AN EXPERIMENT TO EXAMINE THE PERFORMANCE OF AN IPV6 MOBILE AD-HOC NETWORK ON VARIABLE VOICE PAYLOAD SIZE

NG WAI SHYAN

SCHOOL OF ENGINEERING AND INFORMATION TECHNOLOGY
UNIVERSITI MALAYSIA SABAH

2006

PUMS 99:1

UNIVERSITI MALAYSIA SABAH

JUDUL: AN EXPERIMENT TO EXAMINE THE PERFORMANCE OF AN IPV6 MOBILE AD-HOC NETWORK ON VARIABLE VOICE PAYLOAD

IJAZAH: BACHELOR OF ENGINEERING (ELECTRICAL AND ELECTRONIC)

SESI PENGAJIAN: 2002/2003 —— 2005/2006

Saya NG WAI SHYAN (HURUF BESAR)

Mengaku membenarkan tesis (LPS/Sarjana/Doktor Falsafah) ini di simpan di Perpusatakaan Universiti Malaysia Sabah dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Malaysia Sabah.
2. Perpustakaan Universiti Malaysia Sabah dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/).

☐ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972).

☐ TERHAD

☑ TIDAK TERHAD

(TANDATANGAN PENULIS)

Alamat Tetap: 86, ANTEK AVENUE 36000 TELUK INTAH, PERAK

Tarikh: 3/5/2006

Disahkan oleh

(TANDATANGAN PUSTAKAWAN)

Mr. Liawas Barukang

Nama Penyelia

Tarikh: 3/5/2006

CATATAN: * Potong yang tidak berkenaan.
* Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada berkuasa/organasasi berkenaan dengan menyatakan sekali sebab dan tempoh tesis ini perlu dikelaskan sebagai SULIT dan TERHAD.
* Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan Sarjana secara penyelidikan atau disertasi bagi pengajian secara kerja kursus dan penyelidikan, atau Laporan Projek Sarjana Muda (LPSM)

DECLARATION

I declare that this writing is my work except for the quotation which I have explained the source of each one of them.

03 MAY 2006

NG WAI SHYAN

APPROVAL

MR. LIAWAS BARUKANG
(SUPERVISOR)

MRS. WAN MAHANI ABDULLAH
(EXAMINER)

MR. LIAU CHUNG FAN
(CHAIRMAN)

ACKNOWLEDGMENTS

I would like to take this opportunity to express my gratitude to Mr. Liawas Barukang, for showing me patience, understanding and advice throughout this project. A deep grateful to Assoc. Prof. Dr. Ali Chekima for his guidance and help on this project. Without his help, the difficult arise would not have passed so much easy.

A special gratitude to my project partner Mr. Bernard Lai Yen Ping in helping setup the network infrastructure and problem occur. Besides that, I also wish to express my gratitude to all who have helped me directly or indirectly in my project.

To my parents, who raised me right, whose love and support me going I give my highest gratitude to them.

