ANALYSIS OF PERFORMANCE OF VOIP OVER VARIOUS SCENARIOS

A Project Report

Submitted by

Ms. PRIYANKA TANAJI LIGADE
Ms. SHRUTHI MURUGAN THEVAR
Mr. MOHAMMED ISHAQ ABDUL QAIYUM
Mr. CHOUGULE MUBEEN

in partial fulfillment for the award of the degree

of

B.E.

IN

ELECTRONICS & TELECOMMUNICATION

At

ANJUMAN-I-ISLAM'S

KALSEKAR TECHNICAL CAMPUS

PANVEL

OCT 2014

DECLARATION

We hereby declare that the project entitled **"Analysis of Performance of VoIP Over various scenarios"** submitted for the B.E. Degree is Our original work and the project has not formed the basis for the award of any degree, associateship, fellowship or any other similar titles.

Signature of the Students:
Ms. Priyanka Tanaji Ligade
Ms. Thevar Shruthi Murugan
Mr. Mohammed Ishaq Abdul Qaiyum
Mr. Chougule Mubeen

Place: Navi Mumbai
Date:

CERTIFICATE

This is to certify that the project entitled **“Analysis of Performance of VoIP Over various scenarios”** is the bonafide work carried out by students of B.E., KALSEKAR Technical Campus, Panvel, during the year 2014-2015, in complete fulfillment of the requirements for the award of the Degree of B.E EXTC and that the project has not formed the basis for the award previously of any degree, diploma, associateship, fellowship or any other similar title.

________________	________________
(Prof. Mujib Tamboli)	(Prof. Mujib Tamboli)
H.O.D	Internal guide

(External)

ACKNOWLEDGEMENTS

We take this opportunity to offer our gratitude to our guide **Prof. Mujib Tamboli** for his support and guidance. He allowed us a great deal of freedom in choosing our topics for study and also provided us encouragement throughout this venture.

We also wish to thank **Mr. Yashwant Singh** and **Mr. Ravindra** of CETTM (Centre for Excellence in Telecom Technology and Management) MTNL who took time off from their busy schedules to help us with the project. They allowed us full access to many facilities without which our project would have not been possible.

Last but not the least we are grateful to our parents for all their support and encouragement.

ABSTRACT

Voice over IP (VOIP) uses the Internet Protocol (IP) to transmit voice as packets over an IP network. So VOIP can be achieved on any data network that uses IP, like Internet, Intranets and Local Area Networks (LAN). Here the voice signal is digitized, compressed and converted to IP packets and then transmitted over the IP network. Signaling protocols are used to set up and tear down calls, carry information required to locate users and negotiate capabilities. VoIP is an advanced technology that has a great potential to develop new telecommunication with much lower cost and better QoS. In our project, we shall analyze the performance of VoIP over digital communication on popular application such as Skype and msn. Parameters of interest are the quality of service, the Mean Opinion Score, packet loss ratio and jitter. We also plan to examine the delays and distortion issues that VoIP might have while increasing the traffic load and generate a more realistic topology by adding extra models to the system and evaluate the impact to the overall QoS.

LIST OF FIGURES

TABLE OF CONTENTS

1. PURPOSE AND BACKGROUND

1.1. OUTLINE OF THE REPORT

Until today data networks and voice (telephony) networks have always treaded their separate ways. With the dawn of the 21st century they seem to have reached the crossroad. We have entered into an age of 'CONVERGENCE'. The border separating the two has narrowed to a thin red line. Thin red line- because the integration must be done carefully and intelligently. 'VoIP' is a tool that would greatly hasten this process.

This thesis is logically divided into 3 sections.

Section 1 discusses the following points.

- The history of VoIP
- The traditional telephony System
- What is VoIP?
- Objective of Study
- The advantages involved

Section 2 discusses the following points

- OSI and TCP/IP Models
- Routing protocols
- Networks and other protocols used

Section 3 discusses the following points

- Description and overall design
- Configurations and design model
- Topologies of all the five scenarios

Section 4 discusses the following points

- Hands on Experience in the CETTM Lab
- 6 Labs on various routing protocol and switching
- Setting up actual VoIP connection between 3 PCs using asterisk

Section 5 discusses the following points

- Simulations results and comparison of all the 5 scenarios

Finally we end conclusion , Appendices, Technical Papers, Reference Books etc.

1.2. PURPOSE OF THE REPORT

This project report is part of the curriculum for the final year of the Electronics and Telecommunications Engineering Bachelor's program as prescribed by Mumbai University. The project has involved six months of reading, understanding and thinking and another two months of analysis. The seventh semester involved a theoretical study, we used the 'CISCO PACKET TRACER' to study practical router configuration. We visited the CETTM(MTNL) at Mumbai to have a hands-on-experience with the hardware. And the eighth semester involved simulating various scenarios using 'OPNET','WIRESHARK and coming to conclusion that is relevant to the objective of the project. We have found the overall experience very enlightening and interesting.

1.3. HARDWARE SPECIFICATION

A. CISCO WS- C2960- 24TT-L SWITCHES

These Switches are stand-alone fixed configuration switches offering Fast Ethernet and Gigabit Ethernet connectivity with LAN services. Cisco Catalyst 2960 Series Switches with LAN Base software deliver intelligent services for commercial and midsize enterprise wiring closets and branch offices. The LAN Base software supports enhanced integrated security, including Network Admission Control (NAC), advanced quality of service (QoS), availability, and scalable management to enable new converged application.

B. CISCO 2811 INTEGRATED SERVICES ROUTERS

The Cisco 2811 Integrated Services Router is part of the Cisco 2800 Integrated Services Router Series which complements the Integrated Services Router Portfolio.

The Cisco 2811 Integrated Services Router provides the following support:

- Wire-speed performance for concurrent services such as security and voice , and advanced services to multiple T1/E1/xDSL WAN rates
- Enhanced investment protection through increased performance and modularity
- Increased density through High-Speed WAN Interface Card Slots (four)
- Enhanced Network Module Slot
- Support for over 90 existing and new modules
- Support for majority of existing AIMs, NMs, WICs, VWICs, and VICs
- Two Integrated 10/100 Fast Ethernet ports
- Optional Layer 2 switching support with Power over Ethernet (PoE) (as an option)
- Security
    - On-board encryption

    - Support of up to 1500 VPN tunnels with the AIM-EPII-PLUS Module
    - Antivirus defense support through Network Admission Control (NAC)
    - Intrusion Prevention as well as stateful Cisco IOS Firewall support and many more essential security features
- Voice
    - Analog and digital voice call support
    - Optional voice mail support
    - Optional support for Cisco CallManager Express (Cisco CME) for local call processing in stand alone business for up to36 IP Phones
    - Optional support for Survivable Remote Site Telephony support for local call processing in small enterprise branch offices for up to 36 IP phones

1.3. SOFTWARE SPECIFICATION

A. CISCO PACKET TRACER

Cisco Packet Tracer is a powerful network simulation program that allows students to experiment with network behavior and ask “what if” questions. As an integral part of the Networking Academy comprehensive learning experience, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the teaching and learning of complex technology concepts.

Packet Tracer supplements physical equipment in the classroom by allowing students to create a network with an almost unlimited number of devices, encouraging practice, discovery, and troubleshooting. The simulation-based learning environment helps students develop 21st century skills such as decision making, creative and critical thinking, and problem solving. Packet Tracer complements the Networking Academy curricula, allowing instructors to easily teach and demonstrate complex technical concepts and networking systems design.

The Packet Tracer software is available free of charge to Networking Academy instructors, students, alumni, and administrators who are registered NetSpace users.

B. ASTERISK

Asterisk is an open source framework for building communications applications. Asterisk turns an ordinary computer into a communications server. Asterisk powers IP PBX systems, VoIP gateways, conference servers and more.

Asterisk can run on multiple base architectures including embedded systems and there are no strict requirements on CPU speed or memory size.

Asterisk can run on a number of Operating Systems. Linux is the only officially supported OS, and it is recommended to use a 2.6.25 or higher kernel.

Finally, and most importantly, Asterisk is a framework that allows selection and removal of particular modules, allowing us to create a custom phone system.

C. JITSI

Jitsi is a open-source software with following characteristics.

Jitsi is written in java for cross-platform compatibility with other operating systems.

In addition to supporting traditional SIP for online communications, google talk's protocol (XMPP) is also supported for audio and video chats as well as AIM, ICQ, Facebook, Yahoo and MSN

.

With the emergence of IPv6 connectivity, Jitsi is capable of initiating direct connect VoIP sessions, simply by providing the appropriate IPv6 address of the machine to connect to.

Jitsi also provides a means to encrypt VoIP traffic using SRTP or ZRTP encryption method.

2.1. INTRODUCTION

2.1.1. Overview of VoIP Technology

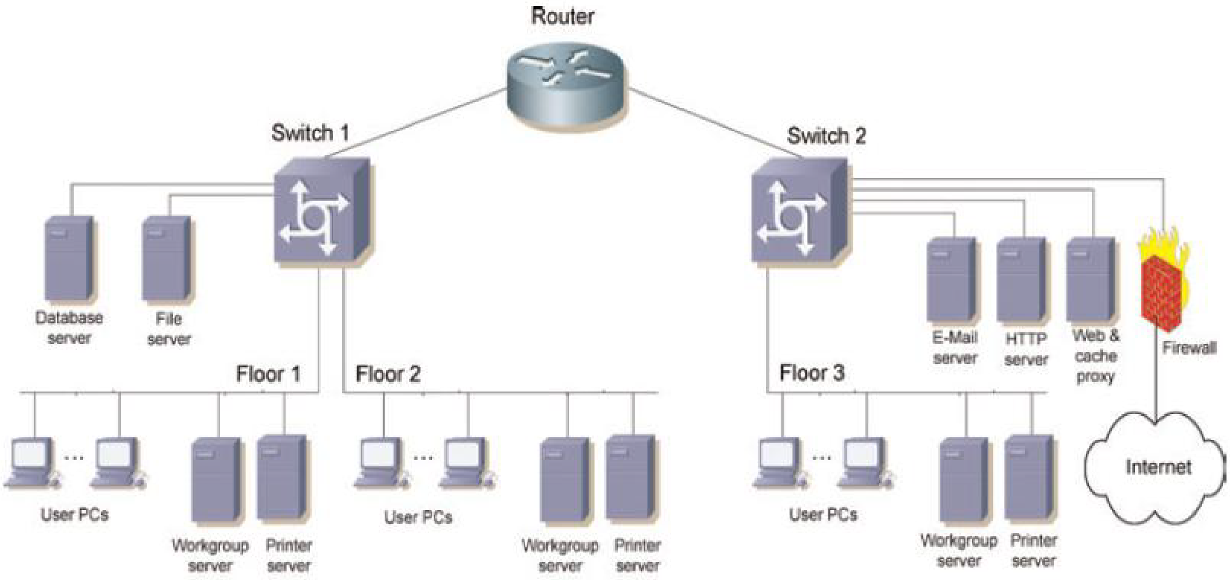


Figure 1.1 Typical VoIP Network

Voice over IP (VOIP) uses the Internet Protocol (IP) to transmit voice as packets over an IP network. So VOIP can be achieved on any data network that uses IP, like Internet, Intranets and Local Area Networks (LAN). Here the voice signal is digitized, compressed and converted to IP packets and then transmitted over the IP network. Signaling protocols are used to set up and tear down calls, carry information required to locate users and negotiate capabilities. One of the main motivations for Internet telephony is the very low cost involved.

As the advancement of technology progresses in a dramatic rate, a new age of digital communication has been established. A tremendous increase in popularity over the real-time voice communication over Internet protocol (IP) is observed in recent years. Voice over Internet Protocol (VoIP) is a high modern technology that provides the capability of users to generate telephone calls over an IP data network (Internet) using packet-switching technology instead of the traditional Public Switched Telephone Network (PSTN). With the creation of VoIP, the nowadays digital communication has greatly reduced in cost while preserving high quality service, as VoIP's capabilities to merges both data and voice in a single channel[1].

Not only limit to internet, VoIP has also shown its popularity in data networks such as Ethernet LANs. The reason is that Ethernet would be an ideal data networking platform for enterprises and other organizations to establish LAN communication[2], as it provides its user with a high level quality of services while greatly reducing cost comparing to the traditional PSTN . In addition to that, wireless Ethernet networks (IEEE 802.11) allow distance digital communication for users to connect to the network, which is ideal for locations that are difficult to setup tool such as Hospitals, two offices located far apart and conference rooms.

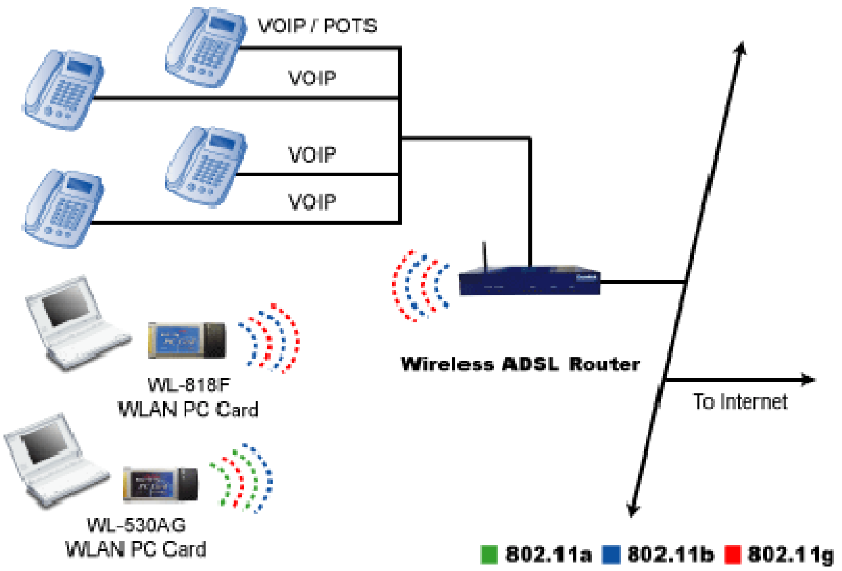


Figure 1.2 Ethernet of VoIP

Today, VoIP has becoming one of the most widely used technologies in a global aspect; as it shows an amazing grow of usage in homes and organization. Up to now, a variety of VoIP communication software has already in use on the market, such as Skype, AIM and Windows live messenger[3].

2.1.2. Comparison between PSTN and VoIP

PSTN	VoIP
Dedicated Lines.	All channels carried over one internet connection.
Each line is line 64kbps(in each direction).	Compression can result in 10kbps(in each direction).
Features such as call waiting, Caller ID and so on are usually available at an extra cost.	Features such call waiting, Caller ID and so on are usually included free with services.
Can be upgraded or expanded with new equipment and line provisioning.	Upgrades usually requires only only bandwidth and software upgrades.
Long distance is usually per minute or bundled minute subscription.	Long distance is often included in regular monthly plan.
Hardwared landline phones (those without an adapter) remain active during power outage.	Loses phone services without power backup in place.

2.1.3. Important Concepts

A .End to end Delay

End to end Delay is the total transit time for packets in a data stream to arrive at the endpoint and it is inevitable in communication system. Delay time is one of the most important factors in determining the quality of a call. Echoing has been a major problem that is caused by end to end delay. However, delay is able to be kept as small as possible by utilizing the project model/ topology. Typically, for optimum VoIP call quality, end to end delay must be less than 150ms. To address this problem, we will simulate our model to see if VOIP can operate within the end-to-end delay of 200 ms threshold.

B. Jitter

Jitter is one the most common VoIP problems. Jitter is the undesired time delay from the packets sending end to receiving end in VoIP or other video communication network. The jitter can be affected by computer usage, the length and quality of the Ethernet cables and some other issues. The delay is inevitable and high levels of jitter leads to large numbers of packets to be discarded by the jitter buffer in the receiving IP phone or gateway. This will result in severe distortion in call quality or large increases in delay. Therefore in our case, we want to minimize the jitter as possible as we can.

C. Packet Loss

Failure or one of more packets to reach their destination across the network is recognized as packet loss. The occurrence of lost and dropped packets are extremely noticeable with real time streaming technology such as Skype and online gaming. On another hand, there is always a degree of packet loss allowance in almost every network. There are possible causes that lead to packet loss, such as channel congestion, corrupted packets rejected in-transit and poor networking hardware. To properly recover the loss packets, reliable network transport protocol such as TCP are used insure an acceptable and stable transmission. Using the Acknowledge technology, the network can reassure that the packets have been successfully delivered. In our simulation, we would try to maintain an maximum of 10% packet loss threshold.

2.2. HISTORY OF TELEPHONY

This module explains the general history of telephony. The telephone network, as we know it today, including many of the terms and acronyms and much of the network architecture and existing paradigms, has a foundation in the early days of the telephone and the first telephone systems.

2.2.1. Voice Communication

When humans talk, we expel air from the lungs and move the lips, tongue, and larynx to generate sound waves. The sound waves traverse the air and reach the inner ear of the other party, stimulating the sense of hearing. There is a limitation, however, in the distance and energy level of the sound wave. The distance at which a sound can be heard depends upon the intensity (decibels) and volume (amplitude) of the sound. A walkie-talkie, a microphone, and a residential telephone are all examples of devices that can be used to carry and amplify the sound so it can be heard over a distance. Basically, these and other electronic devices convert voice activity into electrical current or voltage, helping to overcome the problems associated with the nature of the sound wave. The most common example of a telecommunications device is your telephone at home. When you plug an ordinary analog phone into the phone jack installed by the telephone service provider, you are then able to place phone calls. (Note that the voice still could be digitized at some point along the transmission path from source to destination.)

2.2.2 The First Telephone Network

The basic residential analog phone system that exists today is a direct descendent of the company started by the inventor of the telephone, Alexander Graham Bell. In the late nineteenth century if one wanted phone service, one would have to contact the Bell Company to request service and tell the company exactly whom you wanted to be able to call. The phone company would then install wiring between your home or business and that of the party you wanted to call. You, as the customer, would have to provide the telephone itself (it was leased from the Bell company), along with the wiring; you also would be responsible for all installation and maintenance costs. There was no real amplification, so a call would have traveled only as far as the physical wire would carry it.

Within about two years after its founding, the Bell Company realized that it needed some kind of a switching system to be able to service a greater number of customers. The early switches were literally cord boards, which would alert an operator at a central office (CO) to an incoming call, typically by ringing a bell or lighting some type of lamp at the operator's station. This system was user friendly and highly intelligent, but the system did not offer very good performance. Even a fast operator worked at the pace of a human and was capable of handling only one call at a time.

2.2.3. History of VoIP

The concept of VoIP (Voice over Internet Protocol) originated in about 1995, when hobbyists began to recognize the potential of sending voice data packets over the Internet rather than communicating through standard telephone service. This concept allowed PC users to avoid long distance charges, and it was in 1995 that the first Internet Phone Software appeared. While contemporary VoIP uses a standard telephone hooked up to an Internet connection, early efforts in the history of VoIP required both callers to have a computer equipped with the same software, as well as a sound card and microphone. These early applications of VoIP were marked by poor sound quality and connectivity, but it was a sign that VoIP technology was useful and promising.

VoIP evolved gradually over the next few years, gradually reaching the point where some small companies were able to offer PC to phone service in about 1998. Phone to phone service soon followed, although it was often necessary to use a computer to establish the connection. Like many Internet applications in the late 1990's, early VoIP service relied on advertising sponsorship to subsidize costs, rather than by charging customers for calls. The gradual introduction of broadband Ethernet service allowed for greater call clarity and reduced latency, although calls were still often marred by static or difficulty making connections between the Internet and PSTN (public telephone networks). However, startup VoIP companies were able to offer free calling service to customers from special locations.

The breakthrough in VoIP history came when hardware manufacturers such as Iwatsu started producing VoIP equipment that was capable of switching. What that meant was that functions that previously had to be handled by a computer's CPU, such as "switching" a voice data packet into something that could be read by the PSTN (and vice versa) could now be done by another device, thus making VoIP hardware less computer dependent. Once hardware started becoming more affordable, larger companies were able to implement VoIP on their internal IP networks, and long distance providers even began routing some of the calls on their networks over the Internet.

Since 2000, VoIP usage has expanded dramatically. There are several different technical standards for VoIP data packet transfer and switching and each is supported by at least one major manufacturer – Iwatsu a clear "winner" has emerged to adopt the role of a universal standard. While companies often switch to VoIP to save on both long distance and infrastructure costs, The true benefit of VoIP service is to extended the office beyond the borders of a single office location into multiple locations. In just a few short years, VoIP has gone from being a fringe development to a mainstream alternative to standard telephone service.

.2.3. OBJECTIVE OF STUDY

The purpose of the project is to conduct several of test cases in VoIP by constructing different simulation scenarios under CISCO PACKET TRACER Software. The reason behind it is that the successful implement of the project would reflect the advantage of VoIP over the traditional PSTN and thus proving that VoIP would be ideal candidate for the modern technology in network communication.

In the perspective of a good design of VoIP, the most important factor would be the quality of service (QoS) provided to all users on the network, while considering medium-to-high traffic loads that is most likely to occur in reality. Due to the fact that initially IP networks were designed to handle data traffic and not voice, there was no issue regarding to real-time communication. However, factors that might influence the overall performance of VoIP are bandwidth, end-to-end delay, jitter, packet lost rate and utilization[4]. Base on the standard provided by the International Telecommunications Union, the acceptable Mean Opinion Score (MOS) for VoIP is in the range of 4 to 4.5. As indicated in the following figure, the latency (ETE delay) shall not be above 150ms in one way service level. As in terms of jitter, which is the measure of the inconsistency of delay of packet delivery, is approximately 20 ms in range of tolerance under the recommendation of ITU.

