NEAR EAST UNIVERSITY

FACULTY OF ENGINEERING

Department of Electrical and Electronic Engineering

THE PERFORMANCE OF VOICE OVER INTERNET PROTOCOL

Graduation Project
EE-400

Student: Ahmad Alkafaween (20032943)

Supervisor: Prof. Dr.Sc. Fakhreddin Mamedov

Nicosia - 2005

ACKNOWLEDGEMENTS

Firstly I would like to present my special appreciation to my supervisor Prof. Dr. Fakhreddin Mamedov, without whom it is not possible for me to complete the project. His trust in my work and me and his priceless awareness for the project has made me do my work with full interest. His friendly behavior with me and his words of encouragement kept me doing my project.

I feel proud to pay my special regards to Mr. Cemal Kavalcioglu, He never disappointed me in any affair. He delivered me too much information and did his best of efforts to make me able to complete my project

Secondly I offer special thanks to my parents, who encouraged me in every field of life and try to help whenever I needed. They enhanced my confidence in myself to make me able to face every difficulty easily. I am also grateful to my mother whose prayers and my father whose words for me had made this day comes true. And because of them I am able to complete my work

I would also like to pay my special thanks to my all friends who helped me and encouraged me for doing my work. Their reluctance and friendly environment for me has helped me. I want to thank them as they contributed their time and provided very helpful suggestions to me.

ABSTRACT

Ever tried placing a voice call over the Internet. If you have, we are sure you haven't had a pleasant experience. You might have even promised yourself never to try it again.

Stop right there!!

Take some time-off from your busy schedules and have a look at what we have to say. We guarantee that you will change your mind.

In the near future, if you make a telephone call, it is more than likely that it would be over the Internet or some other packet network. But, what is it that would make this possible? It is a bunch of protocols and standards; and years of research done by organizations all over the world that would bring about this revolution.

They call it 'VOICE OVER IP', 'INTERNET TELEPHONY' & a host of other names.

We like to refer to it as 'A Dawn Of a New Era in Telecommunications'.

The next few chapters of this project report will discuss this phenomenon in detail.

TABLE OF CONTENTS

List of Figures

INTRODUCTION

The incredible growth of two leading technologies, wireless LAN and voice over IP (VOIP), has come together to provide an exiting new application, Voice over Wireless LANs (VOWLANs). The most prevalent usage of VOWLAN today is in the retail, warehousing, manufacturing, and healthcare, education, and hospitality industries. Employees in these industries are more mobile than the average office worker and have specific application needs that lend well to handheld devices. Adding VOWLAN can increase productivity and responsiveness for mobile employees in the workplace.

The project consists of three chapters, Introduction To Voice Over IP Over WLAN, Background, and Applications.

In the first chapter I will introduce voice over IP and it background.

In the second chapter I will discuss in details about the background and function of different protocols.

In third chapter I will give an overview of Voice Over IP Applications and Softwares and I will discuss in details about advantages and disadvantages of voice over IP

CHAPTER ONE

INTRODUCTION TO VOICE OVER IP

1.1 Overview

Voice-over-Internet Protocol (Voice-over-IP, or VoIP) is being adopted by more and more businesses around the world and is not only emerging, but flourishing. Moreover, VoIP is not a new technology; it is an old technique that has been around for about a decade. Simply, VoIP uses Internet Protocol to digitize voice calls into packets using the existing company network connection. Calls placed by using Internet Protocol bypass traditional phone networks that have toll-based charges, so calls are generally less expensive.

Although many people are unfamiliar with VoIP, the technology has been around for years. In the late 1970's, there were experiments with ARPANET (the predecessor to the Internet) using IP to send packetized voice messages. In the mid 1990's, IP telephony started being used to open a voice connection between two PCs over the Internet. Initially, the quality of calls was of concern, so most people who used IP telephony were hobbyists and experimenters. However, today with the extended extensive research and development, the quality of VoIP has surpassed cellular service and is equal to that of the traditional phone line. "VoIP will account for

In addition to the long history of IP telephony, many consumers and businesses have most likely used VoIP without even knowing it. For voice services by 2007, most traditional phone companies have been using it within their regional networks. Consequently, consumers who use any cheap, long distance phone service today are probably already using IP telephony technology without realizing it. In addition, most phone companies are already using VoIP to carry international calls, resulting in 6% of all international phone traffic now being internet-based. These phone companies have been using VoIP technology for years and its adoption rates are on the rise among businesses of all types and sizes.

There is little doubt that VoIP technology will continue to be developed and implemented over the next few years. One study estimated that corporate phone lines that adopt VoIP will leap from 4% in 2004 to 44% in 2008 due to the reduced equipment costs that will occur over the next few years Another study finds that VoIP will account for approximately 75% of world voice services by 2007 In addition, in 2002, 75% of large US organizations planned to switch to IP systems for voice within the next two years. Furthermore, 90% of enterprises with multiple locations will adopt VoIP systems over the next 5 years. As a result, a technology that has been around for years is now a proven telecommunications tool, being adopted by businesses worldwide.

VoIP has helped the phone companies and now many other businesses save money, and by implementing a VoIP phone system on your own computer networks, you could too. Many of the benefits are immediate, such as the cost savings for external calls and depending on the type of VoIP solution, free internal calls to all parts of your company that share a computer network. Cost savings are not the only advantage to adopting VoIP. The other benefits include enhanced features that help to streamline your business operations and allow for greater business continuity. For any business, IP telephony is the next wave of voice and data communications. For most businesses, it is not a matter of if they will implement VoIP; it is a matter of when and how. If you are not considering this technology today, you will be tomorrow

1.2. Background

1.2.1. VoIP, Internet Telephony, Voice-over-the-Internet:

The terms Voice-over-Internet Protocol ("VoIP"), IP telephony, Internet telephony, and Voice-over-the-Internet ("VoN") are given different meanings by different commentators and in fact have no universally agreed-upon meaning. There are, however, distinctions to be kept in mind, for IP can be used in various ways for the transmission of voice. As used in this memo, –

VoIP is a generic term that refers to all types of voice communication using Internet protocol (IP) technology instead of traditional circuit switched technology. This

includes use of packet technologies by telecommunications companies to carry voice at the core of their networks in ways that are not controlled by and not apparent to end users.

VoN, also called Internet telephony, on the other hand is a service that end users decide to use -- it is a specialized form of VoIP in which a regular voice telephone call is transmitted via the public Internet, thus bypassing all or part of the public switched telephone network (PSTN). Internet telephony can occur between computers (computer-to-computer), between a computer and a phone (computer-to-phone), and between phones (phone-to-phone).

1.2.2. Transmission Of Voice Using IP Networks.

Here is how a VoIP transmission is completed:

Step 1: Because all transmissions must be digital, the caller's voice is digitized. This can be done by the telephone company (which is how carriers use IP in their networks), by an Internet service provider (ISP), or by a PC on your desk.

Step 2: Next using complex algorithms the digital voice is compressed and then separated into packets; and using the Internet protocol, the packets are addressed and sent
across the network to be reassembled in the proper order at the destination. Again, this reassembly can be done by a carrier, and ISP, or by one's PC.

Step 3: During transmission on the Internet, packets may be lost or delayed, or errors may damage the packets. Conventional error correction techniques would request retransmission of unusable or lost packets, but if the transmission is a real-time voice communication that technique obviously would not work, so sophisticated error detection and correction systems are used to create sound to fill in the gaps. (This process stores a
portion of the incoming speaker's voice, and uses a complex algorithm to "guess" the contents of the missing packets and create new sound information to enhance the communication.)

Step 4: After the packets are transmitted and arrive at the destination, the transmission is assembled and decompressed to restore the data to an approximation of

the original form.

As this explanation suggests, technology that works fine for sending data may be less than perfect for voice transmissions. The technology is improving, but still the quality of a voice transmission using packet technology is inferior to a circuit-switched connection, and that difference in quality would normally be obvious to any listener. As IP technology improves, the quality advantage for voice communication enjoyed by the circuit-switched will decrease, but most experts see parity in quality as still a distant prospect.

1.3. Types of VoIP Adoption

Depending on the type of results you are looking for in your VoIP solution, the number of features and customizations you need, the education and efforts of your staff, and the money you choose to invest, your company has a choice to make on what type of VoIP solution will benefit and work most effectively in your

Dedicated – more customization, manage and deploy your own environment
Hosted – lower upfront costs, hosted and managed by a VoIP provider

There are two types of VoIP solutions that you can take advantage of: a dedicated environment or a hosted offering.

1.3.1 Dedicated VoIP

A dedicated solution is one in which your company hosts the VoIP server and your IT staff has the ability to customize settings and manage and deploy your own environment. Generally, this solution is best for large companies that need extensive customization and have a skilled IT staff on networking and security issues to operate and host their own VoIP solution. In addition, the dedicated VoIP solution has a larger upfront cost since the company will maintain its own VoIP server. Consequently, many

Fortune 500 companies (i.e. Ernst & Young, Hewlett Packard, Boeing) have already begun to adopt VoIP using the dedicated environment and will continue to do so in the near future.

1.3.2 Hosted VoIP

A hosted solution is one in which your company outsources your VoIP project and the server is hosted and managed by a VoIP provider. Generally, this solution is best for small to medium enterprises (SMEs) with multiple locations. With a hosted environment, the company has less upfront costs and less to maintain with a reduced overall cost of ownership. However, the small to medium sized company can take advantage of the same features and cost savings as large companies by implementing a hosted solution. By selecting the hosted VoIP solution, your company can choose only the features that will most benefit your company, while leaving the setup and maintenance to your VoIP provider's experts. In the past, many SMEs dismissed VoIP services as too costly, but now with the hosted VoIP option SMEs are using their existing investment in traditional data communications equipment to enable rich IP features like voicemail, fax support, a one-number system and free inter-office calls.

Hosted and Dedicated VoIP both offer compelling benefits and it is now your responsibility to research and investigate which option is best for you and your business. Whether you have a large company and desire extensive customization and the freedom and ability to manage your own VoIP server, or a small company and still want to take advantage of VoIP's cost savings and enhanced features, nothing is stopping you from becoming a part of the next generation of corporate communications.

1.4. Outside Technicians Or IT Staff.

To your normal functioning by including many business continuity features. For example, if an office phone becomes damaged or unusable for any reason, the calls going to that phone can be forwarded to workers at home over broadband connections. Thus, through universal IP addressing, if you lose a connection, it's much easier to switch to another connection than your traditional phone service.

In addition, hosted VoIP solutions are hosted in multiple, fully redundant, clustered environments that ensure that if one switch fails, the others can maintain uninterrupted operation. This gives users the ability to access a backup system at an off-site location in the event of a failure to the main system and can be a critical part of any overall recovery plan given the volume of messages received on a daily basis.

1.5. VoIP Components

The major components of a VoIP network are very similar in functionality to that of a circuit-switched network. VoIP networks must perform all of the same tasks that the PSTN does, in addition to performing a gateway function to the existing public network. Although using different technology and approach, some of the same component concepts that make up the PSTN also create VoIP networks. There are three major pieces to a VoIP network.

- Media gateways
- Media gateway / signaling controllers
- IP network

1.5.1 Media Gateways

Media gateways are responsible for call origination, call detection, analog-to-digital conversion of voice, and creation of voice packets (CODEC functions). In addition, media gateways have optional features, such as voice (analog and/or digital) compression, echo cancellation, silence suppression, and statistics gathering.

The media gateway forms the interface that the voice content uses so that it can be transported over the IP network. Media gateways are the sources of bearer traffic. Typically, each conversation (call) is a single IP session transported by a Real-time Transport Protocol (RTP) that runs over UDP.

Media gateways exist in several forms. For example, media gateways could be a dedicated telecommunication equipment chassis, or even a generic PC running VoIP software. Their features and services can include some or all of the following.

Trunking gateways that interface between the telephone network and a VoIP network. Such gateways typically manage a large number of digital circuits.

Residential gateways that provide a traditional analog interface to a VoIP network. Examples of residential gateways include cable modem/cable set-top boxes, xDSL devices, and broadband wireless devices.

Access media gateways that provide a traditional analog or digital PBX interface to a VoIP network. Examples include small-scale (enterprise) VoIP gateways.

Business media gateways that provide a traditional digital PBX interface or an integrated soft PBX interface to a VoIP network.

Network access servers that can attach a modem to a telephone circuit and provide data access to the Internet.

Discreet IP telephones units.

