

Voice Over Internet Protocol Based Communication Design (VoIP) With 3CXSystemPhone On Android Smartphone

Riki^{1)*}, Aditiya Hermawan²⁾, Yusuf Kurnia³⁾

¹⁾³⁾Buddhi Dharma University

Jl. Imam Bonjol No. 41 Karawaci Ilir, Tangerang, Indonesia

¹⁾riki@ubd.ac.id

²⁾aditiya.hermawan@ubd.ac.id

³⁾yusuf.kurnia@ubd.ac.id

Article history:

Received 10 August 2018;
Revised 16 August 2018;
Accepted 25 August 2018;
Available online 19 September 2018

Keywords:

TCP/IP
Nirkabel
Voice
Smartphone
WiFi

Abstract

TCP/IP protocol can be connected to various computer data networks in the world. This protocol increasingly exists and is needed so that many parties develop it to vote through this protocol. Voice Over Internet Protocol technology is the answer to that desire. This technology is able to convert analog voice (human voice) into data packets then through public internet data networks and private intranet data packets are passed, so that communication can occur. With VoIP communication costs can be reduced so that it can reduce investment costs and conversations (cost saving) or even up to 100% free. VoIP implementation can be done by designing a wireless VoIP network (cable) using 3CXSystemPhone software as a PBX. In this scientific work the software used is 3CXSystemPhone 11.0, where SIP is a VoIP server which is a freeware software, in its application only requires one PC server and several PC clients (2 for example) that are connected to each other.

I. INTRODUCTION

The development of technology, especially information technology, brings very fundamental changes to the world of telecommunications. In communication technology, voice communication is one thing that will be a very important part, because currently voice communication is considered the most practical communication. This has led to the presence of digital signal processing technology that has modular capabilities based on IP (Internet Protocol) technology that is integrated between data and voice communication. VoIP (Voice Over Internet Protocol) is a technology that can pass "voice calls", videos and data over an IP network. Analog call forms are converted to digital form and run as data by the internet protocol. The IP network itself is a packet-switch data communication network, so we can call using an IP network or the internet. VoIP networks can be built using wireless and cable networks. VoIP allows routing, access servers and multiservice access concentrators to carry and send voice and fax across IP networks.

In VoIP, digital signal processor (DSP) through segmentation (breaking) of sound signals to various forms of frames and storing them in sound packages. These voice packages are sent via IP in collaboration with the Problem Scope Formulation of voice communication protocols such as: Session Initiation Protocol (SIP), H.323 or Media Gateway Control Protocol (MGCP).

The use of VoIP-based telephones provides many advantages, especially in terms of cost, obviously cheaper than traditional telephone costs, because IP networks are global. This is because VoIP can be installed in any Ethernet and IP address, unlike a traditional telephone that must have a separate port in the Central or PBX. In planning a VoIP network we must have a server that functions as an IP PBX, this research will discuss Asterisk VoIP Server which is an Open Source software, in its application only requires one PC Server and several PC Clients (2 for example) connected one each other. Asterisk architecture is basically simple, but very different from PBX (traditional telephone). Basically Asterisk is used as an intermediary between telephone technology, where VoIP

* Corresponding author

protocol technologies such as, SIP, H.323 or MGCP are the same as traditional technology, namely PBX phones (traditional telephone).

In this research VoIP application will be implemented between two clients and one VoIP server that uses Asterisk as VoIP Server.

II. RELATED WORKS/LITERATURE REVIEW (OPTIONAL)

The internet network currently uses the concept of internetworking by connecting a number of gateways in the same communication, where TCP/IP internetworking protocols are called Internet Protocols. The internet is seen as a set of subnetworks that are linked together. The following is an example of an internet network:

