VoIP over Vehicular Ad Hoc Network for Inter Vehicle Communication

MINT 709- INTERNET PROJECT

8/8/2013

Subhashree Pugazhenthi

ACKNOWLEDGEMENT

I acknowledge my debt of thanks to Professor M.H MacGregor and Jagdeep Sandhu (Administrator at MD Opportunity) for their aid and foresight.

TABLE OF CONTENTS

INTRODUCTION

1.1 Introduction

Vehicle plays an important role in today's world. Bringing software-based intelligence into vehicles has intensively improved the passenger's quality of life. There is high demand for reliability, safety in automobiles, which resulted in deployment of vehicular networks and its applications. Application provides Internet access such as downloads, e-mail access, etc. vehicular networks also information about the local service such as restaurant, gas station, etc.

Car manufactures with agencies have come up with an idea of providing assistance to drivers. This idea led to Intelligent Transportation Systems, which is the primary reason for inter-vehicular communications. Aim of ITS, is to minimize the accidents and provide better traffic conditions by exchanging the traffic information between drivers by wireless communications. This information exchange mechanism led to VANET (Vehicular Ad Hoc Network).

1.2 Project Description

This project focuses on providing Vehicular communication between vehicles through VoIP. Vehicular communication between vehicles provides safety driving avoids accidents and it also alerts and updates the driver about the upcoming roads. Vehicular ad-hoc network (VANET) recently developed inter vehicle communication technology is used in this project, were each vehicles communicate among them forming a wireless link between themselves. There are two types of communications, Vehicle to Vehicle communication and Vehicle to infrastructure communication. The vehicles get the signal from nearby infrastructure (example tower) and each vehicle can act as a router and can provide signal to vehicle within the wireless link when needed. Vehicle to vehicle communication happens through Wi-Fi. The wireless link between the vehicles might get disconnected due to signal loss, interference, noise, etc. If a vehicle gets disconnected from the link, the next reachable neighborhood vehicle gets connected to the link automatically. The link between the vehicles gets restructured dynamically.

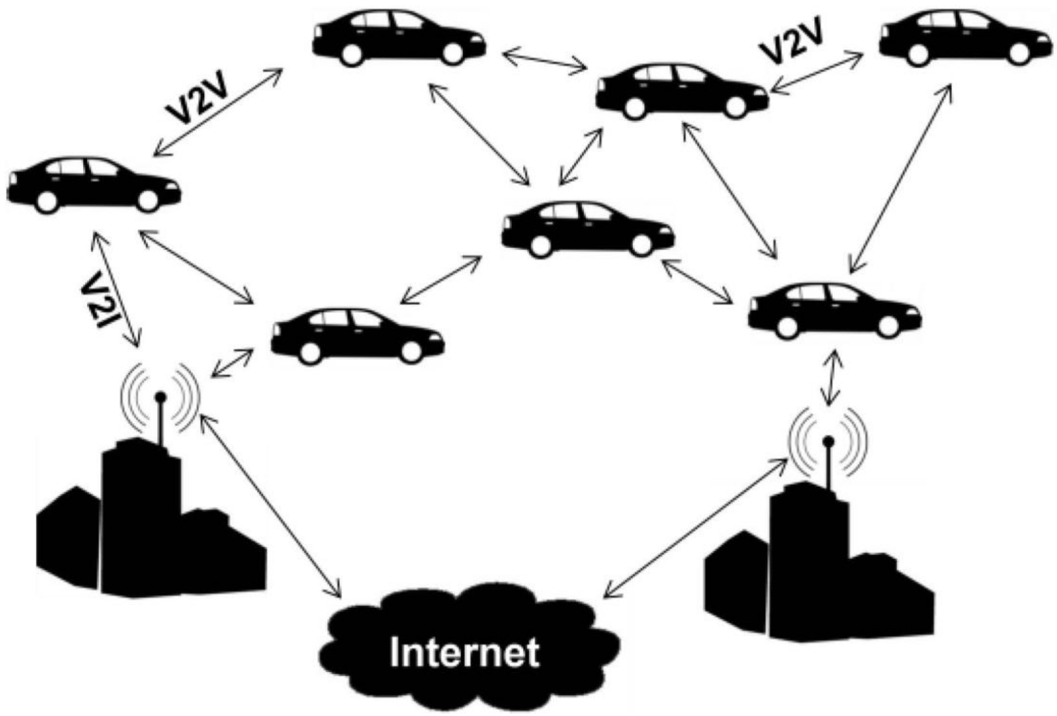


Fig 2.1: VANET

VoIP allows making calls using Internet instead of analog phone. VoIP converts the analog voice signal to digital and compresses the digital voice signal and transmits as packets to the destination. Analog to digital conversion and compression are done through CODEC. CODEC such as G.711, G.723.1, and G.729A can be used. SIP stands for session initiation protocol is used in this project for initializing a call, controlling and terminating a call.

