

STUDY OF VOICE OVER INTERNET PROTOCOL (VoIP) IN AN ENTERPRISE NETWORK THROUGH SIMULATION

NUSAIBA BINTE MAHBUB
Student Id: 012142015

A Project
in
The Department
of
Computer Science and Engineering



Presented in Partial Fulfillment of the Requirements
For the Degree of Master of Science in Computer Science and Engineering
United International University
Dhaka, Bangladesh
February 2018

©Nusaiba Binte Mahbub, 2018

APPROVAL CERTIFICATE

This project titled “**Study of Voice Over Internet Protocol (VoIP) in an Enterprise Network Through Simulation**” submitted by **NUSAIBA BINTE MAHBUB**, Student ID: **012142015**, has been accepted as Satisfactory in fulfillment of the requirement for the degree of Master of Science in Computer Science and Engineering on February, 2018.

Board of Examiners

1.

Supervisor

Mohammad Mamun Elahi

Assistant Professor

Department of Computer Science & Engineering (CSE)

United International University (UIU)

Dhaka-1209, Bangladesh

2.

Examiner

Dr. Salekul Islam

Associate Professor & Head

Department of Computer Science & Engineering (CSE)

United International University (UIU)

Dhaka-1209, Bangladesh

3.

Ex-Officio

Dr. Mohammad Nurul Huda

Professor & Coordinator – MSCSE

Department of Computer Science & Engineering (CSE)

United International University (UIU)

Dhaka-1209, Bangladesh

DECLARATION

This is to certify that the work entitled “**Study of Voice Over Internet Protocol (VoIP) in an Enterprise Network Through Simulation**” is the outcome of the research carried out by me under the supervision of Mohammad Mamun Elahi, Assistant Professor, Department of CSE.

NUSAIBA BINTE MAHBUB

ID: 012142015

Department of MSCSE

In my capacity as supervisor of the candidate’s project, I certify that the above statements are true to the best of my knowledge.

Mohammad Mamun Elahi

Assistant Professor, Department of CSE

**Dedicated to my parents
For their love and inspiration**

**And to my husband
For his extraordinary love and support
and for believing in me.**

ABSTRACT

Voice over IP (VoIP) is an alternative option to conventional circuit-switched telephony that allows human voice and video to travel over accessible packet data networks along with traditional data packets. Because of its ever evolving nature, VoIP is already considered an optimum choice for business and enterprises that want to achieve their goals and continue to in the future. As our project, we have therefore decided to study VoIP; its characteristics and features. Alongside, we have set an enterprise network using packet tracer software whereby we have implemented the VoIP system in our proposed enterprise network. This gave us a more clear idea and helped us to visualize the scenario that happens when VoIP is deployed. Through this project, we were able to have an overview of the VoIP system, its structure and components and why it is being preferred over public switched telephony.

ACKNOWLEDGEMENTS

All praises belong to Allah, the most Gracious, and most Merciful. I would like to pay my gratitude to Allah for giving me the will and strength to accomplish my final project. Very special thanks to Mohammad Mamun Elahi, who acted as my project supervisor and examiner respectively. I am indebted to him for his ideas, patience, support and guidelines to come up with this project. Throughout my project work, he has mentored me with his excellent skills and understanding on the subject matters. With no exception, a million of thanks go to my beloved husband and my family for their morals and material supports. They never give up teaching and motivating me to become who I am today indeed. I also would like to extend the appreciation to Azim Vai, for his exceptional support and giving me his precious time for helping me out. Last but not least, to all people that I forgot to mention here, who have contributed towards the completion of this project either directly or indirectly. Your kindness and cooperation in completion of this final year project paper are very much appreciated. Thank you very much in advance and May Allah bless all of you.

TABLE OF CONTENTS

ABSTRACT	V
ACKNOWLEDGEMENTS	VI
LIST OF FIGURES	IX
1. Introduction	11
1.1 Problem statement and motivation.....	11
1.2 Theoretical background.....	12
1.3 Methodology and implementation steps.....	13
1.4 Organization of the report.....	14
2. Background and Literature Review	15
2.1 VoIP system structure and components.....	15
2.2 VoIP signaling protocols.....	18
2.2.1 Session Initiation Protocol.....	19
2.2.2 Overview of SIP operation	20
2.2.3 Overview of VOIP Data Handling.....	23
2.3 VOIP Benefits/Drawbacks.....	24
2.3.1 Benefits of VoIP.....	25
2.3.2 Advantages and disadvantages of using VoIP over PSTN.....	27
2.4 Risks of VoIP.....	28
2.4.1 Protection against threats.....	29
2.5 PSTN vs. VoIP: Feature-by-feature comparison.....	30
2.6 Quality of Service (QoS) of VoIP.....	31
3. Our project: design of an enterprise network	32
3.1 VoIP setup in an enterprise network Packet Tracer scenario.....	34
3.1.1 Enterprise Network setup components.....	34

4. Configuration tasks.....	37
4.1 DHCP configuration	37
4.2 Telephony commands configuration.....	38
4.2.1 Configuration for each phone number.....	39
4.2.2 Configuration for max-d.....	39
4.2.3 Configuring Auto-assign	40
4.3 Dial-peers and destination pattern configuration.....	40
4.3.1 VoIP dial peers.....	40
4.3.2 Destination patterns.....	41
5. VoIP Routing Protocol Configuration (EIGRP), ACL and NAT and Tunneling configuration.....	42
5.1 Enhanced Interior Gateway Routing Protocol (EIGRP).....	42
5.2 Access List (ACL) configuration.....	43
5.3 Network Address Translation (NAT).....	44
5.4 Tunneling Implementation.....	46
5.4.1 Tunneling configuration: for main router.....	46
5.5 Router and Switch configuration commands.....	48
6. Results.....	49
6.1 Testing: Verifying the connectivity.....	49
6.1.1 Checking DHCP configuration for the PCs.....	49
6.2 Powering up the IP phones.....	50
6.2.1 Verifying if the IP phones are assigned with their respective phone numbers.....	50
6.3 Verifying the connectivity by calling from one IP phone to another.....	51
7. Conclusion	52
8. References.....	53

LIST OF FIGURES

Figure 1.1	How data is sent and received in VoIP
Figure 1.2	Block diagram of circuit switched network
Figure 1.3	Block diagram of packet switched network
Figure 2.1	A basic VoIP system
Figure2.2	Basic VoIP system structure consisting its components (i)
Figure2.3	Basic VoIP system structure consisting its components (ii)
Figure 2.4	H.232 Layered Architecture
Figure2.5	Session Initiation Protocol call forwarding
Figure2.6	Flowchart for the VoIP system
Figure2.7	State Diagram for the Simulation of the Cisco IP phone calling process
Figure 2.7.1	How VoIP works (basic system)
Figure2.8	PSTN vs. VoIP: Feature-by-feature comparison
Figure 3.1	Basic schematic diagram of enterprise network scenario
Figure 3.2	Cisco Packet Tracer sample network scenario
Figure3.2.1	Enterprise network diagram
Figure 3.3	Dhaka branch network diagram
Figure3.4	Dhaka-Chittagong Branch network diagram
Figure3.5	Connection of Main router to the other routers
Figure 4.1	DHCP configuration commands for packet tracer
Figure4.2	max-dn and Ephone-dn configuration command for packet tracer
Figure4.3	Ephone configuration command for packet tracer
Figure4.4	Ephone connectivity diagram
Figure 4.5	VoIP dial-peer configuration diagram
Figure5.1	EIGRP Topology
Figure 5.2	EIGRP configuration example with the aid of network diagram
Figure 5.3	Virtual Private Network(VPN)
Figure 5.4	Tunneling done between main router and remote location router
Figure 6.1	DHCP connectivity for PC
Figure 6.2	DHCP connectivity for PC
Figure 6.3	Powering the IP phone
Figure 6.4	Obtaining IP phone numbers
Figure 6.5	Calling from one IP phone to another
Figure 6.6	Ping from one PC to another

CHAPTER 1

INTRODUCTION

1.1 Problem statement and motivation

Introduction to VoIP

Voice over internet protocol- commonly known as VoIP, is a communication technology by which voice conversation is transmitted over the internet or any other IP based networks using packet switching mechanism. VoIP technology uses IP-based networks to establish and manage communication sessions between end devices [1].

Why VOIP deploys packet switching

Circuit switching is not the most preferred mechanism that is chosen by data networks. That is because the speed of the internet connection would decrease by a great amount if it had to maintain a continuous connection to the web page that is being viewed at any given time. So as an alternative, data networks simply send and recover data as needed. Also, instead of choosing to route the data over a dedicated channel, the packets of data flow through a hectic network that consists of various possible routes.

In that case, contrary to circuit switching, packet switching mechanism is quite proficient. It allows the course of packets through the least crowded and inexpensive lines and liberates the two computers communicating with each other so that they are free to accept information from other computers too.

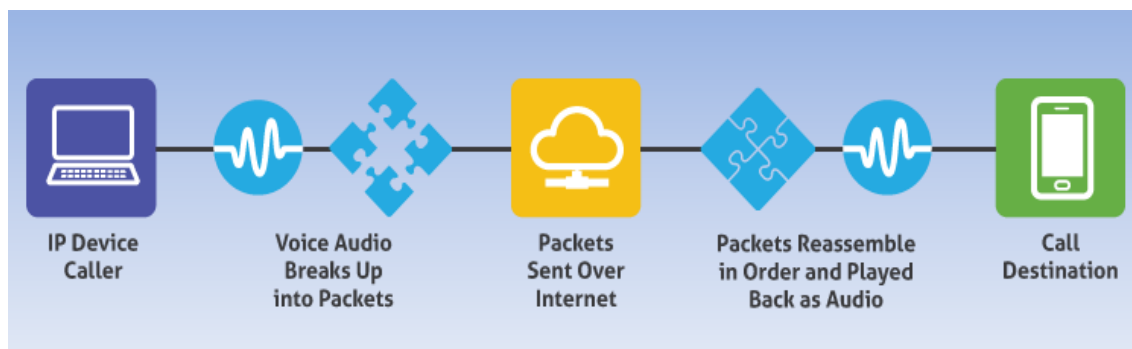


Figure 1.1: How data is sent and received in VoIP

In the past, Circuit switching process was the most widely used to build communications network. It was used for ordinary telephone calls and allowed the sharing of communication equipment and circuits among users. The connection was established first between source and destination and after transfer of information, it was terminated.

Public switched telephone networks (PSTN) which is a traditional phone network system, used circuit switching mechanism for voice transmissions. Basically in circuit switching, resources are reserved along the entire communication channel for the duration of the call, whereas in packet switching, information is digitally transmitted into one or more packets.

Packets know their destination, and may arrive there via different paths. With VoIP, as it deploys packet switching mechanism, instead of leaving an entire circuit opens while conversations take place, it breaks the conversation into small packets of data and then transmits it over the internet. Overall, this project will help us identify the main issues and problems that has to be dealt with when a VoIP system is to be implement for a particular scenario.

1.2 Theoretical background

Circuit switching

Circuit switching consists of three phases which are i) connection establishment ii) data transfer iii) connection released. To sum it up, in circuit switching the source provides the entire path address for each data. Thereby resource is reserved and there is more wastage of resources. Delay between data in circuit switching is uniform. However circuit switching is more reliable.

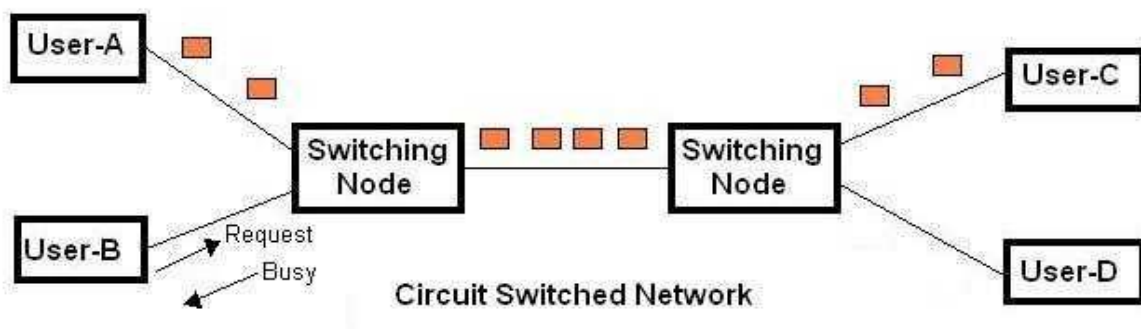


Figure 1.2: Block diagram of circuit switched network

Packet switching

In packet switching, contrary to circuit switching each data knows the final destination address and the intermediate path is decided by the routers. Data is processed at all intermediate nodes and also at the source. Unlike circuit switching delay of data is not constant. Resources are not reserved because users share bandwidth. It is less reliable than circuit switching.

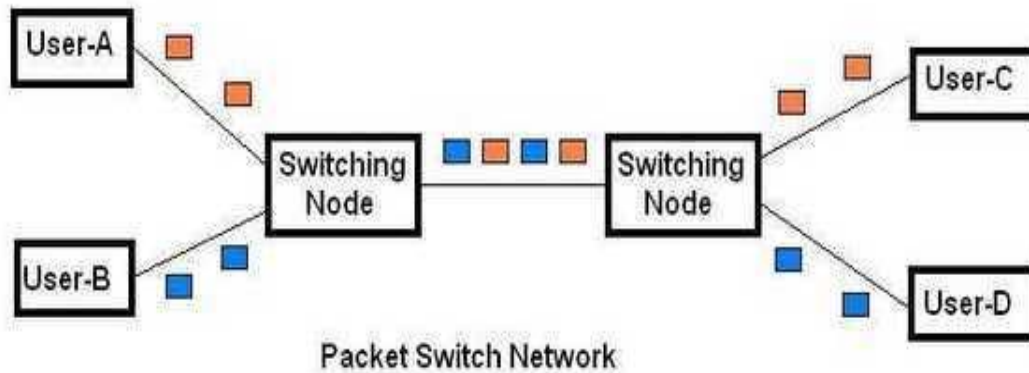


Figure1.3: Block diagram of packet switched network

Packet switching steps:

- i. At first the data is divided into packet/s. The first step in packet switching process is to break the data into blocks with a size of few hundred bytes.
- ii. Then each packet is attached with a header that has a “from” address, “to” address and “payload”. Packets are given a destination IP address and forwarded to the router that is closer to the destination.
- iii. If data requires multiple packets, then the order of each packet is noted.
- iv. After that Packets sent onto the network, they move from router to router taking different paths which are set by the router. Each packet's journey time can therefore vary.
- v. Once packets arrive they are re-ordered and reassembled into readable data.
- vi. Then Message sent from recipient to sender indicating that the message has been received.
- vii. If there is no confirmation message, data is re-transmitted by the sender.
- viii. If one of the routers in the route fails, then packets are automatically routed again so that they can avoid that device and reach destination via other path.

