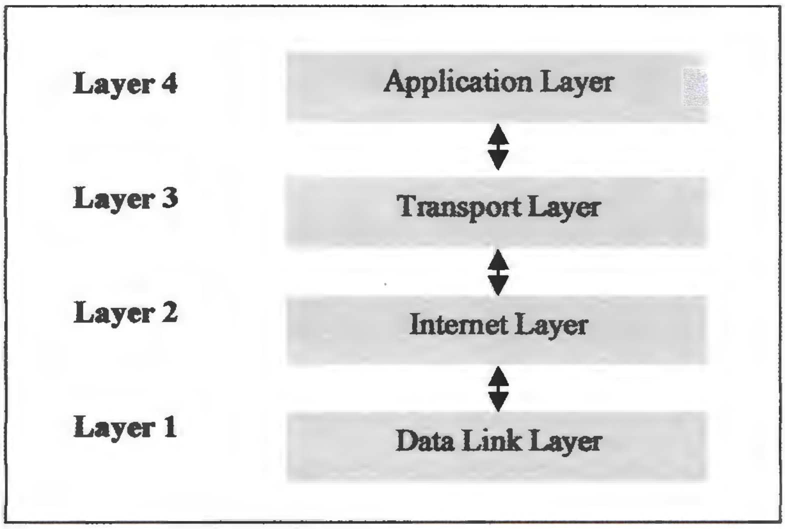


Figure 1.2: TCP/IP Reference Model

These models will be discussed in detail in Chapter 2 to explain why the TCP/IP reference model is the most suitable model for VoIP Networks.

1.3.3.3 CONCEPTS IN VoIP ARENA

Due to the technical nature of the study, one has to establish the concepts at play in the VoIP arena in relation to the purpose of the study. This would assist one to select the literature best suited to enhance these concepts. The concepts that form the basis for the literature review of this study are as follows: Layered Design, Network Software Architecture, Characteristics of IP Networks and Practical Implications of VoIP. These are discussed below:

1.3.3.3.1 LAYERED DESIGN

To facilitate the design of network software, the approach of a `layered design' is usually used. In this approach, each layer provides a certain functionality which can be used by the layer directly above. Several advantages to this approach are as follows:

- Firstly, the software is much easier to design. Trying to implement the desired functionality all at once will be very difficult and will probably result in many flaws in the programme. Furthermore, these flaws will be difficult to track,
- Another advantage is the adaptability. If one wants to make some changes to the software, for example, to correct a flaw or to improve an algorithm, one will only have to change the relevant layers of the interface while the layer above stays the same,
- Closely related to this is portability. If the layers are well designed, only a few will have to be changed to be able to use the software with other networking hardware or on another operating system, and
- Finally, since many layers will probably be implemented as part of the operating system itself, the end-user applications do not have to contain those layers. This way, the size of those applications can be reduced (Thomson Learning, 2001:17, 450 - 462).

To make communication between two hosts possible, they have to be connected to some kind of physical medium. All data will be sent over this medium, but only the lowest layer will have direct access to it. Conceptually two layers on different machines but at the same level can be thought to communicate directly. The rules and conventions that are used in this communication are contained in the protocol for that level. The whole set of protocols is often referred to as the protocol stack. For the purpose of easier understanding of the protocol stack (layered design), figure 1.3 below was developed during the course of this research study.

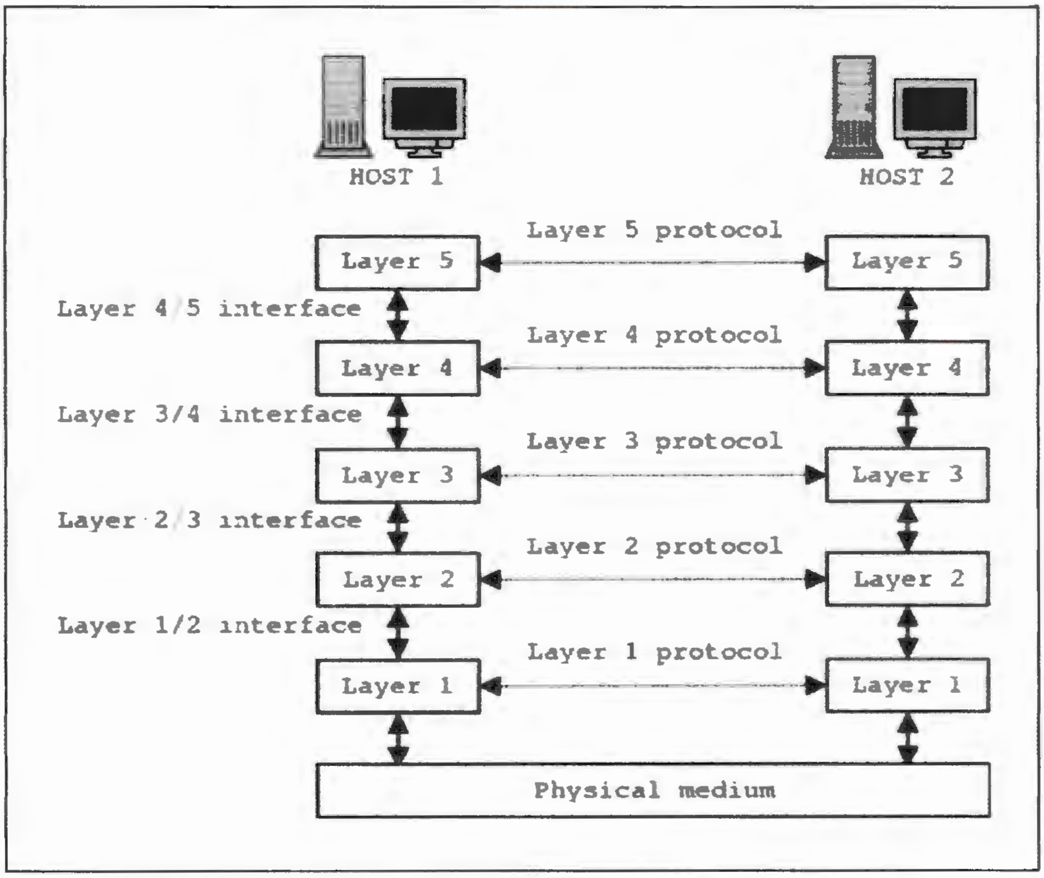


Figure 1.3: Illustration of Layered Design

1.3.3.3.2 NETWORK SOFTWARE ARCHITECTURE

Nowadays, network software is usually very structured. As mentioned earlier, there are two reference models, namely: the OSI reference model, which is a good example of a structured design and the TCP/IP reference model, in which - as the name suggests - IP plays a very important role. These two models will be discussed in detail in Chapter two.

1.3.3.3.3 CHARACTERISTICS OF IP NETWORKS

When datagrams have to travel across several networks, they need to pass through a number of routers. Each router has to examine all incoming packets and this will introduce a certain delay in the communication. Studies even show that the time it takes for a packet to reach its destination is much more affected by the number of hops the packet makes than the actual geographical distance covered (Thomson Learning, 2001: 344).

When a router gets too heavily loaded, some packets will have to be discarded. This packet loss is usually bursty. This means that for a short period of time several consecutive packets will be lost. Routers communicate with each other to dynamically adapt their routing tables to the current state of the network. This means that datagrams going to the same destination can sometimes follow different routes. Although it turns out that routes do not change very often during a transmission, it does happen. Such a change can cause datagrams to arrive out of order (Ryan, 1999: 12, 13).

Besides packet loss and out-of-order arrival of packets, it can also happen that a datagram gets duplicated during its transmission. This will cause two or more identical datagrams to arrive at the destination, possibly with some delay in between. Finally, another important feature of IP networks is the fact that when a source sends datagrams to a certain destination, the amount of time it takes to reach the destination will differ for each datagram. This is usually called inter arrival delay, inter arrival jitter or simply jitter (Ryan, 1999: 12, 13).

1.3.4 CONVERGENCE OF TELEPHONY AND NETWORK SYSTEMS

It is becoming increasingly clear that the days of the PSTN as a separate network are numbered. The implications of Moore's Law are very clear. Computing capability increases exponentially while the cost of computing capability remains constant or drops gradually. Because of technologies such as VoIP, voice can be successfully transmitted over data infrastructure reducing the need for separate networks. This convergence reduces costs, simplifies infrastructure needs and management of the infrastructure (Youngburg, 1999: 3).

Enterprise applications requiring simultaneous access to voice, video and data have created an urgent requirement for multi-service networks and multimedia system platforms. A new generation of networks that can handle all traffic equally well, provide more consistency, convenience and compatibility is emerging (Bull, 2002: 2).

IP Convergence takes advantage of the widespread use of the TCP/IP protocol in the Internet and across corporate networks. IP Convergence significantly enhances the level of network resource integration, increases the flexibility of customer interface devices, allows new types of business process re-engineering, and makes information more readily accessible. Moreover, IP Convergence allows users to maximize their in-place investment value while also leveraging the new infrastructure (Youngburg, 1999: 3).

In addition, by treating voice as another form of data and sending it over the same network as data, IP telephony enables new applications that can use the best characteristics of voice communication and data processing. These applications can include PC-to-PC connections, PC-to-phone connections, and phone-to-phone connections. Examples of applications include voice over private IP backbones and Internet or intranets', fax traffic (both real-time and store-and-forward), unified messaging, multicasting and much more (Ryan, 1999: 16, 17).

1.3.4.1 OPERATIONAL DEFINITIONS OF VARIABLES

In order to understand the variables at play in VoIP networks and VoIP systems, the core components of such networks and systems are discussed below:

1.3.4.1.1 CORE COMPONENTS OF VoIP NETWORKS

The major components featuring in network based VoIP systems are gateways, gatekeepers, PC Software phones, etc. These will be discussed in more detail later in this document. However, to create a platform for better comprehension, figure 1.4 below has been adapted to illustrate the basic interaction between these components.

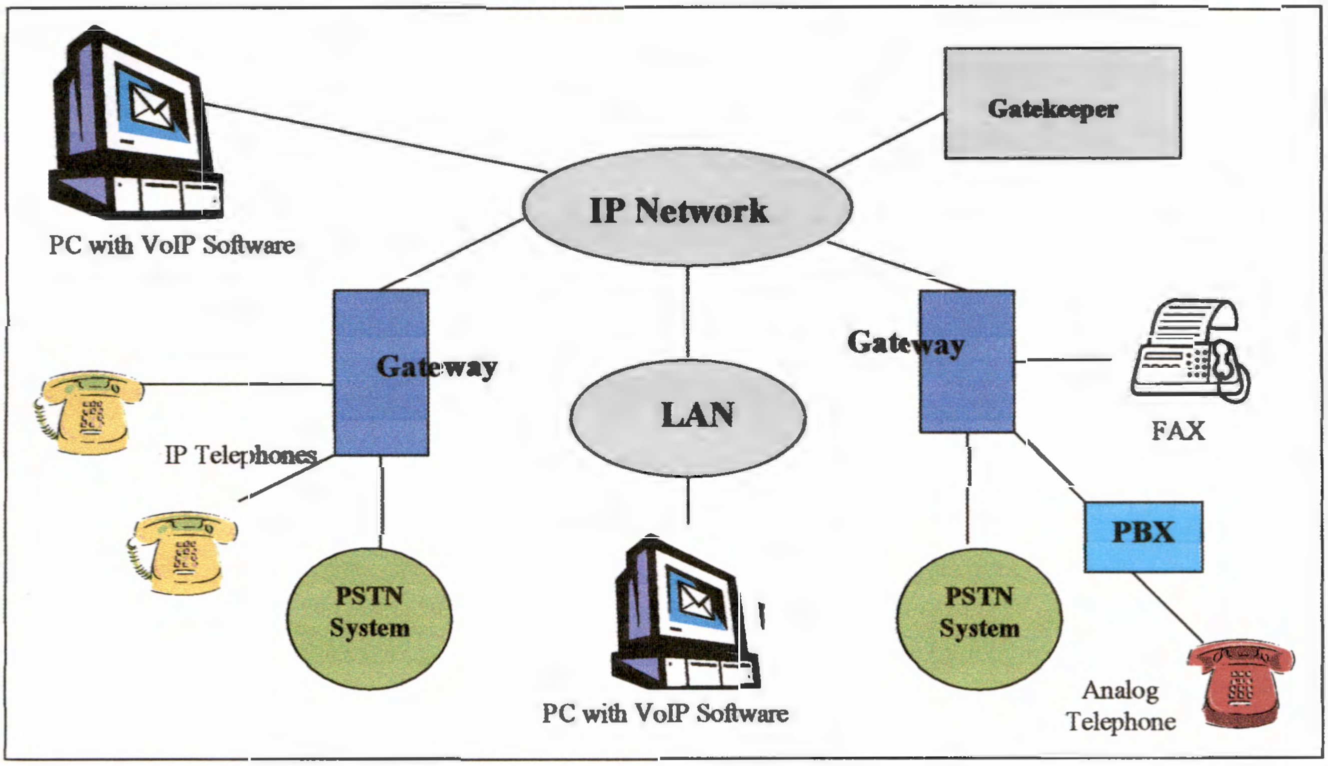


Figure 1.4: Components of a VoIP System

(Source: Black, 2000)

When using VoIP over a Local Area Network (LAN), there is usually plenty of bandwidth available and the delay between sending and receiving is usually very low.

1.3.4.1.2 CORE COMPONENTS OF VOIP SYSTEMS

The core components of a VoIP system, which are at work during conversations, are: Grabbing/Regenerating, 3D Effect (applicable to video applications), Compression/Decompression, Transmission/Reception, and Networks. These, except the 3D Effect, are the main components of digitizing sound during speech transmission (Wirbel *et al,* 1999: 2 and Ryan, 1999: 19, 20).

To illustrate how these components basically interact, figure 1.5 below was designed for easier understanding:

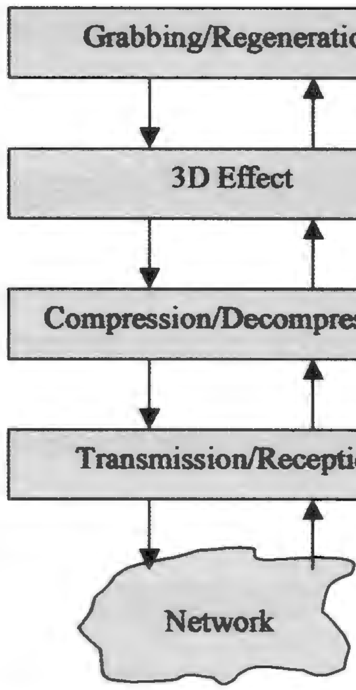


Figure 1.5: VoIP process for speech (and video) transmission

The arrows that point downward define the path that is followed when sending speech signals; the arrows that point upward define the processing sequence when speech signals are received. When the label of a box contains two items, the left one is about the sending of speech signals and the right one about the reception of such signals. They are grouped together because they operate at the same level: the right item does approximately the opposite of the left one.

Figure 1.5 above can easily be adapted for VoIP applications that are not intended for virtual environments. The only thing that needs to be changed is the

`3D effects' step. In those applications the 3D effects are not needed, so the entire step can just be left out.

All these components will be described in detail in Chapter two. This will create a general image of the workings of the VoIP system and networks, which is useful to keep in mind when delving deeper to enhance understanding.

1.3.4.2 PRACTICAL IMPLICATIONS OF VOICE OVER IP

As mentioned in the introduction, there are many applications for VoIP, e.g. Fax over IP (FoIP), IP Telephony, IP based call centers, Video conferencing, multicasting, to mention but a few (Ryan, 1999: 6, 7).

1.3.4.2.1 IP TELEPHONY

The basic concept behind IP telephony is deceptively simple: convert voice into a series of packets, and transmit them across an IP network to be reassembled on the receiving end. While theoretically simple, IP telephony designers face a number of technical challenges, many of them similar to those encountered in designing a digital cellular network (Innomedia, 2000: 1).