1.3 Project Objectives

The key features required for the successful implementation of this project are,

1. VANET Device
2. VoIP Server
3. VoIP CODECs support : SpeeX, Opes, G.711, G.723.l, and G.729A
4. VoIP Client Softphone Application

Development Platform

In this project, Raspberry Pi with Debian Linux Operating System is required to build a Voice over VANET system. It performs two major roles of being the VoIP Server, and the VANET Device.

Reference:

http://downloads.raspberrypi.org/images/raspbian/2013-07-26-wheezy-raspbian/2013-07-26-wheezy-raspbian.zip.torrent

VANET

Raspberry Pi (server) makes use of wireless connectivity to form a Vehicular Ad-hoc Network. Raspberry Pi makes use of wired Internet to transforms itself into a Wi-Fi access point by means of a Wi-Fi dongle. Required drivers were installed to make the Wi-Fi dongle functional.

Reference:

https://github.com/jenssegers/RTL8188-hostapd/archive/v1.1.tar.gz

VoIP Server

VoIP server is needed to test VoIP over VANET functionality. Asterisk is installed on Raspberry Pi and it is configured to support VOIP calls.

Voice CODECs

FFMPEG CODEC is installed on Raspberry Pi and the required configurations are updated to support following CODECs: SpeeX, Opes, G.711, G.723.l, and G.729A.

VoIP Client

Portable android devices are used to test VoIP over VANET. Android based softphone application is installed on the android device, to make VoIP calls in VANET. To make VoIP calls in android phones, softphone application called CSIPSIMPLE is installed. The Android phones were registered with the server to makes Voice calls over Internet. The Screen shots of registering the phones are shown in the result.

Once the phone gets registered with the server, the communication happens between the peers through Wi-Fi. For instance, vehicle 1 (already registered with Raspberry Pi server) is connected to different network and vehicle 2 is connected to the server (Raspberry Pi). If in case vehicle 1 gets disconnected from its network, it automatically gets connected to vehicle 2 which also acts as a Wi-Fi hotspot. Now both the vehicles are connected with each other and are ready for data exchange.

Test VoIP on VANET

The VANET test environment is created and voice calls were tested between two Android based portable devices with various voice CODECs.

Note: The above features were successfully implemented and the output is shown as screen shots in Chapter 8.

1.4 Problem Specification

Vehicular networks have no definite infrastructure. Unlike other networks the vehicles rely on themselves to provide network functionality. Due to mobility restraints, driver's behavior and change in topology and connectivity in VANETs is not guaranteed always.

When vehicles are far apart, there is a lack of connectivity and this can be an advantage, as there is a low risk in terms of safety, but on other hand commercial application requires constant connecting to enable data sharing.

This research aims to deliver how vehicular networks will perform under realistic vehicular environments and performance of VANET which uses Wi-Fi for Inter Vehicle Communication and also for Vehicle to Infrastructure communication.

VOICE OVER INTERNET PROTOCOL

2.1 Introduction

Information exchanged over public telecommunication network is mostly voice. ISDN and voice communication use digital technology and provides services through circuit switching. This provides a dedicated path between the source and destination. This method provides a fixed Bandwidth and less latency. It doesn't require complicated coding algorithm, provides fixed bandwidth and less latency.

Another technology which provides service through packet switched network. The data are divided equally into packets. Each packet has it destination address on it and is routed independently through Internet. This concept is ideal for non-voice data, where throughput is more important than latency and jitter, hence sending voice data will lead to poor and degraded quality.

VoIP needed to transmit voice over a packet switched network. VoIP helps to transmit voice over Internet, but yet the quality is not good as circuit switched network. There is abundance of activity to improve the voice quality.

2.2 What is VoIP?

VoIP is a technology that delivers Voice Communications over Internet Protocol (IP). This communication allows making phone communication over broadband Internet connection instead of typical Analogue telephone lines. VoIP service allows you to make and receive calls to and from land-line phone by using special adapters and some VoIP services require computers or a dedicated VoIP phone. Some common VoIP services are IP telephony, Voice over broadband, broadband telephony, Internet telephony, IP communications, and phone service using Broadband. VoIP is also referred as Internet Multimedia subsystem (IMS).