1.3 Methodology and Implementation steps

Determining methodology of the project is one of the crucial part of the project. In order to carry out the objective of the project, it is very important to figure out the correct and feasible method of procedures that is required in order to do so. The methodology that we developed to implement a VoIP system in an enterprise network consists of these steps:

- i. First study and analyze various VoIP network implementatins
- ii. Then design a sample scenario of a network consisting of two branches at two different locations
- iii. Enriching the network by adding data centre, remote locations etc
- iv. Build the network in packet tracer software

- v. Test run the connectivity of the network

After the correct methodology is established, the project is implemented. Implementation includes:

- i. Configuring codes on routers and switches
- ii. Implementing IP phones and Configuring telephony commands
- iii. Establishing a virtual tunnel in the network
- iv. Assigning telephone numbers to IP phones so that calls can be made from one network location to another.

1.4 Organization of the report

Chapter 1 is basically about introducing VoIP and brief outlook into circuit switching and packet switching mechanisms and why VoIP is deployed with packet switching. The rest of the project is organized as follows—

Chapter 2 provides an overview of the VoIP system structure, signaling protocols, overview of data handling. It also presents the benefits and drawbacks of VoIP system and the risks involved, how to take security measures against threats and Quality of Service parameters of VoIP.

Chapter 3 deals with designing of our enterprise network in packet tracer and VoIP setup.

Chapter 4 contains the implementation of VoIP phones and configuring telephony commands and DHCP protocols.

Chapter 5 deals with the configuration of access lists (ACL), NAT , EIGRP and tunneling implementation.

In chapter 6, we power up the IP phones and check the connectivity by calling from one location to another.

Chapter 7 discusses the reasons why VoIP is preferred by businesses nowadays and its bright prospective in the future.

CHAPTER 2

BACKGROUND AND LITERATURE REVIEW

2.1 Introduction to VOIP system structure and components

A Basic VoIP System

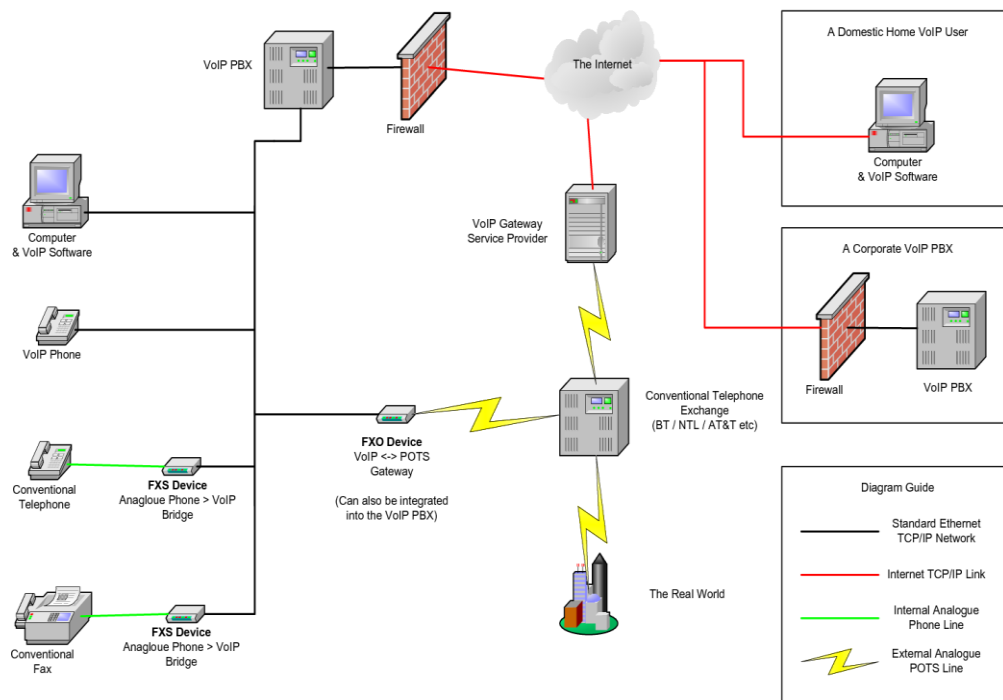


Figure 2.1: A basic VoIP system

VoIP Components

The four most important VoIP components in a basic VoIP system are:

- i. Signaling Gateway Controller
- ii. Media Gateway
- iii. Media Server
- iv. Application Server

In addition to this there are:

- i. **IP phone** – In order to send and receive voice calls, IP phones use a type of network connection known as Ethernet network connection.
- ii. **Gateway** – A gateway is able to promote calls which take place between various networks.
- iii. **Call agent** –part of the former characteristics of PBX have now been replaced by Call Agents e.g CUCME
- iv. **Application server** –in a VoIP environment, Application Servers provide the top services such as voice mail
- v. **Gatekeeper** -The bandwidth in WAN network is usually not widely available and so, a gatekeeper can keep an eye on the amount of bandwidth which is accessible.
- vi. **Voice-enabled switch** –It is a Cisco mechanism switch with voice feature and can be powered to a connected Cisco IP phone.
- vii. **Multipoint Control Unit (MCU):** participants in multiple locations can attend the same videoconference or meeting through MCU
- viii. **Videoconference station:** A videoconference station provides access for end-user participation in videoconferencing. The videoconference station contains a video capture device and a microphone for video/audio input.

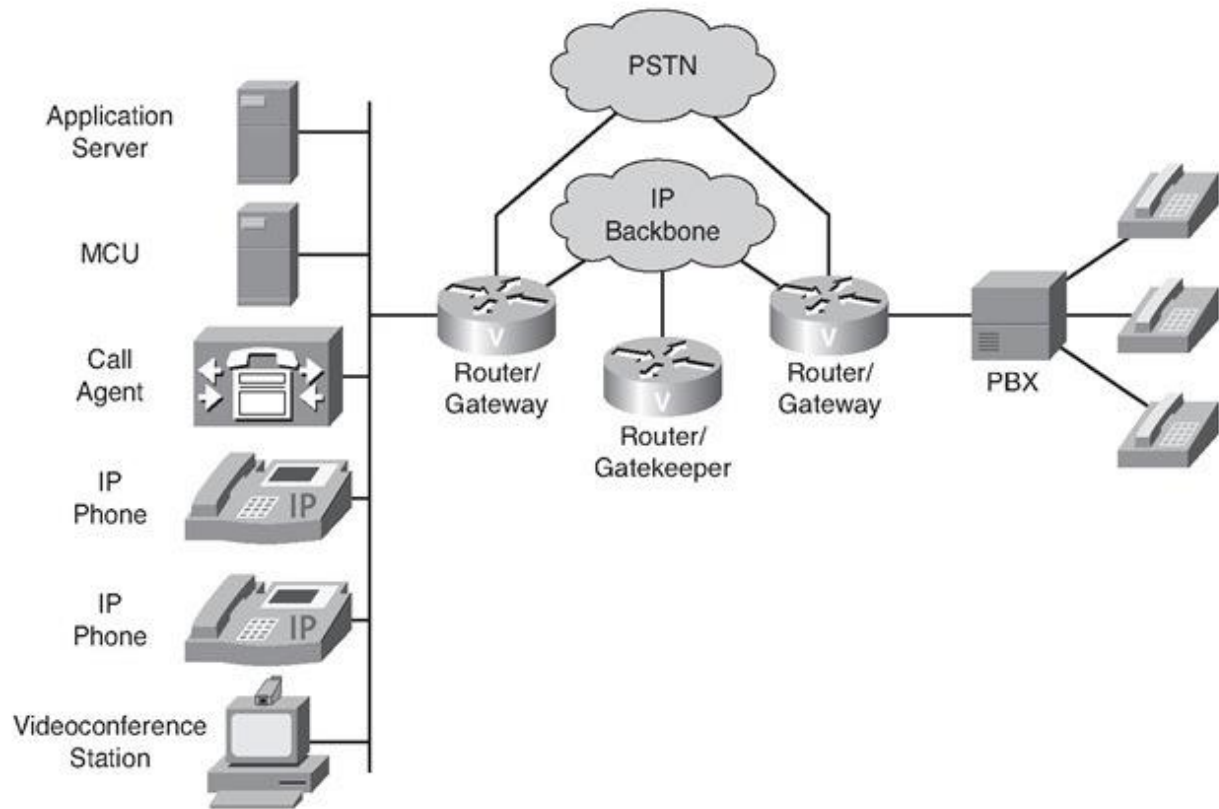


Figure 2.2: Basic VoIP system structure consisting its components (i)

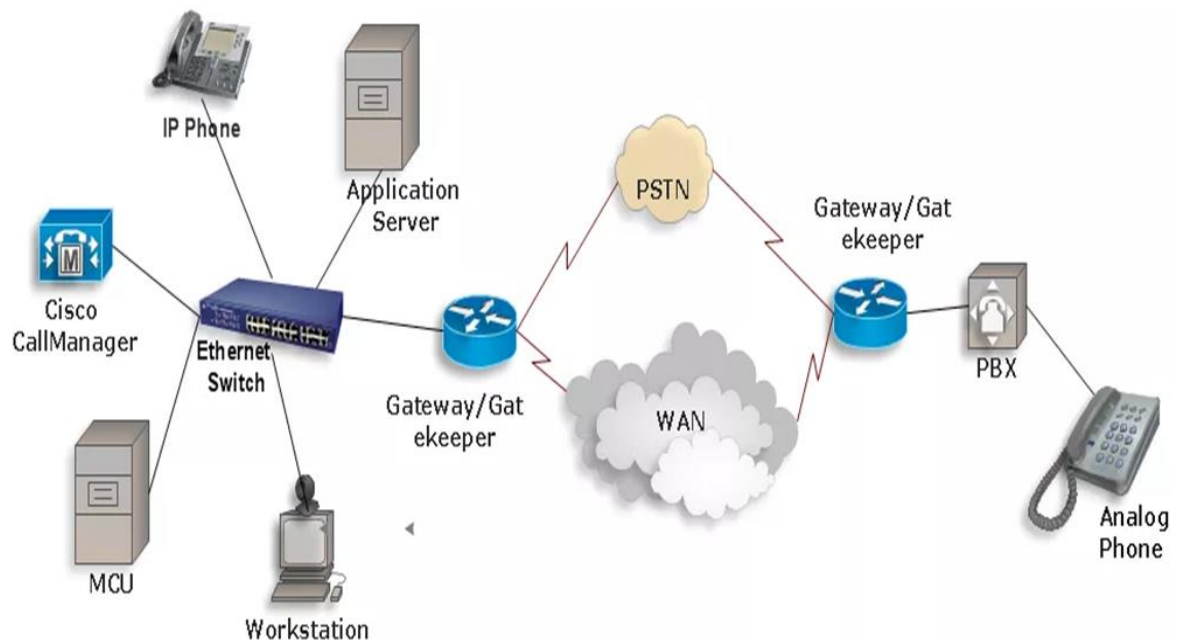


Figure 2.3: Basic VoIP system structure consisting its components (ii)

2.2 VoIP Signaling Protocols

In VoIP networks, voice and signaling are multiplexed and travel as normal data inside LANs, WANs or the Internet. Signaling protocols are required in packet networks for transport and control. The VoIP infrastructure is designed to initially support simultaneous users and is capable of scaling. This pattern assumes the availability of multiple Internet Service Provider (ISP) partners to provide edge termination for diverse users [4].

In order to provide VOIP communication services, a number of protocols are to be employed. In this section, we will concentrate on the majority of protocols that are already deployed or being deployed today.

Virtually every device in the world uses a standard called Real-Time Protocol (RTP) for transmitting audio and video packets between communicating computers. RTP is defined by the Internet Engineering Task Force (IETF).

The H.323 Protocol and Session Initiation Protocol (SIP) have their roots in 1995 as scientists hoped to take care of the issue of how two PCs can start correspondence keeping in mind the end goal to trade sound and video media streams.

Today, H.323 still charges most of the VoIP arrangements in the service provider market for voice travel especially to transport voice calls all around. H.323 is also comprehensively used as a piece of room-based video conferencing structures and is the essential tradition for IP-based video systems. SIP has, in recent times, ended up being all the more notable for use in messaging systems.