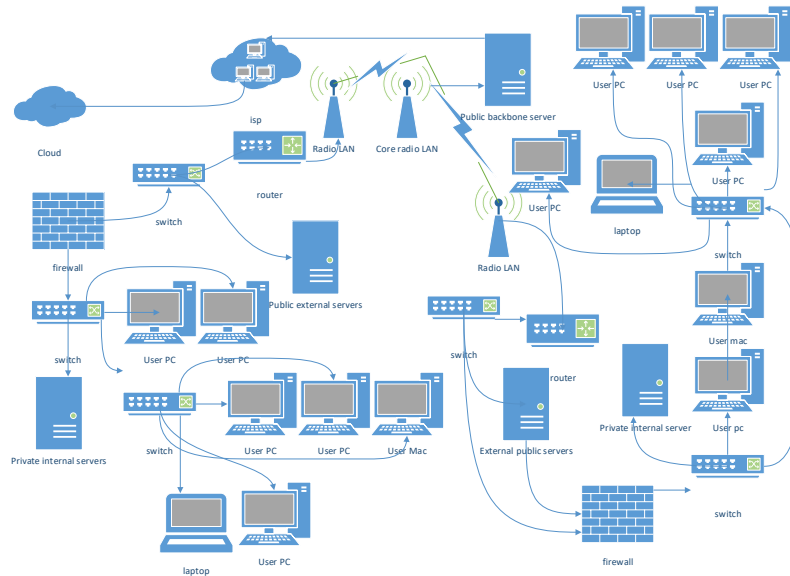


Fig. 1 Internet networks that connect various computer networks

Backbone (backbone network) is built from channels that have high bandwidth and fast routers. The backbone network connects regional networks (middle level). Regional networks connect Local Area Networks (LAN). A LAN is the smallest network that can take the form of a Bus token, Ring token or Ethernet. The task of IP is to provide the best way to carry the datagram from source to destination. The internetworking protocol used by the internet network at this time is TCP / IP version 4, but over the times to overcome and improve the internet network, the TCP / IP internetworking protocol has emerged, TCP / IP version 6.

The TCP / IP protocol communication standard consists of layers (layers). But it's not like the OSI standard which has 7 layers, while the TCP / IP standard only has 4 layers, but each layer communicates with each other.

IP provides a connectionless delivery service which means that data is sent just like that without the establishment of a path in advance (connection set-up), but directly sent from the network. If in the course of the package there are things that are not desirable (one path is broken, the router has congestion / traffic jam, or the destination host / network is down), the IP protocol only tells the packet delivery via ICMP protocol, that there is a problem in sending IP packets to the sending host. The basic unit used for data transfer is datagram. IP is also a Datagram delivery service which means that every data packet sent is independent of other data. As a result, the path taken by each IP data packet to its destination can be different from one another. Because the path taken is different, the arrival of the package becomes out of sequence. Every data that is passed is always added with a header.

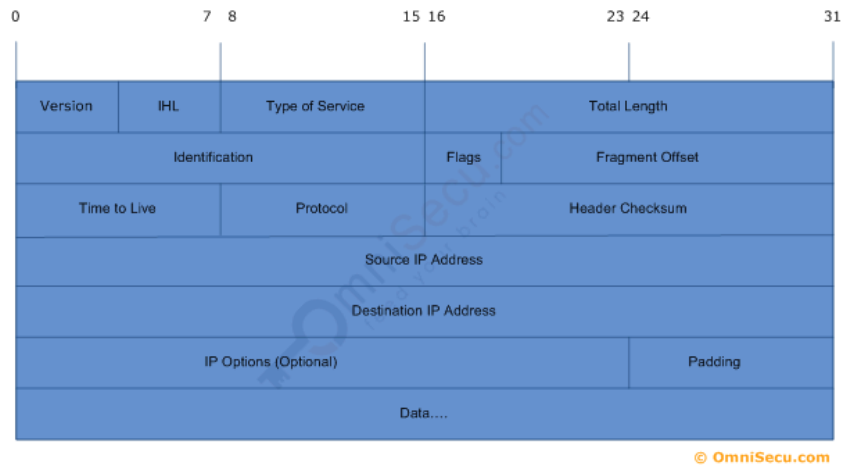


Fig. 2 Datagram Header

In the picture above is given an IP datagram format. Each IP packet carries data consisting of:

1. Version, contains the version of the IP protocol used. Currently the internet protocol used is IP version 4 (Ip4).
2. Header Length, contains the length of the IP packet header (in 32 bits).
3. Type Of Service, indicating how the datagram is processed.
4. Total Length of datagram, indicating the total length of the datagram in bytes, including the IP header and TCP / IP header.
5. Identification, Flags, and FragmentOffset, contains some data related to packet fragmentation. Packages that are passed through various types of paths will experience fragmentation (broken down into smaller packages) according to the maximum amount of data that is normally transmitted through that path.
6. Time to Live, contains the maximum number of routers that IP packets can pass. Every time the IP packet passes through one router, the contents of this field are reduced by one. If the TTL has been used up and the package still hasn't reached its destination, then this packet will be discarded and the last router will send the ICMP time exceeded packet. This is done to prevent IP packets continuously being in the network.
7. Protocol, shows the type of transport layer protocol used by IP (contents of data from the package).
8. Header Checksum, contains checksum values calculated from all fields of the IP packet header. Before being sent the protocol first calculates the checksum of the IP packet to later be recalculated on the receiving side. If there is a difference, then this package is considered damaged or discarded.
9. Source and Destination IP Address, mark the network number and number of the sender and recipient host. With this field can be known the sender and recipient address so that the IP packet will only arrive at the destination IP address.
10. Option, including:
 - a. Strict source route, contains a complete list of IP addresses from the router that this packet must pass on the way to the destination host. Replies from the destination host to the sending host are required via the same router.
 - b. Loose source route, by setting this option, the package sent must stop at several routers. If between the two routers there is another router, the packet can still be through the router.