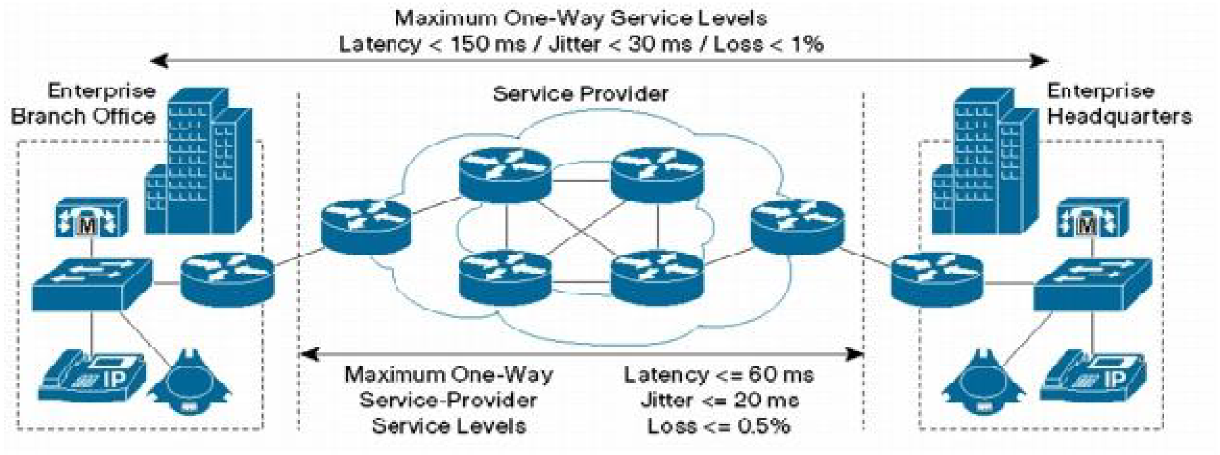

Maximum One-Way Service Levels
Latency < 150 ms / Jitter < 30 ms / Loss < 1%
Enterprise Branch Office
Service Provider
Enterprise Headquarters
M
IP
M
IP
Maximum One-Way Service-Provider Service Levels
Latency <= 60 ms
Jitter <= 20 ms
Loss <= 0.5%

Figure 1.3 Tolerance range of VoIP

Statistics parameters to be collected and evaluated are ETE delay, delay variation, packet sent and drop rate, and jitter under WLAN802.11g and Ethernet networks under the scenarios shown in Figure 1.5. Based on the result, reflections upon the data would be made to ensure the parameters are within the standard of ITU[5][6].

2.4. BENEFITS OF VoIP

2.4.1. Corporate Advantages

A) Lower Recurring Transmission Charges: By directing voice calls over the corporate data network, rather than through a carrier, companies can significantly reduce their monthly phone bills. These savings are obviously dependent on several factors, including the volume of intracompany calls and the distances between company offices. Companies with overseas offices, obviously, can experience the greatest savings, since they can eliminate a great deal of international long-distance charges. These charges are often particularly high when the call originates in a foreign country that still has a highly monopolistic telecom market. In some configurations, these savings can be extended to calls outside of the company as well using PSTN gateways.

B) Economic Factors: The economic appeal of transmitting voice calls over the data network arises from two technical factors. First, data networks almost always have spare capacity. Network managers typically over-provision IP networks to allow room for growth and to avoid congestion during periods of peak utilization. At the same time, voice calls consume relatively little bandwidth. The characteristics of human speech, especially the comparatively large amount of silence that takes place during conversations, allows for a great deal of compression in the digitized transport of the call. This makes it possible for voice to ``piggyback" on existing data network connections without requiring investments in adding to the capacity of those connections. Even when such additions have to be made to the existing network because of call volumes, those costs are insignificant compared to the recurring costs charged by carriers to carry that same calling volume.

C) Reduced Long-term Network Ownership Costs: In addition to reducing a company's monthly phone bills, converged network architecture also reduces the ongoing costs of owning two separate networks --- one for voice and one for data. These costs include the need to buy two separate sets of equipment, the staff time dedicated to the operation and maintenance of that equipment, the licensing of any software relating to the management of that equipment, and the monitoring of traffic on the two networks. With the Internet revolution in full swing, the demand for skilled, experienced technicians far outstrips supply. This has driven salaries for voice and data network staff through the roof, and has also made it difficult to recruit and retain such engineering talent. Companies that are able to reduce their need for technical staff by streamlining their network operations can therefore eliminate many of the human resource management headaches that plague their competitors.

D) Advanced Applications: The most compelling aspect of converged voice/data networking may well be the new generation of applications it enables. These applications include Web enabled call centers, unified messaging and real-time collaboration. Other examples include real-time multimedia video/audio conferencing, distance learning, and the embedding of voice links into electronic documents. Three or four years ago, the Internet was not ready for prime time as a medium for commerce. But now it is. VoIP will be a valuable enhancement.

2.5 APPLICATIONS OF VoIP

VoIP can be defined as the ability to make telephone calls (i.e., to do everything we can do today with the PSTN) and to send facsimiles over IP-based data networks with a suitable quality of service (QoS) and a much superior cost/benefit. VoIP could be applied to almost any voice communications requirement, ranging from a simple inter-office intercom to complex multi-point teleconferencing/shared screen environments. The quality of voice reproduction to be provided could also be tailored according to the application. Customer calls may need to be of higher quality than internal corporate calls, for example. Hence, VoIP equipment must have the flexibility to cater to a wide range of configurations and environments and the ability to blend traditional telephony with VoIP.

Some examples of VoIP applications that are likely to be useful would be:

a) **PSTN gateways**: Interconnection of the Internet to the PSTN can be accomplished using a gateway, either integrated into a PBX or provided as a separate device. A PC-based telephone, for example, would have access to the public network by calling a gateway at a point close to the destination (thereby minimizing long distance charges). This will be discussed in detail later.

b) **Internet-aware telephones**: Ordinary telephones (wired or wireless) can be enhanced to serve as an Internet access device as well as providing normal telephony. Directory services, for example, could be accessed over the Internet by submitting a name and receiving a voice (or text) reply.

c) **Remote access from a branch (or home) office:** A small office (or a home office) could gain access to corporate voice, data, and facsimile services using the company's Intranet (emulating a remote extension for a PBX, for example). This may be useful for home-based agents working in a call center, for example.

d) **Voice calls from a mobile PC via the Internet:** Calls to the office can be achieved using a multimedia PC that is connected via the Internet. One example would be using the Internet to call from a hotel instead of using expensive hotel telephones. This could be ideal for submitting or retrieving voice messages.

e) **Internet call center access:** Access to call center facilities via the Internet is emerging as a valuable adjunct to electronic commerce applications. Internet call center access would enable a customer who has questions over the Internet to access customer service agents online. Another VoIP application for call centers is the interconnection of multiple call centers. Take the example of a Web-enabled call center. One of the biggest obstacles that companies face in converting Web site visitors into Web site buyers is poor online interaction. In a store, customers can ask a nearby salesperson a question that may end up determining whether or not they head for the checkout line. On a Web site, that kind of interaction is more problematic. But using VoIP, site visitors can click a button and open up a voice conversation with a real, live call center agent who can quickly address any question or problem the customer might have.

SECTION – II

3.1. BASICS OF PROTOCOLS AND PROTOCOL ARCHITECTURE

3.1.1. OSI Reference Model

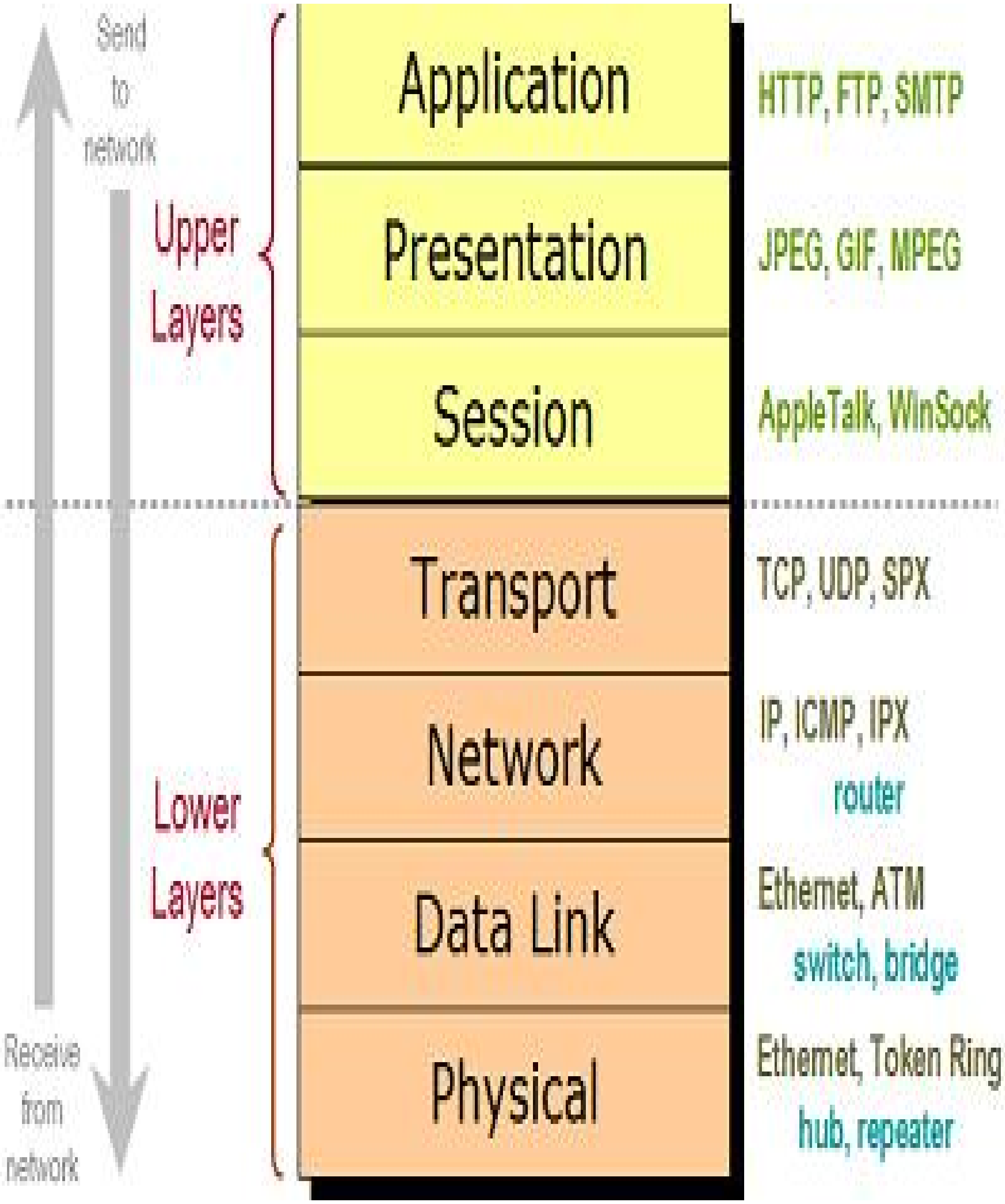


Figure 2.1 OSI Reference Model

Physical layer:This layer is responsible for the mechanical, electrical, functional and procedural mechanism required for the transmission of data. It can be considered to represent the physical connection of a device to a transmission media.

Data link layer: The data link layer is responsible for the manner in which data is formatted into defined fields and the correction of any errors occurring during a transmission session. It is responsible for framing as well as flow control, error detection and correction.

Network layer: Provides upper layer with independence from the data transmission and switching technologies used to connect system. Responsible for establishing, maintaining and terminate connections.

Transport layer: Provides reliable and transparent transfer of data between end points. The transport layer also provides end-to-end error recovery and flow control.

Session layer: This layer is responsible for establishing and terminating data streams between network nodes. Since each data stream can represent an independent application, the session layer is also responsible for coordinating communications between different applications that require communications.

Presentation layer: Provides independence to the application processes from differences in data representation.

Application layer: Provides access to the OSI environment for users and also provides distributed information services.

3.1.2. TCP/IP Protocol Suite

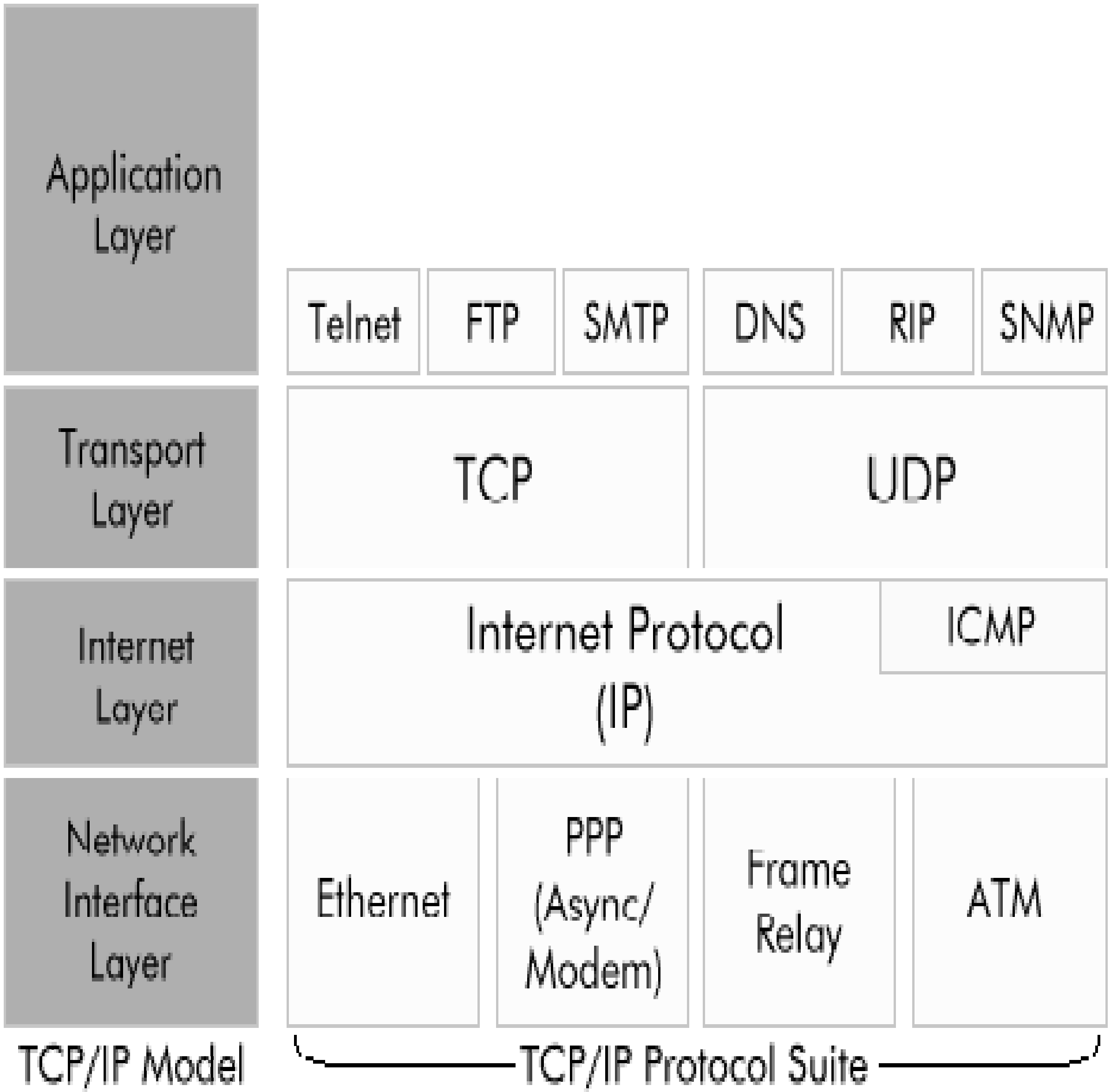


Figure 2.2 TCP/IP Reference Model

TCP/IP is a result of protocol research and development conducted on the experimental packet-switched network, ARPANET, funded by the Defense Advanced Research Projects Agency (DARPA), and is generally referred to as the TCP/IP protocol suite. This protocol suite consists of a large collection of protocols that have been issued as Internet standards by the Internet Architecture Board (IAB). There is no official TCP/IP protocol model as there is in the case of

OSI. However, based on the protocol standards that have been developed, the communication task for TCP/IP can be organized into five relatively independent layers. The most common protocols are presented.

Physical layer: This Layer is responsible for the mechanical, electrical, functional and procedural mechanism required for the transmission of data. It can be considered to represent the physical connection of a device to a transmission media.

Network access layer: This layer is responsible for accepting and transmitting IP datagrams. It is also concerned with the exchange of data between an end system and the network to it is attached. The sending computer must provide the network with the physical address of the destination computer, so that the network may route the data to the appropriate destination. Ethernet, IBM token ring, PPP (Point to Point Protocol), LAPD, LAPB etc are used at this level. It is analogous to the data link layer of OSI.

Internet layer: This layer handles communication from one machine to the other. It accepts a request to send data from the transport layer, along with the identification of the destination. It encapsulates the transport layer data unit in an IP datagram and uses the datagram routing algorithm to determine whether to send the datagram directly onto a router. The Internet layer also handles the incoming datagrams and uses the routing algorithm to determine whether the datagram is to be processed locally or to be forwarded.

3.2. ROUTING

Routing is the process of selecting paths in a network along which to send network traffic and route is the path to send the network traffic.

There are two ways a router learn a route: static and dynamic. The difference between static route and dynamic route is as below. A static route is a route that is manually configured on the router. Simply we can say a static route is a route that is created manually by a network administrator. The information about the networks that are directly connected to the active router interfaces are added to the routing table initially and they are known as connected routes. The second way that the router can learn static routes are by configuring the routes manually.

Dynamic routes are routes that a router learns by using a routing protocol. Routing protocols will learn about routes from other neighbouring routers running the same routing protocol. Dynamic routing protocols share network numbers a router knows about and how to reach these networks. Through this sharing process, a router can learn about all of the reachable network numbers in the network.

3.2.1. Routing Information Protocol (RIP)

The **Routing Information Protocol** (**RIP**) is one of the oldest distance-vector routing protocols, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance, in other words the route is considered unreachable. RIP implements the split horizon, route poisoning and hold down mechanisms to prevent incorrect routing information from being propagated.

Originally, each RIP router transmitted full updates every 30 seconds. In the early deployments, routing tables were small enough that the traffic was not significant. As networks grew in size, however, it became evident there could be a massive traffic burst every 30 seconds, even if the routers had been initialized at random times. It was thought, as a result of random initialization, the routing updates would spread out in time, but this was not true in practice. Sally Floyd and Van Jacobson showed in 1994 that, without slight randomization of the update timer, the timers synchronized over time. In most current networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS (the latter two being link-state routing protocols), and a hop limit severely limits the size of network it can be used in. However, it is easy to configure, because RIP does not require any parameters on a router unlike other protocols.

RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.

There are three versions of the Routing Information Protocol: *RIPv1*, *RIPv2*, and *RIPng*.

RIP version 1

The original specification of RIP, defined in RFC 1058, was published in 1988 and uses classful routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). This limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size. There is also no support for router authentication, making RIP vulnerable to various attacks.

RIP version 2

Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed in 1993[4] and last standardized in 1998. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier specification if all *Must Be Zero* protocol fields in the RIPv1 messages are properly specified. In addition, a *compatibility switch* feature allows fine-grained interoperability adjustments.

In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 *multicasts* the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications.

(MD5) authentication for RIP was introduced in 1997.

RIPv2 is Internet Standard STD56 (which is RFC 2453).

Route tags were also added in RIP version 2. This functionality allows for routes to be distinguished from internal routes to external redistributed routes from EGP protocols.

RIPng

RIPng (RIP next generation), defined in RFC 2080, is an extension of RIPv2 for support of IPv6, the next generation Internet Protocol. The main differences between RIPv2 and RIPng are:

- Support of IPv6 networking.

- While RIPv2 supports RIPv1 updates authentication, RIPng does not. IPv6 routers were, at the time, supposed to use IPsec for authentication.
- RIPv2 allows attaching arbitrary tags to routes, RIPng does not,
- RIPv2 encodes the next-hop into each route entry, RIPng requires specific encoding of the next hop for a set of route entries.

RIPng sends updates on UDP port 521 using the multicast group FF02::9.

3.2.2. Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a routing protocol developed for Internet Protocol (IP) networks by the interior gateway protocol (IGP) working group of the Internet Engineering Task Force (IETF). OSPF is a classless routing protocol, which means that in its updates, it includes the subnet of each route it knows about, thus, enabling variable-length subnet masks. With variable-length subnet masks, an IP network can be broken into many subnets of various sizes. This provides network administrators with extra network-configuration flexibility

OSPF has two primary characteristics:

1) The protocol is open (non proprietary), which means that its specification is in the public domain. The OSPF specification is published as Request For Comments (RFC) 1247.

2) The second principal characteristic is that OSPF is based on the SPF algorithm, which sometimes is referred to as the Dijkstra algorithm, named for the person credited with its creation.

3.2.3. Border Gateway Protocol (BGP)

BGP stands for Border Gateway Protocol and the most current version is BGP4. BGP is a routing protocol (software) that runs on routers._ BGP allows decentralized management of the Internet,that means, if you have a BGP router on the Internet, you can tell all other routers what networks you have available to everyone in the world._ BGP is called a path vector routing protocol and its main metric is “shortest AS path”. That means that it selects the best path, through the Internet, by choosing the route that has to traverse the fewest autonomous systems. If you want to run BGP, you will have to talk to your Internet Service Providers to see if they will agree to communicate with you via BGP. You will have to show your need to run BGP.

3.2.4. Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary gateway protocol. EIGRP uses a composite metric composed of Bandwidth, Delay, Reliability, and Loading to determine the best path between two locations. In a EIGRP network, each router multi-casts "hello" packs to discover its adjacent neighbor. This adjcency database is shared with other router to build a topology database. From the topology database the best route (Successor) and the second best route (Feasible Successor) is found. EIGRP is classless, meaning it does include the subnet mask in routing updates.