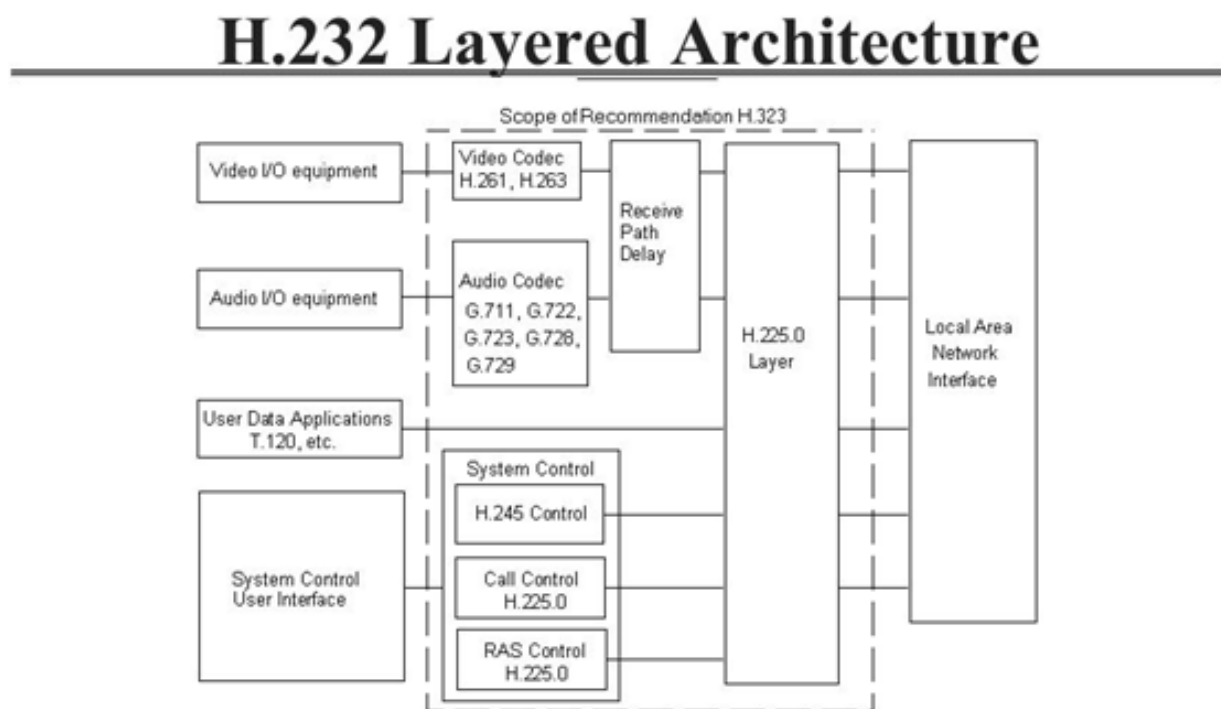


Figure 2.4: H.323 Layered Architecture

2.2.1 Session Initiation Protocol

The Session Initiation Protocol (SIP) is an application-layer signal control protocol used to build up, keep up, and end sight and sound sessions. Mixed media sessions incorporate VOIP, meetings and other comparable applications including such media as sound, video and information.

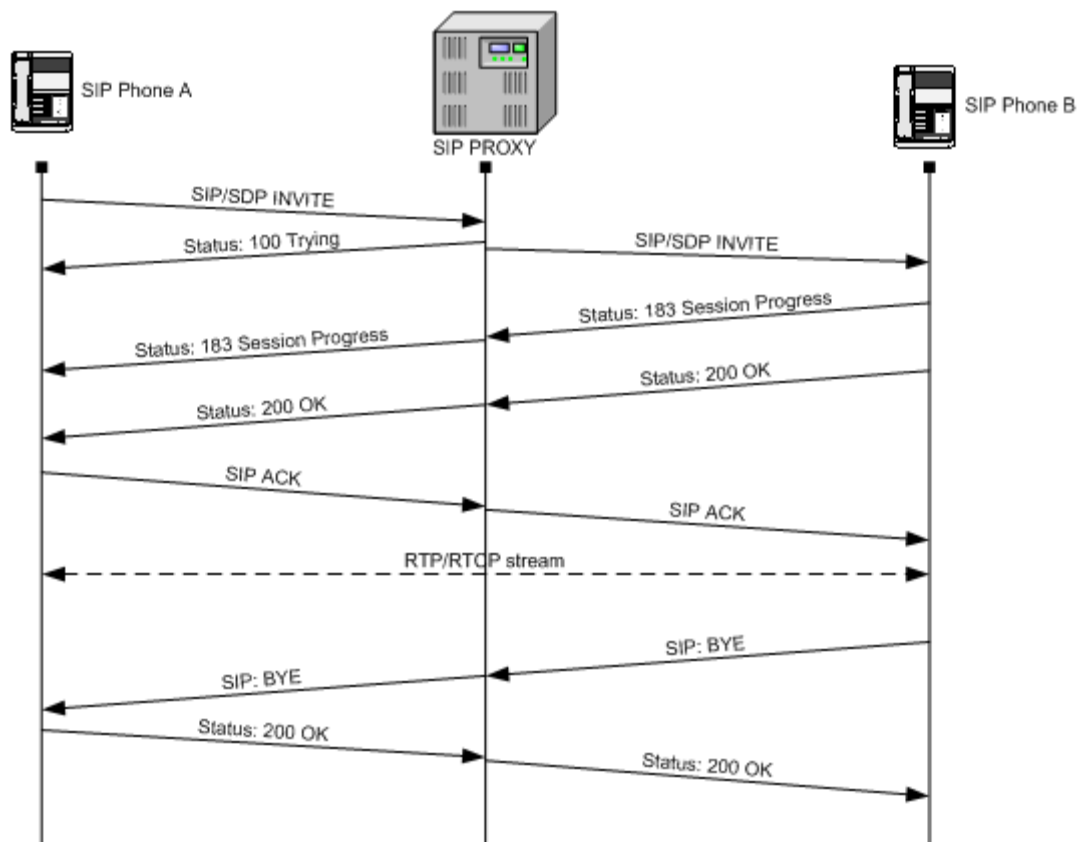


Figure 2.5: Session Initiation Protocol call forwarding

2.2.2 Overview of SIP operations

SIP addresses identify callers. When initiating a SIP to call, a guest first needs to find the suitable server and send it a demand. The guest can either specifically come to the callee or in a roundabout way through the divert servers. The Call ID field in the SIP message header uniquely identifies the calls. Below is the brief explanation of how the protocol performs its operations.

SIP Addressing:

The SIP hosts are identified by a SIP URL. A SIP address can either designate an individual or a whole group.

Locating a SIP server:

The client can either send the request to a SIP proxy server or it can send the request directly to the IP address and port corresponding to the Uniform Request Identifier (URI).

SIP Transaction:

Once the host part of the Request URI has been sent to a SIP server, the client can send requests to that server. A request together with the responses triggered by that request makes up a SIP transaction. The requests can be sent through reliable TCP or through unreliable UDP.

SIP Invitation:

Two requests are required for a successful SIP invitation. First is an INVITE and then an ACK. When the agreement is made by the callee for joining in the call, the caller sends an ACK request confirming the reception of the callee's agreement. A session description is contained within the INVITE request. It provides the required information to the called party for joining the session [1]. The callee returns a similar session description as a response to the invitation provided that the callee agrees to accept the call.

Locating a User:

The position of a callee may vary from time to time. All these locations of the callee are registered dynamically within the SIP server. The SIP server provides a list of probable locations of a callee if a query is made. A location server is used to generate the list which it passes to the SIP server.

Changing an existing session:

A change of the parameters of an existing session can be changed by a re-issue of the INVITE message. This uses the same Call ID with a new body to pass the updated information.

The Hop Server:

The UAS (User Agent Server) sends a response to the proxy server after it is reached. Then the proxy server responds to the client and the client sends an ACK as the confirmation of receiving the response. It was assumed that the proxy server received the INVITE request from the client. On the contrary if the INVITE request was forwarded to a redirect server instead of the proxy server, the redirect server would return the IP of the hop server next to it to the client. After that the hop server communicates with the User Agent Server directly.

How VoIP works: Flowchart and State Diagram

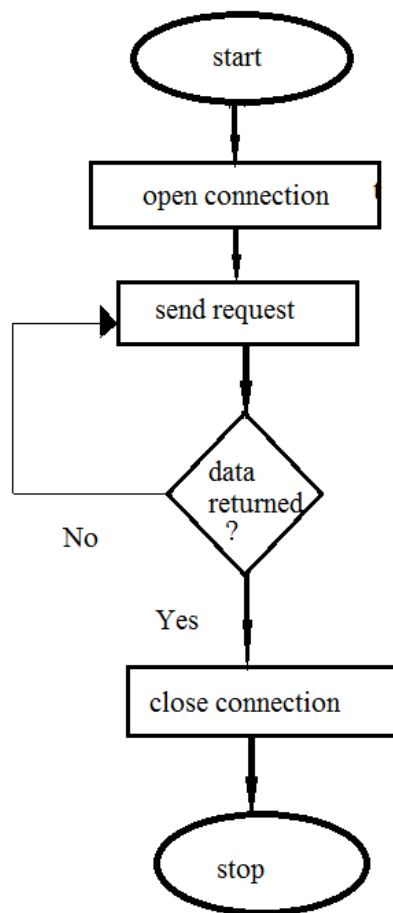


Figure 2.6: Flowchart for the VoIP system

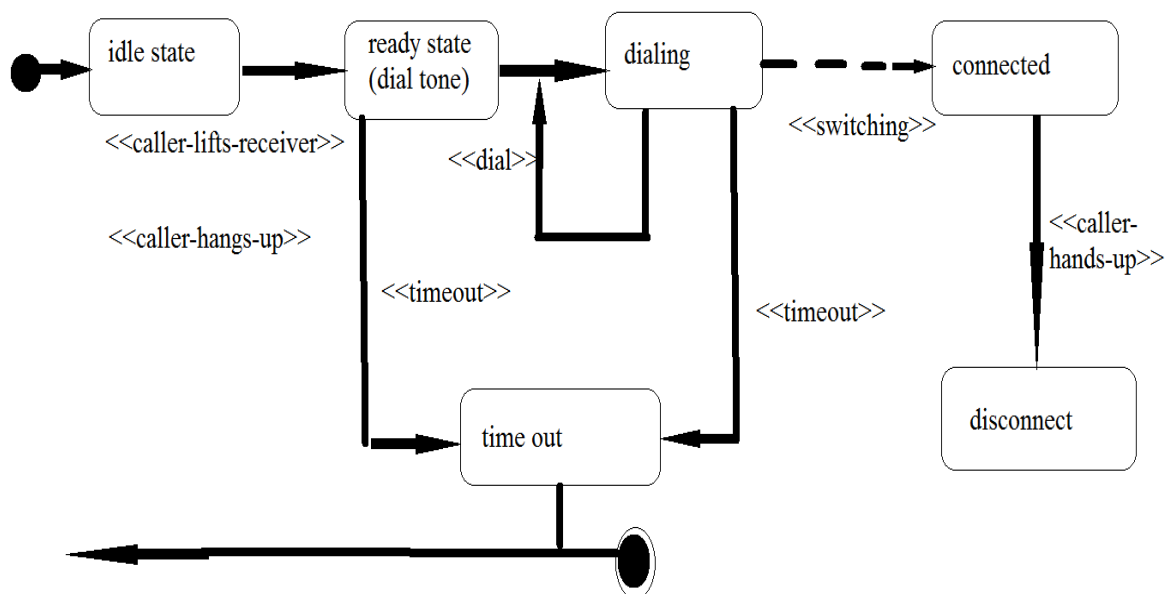


Figure 2.7: State Diagram for the Simulation of the Cisco IP phone calling process

How VoIP works: Summary

VoIP provides the transmission of digitized voice in packet network (e.g IP, ATM, Frame Relay). It also enables telephone conversation to be carried over IP network (in part or end-end) and provides a toll bypass path for telephone calls. It also allows telephony providers to provide cheaper service.



Figure 2.7.1: How VoIP works (basic system)

2.2.3 Overview of VOIP Data Handling

A call needs to be made before sending any voice data. For usual telephony system, a user needs to dial a number and the system then processes it and ring the called person's phone. But for VoIP, the process is much more complex as IP addresses of the computers which are associated with the call needs to be recognized as well. Linking the IP address with the telephone number is a necessary and several protocols are maintained to ensure this. .

To send voice, the callee needs to respond to the call first. Then to send the voice as data, the voice signal is first transformed into digital signal through an analog to digital converter. After this the voice data is represented by a large amount of bits. During this time, a compression algorithm is used to reduce the size of data. With the use of a protocol the voice packets are inserted into data packets and this protocol is known by Real Time Protocol or RTP. The RTP packets contain specific place for data to be sent and this data need to be collected from these packets on the receiver side before turning it into the original voice message. However the RTP packets themselves are carried within UDP packets as payload by UDP protocols. As a result general network nodes can process the packets anywhere in the Internet. At the receiving side, the process is reversed and the data is dissembled, then it is reordered properly. After this the digitized voice data is taken from the packet and is converted into the original analog voice data which is then delivered to the called party through phone's speaker.

2.3 VOIP Benefits/Drawbacks

2.3.1 Benefits of VoIP

VoIP provides an economical alternative options for phone calls. It can also combine business data with calls made by phones. As a result, like the typical call centers, screen pop ups with customer details is used for every incoming calls. Additionally, a 'Click to call' tab can be added on the website. The popularity of VOIP is easily understandable when the staggering amount of phone call hours is considered that is spent by an average employee. The user list of VoIP ranges from retail companies to banks. With the decrease in cost of Broadband Internet, small businesses are now able to use it and lately some of the ISPs (Internet Service Provider) are offering VoIP as well as some telecommunication companies.

VoIP technology increases the opportunity of enhancing call capacity without using extra cabling because it does not use the same process as for general phone calls. Here the voice data is compressed and a single call does not occupy an entire phone line.

Scalability in VoIP

VoIP provides extra flexibility than the usual Private Branch Exchanges (PBX) as a number of 'virtual users' can be connected through each network socket. In the PBX system, the number of ports for plugging telephones is limited.

Reduction in Operating Cost

One of the key advantages of VoIP lies in the fact that it relies on software. Maintaining and managing the software bases system is much more easier than the systems that heavily relies on hardware.

.

Enhancing Productivity

In VoIP, the users can attach documents to voice messages and teleconferencing is easier with this technology. Thus virtual meetings are much common and more productive these days.

Compatibility with Wireless technology

Mobile devices like new generation smart phones and tabs can easily access to VoIP by using a Wireless LAN. Appropriate measures for security has to be there in case of installing LAN and these measure include encryption, firewall etc.

.

Improvement in customer service

There has been a significant improvement in the quality of the customer service in the VoIP based enterprises as all the users need to do to contact a support stuff is to click a button on the website only. Different Customer Relationship Management software can be

implemented easily. The stuff can also operate effectively with the contact history and users information altogether readily available in the screen pops.

Improved Call Management

The employees can easily manage and update the voice related services like caller-ID, broadcast messaging, roaming etc.

Flexibilities of VoIP

Combining the use of VPN (Virtual Private Network) with VoIP makes it much more easier of operating a fully fledged office through a broadband connection. Now it only takes minutes to up and run green-field sites which previously used to take weeks.

2.3.2 Advantages and disadvantages of using VoIP over PSTN

Voice over Internet Protocol (VoIP) is an edge of correspondence that licenses you to make phone calls over a broadband web connection rather than conventional simple telephone lines. Key VoIP benefits conventionally allows us to call other people who are getting calls over the web. Interconnected VoIP organizations too allow us to make and get calls to and from conventional landline numbers, normally for an advantage charge. A couple of VoIP organizations require a PC or a devoted VoIP telephone, while others allow you to use your landline telephone to put VoIP calls through an special connector.