It should be clear that the real-time aspects of VoIP are very important. A virtual environment in which persons can communicate with each other resulting in the overall delay between talking at one end and hearing what is said at the other end should be as small as possible. All the internal calls can be made using VoIP utilities. For outgoing and incoming calls, however, there still has to be some connection to the telephone network. This can be remedied by installing a gateway that is connected to the computer network and the telephone network. This gateway will then perform the necessary signaling and conversations to make these calls possible (Innomedia, 2000: 1, 2).

IP telephony offer corporations the possibility of reducing their telecommunications expense by taking advantage of the less expensive cost structure of the Internet and ultimately consolidating network management and administration in a single wide area network (Innomedia, 2000: 2).

1.3.4.2.2 FAX OVER IP (FoIP)

Real time facsimile transmission is an immediate application of VoIP. Fax services which use dial-up PSTN services are affected by high cost for long distance, analog signal quality and machine compatibility. Instead a fax data interface unit can convert the data to packet form, handle the conversion of signaling and controlling protocols to ensure complete delivery of the data in the correct order. For this application, packet loss and end-to-end delay are more critical than in voice applications (Ryan, 1999: 7).

1.3.4.2.3 CONFERENCING

Users seek for new types of integrated voice/data applications, while managers seek for this as well as cost benefits. Audio, Video and document conferencing can be realized especially with VoIP on PC. Collaborative white-boarding could be used to make working together easier, a log book with information about incoming and outgoing calls could be kept, conversations could easily be recorded and security could be enhanced by using encryption algorithms. A microphone connected to a PC interface via a card and running software which permits voice and multimedia transfer over the internet e.g. Microsoft NetMeeting, can open up a whole new world of communication possibilities (Youngburg, 1999: 3 and Palosuo, 2000: 2).

Several other applications can be thought of. One of them is the use of VoIP techniques to create an on-line radio station, or perhaps even an on-line jukebox, where you can select the song you want to hear, which is then played almost immediately. If enough bandwidth is available, it would even be possible to add video data to all this. This way, television broadcasts and video on demand over IP networks could be made possible. In a similar way, we could extend a VoIP telephone conversation with video information about the persons involved in the call, creating a videophone application (Ucitytech, 2000: 1).

1.4 OBJECTIVES OF THE STUDY

From the above clarification of concepts, one can ascertain that VoIP holds definite benefits for large enterprises and institutions. This study seeks to achieve the following purposes for the NWPG, namely:

- To establish the to network capabilities and efficiencies in relation VoIP;
- To establish the impact of implementing a VoIP solution on the administrative and management systems;
- To establish the levels of simplification and integration of systems and what impact this has on overall service delivery;
- To establish whether there is and the significance of the cost reduction factor of implementing a VoIP solution, and
- To establish the cost of convergence between VoIP telephony and traditional telephony.

The above points will essentially be evaluated and explained with the TCP/IP Reference Model as the platform for the convergence of voice and data or Voice of IP.

1.5 SIGNIFICANCE OF THE STUDY

There are three reasons why the study is significant:

- Government is always looking for ways to cut costs – the study will establish whether VoIP is an alternative for the NWPG to cut costs;
- The convergence of systems is a very new area and Voice over IP has not yet been implemented in the public sector in South Africa, specifically the NWPG – therefore, if the NWPG implements a VoIP solution successfully

they will become the front runners in technology and information redeployment; and

- VoIP can be used as a management tool and, as such, its implementation into the NWPG could go a long way toward promoting private sector management principles into public management – this infusion will pave the way for a more effective and efficient NWPG and faster achievement of the "Batho Pele" principles (Appendix 5: 126).

As with everything, VoIP also has drawbacks for example, the cost of reconstructing a network to accommodate the needs of a VoIP system. Another drawback could be the skills needed to facilitate VoIP. Although these drawbacks exist, if effectively managed, the pros far outweigh the cons.

1.6 LIMITATIONS OF THE STUDY

Because this study focuses on the NWPG, certain information may be considered highly confidential and may not be disclosed. For this reason, assumptions may have to be made concerning these confidentialities. For example, financial information concerning expenditure may not be disclosed at all or only partially. Thus, to establish the cost benefit of VoIP, one would have to depend on trends in enterprises of a similar size.

1.7 ORGANISATION OF THE STUDY

This thesis comprises the following chapters:

- Chapter One: Orientation. Here an overview of the study with its various facets has been given.
- Chapter Two: Theoretical Framework and Literature Review. Here an attempt will be made to place the research into the context of the theoretical background and a sound technical framework to enhance the understanding of the technology and its uses.

- Chapter Three: Defining the Problem and Rationale to the Problem. Here the primary and secondary problems, the rationale to the problem and research questions are discussed.
- Chapter Four: Research Design. Here the research will be contextualised and the rationale to the research design will be discussed.
- Chapter Five: Results and Interpretation. Here the data that has been collected will be analysed and interpreted.
- Chapter Six: Summary, Recommendations and Conclusion. Here the previous chapters will be summarized and the limitations experienced during the course of the study will be highlighted. Recommendations will be made based on the findings of the study and the study will be concluded.
- References. All the literature used for the study is referenced here.
- Appendices. Documentation specifically used as a basis for analysis, data extraction and/or recommendations, are included here. These appendices will be referred throughout the manuscript where applicable.

1.8 SUMMARY

Voice over IP (VoIP) is about transmitting a voice signal across an IP network (the Internet for example). The context of this voice signal determines constraints for this transmission. However, VoIP has many other applications and benefits.

This study will explore some of these benefits and applications in detail in order to investigate the role that Voice over IP (VoIP) can play in integrating voice and data communication channels efficiently for the purpose of reducing costs in the administrative and management systems used by NWPG across their networks.

CHAPTER 2

THEORETICAL FRAMEWORK AND LITERATURE REVIEW

2.1 INTRODUCTION

Before discussing Voice over IP, it is necessary to explain what IP is. As mentioned in Chapter 1, the abbreviation IP stands for Internet Protocol and it will be discussed in detail later in this chapter. The OSI and TCP/IP Reference Models will also be discussed in this chapter. The discussion will emphasis why the TCP/IP reference model is the most suitable model for VoIP Networks.

Furthermore, Voice Communication, Related topics such as H.323 and other protocols. Finally, IP Convergence and the business environment in which large enterprises and organizations operate will be briefly discussed.

2.2 NETWORK MODELS

The two network models explored here are the OSI Reference Model and the TCP/IP Reference Model.

2.2.1 OSI REFERENCE MODEL

As mentioned in chapter 1, the Open Systems Interconnection (OSI) reference model is a model with seven layers which was developed by the International Standards Organization (ISO). The model only specifies what each layer should do, without going into any detail about, for example, the protocols that should be used.

Figure 2.1 below was adapted from figures 1.1 and 1.2 of Chapter 1, with the eye on highlighting the relationship between the OSI and the TCP/IP Reference Models:

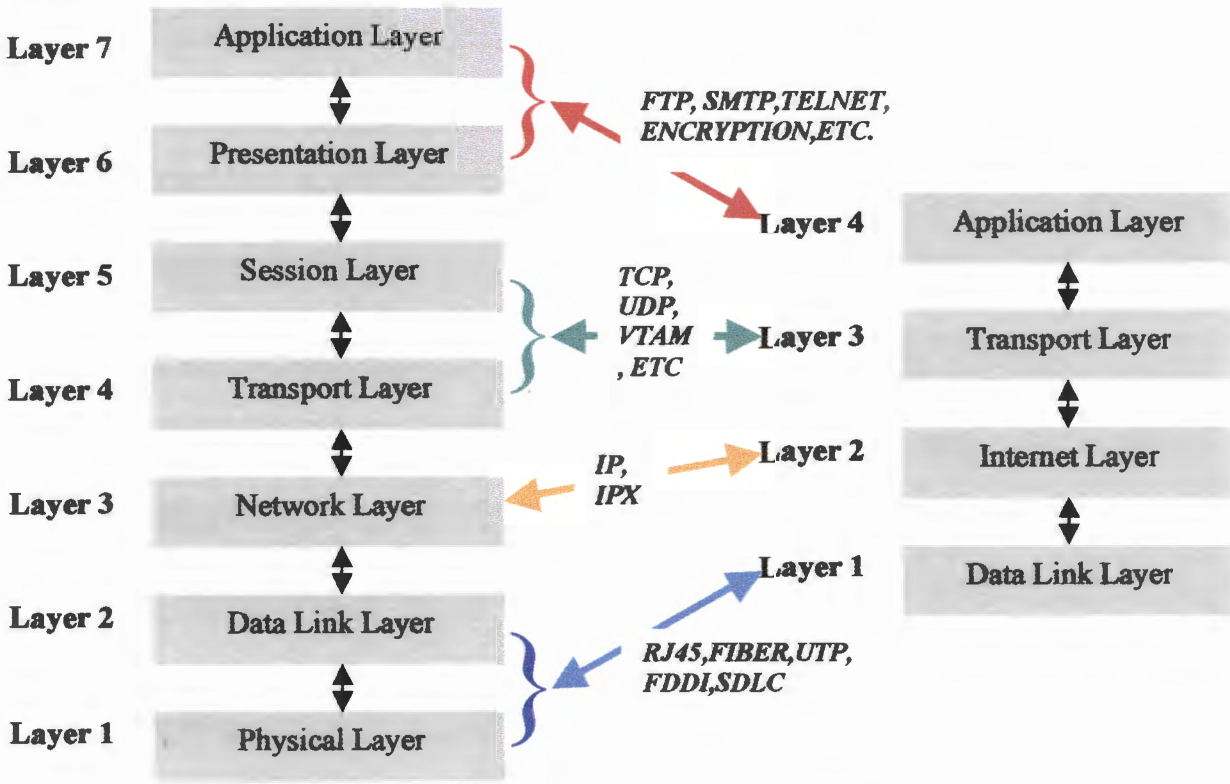


Figure 2.1: Matching OSI & TCP/IP Reference Models

In actual implementations of the OSI Reference model it turns out that some of the layers are almost empty and others are too elaborate. However, conceptually the model is quite nice and it is a good example of layered design. This is why it will be described briefly.

2.2.1.1 THE PHYSICAL LAYER

The physical layer is the lowest layer in the model and describes the physical medium which is in this case the cable, connectors, and so on. It also describes how it is attached to the network adapter and defines the mechanical and electrical characteristics of the physical medium that link the network components (Thomson Learning, 2001: 452).

2.2.1.2 THE DATA LINK LAYER

The Data Link layer specifies how devices linked to the network gain access to the various computing resources. Certain error checking and retransmission responsibilities are built into this layer. The Institute of Electrical and Electronic Engineers (IEEE) in conjunction with the International Standards Organisation (ISO), established the IEEE 802 specification series which divides the layer into two sublayers: Logical Link Control (LLC) and Media Access Control (MAC) The LLC sublayer provides software controls to manage multiple protocols that are simultaneously accessing the network. The MAC sublayer physically defines how devices control access to the network (Thomson Learning, 2001: 454).

2.2.1.3 THE NETWORK LAYER

The Network layer is responsible for establishing unique network addresses and managing the transport of information packets between networks. Firstly, it is possible that between a certain source and destination there exists several possible routes. The network layer then has to determine which one to choose. These routes can be determined in advance but it is also possible that the network layer dynamically adjusts the routing information to achieve better performance. Secondly, since the flow between adjacent networks can get very large, it is possible that a router cannot cope with all that traffic. The router then becomes a bottleneck for the data flow. The network layer tries to control such congestions (Thomson Learning, 2001: 455, 456).

2.2.1.3.1 ROUTING

The Internet layer uses the link layer to actually transmit its data. The link layer, however, can only deliver this data to hosts that are connected to the same medium. To be able to send this data across several networks, routers are used. These devices connect to several networks and make sure that incoming IP datagrams are forwarded to the appropriate network. What follows is a closer look at how this process works. Note that only the basic mechanisms of routing are explained here (Thomson Learning, 2001: 583).

When the Internet layer of the sending host has to transmit a datagram to a certain destination, it first examines the destination IP address. This is necessary because the Internet layer has to tell the link layer to which machine the data has to be sent. If the destination IP address is on the same network, the machine that will receive the datagram will simply be the destination for the transmission (Thomson Learning, 2001: 587).

If the address does not specify a host on the local network, the Internet layer examines its routing table. The entries of such a routing table can be seen as pairs of a destination address and a router address. The destination address can be an address of a host or of a network (Thomson Learning, 2001: 592).

The Internet layer then starts looking for a router to send the datagram to. To do this, it compares the destination address of the datagram with the destination addresses in the routing table. If no complete match can be found, it checks if a matching network entry can be found. If not, it uses a default entry. If an entry was found, the Internet layer takes the corresponding router address and tells the link layer to send the datagram to that address (Thomson Learning, 2001: 592).

To make sure good routes are chosen, many routers communicate with each other. They exchange their routing information and, based upon this information, each router updates its routing table to contain the best-known route for each destination. The type of information and the way it is exchanged are determined by the routing protocol that is used. Examples of routing protocols are the Open Shortest Path First (OSPF) protocol and the Border Gateway Protocol (BGP) (Thomson Learning, 2001: 587).

2.2.1.3.2 MULTICASTING

Basically, there are three transmission modes that can be used when sending an IP datagram. They are called unicast, multicast and broadcast. Unicasting simply means sending a datagram from a source to one destination. The term broadcasting is used when you want to send a datagram to all hosts on a specific network. When you want to send a datagram to an arbitrary set of hosts, it is called multicasting.

A simple way to implement multicasting would be to unicast a copy of the datagram to each destination. This method obviously wastes a lot of resources. A better way would be to transmit one datagram that is copied only at points where it needs to follow different routes to reach its destinations. This is the way it is done on IP networks. To be able to receive datagrams directed to a certain multicast address, a host must first join the multicast group associated with that address. Similarly, when it no longer wants to receive those datagrams, it leaves the multicast group. This group management is done according to the Internet Group Management Protocol (IGMP) (UCL On-line, 2002: 1).

In general, the protocol works as follows. Each host maintains a list of multicast groups from which it wants to receive datagrams. Multicast routers periodically broadcast IGMP queries on the networks to which they are connected. The hosts then send IGMP replies, containing the groups in which they are interested. Once these replies have been gathered using IGMP, multicast routers exchange this data with each other and use all this information to build their routing tables. When they receive a multicast datagram, they can then determine to which hosts and multicast routers the datagram should be sent (UCL On-line, 2002: 1).

2.2.1.4 THE TRANSPORT LAYER

The Transport layer is responsible for the accuracy of the data transmission. The network layer made it possible to actually send data from source to destination. In the network layer communication is achieved by exchanging packets. The transport layer makes it possible to consider the data as a stream of bytes and not in terms of packets. The layer itself will divide the data in smaller units and hand it over to the network layer. The transport layer maintains overall management and control responsibilities. If some packets get lost, the layer handles this and the receiver will still receive the correct stream of bytes. To enable it to keep track of which data has already been sent and which has not, the transport layer uses a connection-oriented approach (Thomson Learning, 2001: 457).

The transport layer will also have flow control mechanisms to prevent the flooding of a slow receiver and congestion prevention mechanisms. Note that the network layer also has congestion control functionality. However, the best way to handle congestions is to prevent them from happening in the first place. This is what the transport layer does. This layer is the first true end-to-end layer. The physical and data link layers were only able to communicate with an immediate neighbour. The network layer actively had to transport the packets step by step from source to destination. In this layer however, the underlying topology is transparent to its user (Thomson Learning, 2001: 457, 458).

2.2.1.5 THE SESSION LAYER

The session layer is responsible for the integrity of the logical connection of the software session. One can say that the session layer is the traffic cop of the information or data highway as a network is often referred to (Thomson Learning, 2001: 458, 459).

2.2.1.6 THE PRESENTATION LAYER

The presentation layer translates data into an appropriate transmission format. One function maintained at this layer is terminal emulation, which enables workstations using different local data formats to communicate. Other reformatting functions include data encryption and compression (Thomson Learning, 2001: 459, 460).