3.3. WLAN 802.11g

802.11 and 802.11x refers to a family of specifications developed by
the IEEE for ***wireless*** **LAN** (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

802.11g — applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands.

3.4. ETHERNET LAN NETWORK

Ethernet is a physical and data link layer technology for local area networks (LANs). Ethernet uses a bus or star topology and supports data transfer rates of 10Mbps. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards. Ethernet is the major LAN technology because of the following characteristics:

- Is easy to understand, implement, manage, and maintain
- Allows low-cost network implementations
- Provides extensive topological flexibility for network installation
- Guarantees successful interconnection and operation of standards-compliant products, regardless of manufacturer.

3.5. LAN WITH FTP

FTP stands for File Transfer Protocol and is a way of uploading and downloading your data to the internet.

To make an FTP connection you can use a dedicated FTP software program, also referred to as a FTP client.

FTP makes data sharing faster between two systems on LAN.

3.6. ELECTROMAGNETIC INTERFERENCE AT 2.4GHz

Many short-range wireless devices such as Bluetooth and wireless LANs operate in the 2.4 GHz ISM band as specified by the standards 802.11b, 802.11g and 802.11n. this can cause a significant decrease in speed, that’s why its necessary to monitor VoIP performance at 2.4GHz

3.7. WLAN NETWORK

A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. The key hardware components of a wireless computer network include adapters, routers and access points, antennas and repeaters.

Wireless routers function comparably to traditional routers for wired Ethernet networks.

Access points and routers often utilize a Wi-Fi wireless antenna that significantly increase the communication range of the wireless radio signal.

A wireless repeater connects to a router or access point. Often called signal boosters or range expanders.

SECTION – III

4.1. DESCRIPTION OF OVERALL DESIGN

4.1.1. Overall LAN and WLAN Model

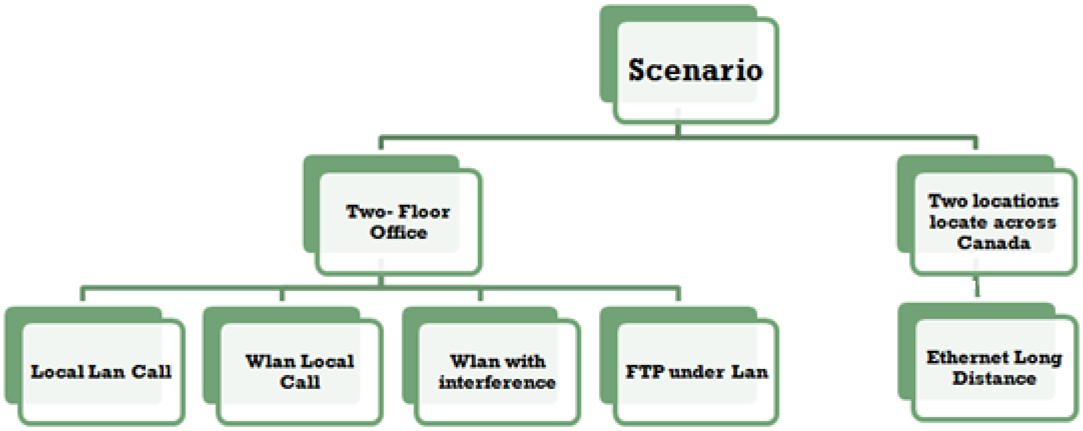


Figure 3.1 Simulation scenarios break down

The overall network model is shown below – a model implemented in CISCO PACKET TRACER

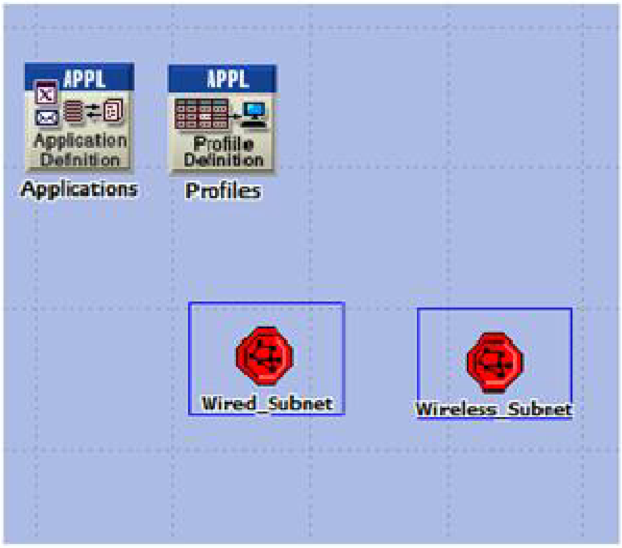
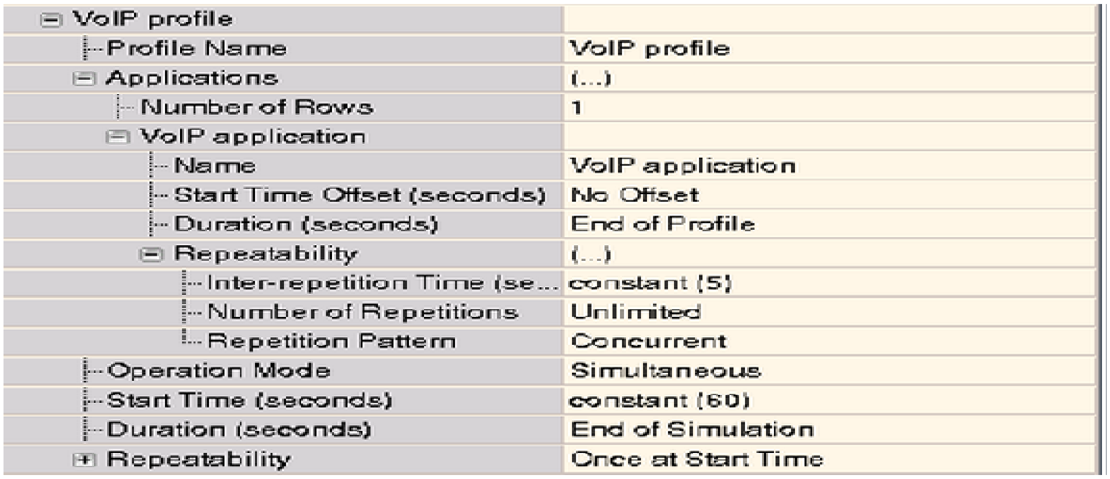
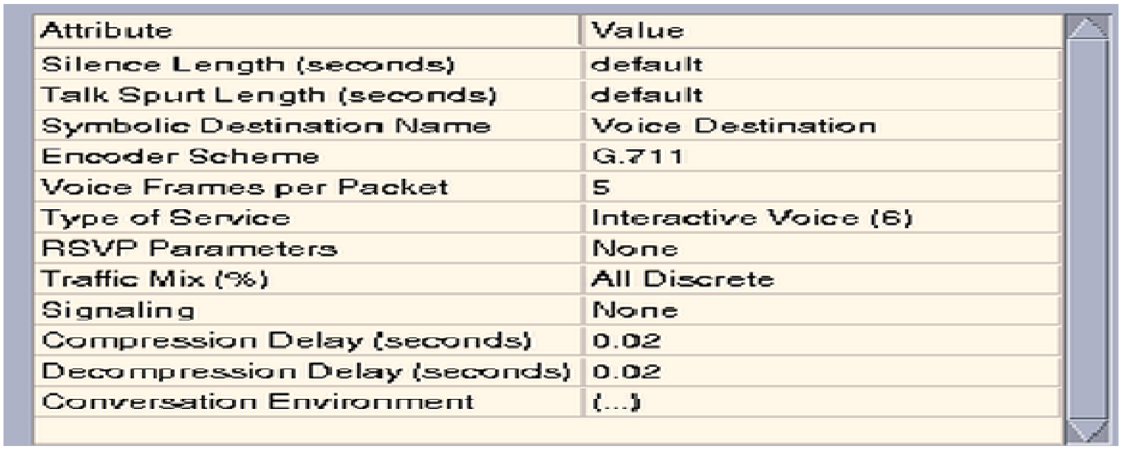


Figure 3.2 Implementation of VoIP

The Project divided into two major scenarios parts: Local two-floor office model and two-locations-far model.



⊟ VoIP profile	
Profile Name	VoIP profile
⊟ Applications	(...)
Number of Rows	1
⊟ VoIP application	
Name	VoIP application
Start Time Offset (seconds)	No Offset
Duration (seconds)	End of Profile
⊟ Repeatability	(...)
Inter-repetition Time (se...	constant (5)
Number of Repetitions	Unlimited
Repetition Pattern	Concurrent
Operation Mode	Simultaneous
Start Time (seconds)	constant (60)
Duration (seconds)	End of Simulation
⊞ Repeatability	Once at Start Time



Attribute	Value
Silence Length (seconds)	default
Talk Spurt Length (seconds)	default
Symbolic Destination Name	Voice Destination
Encoder Scheme	G.711
Voice Frames per Packet	5
Type of Service	Interactive Voice (6)
RSVP Parameters	None
Traffic Mix (%)	All Discrete
Signaling	None
Compression Delay (seconds)	0.02
Decompression Delay (seconds)	0.02
Conversation Environment	(...)

3.3 Configuration and Designs

The project consist total of six independent scenarios as shown in Figure 3.1. Using these models as backbone, the performance of VoIP shall be compared under the follow circumstances:

1. Local call versus Long Distance Calls
2. WLAN 802.11g versus Ethernet LAN Network
3. Increasing Traffic Load
4. LAN with FTP access during Voice transmission
5. 2.4GHz Interference to WLAN Network

4.1.3. Topology of company with two floors

As indicated in the scenarios break down chart, this section provides the detail of the CISCO PACKET TRACER simulation with specific parameters and topology. First is the network with the size of 100 X 100 m in dimension, or categorized as office in OPNET. The office is divided into two floors with multiple work stations in each floor. The stations are located 15m apart from each other and are connected through 10 Base T line to the Ethernet switch. The overall network is hooked up to a CISCO 400 which acts has router. The topology is setup in such way to achieve an LAN environment for the small office to establish VoIP communications.

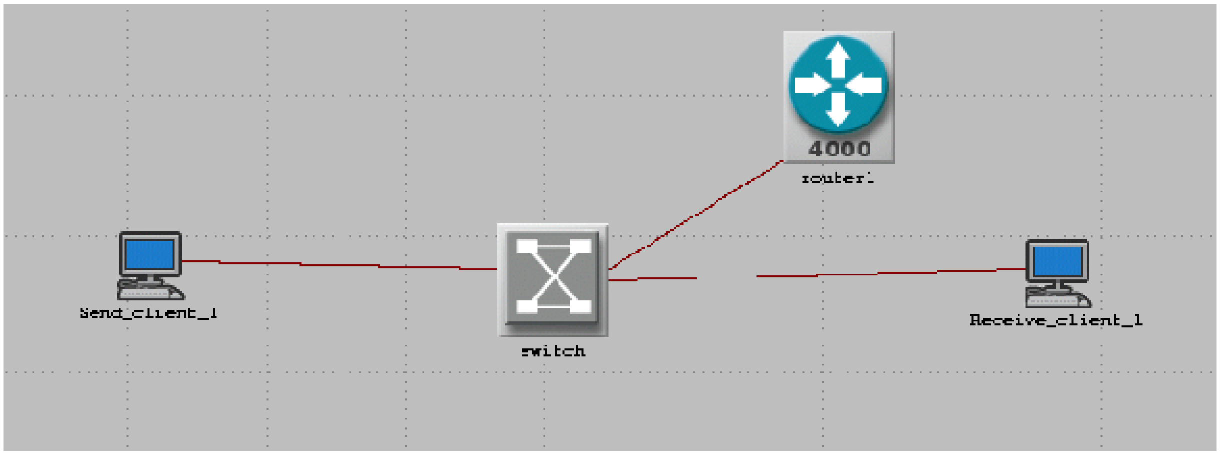


Figure 3.4 Basic LAN VoIP network

After implementing the backbone structure of the two-floor office LAN model, we increase the amount of Ethernet work station and compare the overall performance to the initial model.
One special note, although there are many Ethernet stations presents in each floor, only one work station (send client) is making a one to one VoIP call to another work station (Receive client) located in the other floor, no conference has been establish.

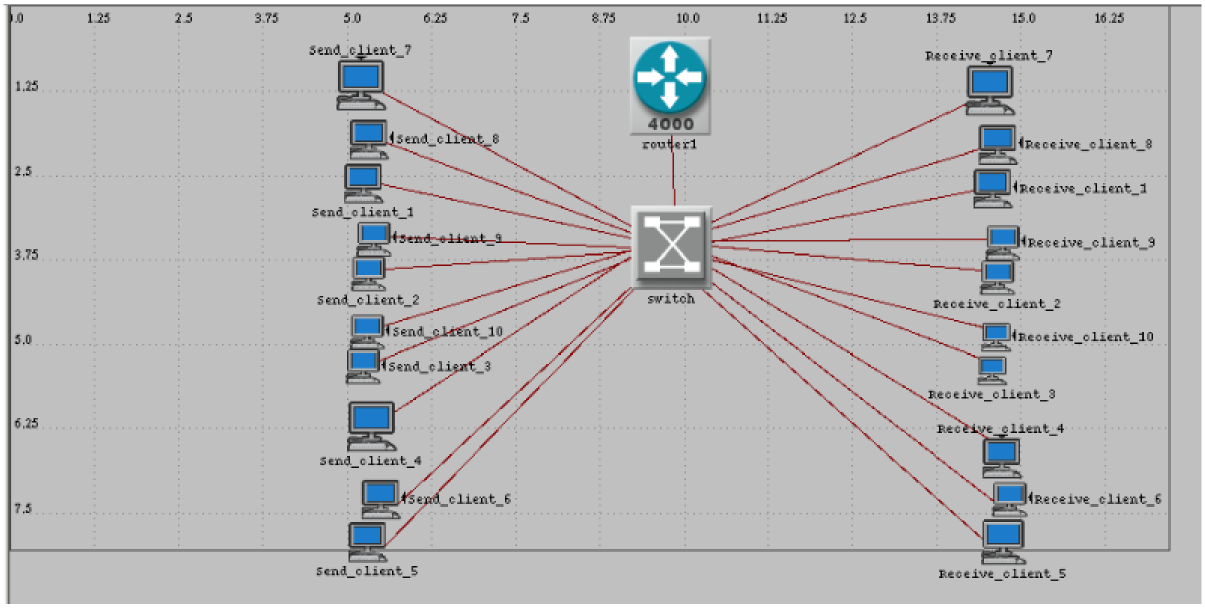


Figure 3.5 LAN 20 VoIP Network

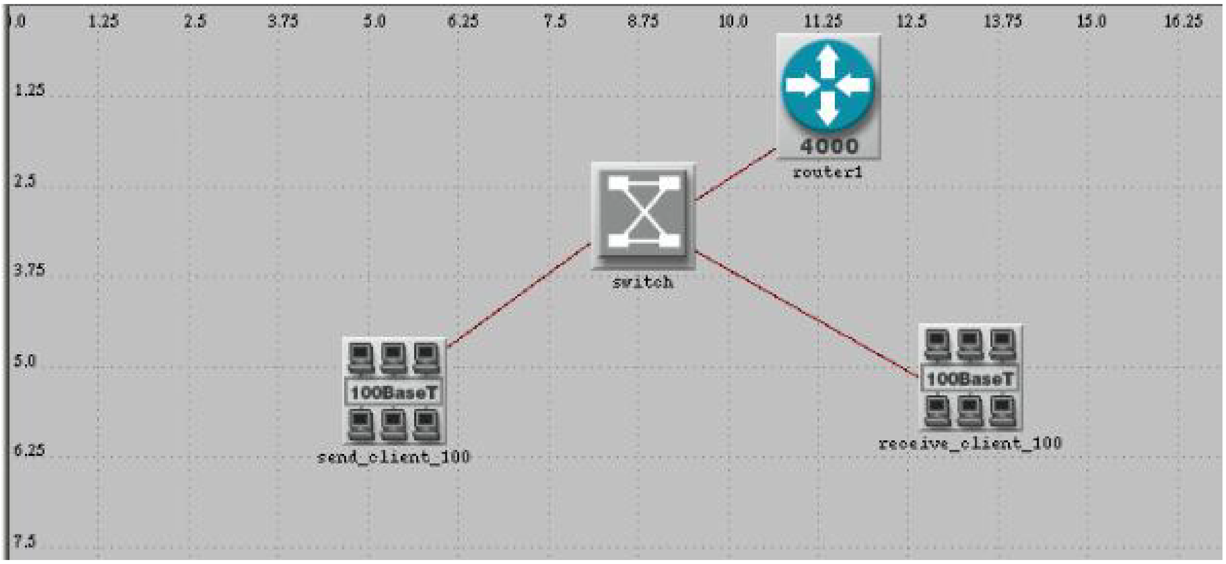
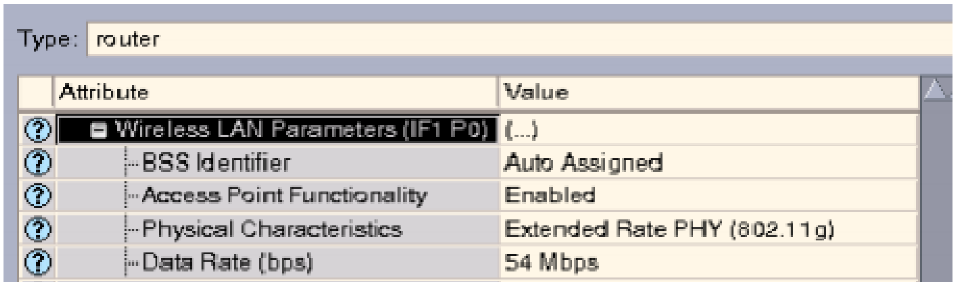


Figure 3.6 LAN 100 VoIP Network

4.1.4. Topology of Wireless Network

The topology for wireless (WLAN) VoIP connection under the standard of IEEE 802.11g between the two floor office is shown in Figure 2.1.2. The router is located in the center of the two wireless work stations. The data rate is setup to be 54Mbps. Applying the same method, we added more wireless work stations around the wires router and compare the result. However, there is no conference call in the WLAN network.



Type: router

Attribute	Value
⊟ Wireless LAN Parameters (IF1 P0)	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Enabled
Physical Characteristics	Extended Rate PHY (802.11g)
Data Rate (bps)	54 Mbps

Figure 3.7 Configuration of Router

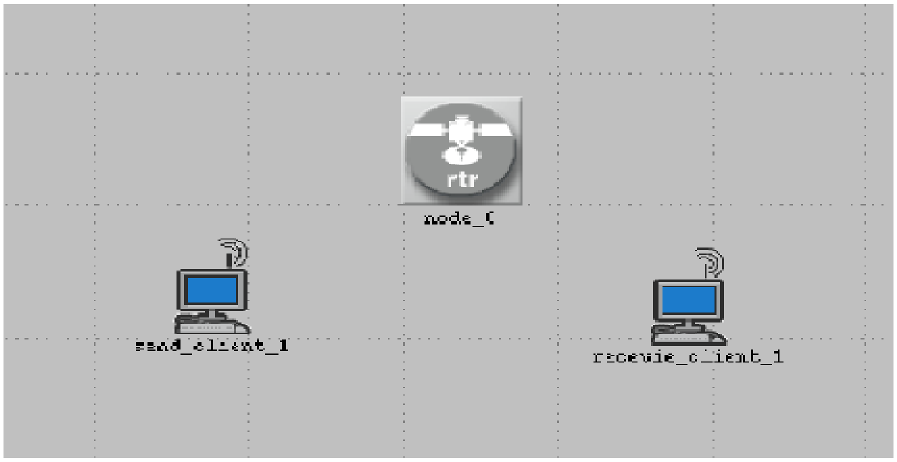


Figure 3.8 Basic WLAN VoIP Network

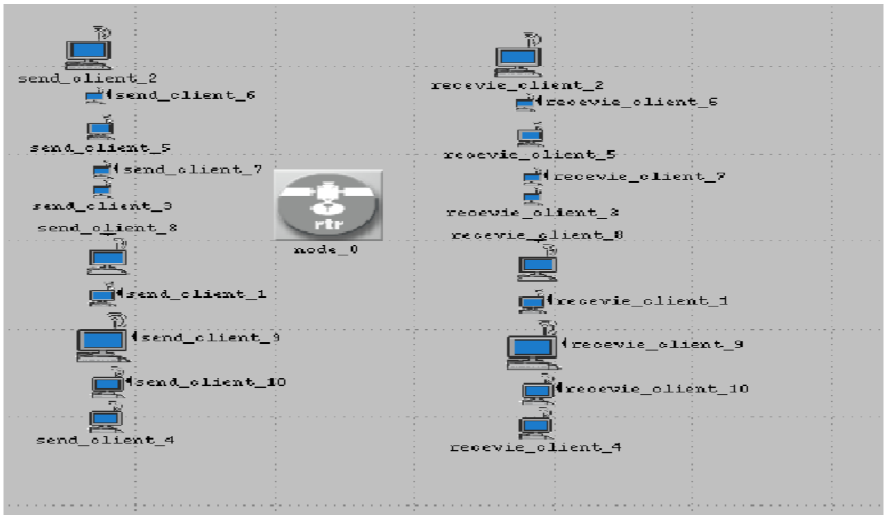


Figure 3.9 Multiple WLAN Network

4.1.5. Topology of two companies located far apart

The network which two locations (offices) are located relative far apart from each other provide an realistic simulation on long distance VoIP communication under Ethernet connect. The two locations' routers are interconnected with PPP DS0. One interest thing to note, WiMAX along with WiFi would also be an ideal candidate to establish long distance VoIP calls. The topology inside the two subnet applies the same network structure as the initial two-floor-office topology.