Below is a summary of the benefits and disadvantages of VoIP phone network systems.

Advantages of VoIP include:

- Cost
- Accessibility
- Flexibility
- Voice Quality
- Extra/Less Expensive Features [9]

Cost

The starting setup and progressing costs are generally less for operating a VoIP system than a more conventional phone framework. As VoIP works off the internet connection, there is no requirement for a conventional phone line. This implies that we only need to deal with one account, one bill, for both internet and phone. Calls from PC to PC over the web are free. Calls from PC to landline ordinarily are not totally free but the rates are essentially less than with a conventional phone line.

Accessibility

A VoIP phone system is very different from a traditional phone system. Distance or location makes no difference to a VoIP system, As long as you both have an internet connection, communication is possible whether you are calling your head office on the other side of the country or making a call to the other side of the world.

All that one requires is to have a broadband connection. If we are frequently on the road, or away from the office but wish to remain connected, we can do so at the least cost thus making VoIP much more convenient than a traditional phone line.

Flexibility

Unlike a PBX (Private Box Exchange), a VoIP network has a distinct feature of adaptability. With a private phone network, we are restricted to how numerous phones can be included to the system by the number of lines accessible inside the network. With a VoIP connection, we are only restricted by bandwidth capacity, so thousands of connections can conceivably be made.

Voice Quality

If we have a reliable internet connection with good bandwidth, we should experience voice quality that is the equal of, if not better than, a traditional phone connection. If we are in a rural area without a strong connection, we will receive poor voice quality.

Extra /Cost efficient Features

Traditional phone services have a selection of extra features for which we usually pay more. VoIP is different. It comes with a wide selection of extra features like call forwarding, call waiting, voicemail, caller ID, three-way calling and more. We can also send data like documents and pictures while you are engaging in conversation.

VoIP also has the advantage of allowing everyone including staff and clients to hold video conversations, access and exchange data files, and more, while the conversation is ongoing. This allows for more integrated and flexible meetings that can seamlessly include people from multiple office locations throughout the world.

Disadvantages

Internet Connection A Must

To operate a VoIP phone system, It is required to have a reliable internet connection with sufficient bandwidth.

Power Outages/Emergencies

If there is ever any power outage, there will be no internet connection and so we will lose contact with the phone system. Though this scenario might happen less often than usual, still it might be considered as an issue.

Emergency services can find it difficult to trace calls to a VoIP system.

For these two reasons, many businesses will maintain at least one traditional phone line in order to maintain communications in power outages and emergencies.

Latency

Due to bandwidth requirements, some calls may appear to lag, delay, or disappear altogether. This is because the packets of information need time to reassemble in order for an effective call to be made. This problem is becoming less of an issue as newer, more sophisticated data algorithms come into use.

2.4 Risks of VoIP

Like any application that uses internet, many risks are associated with VoIP too. Like spam and phishing in the emailing, VoIP makes way for a problem which is named as Spam over Internet Telephony (SPIT). Identity theft is another crime that is increasing as well using VoIP. Furthermore, there are issues relating with the privacy of VoIP conversations. [10]

Spam over internet telephony (SPIT)

Spamming in email has already been there for a long time and now with the usage of VoIP, the telemarketers find it easier and cheaper to send their commercial advertisement to the customers of this particular technology. These unwanted VoIP mails may use up several megabytes of data which is very high compared to spam emails.

Spoofing/Imitating

With VoIP systems, it is now possible to imitate and trick a VoIP caller by injecting a false caller ID into an ordinary call. So the user can be tricked into believing the call to be coming from a bank or some other monetary related institutions and may even disclose sensitive information like account numbers, password, any authentication information etc to the other end. The miscreants may use this information for identity theft. This is essentially known as Phishing in VoIP.

Problems related with confidentiality

There is section in the critics who argue that as the data in the VoIP systems sometimes travel without encryption, some might fight the bits and pieces and use it to structure a conversation. The good thing is this process is very complex and software which might be able to pull something this tough is very rare. But as VoIP becomes more popular this side of risking confidentiality should be kept in mind and planning should be done accordingly.

2.4.1 Protection against threats

The first measures for safeguarding VoIP usage is basically the same guidelines that are used commonly for the other internet related applications. These pretty much general rules should be strictly maintained so that the attackers cannot exploit software flaws and gain control over the users' computers. Failure in doing so can expose user's VoIP configuration and the attackers may easily end up having the personal details of the user's shared content over VoIP.

Some general measures that a user may take for safeguarding personal computing:

- i. Using updated and powerful anti-virus and anti spyware programs.
- ii. Using strong passwords and updating them regularly.
- iii. Using a firewall all the time.
- iv. Safe configuration of web browser(s).
- v. Always make sure to verify security and authenticity of new software of downloads.
- vi. Backing up personal data.
- vii. Not sharing sensitive personal details to strangers.
- viii. Update and patching of application software needs to be done regularly.
- ix. Encrypting the software on both end for VoIP applications is very important.

2.5 PSTN vs. VoIP: Feature-by-feature comparison

Feature	VoIP	PSTN
Connectivity type	Internet connectivity	Dedicated telephone lines
Required bandwidth	Requires about 10 Kbps in each direction	Typically requires 64 Kbps in each direction
Pricing	Free VoIP-to-VoIP calling (local and international), but calls to mobile and landline phones have nominal subscription fees of around 1.2 cents to 2.6 cents a minute.	No free calls can be made. Costly international calling. Monthly phone plans usually cost around \$25 to \$30 per month depending on service provider.
Scalability	Upgrades usually require more bandwidth and simple software updates.	Upgrades require purchasing more hardware and dedicated lines, which can be very complex and costly.
Remote extensions	This feature is typically standard.	This feature typically requires dedicated lines for each extension and is very pricey.
Business continuity/disaster recovery	Service terminates when Internet connectivity (power) is lost. Organizations must have a VoIP disaster recovery plan.	Service usually remains active during power outages because phone jacks do not require electricity. But cordless phones do and would be unusable.

Call waiting	Most VoIP options offer free call waiting, such as Google Voice and Skype.	Available at extra cost
Call forwarding	Some VoIP options provide free call forwarding (Google Voice), while others offer it for an extra fee or through a subscription (Skype).	Available at extra cost
Call transferring	Some VoIP options provide free call transferring (Google Voice), while others do not support call transferring at all(Skype).	Available at extra cost
Emergency calling	Depends on the service, but emergency calling is usually not provided by VoIP or is very limited(Skype). 911 calls are also typically untraceable.	Emergency calling is enabled, and services are traceable to location.

Figure 2.8: PSTN vs. VoIP: Feature-by-feature comparison

2.6 Quality of Service (QoS) of VoIP

QoS parameters

Parameters like bandwidth, jittering, packet loss ratio, OWD etc. are very important in determining the quality of service. These affect the quality of voice highly [8].

One way delay

One way delay is the time that is needed for a data packet to travel from its source to destination. The delay depends on the various aspects related with propagation and processing.

Jittering

Jittering is the variable delay the data packets experience while getting sent from source to destination using the Internet Protocol (IP) networks. The inter-departure time on the transmitting side is always the same but it is not the case for the receiving side. Thus the data packets suffer from varying delay.

Packet Loss

UDP and TCP are the two basic transport protocols in IP networks. The TCP protocol has a error recovery process but it is not very much plausible as it relies heavily on the real time operations. On the other hand UDP protocols does not have the recovery option for the transmission errors. So using UDP is problematic as well. Packet loss is the primary concern for VoIP technology. This particular problem may arise even from congestion in network.

CHAPTER 3

OUR PROJECT: DESIGN OF AN ENTERPRISE NETWORK

The objective of our project is to design and implement a Voice over IP (VOIP) system in an enterprise network. Since we want to implement VoIP in an enterprise environment, to demonstrate that we chose to create a scenario that would consist of a head office or data center and two branches of the office at two different locations. All these would be connected to the internet.

Our network would consist of a typical enterprise network:

- ▶ Head office : consists of web servers and file servers, PCs
- ▶ Two branch offices at two locations : Dhaka and Chittagong

These branches would each contain PCs; laptops and IP phones for VoIP connection. Below we have depicted the block diagram of our enterprise network.

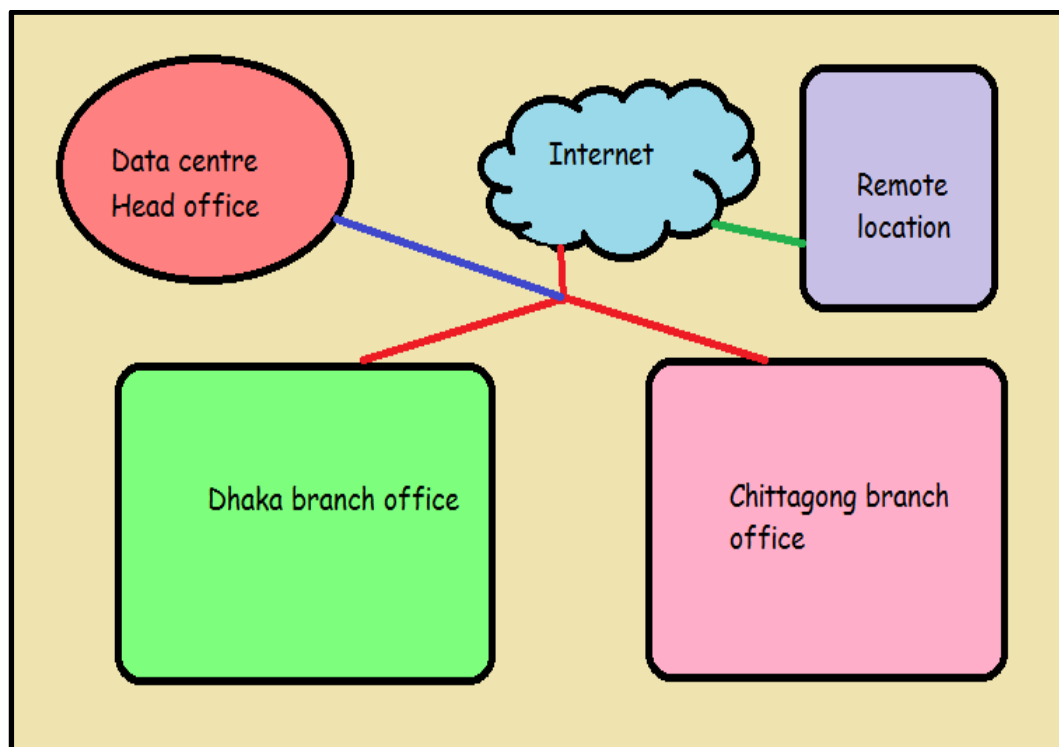


Figure 3.1: Basic schematic diagram of enterprise network scenario

SOFTWARE used for demonstration of VoIP in an enterprise network

We have opted to implement this design in **Packet Tracer** software.

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks [2].

Cisco packet tracer is network simulator software, basically it is used for practicing labs. With the help of this tool we can build our own network topology, and can practice different scenarios.

Also we can use it for testing purpose. Suppose, if we want to deploy any change in our production network, we can use packet tracer to first test the required changes and if everything is working fine then we can deploy that changes into production.

Therefore we have opted to exhibit the project in Packet Tracer. For this we have used Packet Tracer 7.1.0.022