1.5.2 Media Gateway Controllers

Media gateway controllers house the signaling and control services that coordinate the media gateway functions. Media gateway controllers could be considered similar to that of H.323 gatekeepers. The media gateway controller has the responsibility for some or all of the call signaling coordination, phone number translations, host lookup, resource management, and signaling gateway services to the PSTN (SS7 gateway). The amount of functionality is based on the particular VoIP enabling products used.

In a scalable VoIP network, you can breakup the role of a controller into signaling gateway controller and media gateway controller. For calls that originate and terminate within the domain of the VoIP network, only a media gateway controller might be needed to complete calls. However, a VoIP network is frequently connected to the public network. You could use a signaling gateway controller to directly connect to the SS7 network, while also interfacing to the VoIP network elements. This signaling controller would be dedicated to the message translation and signaling needed to bridge the PSTN to the VoIP network.

The services of these devices are defined by the protocols and software they are running. There are several protocols and implementations that any number of vendors could deploy. Knowing the details of how the devices use their suite of protocols is important to designing the IP backbone that is to service the VoIP elements.

1.5.3 IP Network

You can view the VoIP network as one logical switch. However, this logical switch is a distributed system, rather than that of a single switch entity; the IP backbone provides the connectivity among the distributed elements. Depending on the VoIP protocols used, this system as a whole is sometimes referred to as a softswitch architecture.

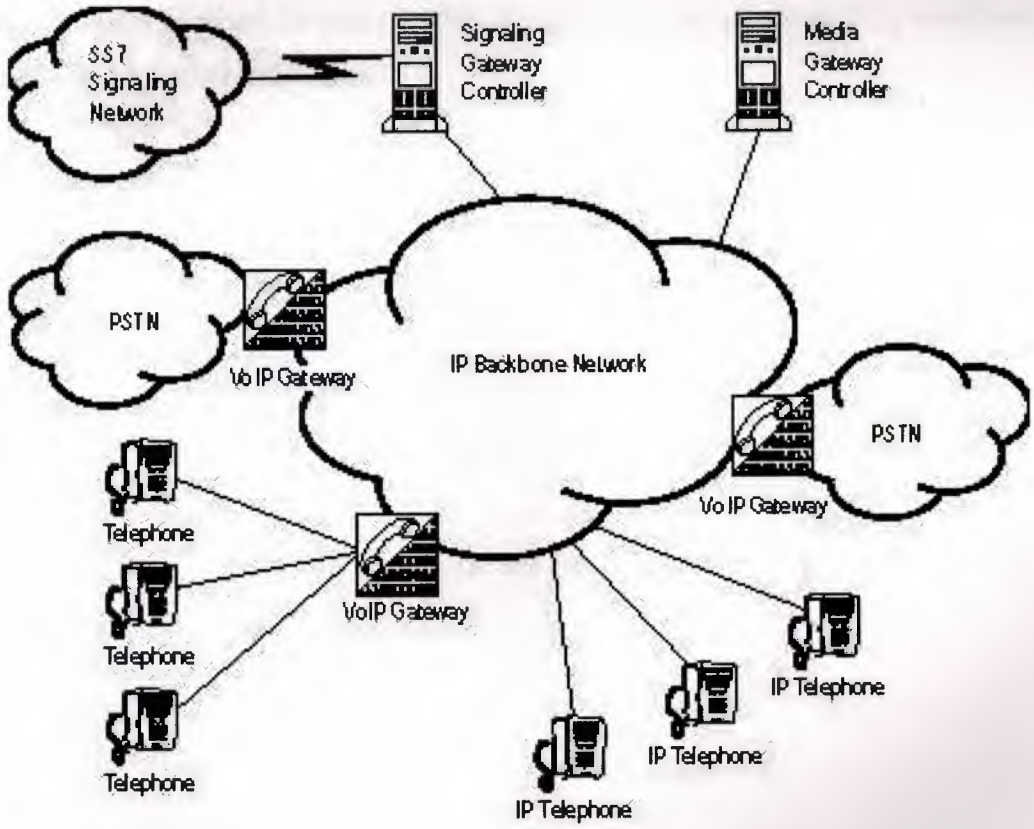

Figure 1.1: Full Service VoIP Network

The IP infrastructure must ensure smooth delivery of the voice and signaling packets to the VoIP elements. Due to their dissimilarities, the IP network must treat voice and data traffic differently. If an IP network is to carry both voice and data traffic, it must be able to prioritize the different traffic types.

There are several correlations to the VoIP and circuit-switching components, however

there are many differences. One is in the transport of the resulting voice traffic. Circuit-switching telecommunications can be best classified as a TDM network that dedicates channels, reserving bandwidth as it is needed out of the trunk links interconnecting the switches. For example, a phone conversation reserves a single DS-0 channel, and that end-to-end connection is used only for the single conversation.

IP networks are quite different from the circuit-switch infrastructure in that it is a packet-network, and it is based on the idea of statistical availability. Class of service (CoS) ensures that packets of a specific application are given priority. This prioritization is required for real-time VoIP applications to ensure that the voice service is unaffected by other traffic flows.

1.6. Summary

VoIP is here and it is now. VoIP can offer your business substantial savings in capital and operating costs as well as enhanced functionality by converging separate voice and data networks into a single multi-service network. Whether your office consists of 25 employees, 500 employees, or thousands of employees across the globe you have a choice in the type of VoIP solution you wish to implement. Both dedicated and hosted options are available to SMEs and large multi-national corporations. The many advantages and benefits of implementing VoIP outweigh the risks; hence, most businesses are planning to implement some type of VoIP solution in the upcoming year. In a competitive marketplace, businesses most always be sure to investigate any and all opportunities for growth and efficiency. As a result, it is important that your business investigate how VoIP can help you to achieve this goal. This flourishing telecommunications tool cannot be stopped. Investigation of IP telephony, and how it can better serve your employees, clients and vendors is vital in order to maintain an efficient and productive business.

CHAPTER TWO

VOIP BACKGROUND

2.1 Overview

In this chapter we will discuss in detail about the background and functions of different protocols .We will discuss the background and functions of the following protocols:

1-TCP/IP (Transmission Control Protocol/Internet Protocol)

2-H.323 (Multimedia Protocol)

3-802.11b

4-RTP (Real Time Protocol)

5-UDP (User Datagram Protocol)

6-CSMA/CD (Carrier Sense Multiple Accesses / Collision Detection.)

7-CSMA/CA (Carrier Sense Multiple Accesses / Collision Avoidance)

2.2 Background of TCP/IP

When communication is desired among computers from different vendors, the software development effort can be a nightmare. Different vendors use different data formats and data exchange protocols. Even within one vendor's product line, different model computers may communicate in unique ways.

As the use of computer communications and computer networking proliferates, a one-at-a-time special-purpose approach to communications software development is too costly to be acceptable. The only alternative is for computer vendors to adopt and implement a common set of conventions. For this to happen, standards are needed.

However, no single standards will suffice. Any distributed application, such as electronic mail or client/ server interaction, requires a complex set of communications functions for proper operation. Many of these functions, such as reliability mechanisms, are common across many or even all applications. Thus, the communications task is best viewed as consisting of a modular architecture, in which the various elements of the architecture perform the various required functions. Hence, before one can develop standards, there should be a structure, or *protocol architecture*, that defines the communications tasks.

Two protocol architectures have served as the basis for the development of interoperable communications standards: the TCP/IP protocol suite and the OSI (Open Systems Interconnection) reference model. TCP/IP is the most widely used interoperable architecture, and has won the "protocol wars." Although some useful standards have been developed in the context of OSI, TCP/IP is now the universal interoper-able protocol architecture. No product should be considered as part of a business information system that does not support TCP/IP.

2.2 1.TCP/IP Layers

The communication task using TCP/IP can be organized into five relatively independent layers: physical, network access, internet, transport, and application. The physical layer covers the physical interface between a data transmission device (e.g., workstation, computer) and a transmission medium or network. This layer is concerned with specifying the characteristics of the transmission medium, the nature of the signals, the data rate, and related matters. The network access layer is concerned with the exchange of data between an end system and the net-work to which it is attached.

The sending computer must provide the network with the address of the destination computer, so that the network may route the data to the appropriate destination. The sending computer may wish to invoke certain services, such as priority, that might be provided by the network. The specific software used at this layer depends on the type of network to be used; different standards have been developed for circuit-switching, packet-switching (e.g., X.25), local area networks (e.g., Ethernet), and others. Thus it makes sense to separate those functions having to do with network access into a separate layer. By doing this, the remainder of the communications software, above the network access layer, need not be concerned about the specifics of the network to be used. The same higher-layer software should function properly regardless of the particular network to which the computer is attached. The network access layer is concerned with access to and routing data across a network for two end systems attached to the same network. In those cases where two devices are attached to different net-works, procedures are needed to allow data to traverse multiple interconnected networks. This is the function of the internet layer. The internet protocol (IP) is used at this layer to provide the routing function across multiple networks. This protocol is implemented not only in the end systems but also in routers. A *router* is a processor that connects two networks and whose primary function is to relay data from one network to the other on its route from the source to the destination end system. Regardless of the nature of the applications that are exchanging data, there is usually a requirement that data be exchanged reliably. That is, we would like to be assured that all of the data arrive at the destination application and that the data arrive in the same order in which they were sent. As we shall see, the mechanisms for providing reliability are essentially independent of the nature of the applications. Thus, it makes sense to collect those mechanisms in a common layer shared by all applications; this is referred to as the host-to-host layer, or transport layer. The transmission control protocol (TCP) is the most commonly-used protocol to provide this functionality. Finally, the application layer contains the logic needed to support the various user applications. For each different type of application, such as file transfer, a separate module is needed that is peculiar to that application.

2.2 2.Operation of TCP/IP

Figure 2.1 indicates how these protocols are configured for communications. To make clear that the total communications facility may consist of multiple networks, the

constituent networks are usually referred to as subnetwork*s*. Some sort of network access protocol, such as the Ethernet logic, is used to connect a computer to a sub network. This protocol enables the host to send data across the subnetwork to another host or, in the case of a host on another sub network, to a router. IP is implemented in all of the end systems and the routers. It acts as a relay to move a block of data from one host, through one or more routers, to another host. TCP is implemented only in the end systems; it keeps track of the blocks of data to assure that all are delivered reliably to the appropriate application.

For successful communication, every entity in the overall system must have a unique address. Actually, two levels of addressing are needed. Each host on a subnetwork must have a unique global internet address; this allows the data to be delivered to the proper host. This address is used by IP for routing and delivery. Each application within a host must have an address that is unique within the host; this allows the host-to-host protocol (TCP) to deliver data to the proper process. These latter addresses are known as ports.

Let us trace a simple operation. Suppose that an application, associated with port 1 at Host A Host B

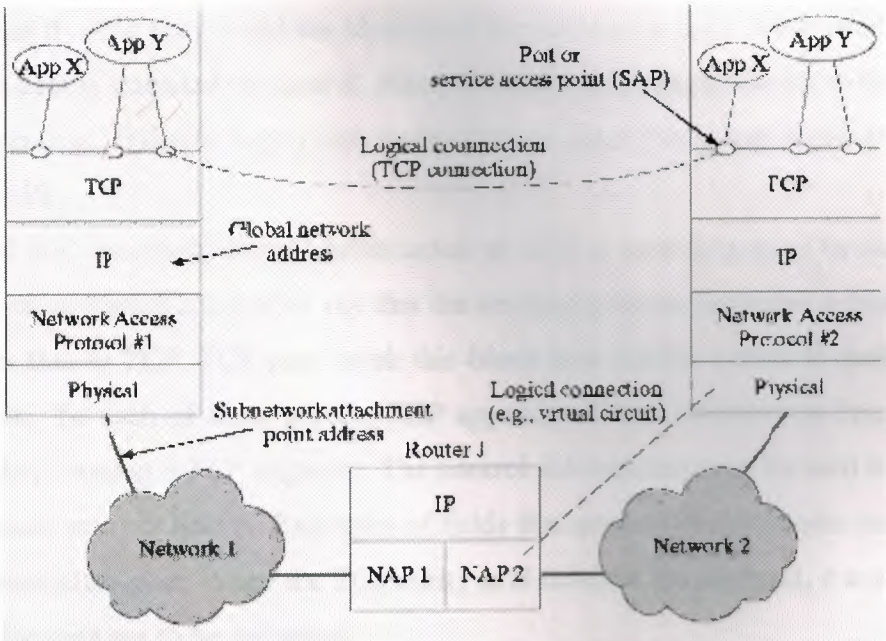

Figure 2.1: TCP/IP Concepts

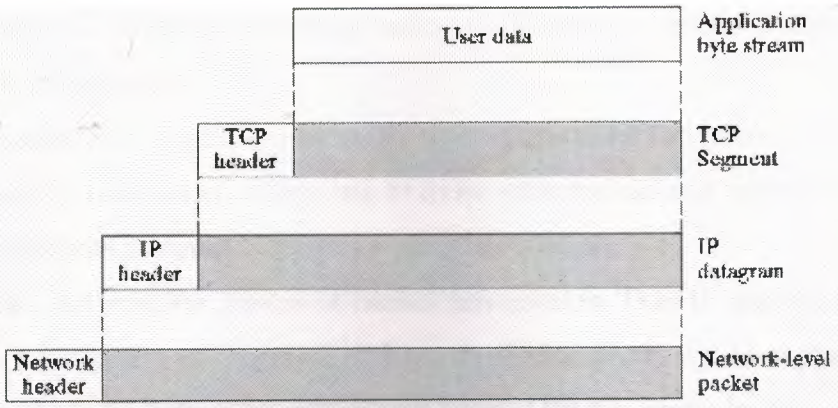

Figure 2.2: Protocol Data Units In The TCP/IP Architecture

Host *A*, wishes to send a message to another application, associated with port 2 at host *B*. The application at *A* hands the message down to TCP with instructions to send it to host *B*, port 12. TCP hands the message down to IP with instructions to send it to host *B*. Note that IP need not be told the identity of the destination port. All it needs to know is that the data is intended for host *B*. Next, IP hands the message down to the network access layer (e.g., Ethernet logic) with instructions to send it to router *X* (the first hop on the way to *B*).