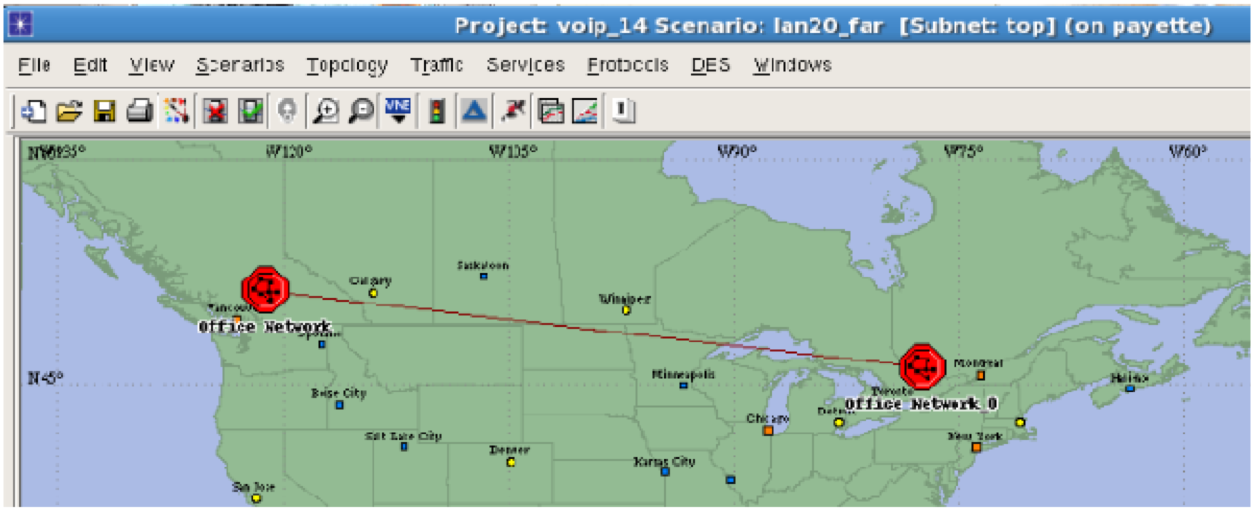


Figure 3.10 LAN VoIP for far apart locations

4.1.6. Topology of LAN with FTP

Under the FTP scenario, a **File Transfer Protocol** (**FTP**) model is added to the Ethernet switch. By adding the FTP, we would expect the traffic load to increase and reduce in bandwidth usage since the work stations are making a VoIP call and accessing the FTP simultaneously. We are interested in whether the FTP is TCP-friendliness with VoIP or not.

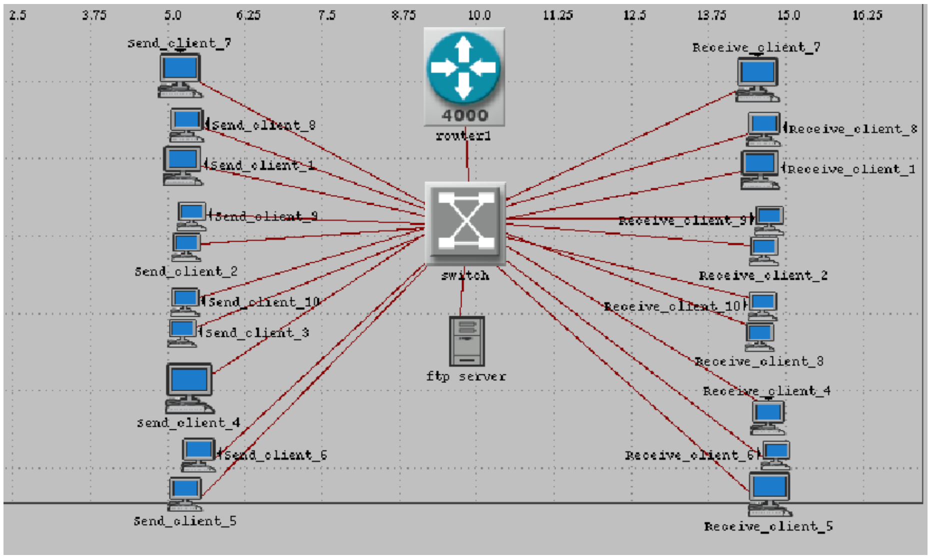
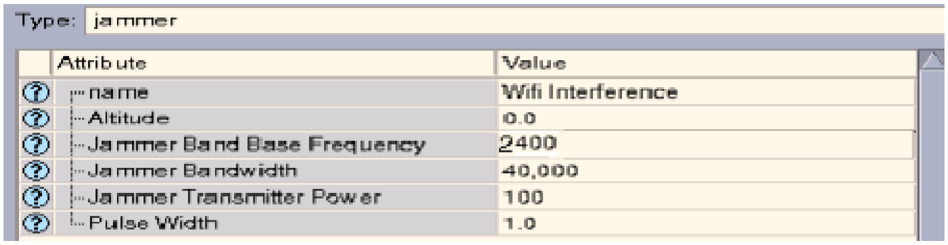


Figure 3.11 FTP in VoIP

4.1.7. Topology of wireless network with interference

Since the WLAN 802.11g operates in the frequency range of 2.4GHz, and it is known that many other electronic devices such microwave, Bluetooth and video devices are also potential user of the 2.4GHz band user, interference is inevitable. Under this section, a 2.4 GHz jammer next is added to the model to simulate this situation.



Type: jammer

Attribute	Value
name	Wifi Interference
Altitude	0.0
Jammer Band Base Frequency	2400
Jammer Bandwidth	40,000
Jammer Transmitter Power	100
Pulse Width	1.0

Figure 3.12 Configuration of Jammer

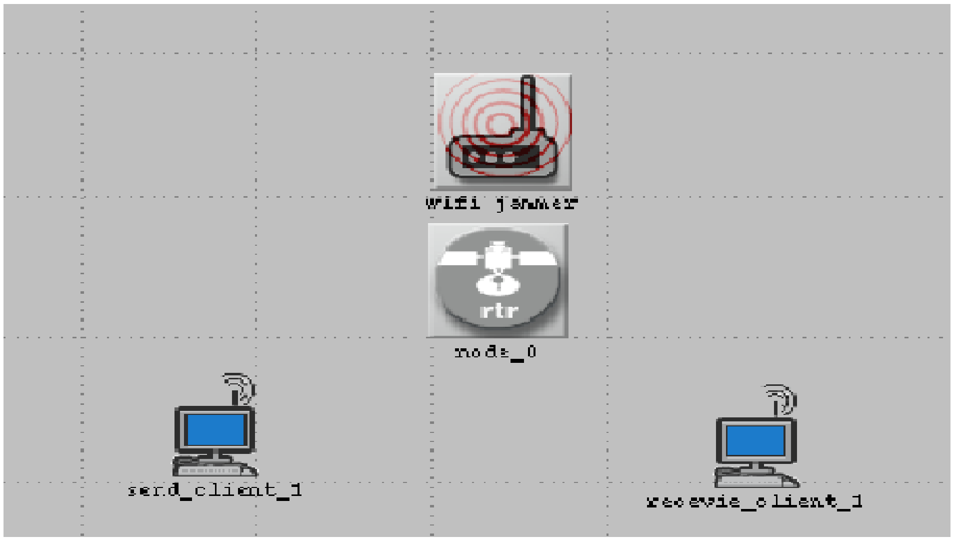


Figure 3.12 Basic WLAN with Jammer

SECTION IV

5.1 HANDS ON EXPERIENCE

5.1.1 LAB-1: CISCO IOS COMMAND LINE INTERFACE

OBJECTIVE: Configure ROUTERS with IP addresses and configure static on the routers

Goals:

1. Set the Host name and bring up the interface.
2. Ping the directly connected Networks
3. Configure static routing.
4. Verify that you can ping all routers.

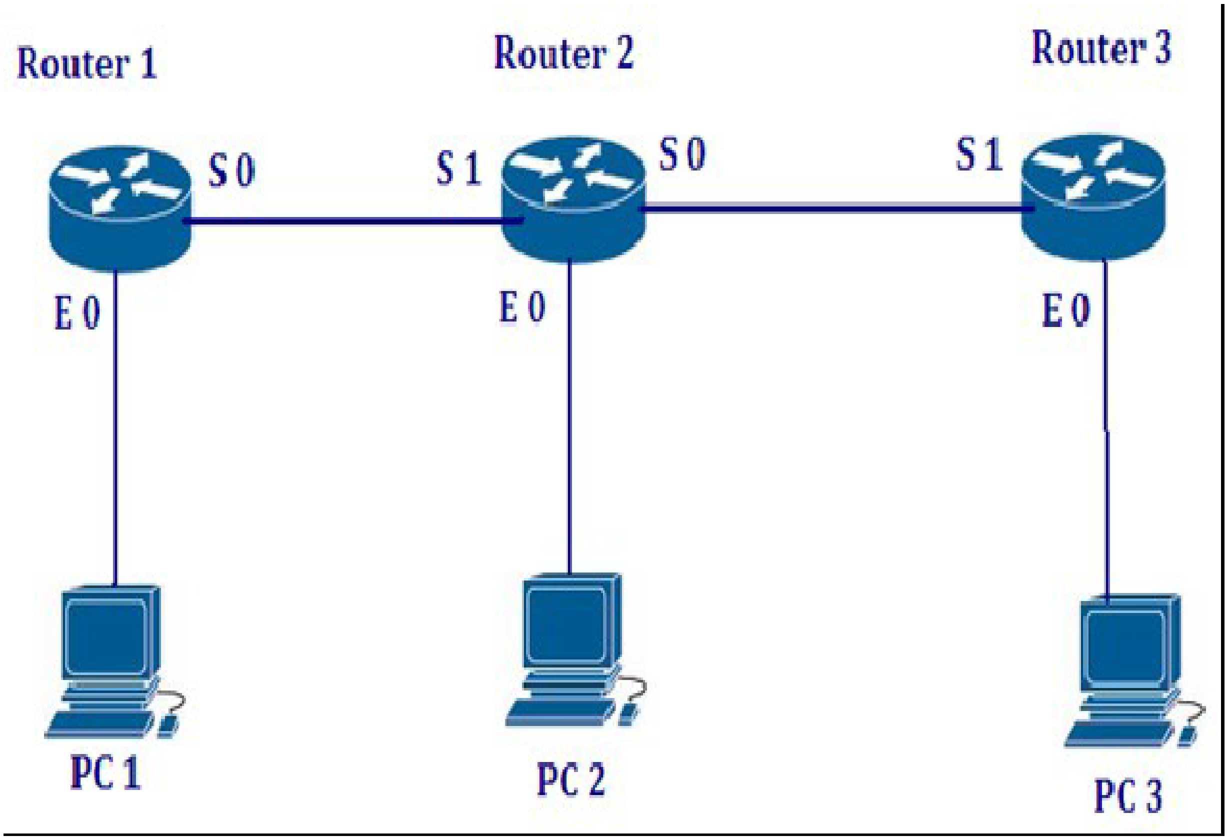


Figure 4.1

DEVICE	INTERFACE	IP ADDRESS	SUBNET MASK
ROUTER 1	S0	192.168.20.1	255.255.255.0
ROUTER 1	E0	192.168.10.1	255.255.255.0
ROUTER 2	S0	192.168.40.1	255.255.255.0
ROUTER 2	S1	192.168.20.2	255.255.255.0
ROUTER 2	E0	192.168.30.1	255.255.255.0
ROUTER 3	S0	192.168.40.2	255.255.255.0
ROUTER 3	E0	192.168.50.1	255.255.255.0
PC 1	GATEWAY=192.168.10.1	192.168.10.5	255.255.255.0
PC 2	GATEWAY=192.168.30.1	192.168.30.9	255.255.255.0
PC 3	GATEWAY=192.168.50.1	192.168.50.4	255.255.255.0

Router1

```
Router>enable
Router#config terminal
Router(config)#hostname Router1
Router1(config)#interface serial 0
Router1(config-if)#clock rate 64000
Router1(config-if)#ip address 192.168.20.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface Ethernet 0
Router1(config-if)#ip address 192.168.10.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#exit
```

```
Router1#show ip interface brief
Router1#show ip route [to display routing table]
Router1(config)#ip routing
Router1(config)#ip route 192.168.30.0 255.255.255.0
192.168.20.2
Router1(config)#ip route 192.168.40.0 255.255.255.0
192.168.20.2
Router1(config)#ip route 192.168.50.0 255.255.255.0
192.168.20.2
Router1(config)#exit
Router1(config)#exit
Router1#show ip route
```

TESTING:

From Router

```
Router1#ping 192.168.30.9
Router1#ping 192.168.40.2
Router1#ping 192.168.50.4
Router1#traceroute 192.168.50.4
```

From the PC

```
ping 192.168.50.4
tracert 192.168.50.4
```

CONFIGURE ROUTER 2, ROUTER 3 ACCORDINGLY AND PING THE ROUTERS AND DEVICES TO CONFIRM CONNECTION.

5.1.2. LAB-2: IP ROUTING (STATIC)

OBJECTIVE: Configure ROUTERS with IP addresses and configure static on the routers

Goals:

1. Set the Host name and bring up the interface.
2. Ping the directly connected Networks
3. Configure static routing.
4. Verify that you can ping all routers.

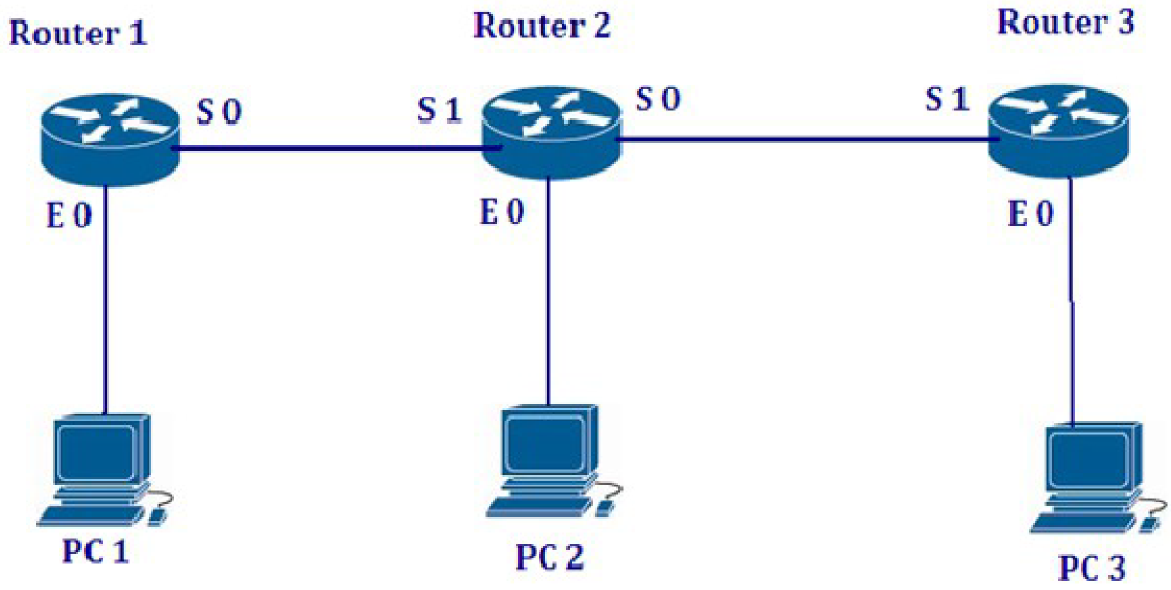


Figure 4.2

DEVICE	INTERFACE	IP ADDRESS	SUBNET MASK
ROUTER 1	S0	192.168.20.1	255.255.255.0
ROUTER 1	E0	192.168.10.1	255.255.255.0
ROUTER 2	S0	192.168.40.1	255.255.255.0
ROUTER 2	S1	192.168.20.2	255.255.255.0
ROUTER 2	E0	192.168.30.1	255.255.255.0
ROUTER 3	S0	192.168.40.2	255.255.255.0
ROUTER 3	E0	192.168.50.1	255.255.255.0
PC 1	GATEWAY=192.168.10.1	192.168.10.5	255.255.255.0
PC 2	GATEWAY=192.168.30.1	192.168.30.9	255.255.255.0
PC 3	GATEWAY=192.168.50.1	192.168.50.4	255.255.255.0

Router1

```
Router>enable
Router#config terminal
Router(config)#hostname Router1
Router1(config)#interface serial 0
Router1(config-if)#clock rate 64000
Router1(config-if)#ip address 192.168.20.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface Ethernet 0
Router1(config-if)#ip address 192.168.10.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#exit
Router1#show ip interface brief
Router1#show ip route [to display routing table]
Router1(config)#ip routing
Router1(config)#ip route 192.168.30.0 255.255.255.0
192.168.20.2
Router1(config)#ip route 192.168.40.0 255.255.255.0
192.168.20.2
Router1(config)#ip route 192.168.50.0 255.255.255.0
192.168.20.2
Router1(config)#exit
Router1(config)#exit
Router1#show ip route
```

TESTING:

From Router

```
Router1#ping 192.168.30.9
Router1#ping 192.168.40.2
Router1#ping 192.168.50.4
```

```
Router1#traceroute 192.168.50.4
```

From the PC

```
ping 192.168.50.4
tracert 192.168.50.4
```

Router 2

```
Router>enable
Router#config terminal
Router(config)#hostname Router2
Router2(config)#interface serial 0
Router2(config-if)#ip address 192.168.40.1 255.255.255.0
Router2(config-if)#clock rate 125000
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#interface serial 1
Router2(config-if)#ip address 192.168.20.2 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#interface Ethernet 0
Router2(config-if)#ip address 192.168.30.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#ip routing
Router1(config)#ip routing
Router2(config)#ip route 192.168.10.0 255.255.255.0
192.168.20.1
Router2(config)#ip route 192.168.50.0 255.255.255.0
192.168.40.2
Router2(config)#exit
Router2#show ip route
```

From Router

```
Router2#ping 192.168.10.5
Router2#ping 192.168.50.4
```

From the PC

```
ping 192.168.10.5
ping 192.168.50.4
```

Router 3

```
Router>enable
Router#config terminal
Router(config)#hostname Router3
Router3(config)#interface serial 1
Router3(config-if)#ip address 192.168.40.2 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#interface Ethernet 0
Router3(config-if)#ip address 192.168.50.1 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#ip routing
Router3(config)#ip routing
Router3(config)#ip route 192.168.10.0 255.255.255.0
192.168.40.1
Router3(config)#ip route 192.168.20.0 255.255.255.0
192.168.40.1
Router3(config)#ip route 192.168.30.0 255.255.255.0
192.168.40.1
Router3(config-router)#exit
Router3(config)#exit
Router3#show ip route
```

TESTING:

From Router

Router3#ping 192.168.10.5

From the PC

ping 192.168.10.5

5.1.3. LAB-3: Open Shortest Path First (OSPF)

OBJECTIVE: Configure ROUTERs with IP addresses and configure OSPF on the routers

Goals:

1. Set the Host name and bring up the interface.
2. Ping the directly connected Networks.
3. Configure inter connectivity using OSPF.
4. Verify that you can ping all routers.