ABSTRAK

AN EXPERIMENT TO EXAMINE THE PERFORMANCE OF AN IPV6 MOBILE AD-HOC NETWORK ON VARIABLE VOICE PAYLOAD SIZE

Projek ini membincangkan suatu ujikaji suara menggunakan IP melalui persekitaran WLAN. Ini termasuk membangunkan sebuah model *multi hop* bagi komunikasi jaringan dan menggunakan Linux sebagai sistem operasi. Metrik yang perlu diambil perhatian ialah *streaming, unidirectional, bidirectional request and* responds oleh suara mengunakan IP melalui *Ad-Hoc* jaringan *WLAN*. Ujikaji ini termasuk membina 3 penyambungan pada jarigan wayar dan tanpa wayar. Suara memerlukan *end-to-end delay, jitter* dan peratusan *packet loss* yang rendah. Suara terima keutamaan perkhidmatan dan keutamaan menerima jumlah lebar jalur padanya berdasarkan VoIP *codec*. Sebab-sebab minor yang menyebabkan lebar jalur dan bilangan *packet* melalui jaringan termasuk *IP, UDP headers* dan *Layer 2 overhead*. Tambahan pula *delay jitter, packet error* dan *packet loss* disebabkan penyambungan dan jarigan infrastuktur. Untuk mengkaji ciri-ciri aliran *packet*, beberapa program untuk melihatnya di antaranya ialah *Ethereal, Netperf,* dan *Iperf* untuk mengukur *throughput,* lebar jalur, *delay, jitter, packet error* dan *packet drop*. Sebab utama IPv6 dibangunkan ialah untuk menggantikan IPv4. Pelbagai sistem operasi sekarang dapat menerapkan pentas protokol IPv6 dan juga jaringan infrastruktur pada masa kini telah dibina berdasarkan kelebihan IPv6. Untuk mengkaji kesan IPv6 pada VoIP, suatu ujikaji empirikal telah dijalankan untuk melihat prestasi IPv4 and pentas protokol IPv6 pada sistem operasi Linux pada UDP protokol. Prestasi IPv6 pada Linux dibandingkan dengan prestasi IPv4. Dalam ujikaji ini keputusan kemampuan WLAN pada sistem operasi Linux diambil kira pada pentas protokol IPv6 untuk menghantar packet UDP. Keputusan ujikaji ini menunjukkan *codec* dan WLAN yang digunakan pada masa kini dapat menampung *streaming* dan voice *conferencing*.

ABSTRACT

AN EXPERIMENT TO EXAMINE THE PERFORMANCE OF AN IPV6 MOBILE AD-HOC NETWORK ON VARIABLE VOICE PAYLOAD SIZE

This project discusses about an experimental test bed for voice over IP in Wireless LAN environment. This includes setting a multi hop mode for wireless communication and using Linux as an operating system. The metrics to evaluate are streaming, unidirectional, bidirectional request and responds of VoIP in an Ad-Hoc WLAN network. The experiment setup includes three nodes in the wired and wireless network.Voice requires low end-to-end delay, jitter and percent packet loss. Voice receives strict priority servicing, and the amount of priority bandwidth assigned to it should take into count the VoIP codec. The packet that include IP, UDP headers and Layer 2 overhead are the minor criteria effect the bandwidth and rate of packet through the network. Additionally, delay jitter, packet error and packet loss are effeted by node and the network infrastructure. To analyze the packet flow characteristic, few program which include Ethereal, Netperf, and Iperf to measure the throughput, bandwidth, delay, jitter, packet error and packet drop. The IPv6 has been developed to replace the current IPv4 protocol. Various operating systems running at end-systems now support IPv6 protocol stacks and network infrastructures (hosts, routers) are currently being deployed to support IPv6 features. To investigate the impact of IPv6 on VoIP, an empirical evaluation was conducted on the performance of IPv4 and IPv6 protocol stacks on the Linux operating system for UDP protocols. The IPv6 performance obtained on Linux was compared with the performance of IPv4. The experimental results on WLAN also been taken demonstrate that IPv6 protocol stack for Linux giving the capability to delivery UDP packet. The experimental result show that the current codec and WLAN are able to support voice streaming and conferencing.

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

TERM	DEFINATION
bps	bits per second
CRC	Cyclical Redundancy Check. Error-checking component in the trailer, perform calculation before and reaches the destination
DiffServ	Differentiated Services
GPL	General Public License
IntServ	Integrated Services
Interactive	Bidirectional transferring
LAN	Local Area Network
MTU	Maximum Transfer Unit
NIC	Network Interface Card
Node	A host or a router
OS	Operating System
QoS	Quality of Services
RSVP	Resource Reservation Protocol
Streaming	Unidirectional transferring
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

This project discusses how voice rapid and widespread movement toward integrated transport of voice and data across IPv6, to bring forth specific requirements and challenges best addressed by strategic deployment of QoS technologies. This is because requirements of real-time voice applications are so different from those of traditional data applications.