To control this operation, control information as well as user data must be transmitted, as suggested in Figure 2.2. Let us say that the sending process generates a block of data and passes this to TCP. TCP may break this block into smaller pieces to make it more manageable. To each of these pieces, TCP appends control information known as the TCP header, forming a *TCP* segment. The control information is to be used by the peer TCP protocol entity at host B. Examples of fields that are part of this header include:

Destination port: When the TCP entity at *B* receives the segment, it must know to whom the data are to be delivered.

Sequence number: TCP numbers the segments that it sends to a particular destination port sequentially, so that if they arrive out of order, the TCP entity at *B* can reorder them.

Checksum: The sending TCP includes a code that is a function of the contents of the remainder of the segment. The receiving TCP performs the same calculation and

compares the result with the incoming code. A discrepancy results if there has been some error in transmission.

Next, TCP hands each segment over to IP, with instructions to transmit it to *B*. These segments must be transmitted across one or more subnetworks and relayed through one or more intermediate routers.

This operation, too, requires the use of control information. Thus IP appends a header of control informa-tion to each segment to form an *IP datagram*. An example of an item stored in the IP header is the desti-nation host address (in this example, *B*).

Finally, each IP datagram is presented to the network access layer for transmission across the first subnetwork in its journey to the destination. The network access layer appends its own header, creating a packet, or frame. The packet is transmitted across the subnetwork to router J. The packet header contains the information that the subnetwork needs to transfer the data across the subnetwork. Examples of items that may be contained in this header include:

Destination subnetwork address: The subnetwork must know to which attached device the packet is to be delivered.

Facilities requests: The network access protocol might request the use of certain subnet-work facilities, such as priority.

At router J, the packet header is stripped off and the IP header examined. On the basis of the destina-tion address information in the IP header, the IP module in the router directs the datagram out across sub-network 2 to *B*. To do this, the datagram is again augmented with a network access header.

When the data are received at *B*, the reverse process occurs. At each layer, the corresponding header is removed, and the remainder is passed on to the next higher layer, until the original user data are delivered to the destination application.

2.3.Background of H.323

H.323 is the ITU specification for audio and video communication across packetized networks. H.323 is actually an umbrella standard, encompassing several other protocols, including H.225, H.245, and others. It acts as a wrapper for a suite of media control recommendations by the ITU. Each of these protocols has a specific role in the

call setup process, and all but one are made to dynamic ports. Figure 4 provides an overview of the H.323 call setup process.

2.3.1 H.323 Architecture

An H.323 network is made up of several endpoints (terminals), a gateway, and possibly a gatekeeper, Multipoint control unit, and Back End Service. The gateway is often one of the main components in H.323 systems. It serves for address resolution and bandwidth control. The gateway serves as a bridge between the H.323 network and the outside world of (possibly) non-H.323 devices. This includes SIP networks and traditional PSTN networks. This brokering can add to delays in VOIP, and hence there has been a movement towards the consolidation of at least the two major VOIP protocols .A Multipoint Control Unit is an optional element that facilitates multipoint conferencing and other communications between more than two endpoints. Gatekeepers are an optional but widely used component of a VOIP network that perform several network optimization tasks .If a gatekeeper is present, a Back End Service (BES) may exist to maintain data about endpoints, including their permissions, services, and configuration.

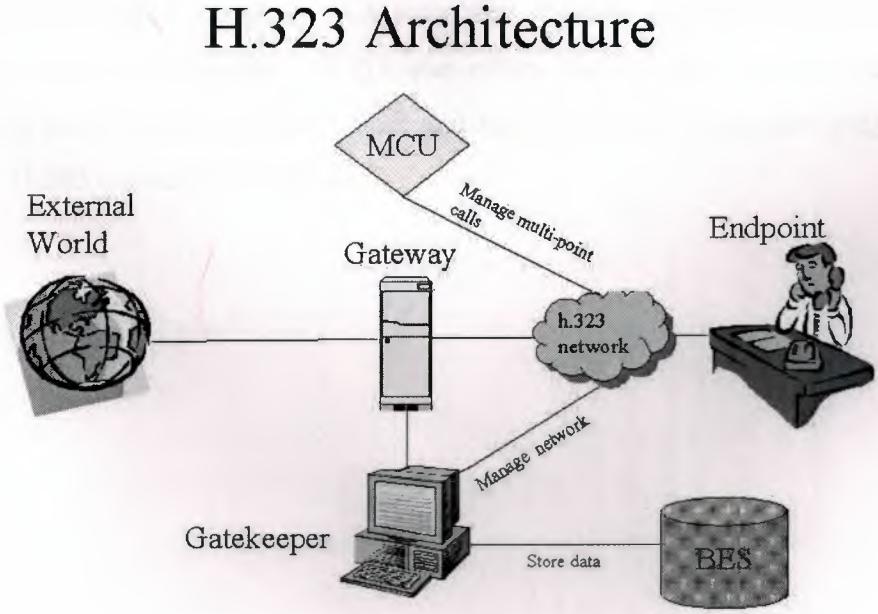

Figure 2.3: H.323 Architecture

Generally, there are different types of H.323 calls defined in the H.323 standard:

- Gatekeeper routed call with gatekeeper routed H.245 signaling
- Gatekeeper routed call with direct H.245 signaling
- Direct routed call with gatekeeper
- Direct routed call without gatekeeper

An H.323 VOIP session is initiated (depending on the call model used) by either a TCP or a UDP (if RAS is the starting point) connection with an H.225 signal. In the case of UDP this signal contains the Registration Admission Status (RAS) protocol that negotiates with the gatekeeper and obtains the address of the endpoint it is attempting to contact. Then a "Q.931-like" protocol (still within the realm of H.225) is used to establish the call itself and negotiate the addressing information for the H.245 signal. (This is done via TCP; Q.931 actually encapsulates the H.225 Call Signaling messages.) This "setup next" procedure is common throughout the H.323 progression where one protocol negotiates the configuration of the next protocol used. In this case, it is necessary because H.245 has no standard port. While H.225 simply negotiates the establishment of a connection, H.245 establishes the channels that will actually be used for media transfer. Once again, this is done over TCP. In a time-urgent situation, the H.245 message can be embedded within the H.225 message (H.245 tunneling), but the speed of a call setup is usually a QoS issue that vendors and customers are willing to concede for better call quality. H.323 also offers Fast Connect. Here, a call may be setup using one roundtrip. The SETUP and the CONNECT messages piggyback the necessary H.245 signaling elements.

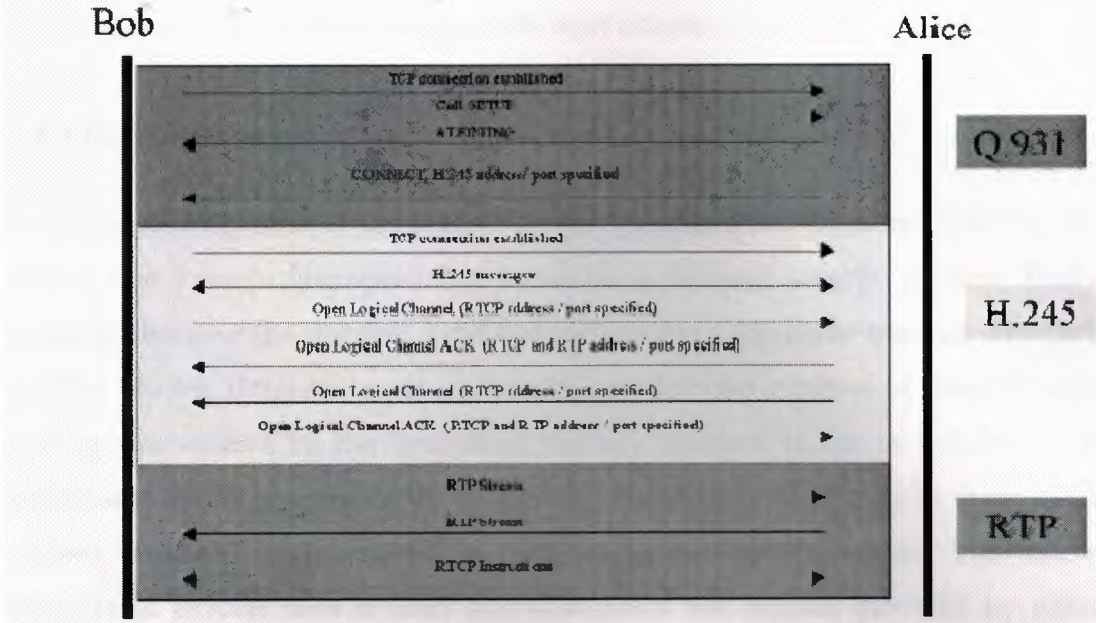

Figure 2.4: H.323 Call Setup Process

2.3.2 H.245

H.245 must establish several properties of the VOIP call. These include the audio codices that will be used and the logical channels for the transportation of media. The "Open Logical Channel" signal also brokers the RTP and RTCP ports. Overall, connections must be established because the logical channels (RTP and RTCP) are only one direction. Each one-way pair must also be on adjacent ports as well. After H.245 has established all the properties of the VOIP call and the logical channels, the call may begin.

The preceding described the complicated VOIP setup process based on H.323, although the complexities have been somewhat reduced with version 4 of H.323. The H.323 suite has different protocols associated with more complex forms of communication including H.332 (large conferences), H.450.1, H.450.2, and H.450.3 (supplementary services), H.235 (security), and H.246 (interoperability with circuit switched services) . Authentication may also be performed at each point in the call setup process using symmetric keys or some prior shared secret The use of these extra protocols and/or

security measures adds to the complexity of the H.323 setup process. We shall see that this complexity is paramount in the incompatibility of H.323 with firewalls and NATs. These issues are discussed at length in the next section.

2.3.3 H.235 Security Profiles

With the establishment of the H.235 version 2 standard in November 2000 the ITU-T took a step towards interoperability by defining different security profiles. This was necessary because the standard itself does not mandate particular features. The defined profiles provide different levels of security and describe a subset of possible security mechanisms offered by the considered security standard H.235 as mandatory. They comprise different options for the protection of communication, e.g., by using different options of H.235, which results in different implementation impact. The following subsections provide here a short overview about the profiles provided by different organizations.