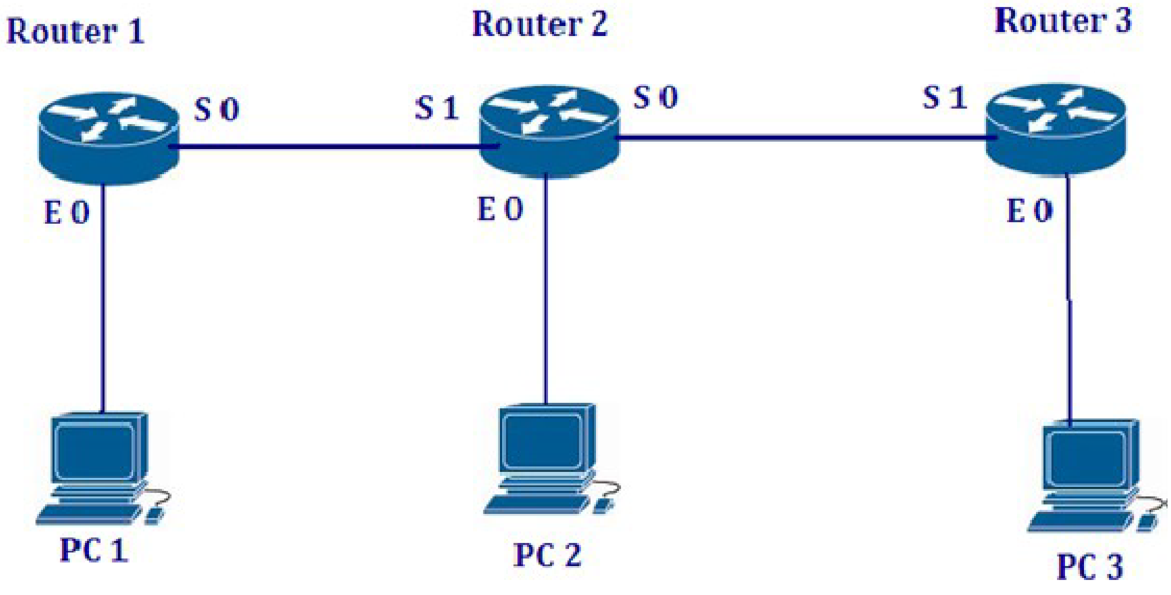


Figure 4.3

DEVICE	INTERFACE	IP ADDRESS	SUBNET MASK	
ROUTER 1	S0	192.168.20.1	255.255.255.0	
ROUTER 1	E0	192.168.10.1	255.255.255.0	
ROUTER 2	S0	192.168.40.1	255.255.255.0	
ROUTER 2	S1	192.168.20.2	255.255.255.0	
ROUTER 2	E0	192.168.30.1	255.255.255.0	
ROUTER 3	S0	192.168.40.2	255.255.255.0	
ROUTER 3	E0	192.168.50.1	255.255.255.0	
PC 1	GATEWAY=192.168.10.1	192.168.10.5	255.255.255.0	
PC 2	GATEWAY=192.168.30.1	192.168.30.9	255.255.255.0	
PC 3	GATEWAY=192.168.50.1	192.168.50.4	255.255.255.0	

Router1

```
Router>enable
Router#config terminal
Router(config)#hostname Router1
Router1(config)#interface serial 0
Router1(config-if)#clock rate 64000
Router1(config-if)#ip address 192.168.20.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface Ethernet 0
Router1(config-if)#ip address 192.168.10.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#exit
Router1#show ip interface brief
Router1#show ip route [display routing table]
Router1(config)#ip routing [starting routing]
```

NOTE:

Now ospf will be configured. 23 is process ID number. Router1 will advertise its neighboring Networks 192.168.20.0 and 192.168.10.0 to other routers. "0.0.0.255" is wild card mask which is reverse of subnet mask of given network. We will configure all network in AREA = 0.

```
Router1(config)#router ospf 23
Router1(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router1(config-router)#network 192.168.10.0 0.0.0.255 area 0
Router1(config-router)#exit
Router1(config)#exit
Router1#show ip route
```

TESTING:

From Router

```
Router1#ping 192.168.30.9
Router1#ping 192.168.40.2
Router1#ping 192.168.50.4
Router1#traceroute 192.168.50.4
```

From the PC

```
ping 192.168.50.4
tracert 192.168.50.4
```

Router 2

```
Router>enable
Router#config terminal
Router(config)#hostname Router2
Router2(config)#interface serial 0
Router2(config-if)#ip address 192.168.40.1 255.255.255.0
Router2(config-if)#clock rate 125000
Router2(config-if)#no shutdown
```

```
Router2(config-if)#exit
Router2(config)#interface serial 1
Router2(config-if)#ip address 192.168.20.2 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#interface Ethernet 0
Router2(config-if)#ip address 192.168.30.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#ip routing
```

NOTE:

Now ospf will be configured. 23 is process ID number. Router2 will advertise its neighboring Networks 192.168.20.0, 192.168.40.0 and 192.168.30.0 to other routers. "0.0.0.255" is wild card mask which is reverse of subnet mask of given network. We will configure all network in AREA = 0.

```
Router2 (config)#router ospf 23
Router2(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router2(config-router)#network 192.168.40.0 0.0.0.255 area 0
Router2(config-router)#network 192.168.30.0 0.0.0.255 area 0
Router2(config-router)#exit
Router2(config)#exit
Router2#show ip route [Note the OSPF routes as "0"]
```

TESTING:

From the Router

```
Router2#ping 192.168.10.5
Router2#ping 192.168.50.4
```

From the PC

```
ping 192.168.10.5
ping 192.168.50.4
```

Router 3

```
Router>enable
Router#config terminal
Router(config)#hostname Router3
Router3(config)#interface serial 1
Router3(config-if)#ip address 192.168.40.2 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#interface Ethernet 0
Router3(config-if)#ip address 192.168.50.1 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#ip routing
```

NOTE:

Now ospf will be configured. 23 is process ID number. Router3 will advertise its neighboring Networks 192.168.40.0 and 192.168.50.0 to other routers. "0.0.0.255" is wild card mask which is reverse of subnet mask of given network.We will configure all network in AREA = 0.

```
Router3(config)#router ospf 23
Router3(config-router)#network 192.168.40.0 0.0.0.255 area 0
Router3(config-router)#network 192.168.50.0 0.0.0.255 area 0
Router3(config-router)#exit
Router3(config)#exit
Router3#show ip route
```

TESTING:

From the Router

```
Router3#ping 192.168.10.5
```

From the PC

```
ping 192.168.10.5
```

5.1.4. LAB-4: Border Gateway Protocol (BGP)

Enabling BGP Routing

To enable BGP routing and establish a BGP routing process, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# router bgp as number	Enables a BGP routing process, which places the router in router configuration mode.
Step 2	Router(config-router)# network network-number [mask network-mask] [route-map route-map-name]	Flags a network as local to this autonomous system and enters it to the BGP table.

Configuring BGP Neighbours

Like other EGPs, BGP must completely understand the relationships it has with its neighbors. Therefore, this task is required.

BGP supports two kinds of neighbors: internal and external. Internal neighbors are in the same autonomous system; external neighbors are in different autonomous systems. Normally, external neighbors are adjacent to each other and share a subnet, while internal neighbors may be anywhere in the same autonomous system.

To configure BGP neighbors, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# neighbor {ipaddress | peer-group-name} remote-as asnumber	Specifies a BGP neighbor.

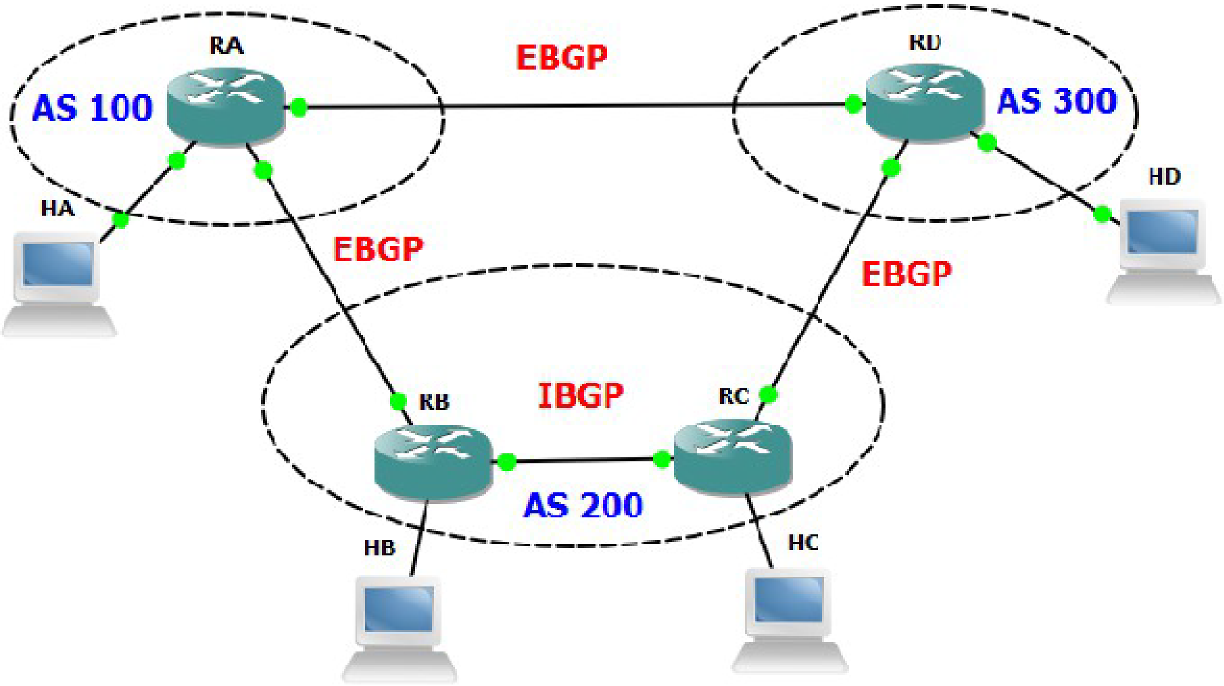


Figure 4.4

Description of BGP Network

Autonomous systems: 100, 200 & 300

Routers: RA in AS-100, RB &RC in AS-200,RD in AS-300

Hosts: HA, HB, HC, HD connected to Routers RA, RB, RC, RD at ports Fa0/1

EBGP relation between Routers RA & RB, RC & RD, RA & RD

IBGP relation between RB & RC

Networks & Hosts connected

LAN at Router RA 172.16.1.0/24
LAN at Router RB 172.16.2.0/24
LAN at Router RC 172.16.3.0/24
LAN at Router RD 172.16.4.0/24

Network 192.168.10.0/30 for Serial Links between RA & RB
IP Addresses 192.168.10.1/30 at RA Serial port serial 0/3/0
192.168.10.2/30 at RB Serial port serial 0/3/1
Network 192.168.20.0/30 for Serial Links between RB & RC
IP Addresses 192.168.20.1/30 at RB Serial port serial 0/3/0
192.168.20.2/30 at RC Serial port serial 0/3/1
Network 192.168.30.0/30 for Serial Links between RC & RD
IP Addresses 192.168.30.1/30 at RC Serial port serial 0/3/0
192.168.30.2/30 at RD Serial port serial 0/3/1
Network 192.168.40.0/30 for Serial Links between RA & RD
IP Addresses 192.168.40.1/30 at RA Serial port serial 0/3/1
192.168.40.2/30 at RD Serial port serial 0/3/0
HA- Host IP 172.16.1.2 Router Interface Fa0/0 IP 172.16.1.1
HB- Host IP 172.16.2.2 Router Interface Fa0/0 IP 172.16.2.1
HC- Host IP 172.16.3.2 Router Interface Fa0/0 IP 172.16.3.1
HD- Host IP 172.16.4.2 Router Interface Fa0/0 IP 172.16.4.1

Configuration of Router RA

```
Router>enable
Router#config terminal
Router(config)#hostname RA
```

```
RA(config)#interface serial 0/3/0
RA(config-if)#ip address 192.168.10.1 255.255.255.252
RA(config-if)#clock rate 128000
RA(config-if)#no shutdown
RA(config-if)#exit
RA(config)#interface serial 0/3/1
RA(config-if)#ip address 192.168.40.1 255.255.255.252
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#interface fastethernet 0/0
RA(config-if)#ip address 172.16.1.1 255.255.255.0
RA(config-if)#no shutdown
RA(config-if)#exit
RA(config)#interface loopback 0
RA(config-if)#ip address 1.1.1.1 255.255.255.255
RA(config-if)#no shutdown
RA(config-if)#exit
RA(config)# router bgp 100
RA(config)# neighbor 192.168.10.2 remote-as 200
RA(config)# neighbor 192.168.40.2 remote-as 300
RA(config)# network 192.168.10.0 mask 255.255.255.252
RA(config)# network 192.168.40.0 mask 255.255.255.252
RA(config)# network 172.16.1.0 mask 255.255.255.0
RA(config)#exit
RA# wr mem
```

Configuration for the Host connected to RA

IP Address 172.16.1.2

Subnet mask 255.255.255.0

Default Gateway 172.16.1.1

Configuration of Router RB

```
Router>enable
Router#config terminal
Router(config)#hostname RB
RB(config)#interface serial 0/3/1
RB(config-if)#ip address 192.168.10.2 255.255.255.252

RB(config-if)#no shutdown
RB(config-if)#exit
RB(config)#interface serial 0/3/0
RB(config-if)#ip address 192.168.20.1 255.255.255.252
RB(config-if)#clock rate 128000
RB(config-if)#no shutdown
RB(config-if)#exit
RB(config)#interface fastethernet 0/0
RB(config-if)#ip address 172.16.2.1 255.255.255.0
RB(config-if)#no shutdown
RB(config-if)#exit
RB(config)#interface loopback 0
RB(config-if)#ip address 2.2.2.2 255.255.255.255
RB(config-if)#no shutdown
RB(config-if)#exit
RB(config)# router bgp 200
RB(config)# neighbor 192.168.10.1 remote-as 100
RB(config)# neighbor 192.168.20.2 remote-as 200
RB(config)# network 192.168.10.0 mask 255.255.255.252
RB(config)# network 192.168.20.0 mask 255.255.255.252
RB(config)# network 172.16.2.0 mask 255.255.255.0
RB(config)# exit
RB#wr mem
```

Configuration for the Host connected to RB

IP Address 172.16.2.2

Mask 255.255.255.0

Default Gateway 172.16.2.1

Configuration of Router RC

```
Router>enable
Router#config terminal
Router(config)#hostname RC
RC(config)#interface serial 0/3/1
RC(config-if)#ip address 192.168.20.2 255.255.255.252
RC(config-if)#no shutdown
RC(config-if)#exit
RC(config)#interface serial 0/3/0
RC(config-if)#ip address 192.168.30.1 255.255.255.252
RC(config-if)#clock rate 128000
RC(config-if)#no shutdown
RC(config-if)#exit
RC(config)#interface fastethernet 0/0
RC(config-if)#ip address 172.16.3.1 255.255.255.0
RC(config-if)#no shutdown
RC(config-if)#exit
RC(config)#interface loopback 0
RC(config-if)#ip address 3.3.3.3 255.255.255.255
RC(config-if)#no shutdown
RC(config-if)#exit
RC(config)# router bgp 200
RC(config)# neighbor 192.168.20.1 remote-as 200
RC(config)# neighbor 192.168.30.2 remote-as 300
RC(config)# network 192.168.20.0 mask 255.255.255.252
RC(config)# network 192.168.30.0 mask 255.255.255.252
RC(config)# network 172.16.3.0 mask 255.255.255.0
RC(config)#exit
RC#wr mem
```

Configuration for the Host connected to RC

IP Address 172.16.3.2

Mask 255.255.255.0

Default Gateway 172.16.3.1

Configuration of Router RD

```
Router>enable
Router#config terminal
Router(config)#hostname RD
RD(config)#interface serial 0/3/1
RD(config-if)#ip address 192.168.30.2 255.255.255.252
RD(config-if)#no shutdown
RD(config-if)#exit
RD(config)#interface serial 0/3/0
RD(config-if)#ip address 192.168.40.2 255.255.255.252
RD(config-if)#clock rate 128000
RD(config-if)#no shutdown
RD(config-if)#exit
RD(config)#interface fastethernet 0/1
RD(config-if)#ip address 172.16.4.1 255.255.255.0
RD(config-if)#no shutdown
RD(config-if)#exit
RD(config)#interface loopback 0
RD(config-if)#ip address 4.4.4.4 255.255.255.255
RD(config-if)#no shutdown
RD(config-if)#exit
RD(config)# router bgp 300
RD(config)# neighbor 192.168.30.1 remote-as 200
RD(config)# neighbor 192.168.40.1 remote-as 100

RD(config)# network 192.168.30.0 mask 255.255.255.252
RD(config)# network 192.168.40.0 mask 255.255.255.252
RD(config)# network 172.16.4.0 mask 255.255.255.0
RD(config)#exit
RD#wr mem
```

Configuration for the Host connected to RD

IP Address 172.16.4.2

Mask 255.255.255.0

Default Gateway 172.16.4.1

Verification at each Router

```
show ip route
show ip bgp
show ip bgp neighbors
show ip bgp summary
ping
traceroute
```

Verification at each Host

ping to all other hosts

tracert to remote hosts

5.1.5. LAB-5: Enhanced Interior Gateway Routing Protocol (EIGRP)

OBJECTIVE: Configure ROUTERs with IP address and configure EIGRP on the routers.

Goals:

1. Set the Host name and bring up the interface.
2. Ping the directly connected Networks
3. Configure eigrp
4. Verify that you can ping all routers.

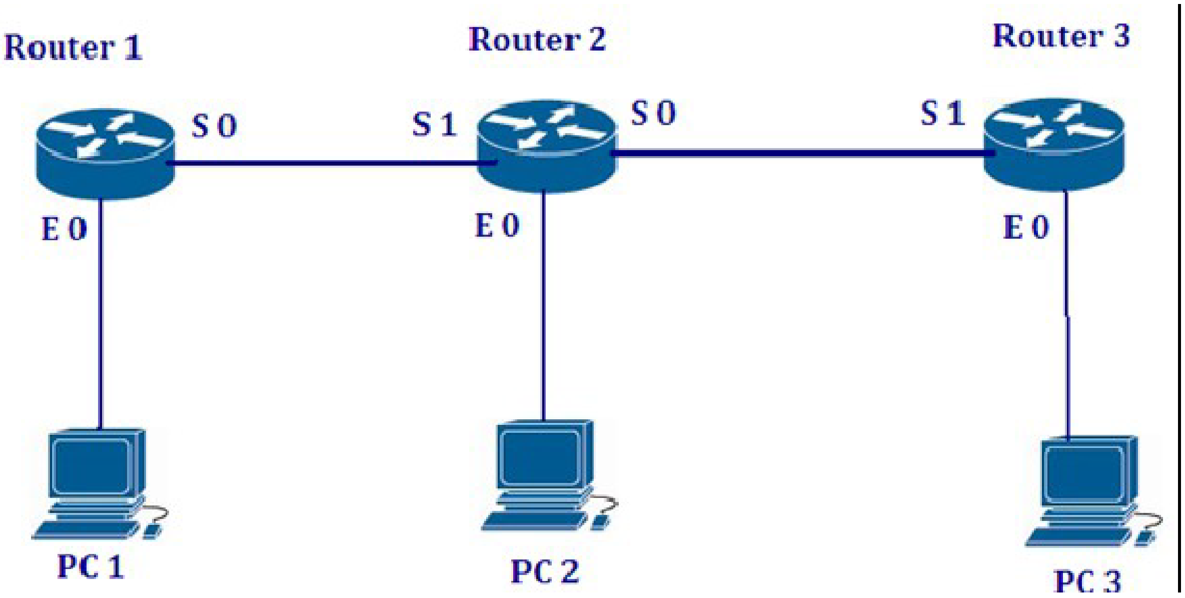


Figure 4.5

DEVICE	INTERFACE	IP ADDRESS	SUBNET MASK	
ROUTER 1	S0	192.168.20.1	255.255.255.0	
ROUTER 1	E0	192.168.10.1	255.255.255.0	
ROUTER 2	S0	192.168.40.1	255.255.255.0	
ROUTER 2	S1	192.168.20.2	255.255.255.0	
ROUTER 2	E0	192.168.30.1	255.255.255.0	

ROUTER 3	S0	192.168.40.2	255.255.255.0	
ROUTER 3	E0	192.168.50.1	255.255.255.0	
PC 1	GATEWAY=192.168.10.1	192.168.10.5	255.255.255.0	
PC 2	GATEWAY=192.168.30.1	192.168.30.9	255.255.255.0	
PC 3	GATEWAY=192.168.50.1	192.168.50.4	255.255.255.0	

Router1

```
Router>enable

Router#config terminal

Router(config)#hostname Router1

Router1(config)#interface serial 0

Router1(config-if)#clock rate 64000

Router1(config-if)#ip address 192.168.20.1 255.255.255.0

Router1(config-if)#no shutdown

Router1(config-if)#exit

Router1(config)#interface Ethernet 0

Router1(config-if)#ip address 192.168.10.1 255.255.255.0

Router1(config-if)#no shutdown

Router1(config-if)#exit

Router1(config)#exit

Router1#show ip interface brief

Router1#show ip route [display routing table]

Router1(config)#ip routing
```

NOTE:
Now eigrp configuration will start. Router1 will advertise its neighboring Networks 192.168.20.0 and 192.168.10.0 to other routers. "no auto-summary" this will not summarize or club all similar networks together in routing table. "100" is process id.

```
Router1(config)#router eigrp 100

Router1(config-router)#network 192.168.20.0

Router1(config-router)#network 192.168.10.0

Router1(config-router)#no auto-summary
```

```
Router1(config-router)#exit
Router1(config)#exit
Router1#show ip protocols
Router1#show ip route
```

TESTING:

From Router

```
Router1#ping 192.168.30.9
Router1#ping 192.168.40.2
Router1#ping 192.168.50.4

Router1#traceroute 192.168.50.4
```

From the PC

```
ping 192.168.50.4
tracert 192.168.50.4
```

Router 2

```
Router>enable
Router#config terminal
Router(config)#hostname Router2
Router2(config)#interface serial 0
Router2(config-if)#ip address 192.168.40.1 255.255.255.0
Router2(config-if)#clock rate 125000
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#interface serial 1
Router2(config-if)#ip address 192.168.20.2 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#interface Ethernet 0
```

```
Router2(config-if)#ip address 192.168.30.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#ip routing
```

NOTE:

Now eigrp configuration will start. Router2 will advertise its neighboring Networks 192.168.20.0, 192.168.40.0 and 192.168.30.0 to other routers. "no auto-summary" this will not summarize or club all similar networks together in routing table. "100" is process id.

```
Router2 (config)#router eigrp 100
Router2(config-router)#network 192.168.20.0
Router2(config-router)#network 192.168.40.0
Router2(config-router)#network 192.168.30.0

Router2(config-router)#no auto-summary
Router2(config-router)#exit
Router2(config)#exit
Router2#show ip route
```

TESTING:

From the Router

```
Router2#ping 192.168.10.5
Router2#ping 192.168.50.4
```

From the PC

```
ping 192.168.10.5
ping 192.168.50.4
```

Router 3

```
Router>enable
Router#config terminal
Router(config)#hostname Router3
Router3(config)#interface serial 1
Router3(config-if)#ip address 192.168.40.2 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#interface Ethernet 0
Router3(config-if)#ip address 192.168.50.1 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#ip routing
```

NOTE:

Now eigrp configuration will start. Router3 will advertise its neighboring Networks 192.168.40.0 and 192.168.50.0 to other routers. "no auto-summary" this will not summarize or club all similar networks together in routing table. "100" is process id.

```
Router3(config)#router eigrp 100
Router3(config-router)#network 192.168.40.0

Router3(config-router)#network 192.168.50.0
Router3(config-router)#no auto-summary
Router3(config-router)#exit
Router3(config)#exit
Router3#show ip route
```

TESTING:

From the Router

```
Router3#ping 192.168.10.5
```

From the PC ping 192.168.10.5

5.1.6. LAB-6: Switching and VLAN

OBJECTIVE

1. Create three VLAN

i. MPLS

ii. CDMA

iii. GSM

2. Configure Switch so that port 2 and 3 will be in vlan mpls port 4 will be in vlan CDMA port 5 will be in vlan GSM

3. Put port 10,11,12,13,14,15,16,17 of switch in vlan GSM using single command.

4. Put port 22 in vlan CDMA and check it.

5. Give management IP to the Switch.

6. Configure it for *telnet* and restrict that at a time only 3 persons will be able to telnet also enable secret password.