QoS related to use of design criteria, selection of protocol, determination of architecture, identification of approach, choice of network restoration techniques, design of node buffer management, and other network aspects to ensure that end-to-end goals. The network is possible and statistical guarantees, congestion and availability, delay, jitter, throughput, and loss over specified time span traffic load between any two chosen points in the network. The upsurge in number of mobile device using wireless LAN has lead to an increased requirement for IP number, which is rapidly running out. In this project we will use a new kind of protocol named IPv6 that is a new protocol to addressing network IP, to replace the old protocol IPv4. [21]

This new IPv6 protocol has new features that were lack in previous version. IPv6 availability has overcome IPv4 scaling, this is because the world population access to internet has increased, the number of IP address is not enough to support the amount of users. The IPv6 will solve the lack of address space for this moment. The new IP protocol is flexible transition mechanism, because IPv4-Mapped addresses allow a host that support both IPv4 and IPv6 to communicate with a host that supports only IPv4. The IPv6 address is based completely on the IPv4 address. IPv4 is compatible with IPv6 address. The IPv4 compatible address allows a host supporting IPv6 to talk IPv6 even if the local routers do not communicate with IPv6. IPv4 compatible addresses tell the endpoint software to create a tunnel by encapsulating the IPv6 packet in an IPv4 packet. Tunneling is done automatically by kernel when IPv4-Compatible IPv6 addresses are used.

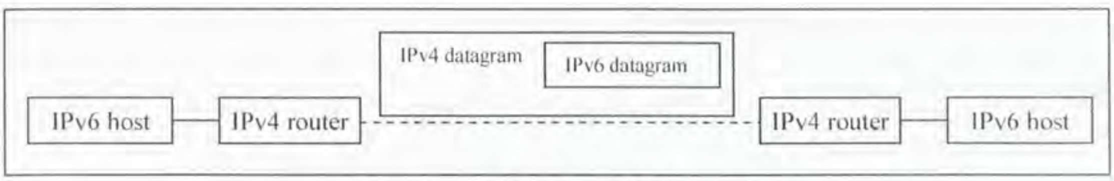

Figure 1.1 IPv4 and IPv6 routing.

There are new improvements in IPv6, these include new routing capabilities, Quality of service, security, and ability to add features in the future. IPv6 is generally available with new versions of most operating systems this include BSD, Linux 2.2 Solaris 8 and option with Windows 2000/NT and Windows XP. For the hardware most routers can support IPv6. [9]

TCP offers reliability in that it guarantees retransmission of lost frames, but this reliable delivery is useless in the intranetworking transportation of packetized voice because a frame that arrives late as a result of retransmission is as useful as no frame at all, that is, it has no effect. In other words, retransmission of packets is not meaningful. By the time the resent packet arrives at the end user endpoint, the required delivery time has long been transgressed.

The IETF has defined two approaches to provide forms of QoS, the IntServ model and DiffServ model. Integrated services approach is based on the reservation, across the network, of the resources needed to guarantee the required QoS for the call.

At the moment, two service classes are defined besides best-effort. The application of this model implies the exchange of signaling between the terminals prior to the beginning of the call establishment itself.

A signaling protocol has been defined at this purpose, called RSVP. Differentiated services approach is based on a classification of the IP packets on the basis of the required QoS; all the packets belonging to the same class will receive the same treatment inside each network node, independently of the call they belong to. The DS approach defines a set of code points for the DS field in the IP packet, and a set of packet forwarding treatments inside the nodes. [1]

1.1 OBJECTIVE

The main objectives of this project are to test and verify the Ad-Hoc mode and multi hop routing network environment and test the reliability of voice transfer over IPv6.

1.2 ORGANIZATION OF PROJECT

Chapter 1 gives an overview of this project and the objectives of this work are highlighted.

Chapter 2 summaries the extensive works done from the literature and compares of various kind of network and QoS method in dealing with wire and wireless networks.

Chapter 3 shows how the networks are setting with some assumption to suit the real world application and the network infrastructure setup which includes hardware and software setting.

Chapter 4 performing test and analysis to the network best effort of transferring voice packet in good in shape.

In Chapter 5, the conclusion of the project was stipulated and a few ideas were given on some future work that can be done.