2.2.1.7 THE APPLICATION LAYER

Finally, the highest layer in the model is the application layer. The Application layer provides a series of definitions that are used to provide networkwide system management functions. This is the layer in which most end-user networking applications reside. To communicate, such programmes mostly use their own protocols. Examples of such applications are applications for file transfer and applications that represent a virtual terminal (Thomson Learning, 2001: 461, 462).

2.2.2 TCP/IP REFERENCE MODEL

As also mentioned in Chapter 1, the Internet Protocol is a protocol that is used in the TCP/IP reference model *(see Figure 2.1 pg 18)*. The TCP/IP model was originally designed for use on the ARPANET, a military network in the late 1960s. It is, in fact, this concept grew out to become the Internet as we know it today.

Compared to the OSI model there is a big difference in the way that the model came to existence. The OSI model was first carefully designed, and later on protocols were designed to fit the model. This makes the OSI model a very general one. The TCP/IP model however, originated in the opposite way. First the protocols were designed to meet the requirements of the DoD. Later, these protocols were described so as to form the reference model. With TCP/IP the layered design is not followed very strictly. There are some violations to this principle in the model (Thomson Learning, 2001: 688, 450 - 462).

2.2.2.1 THE DATA LINK LAYER

The data link layer is the lowest layer of the model. Sometimes it is also called the link layer or the network interface layer. The only requirement prescribed by the model is that this layer should be able to transmit and receive the IP datagrams of the layer above over the network. The layer has somewhat the same function as the physical and data link layers in the OSI model. This means that this layer is able to send data to hosts that are connected to the same medium (Thomson Learning, 2001: 452, 454, 594).

2.2.2.2 THE INTERNET LAYER

The Internet layer corresponds to the network layer in the OSI reference model. Its job is to bring packets from source to destination, across different types of networks if necessary. There are, however, no guarantees that the packets will arrive or that their order will be preserved. The service that this layer offers is therefore called a best-effort service. There is no notion of a connection in this layer. The packets that are exchanged are called Internet Protocol datagram or IP datagrams and the protocol that is used is called the Internet Protocol or IP. The datagrams consist of a header and the actual data (Thomson Learning, 2001: 455, 694, 695).

Like in the OSI network layer, intermediate devices called routers are needed to make transmission of data across different types of networks possible. The IP datagrams can then be sent from source to destination, on a hop-by-hop basis. Again, like in the OSI network layer, this also means that routing algorithms and congestion control are important aspects of the Internet layer (Thomson Learning, 2001: 456, 587, 695).

2.2.2.2.1 THE INTERNET PROTOCOL (IP)

What follows is a closer look at the Internet protocol itself and how it makes communication between two hosts possible.

First, a description of the IP packet format will be given. Next, the addressing mechanism used by IP is discussed, followed by a closer look at how packets are routed from source to destination. Finally, an explanation of multicasting, a technique that allows us to save bandwidth when the same data has to be sent to multiple destinations, is given. This is, of course, a very interesting feature when using VoIP in virtual environments, since there will typically be many receivers for each talking participant.

2.2.2.2.1.1 PACKET FORMAT

Any packet sent by the IP layer consists of an IP header, followed by the actual data. The most significant bit is the one on the left, numbered zero. The least significant bit is the one on the right, numbered thirty-one. Transmission is done in network byte order, also called big endian format. This means that in each 32-bit word the most significant byte is sent first and the least significant byte is sent last (Thomson Learning, 2001: 553, 694).

2.2.2.2.1.2 HIGHER LEVEL PROTOCOLS

As mentioned above, the two most common transport level protocols in the TCP/IP architecture are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). Each of these protocols offers a specific kind of service that applications can use to communicate across networks.

2.2.2.2.1.2.1 TCP VS UDP

Currently, TCP is undoubtedly the most used protocol of the two. This protocol transforms the unreliable packet-based service of the Internet layer into a reliable byte stream. The protocol is designed for communication between two hosts, so it only supports unicasting (Wave Technology, 1999: 110, 112).

Applications that do not require the functionality that TCP provides can use UDP. To transmit data, the UDP module simply passes a UDP header followed by that data to the Internet layer that then sends the datagram on its way. This means that, just like IP itself, UDP is a best-effort service. No guarantees about delivery are given, data grams can get reordered and be duplicated (Wave Technology, 1999: 111).

2.2.2.3 THE TRANSPORT LAYER

To make sure that multiple applications can use the network facilities at once, some extra naming mechanism is needed. The Internet layer does contain a naming mechanism to identify different hosts, but there still has to be some way to differentiate between the processes that are using the network. This is done in the transport layer by the use of a port number. This layer has somewhat the same functionality as the transport layer in the OSI model. Here also, the transport layer is the first real end-to-end layer (Thomson Learning, 2001: 457, 458).

The TCP/IP model has two major transport layer protocols. One of them is the Transmission Control Protocol (TCP). This protocol transforms the connectionless unreliable packet based service of the Internet layer into a connection-oriented reliable byte stream. It is a very important protocol since it makes reliable communication possible. This is why its name is also in the name of the reference model (Thomson Learning, 2001: 694).

The other protocol is the User Datagram Protocol (UDP). This is a protocol for applications that do not need the service offered by TCP or that want to use a protocol of their own. The UDP is merely a small extension to IP. It is also an unreliable packet based connectionless protocol and the only real extension to IP itself is the presence of a port number and an optional checksum of the data (Wave Technology, 1999: 111).

2.2.2.4 THE APPLICATION LAYER

As in the OSI model, the application layer contains the protocols of networking applications. Among these are virtual terminal applications (TELNET protocol), file transfer utilities (FTP protocol) and electronic mail (SMTP protocol) (Thomson Learning, 2001: 459, 461 and Wave Technology, 1999: 111, 112).

2.3 VOICE COMMUNICATION

In the above section, the Internet Protocol was explained. This was done in a general way, without paying much attention to Voice over IP. Since the most important features of the protocol are known, other components of VoIP can be brought into the picture. In this section, a closer look at some aspects of voice communication (conversation) will be taken.

Some of these aspects are indicated in figure 2.2 below which is adapted from figure 1.2 of Chapter 1, to illustrate the relationship between these aspects and the TCP/IP model.

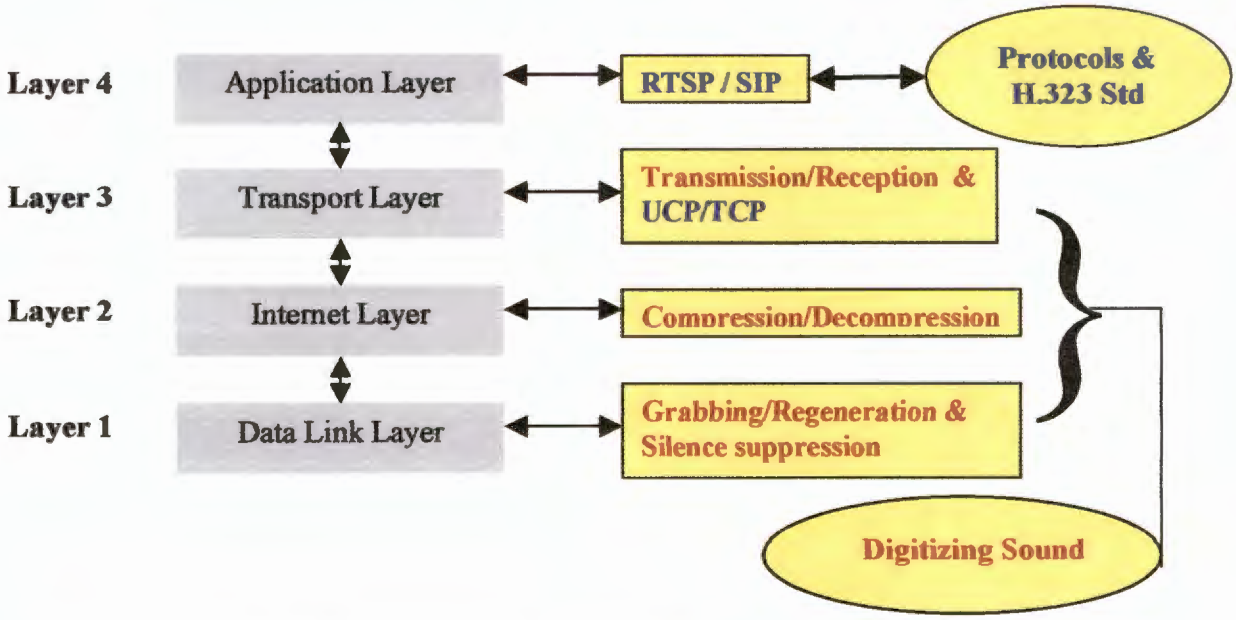


Figure 2.2: TCP/IP Reference model in relation to voice communication

2.3.1 SPEECH SOUNDS

Figure 2.3 shows the human vocal cord system and assists with the examination of types of speech sounds produced by this system.

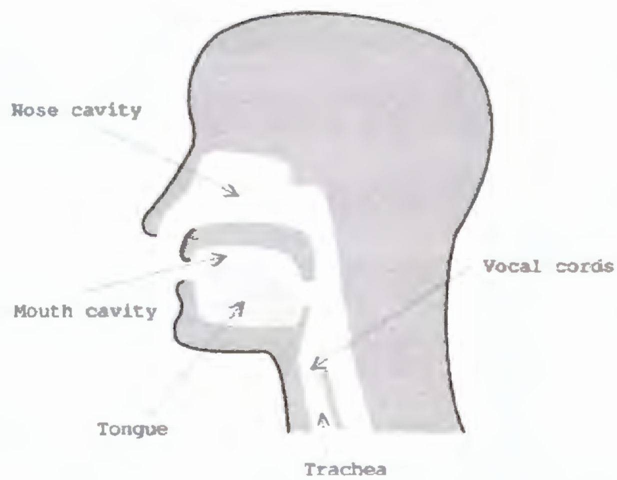


Figure 2.3 : The human vocal system

(Source: William *et al*, 1982)

Basically, there are three classes of speech sounds that can be produced namely:

- **Voiced sounds** which are created when the vocal cords vibrate open and closed. This way, periodic pulses of air come out of the opening of the vocal cords. The rate at which the opening and closing occurs, determines the pitch of the sound.
- To produce **unvoiced sounds**, the vocal cords do not vibrate, they are held open. Air is then sent at high velocities through a constriction in the vocal tract, creating a noise-like turbulence.
- **Plosive sounds** result from building up air pressure behind a closure in the vocal tract and then suddenly releasing this air.

Other sounds belong to a mixture of the classes (William *et al*, 1982: 161 - 163).

2.3.2 IP NETWORK SUPPORT FOR VOICE

A key requirement for successful VoIP deployment ia the availability of an underlying IP-based network that is capable of supporting real-time telephone and fax. As was noted in Chapter one, delay, jitter and unreliable packet delivery affects voice quality and these are typical characteristics of IP Networks. There are three different techniques (either combined or used separately) used to improve network QoS:

- Providing a controlled networking environment in which capacity can be pre-planned and adequate performance can be assumed (at-least mostly). This would generally be the case with Intranets;
- Using management tools to configure the network nodes, monitor performance and manage capacity and flow on a dynamic basis. Most internetworking devices (routers, switches, etc.) include a variety of mechanisms that can be useful in supporting voice; and
- Adding control protocols (such as RTP and PSVP used to provide better assurance of controlled QoS) and mechanisms (such as admission control

and traffic shaping used to avoid overloading the network) that help avoid or alleviate the problems inherent in IP networks (Ryan, 1999: 14, 15).

The protocols already mentioned together with others will be elaborated on later in this chapter.

2.3.3 DIGITIZING SOUND

Speech transmission is characterized by the areas depicted in figure 2.4 below (refer to figure 1.5 Chapter 1) and is discussed in detail thereafter:

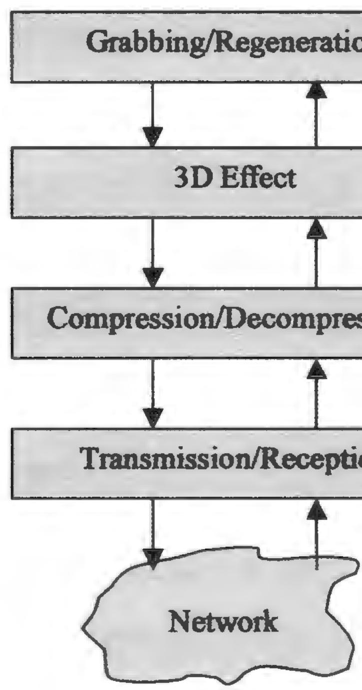


Figure 2.4: VoIP Process for Speech (and Video) Transmission

2.3.3.1 GRABBING AND RECONSTRUCTION

The first stage of the VoIP process for speech transmission is called `grabbing' of the voice signal and the second stage is called regeneration (reconstruction). In general, these stages are also referred to as analogue-to-digital (A/D) conversion and digital-to-analogue (D/A) conversion, respectively. This would occur at the Data Link layer of the TCP/IP model.

As for terminology, it is useful to know that digitizing an audio signal is often referred to as pulse code modulation (PCM). Nowadays, digitization and reconstruction of voice signals can be done by any PC soundcard, so this is not the most difficult step in creating VoIP applications. Although, it should be noted that this has not yet been perfected and some work is still necessary in this regard (Ryan, 1999: 20).

2.3.3.2 COMPRESSION AND DECOMPRESSION

A LAN may get heavily loaded when VoIP is used in virtual environments, since there could be incoming packets from a large amount of senders at the same time. If we consider a WAN, it is also not always possible to attain that rate since one slower link is enough to prevent it. Because with VoIP, unreliable protocols are usually used and VoIP can tolerate corrupted or lost packets very well, an unreliable protocol normally does not cause a bad communication quality. Furthermore, reliable protocols rely on the retransmission of packets and these retransmissions add to the overall delay (Ryan, 1999: 12).

Figure 2.5 below was adapted from figure 2.4 above to illustrate the types of delay experienced at different intervals during the VoIP process for speech transmission.

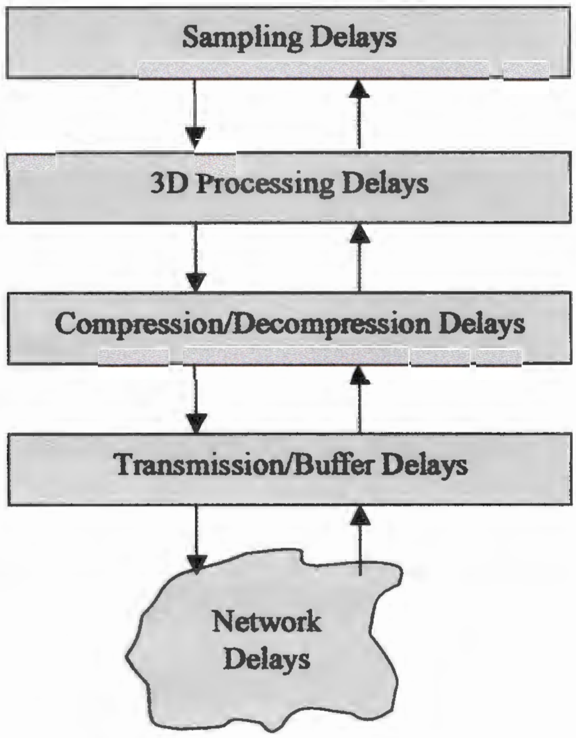


Figure 2.5 : Types of delay

There is clearly a need for compression at the Internet layer of the TCP/IP model and luckily voice information offers the possibility of large compression ratios. An important consequence of using unreliable protocols is that compression techniques can only rely on the data in the packet that is to be compressed. Compression algorithms that need information from previous packets cannot be used since it is possible that one of them did not reach the destination. This would either make decompression impossible or would reconstruct an invalid packet (Wirbel, 1999: 1, 2; Ryan, 1999: 13 and Cisco White paper, 2002: 1).