7. Set secret password.

8. Set console password.

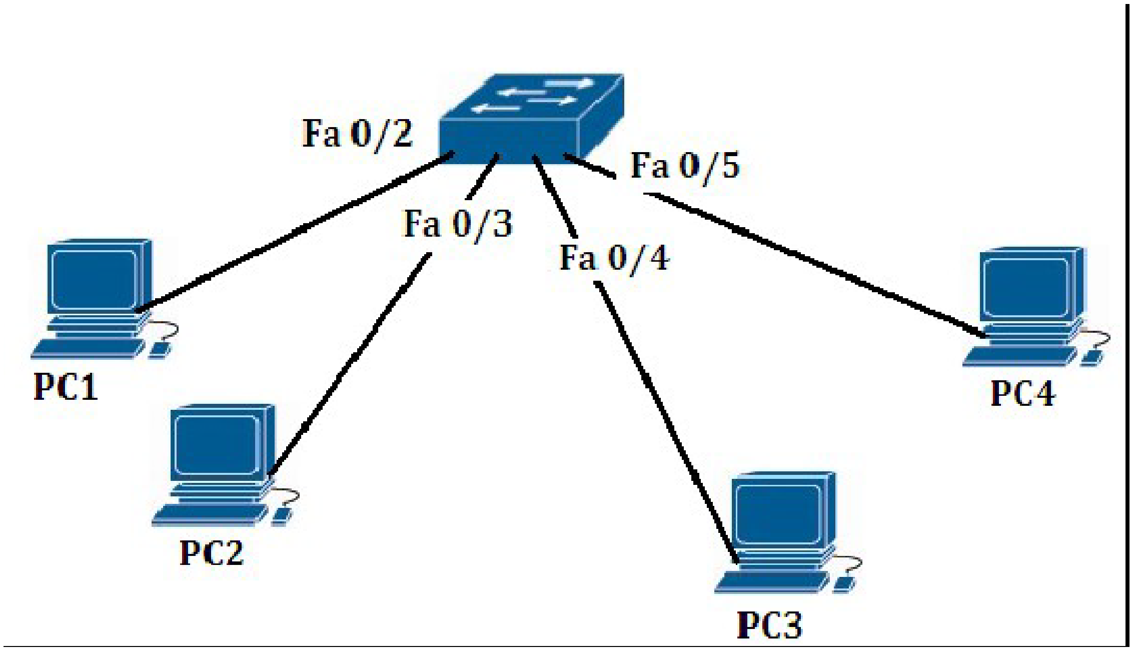


Figure 4.6

SWITCH CONFIGURATION

```
Switch con0 is now available
Press RETURN to get started.
Switch>
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

1.Vlan Creation

```
Switch(config)#vlan 5
Switch(config-vlan)#name MPLS
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 60
Switch(config-vlan)#name CDMA
Switch(config-vlan)#exit
Switch(config)#vlan 22
Switch(config-vlan)#name GSM
Switch(config-vlan)#exit
Switch(config)#
```

2. Port Configuration

```
Switch(config)#int fastEthernet 0/2
Switch(config-if)#switchport access vlan 5
Switch(config-if)#exit
Switch(config)#int fastEthernet 0/3
Switch(config-if)#switchport access vlan 5
Switch(config-if)#exit
Switch(config)#int fastEthernet 0/4
Switch(config-if)#switchport access vlan 60
Switch(config-if)#exit
Switch(config)#int fastEthernet 0/5
Switch(config-if)#switchport access vlan 22
Switch(config-if)#ctrl + Z
```

3. To put port 10,11,12,13,14,15,16,17 of switch in vlan GSM use

```
Switch(config)#int range fastEthernet 0/11 - 17
Switch(config-if-range)#switchport access vlan 22
```

4. To put port 22 in vlan CDMA and check it

```
Switch(config)#int fastEthernet 0/22
Switch(config-if)#
Switch(config-if)#switchport access vlan 60
Switch(config-if)#ctrl + Z
switch#
Switch#show vlan brief
```

5. Giving IP to Switch

```
Switch(config)#int vlan 1
Switch(config-if)#ip address 192.168.1.10 255.255.255.0
```

Now connect a pc to any port of the switch which are in vlan 1,you can use port Fa 0/24, and set the pc with: IP: 192.168.1.20, Mask: 255.255.255.0

6.For Telnet

```
Switch(config)#line vty 0 2
Switch(config-line)#
Switch(config-line)#password mtnl123
Switch(config-line)#login
```

7.Setting secret password

```
Switch(config)#enable secret cettm123
```

8. Setting Console password

```
Switch(config)#line console 0
Switch(config-line)#
Switch(config-line)#password mum123
Switch(config-line)#login
```

Now assign the following settings to PC:

PC1 with IP=192.168.1.101 mask=255.255.255.0 Gateway=192.168.1.1

PC2 with IP=192.168.1.102 mask=255.255.255.0 Gateway=192.168.1.1

PC3 with IP=192.168.1.103 mask=255.255.255.0 Gateway=192.168.1.1

PC4 with IP=192.168.1.104 mask=255.255.255.0 Gateway=192.168.1.1

Ping each others PC.

Now to put all the ports in one vlan 1:

```
Switch(config)#int range fastEthernet 0/1 - 24
Switch(config-if-range)#switchport access vlan 1
```

INTER-VLAN ROUTING

OBJECTIVE:

Here PC1 and PC2, PC3, PC4 are on different VLAN and our purpose is that any file shared by any PC must be access-able from other PC's.

For this a layer 3 device is needed so we will use one Router.

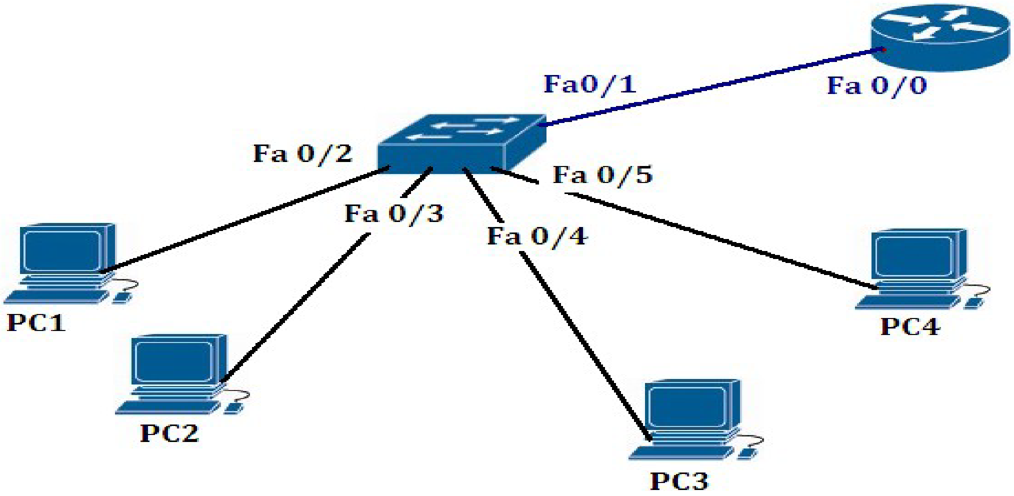


Figure 4.7

SWITCH CONFIGURATION

```
Switch con0 is now available
Press RETURN to get started.
Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#vlan 5
Switch(config-vlan)#name MPLS
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 60

Switch(config-vlan)#name CDMA
Switch(config-vlan)#exit
Switch(config)#vlan 22
Switch(config-vlan)#name GSM
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#int fastEthernet 0/2
Switch(config-if)#switchport access vlan 5
Switch(config-if)#exit
Switch(config)#int fastEthernet 0/3
Switch(config-if)#switchport access vlan 5
Switch(config-if)#exit
Switch(config)#int fastEthernet 0/4
Switch(config-if)#switchport access vlan 60
Switch(config-if)#exit
Switch(config)#int fastEthernet 0/5
Switch(config-if)#switchport access vlan 22
Switch(config-if)#^Z
```

```
Switch#
Switch#
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#int fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
Switch(config-if)#ctrl + Z
```

ROUTER CONFIGURATION

```
Router con0 is now available
Press RETURN to get started
Router>en
Router#
Router#config t