Internet telephony provides voice, fax, SMS and voice messaging over public Internet instead of Public switched telephone network (PSTN). VoIP telephony is similar to digital telephony in signalling, channel setup, digitization of the analogue voice signals and encoding. Both differ only in way of transmission. Digital telephony signal are transmitted through circuit-switched network whereas digital information is packetized and transmitted over Internet Protocol.

Technology required for an IP telephony solution can be split into four categories:

- **Signalling**: Signalling is used to create and manage connection between endpoints and also to manage calls between the endpoints.
- **Encoding**: Analogue signal produced by human voice should be encoded into digital for transmission across IP network.
- **Transport**: IP network must make sure that real-time conversation is transported and acceptable voice quality is produced.
- **Gateway**: It is necessary that IP telephony system needs to be converted by a gateway to another format.

2.3 VoIP Architecture

VoIP architecture is partitioned into signalling and media transfer. Signalling covers, endpoint naming and addressing and concrete protocol functions such as parameter negotiation, access control, billing, proxy, NAT traversal. Depending on the architecture, quality of service and device configuration may also be part of signalling protocol.

Media transfer includes encapsulating data, with support for multiple codec and content security. Commonly used media transfer is RTP.

2.4 Requirements, Availability, and Service Limitations

2.4.1 Requirements

- VoIP requires Internet connection through an ISP
- VoIP service to phone lines and VoIP software to place calls
  Plain Old Telephone Service (POTS) requires none of the above prerequisites

2.4.2Power Outage

VoIP becomes unavailable because VoIP devices such as Routers, computers, adapters require power to function. Traditional phone lines are usually available during power outage, which is a major advantage in an emergency. UPS can be used with VoIP installation to avoid discrepancy during power outage.

2.4.3Bandwidth

VoIP communication requires high-speed Internet connection for reliable functionality. There are chances of calls drops or degradation of quality due to high Internet traffic.

2.5 VoIP Configurations

2.5.1 Dedicated routers

Analogue telephones can be used to make VoIP calls; all that is needed is high speed Internet. DSL modem is required to provide Internet and the phone adapter is needed to make calls using traditional telephones. Once the adapter is connected to the phone, acts like a standard phone. Modem is connected to adapter and adapter is connected to phone. Once this setup is done with appropriate VoIP provider and service plan, VoIP calls can be made without any special software. Pick the phone and dial a number once the dial tone is heard.

Fig 2.1: Dedicated Routers

2.5.2 Dedicated VoIP Phones

VoIP phone looks like an ordinary corded or cordless telephone. It is connected directly to the computer network rather than traditional telephone line. Dedicated VoIP line consists of a phone, base station that connects to the Internet. It can also operate on local wireless network. Like VoIP adapters mentioned in previous paragraph, it requires provider and VoIP service plan to make calls.

2.5.3 Software based VOIP application

Softphone is the application that allows making calls from Computer directly with need of headset, microphone and sound card. Software based services are free mostly for PC to PC communication. The Softphone software has to be installed on the computer should be registered for free account to make free calls. Software based VoIP applications are quite attractive among consumers, as consumers have most of the components required to make calls. Skype is one of the software which allows making free calls upon same service.

Pros of Software based VoIP application:

- Key benefit of VoIP/IMS are low cost and its flexibility.
- Free International calls can be made by using the same service.
- Quick and easy to get started with Softphone.
- Some Softphones provide voicemail, video-conferencing facilities

Cons of software based VoIP application:

1: Call quality is not as good as with hardware based services

2: Softphones are more vulnerable to spam and security threats.

2.6 Cost of VoIP

The communicating machines need same service on their machine to make free calls, whether it is local or international. However to make and receive calls from mobile phones or PSTN, the service is no longer free, but the charge is cheaper.

2.7 Complications in VoIP

- The number and complexity of various features integrated in a product is the largest source of complexity.
- VoIP systems operate in various environments, business settings and network conditions. The above mentioned should have considerable configurability. If not it might lead to complexity.

- VoIP generally works over public data network or enterprise operator network that uses same underlying technology. There is a considerable amount of non-VoIP infrastructure that is critical for the correct operation of the system.

Because of this complexity, both in terms of configuration options and size of code base, VoIP systems represent a very large attack surface.

2.8 Threats in VoIP

2.8.1 Social threats

Social threats due to problems in configurations, bugs or bad protocol interactions in VoIP system may lead to misrepresentation of malicious parties to users.

2.8.2 Physical access threats

This refers to an unauthorized physical access to VoIP equipment or to the physical layer of the network.

2.8.3 Interruption of services threats

This refers to Non- intentional problems that cause VoIP services to become unusable or inaccessible. This might be because of loss of power due to weather, degrade of call quality.