One could argue that because of the tolerability of voice communication to errors, this is not a problem. However, with such methods it would mean that one lost or one corrupted packet can create several lost packets: all those that relied on the lost packet for compression. So, unless the transmission path is highly reliable, it is probably better to avoid such compression schemes. The quality of voice compression is usually measured in terms of Mean Opinion Score (MOS). This is a value between one and five that expresses how close the voice quality is to real-life communication (Cisco White paper, 2002: 2 and Mockingbird White Paper, 1998: 12).

Figure 2.6 below was designed during the course of this research, to diagrammatically represent MOS and make it more understandable in laymen's terms.

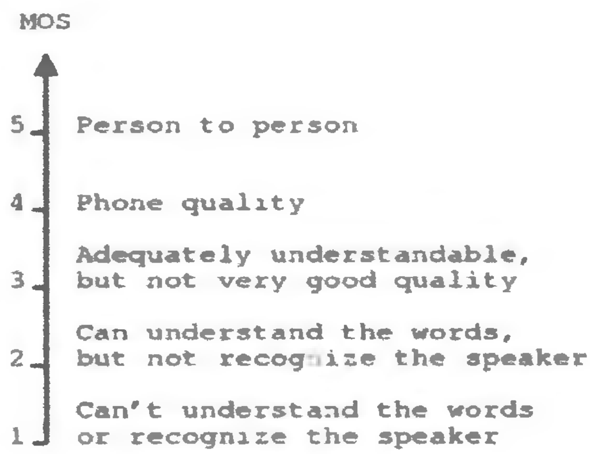


Figure 2.6: Mean Opinion Score (MOS) represented Diagrammatically

The General Compression Techniques used are: Lempel-Ziv compression and Huffman coding, to mention but a few. Figure 2.7 below illustrates how the Huffman compression technique works assuming, for example, that a file has only the five characters a,b,c,d and e which occur with certain frequencies.

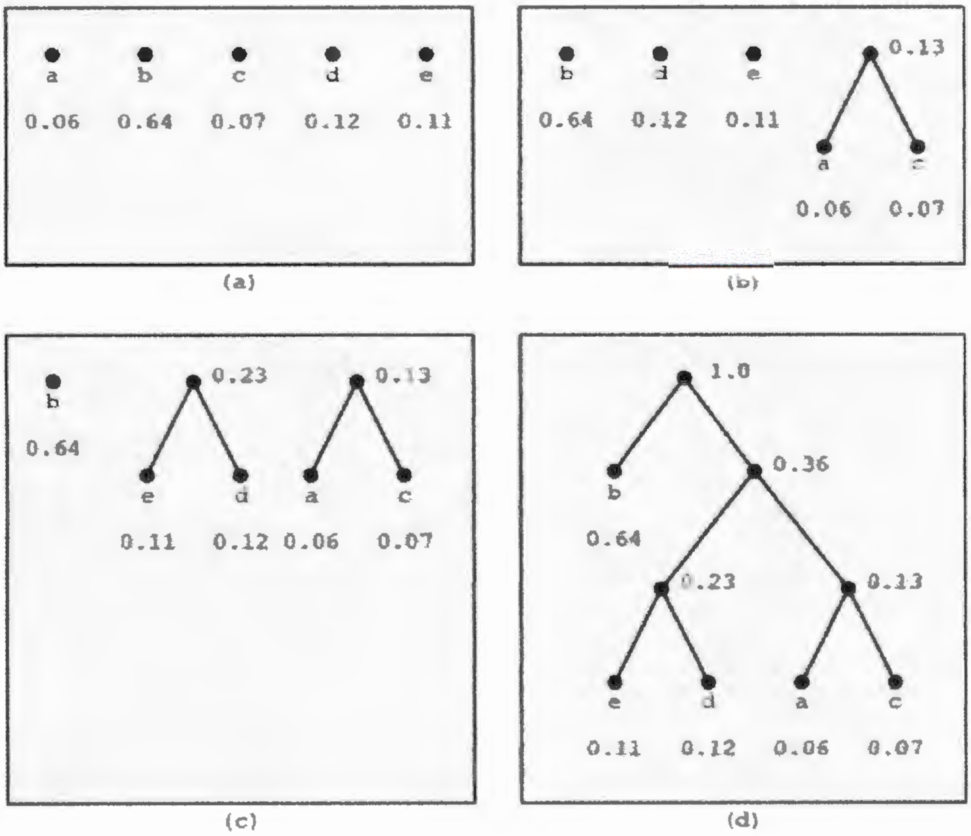


Figure 2.7: Illustrations of Huffman binary tree construction

The Huffman coding illustrated in Figure 2.7 above (developed from illustrations in Smith *et al*, 1999) is a loss-less compression techniques which mean that when data is decompressed, the original data will be restored without any modifications. The same applies to Lempel-Ziv compression. This implies that these techniques can be used for both data in general and voice information. When these methods are directly applied to voice data they do not offer very good compression ratios and for this reason compression is almost never done this way. However, the algorithms can be used as a post-processing step for other compression methods to further enhance the compression ratio (Smith *et al*, 1999:).

2.3.3.3 SILENCE SUPPRESSION

In a conversation, there is usually one person speaking at a time. In packetized voice, this gives us the opportunity to save bandwidth because packets containing only silence do not need to be sent. Bandwidth is a measurement of how much data can be carried, therefore, the greater the bandwidth the greater the data carrying potential. However, before we can discard packets, we must first be able to determine whether they contain silence or not. One way this could be done is by calculating the amount of energy of the voice signal in a packet. Packets that do not contain a sufficient amount of energy are assumed to hold only silence and can be discarded.

Silence suppression does have a minor side effect. Because the `silent' packets are discarded, there is absolutely no sound at all at the receiving side, not even background noise. This is truly a deadly silence and it might even seem that the connection has gone. The solution is to artificially introduce some background noise at the receiver side. Silence suppression takes place at the Data Link layer of the TCP/IP model (Ryan, 1999: 13, 20, 21).

2.3.3.4 TRANSMISSION AND RECEPTION

The Internet Protocol only offers a best-effort service without any QoS guarantees. For decent voice communication it is, however, necessary to have certain guarantees since too much delay or too many lost packets will seriously affect the quality of the conversation (Ryan, 1999: 12, 23).

If an application wants to transmit data, it uses certain protocol to do this. Recall that in the TCP/IP architecture, TCP and UDP are the protocols that an application can use. The Real-time Transport Protocol (RTP) is defined as a protocol that provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. So this protocol can also be used for VoIP applications (Wave Technology, 1999: 110, 111).

The RTP specification actually defines two separate protocols. The first one is the Real-time Transport Protocol (RTP), the second one is called the Real-time Transport Control Protocol (RTCP). The function of RTP is to transfer the real-time data. The control protocol supplies information about the participants in the session. The protocols are defined in such a way that they can be used on a lot of network architectures and not just on TCP/IP networks. However, if RTP is used on a TCP/IP network, it is typically run on top of UDP which usually takes place at the Transport layer of the TCP/IP model (Ryan, 1999: 15, 18).

The protocols themselves do not provide mechanisms to ensure timely delivery. They also do not give any QoS guarantees. These things have to be provided by some other mechanism. Also, out of order delivery is still possible, and flow and congestion control are not directly supported. However, the protocols do deliver the necessary data to the application to make sure it can put the received packets in the correct order. Also, RTCP provides information about reception quality that the application can use to make local adjustments. For example if congestion is forming, the application could decide to lower the data rate (Ryan, 1999: 15, 18).

2.3.3.5 VIRTUAL ENVIRONMENT (3D EFFECT)

When using voice in virtual environments, adding a 3D effect to the speech signal will create more realism. But this 3D effect can be generated both at the receiver and at the sender side. When it comes to processing delay, it makes no difference where the 3D sound is created. If it is generated at the sender side, processing will have to be done on outgoing packets for each possible receiver, since they all need a slightly different effect. If it is generated at the receiver side, processing will have to be done on incoming packets from each sender. So, the net result for these methods will be the same (Palosuo, 2000: 4).

But when it comes to bandwidth utilization, processing at the receiver side has some advantages. To create a 3D effect, a stereo sound signal is needed. This means that when the 3D sound is generated at the sender, the mono speech signal will be converted into a stereo one, which needs at least twice the amount of storage space. Consequently, when this data is transmitted, it will need at least twice the bandwidth as the unprocessed data. Furthermore, due to the 3D effect, the data that has to be transmitted will differ for each receiver. This eliminates the possibility of multicasting the data to reduce the required bandwidth (Palosuo, 2000: 5, 6).

In contrast, when the 3D sound is generated at the receiver side, the sender can distribute the mono data that is the same for all receivers. This requires less bandwidth than a stereo signal and it also allows the sender to multicast this information, making very efficient use of the available bandwidth. Note that using this approach, the receiver must somehow know the position of the sender of the data to be able to generate the 3D effects (Palosuo, 2000: 6).

2.4 RELATED TOPICS

Technology is dynamic and exciting by nature and VoIP, being a relatively new technology, is equally dynamic and exciting. It would be impossible to describe every facet of technology related to VoIP. Therefore, a brief overview of some facets that are most relevant to our focus area will be given. This also gives an added insight into the goings-on in the VoIP and related arenas.

Firstly, a description and functionality of H.323 standard and the Session Initiation Protocol (SIP) will be given, and then a comparison will be drawn between the two.

2.4.1 H.323

H.323 is an International Telecommunications Union (ITU) standard that provides specifications for computers, equipment, and services for multimedia communication over networks that do not provide a guaranteed quality of service (such as TCP/IP networks). H.323 computers and equipment can carry real-time video, audio, and data, or any combination of these elements. H.323 is supported by the Internet Engineering Task Force (IETF) RTP and RTCP, with additional protocols for call signaling, data and audiovisual communication (Karve, 1999: 3).

The ITU-T documents' recommendations for the H.323 series, is as follows:

Recommendation	Network
H.320	Narrowband Integrated Services Digital Network (N-ISDN)
H.321	Broadband Integrated Services Digital Network (ISDN)
H.322	Guaranteed bandwidth packet switched network
H.323	Non-guaranteed bandwidth packet switched network
H.324	The analogue phone system

(Source: Karve, 1999)

2.4.1.1 Functionality

End systems conforming to the H.323 recommendation can communicate with each other, either point-to-point or in a multipoint conference. These end systems may have different capabilities, but each must at least support G.711 audio encoding. Video support and other audio coders are optional. H.323 also defines how to do general data transfers, but this feature is also optional (Karve, 1999: 1, 2).

The recommendation allows communication with end systems on a different type of network conforming to other H.32X standards. This requires special devices that connect to the different networks and do the necessary conversions. Management and accounting support is also provided. This way it is possible to specify, for example, the maximum amount of bandwidth that may be occupied with H.323 calls. Accounting is provided to support billing of the callers (Databeam, 1998: 2 and Karve, 1999: 3, 4).

The H.323 recommendation defines a framework for the development of supplementary services. Currently, two such services are already defined: call transfer and call forwarding. Finally, since packet based networks - like IP networks - are often not very secure, H.323 defines several mechanisms to provide better security (DataBeam, 1998: 2, 3 and Karve, 1999: 3, 4).

2.4.2 Session Initiation Protocol (SIP)

As is mentioned above, the Internet Engineering Task Force (IETF) has also been working on protocols to provide multimedia communication. Like with H.323, the media themselves are transported with RTP, so the main difference between the approaches of the ITU-T and IETF is how call signaling and control is done. The Session Initiation Protocol (SIP) covers these functions (SIP Center, 2002: 1, 2).

SIP is described as an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. Although no real assumptions are made about the underlying network and protocols, SIP has been designed with the TCP/IP architecture in mind. Unlike call signaling and control protocols in the H.323 recommendation, SIP is a text-based protocol (SIP Center, 2002: 1, 2). It resembles somewhat the Simple Mail Transfer Protocol (SMTP) and the Hypertext Transfer Protocol (HTTP), the protocols used to transfer e-mail and World Wide Web pages respectively (Thomson Leaning, 2001: 698 and Wave Technology, 1999: 112).

2.4.2.1 Functionality

Somehow, you must specify to whom you want to make a call. A SIP Uniform Resource Locator (SIP-URL) identifies a SIP user. Such a URL looks somewhat like a World Wide Web URL or an e-mail address. An example is `sip:me@home.net'.

When a user wants to invite someone into a session or wants to make a call to someone, the user can send an invitation request to the end system specified in the destination's SIP-URL. In the above example, the request would be sent to `home.net'. If the called user is available at that system, he can send a response, indicating whether he wants to participate in the communication or not. When the caller receives this response, he sends an acknowledgement to the other system (SIP Center, 2002: 1, 2).

The invitation request could also be sent to a redirect server. This redirect server would then look for possible locations of the called user and send the corresponding SIP-URLs back to the caller. Based upon this information, the caller could then try to contact the other user directly, as described above. The caller could also send its invitation request to a proxy server. This proxy server then looks for possible locations of the other user and tries to invite that user itself. When the proxy knows that the invitation was either accepted or denied, it can send an appropriate response back to the caller. This way, a proxy acts as both a client and a server (SIP Center, 2002: 1, 2).

The invitation request normally contains information about the media that will be sent. If the invitation was successful, the response will also contain a description about the media that the other user will use. The SIP specification does not demand a specific format, but the Session Description Protocol (SDP) was designed for this purpose. Note that SIP can be used to invite parties to both unicast and multicast sessions and that the initiator of the invitation does not actually have to participate in the session. SIP also offers services to provide secure communications (SIP Center, 2002: 1, 2).

2.4.3 H.323 vs. SIP

When comparing the complexity of the two protocols, it seems that SIP is far less complex than H.323. The specification of H.323 is more extensive than that of SIP and defines a lot more elements. Furthermore, H.323 uses a binary encoding mechanism for call signaling and control, whereas SIP is text based. This textual format is easy to decode and much easier to debug than a binary representation. A part of the complexity of H.323, stems from the interaction between several components that are not clearly separated. Also, in H.323 there may be several ways to accomplish a single task and some of the functionality is present in several parts of the protocol (SIP Center, 2002: 1, 2).

Considering the extensibility of the protocols, the experience with other protocols like SMTP and HTTP has been used to make SIP very extensible: new features can easily be incorporated into the protocol. H.323 also allows some extensions, but only at predefined places within the protocol. SIP is quite modular which allows its components to be changed quite easily. H.323 on the other hand, is less modular. Since various protocol components usually need to work together to accomplish a task, it will be difficult to simply replace one component (SIP Center, 2002: 1, 2).

H.323 was originally intended for use on a single LAN. Currently, this restriction is no longer present, but H.323 can have some difficulties in detecting looping messages. SIP can be used over wide area networks without any difficulties, easily detecting loops when they occur. H.323 also has some difficulties when the conference size keeps increasing. The use of a Multipoint Controller (MC) is a bottleneck for the conference. When the conference size keeps growing, eventually another protocol will have to be used: H.332. Since SIP does not have something similar to an MC, it does not suffer from such scalability problems (SIP Center, 2002: 1, 2).

2.5 IT SECURITY

There are three steps to be considered when the issue of IT Security is raised, namely: Develop a Security Policy, Firewall deployment, and Additional Security Tools. In addition to these steps, the ISO/IEC 17799 and ISO/IEC 15408 standards and relevant South African legislation will be examined in relation to IT Security.

2.5.1 DEVELOPING A SECURITY POLICY

The first step toward developing a security policy is to do a full risk analysis. This would include assessment of the current type, path and direction of information passing through ones network to identify the real and potential holes which exists or could develop with time. During this process a number of questions would have to be asked and answered (Bryant, 2003: 2).

The second step is for network administrators and Chief Information Officers to have a complete and comprehensive understanding of Internet activity, network traffic, bandwidth requirements, protocols in use, and access requirements (Bryant, 2003: 2).

The third and final step is to take into account the financial considerations of a firewall architecture implementation and ongoing maintenance costs. Remember, the firewall architecture deployment should be tied directly to the developed security policies, which address and support the organizations objectives (Bryant, 2003: 1, 3).