CHAPTER 2

NETWORK OVERVIEW

2.1 NETWORK FUNDAMENTAL

The open systems interconnection model is a reference for network communication. The OSI model shows how network functions that will go through every layer. The OSI layer can be used to visualize how the information is sending and received on a network in Figure 2.1

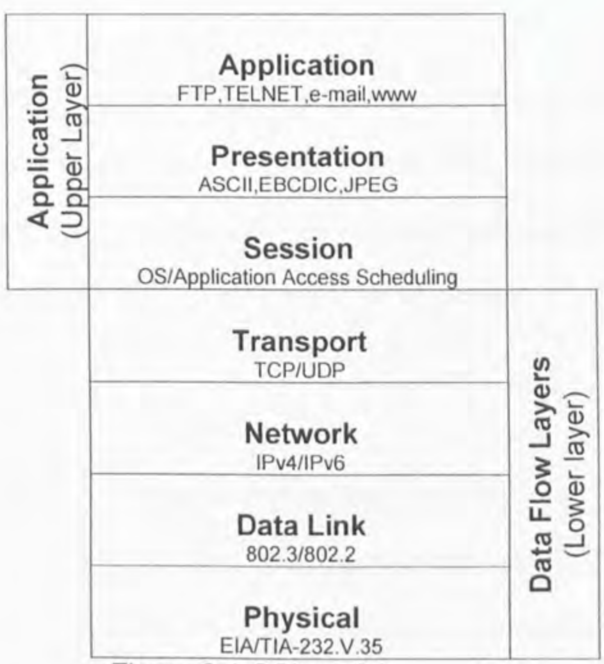

Figure 2.1 OSI model

The upper layer consists of application layer to provide network services, such as spreadsheet program and word-processing program. The presentation layer is to make sure the information sent out is readable by another system, it translates between multiple data format by using a common data format. The session layer is to establish, manages, synchronizes and terminates sessions between communication hosts. It provides services to presentation layer.

The lower layer include transport layer functions as segments data in sending host and reassemble data into data stream on receiving host system, it provides data transport services. TCP and UDP are one of component in transport layer. The network layer provides connectivity and path to the host system. The example of network layer for routing and logical addressing is IP. The Data layer provides transit of data across physical link. It combines bits into bytes and bytes into frames, access to media using MAC address and error detection. The physical layer is a control over the activating, maintaining and deactivating the physical link between end systems

Networks are collections of two or more connected computers. When computers are joined in a network, it can share files, peripherals, internet and conduct videoconferences or voice call in real time with other remote users on the network. LANs accommodate local user's people within a building or on a campus.

2.2 IP ADDRESS

IP is network layer protocol. Network layer moves data through a set of networks. The network layer addressing scheme is used to determine the destination of data as it moves through the network. The network layer uses logical address associate with the source and destination address and paths through the network to reach the desired destination.

2.2.1 IPV4 SCHEME

The Internet Protocol version 4 is the routing layer datagram service of the TCP/IP suite which consists of 32 bit address. The IPv4 address is expressed as dotted-decimal numbers, the 32 bits of the address are broken into four octets. The network IP address identifies the network to which a device is attached.

Class A

1 bit	7 bit	24 bit
0	Network #	Host #

Class B

1 bit	14 bit	16 bit
0	Network #	Host #

Class C

1 bit	1bit	1 bit	21 bit	8 bit
1	1	0	Network #	Host #

Figure 2.2 IP address class and bit patterns

With reference to Figure 2.2 Class A address is to support extremely large networks. The architecture was developed to maximize the possible number of host address. The first octets of its IP address range from 1 to 126. The first 8 bits is to identify network part. Class B address were designed to support moderate to large sized network. The class B network have a value address range from 128.0.0.0 to 191.255.0.0. Class C address was intended to support a small network. The class C IP network address always have value ranging from 192.0.0.0 to 223.255.255.0. To calculate the number of possible IP address that can be assigned, the following formula can be used.

Number of IP address = $2^{\#\text{ bit for host}} - 2$

2.2.2 IPV6 SCHEME

IPv6 is a layer 3 protocol which will replace IPv4. The major changes in IPv6 are the redesign of the header, including the increase of address size from 32 bits to 128 bits. Because layer 3 is responsible for end-to-end packet transport using packet routing based on addresses, it must include the new IPv6 addresses.

Prefix/address	significance
fe80::/10	Link local prefix
fec0::/10	Site-local prefix
::1	Loopback address
::/0	Default route

Table 2.1 Common IPv6 Address and prefix

With reference to Table 2.1, link local are addresses which will only be valid on a link of an interface. Using this address as destination the packet would never pass through a router. Site-local are addresses similar to the RFC 1918 / Address Allocation for Private Internets in IPv4, with the added advantage that everyone who use this address type has the capability to use the given 16 bits for a maximum number of 65536 subnets. The advantage is that it can assign more than one address to an interface with IPv6.