2.3.4 H.235v2

H.235v2 is the follow up version of H.235 that was approved in November 2000. Besides enhancements such as the support of elliptic curve cryptography and the support for AES, several security profiles are defined to support product interoperability. These profiles are defined in annexes to H.235v2 as follows:

- Annex D – Shared secrets and keyed hashes
- Annex E – Digital signatures on every message
- Annex F – Digital signatures and shared secret establishment on first handshake, afterwards keyed hash usage

2.3.4.1 H.235v2 Annex D – Baseline Security Profile

The Baseline Security Profile relies on symmetric techniques. Shared secrets are used to provide authentication and/or message integrity. The supported scenarios for this profile are endpoint to gatekeeper, gatekeeper to gatekeeper, and endpoint to endpoint. For the profile the gatekeeper-routed signaling (hop-by-hop security) is favored. Using it for the direct call model is generally possible but limited due to the fact that a shared secret has to be established between the parties that want to communicate before the actual

communication takes place. This might be possible in smaller environments but will lead to huge administrative effort in larger environments.

Note: This profile is easy to implement but it is not really scalable for "global" IP telephony due to the restricted key management.

2.3.4.2 H.235v2 Annex E – Signature Security Profile

The Signature Security Profile relies on asymmetric techniques. Certificates and digital signatures are used to provide authentication and message integrity. The signature security profile mandates the gatekeeper-routed model. Other call models are for further study. Since this profile relies on a public key infrastructure rather than on pre-established shared secrets it scales for larger, global environments. In addition to the Baseline Security Profile it provides non-repudiation.

This profile supports secure fast connect and H.245 tunneling and may be combined with the Voice Encryption Option described in section 3.3.1.3.

Note: This protocol may have a critical impact on overall performance. This is due to the use of digital signatures for every message, requiring signature generation and verification on the sender's and the receiver's side. The Hybrid Security Profile described in section 3.3.1.4 provides an alternative to the Signature Security Profile.

2.3.4.3 H.235v2 Annex D - Voice Encryption Option

The voice encryption option offers confidentiality for the voice media stream data and may be combined with the baseline or the signature security profile.

The voice encryption option describes the master key exchange during H.225.0 call signaling and the generation, and distribution of media stream keys during H.245 call control. The encryption algorithms are to be used in CBC mode. New is the support of the AES. AES and TDEA may also be used in EOFB mode.

The following security mechanisms are described within the voice encryption security profile:

- Encryption of RTP packets with an assortment of algorithms and modes to be taken;
- Key management with key and security capability exchange;

- Key update mechanism and synchronization.

The following issues are not covered by this profile:

- Encryption and key management for RTCP;
- Authentication and integrity for RTP and RTCP (a lightweight authentication and integrity could be provided by media anti-spamming).

To counter denial of service and flooding attacks on discovered RTP/UDP ports, the H.235 standard defines the media anti-spamming procedure, which provides lightweight RTP packet authentication and integrity on selected fields through a computed message authentication code (MAC). The algorithms used are triple-DES-MAC or the cryptographic one-way function SHA1. Media anti-spamming uses the padding mechanism of RTP. For this feature no special security profile was specified in H.235 like the voice encryption security profile for the RTP encryption. But media anti-spamming may be used in combination with media encryption.

2.3.4.4 H.235v2 Annex F – Hybrid Security Profile

The Hybrid Security Profile relies on asymmetric and symmetric techniques. It can be seen as a combination of the Baseline and the Signature Security Profile. Certificates and digital signatures are used to provide authentication and message integrity (as in the Signature Security Profile) for the first handshake between two entities. During this handshake a shared secret is established that will be used further on in the same way described for the Baseline Security Profile. The hybrid security profile mandates the gatekeeper-routed model. Other call models are open for further study.
Since this profile relies on a public key infrastructure rather than on pre-established shared secrets it scales for larger, global environments.
Note: This profile provides high security without relying on pre-established shared secrets. Due to the key management using digital signatures it is scalable for "global" IP telephony. Moreover, it does not suffer from the same performance requirements as the Signature Security Profile described in section 3.3.1.2.

2.3.5 H.235v3

Version 3 of H.235 supersedes H.235 version 2 featuring a procedure for encrypted DTMF (touch tone) signals, object identifiers for the AES encryption algorithm for media payload encryption, and the enhanced OFB (EOFB) stream-cipher encryption mode for encryption of media streams. Moreover, an authentication-only option in Annex D for smooth NAT/firewall traversal is introduced as well as better security support for direct-routed calls in a new Annex I. Also improved is the error reporting.

Annex G is also discussed to support H.235v3. Annex G describes a profile to support SRTP.

2.3.5.1 H.235v3 Annex D – Baseline Security Profile Enhancements

Using this profile, either message authentication and integrity is achieved by calculating an integrity check value over the complete message, or authentication only by computing an integrity check over a special part of the message. The latter option is useful in environments where NAT and Firewalls are applied. The version used is distinguished by an identifier.

2.3.5.2 Draft H.235v3 Annex G – SRTP & MIKEY usage

Annex G discusses the incorporation of a key management supporting the Secure Real-time Transport Protocol (SRTP). This Annex is still not standardized since the referenced IETF documents for key management MIKEY, as well as for media data security SRTP are also not determined and thus not available as a proposed standard.
The Secure Real-time Transport Protocol (SRTP) provides confidentiality, message authentication and replay protection to the RTP/RTCP traffic. The RTP standard provides the flexibility to adapt to application specific requirements with the possibility to define profiles in companion documents. SRTP is defined as such a profile of the RTP protocol and it is currently in the status of an Internet-Draft. The draft is currently in the editor's queue of IETF and is expected to be a standard soon. SRTP may be used within multimedia sessions to ensure a secure media data exchange. It can be used with several session control protocols, e.g., with H.323 or SIP.

SRTP does not define key management by itself. It rather uses a set of negotiated parameters from which session keys for encryption, authentication and integrity protection are derived. The key management is not fixed. Within the IETF, the working group MSEC discusses key management solutions to be used beyond other protocols with SRTP. The preferred solution here is MIKEY which is also part of the group key management architecture.

MIKEY describes a key management scheme that addresses real-time multimedia scenarios (e.g. SIP calls and RTSP sessions, streaming, unicast, groups, multicast). The focus lies on the setup of a security association for secure multimedia sessions including key management and update, security policy data, etc., such that requirements in a heterogeneous environment are fulfilled. MIKEY also supports the negotiation of single and multiple crypto sessions. This is especially useful for the case where the key management is applied to SRTP, since here RTP and RTCP may to be secured independently. Deployment scenarios for MIKEY comprise peer-to-peer, simple one-to-many, and small-size interactive group scenarios.

MIKEY supports the negotiation of cryptographic keys and security parameters (SP) for one or more security protocols. This results in the concept of crypto session bundles, which describe a collection of crypto sessions that may have a common Traffic Encryption Key (TEK) Generation Key (TGK) and belonging session security parameters.

MIKEY defines three options for the user authentication and negotiation of the master keys all as 2 way-handshakes. They are:

- Symmetric key distribution (pre-shared keys, MAC for integrity protection)
- Asymmetric key distribution
- Diffie Hellman key agreement protected by digital signatures

A fourth version exists, which is not part of MIKEY itself. It is specified as an extension to MIKEY and describes the Diffie Hellman key agreement protected by symmetric pre-shared keys.

The default and mandatory key transport encryption is AES in counter mode. MIKEY uses a 160-bit authentication tag, generated by HMAC with SHA-1 as the mandatory

algorithm as described in [RFC2104]. Also mandatory, when asymmetric mechanisms are used, is the support of X.509v3 certificates for public key encryption and digital signatures.

Annex G discusses the utilization of MIKEY to integrate a key management suitable for SRTP in three profiles as there are:

- Profile 1 using symmetric techniques to protect the key management data in gatekeeper routed scenarios;
- Profile 2 using asymmetric techniques to protect the key management data in scenarios with a single gatekeeper instance;
- Profile 3 describes Profile 2 for multiple intermediate gatekeepers.

The basic concept of all profiles is the protected transmission of the key management data as self-contained container.

2.3.5.3 Draft H.235v3 Annex H – RAS Key Management

The basic idea formulated in H.235 Annex H is key management negotiation during the RAS gatekeeper discovery phase. During gatekeeper discovery a shared secret is established between the endpoint and the gatekeeper. The negotiation of the shared secret may be protected using PINs or passwords (shared secrets).

The draft references two protocols for Encrypted Key Exchange using a shared secret to "obscure" a Diffie-Hellman key exchange. The first one is the Encrypted Key Exchange (EKE), where the shared secret is used to encrypt the Diffie-Hellman public keys under a symmetric algorithm. The second one is the Simple Password-authenticated Exponential Key Exchange (SPEKE) method, where the shared secret builds a generator for the Diffie-Hellman group. The usage of these protocols leads to a strong Diffie-Hellman key exchange with use of the shared secret. A potential disadvantage of these protocols is that they are typically subject to patent protection.

The draft discusses the utilization of the PIN or password for the protection of the exchange of the public parameter of public key system (Diffie Hellman, elliptic curves) by encryption using a symmetric algorithm in CBC mode. To be more specific, the password or PIN is used to derive the initialization vectors for the encryption

algorithms. The negotiated keys and algorithms may then be applied later on to protect the further RAS and call signaling phase.

One option to protect the call signaling phase is TLS, which is discussed further in the draft Annex H. Here, the RAS negotiation replaces the initial TLS handshake protocol. This is obviously only useful if the call signaling is gatekeeper routed. The approach is especially useful for inter-gatekeeper authentication and signaling using the LRQ/LCF exchange. In this case, there is no third RAS message by which the calling gatekeeper can authenticate itself to the called gatekeeper using the negotiated key material, but the caller can be implicitly authenticated by its ability to establish the call signaling channel with the correct TLS session parameters. TLS can then be deployed without the costly handshake phase using only the recode layer of TLS together with the negotiated key material and algorithms from the RAS phase.

2.3.5.4 H.235v3 Annex I – H.235 Annex D for Direct Routed Scenarios

Both Annex D and Annex F are to be used in gatekeeper routed environments. Annex I of H.235 enhances the Baseline Security Profile (Annex D, section 3.3.1.1) as well as the Hybrid Security Profile (Annex F, section 3.3.1.3) with the option to be applied in an environment were direct routed calls (endpoint to endpoint) are performed using the gatekeeper for address resolution. Since endpoints do not possess a shared secret from scratch, a Kerberos-like approach is taken to establish a shared secret between the communicating endpoints. This is done using the admission phase from the calling endpoint and the call signaling between the calling and the called endpoint. The gatekeeper serves in this scenario also as the key distribution center (KDC), issuing two "tickets" (tokens), one containing the key material secured with the caller's encryption key and the other one secured with the called party encryption key. The encryption keys are derived form the shared secret between the caller and the gatekeeper using a pseudo random function (PRF), which is also defined by H.235 Annex I. The PRF is basically the same as used in TLS.

The gatekeeper also generates a session key, which is applicable for the communication between the two endpoints involved in the call, and encrypts this key material using the previously derived encryption keys. The encrypted session keys are then transmitted

back to the caller. The caller utilizes the encrypted session key destined to him, the other one is sent to the called party as part of the SETUP message.

The messages exchanged between the gatekeeper and the calling endpoint carrying the tickets are secured with either the H.235 Annex D or with H.235 Annex F. The shared secret established via the "ticket" (token) exchange between caller and caller may be used in subsequent direct messages to provide an integrity protection according to H.235 Annex D.

2.3.6 H.323 Annex J

H.323 Annex J describes security for simple endpoint types, which are defined by H.323 Annex F. This profile relies on the Baseline Security Profile described in section 3.3.1.1.

2.3.6.1 H.323 Security Issues

Firewalls pose particularly difficult problems for VOIP networks using H.323. With the exception of the "Q.931-like" H.225, all H.323 traffic is routed through dynamic ports. For H.323 Fast Start and H.245 tunneling just one channel (H.225 Call Signaling) is used. Usually the call signaling is performed via port 1720. If additionally H.225 RAS communication is done with the gatekeeper (UDP), this is done via port 1719. That is, each successive channel in the protocol is routed through a port dynamically determined by its predecessor. This ad-hoc method of securing channels does not lend itself well to a static firewall configuration. This is particularly true in the case of stateless firewalls that cannot comprehend H.323 traffic. These simple packet filters cannot correlate UDP transmissions and replies. This necessitates punching holes in the firewall to allow H.323 traffic to traverse the security bridge on any of the ephemeral ports it might use. This practice would introduce serious security weaknesses because such an implementation would need to leave 10,000 UDP ports and several H.323 specific TCP ports wide open [sample configuration provided in 1]. We see here the need for a stateful firewall that understands VOIP, specifically H.323. Such a firewall can read H.323 messages and dynamically open the correct ports for each channel as the protocol moves through its call setup process. Such a firewall must be part of a security architecture especially in scenarios where protocol–provided security measures are

applied, e.g. message integrity. Barring this, some kind of proxy server or middlebox would have to be used.