2.5.2 FIREWALL DEPLOYMENT

Firewalls are an extra layer of security built in to routers to protect private networks from external intruders. When a user accesses a site on the Internet, the source IP address can be read by anyone tracking the Web. Activating firewall software at the router provides a filter for both outgoing and incoming transmissions. Access between an intranet and the Internet is controlled by the use of a firewall (Thomson Learning, 2001: 692, 693 and Langford, 2000: 35).

A firewall can be hardware- or software-based, however, the tightest security is obtained when the two options are used in combination. There are two architecture choices when deploying firewall technology: a single firewall architecture- or a multilayer firewall architecture-approach. The security policies of a particular organisation will advise an organisation as to the architecture-approach best aligned with its security policies (Bryant, 2003: 1, 2, 3).

2.5.3 ADDITIONAL SECURITY TOOLS

Because no one solution is one hundred percent secure, in addition to firewalls, other security tools or best action steps should form part of the security policy. Things such as:

- virus protection through the use of anti-virus software and specialized technologies,
- access control either through limited or authorised access or password protection,
- not allowing dial-up devices to link onto the network, and
- encryption and authentication, are but a few options to supplement the need for additional security on a network (Bryant, 2003:1, 2 and Cronkhite *et al*, 2001: 190).

Dependent on the sensitivity of information to an organization, access control and authentication take on a whole new meaning with the introduction of Biometric Systems. Biometric systems authenticate ones identity based on unique physical characteristics, such as: fingerprints, hand geometry, retinal scanning, voice recognition, signature and keystroke analysis, to mention but a few (Cronkhite *et al*, 2001: 158 – 160).

2.5.4 INTERNATIONALLY RECOGNISED STANDARDS

Some internationally recognized standards are management- and others technically-based. Standards are necessary to introduce a basis to which organizations should conform. The same applies to standards pertaining to security issues. The ISO/IEC 15408:1999, the Common Criteria for IT Security Evaluation is a technical standard. It is intended to support the specification and technical evaluation of IT security features in products. The ISO/IEC 17799:2000, Code of Practice for Information Security Management is a management standard, and deals with an examination of non-technical issues relating to installed IT systems. The ISO/IEC TR 13335, Guidelines for the Management of IT Security (GMITS) series of Technical Reports are useful as a technical supplements for security reviews to the ISO/IEC 17799 (NIST, 2002: 1, 2).

Organisations should also consider the ISO/IEC TR 15947, Security techniques for intrusion detection framework which focuses on the security principles for intrusion of computer systems by outsiders or trusted employees of the organization. Organisations can use the ISO/IEC TR 15947 as a guideline for it to establish a framework to enable a comprehensive detection system (http://www.iso.ch/iso/en/commcentre/news/2002/itintrusions.html).

2.5.5 SOUTH AFRICAN LEGISLATION

The Policy Framework for E-government, 2001 had set particular goals for achieving the correct developmental climate for governments E-government objectives. It emphasis the lack of IT security and warns that standards and architectures are not all in the IT security arena. The policy framework outlines policy recommendations for the promotion of IT security (NGSA, 2001: 19 – 22).

The National Council for Library and Information Services Act, 2001 establishes the National Council for Library and Information Services and section 3b makes provision for access to information. This Act supports the Constitution of South Africa in terms of the right to information and security (www. polity.gov.za).

With the Internet, however, the question always arises: Whose laws govern? While much of Internet law can be examining existing laws, some aspects of the Internet stretch fundamental legal concepts beyond recognition. For example, the traditional concept of location has been severely altered by the Internet. The pervasive access provided by the Internet makes for a kind of ‘omnipresence’, where all participants on the Net wherever located can be actors in any other part of the Net (Langford, 2000: 123).

2.6 SUMMARY

The Internet Protocol or IP is part of a layered architecture, called the TCP/IP reference model. The omnipresence of IP is the main reason why this protocol is a good candidate for VoIP connectivity. IP is a connectionless packet based protocol that offers no guarantees about datagram arrival. Datagrams can even be duplicated or delivered out of order. Other characteristics of IP networks are the delay introduced by routers and inter arrival jitter (Thomson Leaning, 1999: 694 and Ryan, 1999: 12).

When transmitting speech data, there are several things that we have to be kept in mind. The RTP provides extra information that can be used for synchronization within a data stream. The RTCP provides additional information that can be used for inter-media synchronization, flow and congestion control and identification (Husman, 2001: 127, 128).

In terms of communication, small packets are to be preferred since this way, a lost or corrupted packet causes a smaller interruption in the communication. The main advantages of packet-based telephony are the possibilities for silence suppression and speech compression. Silence suppression is the opportunity to save bandwidth because packets containing only silence can be discarded (Ryan, 1999: 12, 13).

The services provided by H.323 and SIP are roughly the same. However, when it comes to capability exchange services, it seems that H.323 has a much richer set of functionality than SIP. Also, H.323 has various conference control services for which SIP has to rely on external protocols. On the other hand, the personal mobility services provided by SIP are more extensive than similar support in H.323 (SIP Center, 2002: 1, 2).

IT Security is one of South Africa's biggest problems. Our current legislation does not provide a framework sufficiently pliable to infuse stricter guidelines on security issues. The risks posed to organizations information system (classified or otherwise), is great and it is growing daily. There are Internationally recognized management- and technical-standards which can act as a guide towards developing the necessary security legislation needed to regulate IT security vigorously.

IP Convergence has become a "hot topic" in the telecommunications industry for three reasons: it provides more options for companies to differentiate themselves from their competitors; it offers tools to improve the ability of people to work efficiently and effectively together from anywhere; and it uses valuable network assets more effectively, thereby reducing costs. Side benefits include greater network flexibility, increased reliability and better management control. IP Convergence changes the rules for communicating within the enterprise and with customers (Youngburg, 1999: 2).

CHAPTER 3

DEFINING THE PROBLEM AND THE RATIONALE TO THE PROBLEM

3.1 INTRODUCTION

There is a fundamental difference between a perceived problem and a real problem. Therefore, it is imperative that the problem statement in Chapter one is examined to clearly ascertain whether it is real or perceived. One should then define the problem and pose research arising out of these problems. The abovementioned issues are focused on in this chapter and are expanded on below.

3.2 RATIONALE TO THE PROBLEM

From the statement of the problem in Chapter one, one can ascertain that government is faced with the challenge of cutting costs. One may ask the question: If government is in the service delivery business (Batho Pele, 1999: 1 [Appendix C of this document)), why then do they have to cut costs? The answer is simple: the higher the cost expenditure – be it operating, personnel, infrastructure, and others. - the lower the available revenue for service delivery initiatives – be it new projects, existing projects, infrastructure, and others. This is why there is a drive within government currently to enhance their good governance efforts. This drive is clear through the introduction regulatory frameworks such as the Public Finance Management Act (PFMA), Division of Revenue Act, etc (Kuscus, 2003: 8) as well as other measures.

Although in the public sector the main objective is service delivery and in the private sector the main objective is profitability, the focus for both is to reduce their costs. If reducing costs is key, then any alternative to cutting costs should be investigated.

Technology as a business tool is a given and the business case for VoIP has been proven time and time again (Karve, 1999: 1 7 and Ryan, 1999: 3). Its cost cutting benefits are clear, but are they clear in a government environment? The South African government structure consists of National government and nine Provincial governments. None of these structures are currently using VoIP, therefore, this study may serve as a basis for implementation within all these structures dependent on their individual Information Technology infrastructure. In order to lend the study more impact, the research parameters have been set within the confines of one Provincial government, namely the NWPG (NWPG Network Diagram, 2001: Appendix C and Chapter 4: Diagram 4.1 of this document). These confines and the methodology for the study will be clearly outlined in Chapter 4.

3.3 DEFINING THE PROBLEM

Firstly, the primary and secondary problems will be discussed. Thereafter, research questions that arise out of these problems will be indicated.

3.3.1 PRIMARY PROBLEM

The primary problem is the high level of overhead costs, specifically costs related to the Public Service Telephone Network usage. For example, the costs for the 387 prefixed numbers for a 12-month period 2001/2002 stands at R 14, 907, 920.22 (see Chapter 5: Table 5.4 of this document).

3.3.2 SECONDARY PROBLEMS

The government collects its revenue through payment for services and taxes levied on the public. This revenue is allocated to various cost centers as defined in the budget (Kuscus, 2003: 11, 16). Dependent on the allocation for overhead costs for a specific period, the remainder of the revenue is split to cover the service delivery initiatives for the same period. This leads to a number of problems, namely:

- Reduced available revenue for effective service delivery; and
- Implementing technology solutions to enhance service delivery.

3.3.3 RESEARCH QUESTIONS

The following research questions form the basis for data collection and analysis:

1. What are the current fixed line and telecommunications infrastructure costs?
2. Is there a significant cost reduction factor in implementing a VoIP solution?
3. Would the current network infrastructure and equipment be able to handle a VoIP solution?
4. Is there a cost in the convergence between VoIP telephony and traditional telephony?
5. Is the network capable of handling the current and projected traffic?

3.4 SUMMARY

The South African government is faced with the challenge of reducing costs and improving service delivery. This study investigates these challenges against the backdrop of a technology solution, namely VoIP.

CHAPTER 4

RESEARCH DESIGN

4.1 INTRODUCTION

The Methodology serves as a blueprint for the establishment of the research parameters. This chapter explains the rationale behind the methodology and how the research is conducted. Firstly, the research parameters are contextualised to lend the research more impact. Secondly, the approach adopted to conduct this research is outlined within this context.

4.2 THE SAMPLING FRAME

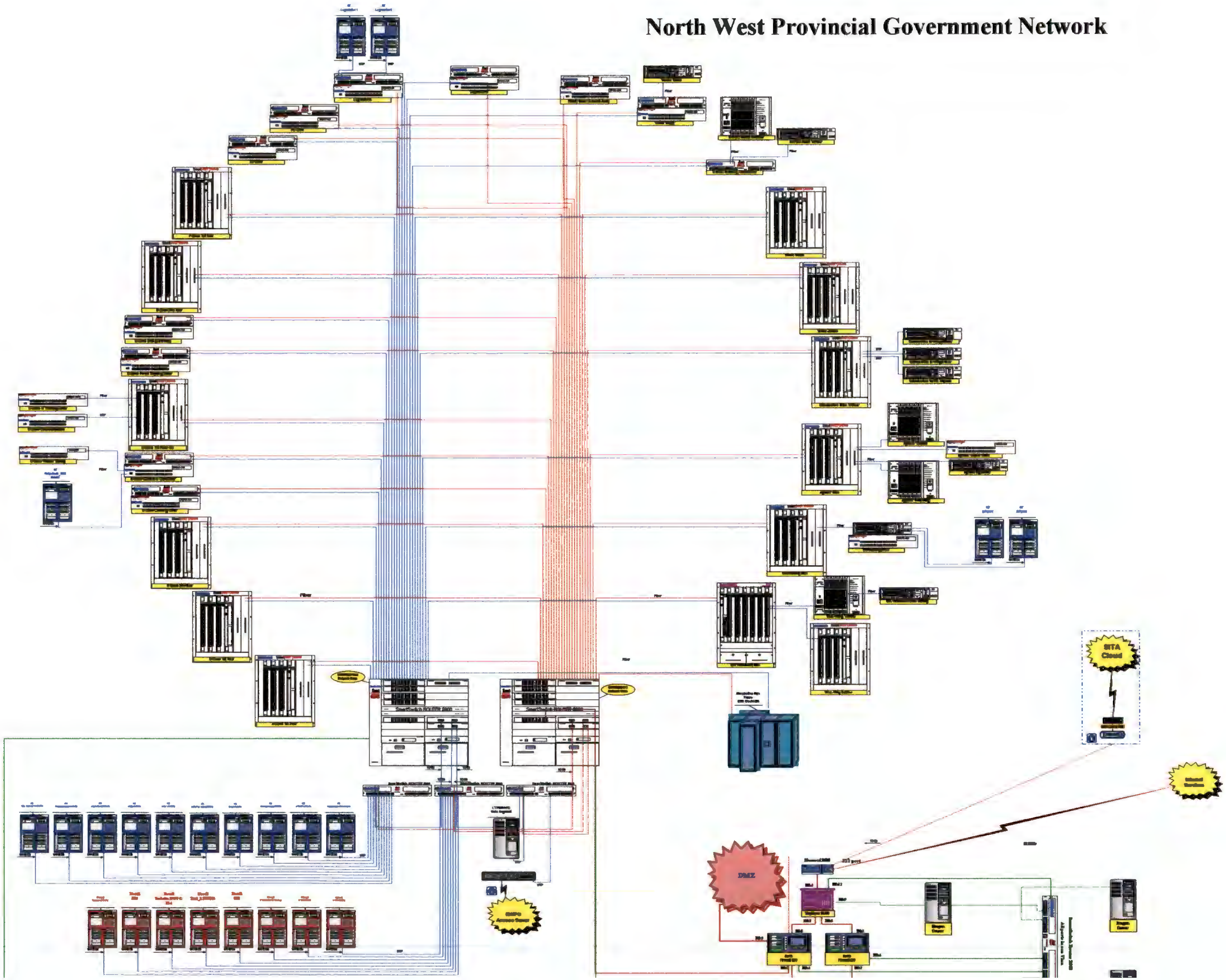
In order to establish some of the objectives of this study, it is important to contextualise the data collection parameters of the NWPG.

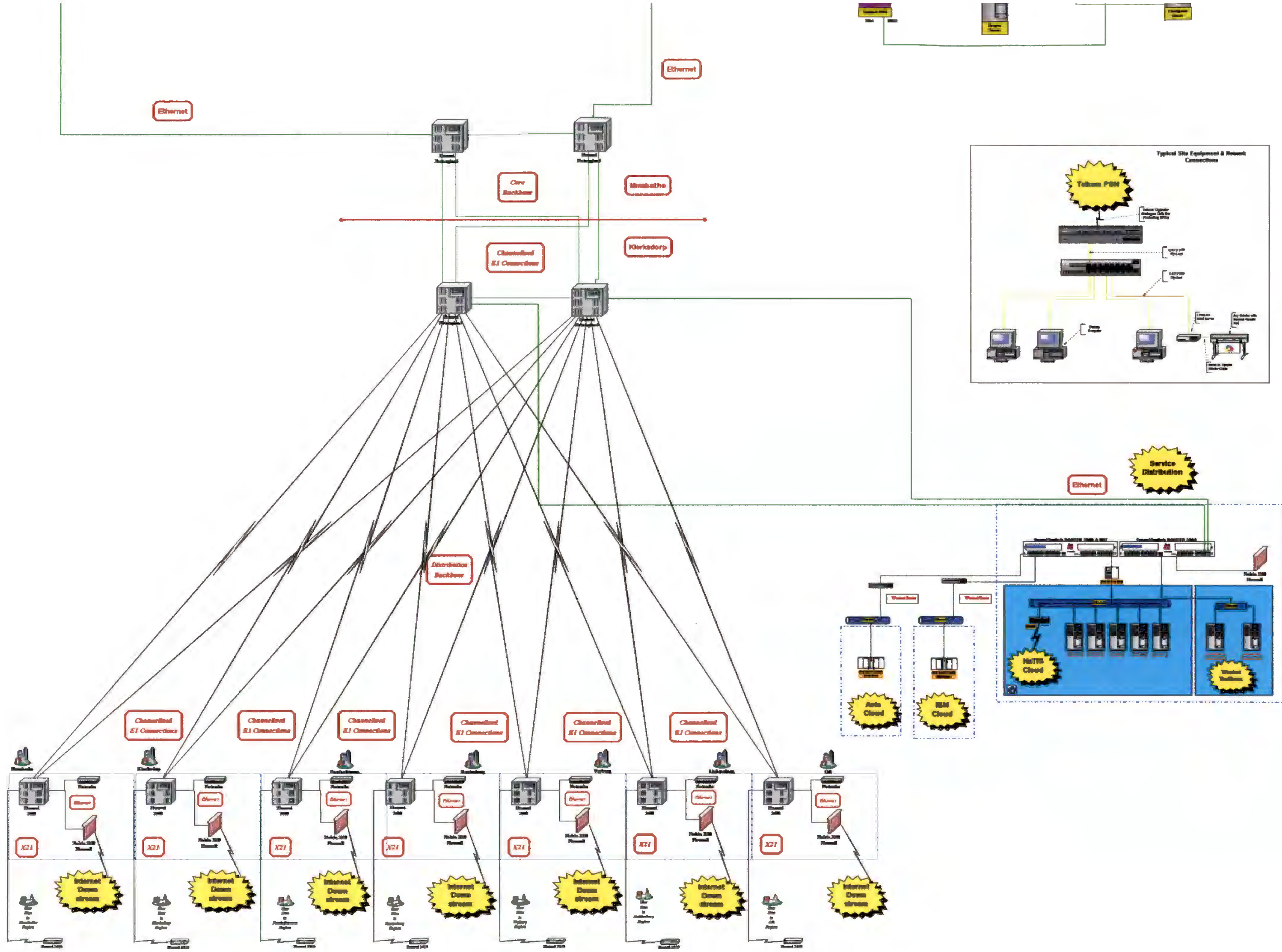
4.2.1 CURRENT NETWORK INFRASTRUCTURE

The NWPG Campus Area Network (CAN) is concentrated mainly in Garona Building with links to surrounding buildings such as Tirelo Building, Agricentre, Old Parliament, Tender Board, Gabomotso Building, ABSA Building, Kupe, etc. The CAN is indicated by the circular formation at the top half of the layout. The rea directly below the circular formation indicated to the left the NT and Novel Fileservers, to the right the Security and Netcache location and between then the Disaster Recovery area.