The address for the loopback interface is similar to IPv4 with its *127.0.0.1*. With IPv6, the localhost address is, *0000:0000:0000:0000:0000:0000:0000:0001* or in compressed form *::1*. Packets with this address as source or destination should never leave the sending host. The default route is a address like *0.0.0.0* in IPv4. For IPv6 it's *0000:0000:0000:0000:0000:0000:0000:0000* or *::*. These addresses are mostly used in socket binding (to any IPv6 address) or routing tables

2.3 SUBNETTING

The reason using subnets is to reduce the size broadcast domain. When broadcast traffic begin to consume too much of the available bandwidth, it is practical to reduce the size of the broadcast domain.

IP subnet is a collection of network address which can communicate directly with each other node without having a router to accomplish the communication. The media protocol drivers support direct communication between all systems in the same subnet.

To transmitting data between two different subnet a router is required. The subnet mask is used to divide the 32 bits for IPv4 and 128 bits for IPv4 into two parts. The subnet mask allocate bits that are in the network address and the remaining bits comprise host address as show in Figure 2.3

Network address	Host

Figure 2.3 Network and Host Portions of IP address

Refer to Figure 2.4 a subnet address is created by borrowing bits from the host field and designating them as subnet bits.

Network	Subnet	Host

Figure 2.4 A class address after subnetting

The subdivide of host address space into groups called subnets. With reference of Figure 2.5 192.168.0.0 as the network address A and 192.168.1.0 as the network address B. The subnet mask is 255.255.255.0.

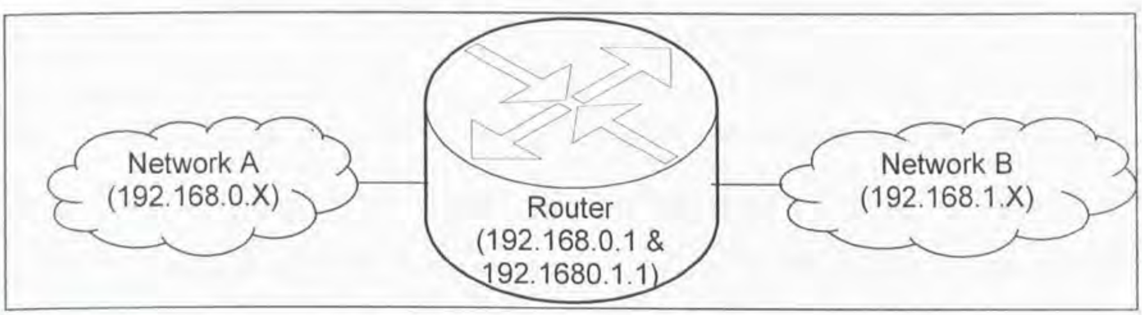

Figure 2.5 Subnetting with 2 segments

There are few different representations, for example /255.255.255.0 is the most commands format used when specifying the subnet mask in command and configuration files and /24 is a maskbits notation.

In a network, all machines must have the same subnet mask. If not, the definition of the network number would vary from one machine to the next, and that would cause the IP software to malfunction.

2.4 UDP PACKET

The User Datagram Protocol (UDP), defined in RFC 768, provides a mechanism for data communication that uses less overhead than TCP. UDP not guarantee the arrival of packets or arrival in sequence. The principle consists in posting applications packets to UDP ports identified by an IP address and a 16-bit port number. Applications using that protocol have to provide their own mechanisms for error correction and congestion control. Figure 2.6 shows how a UDP packet structure with all header required.