Even with a VOIP-aware firewall, parsing H.323 traffic is a non-trivial matter. H.323 traffic is encoded in a binary format based on ASN.1. ASN.1 does not use fixed offsets for address information, and different instances of an application may negotiate different options, resulting in different byte offsets for the same information this level of complexity does not allow for simple parsing tools or uncomplicated Perl scripts to decode the traffic; in fact special code generators are needed such technology is not available on traditional packet filtering firewalls or even simple stateful firewalls. Although this analysis can be done using modern VOIP aware gateways, the complex parsing necessary to discern the contents of the ASN.1 encoded packets introduces further latency into a speed-sensitive system that is already saturated with delays.

NAT is also particularly troublesome for VOIP systems using the H.323 call setup protocol. NAT throws a monkey wrench into the system because the external IP address and port specified in the H.323 headers and messages themselves are not the actual address/port numbers used internally. This disrupts the "setup next" procedure used by each protocol within the H.323 suite (e.g., .225 setting up H.245). Not only does the firewall have to comprehend this, but it is essential that the VOIP application receiving these H.323 communications receives the correct translated address/port numbers. Thus, if H.323 is to traverse a NAT gateway, the NAT device must be able to reconfigure the addresses in the control stream. So with NAT, not only does H.323 traffic need to be read, it must also be modified so that the correct address/port numbers are sent to each of the endpoints.

2.3.7 SIP

SIP is the IETF specified protocol for initiating a two-way communication session. It is considerably simpler than H.323. When simple calls are to be performed. SIP is text based; thereby avoiding the ASN.1 associated parsing issues that exist with the H.323 protocol suite, if S/MIME as part of the SIP inherent security measures is not used. Also, SIP is an application level protocol, that is, it exists independently from the protocol layer it is transported across. It can be based in TCP, UDP, or a number of

different IP protocols. UDP may be used to decrease overhead and increase speed and efficiency, or TCP may be used if SSL/TLS is incorporated for security services. Unlike H.323, only one port is used in SIP (note that H.323 may also be used in a way that uses only one port – direct routed calls). The default value for this port is 5060.

2.4 Background of 802.11b

Although the IEEE 802.11 standard is composed of multiple layers (from the physical layer up through the data-link layer), of particular interest is the 802.11b MAC layer because of its unique interaction with transport layer (TCP in particular). The basic access mechanism in 802.11b MAC is DCF, and is basically a carrier sense multiple access with collision avoidance mechanism. CSMA protocols are common within industry, the most notable being Ethernet which is a CSMA/CD protocol.

A CSMA protocol works as follows: a station desiring to transmit senses the medium; if it is busy (e.g. some other station is transmitting), the station will defer until a later time, and otherwise if the medium is sensed free, the station will transmit.

These types of protocols are very effective if the medium is not heavily loaded, since it allows stations to transmit with minimum delay. But, there is always a chance of two stations transmitting at the same time (if they both sense the medium free at the same moment).

Although Ethernet uses a CD technique to detect when two stations transmit simultaneously and collide, in the wireless environment it turns out that such collision detection cannot be implemented (due to the hidden terminal problem, and half-duplex radios). Thus, instead of using collision detection, 802.11b uses a CA mechanism coupled with a positive acknowledgment scheme.

A station ready to transmit will sense the medium first, if the medium is busy, and then it will defer. If the medium is free for a specified amount of time (called the distributed inter-frame space, DIFS), the station is allowed to transmit. The receiving station will check the CRC of the packet, and if the packet was received successfully, send an acknowledgement packet (ACK). If the sender does not receive the acknowledgment

within a certain time interval, then the sender knows that there was a collision and will retransmit up to a certain retransmission limit. Before retransmitting, the sender will employ a random exponential backoff that prevents the colliding stations from retransmitting at the same exact moment.

In addition to ACKs, 802.11b employs so-called "virtual carrier sense" via the use of RTS/CTS packets. When a station wishes to send to another station, it may optionally first send a RTS packet (containing the length of the requested transmission) in the manner described above. The receiving station will respond with a CTS packet that all other hidden terminals of the sender can hear, with a time period specified that the sender will be allowed to transmit (the "network allocation vector", or NAV). Other senders in the network will respect this CTS packet and corresponding NAV time, preventing collisions. Since RTS/CTS packets are very short, they minimize the overhead related to collisions if they do occur. In actual 802.11b implementations, RTS/CTS is only used when the length of a packet exceeds a "RTS threshold" – which on most typical cards is around 2Kb. Thus, typically RTS/CTS are very rarely used if ever in actual 802.11b networks.

The following diagram in Figure 2.5 illustrates the typical exchange between two 802.11b nodes in a network:

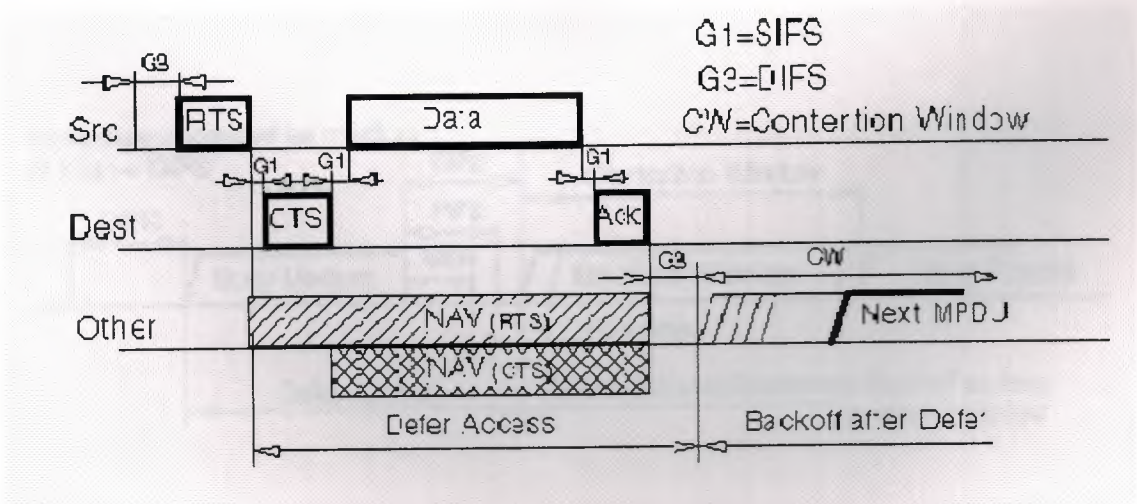

Figure 2.5: The typical exchange between two 802.11b nodes in a network

As mentioned earlier, 802.11b employs random exponential backoff in order to resolve contention after a collision in a crowded network. Effectively random backoff works as follows: the station will choose a random number between zero and a given number, and wait this number of slots before accessing the medium again, always checking again if the medium is busy before accessing.

These slots times are defined in such a way so that a station can detect if another station is transmitting at the beginning of the previous slot. This effectively reduces the collision probability by half (e.g. ALOHA vs. slotted-ALOHA).

The exponential backoff means that each time a station chooses a slot and happens to collide; it will increase the maximum number for the random selection exponentially. In 802.11b, the exponential backoff algorithm MUST be executed in the following cases:

- If, when the station senses the medium before the first transmission of a packet, the medium is busy.
- After each retransmission.
- After a successful transmission.

The only time when exponential backoff is not used is when a station wishes to initially transmit and the medium has been free for more than a DIFS, see Figure 2.6.

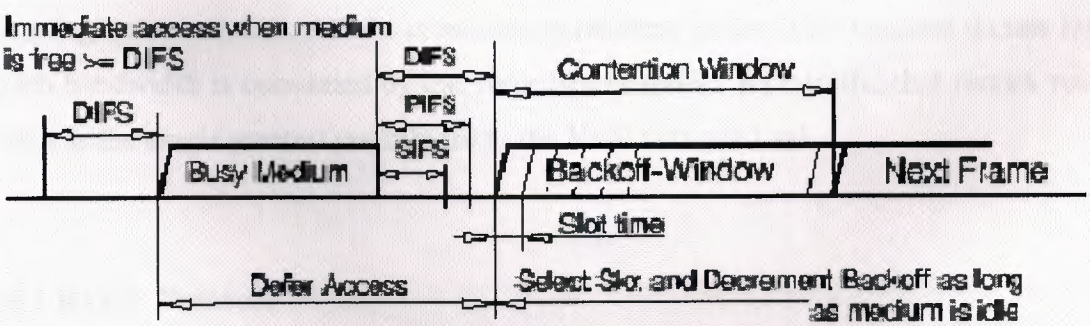

Figure 2.6: The timing structure

2.5.Background of (RTP)

RFC 1889 and RFC 1890 cover the RTP, which provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. Services include payload type identification, sequence numbering, time stamping, and delivery monitoring.

The RTP protocol provides features for real-time applications, with the ability to reconstruct timing, loss detection, security, content delivery and identification of encoding schemes. The media gateways that digitize voice use the RTP protocol to deliver the voice (bearer) traffic. For each participant, a particular pair of destination IP addresses defines the session between the two endpoints, which translates into a single RTP session for each phone call in progress.

RTP is an application service built on UDP, so it is connectionless with best-effort delivery. Although RTP is connectionless, it does have a sequencing system that allows for the detection of missing packets.

As part of its specification, the RTP Payload Type field includes the encoding scheme that the media gateway uses to digitize the voice content. This field identifies the RTP payload format and determines its interpretation by the CODEC in the media gateway. A profile specifies a default static mapping of payload type codes to payload formats. These mappings represent the ITU G series of encoding schemes.
With the different types of encoding schemes and packet creation rates, RTP packets can vary in size and interval. You must take RTP parameters into account when planning voice services. All the combined parameters of the RTP sessions dictate how much bandwidth is consumed by the voice bearer traffic. RTP traffic that carries voice traffic is the single greatest contributor to the VoIP network load.

2.5.1 RTCP Protocol

Real-time Transport Control Protocol (RTCP) is the optional companion protocol to RTP; it is not needed for RTP to work. The primary function of RTCP is to provide feedback on the quality of the data distribution being accomplished by RTP. This function is an integral part of the RTP's role as a transport protocol and is related to the flow and congestion control functions of the network. Although the feedback reports

from RTCP do not tell you where problems are occurring (only that they are), they can be used as a tool to locate problems. With the information generated from different media gateways in the network, RTCP feedback reports enable you to evaluate where network performance might be degrading.

RTCP enables you to monitor the quality of a call session by tracking packet loss, latency (delay), jitter, and other key VoIP concerns. This information is provided on a periodic basis to both ends and is processed per call by the media gateways.

Some gateway devices might not employ RTCP because the facility to report such information is not applicable to the end user. For example, a single residential user (with an analog phone) might not have access to the gateway providing the service. Also, the media gateway vendor can use a more scalable approach of tracking call quality statistics. In this case, the storage, transport and presentation of statistical info are device dependent.

If using RTCP (or a vendor specific implementations) in the network, take into account bandwidth calculations for the protocol. You need to limit the control traffic of RTCP to a small and known fraction of the session bandwidth. It should be small so as not to impair the ability of the transport protocol to carry data. Investigate the amount of bandwidth needed so that you can include the control traffic in the bandwidth specification. RFC specifications recommend that the fraction of the session bandwidth allocated to RTCP be fixed at five percent of RTP traffic.

2.6.Background of the CSMA/CD Protocol

The CSMA/CD protocol functions somewhat like a dinner party in a dark room. Everyone around the table must listen for a period of quiet before speaking (Carrier Sense). Once a space occurs everyone has an equal chance to say something (Multiple Accesses). If two people start talking at the same instant they detect that fact, and quit speaking (Collision Detection).

To translate this into Ethernet terms, each interface must wait until there is no signal on the channel, and then it can begin transmitting. If some other interface is transmitting there will be a signal on the channel, which is called carrier. All other interfaces must

wait until carrier ceases before trying to transmit, and this process is called Carrier Sense.

All Ethernet interfaces are equal in their ability to send frames onto the network. No one gets a higher priority than anyone else, and democracy reigns. This is what is meant by Multiple Access. Since signals take a finite time to travel from one end of an Ethernet system to the other, the first bits of a transmitted frame do not reach all parts of the network simultaneously. Therefore, it's possible for two interfaces to sense that the network is idle and to start transmitting their frames simultaneously. When this happens, the Ethernet system has a way to sense the "collision" of signals and to stop the transmission and resend the frames. This is called Collision Detect.