III. METHODS

Standard VoIP Protocol, VoIP support protocols are actually much more, but here only the H.323 protocol and the SIP protocol are explained, because this protocol is most often used in supporting VoIP network design, while in the design of the author using the SIP protocol [1].

SIP Protocol, SIP (Session Initiation Protocol) is a multimedia protocol standard issued by groups that are members of Multiparty Multimedia Session Control (MMUSIC) which are in the Internet Engineering Task Force (IETF) organization documented in the request for command (RFC) 2543 document in March 1999. SIP is a protocol in the application layer that defines the initial process, change, and termination (termination) of a multimedia communication session. This communication session includes multimedia relationships, distance learning, and other applications.

SIP can be said to be client-server characteristics, this means that the request is given by the client and this request is sent to the server. Then, the server processes the request and gives a response to the request to the client. Requests and responses to requests are called SIP transactions. SIP is also called a text-based (text-based) protocol [2][3].

1. SIP component

In conjunction with IP Telephony, there are two components in the SIP system, namely:

a. User Agent

User Agent is the end system that is used to communicate. User Agent consists of 2 parts, namely:

1) User Agent Client (UAC)

UAC is an application on a client that is designed to start SIP requests.

2) User Agent Server (UAS)

UAS is a server application that gives users if they receive a request and respond to the request. The response can be to accept or reject a request.

b. Network server

So that users on the SIP network can start a call and can also be called, the user must first register so that the location can be known. Registration can be done by sending a REGISTER message to a SIP server, there are two types of network servers, namely:

1) Proxy Server

A Proxy Server is a server that receives requests, processes them, and forwards the received request to the next hop server after changing several headers on the request message. Next hop server can be a SIP server or other server where the proxy server doesn't need to know. The proxy server can function as a client and server because the proxy server can provide requests and responses.

2) Redirect Server

This component is the server that receives the request message and responds to the request containing the address from the next hop server.

2. Addressing the SIP Protocol

In the SIP protocol, the addressing system is assigned a SIP URL attribute (SIP Uniform Resource Locator) that resembles an e-mail address to be easily recognized. The addressing form is:

a. user @ host, as written below: riki@buddhi.ac.id, riki@139.0.11.41.ac.id

b. SIP: riki@buddhi.ac.id. You can also add parameters such as type (user = "phone") or transport protocol.

c. Another form of SIP addressing is a telephone URL (RFC 2806) as a telephone number for example: tel: +12125517853 or fax: +385.558.6820.

3. The process of registering and calling the SIP protocol

When a user runs a SIP client user that can be a SIP IP phone, PC or other SIP device, the client registers himself to the proxy or to the registration server. Registration can also be done when the SIP Client user notifies the server about the location of the user where the registration information is periodically updated and each user must register to the proxy or to the registration server. Proxy or registration server will forward registration information to be stored on the location / redirect server. The registration process is:



Fig 3. The process of registering a SIP User client

While the following is a communication process (call establishment) in the SIP protocol, the stages are [4]:

- User registration process, user recognition and user location determination, then User Agent A initiates a call to User Agent B by sending INVITE signals through Proxy Server, then Proxy Server forwards Invite to Location / Redirect Server which is then forwarded to Proxy Server on User Agent B
- Then User Agent B sends a reply signal to User Agent A and gives the message to accept or reject the call.

- c. User Agent A receives an ACK reply signal from User Agent B in the form of an OK message.
- d. A two-way voice channel is formed in the real-time transport protocol (RTP) and the conversation is carried out between User Agent A and User Agent B.
- e. After the communication process is complete, User Agent B exits and gives a signal in the form of a BYE message to User Agent A
- f. User Agent A receives a BYE message and provides a signal containing an OK message to User Agent B to end the communication process.