The NWPG Wide Area Network (WAN) consists of regional and district offices, and is linked to the CAN. The entire network (CAN and WAN) is known as Westnet of which Mmabatho and Klerksdorp distribution sites forms the Core (located at the center of the diagram and indicated by for Netengines. There are 7 Backbone sites, namely: Potchefstroom, Rustenburg, Lichtenburg, Klerksdorp, Mmabatho, Vryburg and Garankuwa (Odi Region) with an eighth distribution site (service distribution) to come on-line in March 2003. These sites are indicated at the bottom of Diagram 4.1 below.

North West Provincial Government Network




Ethernet
Ethernet
Core Backbone
Mmabatho
Channelised E1 Connections
Klerksdorp
Distribution Backbone
Channelised E1 Connections
Channelised E1 Connections
Channelised E1 Connections
Channelised E1 Connections
Channelised E1 Connections
Channelised E1 Connections
X21
X21
X21
X21
X21
X21
X21
Internet Down stream
Internet Down stream
Internet Down stream
Internet Down stream
Internet Down stream
Internet Down stream
Internet Down stream
Typical Site Equipment & Network Connections
Telkom PSN
Service Distribution
Ethernet
NaTIS Cloud
Arts Cloud
BIN Cloud

The NWPG have a fibre backbone with 100mbps UTP Category 5 cable to end user level, in a star topology. At some sites they also utilize radiolan, laser and/or wireless technology. The IT Directorate has standardized on Cabletron and 3Com network equipment such as Smart Switch Routers (SSR) and 100mbps Hubs. There is a PABX system housed at almost every site (approx. 253 PABX systems currently) and the WAN sites are linked via 64kbps diginet connections to Westnet.

Diagram 4.1 is the Network Design of Westnet and has been included to give one a better view of how the hardware mentioned above and network equipment is laid out including cabling infrastructure. This diagram is, however, very complicated and difficult to read because of the format size and the amount of information it contains. *The diagram has therefore been simplified by Petersen B, 2003 in Diagram 4.2 below and indicates the following:*

- A PBX at every site be it district offices, regional offices or other government building, linked to the PSTN system,
- At least one router at every Regional site, currently Xyplex routers are used (diagram 4.1 indicates Huawei router with a netcache and a Nokia firewall at every regional site as at the end of March 2003),
- Telephone handsets currently used are analog and route via the PBX to the PSTN system,
- There is no link between the PBX's and Westnet,
- There is only one nodal and it is located at Klerksdorp main distribution site,
- Westnet has a fail-safe infrastructure for Disaster Recovery purposes located at Mmabatho as mentioned above,
- Currently, Westnet has the following distribution indicated by $\xrightarrow{512K}$ which shows the available bandwidth. Once the Huawei equipment installation is completed at the end of March 2003, all these distributions will be channelized E1 with a bandwidth of 2mb each.

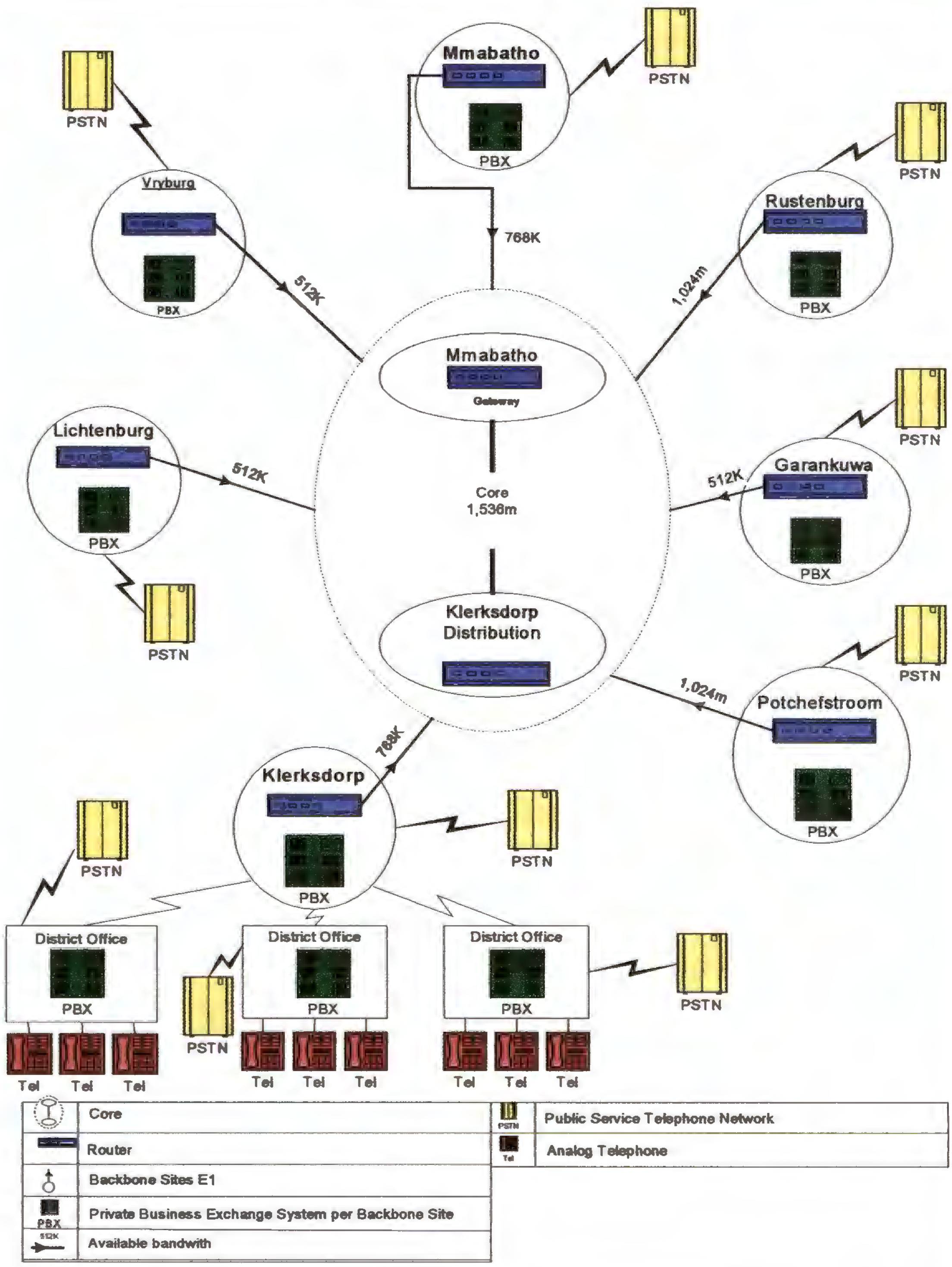


Diagram 4.2: Simplified version of Westnet Network Diagram

(Source: Adapted from NWPG Diagram 4.1 above, 2002)

4.2.2 CURRENT USER SNAPSHOT (FEBRUARY 2003)

There are approximately 2500 users on the CAN (circular formation on the top half of figure 4.1) and 5524 users on Westnet (CAN and WAN – complete diagram of figure 4.1). These users have access to different applications and in-house software such as walker and persal. Microsoft application software is the most commonly used package and includes Netmeeting, which assists with VoIP applications such as video conferencing and IP Telephony. Certain PC's are equipped with a microphone, speakers, soundcard, a camera and enhances VoIP applications. Also integrated into the system are a few IP Telephones (NWPG User Log, 2002).

4.2.3 FUTURE PROJECTED USER SNAPSHOT

By end of March 2004 it is projected that the number of users on Westnet will increase to approximately 9714. This takes into account an average of 10 users per site for the 419 sites to be added to Westnet over a 12-month period. These sites consist of 300 schools and 119 libraries. To facilitate this growth in terms of bandwidth, new services and progressive deployment of information, the IT Directorate has embarked on a Core and Backbone upgrade using Huawei Technology. This upgrade will be completed by the end of March 2003 and will provide channelized E1 connections with a 2mb bandwidth each to each distribution (regional office) (NWPG User Log, 2002).

4.3. SAMPLING

The sampling approach for this study is a non-probability sample because the probability of including all the provincial and national governments is not possible. This is due to the fact that the needs for service delivery and technological advancement may differ from one government structure to another. The sampling method is purposive in that characteristics of the sample were based on the judgement of the researcher.

4.3.1 TIMEFRAME

The research is conducted intermittently over a period of 4 months, from October 2002 to February 2003. This is due to the core and backbone equipment upgrade that commences in February and will be completed by end of March 2003.

4.4 DATA COLLECTION

The Department of Finance houses the Information Technology Chief Directorate who are responsible for the services provided on Westnet as well as the management and maintenance of Westnet. This Chief Directorate is the main provider of information concerning traffic, equipment, configuration, management, etc. of the network. Financial data is obtained from both the Chief Directorate and the Department of Finance.

Case study(s) (refer to Appendix 2) and modeling experiment(s) are used to establish current trends for VoIP in large organizations. Relevant documentation such as white paper(s) (refer to Appendix 4), article(s) (refer to Appendix 1) as well as documentation of the NWPG (refer to Appendices 3 and 5) are used to model a VoIP solution for the NWPG on.

Participant observation was chosen as the main method of data collection as opposed to a questionnaire with a five-point scale, which cover a wide range of topics. The reasoning for this is that instead of generalizing from the results of the questionnaire, participant observation allows for a specific or focused approach.

Although, the case studies, white papers and articles referred to above provides a foundation in relation to measurement of performance and modelling if reconstruction of the current network infrastructure is necessary, participant observation is used to collect data on network traffic (available bandwidth), infrastructure and packet distribution.

Participant observation is used to measure the efficiency and effectiveness of the network, specifically focusing on the following areas:

- a test bed experiment to measure the packet size distribution using different codecs and the H.323 protocol;
- infrastructure testing to measure the different delays and establish a performance baseline; and
- bandwidth measurement to gauge current and future capabilities of Westnet (network traffic) and whether the network can handle a VoIP solution.

This data is compiled using statistical methods and certain assumptions.

Financial information concerning the network budget, telephone accounts for calls and rental equipment, and others is solicited from the Accountant Generals' office. However, due to the nature of the organization, certain aspects of the financial information is not provided and thus assumptions are made within reason.

4.5 DATA ANALYSIS

Due to the bulk of the data collected being qualitative in nature, Non-parametric Statistical Techniques will be employed for data analysis. Descriptive statistics will be used to analyse the data.

4.6 SUMMARY

In conclusion, the approach adopted above is very important because it plots the way forward for the planned research path and necessary analysis tools to be used for data analysis purposes. It also highlights the timeframe limitation due to the roll-out of the installation of the Huawei network equipment as mentioned in the sampling frame discussion.

CHAPTER 5

RESULTS AND INTERPRETATION

5.1 INTRODUCTION

This chapter reports on the results of the imperial investigation conducted to gather information regarding the financial impact of VoIP on the administrative and management systems of the NWPG.

5.2 RESULTS AND INTERPRETATION

The results of the study were examined as follows:

- Firstly the Technical Ambit was under scrutiny. Participant Observation, Test beds, Case Studies and White papers indicated in chapter 1 formed the basis for this section.
- Thereafter the Financial Ambit was scrutinized. The basis here was financial reports for the period December 2001 to November 2002 on telecommunications expenditure.

5.2.1 TECHNICAL AMBIT

Different aspects of the case study, the white paper, an article, as well as the documentation of the NWPG referred to in Appendices 1 to 5, 74 - 116 were used as a basis for the infrastructure testing, modelling experiments (test beds) and bandwidth testing that was undertaken and are discussed below.

5.2.1.1 INFRASTRUCTURE TESTING

The purpose of conducting intranet testing is to provide a performance baseline. A performance baseline provides a minimum performance measure when these experiments are expanded to the Internet. The additional delay elevated by the Internet can be better understood when using a performance baseline.

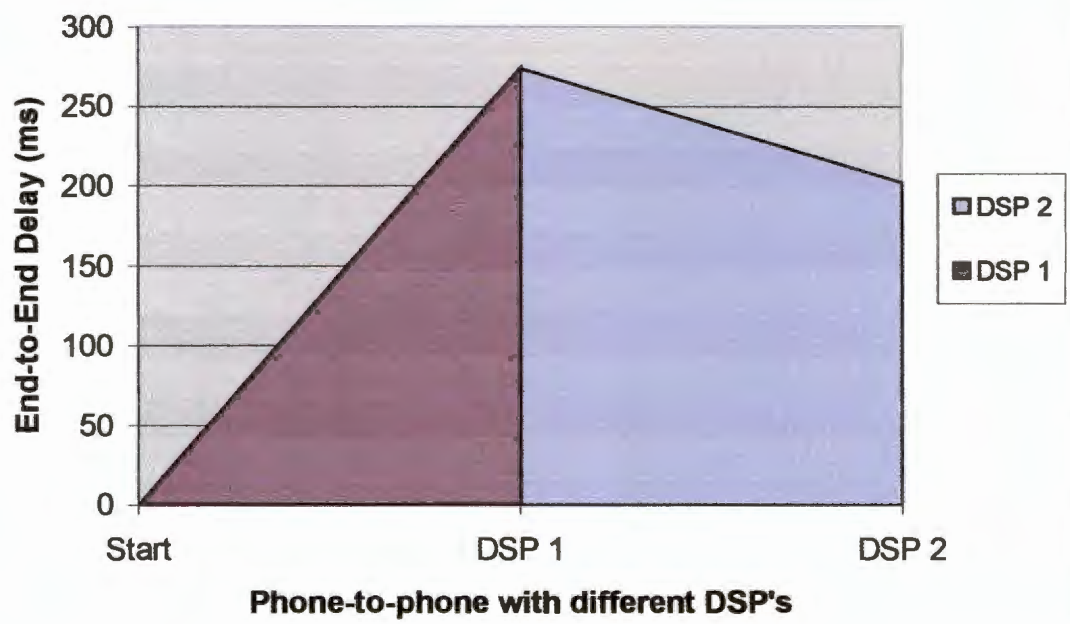


Figure 5.1: Delays Introduced by Equipment

With tests conducted in both PC-to-PC and phone-to-phone testing in an intranet environment (the Westnet CAN), delays were experienced. In figure 5.1 above a phone-to-phone experiment was conducted using different DSP's. The end-to-end delay with DSP 1 was measured as 274 ms. A large portion of this delay was due to the analog/digital conversion, compression, packetization, and OS overhead in the IP gateways. When a faster digital signal processors (DSP 2) was used, the delay introduced by the equipment was 202ms. This indicates the degree of the delay introduced by equipment dependent in this case on speed.