The CSMA/CD protocol is designed to provide fair access to the shared channel so that all stations get a chance to use the network. After every packet transmission all stations use the CSMA/CD protocol to determine which station gets to use the Ethernet channel next.

2.7.Background of CSMA/CA

The basic access mechanism, called the Distributed Coordination Function, is a Carrier Sense Multiple Access (CSMA) algorithm, but with a Collision Avoidance mechanism. In this protocol, both physical channel sensing and virtual channel sensing are used. Two methods of operations are supported by CSMA/CA:

1). Each unit senses the medium before it starts to transmit. If the medium is free for several microseconds, the unit can transmit for a limited time. It does not sense the channel while transmitting, but emits its entire frame, which may be destroyed at the receiver due to interference there. If the medium is busy, the unit will back off for a random time before it senses again. Since transmitting unit competes for airtime, the protocol should ensure equal access of the stations.

Carrier Sense Multiple Access (CSMA) Collision Detection (CD) Mechanisms are effective on a wired LAN, but they cannot be used on a wireless LAN environment for two main reasons:

- Implementing a Collision Detection mechanism would require the implementation of a full-duplex radio capable of transmitting and receiving at the same time, an approach that would increase the price significantly.
- In a wireless environment we cannot assume that all stations can hear each other (a basic assumption of the CD scheme). In the wireless LAN, if a station senses the medium is free, it does not necessarily mean that the medium is free throughout the entire cell.

In order to overcome these problems, IEEE Standard 802.11 implemented a Collision Avoidance (CA) mechanism through a Positive Acknowledge Scheme.

2). This scheme defines a Virtual Carrier Sense (VCS) mechanism that reduces the probability of two stations colliding, because: Is based on MACAW and uses virtual channel sensing, as illustrated in Figure 2.7.

A wants to send to *B*. *C* is station within range of *A* (and possible within range of *B*, (but that does not matter). *D* is a station within range of *B* but not within range of *A*. Protocol starts when *A* decides it wants to send data to *B*. It begins by sending an RTS frame to *B* to request permission to send it a frame. When *B* receives this request, it may decide to grant permission, in which case it sends a CTS frame back. Upon receipt of the CTS, *A* now sends its frame and starts an ACK timer. Upon correct receipt of the data frame, *B* responds with an ACK frame, terminating the exchange. If *A*'s ACK timer expires before the ACK gets back to it, the whole protocol is run again.

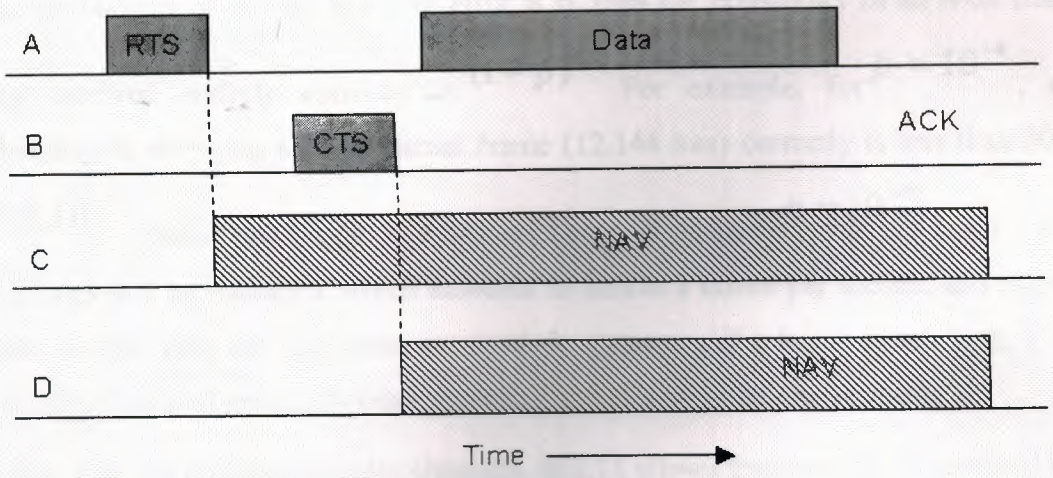

Figure 2.7: The use of Virtual Channel Sensing using CSMA/CA.

Now let us consider this exchange from the viewpoints of *C* and *D*. *C* is within range of *A*, so it may receive the RTS frame. If it does, it realizes that someone is going to send data soon, so for the good of all it desists from transmitting anything until the exchange is completed. From the provided in the RTS request, it can estimate how long the sequence will take, including the final ACK, so it asserts a kind of virtual channel busy for itself, indicated by NAV (Network Allocation Vector), Figure 2.6. *D* does not hear the RTS, but it does hear the CTS, so it also asserts the NAV signal for itself. Note that the NAV signals are not transmitted; they are just internal reminders to keep quiet for a certain period of time.

In contrast to wired networks, wireless networks are noisy and unreliable, in no small part due to microwave ovens. As a consequence, the probability of a frame making it through successfully decreases with frame length.

If the probability of any bit being in error is p, then the probability of an n-bit frame being received entirely correctly is. $(1-p)^n$ For example, for $p = 10^{-4}$, the probability of receiving a full Ethernet frame (12,144 bits) correctly is less than 30%, if $p = 10^{-5}$, about one frame in 9 will be damaged. Even if $p = 10^{-6}$, over 1% of the frames will be damaged, which amounts to almost a dozen per second, and more if frames shorter than the maximum are used. In summary, if a frame is too long, it has very little chance of getting through undamaged and have to be retransmitted.

To deal with the problem of noisy channels, 802.11 allows frames to be fragmented into smaller pieces, each with its own checksum. The fragments are individually numbered and acknowledged using a stop-and-wait protocol (i.e. the sender may not transmit fragment *k+1* until it has received the acknowledgment for fragment *k*). Once the channel has been acquired using RTS and CTS, multiple fragments can be sent in a row, as shown in Figure 2.8. Sequence of fragments is called a fragment burst.

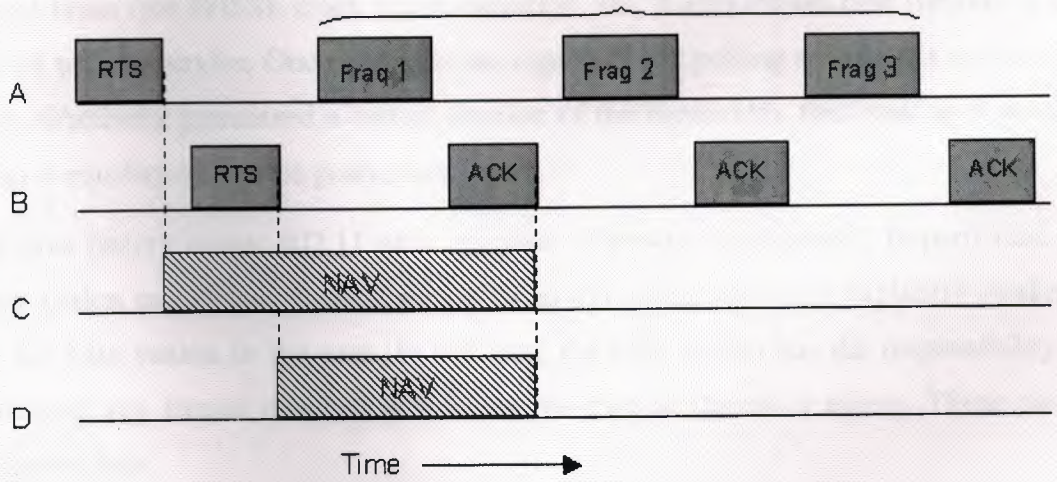

Figure 2.8: A Fragment burst.

Fragmentation increases the throughput by restricting retransmissions to the bad fragments rather than the entire frame. The fragment size is not fixed by the standard but is a parameter of each cell and can be adjusted by the base station.

The NAV mechanism keeps other stations quiet only until the next acknowledgment, but another mechanism is used to allow a whole fragment burst to be sent without interference.

All of the above discussion applies to the 802.11 DCF mode. In this mode, there is no central control, and stations compete for air time, just as they do with Ethernet.

The other allowed mode is PCF (Point Coordination Function), in which the base station polls the other stations, asking them if they have any frames to send. Since transmission order is completely controlled by the base station in PCF mode, no collision over occur.

The standard prescribes the mechanism for polling, but not the polling frequency, polling order, or whether all stations need to get equal service. The base mechanism is for the base station to broadcast a beacon frame periodically (10 to 100 times per second). The beacon frame contains system parameters, such as hopping sequences and dwell times (for FHSS), clock synchronization, etc. It also invites new stations to sign up for polling service. Once a station has signed up for polling service at a certain rate, it is effectively guaranteed a certain fraction of the bandwidth, thus making it possible to give equality-of-service guarantees.

To save battery power 802.11 pays attention of power management. In particular, the base station can direct a mobile station to go into sleep state until explicitly awakened by the base station or the user. In this time the base station has the responsibility for buffering any frames directed at it while the mobile station is asleep. These can be collected later.

PCF and DCF can coexist within one cell. At first it might seem impossible to have central control and distributed control operating at the same time, but 802.11 provides a way to achieve this goal. It works by carefully defined the interframe time interval. After a frame has been sent, a certain amount of dead time is required before any station may send a frame. Four different intervals are defined, each for a specific purpose, see Figure 2.9.

The shortest interval is SIFS (Short Interframe Spacing). It is used to allow the parties in a single dialog the chance to go first. This includes letting the receiver send a CTS to respond to an RTS, letting the receiver send an ACK for a fragment or full data frame, and letting the sender of a fragment burst transmit the next fragment without having to send RTS again. There is always exactly one station that is entitled to respond after a SIFS interval. If it fails to make use of its chance and a time PIFS (PCF Inter Frame Spacing) elapses (passes), the base station may send a beacon frame or poll frame. This mechanism allows a station sending a data frame or fragment sequence to finish its frame without anyone else getting in the way, but gives the base station a chance to seize the channel when the previous sender is done without having to compete with impatient users.

If the base station has nothing to say and a time DIFS (DCF Inter Frame Spacing) elapses, any station may attempt to acquire the channel to send a new frame. The usual contention rules apply, and binary exponential backoff may be needed if a collusion occurs.

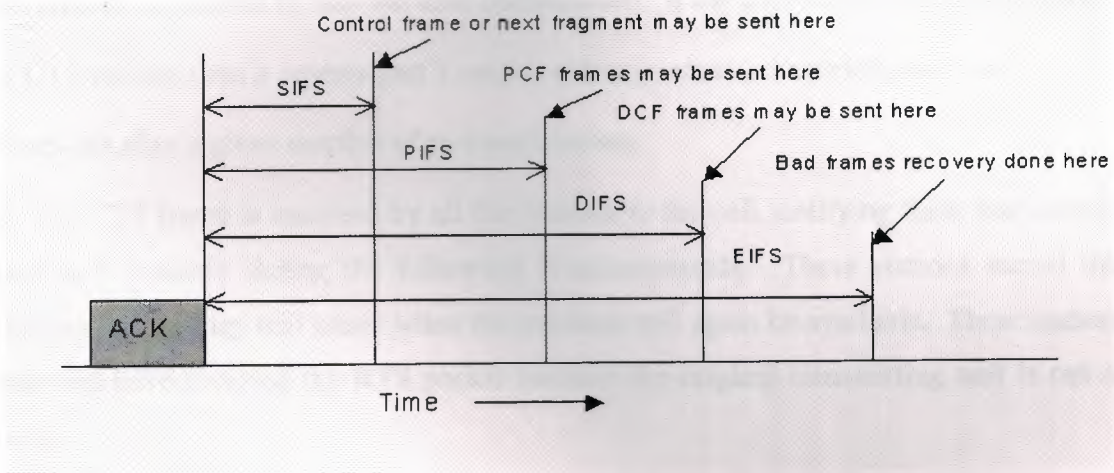

Figure 2.9: Interframe spacing for 802.11.

The last time interval, EIFS (Extended Interframe Spacing), is used only by a station that has just received a bad or unknown frame to report the bad frame. The idea of giving this event the lowest priority is that since the receiver may have no idea of what is going on, it should wait a substantial time to avoid interfering an ongoing dialog between two stations.