2.8.4 Service abuse threats

This refers to improper use of VoIP services, especially when services are offered in a commercial setting. These threats include toll fraud and billing avoidance.

2.8.5 Spoofing

The attacker could create a fake caller ID into ordinary VoIP call. The receiver believes that call comes from a trusted source (bank). The receiver discloses all the personal information such as account number, etc without knowing that it is a fake call.

2.8.6 Spam over Internet telephony

E-mail spamming, sending commercial messages using VoIP is fast and cheap. Unlike traditional telemarketing, VoIP offers large volume of unsolicited calls. There is a wide array of tools available for attackers on the Internet. Telemarketers can easily send large amount of messages to VoIP customers. Spam email messages sent by traditional way require only 10-20 kilobytes whereas VoIP requires megabytes of storage.

2.9 H.323

H.323 is ITU- T standard, which provides a set of protocol required to send voice, data, and video conferencing over packet based networks. This protocol is designed to operate above the transport layer to provide real-time communication, but H.323 is now superseded by SIP.

Multiplex and complex levels of signalling are used to initiate and complete the call, especially when VoIP users communicate with PSTN subscribers, hence signalling protocols plays an important role in VoIP. H.323 or SIP makes up a complete set of IP telephony protocols.

2.9.1H.323 VoIP terminal elements

- Terminal
- Gateway
- Gatekeeper
- MCU

Terminal can be either Personal computers or stand alone device, which can run H.323 or multimedia applications.

Gateway is required when communication is going to happen between two different networks. It provides a protocol translation and media transcoding and acts as an interface between the networks. Gateway provides data format translation, control signalling translation, audio and video codec translation, call setup and termination function on both sides. Gateway is optional, but it’s very useful

The endpoints must be registered with the gatekeeper when it exists. Gatekeeper provides services such as address translation, admission access control of end points, bandwidth arrangement and routing capability. Networks with VoIP needs gatekeeper to translate the E.164 Telephone number to Transport address.

Functions of gatekeeper:

Address Translation- Translates E.164 to Transport Address using translation table.

Admission Control – It authorizes the network access using H.225 messages.

Bandwidth Control- It controls the bandwidth used by the terminal.

Zone Management- The above functions for terminal, Gatekeeper, Gateway and MCU have to be registered within its zone of control.

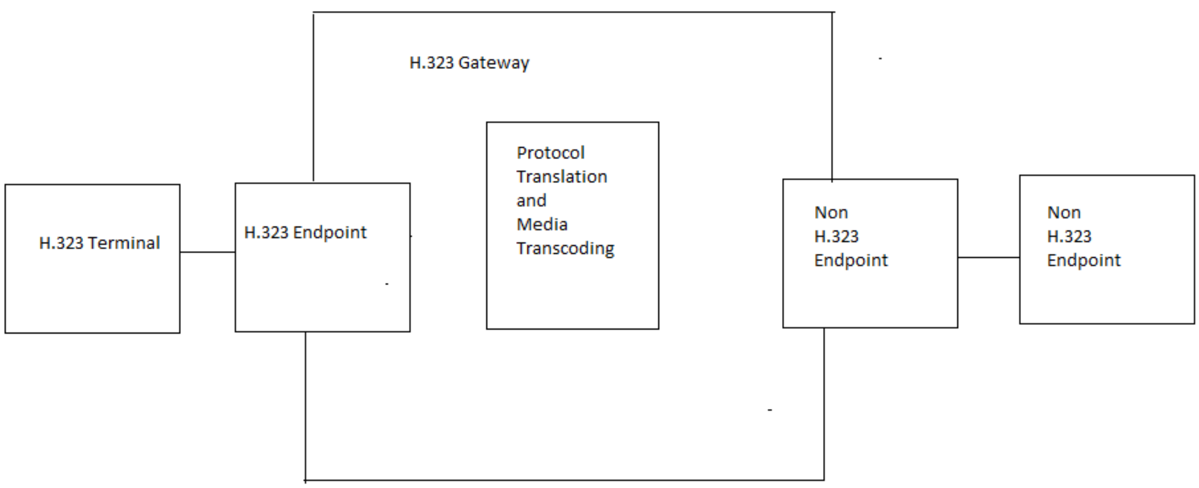


Fig 2.2: H.323 VoIP Terminal

Once an endpoint is connected to the network, RSA (Registration Admission and Status) channel carriers the messages between the endpoint and gatekeeper to associate endpoint E.164 telephone number with IP address and port number, which is required to make call signaling. H.323 uses Q.931 messages to call signaling.