The available infrastructure could adversely affect the implementation of a VoIP solution, therefore, it was important to establish the network capabilities and efficiencies in relation VoIP.

5.2.1.2 TEST BED EXPERIMENT

The purpose of the test bed was to gauge the packet size distribution over a given period using different codecs and the H.323 protocol. This experiment was conducted in the Laboratory at the Department of Finance, Information Technology Directorate situated in Garona Building which lies on the CAN. Table 5.1 below represents the results from a 30-second half-duplex voice session with the IP gateways using the H.323 call protocol.

Table 5.1: Packet size distribution over 30 seconds

Codecs and kilo bites per second		Packet Size (Bytes)					
		<=64	65-84	85-128	129-512	513-1024	>1024
G.723.1 6.4 kbps	Listener	0.20%	81.20%	0.70%	0.30%	0.00%	17.50%
	Talker	0.10%	98.30%	0.90%	0.70%	0.00%	0.00%
G.723.1 5.333 kbps	Listener	0.00%	81.40%	1.10%	0.30%	0.00%	17.20%
	Talker	0.10%	98.10%	1.30%	0.50%	0.00%	0.00%
G.711 64 kbps	Listener	2.30%	0.30%	1.90%	50.60%	0.00%	44.80%
	Talker	4.20%	0.60%	3.50%	91.70%	0.00%	0.00%

The columns are packet sizes. With the G.723.1 coder, 81.2% of the packets from the Listener were 64 to 84 bytes in size. When using G.711, the talker sends data out in 310 frames. The remaining packets from the talker to listener are called control packets from the application ranging in size from 64 to 128 bytes. When using the G.723 codecs, the data are in 78-byte frames. When the listener sends data to the talker, the packet size is between 84 and 100 bytes, regardless of the codec. Other packets are from the Observer software or are call control packets from NetMeeting.

The experiment proves that data behavior is highly application dependent. The packet size distribution is varied for every codec in relation to the H.323 call protocol.

Quality of Service (QoS), jitter, latency, etc. can only be tested once VoIP is implemented on Westnet. Based on the quality and functionality of the equipment currently used on Westnet, these issues would not have a major impact on the service delivery levels of Westnet in terms of VoIP because the majority of the equipment supports the H.323 protocol. This also addresses the issue of interoperability which makes for IP Convergence.

The H.323 protocol is the obvious choice for Westnet because it achieves interoperability between a broad range of products and marries them over an IP based network to facilitate services such as VoIP.

5.2.1.3 BANDWIDTH – CURRENT AND FUTURE

Bandwidth usage is difficult to set at a constant due to the following reasons:

- As mentioned above, data behaviour is highly application dependent – meaning that certain application may need more bandwidth than others;
- VoIP applications vary in size, for example, a combination application of voice and video will need more bandwidth than a FoIP (fax) application or a voice call;
- Other operational software also uses bandwidth.

The gatekeepers will take care of bandwidth control, admission control, Zone management and translation of terminal and gateway aliases to IP or IPX addresses.

Westnet's current packetized capability is:

Table 5.2: Westnet's current capacity			
From	**To**	**Bandwidth**	**7kbps packet size**
Mmabatho	Klerksdorp	1.536m	1.536m/7 = 219.43
Klerksdorp	Rustenburg	1.024m	1.024m/7 = 146.29
Klerksdorp	Potchefstroom	1.024m	1.024m/7 = 146.29
Klerksdorp	Ga-rankuwa	512k	512k/7 = 73.14
Klerksdorp	Vryburg	512k	512k/7 = 73.14
Klerksdorp	Lichtenburg	512k	512k/7 = 73.14

Table 5.2 above indicates the number of concurrent 7kbps packets that can be sent over the lines between the core and the outlaying regions on Westnet at any one time without calculating OS overhead.

This means that on the Mmabatho / Klerksdorp line which forms the core, for example, 219.43 packets can be sent at the exact same time. If each voice call required approximately 64kbps bandwidth, then approximately 24 calls could be placed simultaneously. That would mean that call number 25 would have to be routed either over the PSTN network rather than Westnet or as a second group of simultaneous calls on Westnet. This implies that every 25th call could have a cost implication to the NWPG if it is not routed over Westnet as part of a second group of concurrent calls. This would have a major cost saving implication for the NWPG just in terms of their telephone bills.

The Core and Backbone of Westnet will be upgraded by the end of March 2003 with Huawei Technology, to facilitate the projected growth in terms of bandwidth, new services and progressive deployment of information. With this upgrade, Westnets' bandwidth capacity is shown in Table 5.3 below:

Table 5.3: Westnet Line Capacity and Bandwidth with the Huawei Equipment			
From	**To**	**Capacity**	**Bandwidth**
Mmabatho	**Klerksdorp**	**4 x 5 slot Net-engines**	**E1**
Klerksdorp	Mmabatho	Channelized E1	2m
Klerksdorp	Rustenburg	Channelized E1	2m
Klerksdorp	Potchefstroom	Channelized E1	2m
Klerksdorp	Ga-rankuwa	Channelized E1	2m
Klerksdorp	Vryburg	Channelized E1	2m
Klerksdorp	Lichtenburg (LTX)	Channelized E1	2m
Klerksdorp	Klerksdorp	Channelized E1	2m
Klerksdorp	**SDS**	**Channelized E1**	**2m**

Table 5.3 includes an eighth site namely the Service Distribution Site (SDS) that will house the Natis, Trafman, Avis and SITA Clouds. This means that these applications will run on their own line reducing the network traffic on the other lines. The channelized E1 lines each provides a 2m bandwidth and that means more traffic can be accommodated across these lines. The Huawei Equipment also caters for future expansion to a large extent.

With this upgrade completed, the bandwidth increase will mean even more savings in terms of the above example. In terms of that example it would mean that every 32 call would either be routed over the PSTN network or as part of a second group of concurrent calls over Westnet. This implies a larger cost reduction. With some of the other distribution sites, the savings would be more dramatic because of the newly increased bandwidth.

5.2.2 FINANCIAL AMBIT

The payments made to the service provider for the telephone numbers starting with 387 which are all located on the CAN, the monthly rental costs of the Diginet lines (some on the CAN and others on the WAN), as well as rentals for PBX's located across the province (at each of the more than 250 sites connected to Westnet), are depicted in table 5.4 below:

Table 5.4: A portion of the NWPG Telecommunications Expenditure per annum

Period 01-12-01 to 30-11-02	**387 numbers**	**Diginet lines**	**PBX's (253)**
November 2002	R 978,202.01	R 450,000.00	R 380,000.00
October 2002	R 1,324,248.34	R 450,000.00	R 380,000.00
September 2002	R 1,364,935.74	R 450,000.00	R 380,000.00
August 2002	R 1,213,219.18	R 450,000.00	R 380,000.00
July 2002	R 1,264,766.99	R 450,000.00	R 380,000.00
June 2002	R 1,148,677.95	R 450,000.00	R 380,000.00
May 2002	R 1,131,610.93	R 450,000.00	R 380,000.00
April 2002	R 1,268,662.10	R 450,000.00	R 380,000.00
March 2002	R 1,147,446.59	R 450,000.00	R 380,000.00
February 2002	R 1,419,403.87	R 450,000.00	R 380,000.00
January 2002	R 1,357,685.69	R 450,000.00	R 380,000.00
December 2001	R 1,289,060.83	R 450,000.00	R 380,000.00
Payments for 12 months period	**R 14,907,920.22**	**R 5,400,000.00**	**R 4,560,000.00**

Given the fact that there are other telephone numbers existing on the CAN and WAN as well as other infrastructure for which the financial information was not available, one can safely say that a ***conservative estimate of R100,000,000.00 per annum for Telecommunication services and infrastructure usage is fair.***

Assuming that the NWPG had implemented a VoIP solution over the same period as indicated above the telecommunication bill would look like this:

Table 5.5: A portion of the NWPG Telecommunications Expenditure per annum with VoIP implemented

Period 01-12-01 to 30-11-02	387 numbers	Diginet lines	PBX's (8)
November 2002	R 244,550.50	R 450,000.00	R 70,000.00
October 2002	R 331,062.09	R 450,000.00	R 70,000.00
September 2002	R 341,233.94	R 450,000.00	R 70,000.00
August 2002	R 303,304.80	R 450,000.00	R 70,000.00
July 2002	R 316,191.75	R 450,000.00	R 70,000.00
June 2002	R 287,169.49	R 450,000.00	R 70,000.00
May 2002	R 282,902.73	R 450,000.00	R 70,000.00
April 2002	R 317,165.53	R 450,000.00	R 70,000.00
March 2002	R 286,861.65	R 450,000.00	R 70,000.00
February 2002	R 354,850.97	R 450,000.00	R 70,000.00
January 2002	R 339,421.42	R 450,000.00	R 70,000.00
December 2001	R 322,265.21	R 450,000.00	R 70,000.00
Payments for 12 months period	**R 3,726,980.08**	**R 5,400,000.00**	**R 840,000.00**

Approximate savings on 387 numbers R 11,180,940.14 and R 3,720,000.00 on the PBX's. This is assuming the following:

- **That the 253 PBX's at all the sites is replaced with 8 larger units placed at the regional distribution sites;**
- **That the analog phones remains in use (not replaced by IP Telephones); and**
- **That all the government-to-government calls as well as government-to-business calls are routed over Westnet..**

The cost reduction on the overall telecommunications and service infrastructure account could easily be almost halved resulting in a conservative estimated savings of R 45,000,000.00

5.3 SUMMARY

It is clear that the cost reduction factor would be significant if a VoIP solution should be implemented at the NWPG. The network infrastructure can accommodate VoIP in terms of available bandwidth, network capacity and a fully integrated administrative and management platform.

CHAPTER 6

IMPLICATIONS, RECOMMENDATIONS AND CONCLUSION

6.1 INTRODUCTION

This chapter describes the limitations experienced during the research process. Thereafter, the implications of implementing VoIP to the NWPG are revealed. Finally, recommendations based on the findings of the research are discussed and concluded.

6.2 LIMITATIONS OF THE STUDY

Crucial financial information was not made available for this study due to its sensitive nature and thus a number of assumptions were made. The choice to use case studies, white papers and other relevant document as a basis for the study assisted with these assumptions and contributed to the credibility of this study. The timeframe permitted by the NWPG for the research limited sufficient access to the network facilities.

Due to a security agreement signed prior to the commencement of this study, all information and diagrams of the network security system is classified and may not be discussed in this document.

6.3 IMPLICATIONS

Technically speaking, the NWPG can implement a VoIP solution almost immediately with the current bandwidth. Once the Huawei upgrade is completed, the possibilities are endless. For example, new services such as the SDS can be made available, the increased bandwidth makes for increased savings and better quality of service, effective deployment of information facilitates better communication and information sharing, etc. are highly achievable.

As mentioned in the limitations above the security system of the NWPG may not be discussed except to indicated whether it complies with any recognized standards, which it does. It complies with the minimum requirements of the ISO/IEC 17799 as well as aspects of the ISO/IEC TR 13335 series and the new ISO/IEC TR 15947. It is also in accordance with the Policy Framework for E-government, 2001 as well as the National Council for Library and Information Services Act, 2001.

The financial implication for the NWPG with the implementation of VoIP over Westnet is very positive and is immediately viable. The significance of the cost reduction factor is summarized below:

- Given the fact that there are other telephone numbers existing on the CAN and WAN as well as other infrastructure for which the financial information was not available, one can safely say that a conservative estimate of R100,000,000.00 per annum for Telecommunication services and infrastructure usage is fair (see pg 61).
- With the implementation of a VoIP solution, the cost reduction on the overall telecommunications and service infrastructure account could easily be almost halved resulting in a conservative estimated savings of R 45,000,000.00 (see pg 62).

This estimated cost reduction can be realised without making any changes to the telephony part of the infrastructure (retaining the analog phones). If IP Telephones are introduced there would be a once off cost implication (investment), however, the estimated reduction in costs will be realised over a very short space in time (possibly six months from investment).

Simplification of systems is achieved through convergence of systems, in this case, data, voice and video over the same network using the existing infrastructure with minor modification, which reduces the initial investment and in-turn amplifies the Return On Investment (ROI) by approximately 38%.

As for the business case of VoIP, besides the cost cutting and simplification of systems effect, VoIP holds definite benefits for management and administrative systems used by the NWPG. Technology as a business tool is a given and so is VoIP. For example, video conferencing allows for interactive real-time meetings attended by those requested, without the time and cost consumed by traveling and accommodation costs usually associated with out of office meetings. The administrative and managerial benefits are as follows:

1. More effective time management,
2. Better and more effective financial management, and
3. Opens the door for better service delivery.

This would mean a drop in the operational budget allocation of the NWPG and a rise in the service delivery portion of the budget. This is the main benefit with relation to the NWPG and its' "Batho Pele" – People First – approach to good governance because it will achieve its mandate in terms of the "Batho Pele" principles.

The issue of accountability will also be addressed because government is responsible for spending public funds responsibly. A VoIP solution implementation at the NWPG will not only facilitate the accountability part of good governance, but also allow for new services to be made available to the public. For example, multicasting allows for better utilization of bandwidth and can be used to send information to the entire school site cluster on off-peak (after hours) times when the bandwidth is under utilized. In so doing, the infrastructure is being used effectively and efficient deployment of information is being achieved.

The only possible drawbacks to implementing VoIP over the NWPG network and introducing it into their management and administrative systems is:

1. Possible budgetary constraints, and
2. Skills necessary to implement VoIP effectively.

6.4 RECOMMENDATIONS

The NWPG is in a good position to exploit the advantages of VoIP. Implementation of a VoIP solution should be embarked as soon as possible because it is a viable cost cutting solution. They would also earn the accolade of being groundbreakers by introducing VoIP into a government environment in South Africa. This would present them with the unique opportunity to transform the way government does business.

Both the possible drawbacks mentioned above can be overcome through sound planning and a skills transfer programme. Sound planning is key: financial, technical and logistics planning, etc. because it will minimize the impact of these drawbacks and could even transform them into advantages, for example, enhancing and elevating the skills base of government officials in relation to VoIP and related technologies.

6.5 CONCLUSION

The existing skills base at the NWPG is capable of implementing a VoIP solution to user level with immediate effect. To achieve higher levels of utilization IT consultant(s) services could be utilised in conjunction with a skills transfer programme.

Implementing VoIP holds many benefits for the NWPG: some tangible such as significant savings, better network infrastructure utilization which makes for better ROI, etc. and other non-tangible benefits such as improved service delivery, good governance and accountability, more efficient and effective systems, etc. These benefits have a snowball effect and thus auxillary benefits will be realised long term.

It is time to stop talking about what we might do someday with Voice over IP and start doing it. The technology works, the business case is evident... Making this move will prepare the NWPG for a more customer-centric approach to the business of governing the North-West Province of South Africa. It will give them the competitive edge in their quest for better service delivery, while at the same time significantly reducing their costs and simplifying their administrative and management systems...

APPENDIX A: LITERATURE

This appendix presents a list of books, case studies, white papers and World Wide Web pages used as basis for this research study. Firstly, sources referred to in the text are listed and thereafter other sources consulted are listed.