Full process of signal transmitting finally could be expressed by following steps:

1. A station that wants to transmit will first check to see if another station has reserved medium. If not, the station senses the medium for a specified time called the Distributed Inter Frame Space or DIFS for other stations requesting the medium. If no other station transmits, then the station will transmit a short RTS (Required To Send) packet. This packet includes the source address, destination address, and duration of the following transmission. The duration is the total transmission time for all further packets that will be transmitted (CTS, data, and acknowledgment) plus inter-frame spaces.

2. The Access Point responds (if the medium is free) with a response control packet called Clear To Send (CTS), which includes the same duration information. Receipt of the CTS packet indicates to the transmitter that no collision occurred, and permission is granted to start the data transmission. If the transmitter does not receive a CTS packet, then it repeats part 1 until it either receives acknowledgment or times out after a given number of re-transmissions.

3. The CTS frame is received by all the stations in the cell, notifying them that another unit will transmit during the following X microseconds. These stations record this information so they will know when the medium will again be available. These stations may not have received the RTS packet because the original transmitting unit is out of range.

4. The transmitting station sends its data frame to the access point. After the data frame is transmitted, the access point checks the CRC of the packet and, if correct, returns an Acknowledge (ACK) packet to confirm successful transmission.

5. If the final destination is another station on the WLAN, the access point then reserves the medium with a CTS packet. It proceeds to retransmit the data frame. The destination station checks the CRC of the packet and, if correct, returns an ACK to the access point.

The transmitting station repeats this process for every packet transmitted. If the Access Point is the originating station for the packet, only step 5 above is needed. The access

point reserves the medium by transmitting a CTS packet if it senses the medium is free, and transmits its packet.

The duration information in the CTS packet protects the data transmission from collisions. Because the RTS and CTS are very short packets, this mechanism also reduces the overhead of collisions, since these are recognized faster than if the whole packet was to be transmitted.

If the data packet is very short, the RTS packet may include all the data to be transmitted. On a collision, the overhead will not be significantly higher than with a short RTS packet. If the RTS contains data, the CTS packet contains a duration of zero, and simply functions as an acknowledgement to the transmitter that the RTS packet with data was received.

Typical WLAN protocols use packets several hundred bytes long (up to 1518 bytes). These packets are much smaller than Ethernet packets. It is preferable to use smaller packets in a wireless environment for several reasons:

- Due to the higher Bit Error Rate of a radio link, the probability of a packet getting corrupted increases with the packet size.
- In the case of packet corruption (due to collision or noise), a smaller the packet requires less overhead if it is necessary to re-transmit.

Using FHSS, the medium access is interrupted periodically for hopping (dwell times are 32, 64 and 128 milliseconds). If the packet is smaller, its transmission is less likely to be postponed until after the dwell time.

2.8. Background of (UDP): User Datagram Protocol

2.8.1 What is UDP

UDP stands for User Datagram Protocol and is mostly used for broadcasting data over the Internet. Like TCP, UDP runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services and methods. Instead, it offers a way to directly connect to send and receive datagram's over an IP network. UDP is said to be connectionless because there is no use of any kind of "handshaking" method on server or client side. It's always a direct connection. Since TCP/IP is the widely used standard for internet applications a lot of people tend to look down on UDP because of its differences and faults. The good thing about UDP however is that it's straight forward and isn't too complex.

2.8.2 How UDP is used

There are many programs and services that people use that use UDP.I am going to list a few of these services and programs:

- Video Conferencing systems.
- NetBIOS Datagram Service. (Port 138)
- Microsoft Common Internet File System. (Port 445)
- Multiplayer Online Games (Quake 3, UT Series)
- Streaming Multimedia
- Computer Phones.

2.8.3 Bad things about UDP

UDP do little error checking, so if a packet is lost or corrupted it is lost forever

Not 100% Guaranteed to send all dataThe receipt of a burst of multiple datagram's. The packet information could have been tampered with.

All these bad things about UDP may make the protocol seem very unappealing but UDP can be useful in some situations, and it enjoys one key advantage over TCP: speed. The reliability features built into TCP can be expensive in terms of execution time. Also note that UDP does not preclude reliable message delivery, it merely defers those details to a higher level of the network stack.

2.8.4 Good things about UDP

- Speed.
- There's no real connection establishment. UDP is simply just underlying.
- Unregulated send rate. The sending rate can go to its full potential.

2.8.5 Security Issues

When it comes to UDP and security it all depends on the UDP service that is running on a port and how secure the service is. The service could be vulnerable to hacking if the service has an exploit or a bug in it that allows remote access, overflow, etc. Another aspect of UDP security is the fact that it's underlying, this meaning that there aren't too many user applications that run it so a user wouldn't know that their actually running for example Microsoft Common Internet File System on Port 445 where as in TCP, you could check to see if your running a NetBIOS Session and disable it or see if you have a trojan.

2.9 Summary

As we discussed the details of the protocols in this chapter the outline of these protocols is as follows:

- **TCP/IP** is made up of two acronyms, TCP, for Transmission Control Protocol, and IP, for Internet Protocol. TCP handles packet flow between systems and IP handles the routing of packets.

- **H.323** is the globally accepted standard for audio/video/data communication. It specifically describes how multimedia communications occur between user terminals, network equipment, and assorted services on Local and Wide Area Internet Protocol (IP) networks.

- **IEEE 802.11** specifies a 2.4 GHz operating frequency with data rates of 1 and 2 Mbps using either Direct Sequence Spread Spectrum (DSSS) or Frequency Hopping Spread Spectrum (FHSS).

- **RTP** Real-time transport protocol is an IP-based protocol providing support for the transport of real-time data such as video and audio streams.

- **CSMA/CD** functions as CSMA/CD functions as each interface must wait until there is no signal on the channel, and then it can begin transmitting. If some other interface is transmitting there will be a signal on the channel, which is called carrier. All other interfaces must wait until carrier ceases before trying to transmit, and this process is called Carrier Sense.

- **CSMA/CA** in Carrier Sense Multiple Access with Collision Avoidance. The idea is to prevent collisions at the moment they are most likely to occur.

- **UDP** stands for User Datagram Protocol and is mostly used for broadcasting data over the Internet.

CAPTER THREE

VOIP APPLICATIONS SOFTWARE

3.1 Overview.

It is clear that Public Network Operators (PNOs) are faced with a telecommunications environment which is in a phase of transition. More and more customers have access to the Internet and are being provided with new Internet-based services. These services, developed by Internet service providers, are usually multimedia and interactive in nature. The ability to merge the ubiquitous telephony service and the user friendliness of Internet is recognized as a big opportunity for creating a new class of services characterized by a mix of Internet and Telecom functionalities. The ability to offer these new services will be made possible by the development of new software.
Softwares which provide an open, standard way of provisioning services in both the traditional Telco network and the Internet.

3.2 Microsoft Netmeeting SDK

3.2.1Product description

The Microsoft NetMeeting 2.1 Software Developers Kit (SDK) provides application programming interfaces (APIs) that enable authors and developers to integrate conferencing capabilities into other applications using C, C++, or Visual Basic.

The key features of the NetMeeting 2.1 SDK include:

1-A Component Object Model (COM) interface that enables developers to add NetMeeting functionality to their applications, manage calls, replace the NetMeeting User Interface, and write applications that work within a NetMeeting conference.

2-A complete Lightweight Directory Access Protocol (LDAP) client API for accessing all the capabilities of the Internet Locator Server (ILS) directory used by NetMeeting.

3-Application developers can use the client API for NetMeeting applications or for any Application in need of the dynamic storage facilities provided by ILS servers.

4-Codec installation for enabling vendors of audio and video codecs to install their products, and for making NetMeeting leverage them in calls.

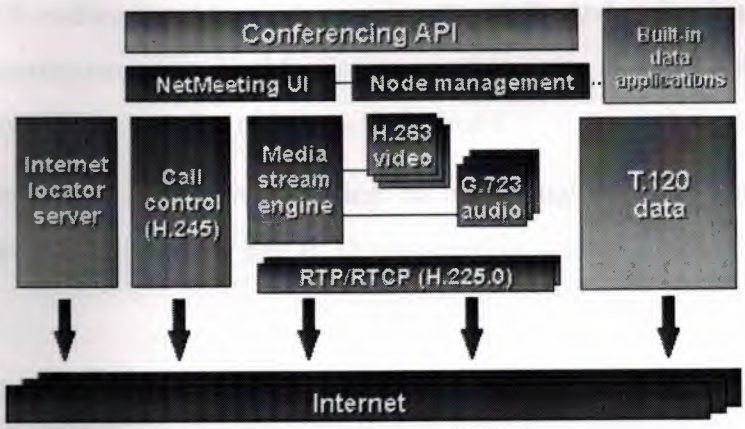

Figure 3.1: Netmeeting Architecture

The Netmeeting SDK allows using the Microsoft NetMeeting conferencing API, shown in orange in the figure above. Developers can then take advantage of the functionality provided at lower layers, including, optionally, the NetMeeting user interface.

3.2.1.1 Compliance to standards

NetMeeting features support for industry standards set by the International Telecommunications Union (ITU) and the Internet Engineering Task Force (IETF), as well as other standards organizations. Among the standards NetMeeting supports are the follwing:

1-ITU T.120:

NetMeeting contains a wealth of collaborative data capabilities, including Chat, Whiteboard, file transfer, and program sharing. The ITU T.120 standard provides the protocols for establishing and managing NetMeeting data flow, connections, and conferences.

2-ITU H.323:

NetMeeting includes audio and video codecs, as well as framing and call control protocols. H.323 codecs provide the format for the audio and video that is transmitted over various connection rates. NetMeeting supports a suite of H.323 audio and video codecs for many different modes of Internet telephony.

ITU H.323 protocols enable NetMeeting to send and receive audio and video information between NetMeeting and H.323-compatible nodes.

3-IETF LDAP:

Directory services for NetMeeting use the LDAP standard. Microsoft Internet Locator Servers (ILSs) utilize the LDAP interface to create directories of current NetMeeting users that people can call and communicate with over TCP/IP connections.

3.2.2 Functionality (related to the reference architecture)

The Netmeeting SDK provides a way to develop applications that will act as VoIP terminal in Windows 95/98/NT based computers. These applications will in fact be customizations of Microsoft Netmeeting, either via a different graphic user interface or a reutilization of its interface but configuring the features offered by it.

It can also provide the means of including audio conferencing facilities in Web pages via the use of ActiveX controls, but it requires the use of Internet Explorer as HTTP client to do so.

A shortcoming that appears in the use of Netmeeting as a VoIP terminal in a PC to phone call is that it is not possible to indicate the calling-party number in the Q.931 setup messages, a feature that could be very useful for the providing of several services

3.2.3 Network Security: Firewall Very Difficult

The H.323 call setup protocol (1720/TCP) dynamically negotiates a TCP port used by H.323 call control protocol. Also, both the audio call control protocol (1731/TCP) and H.323 call setup protocol (1720/TCP) *dynamically* negotiate *UDP* ports for use by H.323 streaming protocol (RTP). The Resource Kit example shows the MS Proxy Server configured to allow outbound connections on all UDP ports 0-65535, and allow inbound/outbound reply packets ("subsequent connections", elsewhere these are called "secondary" connections) to all UDP ports. This makes for a very unsecure firewall configuration unless MS-Proxy is smart enough to decode the H.323 dynamic port negotiation and only allow UDP traffic on ports selected by the peers and between those peers only; according to MicroSoft's NetMeeting lead technical folks, it is not.

3.3 CISCO AS5300 H323 Vocal Gateway

3.3.1 Product description

The AS5300 a member of Cisco's award winning AS5x00 family of universal access servers. The AS5300 raises the bar for performance in high-traffic, real world environments by providing the ability to terminate ISDN and 56K Analog Modem calls on the same interface.

The Cisco AS5300 delivers near line-speed performance for as many as 240 concurrent analog modem calls and ISDN B channels over a single dial-in telephone number. It incorporates high-performance, reduced instruction set computing (RISC)-based processing with high-density Modem ISDN Channel Aggregation (MICA™) technologies.

The Cisco AS5300 universal access server is intended for telecommunications carriers and other service providers, as well as large enterprises that require consistent high-density connectivity for subscribers and telecommuters connecting to the Internet and corporate intranets.

This Voice over IP feature implements high-density voice support on the Cisco AS5300 by using DSPM-549 digital signal processor (DSP) modules. When equipped with

Voice Feature Cards (VFCs) and voice-enabled Cisco IOS software, the AS5300/Voice Gateway supports carrier-class VoIP and FAX over IP services.