4. Order SIP

The SIP component as a whole communicates by exchanging SIP messages between User Agents. SIP messages consist of two parts, namely: Request and Response. When the client sends a request message, the server will respond to this message through a response message. SIP is a text-based protocol where request and response messages use generic messages that are defined on text-based standard messages on the internet. The request and response message consists of start line, one or more header fields (message headers) and empty lines that indicate the end of the header field, and the message body which is the session used for communication, as seen below:

Generic-message = Start line (in message request)
 Status line (in response message)
 Message header
 Empty line
 Message body

Messages in SIP are divided into message messages and message bodies. The contents of the SIP header are in the first line, in the form of the request method, INVITE, then the call destination address (Request URL) and the SIP version number used. While the message body (message body) is often also referred to as the SDP (Session Description Protocol) message. The message code in SIP has certain criteria such as name fields and blank spaces unless the first line is permitted, header fields that have many values can be combined as comma-lists.

The contents of the SIP message consist of groups of SIP Methods or Requests and SIP Responses. The format of both contents is request and response has the same header and message body. Components in the SIP Request consist of:

INVITE : Start a call by inviting other User Agents to participate in the session
ACK : Confirm that the User Agent has received the final response to INVITE requests
BYE : Indicates call termination
CANCEL : Cancel pending requests
REGISTER : Registering User Agent
OPTION : Used to see the capabilities / capabilities of a server
INFO : Used to carry information outside of calls such as DTMF digits.
COMET : Initial conditions have been met (Precondition Met)
PRACK : Provisional Acknowledgment
SUBSCRIBE: Register to the event
NOTIFY : Reminds subscribers
REFER : Ask the recipient of the message to announce the SIP request (Transfer call).

While the contents of SIP Responses contain a numeric code with an outline of the order rules in the form of [5]:

1xx : Information messages
 100 : Try
 180 : Calling (Processed locally)
 181 : Call forwarded
 182 : Queuing / waiting
 183 : State of the session
2xx : Response or answer has been successful
 200 : Ok
3xx : Redirection response
 300 : Give choices
 302 : Temporary disposal
 380 : Alternative server
4xx : Request error message (Request)
 400 : Request wrong (Bad Request)
 401 : Unauthorized

- 403 : Forbidden
- 404 : Not found
- 405 : Wrong method
- 415 : Content not supported by this protocol
- 420 : Incorrect extension
- 482 : Tested loop conditions
- 486 : It's busy here
- 5xx : Error message on server
- 500 : Error on internal server
- 501 : Not implemented in this Protocol
- 503 : Not available
- 504 : Time runs out
- 6xx : Global error messages
- 600 : All busy
- 601 : Refuse
- 604 : None
- 605 : Not acceptable

the message code written above is the message code that most often appears in SIP communication. SIP responses can be shown as shown below:

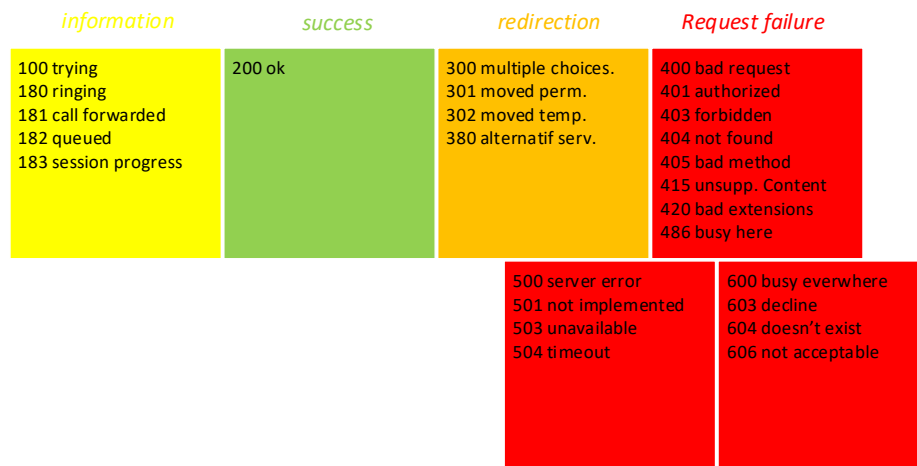


Fig 4. SIP Response

IV. RESULTS

Configuration Design

This configuration design is divided into several stages, namely: Numbering method, Installing Software on the Server and in the Client (User), and Setting Parameters in the Server and in the Client (Use). Because of the limitations of the author and ease of understanding, in this scientific work the author uses the 3cxphonesystem program that runs on the Window operating system and programs on the side of the Proxy server and X-lite on the Client side.

Numbering Method

Based on the network management policy that applies in the university environment, where bandwidth allocation for VoIP communication goes out of the campus network environment is eliminated, then VoIP communication will be carried out on a campus scale.