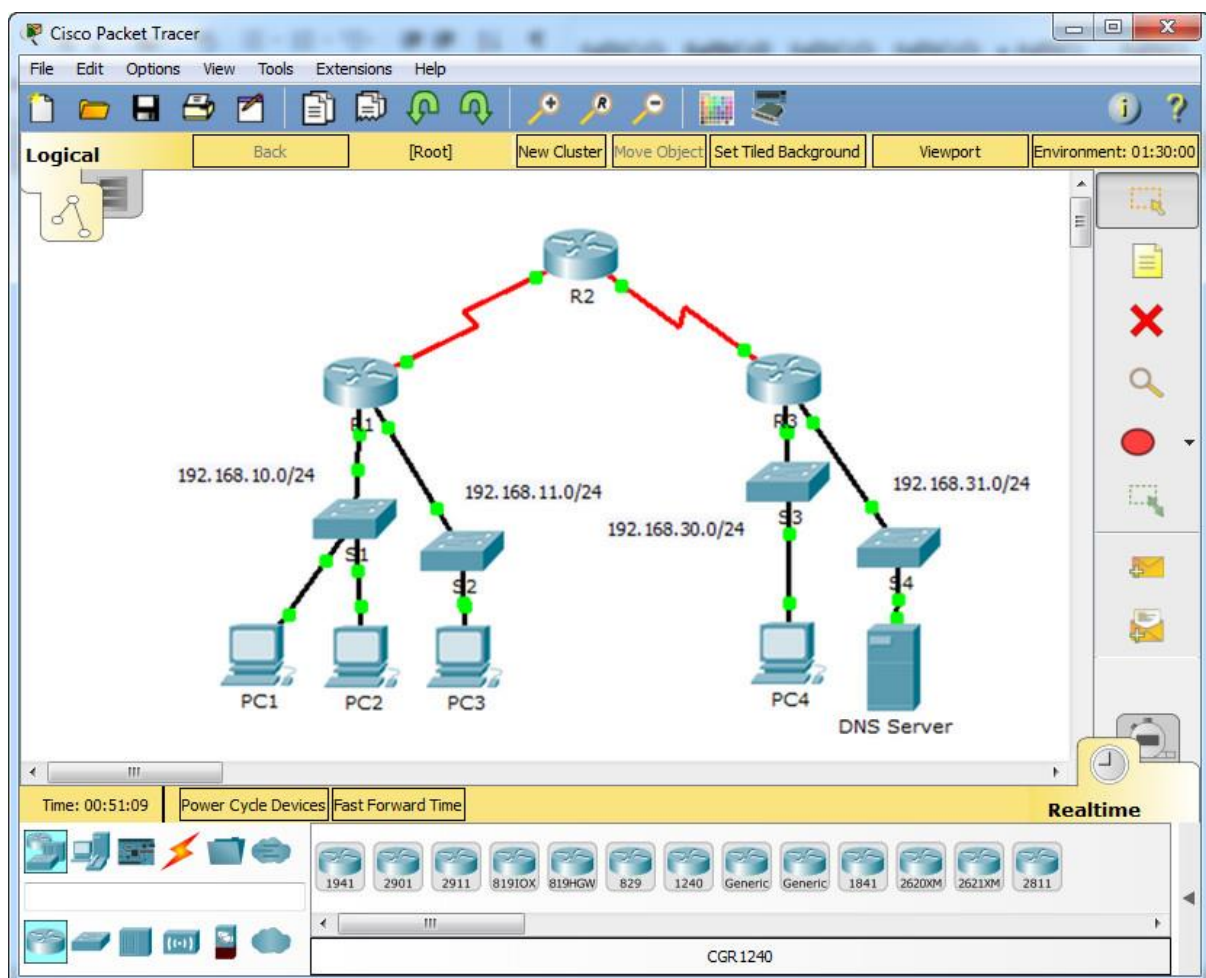


Figure 3.2: Cisco Packet Tracer sample network scenario

3.1 Introduction to VoIP setup in an enterprise network Packet Tracer scenario

Network Diagram

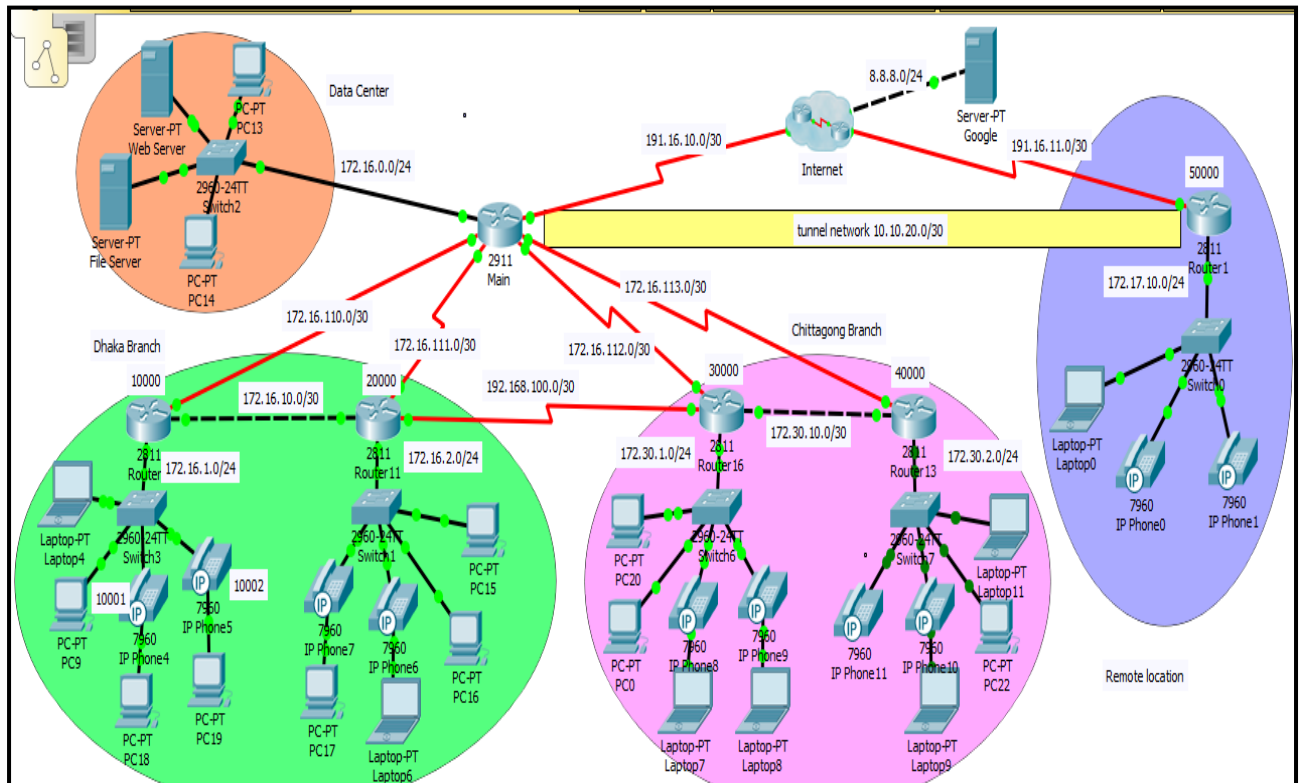


Figure 3.2.1: Enterprise network diagram

3.1.1 Enterprise Network setup components:

Network arrangement and distribution

- For both Dhaka and Chittagong branch, we have assigned Separate Virtual Local Area Networks (**VLANS**).
- Within one branch, we have configured two routers and connected them through copper cross-over cables.
- We assigned some Laptops, PCs and IP phones with each router.
- The same scenario is done for both branches. [3]

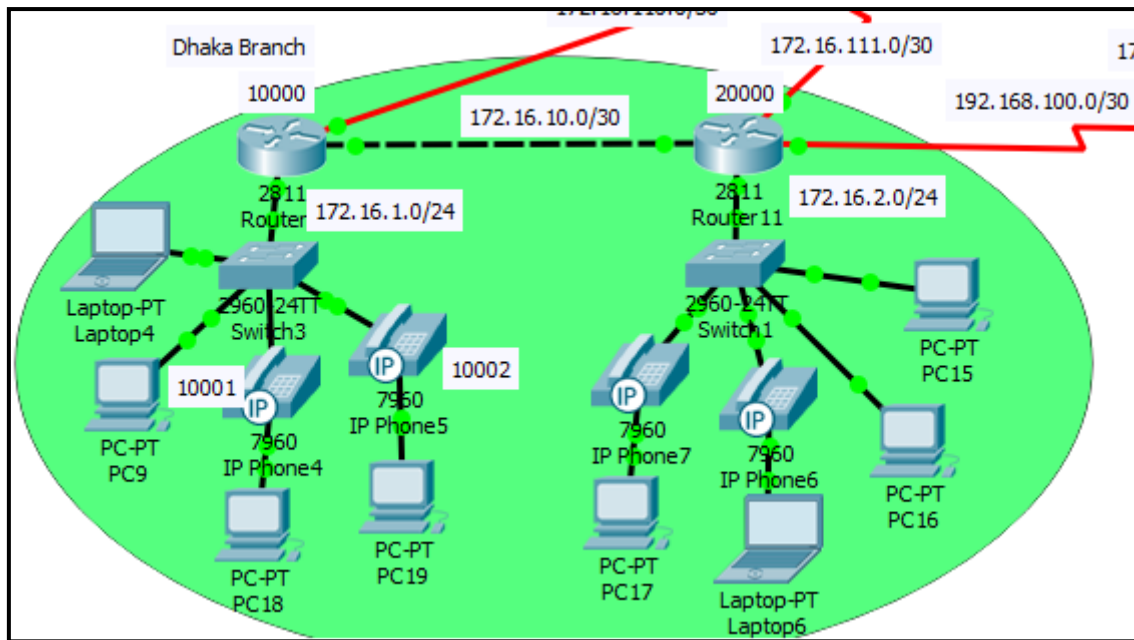


Figure 3.3: Dhaka branch network diagram

Connection between Dhaka and Chittagong Branch:

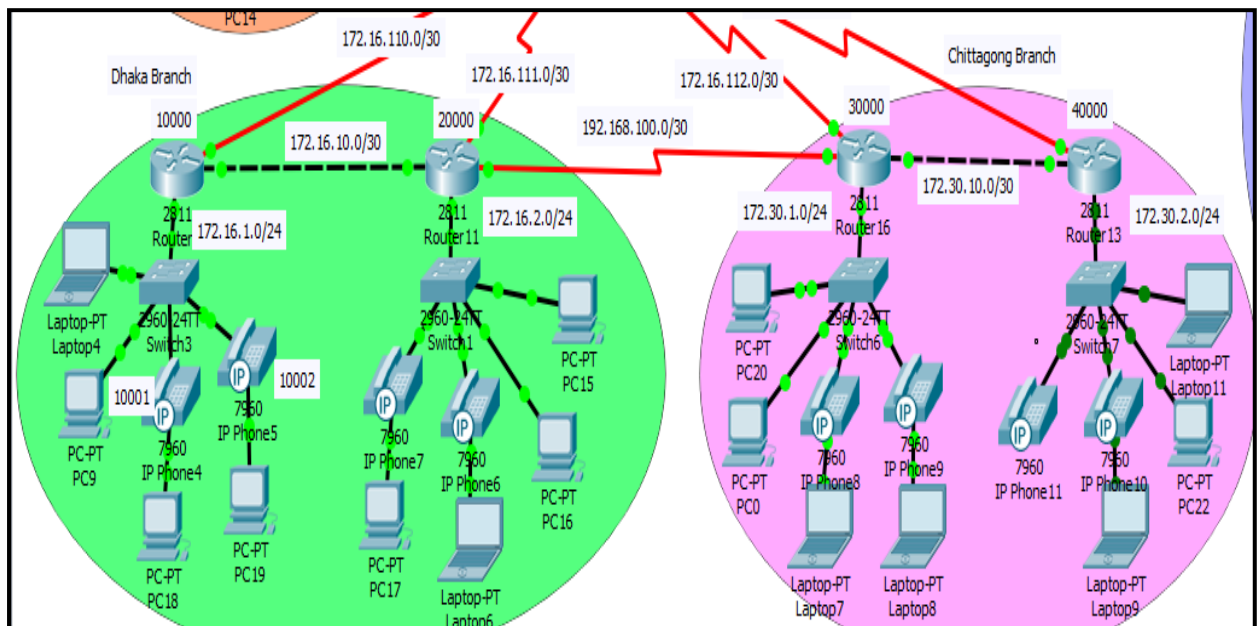


Figure 3.4: Dhaka and Chittagong branch connection diagram

- We have connected both branches through Wide Area Network (WAN).
- This connection is done through serial DTE cables.
- Reason for choosing serial DTE cable is that serial port adapters are usually used for long distance connectivity. Since we have connected two sites, we chose serial DTE.

Router layout:

- For each location, two routers are assigned adding to four routers for both sites.
- To connect the data center, Dhaka and Chittagong branch to the internet, we have used a main router.
- We also have assigned a router to the remote location.

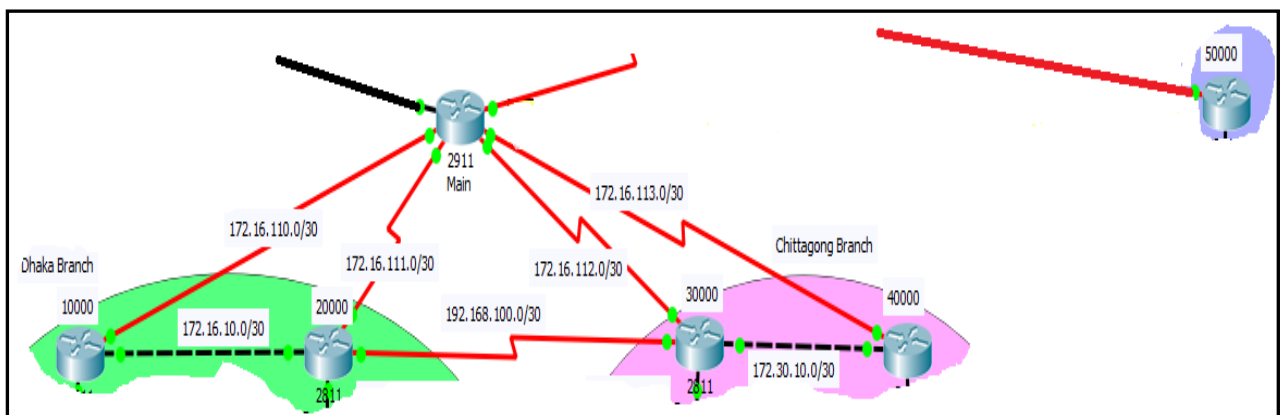


Figure 3.5: Connection of Main router to the other routers

PC, Laptop and IP phone assignment:

- For demonstration purposes, we have assigned few PC , laptop and IP phones at each sites.
- However, number of PC , laptop and IP phones can be added according to need.

CHAPTER 4

CONFIGURATION TASKS

4.1 Introduction to DHCP configuration

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP.

- We have configured **DHCP** to the routers through which we assigned IP addresses and subnet masks for one or more subnets and assigned a default gateway and DNS servers.

Configuring DHCP Service (Cont.)

```
CMERouter(dhcp-config) #
```

```
default-router IP-address
```

- Sets the default gateway that is assigned to DHCP clients

```
CMERouter(dhcp-config) #
```

```
dns-server primary-IP [secondary-IP]
```

- Sets the DNS server or servers that are assigned to the DHCP clients (optional)

```
CMERouter(dhcp-config) #
```

```
option 150 ip IP-address
```

- Defines the TFTP option and what TFTP server to assign to the clients

Figure 4.1: DHCP configuration commands for packet tracer

- Option 150 informs the IP phone of the TFTP server's IP address.
- The TFTP server contains the configuration files and firmware for the IP phone.

4.2 Introduction to Telephony commands configuration:

To get the IP phones to work, we need to configure global telephony commands in the routers so that they can communicate with the IP phones.

At a minimum, the router needs to know:

- i. the maximum number of phones allowed
- ii. the maximum number of phone numbers to be assigned

- iii. the IP address the router uses to respond
- iv. The phones also need a default template file created.