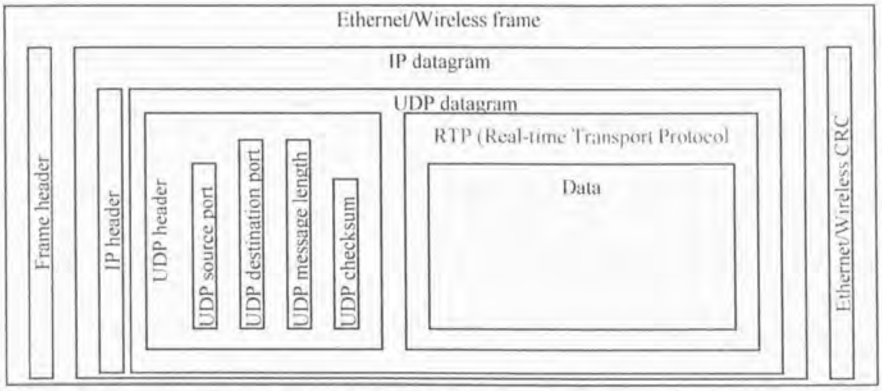

Figure 2.6 Packet encapsulation

UDP is used for applications that transmit short bursts of data, need faster network throughput, or don't require verification of delivery at the destination. UDP packets are organized using source port number to identification of the process which is sending the datagram. Destination port number is to identification of the designated receiving process. UDP length show total length of the datagram and the maximum length of an UDP packet are 1460 bytes. UDP checksum are optional field, verified by the receiver. If the transmitted checksum is 0, it means the sender did not compute the checksum.

Refer to Figure 2.7 each UDP header carries both a source port identifier and destination port identifier, allowing high-level protocols to target specific applications and services among hosts. The UDP header structure is shown as follows

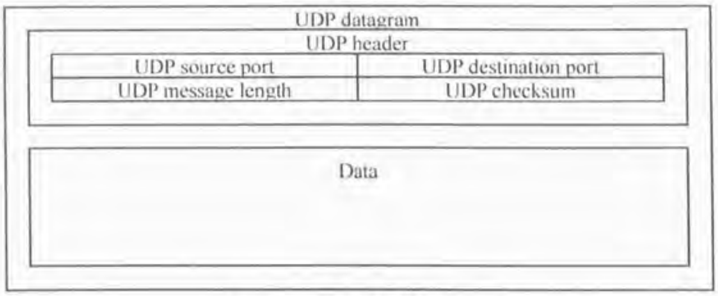

Figure 2.7 UDP structure

Source port is an optional field. When used, it indicates the port of the sending process and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted. Destination port has a meaning within the context of a particular Internet destination address. The length in octets of this user datagram, including this header and the data. The minimum value of the length is eight Checksum. The 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header and the data, padded with zero octets at the end to make a multiple of two octets.

2.5 PACKET FRAGMENTATION

The total length field in the IP header is 16 bits, it means the max size of an IP datagram is 65535 bytes. but the physical layer may not allow a packet size of that large bytes it give a maximum is 1500 bytes only. So, IP must sometimes fragment packets. When an IP datagram is fragmented, each fragment is treated as a separate datagram. It will reassemble at the final destination, and it maybe fragments it again in the path if there is a route.

Each fragment has its own header. The identification number is copied into each fragment. One bit in the flags field indicated that more fragments are coming. If that bit is 0, then it signifies this is the last fragment. The fragment offset field contains the offset of the data. Fragment flag of 0 and offset of 0 means the datagram is not fragmented. Fragment offset is measured in units of 8 bytes (64 bits). That is because the fragment offset field is 3 bits shorter than the total length field (and 2^3 is 8). The final destination reassembles the packet before passing the packet to the upper layers. [16]

2.6 ROUNTING AND BRIDGING

Router pass packet from one network to another with the feature of filtering packet. Router is the best choice to connect LAN to internet. Bridge is use within a network to connect different subnet. It will relay all packets from one subnet to another subnet without any restriction. Bridge can be useful if one subnet in network becoming over burned and need to lighten the load, but is not an idea to connect to internet.

2.6.1 ROUTING

A network by it self is not as much use as one that can connect to other networks. To get a message off the network and onto the others requires knowing where and how to deliver the packets. This is known as routing. In IP each network keeps track of only the first hop on the route to all other networks. It keeps track of which gateway to use for each other network to which it wants to communicate. Those nodes know the next hop for the packet, and so on. Eventually the packet reaches its destination.

This is called store and forward routing, because each node in the chain receives the packet and then forwards it to the next destination. However, it is networks that have routes to gateway nodes, not nodes that have routes. There are several types of routes:

Default: All packets for networks you don't explicitly list elsewhere are sent to this node for forwarding. If your network has only one gateway, this is all you need.

Static: A command is used to add a route for one or more networks, and it never changes. This is used when there are a few gateways to fixed networks, and normally a default route is used for the remaining networks.