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fastEthernet 0/0
Router(config-if)#no ip address
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#int fastEthernet 0/0.1
Router(config-subif)#encapsulation dot1Q 5
Router(config-subif)#
Router(config-subif)#ip address 172.16.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
Router(config)#int fastEthernet 0/0.2
Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip address 172.16.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int fastEthernet 0/0.3
Router(config-subif)#encapsulation dot1Q 22
Router(config-subif)#ip address 172.16.30.1 255.255.255.0
Router(config-subif)#^Z
Router#
```

Points to be Noted:

1.Layer 3 device is needed for Inter-vlan routing.

2.Number of sub-interfaces created on Router is equal to number of Vlans created on Switch.

3.After “dot1q” Vlan-ID is important. i.e. for which Vlan ,which IP will be used. This IP is the gateway for all the PC connected to that vlan.

4.The encapsulation is must in inter-vlan configuration

5.1.7. Setting up a VoIP Connection

ARCHITECTURE

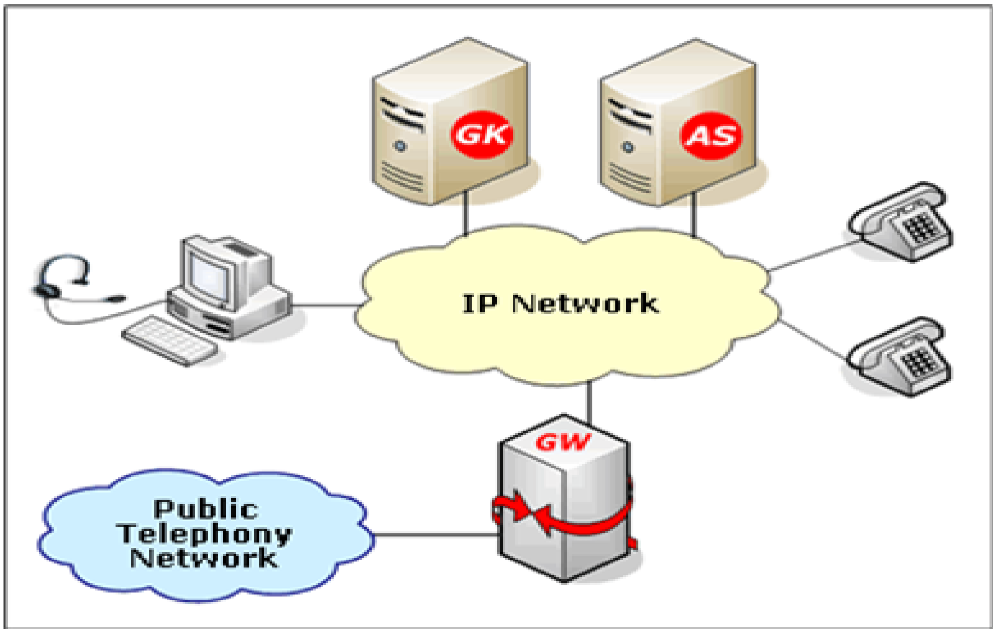


Figure 4.8 Architecture of VoIP

SIP client-server application supports user mobility with 2 modes

1. Proxy mode, SIP clients sends its signaling requests to the proxy server. The proxy server either handles the request or forwards it to other SIP servers.

2. Redirect mode, SIP clients send its signaling requests to the redirect server. The SIP redirect server then looks up the destination (IP) address and then returns it to the originator of the call. SIP has become the protocol of choice SIP is the basis for the new IP Multimedia Subsystem (IMS) protocol; a joint development between the IETE and the Third Generation Partnership Project (3GPP). Analog Voice signal must be converted to Digital

- Compress and translate into IP packet
- Transmit on Internet
- Receiving end must reverse the process

COMPONENTS

1.VoIP softphones (laptop-to-PBX),

VoIP consoles (PC apps),terminal devices end users can use to initiate and receive VoIP calls.

2. A call processing server/PBX

which manages all VoIP control connections

3. Media/PSTN-to-VoIP Gateways

handle analog-to-digital conversion of voice traffic for transport over the IP network

4.The IP network

Transports the audio (voice) payload, Internet

5. One or more Session Border Controllers (SBCs)

Control real-time, session-based traffic at the signaling (call control) and transport layers as it crosses network borders and network domains.

OPERATION

VoIP phone service (Voice over IP; also known as digital phone service, digital telephony, or broadband phone replaces your phone line with a high-speed Internet connection. It's that simple.

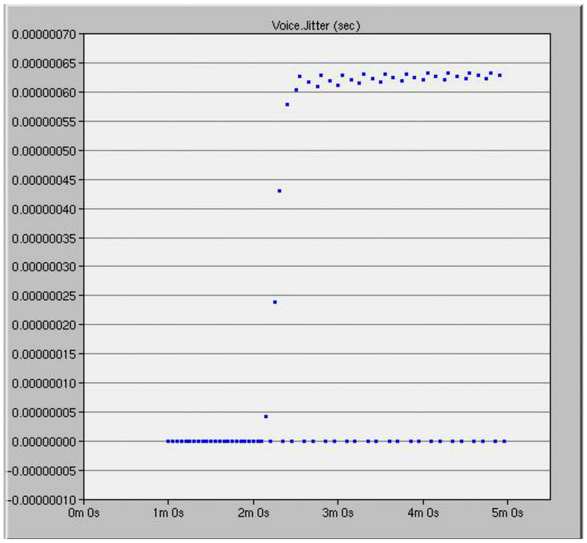
While traditional telephone service compresses your voice into a frequency on a wire, VoIP compresses the sound of your voice into packets of data. In milliseconds, these data packets are sent over the Internet. When the data reaches the final destination, it is converted back to sound. If use VoIP to call someone on the traditional phone network (the "PSTN" or Public Switched Telephone Network), the VoIP call is converted to sound once it reaches the network and the call is routed normally.

SECTION – VI

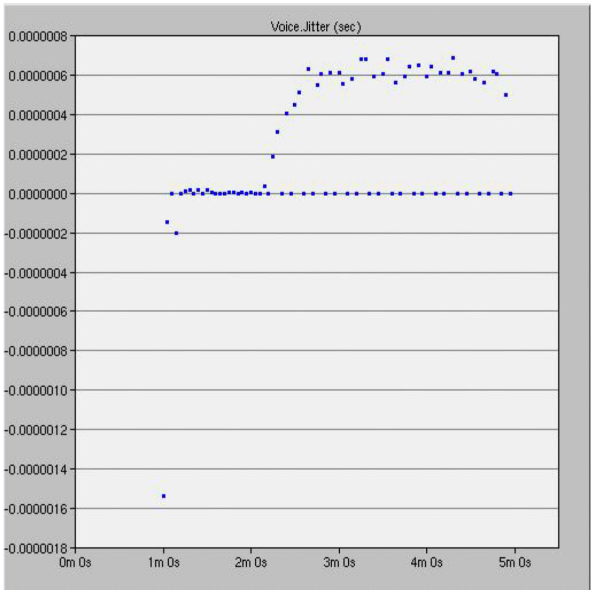
6.1. SIMULATION RESULTS AND COMPARISON

6.1.1. Scenario 1: VoIP Call in LAN

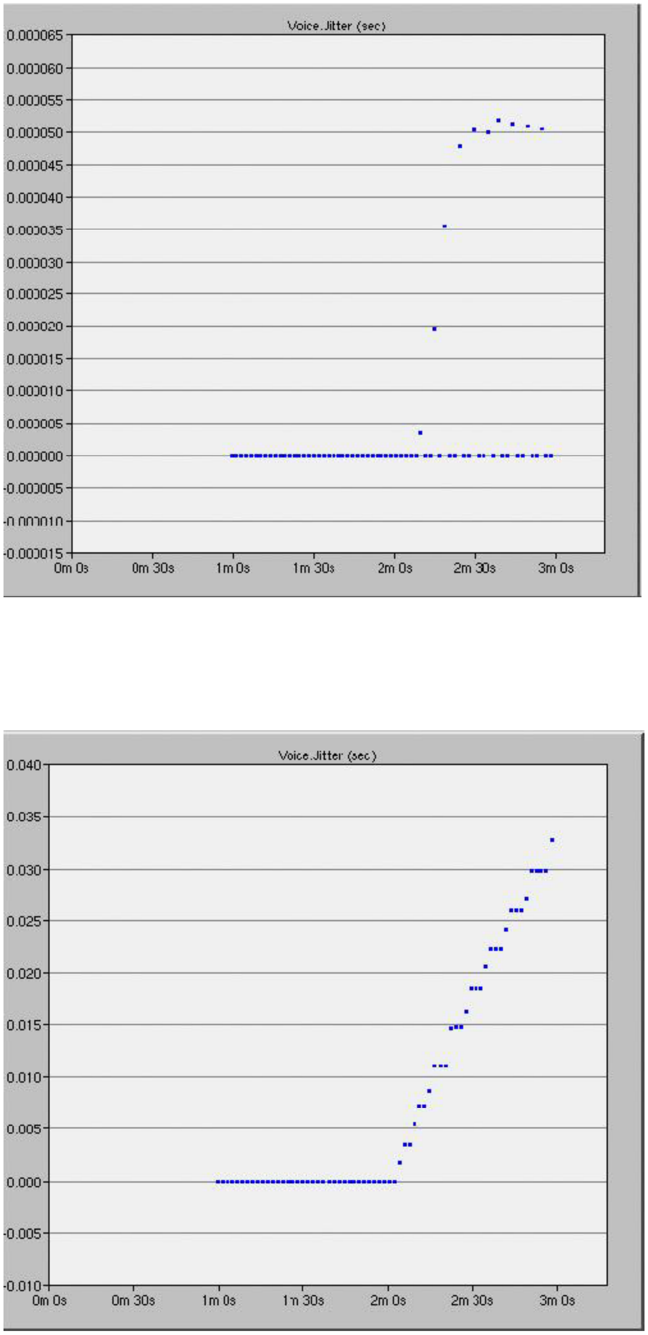
The first scenario tests the performance of VoIP call in LAN of a small office. The number of client is initially set to 2 nodes and gradually increases to 100 nodes.



a. 2 nodes



b. 20 nodes

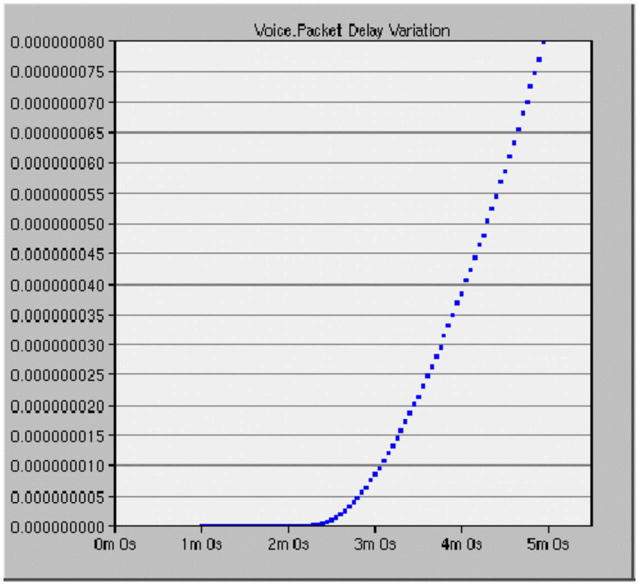


c. 50 nodes

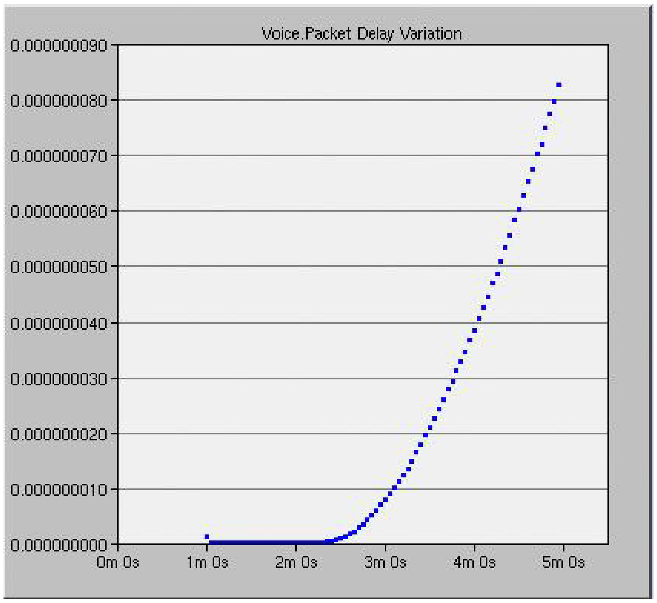
d. 100 nodes

Figure 6.1 Jitter in the voice application

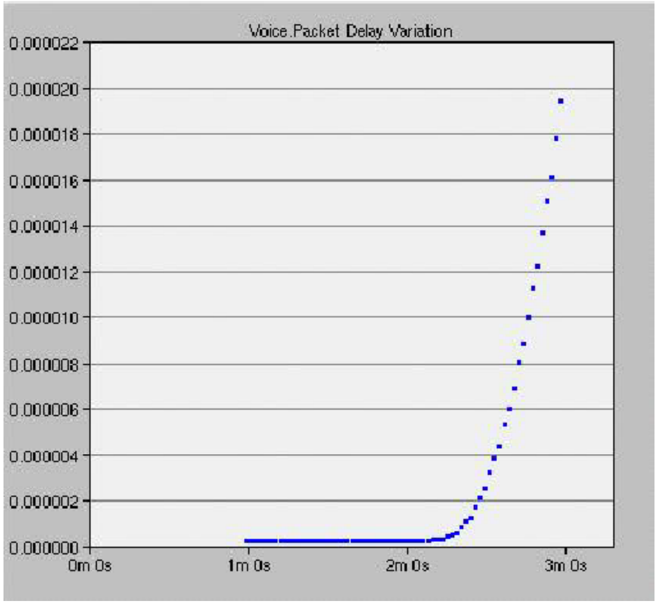
As shown in figure 3.1, the voice jitter increases as the number of nodes increase. When the number of node is between 2 to 20 nodes, the jitter is very small and unnoticeable. When the number of nodes in the LAN increased to 50, the voice jitter is 100 times larger than a LAN with 20 nodes. When the number of nodes in the LAN increased to 100, the voice jitter is 1000 times larger than a LAN with 50 nodes. Also the voice jitter in a LAN with 100 nodes seems to increase at a constant rate at the end of the simulation.



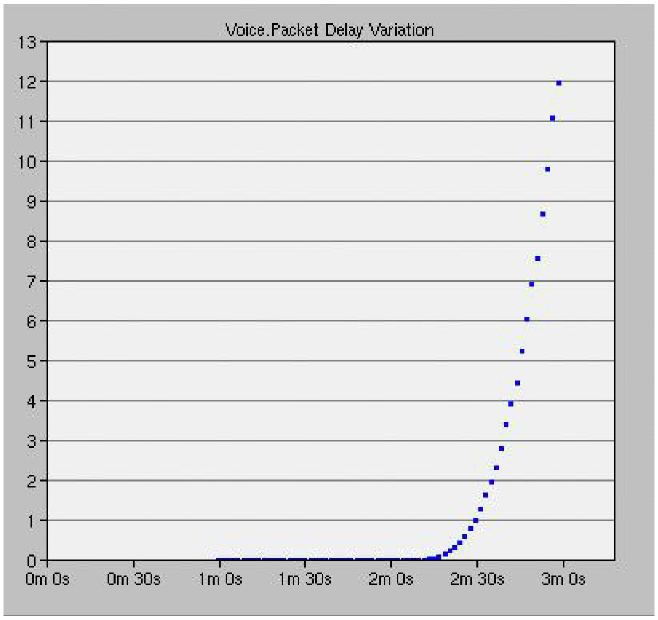
a. 2 nodes



b. 20 nodes



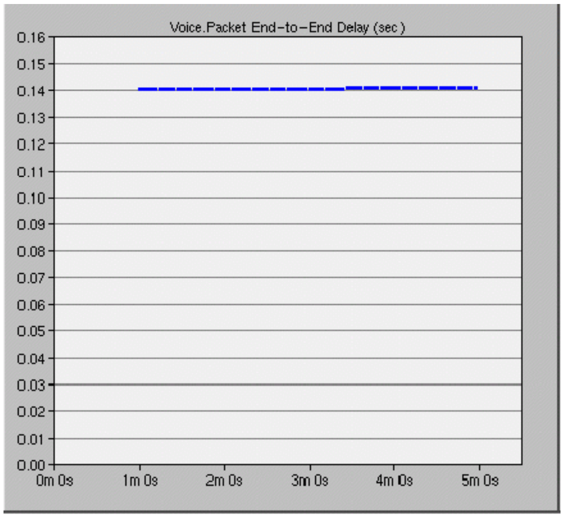
c. 50 nodes



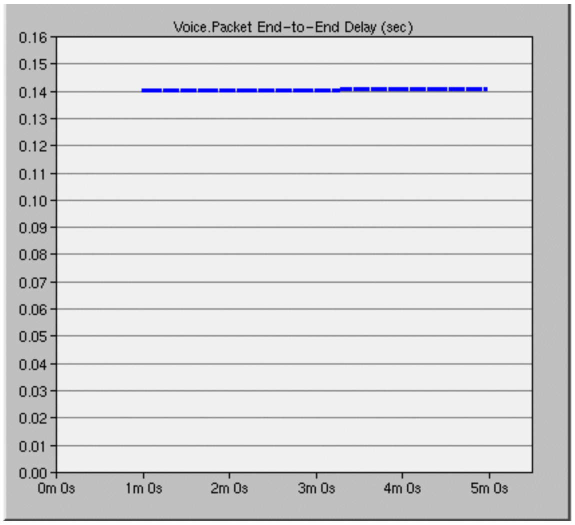
d. 100 nodes

Figure 6.2 Packet Delay Variation

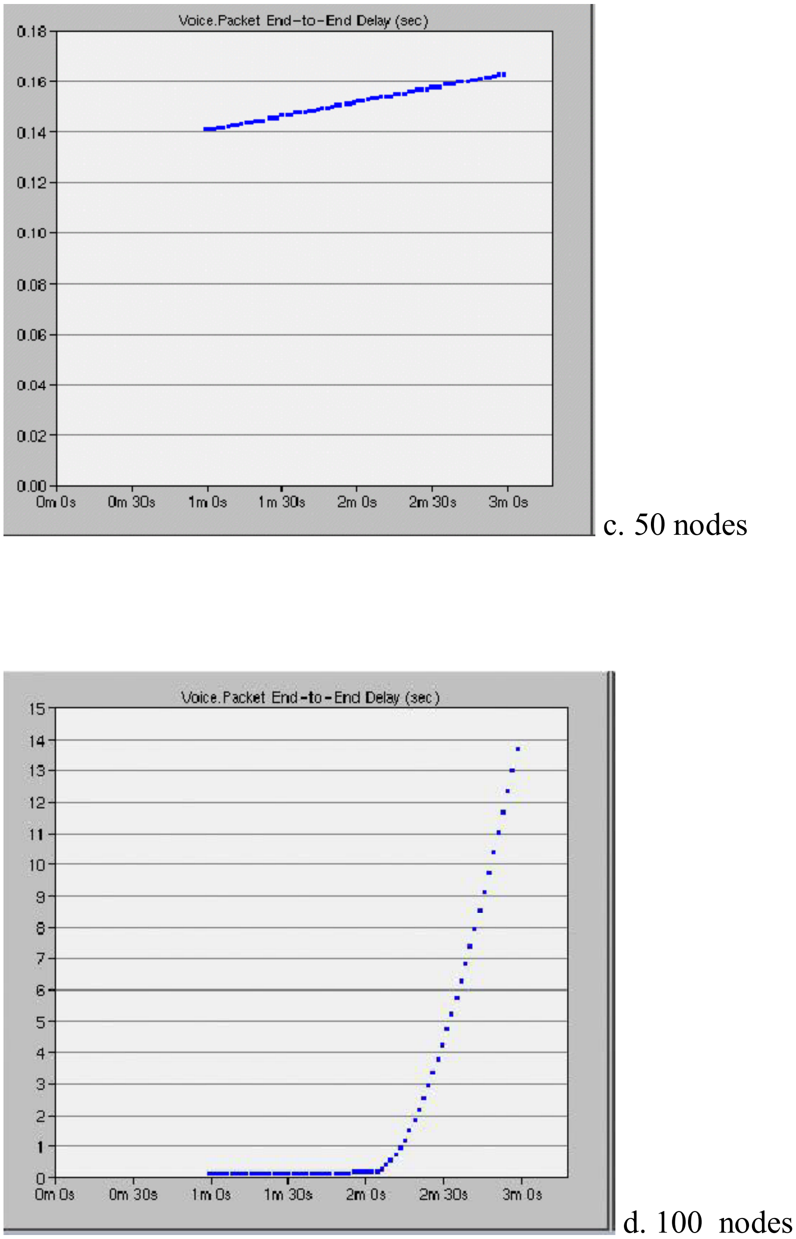
Figure 3.2 show the packet delay variation in a LAN with different number of client nodes. The packet delay variation results are very similar to voice jitter results. When the number of nodes is small, we have a very small and unnoticeable delay variation. The magnitude increases as the number of nodes increase. In the simulation with number of nodes is 100, the delay variation exceed 1 second and reach a maximum of 12 seconds. The delay variation seems to increase exponentially with the number of calls.



a. 2 nodes



b. 20 nodes



c. 50 nodes

d. 100 nodes

Figure 6.3 Packet End to End Delays

Figure 3.3 shows the corresponding packet end to end delay. When the number of nodes is small, between 2 nodes to 20 nodes, we have the identical ETE delay around 140ms. ETE delay increases as the number of client nodes and calls are added into the network. When the nodes increased to 50, ETE delay increased to around 160ms. In the simulation with 100 nodes, approximately 60 seconds after VoIP calls started, ETE delay rapidly increased over 200ms and reach 12 seconds.

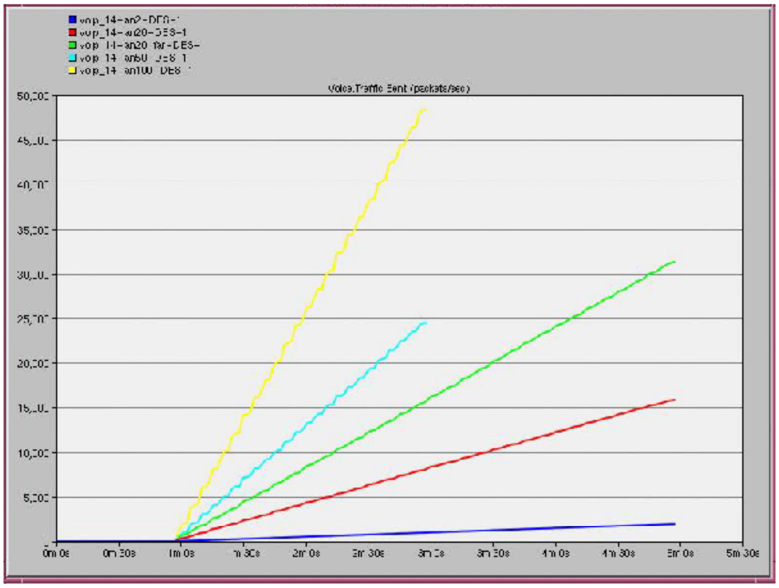


Figure 6.4 Traffic Sent

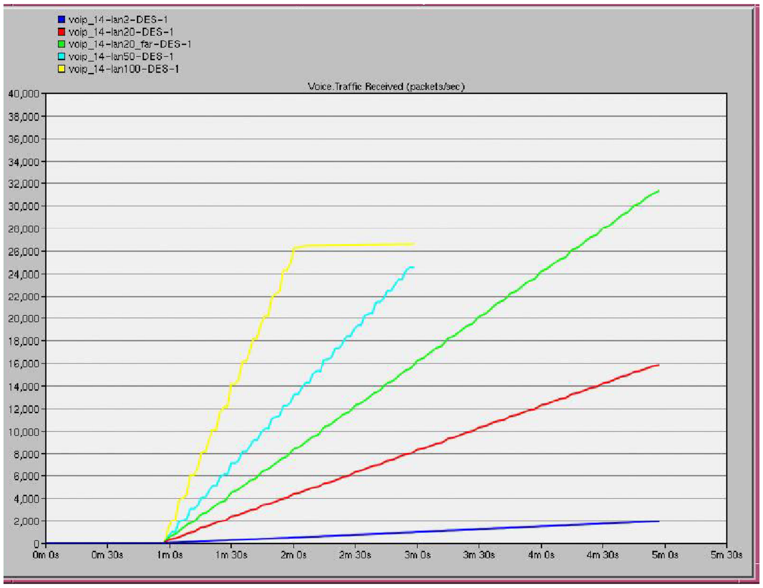


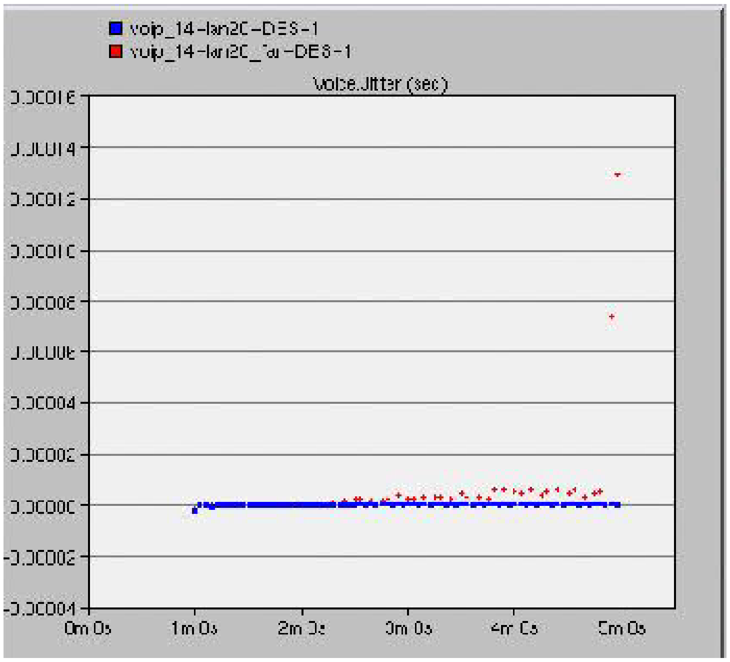
Figure 6.5 Traffic Received

Figure 3.4 and 3.5 show the traffic sent and received with the voice application. For the simulation with less than 50 nodes, the traffic received is consistent with the traffic sent. For the 100 nodes simulation, packets are lost when the numbers of call get too high.

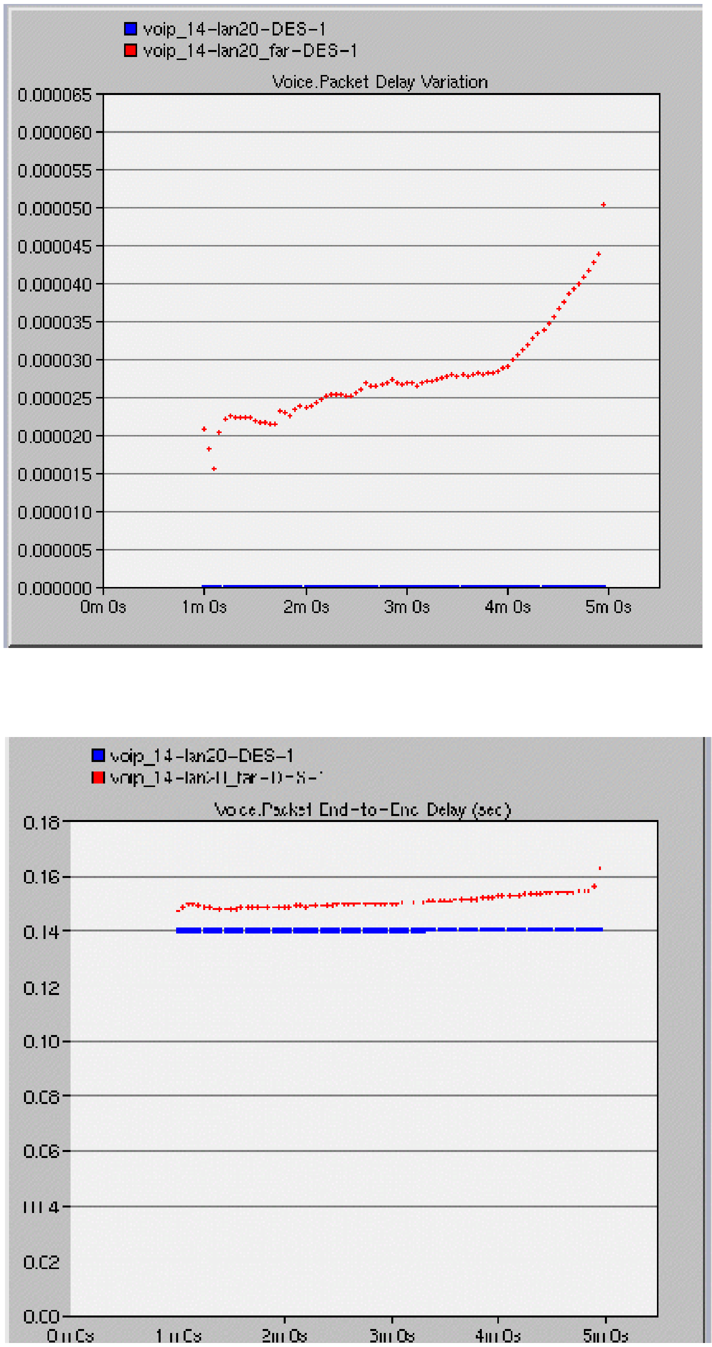
As seem from the results, VoIP calls have stable connection when the number of client is small. However, as the number of VoIP clients and calls increase, the voice jitter, delay variation, and ETE delay become significant factors to the calls quality.

6.1.2. Scenario 2: Long Distance VoIP Calls under LAN

In this scenario, calls are made between two offices with LAN placed across the country. Effect on distance to calls quality will be evaluated.



a. voice jitter



b. Packet Delay Variation

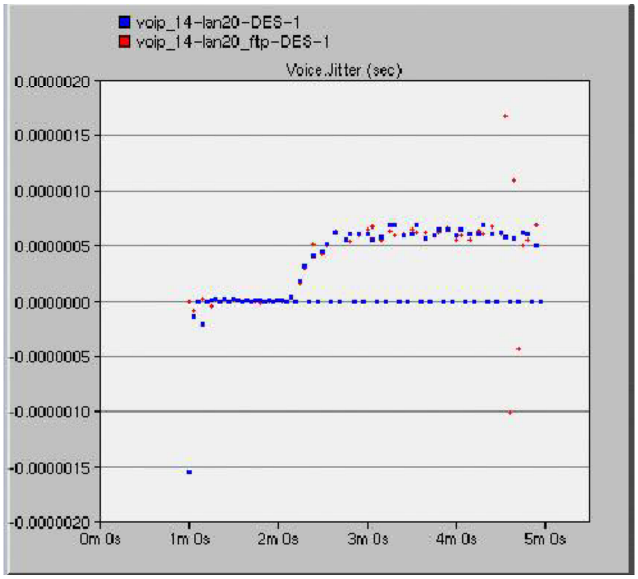
c. Packet End to End Delay

Figure 6.6 Long Distance Call under LAN

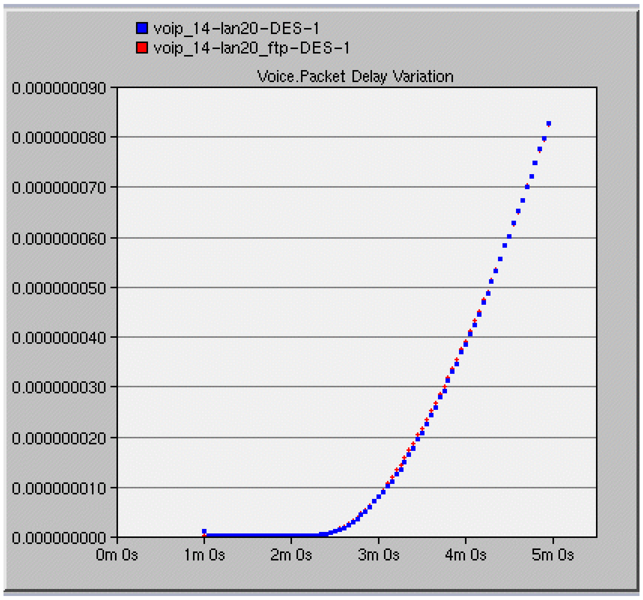
Jitter, delay variation and ETE delay increased as a result of the increased distance. However the value is still very small when compared to the simulation with large number of nodes. The ETE delay is relatively stable around 150ms throughout the simulation. Calls quality is within the acceptable range.