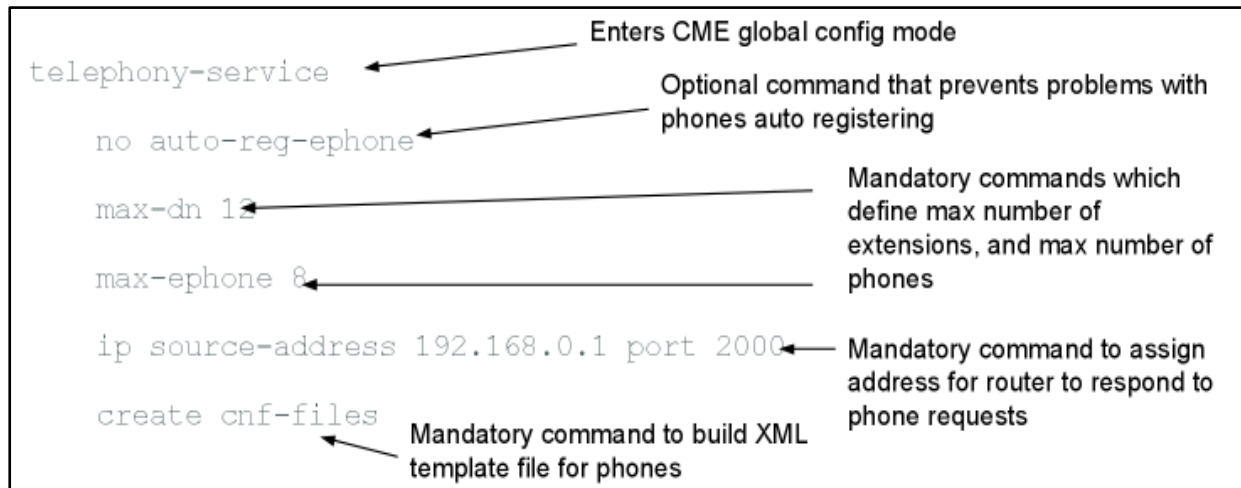


Figure 4.2: max-dn and Ephone-dn configuration command for packet tracer

4.2.1 Configuration for each phone number

Ephone-dn

The command ephone-dn stands for "**e**lectronic **phone** **d**ialing **number**" or as it is commonly known as the "extension" number.

Represents the directory number (i.e. the phone number or extension).

The router model and the max-dn command determines the number of extensions.

Each IP phone must have a directory number assigned before anything else. (Packet Tracer only supports directory numbers.)

On real equipment, ephone-dns can be single-line, dual-line, or octal-line. Packet Tracer only support single-line.

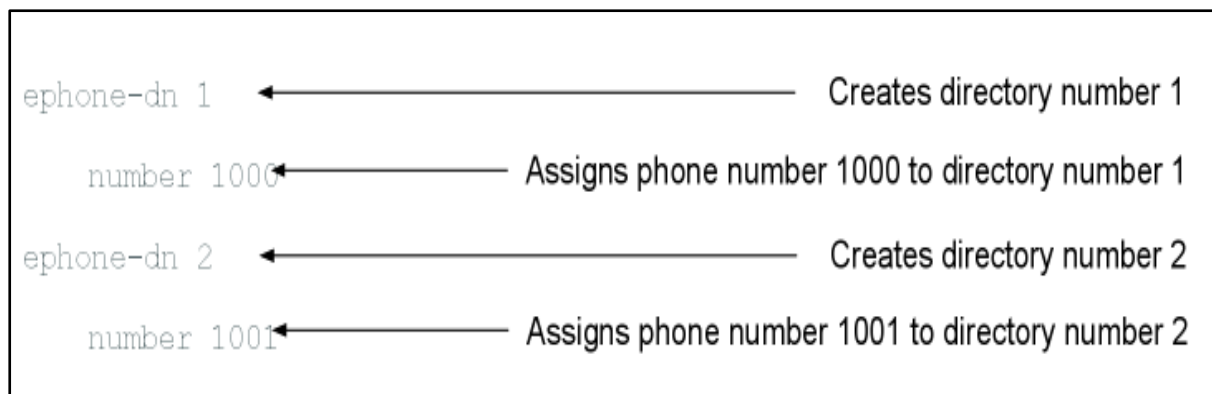


Figure 4.3: Ephone configuration command for packet tracer

4.2.2 Configuration for max-dn

This command decides the maximum number of ephone-dn that can be configured in the system. The maximum number of supported ephone-dn is a feature of the license and the hardware platform. The default is set at 0. In order to make the most efficient use of memory, it is recommended not to set this parameter higher than required.

Multiple Ephones

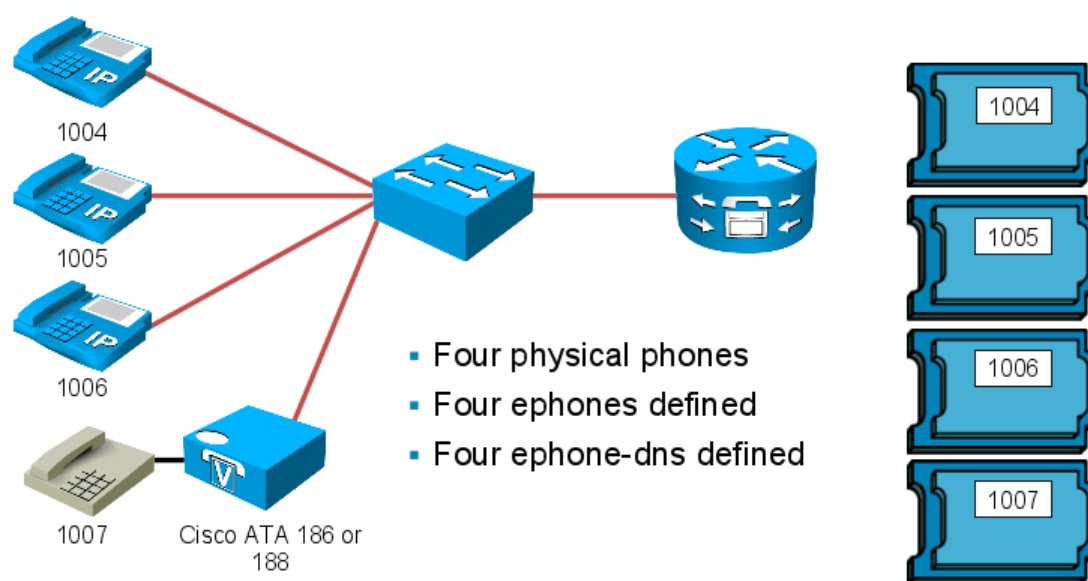


Figure 4.4: Ephone connectivity diagram

4.2.3 Configuring Auto-assign

This command allows Cisco Manager Express (CME) to automatically configure the phones as they are physically connected. The Ephone and Ephone-dn commands will automatically receive the information. If there were more phones, we could change it to "auto assign 1 to 10" [7].

When a Cisco Unified Communications Manager Express system a.k.a. CUCME is registered within a new IP phone, the MAC address of the IP phone is used to create a new e-phone. An Ephone-dn is assigned to the new e-phone within its defined range. In this case the Ephone-dn which is unassigned and lowest in the range, is used. If none of the Ephone-dns is left to assign, some of the phones would not get one or they may receive one using the command for auto assign without a type. This auto assign command without a type is used only when an IP phone is not matched with a type using auto assigned command.

4.3 Dial-peers and destination pattern configuration:

4.3.1 VoIP dial peers:

Dial peers are an addressable call endpoint. They establish logical connections, to complete an end-to-end call.

VoIP dial peers connect over a packet network and perform these functions:

It provides a destination address (telephone number or range of numbers) for the edge device that is located across the network

Associates the destination address with the next-hop router or destination router, depending on the technology used [7].

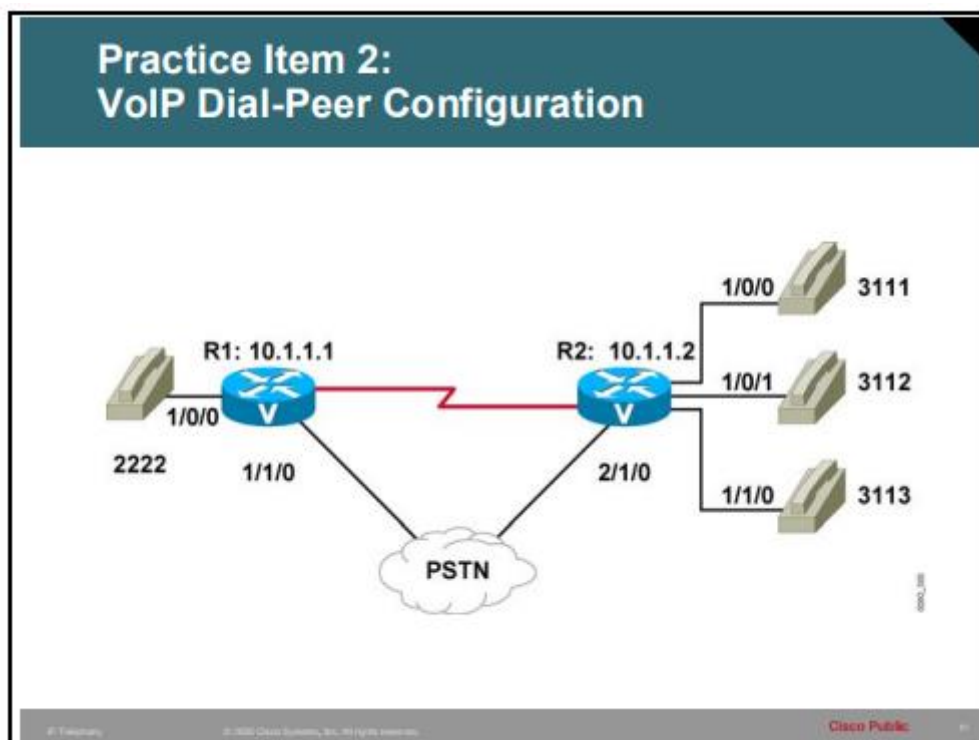


Figure 4.5: VoIP dial-peer configuration diagram

4.3.2 Destination patterns:

The destination pattern associates a telephone number with a given dial peer.

The destination pattern is used to associate a dial string with a particular telephony device.

The call is routed when a dialed string matches a destination pattern.

To provide flexibility in the configuration, a destination pattern can be either an entire telephone number or a partial number using wildcard digits. For example, a wildcard period character (.) represents a single telephone number digit. If a destination pattern were configured as **destination-pattern 28674..**, a telephone number starting with 28674 and ending with any two additional digits would be routed through this port [7].

An Example of dial-peer and destination pattern commands is given below:

```
dial-peer voice 4 voip
destination-pattern 5557000
session target ipv4:12.91.0.1
```

CHAPTER 5

VoIP ROUTING PROTOCOL CONFIGURATION (EIGRP), ACL, NAT and TUNNELING CONFIGURATION

We have implemented **EIGRP** routing protocol to the routers.

5.1 Introduction to EIGRP

EIGRP- Enhanced Interior Gateway Routing Protocol: It is basically a routing protocol and an advanced distance vector. This protocol manages to automate routing decisions and configurations on a computer network.

A routing table is maintained by all routers and this table consists of the rules to dictate the way traffic moves in a network. A traffic is discarded whenever there is no valid path toward the destination.

Routing information is shared automatically within the routers using the EIGRP protocol. As a result, a network administrator does not need to change the configurations manually any more.

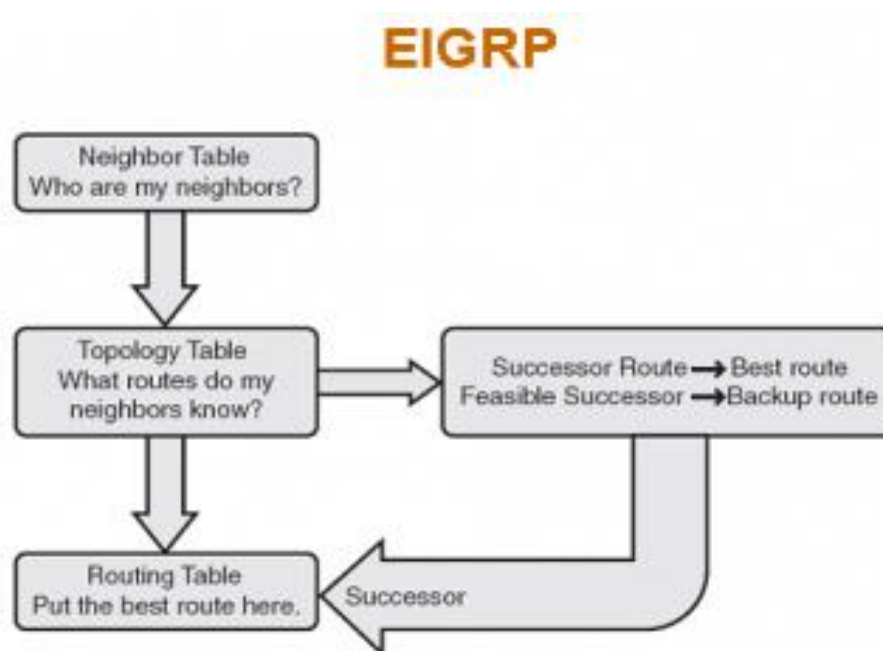


Figure5.1: EIGRP Topology

Below are some key points of EIGRP.

Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of IGRP. It is a Cisco proprietary routing protocol and is called a hybrid protocol. EIGRP is mainly an advanced distance protocol which offers fast convergence. In EIGRP Subnet masks can be of varied lengths and it provides partial updates when the metric for a route changes. It also supports multiple network layer support. A router running EIGRP stores all its neighbor's routing tables so that it can quickly adapt or switch routes.

Let us now look how EIGRP can be configured between routers connected by serial DTE cables.