The addressing used in this scientific work is the use of numbers with 3 digits arranged in the form of: *YYY @ IP_user*. *YYY* is a number given to the user based on an agreement and arrangement that aims to facilitate identification. *IP_user* is the user's computer IP around the environment of the electrical engineering department that is connected to both wireless access media and LAN cable

V. DISCUSSION

Analysis of VoIP Network Needs

VoIP network design has the ability and limitations in its implementation. The capabilities of this VoIP network are as follows:

1. Save telephone costs up to 70%, because IP is global. For Long Distance Direct (SLJJ) and International Direct Dialing (SLI).
2. Can reduce maintenance costs, because voice and data networks are separate so that IP phones can be added, moved or changed.
3. Able to store information about each user
4. Save the conversion database from a telephone number to an IP number or vice versa so that the transmitted packet voice data will reach the correct destination.
5. Translating telephone network standard numbering or private numbering to the IP address.

While the limitations of this VoIP network are:

1. Delay that occurs on large internet networks reaches 500 milliseconds, while on PSTN only reaches 50 to 70 milliseconds.
2. Having a large loss of package (Loss Packet).
3. Service quality (QoS) is influenced by several components, such as delay, jitter, and echo.

In addition, according to its characteristics, this VoIP network is likely to experience an error or reduction in bandwidth if:

1. Many additions to the network.
2. Increased applications run by users.
3. Data traffic on the existing LAN increases
4. Many installation of additional computing facilities for clients and servers.
5. Graphic service intensive applications are increasing.
6. There are several new LANs connected.

Location Analysis

as a VoIP network center node that is designed to take advantage of existing locations that are placed in one room, for example: Computer Laboratory, which has been installed in this space will be drawn distribution points using Wireless to each VoIP network client. As for no room connected but all handhelds owned by employees can be connected to the VoIP node with a 3 digit limit starting from 100-999 line. The LAN cable layout in the VoIP network design can be seen below:

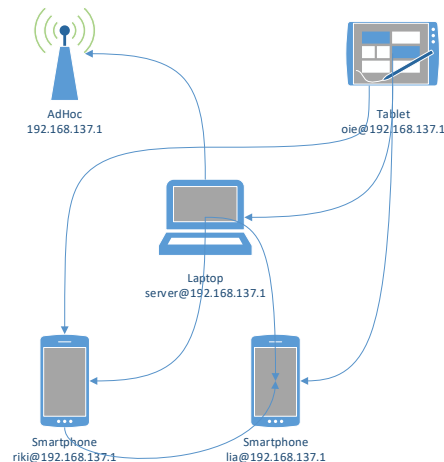


Fig 5. VoIP Network Layout

Analysis of Devices Used

The main device components used to build VoIP networks are server computers, WiFi switches. The hardware specifications used will be explained in this section. Here we will use 4 for devices that will be tested, based on the table below:

Table 1. Device Used

No	Perangkat	Spesifikasi	Ext	Name
1	HTC Rhyme	OS : Android versi 4.0 (Ice Cream Sandwich) Processor : 1 GHz Memory : 768 MB WiFi : 802.11 b/g/n	103	Riki (Client)
2	Lenovo S880	OS : Android versi 4.0 (Ice Cream Sandwich) Processor : 1 GHz Memory : 512 MB WiFi : 802.11 b/g/n	102	Lia (Client)
3	Acer Iconia A701	OS : Android versi 4.0 (Ice Cream Sandwich) Processor : QuadCore 1,3 GHz Memory : 1 GB DDR2 WiFi : 802.11 a/b/g/n	101	Oie (Client)
4	3CX Phone Simulation (for PC/Laptop)	OS : Window 8 Pro Processor : AMD APU A6 Memory : 4 GB WiFi : 802.11 b/g/n	100	Server

VI. CONCLUSIONS

Based on the description above, it can be concluded as follows

1. The design form used is Smartphone and PC by using a Wireless LAN system by utilizing the existing protocol in Buddhi.
2. 3CXPhoneSystem will not be connected if the Management Console is not registered first.
3. Make sure the firewall is enabled (inactive) when we want to Communicate.

REFERENCES

- [1] "www.3cx.com," 28 June 2013. [Online]. Available: www.3cx.com.
- [2] O. W. Purbo, Standart, Desain, dan Implementasi, PT ELEX Media komputindo, 1998.
- [3] W. Stallings, Jaringan Komputer, Edisi Bahasa Indonesia, Jakarta: Salemba Teknika, 2002.
- [4] T. Tharom, Teknis dan Bisnis VoIP, Jakarta: Elek Media Komputindo Kelompok Gramedia, 2002.
- [5] "http://www.voip-info.org/," 28 June 2013. [Online]. Available: http://www.voip-info.org/.