Dynamic: The system listens to broadcasts of routes from the gateways and adjusts automatically. Many Internet nodes use this method.

Routing is transparent and automatic by the system. You can turn it off by performing a modification to the TCP parameters in the operating system. Firewall gateways, which are used to protect networks from security breaches, turn off this automatic forwarding.

2.6.2 BRIDGE

The Linux kernel has built in support for acting as an Ethernet bridge, which means that the different Ethernet segments it is connected to will appear as one Ethernet to the participants. Several bridges can work together to create even larger networks of Ethernets using the IEEE 802.1 spanning tree algorithm. As this is a standard, Linux bridges will interoperate properly with other third party bridge products. Additional packages allow filtering based on IP, IPX or MAC addresses.

2.7 SWITCHING METHODS

When a switch receives a packet from a host, it will look up the destination MAC address in its forwarding table to determine where the frame should be passed next. While this is true, how the switch handles the forwarding process can vary. For example, one kind method used of routers will buffer the entire incoming data packet, and then recalculate its cyclic redundancy check to be sure it not corrupted. Another method will begin forwarding a packet almost immediately as it begins entering the switch, not bothering to

REFERENCES

[1] Antonello Pellegrino, 2005. Quality Measurement in WiFi Environments. European Journal for the Informatics Professional 6 (1) 57-61.

[2] Asuncion Santamaria and Francisco J.Lopez Hernandez, 2001. Wireless LAN Standards and Application. Artech House, Boston London.

[3] Bill Ball and Duff, 2005. Red Hat Fedora 3 Unleashed. Sams Publishing, United States of America.

[4] Cisco System, Inc, 2001. Second Edition. Cisco Networking Academy Program: First-Year Companion Guide, United States of America.

[5] Cisco - Voice Over IP - Per Call Bandwidth Consumption. http://kbase/paws/servlet/ViewFile/7934/bwidth_consume.xml?convertPaths=1. 2005.

[6] Daniel Minoli and Emma Minoli, 2002. Second Edition. Delivering Voice Over IP Networks. Wiley Publishing Inc, Indianapolis, Indiana, Canada.

[7] Daniel Minoli, 2002. Hotspot Networks, WiFi For Public Access Locations. McGraw-Hill. United States of America.

[8] David Mosberger and Stephane Eranian, 2002 IA-64 Linux Kernal Design and Implementation. Prentice Hall PTR. United States of America.

[9] Davices, G 2004. Designing and Developing Scalable IP Networks. Guy Davies

[10] Larry Hettick, 2004. IP Telephony Management: The Essential Top-10 Checklist. Wireless Solutions at Current Analysis.

[11] Netperf benchmark application software. http://www.netperf.org/netperf/training/Netperf.html

[12] Ramjee Prasad and Marina Ruggieri, 2003. Technology Trends In Wireless Communications.Artech House Publishers. Boston, London.

[13] Red Hat Linux Fedora http://fedora.redhat.com

[14] Suse Linux Operating System. http://www.novell.com

[15] Seungjoon Lee, Suman Banerjee, Bobby Bhattacharjee, 2003. The Case for a Multi-hop Wireless Local Area Network. Department of Computer Science, University of Maryland.

[16] Teik-Kheong (TK) and Benny Bing, 2003. World wide Wi-Fi Technological Trends and Business Strategies. Hohn Wiley and Sons Inc. Hoboken, New Jersey, Canada.

[17] Tony Mancil, 2002. Second Edition. Linux Router, A Primer for Network Administrators. Prentice Hall PTR. United States of America.

[18] Ubuntu Linux Operating System. http://www.ubuntulinux.org/download. 2nd August 2005

[19] Newport Networks Ltd. VoIP Bandwidth Calculation, 2005. www.newport-networks.com

[20] Wolisz, A and Berthold Rathke, 2003. Experimental Performance Evaluation of an 802.11b WLAN supporting mixed Multimedia Traffic. Technische Universität Berlin, Telecommunication Networks Group

[21] Zeadally,S Wasseem, R and Raicu, I Comparison of end-system IPv6 protocol stacks, INTERNET PROTOCOLS, TECHNOLOGY AND APPLICATIONS (VoIP), IEE Proc.-Commun., Vol. 151, No. 3, June 2004 238-242