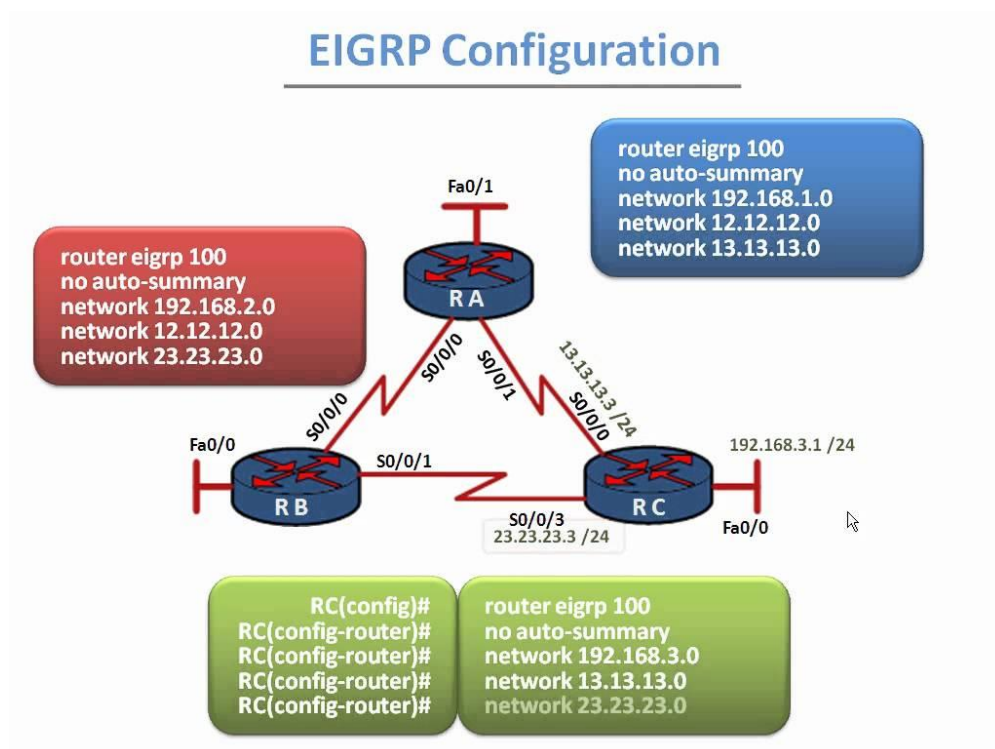


Figure 5.2: EIGRP configuration example with the aid of network diagram

5.2 Introduction to Access List (ACL) configuration:

We have implemented ACL on the main router.

There are a variety of reasons we use ACLs. The primary reason is to provide a basic level of security for the network.

An ACL consists of:

- Access control list name A sequence number or term name for each entry

- A statement of permission or denial for that entry
- A network protocol and associated function or ports
 - Examples include IP, IPX, ICMP, TCP, UDP, NETBIOS and many others
- Destination and Source targets
 - These are typically addresses and can be defined as a single discrete address, a range or subnet, or all addresses
- Additional flags or identifiers
 - These additional statements request additional functions when a match is found for the statement.

An ACL follows a structured set of rules that can be used to filter traffic. Each of the rules of ACL indicates a collection of conditions that a packet must comply with the rules. When the switch establishes that an ACL applies to a packet, it analyzes the packet against the conditions of all the rules. Depending upon the first match that is found, a packet is permitted or restricted.

If no match is found, the switch applies the appropriate default rule. The switch continues to deal each packet by processing the ones that are permitted and dropping the ones that are denied. ACLs can be used to protect networks and particular hosts from unnecessary and useless traffic. As for example, we could use ACLs to prohibit HTTP traffic from a high security network to the internet. ACLs can also be used to allow HTTP traffic only to certain sites by using the IP address of the site to recognize it in an IP ACL.

5.3 Introduction to NAT configuration: Network Address Translation

NAT- Network Address Translation: NAT is used for preservation of IP address. Through this private IP systems are able to put through the unregistered IP addresses to the internet. NAT basically represents a switch, which is used to interface two systems together and it is also used in interpreting the private addresses into legal addresses in the inner network prior to sending packets. NAT is also able to advertise itself to the outside world as the one special address for the whole network . So the whole network can be covered up behind the NAT address and this proves to be an additional safety feature. Thus NAT acts for two purpose, one is to provide additional security and the other one is for preserving addresses. In the remote access situations, NAT is regularly implemented.

NAT is short for *Network Address Translation*. NAT is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

NAT serves three main purposes:

- i. Offers a kind of firewall by hiding internal IP addresses.
- ii. Permits a company to use more internal IP addresses. Since the IP addresses are only used on the inside, there is no chance of any clash with IP addresses used by other companies and organizations.
- iii. It allows a company to merge multiple ISDN connections into a single internet connection.

Therefore we have implemented NAT to the main router and the one router linking to the internet.

NAT command example:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
ip address 10.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

5.4 Introduction to Tunneling and Implementation:

A *virtual private network (VPN)* is a network that is constructed using the Internet — to connect remote users or regional offices to a company's private, internal network.

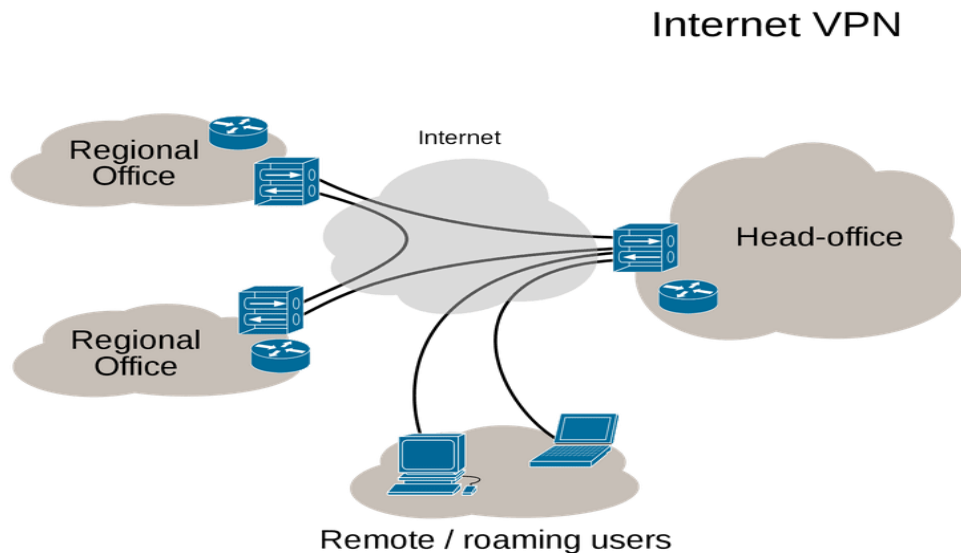


Figure 5.3: Virtual Private Network(VPN)

This type of network is designed to provide a secure, encrypted *tunnel* in which to transmit the data between the remote user and the company network.

In our project, we have created a tunnel between our main router and the remote location router. Since the main router connects data center and the two branch office LANs with the internet, tunneling is only done with that router.

5.4.1 Tunneling configuration: for main router

```
interface Tunnel0
```

```
ip address 10.10.20.1 255.255.255.252
```

```
tunnel source Serial0/2/1
```

```
tunnel destination 191.16.11.1
```

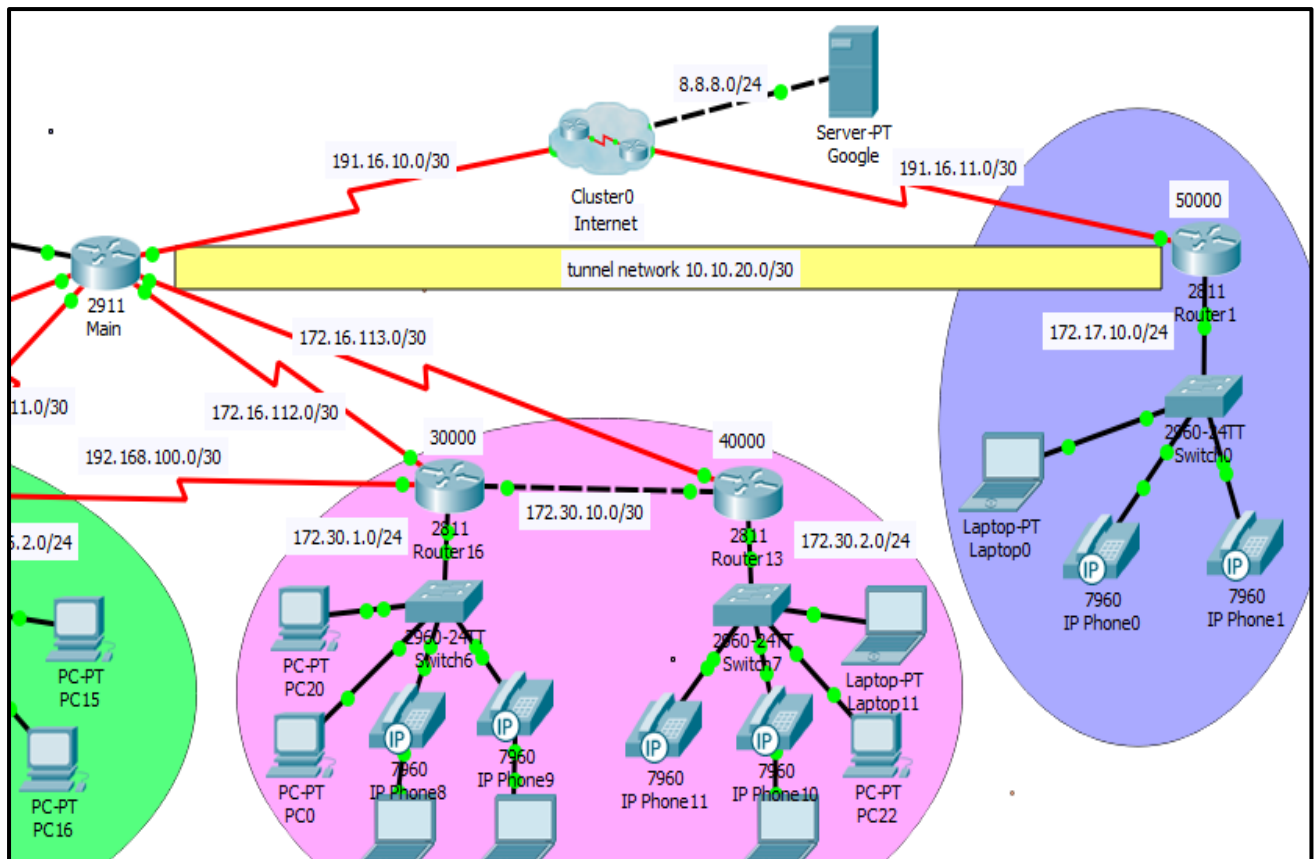


Figure 5.4: Tunneling done between main router and remote location router

5.5 Router and Switch configuration commands

Router 6

```
hostname Router
ip dhcp pool VoIP
network 172.16.1.0 255.255.255.0
default-router 172.16.1.1
option 150 ip 172.16.1.1
dns-server 8.8.8.8
interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet0/1
ip address 172.16.10.1 255.255.255.252
duplex auto
speed auto
interface Serial0/0/0
ip address 171.16.110.1 255.255.255.252
interface Serial0/0/1
no ip address
interface Vlan1
no ip address
shutdown
router eigrp 10
network 172.16.1.0 0.0.0.255
network 172.16.10.0 0.0.0.3
network 172.16.110.0 0.0.0.3
dial-peer voice 1 voip
destination-pattern 200..
session target ipv4:172.16.10.2
dial-peer voice 3 voip
destination-pattern 300..
session target ipv4:192.168.100.2
dial-peer voice 4 voip
destination-pattern 400..
session target ipv4:172.30.10.2
dial-peer voice 10 voip
destination-pattern 500..
session target ipv4:10.10.20.2
telephony-service
max-ephones 10
max-dn 10
ip source-address 172.16.1.1 port 2000
auto assign 1 to 10
ephone-dn 1
number 10001
ephone-dn 2
number 10002
```

Main router

```
interface Tunnel0
ip address 10.10.20.1 255.255.255.252
tunnel source Serial0/2/1
tunnel destination 191.16.11.1
interface GigabitEthernet0/0
ip address 172.16.0.1 255.255.255.0
ip nat inside
duplex auto
speed auto
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
interface Serial0/0/0
ip address 172.16.110.2 255.255.255.252
ip nat inside
interface Serial0/0/1
ip address 172.16.111.2 255.255.255.252
ip nat inside
interface Serial0/1/0
ip address 172.16.112.2 255.255.255.252
ip nat inside
interface Serial0/1/1
ip address 172.16.113.2 255.255.255.252
ip nat inside
interface Serial0/2/0
no ip address
shutdown
interface Serial0/2/1
ip address 191.16.10.1 255.255.255.252
ip nat outside
interface Vlan1
no ip address
shutdown
router eigrp 10
redistribute static
network 172.16.110.0 0.0.0.3
network 172.16.111.0 0.0.0.3
network 172.16.112.0 0.0.0.3
network 172.16.113.0 0.0.0.3
network 172.16.0.0 0.0.0.255
ip nat inside source list 1 interface Serial0/2/1
overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/2/1
ip route 172.17.0.0 255.255.0.0 10.10.20.2
access-list 1 permit 172.16.0.0 0.15.255.255
```

Router 1

```
ip dhcp pool VoIP
network 172.17.10.0 255.255.255.0
default-router 172.17.10.1
option 150 ip 172.17.10.1
dns-server 8.8.8.8
interface Tunnel0
ip address 10.10.20.2 255.255.255.252
tunnel source Serial0/0/0
tunnel destination 191.16.10.1
interface FastEthernet0/0
ip address 172.17.10.1 255.255.255.0
ip nat inside
interface FastEthernet0/1
no ip address
shutdown
interface Serial0/0/0
ip address 191.16.11.1 255.255.255.252
ip nat outside
interface Serial0/0/1
no ip address
interface Vlan1
no ip address
ip nat inside source list 1 interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
ip route 172.16.0.0 255.240.0.0 10.10.20.1
access-list 1 permit 172.17.0.0 0.0.255.255
dial-peer voice 1 voip
destination-pattern 100..
session target ipv4:172.16.1.1
dial-peer voice 2 voip
destination-pattern 200..
session target ipv4:172.16.2.1
dial-peer voice 3 voip
destination-pattern 300..
session target ipv4:172.30.1.1
dial-peer voice 4 voip
destination-pattern 400..
session target ipv4:172.30.2.1
telephony-service
max-ephones 10
max-dn 10
ip source-address 172.17.10.1 port 2000
auto assign 1 to 10
ephone-dn 1
number 50001
ephone-dn 2
number 50002
```

Switch 3

```
interface FastEthernet0/20
switchport mode access
switchport voice vlan 1
!
interface FastEthernet0/21
switchport mode access
switchport voice vlan 1
!
interface FastEthernet0/22
switchport mode access
switchport voice vlan 1
!
```

- Similar configuration as router 6 is done for Router 11, 16 and 13.
- Configuring for Main Router and Router 1 is different than Router 6, 11, 16 and 13.
- As explained in above theory, in main router and router 1, we have additionally configured NAT, ACL and Tunneling.
- Similar configuration is done for Switch 1, 6, 7 and 0.