6.1.3. Scenario 3: VoIP calls in LAN with ftp server

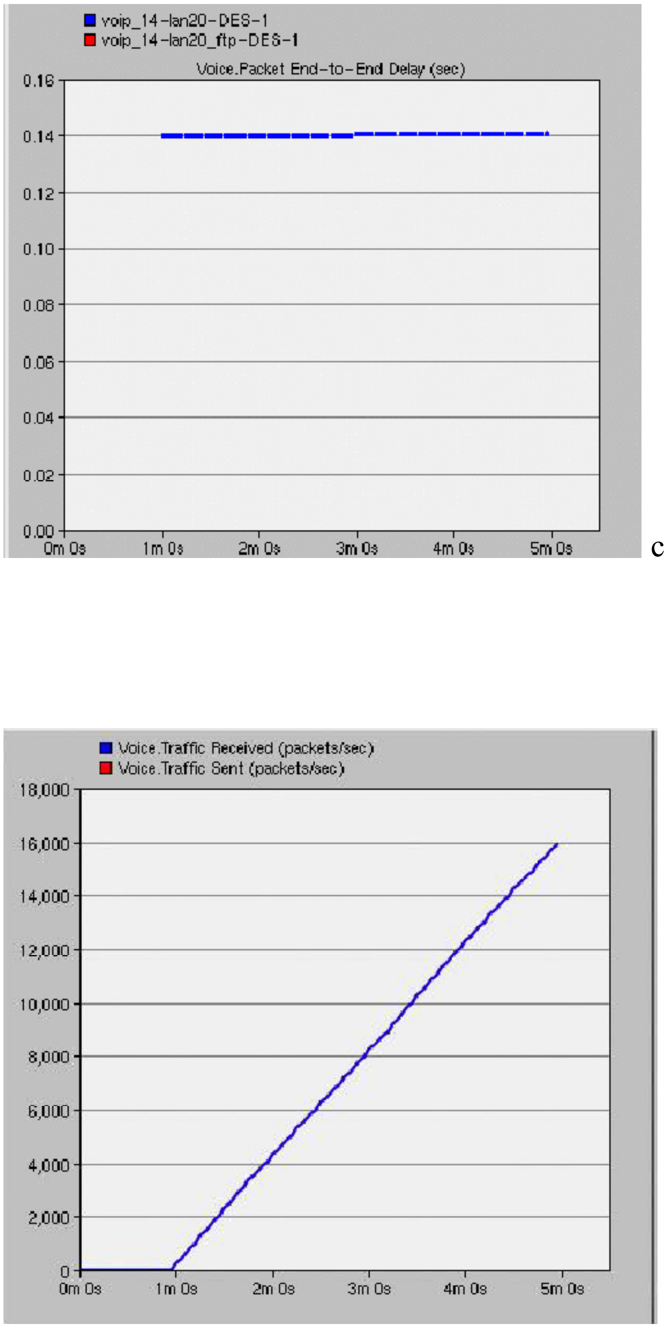
By adding an ftp server and ftp traffic into the network, we would like to produce a more realistic simulation result.



a. Voice Jitter



b. Packet Delay Variation



c. Packet End to End Delay

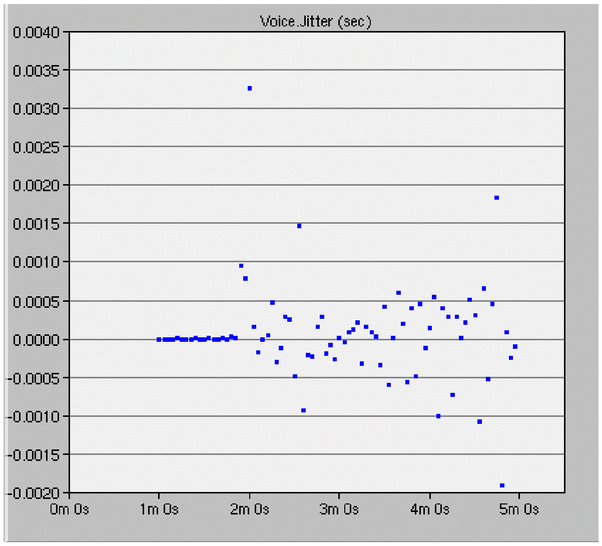
d. Traffic sent and received

Figure 6.7 VoIP calls in LAN with ftp server

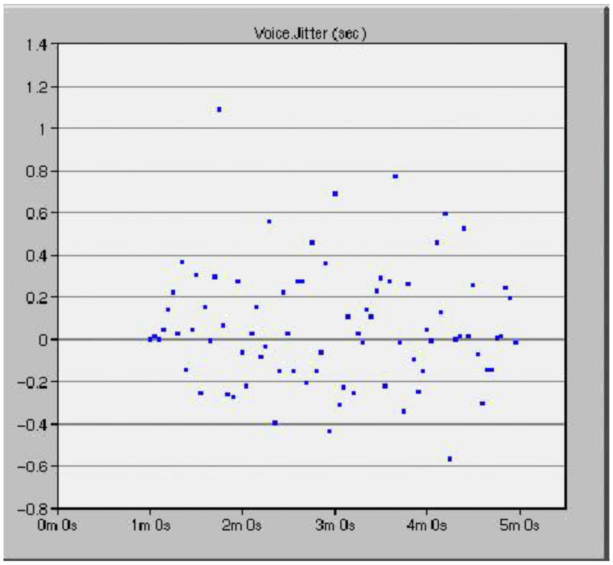
In this case, adding ftp traffic in the network does not affect the voice jitter, delay variation or end to end delay. Traffic sent is identical to traffic received. Since this FTP simulation is done on a LAN with only 20 nodes. There is not much VoIP connection and calls. We assume that there is enough bandwidth to meet the demands of both the VoIP connection and FTP traffic. Therefore, the FTP packets are not dropped at all.

6.1.4. Scenario 4: VoIP Calls in WLAN

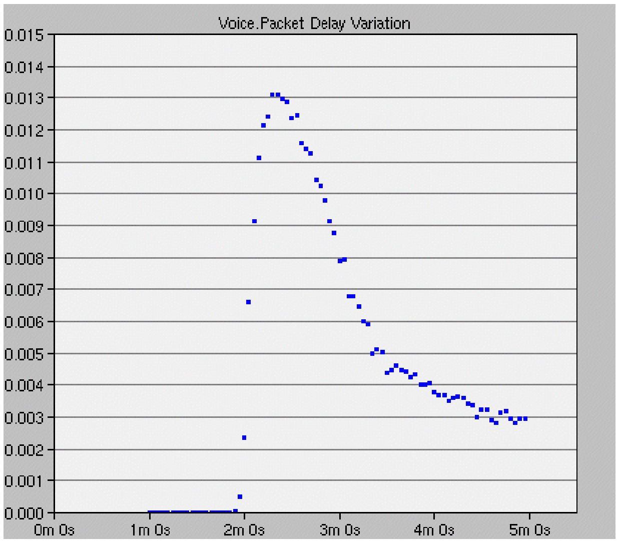
In this scenario, we will simulate a small office using WLAN for their VoIP application and compare the results with LAN.



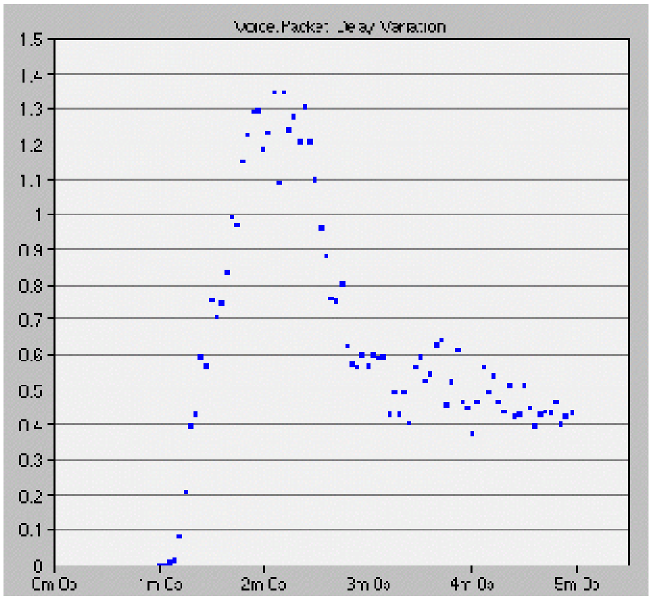
a.2 nodes Jitter



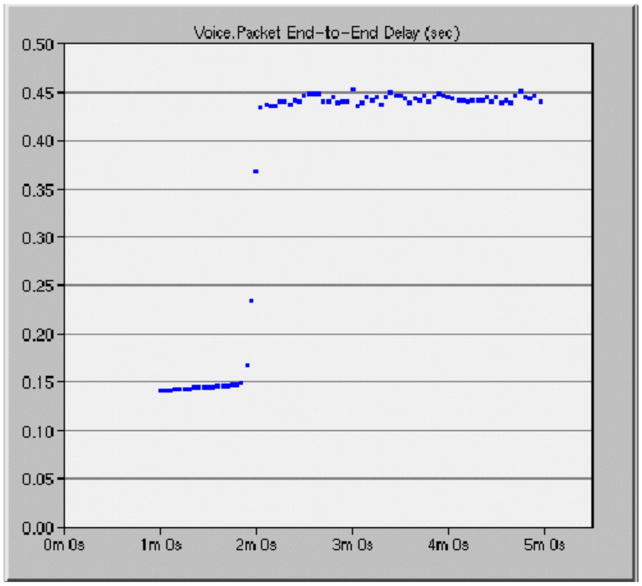
b. 20 nodes Jitter



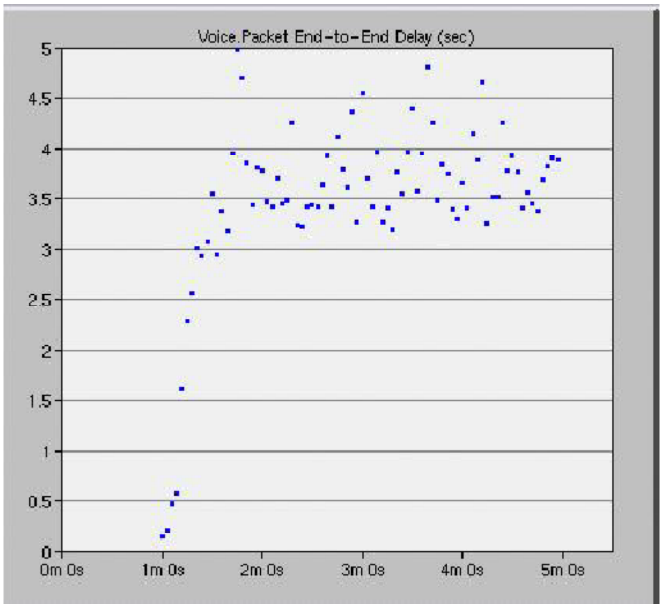
c. 2 nodes Packet Delay Variation



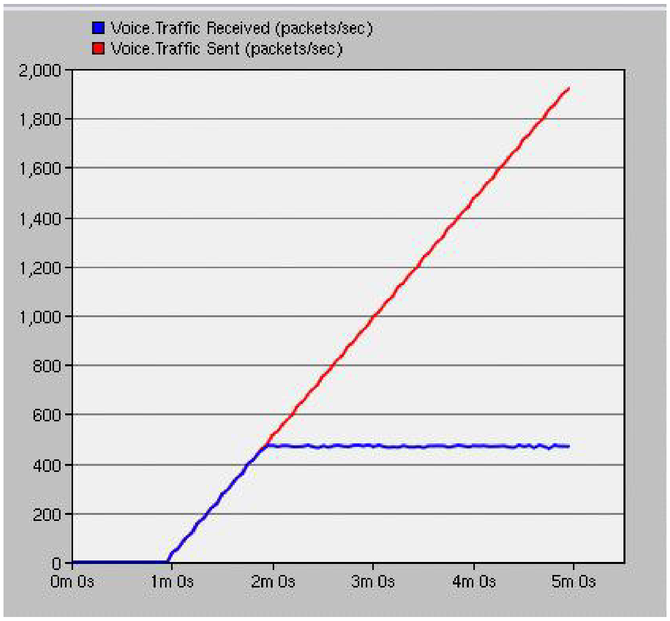
c. 2 nodes Packet Delay Variation



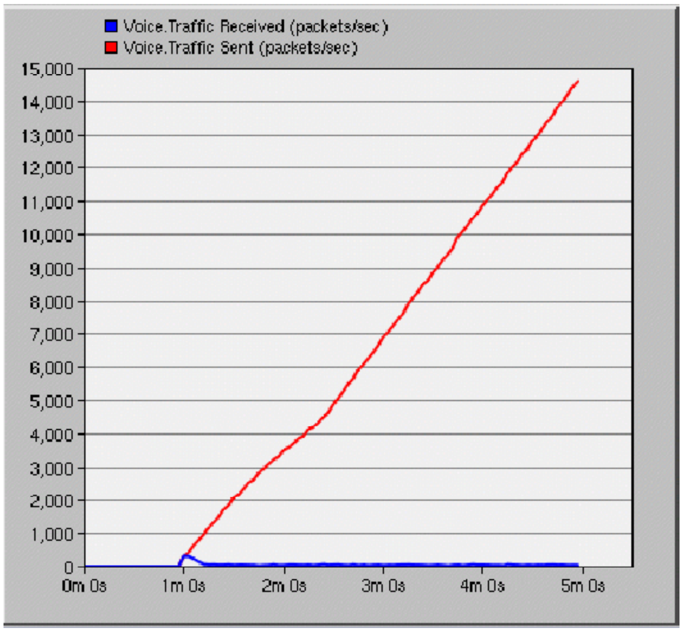
e. 2 nodes Packet ETE delay



e. 2 nodes Packet ETE delay



g. 2 node Traffic sent and received



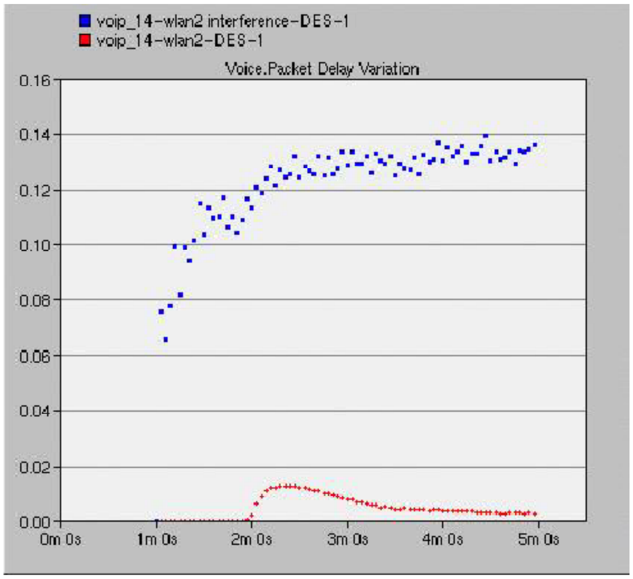
h.20 nodes Traffic sent and received

Figure 6.8 VoIP Calls in WLAN

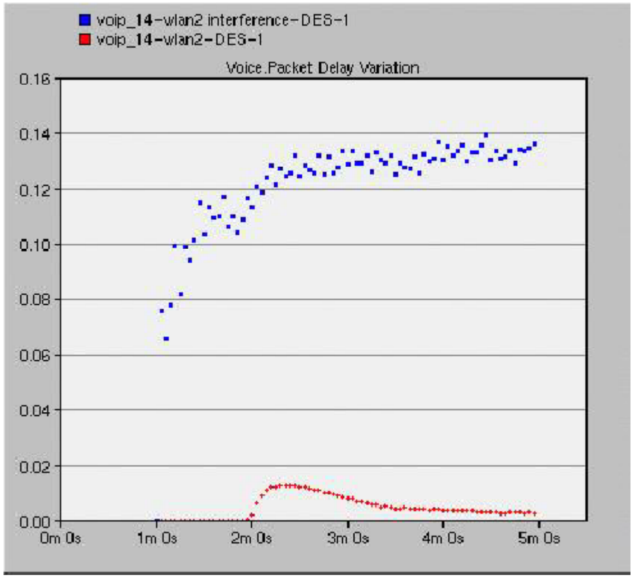
The performance of VoIP in WLAN is quite poor compare to the wired network. The values of jitter, delay variation, and end to end delay in wireless network is multiple times larger the values of wired network. Even with only 2 nodes in the network, the ETE delay starting with 150ms will rapidly increase to approximately 450ms when the network is congested. In addition, when comparing the traffic sent and received in the simulation, we notice that, due to limited bandwidth, most of the packets sent were lost. Since we are simulating using G.711 compression codes which consume the most bandwidth, another compression code with less bandwidth consumption could be used to improve the performance of VoIP.

6.1.5. Scenario 5: VoIP in WLAN with interference

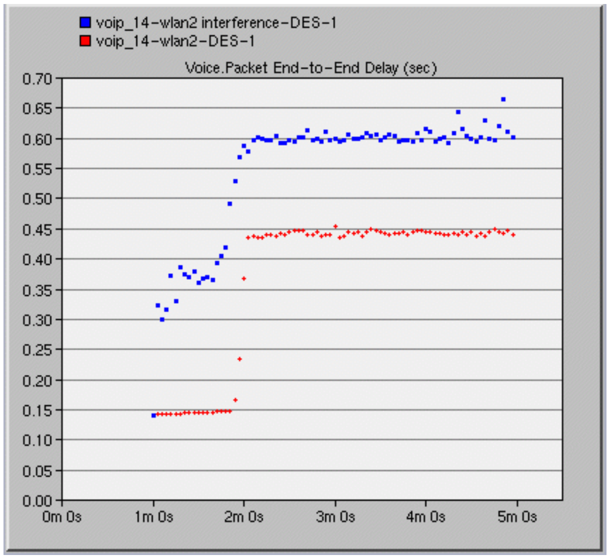
Interference exists in a network and is an inevitable factor in determining the quality of a VoIP calls. We represent the interference by adding a jammer into the network and examine the influence of interference in a network.



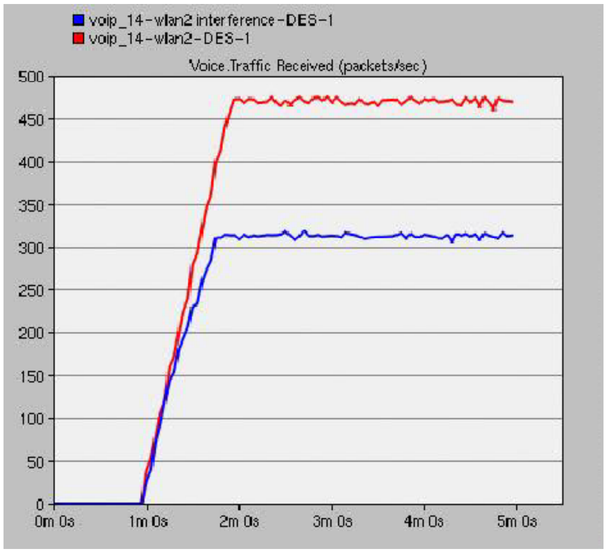
a. Voice Jitter



b. Packet Delay Variation



c. End to End Delay



c. End to End Delay

Figure 6.9 WLAN with interference

The results are consistent with our expectation. In the wireless network with interference, we have a larger jitter, delay variation and packet end to end delay. End to end delay at of the start of simulation is around 350ms which has already exceed the acceptable range. Packet received is approximately 2/3 of the ideal network which means more packets are dropped due to the interference.

SECTION – VII

7.1. CONCLUSION

In this project, we covered five scenarios: VoIP Call in LAN, Long Distance VoIP Calls under LAN**,** VoIP calls in LAN with ftp server, VoIP Calls in WLAN, and VoIP in WLAN with interference. Through the results we got found out that Ethernet has a more stable and less delay connection than wireless connection. Interference near wireless router greatly reduces QoS. Moreover, long distance VoIP introduces greater jitter, ETE and lower MOS. As a result, although VOIP has some negative sides, we consider that VOIP is a great alternative way to replace the traditional circuit switch phone network in the future.

7.2. REFERENCES

[1] Webopedia, “The Difference Between VoIP and PSTN Systems”, Available: http://www.webopedia.com/DidYouKnow/Internet/2008/VoIP_POTS_Difference_Between.asp

[2] Voipunlimited calls, “The Growth of VoIP Usage”, Available: http://www.voipunlimitedcalls.com/the-growth-of-voip-usage/

[3] Voip-Info.org, “VOIP QoS Requirements”, Available: http://www.voip-info.org/wiki/view/QoS

[4] T.Szigeti and C. Hattingh, “Quality of Service Design Overview”, Available: http://www.informit.com/articles/article.aspx?p=357102

[5]Cisco, “Enabling VoIP: Data Considerations and Evolution of Transmission Network Design”, Available: http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/prod_white_paper0900aecd803faf8f_ps2001_Products_White_Paper.html

[6] Cisco, “THE QoS BASELINE”, Available: http://www.cisco.com/en/US/technologies/tk543/tk759/technologies_white_paper0900aecd80295a9b.pdf

[7] W.H. Chiang, W. Xiao, and C. Chou, “A Performance Study of VoIP Applications: MSN vs. Skype”, Available: http://multicomm.polito.it/proc_multicomm06_3.pdf

[8] M. Raj, A. Narayan, S. Datta, S.K. Das, J.K. Pathak, “Fixed mobile convergence: challenges and solutions,” Communications Magazine, IEEE , vol.48, no.12, pp.26-34, December 2010

[9] G. Krzysztof, K. Aleksander, W. Jozef, N. Krzysztof, “Testbed analysis of video and VoIP transmission performance in IEEE 802.11 b/g/n networks,” Telecommunication Systems, Springer Netherlands, vol. 48, no 3-4, pp. 247-260, December 2011

[10] K.Salah, P. Calyam, M.I. Buhari, “Assessing Readiness of IP Networks to Support Desktop Videoconferencing using OPNET,” Elsevier Journal of Network and Computer Applications (JNCA), 2006

[11] R. Gill, T. Farah, and Lj. Trajkovic, “Comparison of WiMAX and ADSL performance when streaming audio and video content,” OPNETWORK 2011, Washington, DC, Aug. 2011

[12] E. Yiu, E. Yiu, and Lj. Trajkovic, “OPNET Implementation of the Megaco/H.248 protocol: multi-call and multi-connection scenarios,” OPNETWORK 2004, Washington, DC, Aug. 2004

[13] K. Salah, A. Alkhoraidly, “An OPNET-based Simulation Approach for Deploying VoIP”, Available: http://faculty.kfupm.edu.sa/ics/salah/misc/RecentPubs/IJNM_VoIP.pdf

[14] A.Kamerman, and N. Erkoçevic, “Microwave Oven Interference on Wireless LANs Operating in the 2.4 GHz ISM Band,” Lucent Technologies, Available: http://archive.devx.com/wireless/articles/bluetooth/whitepapers/1a6900.pdf

[15] Luke Dang, Jeffrey Tam, and Kuo-Sheng Tsai, “Voice over Internet Protocol (VoIP) over Wireless and Ethernet,” April 2010, Available: http://www.ensc.sfu.ca/~ljilja/ENSC427/Spring10/Projects/team1/ENSC_427_Srping_2010_Group_1_Final_Report.pdf

[16] Hin Heng Chan, “Voice over Internet Protocol (VoIP) over 3G networks,” April 2011, Available: http://www.ensc.sfu.ca/~ljilja/ENSC427/Spring11/Projects/team4/ENSC427_Spring2011_Team4_Report.pdf

7.3. REFERENCE BOOKS

- CCNA ELECTRONIC BOOK 6TH EDITION
- DATA AND COMPUTER COMMUNICATION 8TH EDITION WILLIAM STALLINGS.
- DATA COMMUNICATION AND NETWORKING, BEHROUZ A. FOROUZAN