High-density voice support increases the voice capacity of a Cisco AS5300 up to 120 channels. This increase in voice support provides the voice density of up to four T1 lines (96 voice or FAX calls) or four E1 lines (120 voice or FAX calls).

A fully configured voice-capable Cisco AS5300 router includes two voice carrier cards, each capable of supporting 60 concurrent sessions.

3.3.1.1 Technical specifications

Operating System: CISCO IOS in different versions (IOS 12.0 in the evaluated equipment)

Processor: AS5300 Processor (RISC) 150 MHz

DSP:

Ethernet connection: 1 IEEE 802.3 10BaseT and 1 100BaseT with 1RJ45 connector each

T1/E1 Interfaces: up to 4 E1 Trunk interface R1-MFC or PRI ISDN E1 (Euro ISDN) supporting up to 120 voice channels with 4 RJ48C

COM Port 1: RS-232 interface to connect to the system console

3.3.1.2 Setup cabling and software requirements

Ehternet connections: 1 IEEE 802.3 10BaseT and 1 100BaseT with 1RJ45 connector each

System console: an ASCII terminal connected through an RS232 null modem

PSTN interface: one to four E1 facilities from a carrier provider (RJ48C connector)

Power supply: 220-240 volt AC power outlets

Additional software: Microsoft NetMeeting 2.1 (or 3.0 for Gatekeeper enabled function) for PC-to-POTS and POTS-to-PC call support

Each Voice over IP enabled AS5300 Access Server supports up to 120 concurrent calls at the same time through an E1 interface

3.3.1.3 Openness and Interoperability

It lacks a programmable API.

All the configuration is made by means of a text based user interface that allows a wide degree of possibilities.

It does not support the MGCP protocol (though intended for the future).

It is H323 v2 compliant. Its interoperability has been tested against the NetMeeting 2.1 client.

It can be configured to work with an H323 Gatekeeper.

Coders: (In tested equipment) G721 Alaw and G.721 Mlaw

Network layer protocols: H323 on top of TCP: H225, H245, RTP, RAS

3.3.2 Functionality (related to the reference architecture)

The AS5300 Network Access Server with VoIP feature (VoIP gateway) can be use to provide POTS to IP networks interconnection, as it allows:

- POTS to PC calls
- PC to POTS calls

It also allows POTS to POTS calls traversing an IP network, though this feature is less important for the scope of the services that are being defined in the P909 project. Anyway it is important to highlight that for this kind of communication, the protocol between the involved gateways is also H.323 thus making it possible to establish calls from a phone to a PC.

There are no detected interoperability problems for the POTS part (phone to gateway and vice versa) of the communication, though during the configuration problems where found in the Q.931 setup process between the equipment and the switch that were finally solved.

For the VoIP terminal part (PC to gateway) the equipment has been successfully tested with a NetMeeting 2.1 client and with the OpenH323 Voxilla Client for Windows 95. It has been unsuccessfully tested with the IBM java client and the Intel Internet VideoPhone due to problems with the call setup.

It can also work with a gatekeeper using the RAS protocol. It has been successfully tested working with the OpenH323 gatekeeper.

It lacks an API thus limiting the possibilities of its use, but anyway it is possible to use it for services in which voice communications from the POTS world to the PC world are needed. Using it in conjunction with a gatekeeper multiplies the possibilities of configuration.

3.4 OpenH323 Protocol Stack

3.4.1 Description of the product

OpenH323 is a project committed to the collaborative development of an Open Source H.323 protocol stack that is available for use by both private and commercial users. It was started in September 1998 by Equivalence Pty Ltd, a private company based in Australia.

It provides an H323 protocol stack in source code (C++). It has the H225, H235 and H245 protocols implementations.

It is provided in source code and has been tested for Windows and Linux platforms. It has also been compiled for Solaris.

The audio codecs that are bundled with the code are G.711 and GSM, so that they are not covered by patent restrictions.

A test program (voxilla) that interoperates with Netmeeting versions 2 and 3 is provided

Currently the version is coded 0.8alpha1.

3.4.1.1 Technical specifications

Programming language: C++

Operating systems: Linux, Windows 95/98/NT, Solaris

API: Source code provided, The class definition has been designed to use specialisation to treat common protocol needs.

Documentation: No good documentation is provided

3.4.1.2 Compliance to standards

H323: H225/H235/H245

Codecs: G.711/GSM

3.4.2Functionality (related to the architecture)

It provides the H323 protocol stack. It can be used for the call control H.323 wrapper to control H323 endpoints (either gateways, MCUs or terminals).

It provides also the RAS stack, so that it can also be used to build a gatekeeper.

3.5 OpenH323 Gatekeeper

3.5.1 Description of the Product

It is a gatekeeper based on the OpenH323 H323 protocol stack. It is a RAS compliant and allows registration of endpoints and bandwidth control.

3.5.1.1 Technical specifications

Programming language: C++

Operating systems: Linux, Windows 95/98/NT, Solaris

API: Source code provided, The class definition has been designed to use specialisation to treat common protocol needs.

Documentation: No good documentation is provided

3.5.1.2 Compliance to standards

H323: RAS

LDAP

SNMP management is being added

3.5.2 Functionality (related to the architecture)

It is another element involved in VoIP communications that can be controlled from the reference architecture (specially from the call control component).

It can also work together with the Call Control to provide a finer grain control of the communications (address translation and bandwidth control).

In the status it has right now it is only useful for testing purposes, as it doesn't really have a powerful user registry or QoS control.

Anyway it can be useful for address translation and channel control.

3.6 Advantages of VOIP

Cost savings in long distance telephone calls is a great advantage of a VOIP system. Since an organization is already paying Wide Area Network circuits for data usage, the same circuits can be used to transfer voice packets instead of having to use a telephone company's long distance lines.

VOIP systems are able to access data information as well as voice packets. This means that thru a small web browser, it is able to access information that is developed as web pages.

Many of the telephone features of a traditional PBX have been implemented or continue to be developed and perfected. Features such as call on hold, call waiting, multiple line sets, preprogrammed numbers, are considered to be readily available in VOIP systems.

A VOIP server is not required for each physical location. For example, an organization with 80 physical sites can operate using four VOIP servers and still service virtually thousands of handsets for that organization. A VOIP system is able to do this because it does not use traditional telephone switched technologies. Where a traditional system must establish a connection from one telephone to another, thereby limiting the number

of connections and therefore handsets it can support, a VOIP system establishes a connection, and after it determines the connection is operational, releases the connection for the next call request.

The biggest advantage to VOIP systems is it can use the flexibility that IP based systems provides. If the hardware configuration allows, VOIP systems can also send and receive visual representations of the participants of a telephone call using web cameras.

Scalability is an advantage with VOIP systems. There are available VOIP systems that can accommodate small installations requiring 20 handsets up to thousands of handsets

.

With some VoIP Plans users can talk for as long as one wants and also can talk with numbers of people at the same time without additional cost.

There are number of benefits you can gain by using VoIP:

.

At the same time, you can exchange data with people are you talking with, sending images, graphs and videos. .

More efficient business - New applications that capitalise on closer ties between voice and data can make businesses more efficient.

New ways of communication - For example, banks can use it reduce the amount of time it takes to open an account or apply for a mortgage using voice and data interaction. It can be used for CRM (customer relations

3.7 Disadvantages of VOIP

The main disadvantage that a VOIP system has is reliability and robustness. Because this system is part of a data network, it is susceptible to the imperfections inherent in a data network. This means that if computers are susceptible to hackers, and viruses, the VOIP system would also be susceptible.

Another major problem is identification of 911 calls. If a user dials 911, the emergency response team must be able to identify the location of the originator. Theoretically, if a

911 call is made, and the handset is located to a server at a different location, much less state or country, how will an emergency response team member identify the location of the call? In a traditional telephone system, the call is identified through the PSTN line that the telephone number calling from is assigned to. Generally, the PSTN is in the physical vicinity, or at least within the campus serviced by the PBX. In a VOIP system, the system is dependent on the maintenance of a database defining the location of each extension a VOIP telephone is assigned to. This requires additional labor and maintenance. In addition, since a VOIP handset is a device, just like a computer, this device can be removed from one location to another, reconnected to the network at the new location and be operational. This action would also require the notification of the internal telephone systems maintenance staff that a VOIP handset has been moved in order for them to update the database. This act of notification has often been overlooked, thereby providing an inaccurate database of handset locations.

Another disadvantage is a VOIP handset also requires low voltage power in order for it to be operational. Since there is no longer a centralized PBX providing the power, it must obtain it through enhanced switches providing power over Ethernet, or 120 volt power. In order to ensure availability during a power outage, Uninterrupted Power Supplies (UPS's) must be used to protect not only the switches but also each handset, if an enhanced switch is not available. Compared to protecting a centralized PBX with a single UPS, this distributed method of obtaining numerous UPS's is a more costly alternative.

A VOIP system shall require an initial cost to obtain. Even if a VOIP server is already available, a VOIP Telephone is generally more expensive than a cost of a traditional telephone. A "Softphone", software running on a computer allowing it to act as a telephone is $80 per user license. A VOIP Telephone Handset ranges from $150 to $700, depending on the features of the telephone

Equipment premium is not the only cost associated with a migration to voice over IP. The data network may need upgrading to carry voice with sufficient quality of service. Extra bandwidth may be needed over the wide area. And if the intention is also to migrate voice traffic from traditional phone wiring to a local area network (LAN) within the sites, existing LAN switches may need replacing as well. So the LAN, too, can retard migration to all-out VOIP - at least until it needs upgrading for other reasons.

And they have to be good reasons, for the era of regular upgrades for their own sake vanished with the bursting of the dotcom bubble

Advanced programming is required since a VOIP system shares the lines with computers and other devices connected to the network. In doing this, Quality of Service programming and packet prioritization is a requirement to ensure that telephone voice traffic reaches its destination in an orderly manner at all costs. This is because voice traffic cannot handle transmission delays. If this was to occur, a conversation would have numerous gaps and render the conversation unacceptable. This is in contrast to data, where a certain amount of delay is acceptable. For instance, if a person sends an E-mail to a destination, the sender and recipient does not necessarily require that the E-mail is received immediately after transmission. The E-mail can arrive, hours later and the communication is still acceptable. Often times, an organization does not have personnel in house to provide advanced programming to routers and switches which means expensive consulting costs would have to be paid to implement this feature.

Another major disadvantage of VOIP is the quality of the sound which can be uneven, and phone calls often have lot of delay with lot of echo. It makes conversation difficult as you find the other party constantly saying "Excuse Me"! To get lower bandwidth, the voice compression algorithms and echo cancellation requires additional processing power that makes digital phones more expensive than analog phones.

You should be aware of following disadvantages:

VoIP services only work if your computer is switched on and the program running

They only work if the other person is also at their computer and has the same program loaded and running

Quality issues - Although it is improving all the time, the quality of most VoIP services and products can't yet match that of PSTN.

. Despite these disadvantages, VoIP is still an attractive proposition for any budget-conscious manager. Furthermore, better VoIP products are addressing and solving these problems mentioned above.

You can also avoid these disadvantages by choosing the right product from the right service provider.

.

CONCLUSIONS

My project consist of three chapters: an introduction to the topics involved in voice over internet protocol, the background of VOIP transmission of voice using IP Networks, and media gateways controllers.

Background

In this chapter we discussed in detail, the background and functions of different protocols that are being examined in my project. We discussed the background and functions of the following protocols:

1-H323

2-RTP (Real Time Protocol)

3-802.11b

4-TCP/IP (Transmission Control Protocol/Internet Protocol)

5-UDP (User Datagram Protocol)

6-CSMA/CA (Carrier Sense Multiple Accesses / Collision Avoidance).

7-CSMA/CD (Carrier Sense Multiple Accesses / Collision Detection.)

VOIP Applications software

In this chapter we discussed in detail the software and functions of the following products.

1-Microsoft Netmeeting SDK.

2-CISCO AS5300 H323 Vocal Gateway.

3-OpenH323 Protocol Stack.

4-OpenH323 Gatekeeper.

And we discussed the advantages and disadvantages of VOIP

REFERENCES

1. http://www.voip-fourm.com
2. http://www.voip-info.org
3. Draft standard IEEE 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE, 1996
4. http://www.dlink.com
5. http://www.fcc.gov
6. http://www.govtech.net
7. http://www.Ethereal.com
8. http://searchnetworking.techtarget.com
9. http://www.nwfusion.com
10. http://www.cisco.com
11. http://www.voip-info.de