CHAPTER 6 RESULTS

6.1 Testing: Verifying the connectivity

6.1.1 Checking DHCP configuration for the PCs

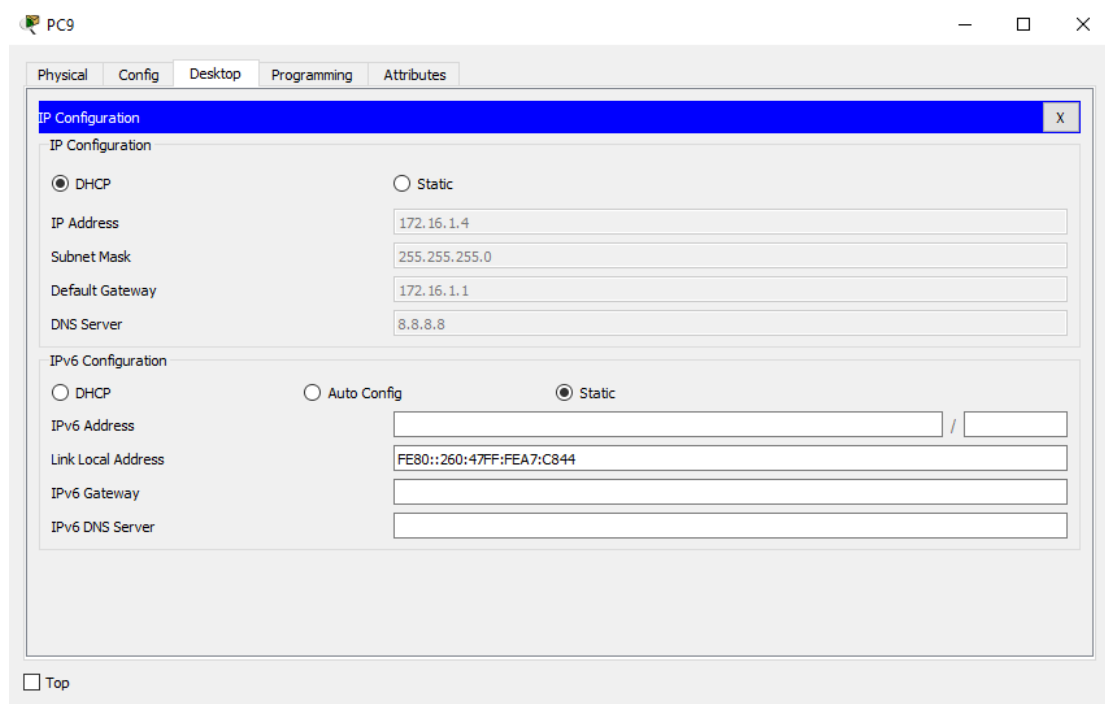


Figure 6.1: DHCP connectivity for PC

Verifying DHCP connection for the Laptops:

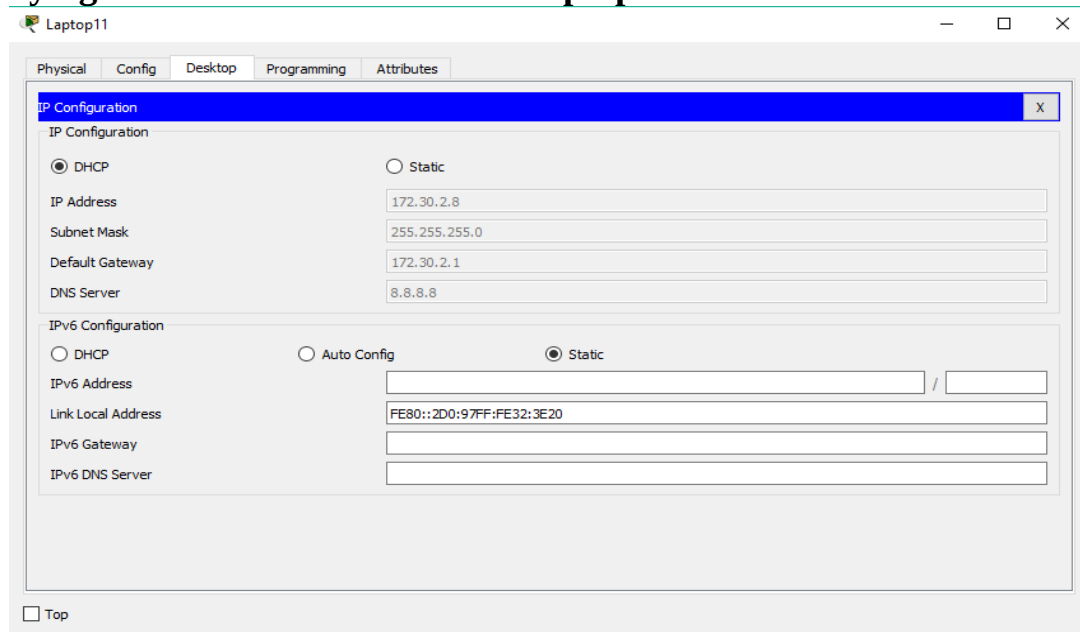


Figure 6.2: DHCP connectivity for PC

6.2 Powering up the IP phones:

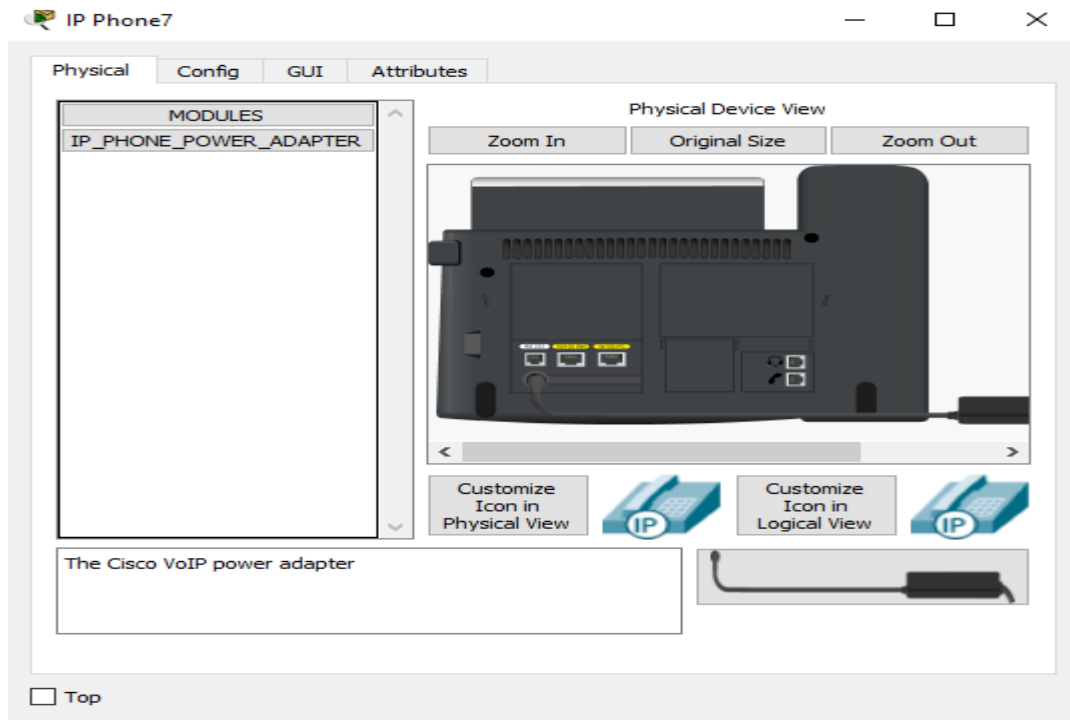


Figure 6.3: powering the IP phone

6.2.1 Verifying if the IP phones are assigned with their respective phone numbers:

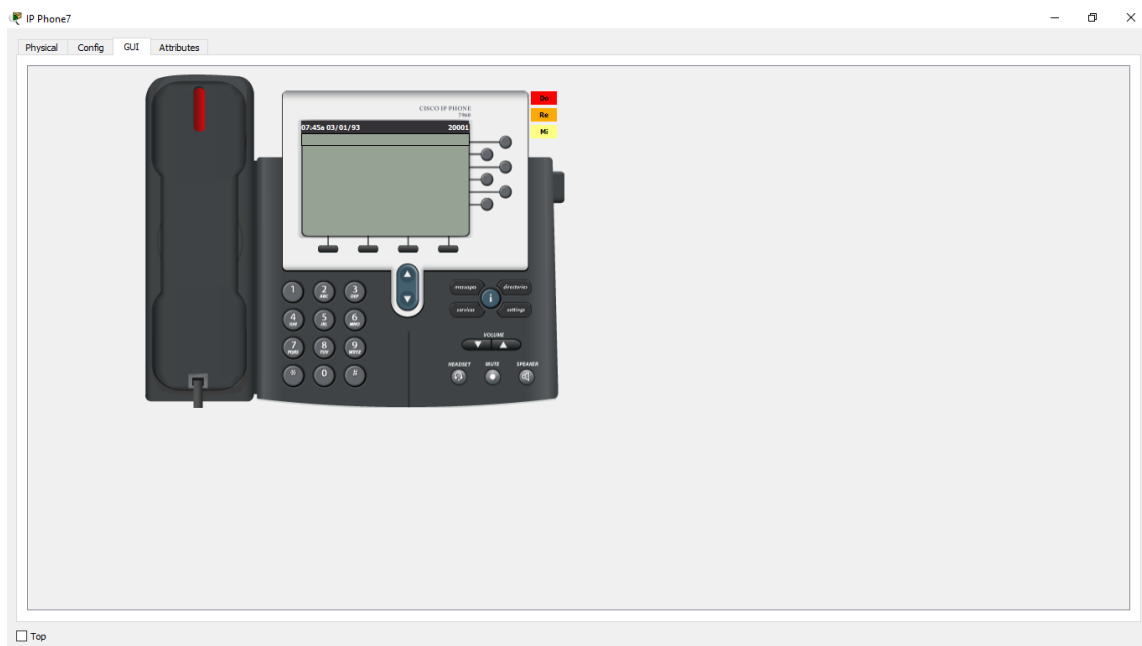


Figure 6.4: Obtaining IP phone numbers

6.3 Verifying the connectivity by calling from one IP phone to another and ping test :



Figure 6.5: Calling from one IP phone to another

Success!!!

Realtime								
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Laptop8	Laptop9	ICMP		0.000	N	0
	Successful	Laptop6	Laptop7	ICMP		0.000	N	1
	Successful	PC18	Laptop11	ICMP		0.000	N	2

Figure 6.6: Ping from one PC to another

CHAPTER 7

CONCLUSION

Benefits of VoIP technology include high flexibility and mobility, increased productivity and it is easy to install, use and troubleshoot. The primary advantages of using VoIP rather than using PSTN (Public Switched Telephone Network) are:

i. As the monthly subscription fees are lower and less equipment is needed for implementation of VoIP, the cost is significantly cheaper.

ii. A whole lot of travelling and training cost can be minimized by using VoIP calls which include video conferencing tools. Only a scalable phone system is needed for this.

A scalable phone system means easy integration of newer extensions into network without the necessity of expensive hardware.

iii. A huge advantage of VoIP is more than two people can be connected in a video conference. In this way teleconferencing is made easier than ever.

iv. VoIP tries to integrate the cutting edge technologies to ensure stronger security and supreme quality.

v. VoIP is always evolving. Thus it is a must choice for all kinds of businesses whether it is a new one or one that has been running for a long time.

vi. The availability of high speed broadband internet of modern times has made it far more easier for common people to adopt VoIP in their day to day communication as well as in the business voice communications.

Therefore, despite its few short-comings, for the enterprise, VoIP lessens the cost for high-end equipment, lines, manpower, maintaining and preservation. Since all of the voice and data traffic of an organization is incorporated into one physical network, it also cuts down the need for separate PBX tie lines.

To summarize our project work, in conclusion what we did was we created an enterprise network scenario and implemented VoIP using Cisco Packet Tracer software. Our objective was to learn from the basics of how to create VLAN and how to configure and establish connection in VoIP phones for a network scenario.

To implement this topology, we had to study the whole VoIP scenario, VoIP background, its features, benefits and drawbacks and its future in the networking world. Overall, this project improved our understanding of the whole concept of VoIP and its ever increasing demand in present times.

REFERENCES

- [1] <http://searchenterprisewan.techtarget.com>
- [2] <https://www.cisco.com>
- [3] http://www.academia.edu/32444198/DESIGN_AND_SIMULATION_OF_AN_ENTERPRISE_NETWORK_USING_PACKET_TRACER_A_Case_Study_of_a_Model_Secondary_School.
- [4] Juan C. Pelaez, Eduardo B. Fernandez, and Christian Wieser, *Patterns for VoIP Signaling Protocol Architectures*,
<https://pdfs.semanticscholar.org/faee/8ee6e1c7e072a643b9711595ebaa9c011191.pdf>
- [5] Francisca O. Oladipo, Christogonus C. Madu, Christopher C. Okoro, *Re-Engineering Campus-Wide Internet Telephony Using Voice over Internet Protocol*, International Journal of Networks and Communications 2015, 5(2): 23-30 DOI: 10.5923/j.ijnc.20150502.01
- [6] Prof. Mr. Altaf. I. Darvadiya ; Ms. Zarna M. Gohil; Ms. Nehalkumari T. Joshi, *Configure A VoIP Network DESIGN AND SIMULATION OF AN ENTERPRISE NETWORK USING PACKET TRACER: A Case Study of a Model Secondary School* By Yahya Faydah U10EE1019, Cisco IOS voice, Video and Fax configuration guide.
- [7] Packet Tracer 6.1 tutorial – IP telephony basic configuration Developed for the Cisco Networking Academy Community by: Bernard Brunet, Anil Datta, Ben Franske, and Brent Seiling, CCNA Voice Primer.
- [8] Bhagyalaxmi Pandi Amity School of Engineering & technology Amity University Jaipur, Rajasthan; *Performance with Voice over Internet Protocol*.
- [9] <http://www.packetworks.net/blog/business-voip-the-benefits-disadvantages-and-how-it-works.htm>
- [10] <https://www.lifewire.com/security-threats-in-voip-3426532>