A.1 REFERENCES

1) Branford W, 1989: South African Oxford Pocket Dictionary, third Edition; University of Oxford press. (6 January 2003)

2) Black U., 2000: Voice over IP; Prentice Hall. (14 August 2002)

3) Bull A., 2002: A business case for IP telephony; http://www.networktimes.co.za/L_SCR.../Regular.ASP?pk1RegularID=1058&pk1IssueID=28 (7 January 2003)

4) Bryant M., 2003: The Firewall in a Multilayer security approach, CNET Networks, Inc; www.techrepublic.com (26 March 2003)

5) Certo S.C., Certo M.W., 2001: Digital Dimensioning – Finding the E-business in Your Business; McGraw-Hill. (5 March 2003)

6) Cisco White Paper, 2002: Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation; www.cisco.com (9 December 2002)

7) Cronkhite C., McCullough J., 2001: Access Denied – The Complete Guide to Protecting Your Business Online; Osbourne/McGraw-Hill. (29 March 2003)

8) DataBeam Corporation, 1998: A Primer on the H.323 Standard; http://www.databeam.com/h323/h323primer.html (8 October 2002)

9) Husman G, 2001: Exchange 2000 Server – On Site; Coriolis Technology Press. (26 March 2003)

10) InnoMedia Solutions, 2000: What is IP Telephony?; http://www.innomedia.com/ip_telephony/voip/index.htm (3 February 2003)

11) InnoMedia Solutions, 2000: What is VoIP?; http://www.innomedia.com/ip_telephony/voip/index.htm (3 February 2003)

12) International Standards Organisation, ISO/IEC 17799:2000 : Information Technology - Code of practice for Information Security Management; www.searchsecurity.com (27 March 2003)

13) International Standards Organisation, ISO/IEC TR 15947: Information technology – Security techniques and intrusion detection framework; http://www.iso.ch/iso/en/commcentre/news/2002/itintrusions.html (27 March 2003)

14) Karve A., 1999: Global Trading Company takes a Chance on IP Telephony; www.networkmagazine.com (4 September 2002)

15) Karve A., 1999: H.323; www.networkmagazine.com (4 September 2002)

16) Kuscus M. (MEC), 2003: Budget Speech 2003 – North West Provincial Legislature; Vision Press. (4 March 2003)

17) Langford D., 2000: Internet Ethics; Macmillan Press LTD. (30 March 2003)

18) Micom White Paper, 2000: Voice/Fax over IP White Paper; www.micom.co.za (29 August 2002)

19) Mockingbird White Paper, 1999: Designing Global VoIP/ and FoIP Solution Networks, with Nuvo200Nuvo 200 IP/SSP; www.telephonyworld.com (10 October 2002)

20) National Government of South Africa (NGSA), 1998: Constitution of South Africa; www.polity.gov.za (29 March 2003)

21) National Government of South Africa (NGSA), 2001: National Council for Library and Information Services Act; www.polity.gov.za (29 March 2003)

22) National Government of South Africa (NGSA), 2001: Policy Framework for E-government; www.polity.gov.za (29 March 2003)

23) Network Appliance, 2002: Network Appliance Netcache Hardware Product Family; Network Appliance, Inc.; www.netapp.com (27 march 2003)

24) NIST, 2002: International Standard ISO/IEC 17799:2000 Code of practice for Information Security management – FAQ; http://csrc.nist.gov/publications/nistpubs/index.html (27 March 2003)

25) North West Provincial Government, Department of Finance, 1999: Batho Pele principles; www.dpsa.gov.za (June 2002)

26) Palosuo N., 2000: Sofor changes IP networks to virtual spaces; Partneri (4 November 2002)

27) Ryan J., 1999: Voice over IP (VoIP); Applied Technologies Group, Inc. (18 November 2002)

28) SIP Center, 2002: SIP and H.323 – A Comparison; http://www.sipcenter.com/aboutsip/siph323sipandh323.hml (3 February 2003)

29) Smith K. A., Brushteyn D., 1999: Internet Telephony and Voice Compression; http://www.cis.upenn.edu/~kellyann/iphone.html (21 May 2002)

30) Thomson Learning, 2001: A+ Certification – A+ Core Hardware, Rev. 1.0; Wave Technologies International, Inc., Missouri. (20 January 2003) www.thomsonlearning.com (28 March 2003)

31) Ucitytech, 2000: What is Videoconferencing?; http://www.ucitytech.com/Whatisvidconf.html (3 February 2003)

32) UCL Online, 2002: Multi-casting; http://www.hep.ucl.ac.uk/~ytl/multi-cast (3 February 2003)

33) Van Rensburg W. (Prof), 2001: The Environment of Management; UNW Press. (13 March 2001)

34) Wave Technology, 1999: N+ Certification – Network Design, Implementation, and Maintenance; Wave Technology, Inc.; www.wavetech.co.uk (28 March 2003)

35) Wave Technology, 1999: N+ Certification – Network Essentials; Wave Technology, Inc.; www.wavetech.co.uk (28 March 2003)

36) Wiiliam S.Y., Wang, 1982: Human Communication – Language and its Psychobiological Bases; Scientific America. (9 July 2002)

37) Wirbel L., 1999: Voice invades packetized networks; EBSCO Publishing. (30 March 2003)

38) Youngburg S., 1999: IP/Convergence – Strategies and Technologies – A Siemens White Paper; Siemens Technologies. (19 June 2001)

A.2 OTHER SOURCES

- Corporate/government; http://www.centralexchange.com.au/html/corporate_gov_main.htm (4 February 2003)
- Delgrossi L., 1995: Internet Streaming Protocol Version 2 (ST2) Protocol Sprcification; RFC 1819. (10 May 2001)
- Fellbaum K., Richter J.: Human Speech Production Based on a Linear Predictive Vocoder; http://www.kt.tu-cottbus.de/speech-analysis/course.Html (16 April 2002)
- Fenner W., 1997: Internet Group Management Protocol, Version 2; RFC 2236. (10 May 2001)
- Liu C., 1998: Multimedia Over IP: RSVP, RTP, RTCP, RTSP; http://www.cis.ohio-state.edu/~jain/cis788-97/ip_multimedia/index.htm (10 May 2001)
- McConnell B., 1998: How to Bypass Your Local Telco; www.hellodirect.com (12 February 2002)
- Minoli E., Minoli D., 1998: Delivering Voice over IP Networks; Wiley Computer Publishing. (8 January 2002)
- Schulzrinne H., Casner S., Fredericks R., Jacobson V., 1996: RTP:A Transport Protocol for Real-Time Applications; RFC 1889. (10 May 2001)
- Schulzrinne H., Rao A., Lanphier R., 1998: Real-Time Streaming Protocol (RTSP); RFC 2326. (10 May 2001)
- Schulzrinne H., Rosenberg J.: A Comparison of SIP and H.323 for Internet Telephony; http://www.cs.columbia.edu/~hgs/papers/Schu9807_Comparison.pdf (12 November 2002)

- Senior G., 2003: Voice over IP: what lies beneath; http://www.europemedia.net/shownews.asp?ArticleID=14836&Print=true (5 March 2003)
- Shields M.G., 2001: E-business and ERP – Rapid Implementation and Project Planning; John Wiley & Sons, Inc. (17 October 2001)
- Tanenbaum A. S., 1996: Computer Networks, third edition; Prentice Hall. (6 February 2001)
- Techguide White Paper, 2000: VoIP / IP Telephony; www.techguide.com (24 July 2002)
- Technology Protocol Group, 2001: IP Telephony / VoIP; www.cisco.com (24 July 2002)
- Wolfe J.: Physics in speech; http://www.phys.unsw.edu.au/PHYSICS_!/SPEECH_HELIUM/speech.html (5 November2002)

Appendix B: Acronyms

-Numeric-

3D	Three Dimensional

-A-

A/D	Analogue- to-Digital
ATM	Asynchronous Transfer Mode
ARPANET	Advanced Research Projects Agency Network

-B-

BGP	Border Gateway Protocol

-D-

D/A	Digital-to-Analogue
DoD	Department of Defence
DSP	Digital Signal Processor

-F-

Fax	Facsimile
FoIP	Fax over Internet Protocol
FTP	File Transfer Protocol

-H-

HTTP	Hypertext Transfer Protocol

-I-

IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol

IP	Internet Protocol
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
ISO	International Standards Organisation
IT	Information Technology
ITU	International Telecommunication Union

-L-

LAN	Local Area Network

-M-

mbps	Megabytes per second
MC	Multipoint Controller
MOS	Mean Opinion Score

-N-

NT	Networking Technologies
NWPG	North West Provincial Government
N-ISDN	Narrowband Integrated Services Digital Network

-P-

PABX	Private Automatic Business Exchange
PBX	Private Business Exchange
PC	Personal Computer
PCM	Pulse Code Modulation
PFMA	Public Finance Management Act
PSTN	Public Service Telecommunications Network

-R-

RSVP	Resource Reservation Protocol
RTP	Real-time Transport Protocol
RTCP	RTP Control Protocol
RTSP	Real-Time Streaming Protocol

-Q-

QoS	Quality of Service

-S-

SDS	Service Distribution Site
SDP	Session Description Protocol
SITA	State Information Technology Agency
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SSR	Smart Switch Router

-T-

TCP	Transmission Control Protocol
TELNET	Telecommunications Network

-U-

UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
URL	Uniform Resource Locator

-V-

VoATM	Voice over ATM
VoFR	Voice over Frame Relay

VoIP	Voice over IP

-W-

WAN	Wide Area Network
WWW	World Wide Web

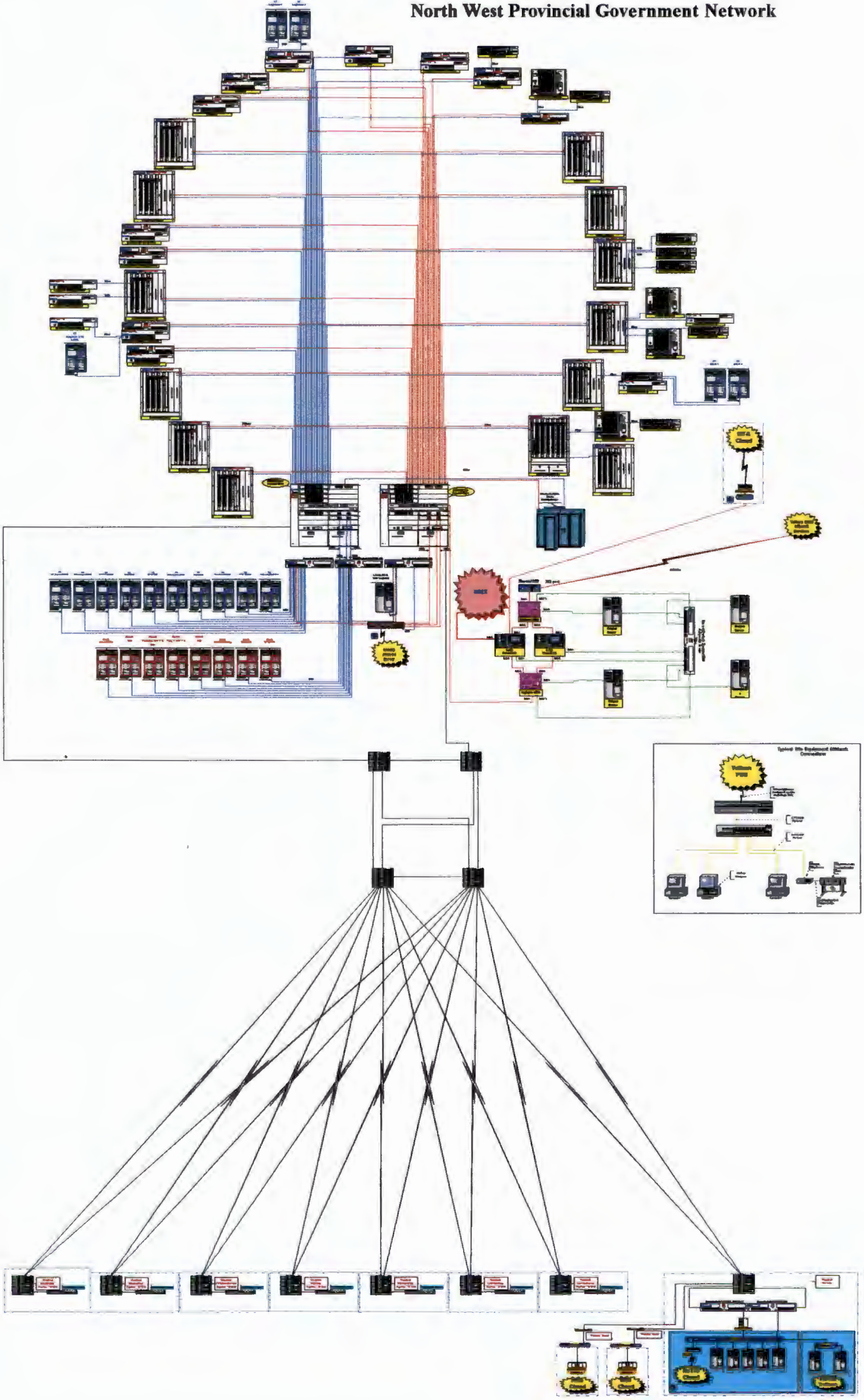
APPENDIX C:

THE NORTH WEST PROVINCIAL GOVERNMENTS DOCUMENTS

- CURRENT NETWORK DIAGRAM
- BATHO PELE PRINCIPLES

"THE PLATINUM PROVINCE OF SOUTH AFRICA…"

North West Provincial Government Network



EIGHT BATHO PELE PRINCIPLES TO KICKSTART THE TRANSFORMATION OF SERVICE DELIVERY

The Public Service will put the following "People First" principles into practice without delay. And we will step up implementation to arrive at acceptable service levels and quality as soon as possible.

CONSULTATION 1

You can tell us what you want from us.

You will be asked for your views on existing public services and may also tell us what new basic services you would like. All levels of society will be consulted and your feelings will be conveyed to Ministers, MECs and legislators.

THE PRINCIPLE: *You should be consulted about the level and quality of the public services you receive and, wherever possible, should be given a choice about the services that are offered.*

SERVICE STANDARDS 2

Insist that our promises are kept.

All national and provincial government departments will be required to publish service standards for existing and new services. Standards may not be lowered! They will be monitored at least once a year and be raised progressively.

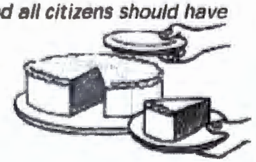
THE PRINCIPLE: *You should be told what level and quality of public services you will receive so that you are aware of what to expect.*

ACCESS 3

One and all should get their fair share.

Departments will have to set targets for extending access to public servants and public services. They should implement special programmes for improved service delivery to physically, socially and culturally disadvantaged persons.

THE PRINCIPLE: *You and all citizens should have equal access to the services to which you are entitled.*



COURTESY 4

Don't accept insensitive treatment.

All departments must set standards for the treatment of the public and incorporate these into their Codes of Conduct, values and training programmes. Staff performance will be regularly monitored, and discourtesy will not be tolerated.

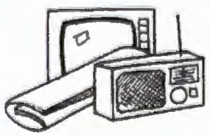
THE PRINCIPLE: *You should be treated with courtesy and consideration.*

INFORMATION 5

You're entitled to full particulars.

You will get full, accurate and up-to-date facts about services you are entitled to. Information should be provided at service points and in local media and languages. Contact numbers and names should appear in all departmental communications.

THE PRINCIPLE: *You should be given full, accurate information about the public services you are entitled to receive.*



OPENNESS AND TRANSPARENCY 6

Administration must be an open book.

You'll have the right to know. Departmental staff numbers, particulars of senior officials, expenditure and performance against standards will not be secret. Reports to citizens will be widely published and submitted to legislatures.

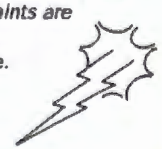
THE PRINCIPLE: *You should be told how national and provincial departments are run, how much they cost, and who is in charge.*

REDRESS 7

Your complaints must spark positive action.

Mechanisms for recording any public dissatisfaction will be established and all staff will be trained to handle your complaints fast and efficiently. You will receive regular feedback on the outcomes.

THE PRINCIPLE: *If the promised standard of service is not delivered, you should be offered an apology, a full explanation and a speedy and effective remedy. When complaints are made, you should receive a sympathetic, positive response.*

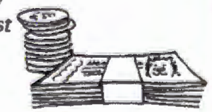


VALUE FOR MONEY 8

Your money should be employed wisely.

You pay income, VAT and other taxes to finance the administration of the country. You have the right to insist that your money should be used properly. Departments owe you proof that efficiency savings and improved service delivery are on the agenda.

THE PRINCIPLE: *Public services should be provided economically and efficiently in order to give you the best possible value for money.*



Designed and issued by the Department of Public Service and Administration.