In network with no gatekeeper, endpoint can send signal message directly to the called endpoint using Call Signaling Transport Address. If the gatekeeper is available in the network, the calling endpoint sends the initial message to gatekeeper's RAS channel Transport Address. Gatekeeper then decides whether to send calling signal directly or route the calling signal through the gatekeeper.

Hence there are two types of calling signal

- Direct endpoint call signaling
- Gatekeeper routed call signaling

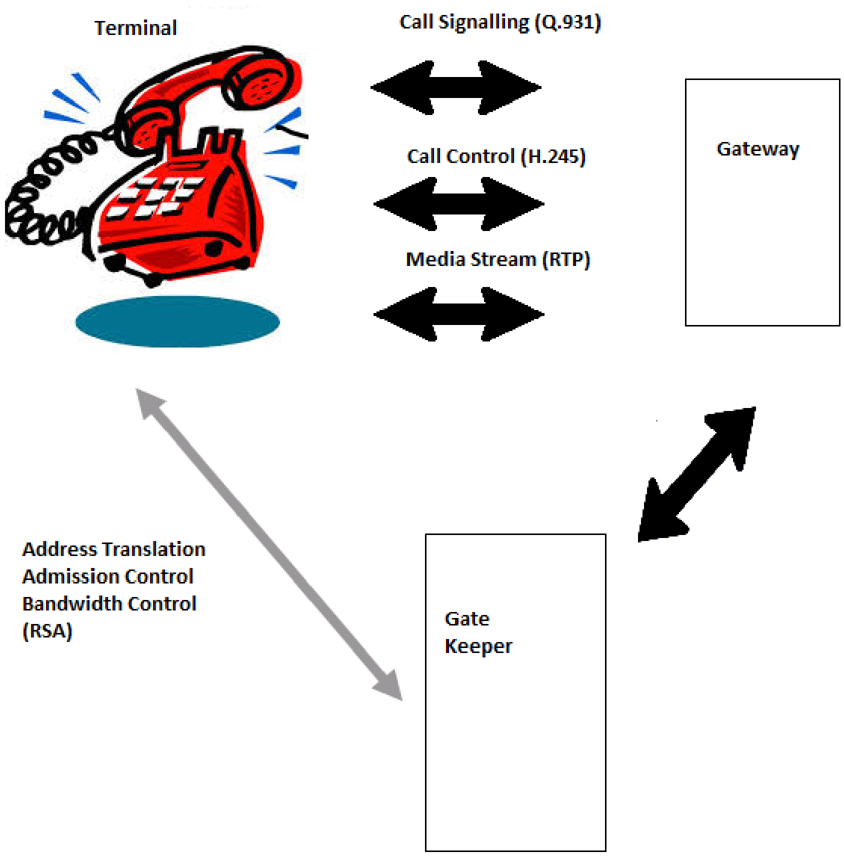


Fig 2.3: Direct Endpoint Call Signaling

2.9.2 Benefits of H.323

Codec Standards: H.323 performs compression and decompression of audio and video data streams, which allows two different endpoints to communicate.

Platform and Application independence: H.323 is not tied to any hardware or operating system and H.323 is available in different size and shapes.

Multipoint Support: H.323 can provide conference between three or more endpoints without any specialized multipoint control unit.

Multicast Support: Multicast has a feature of sending single packets to bank of destinations on the network without any replication. This multicast feature is supported by H.323

Flexibility: For instance, a terminal which can only support audio can have conference with terminal that have video or data capability hence allows conference between two different endpoints.

Inter- Network Conferencing: H.323 allows conference between LAN and remote site. It uses common CODEC to minimize the transcoding delays and to optimize the performance.

Reference:

http://web.mit.edu/chintanv/www/Publications/MIT_TPP_Thesis_Chintan_Vaishnav_Final.pd
fhttp://www.us-cert.gov/sites/default/files/publications/understanding_voip.pdf
http://webcache.googleusercontent.com/search?q=cache:cLlqaoL6RScJ:download.microsoft.com/download/b/0/6/b06e9c6e-cf9c-481f-a6ed-c674e82ed1d1/VOIP.doc+&cd=2&hl=en&ct=clnk&gl=ca
http://www.net130.com/tutorial/other/H323.PDF
http://www.f5.com/pdf/white-papers/sip-defined-wp.pdf
http://www.google.ca/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CDYQFjAB&url=http%3A%2F%2Facademiccommons.columbia.edu%2Fdownload%2Ffedora_content%2Fdownload%2Fac%3A140234%2FCONTENT%2Fcip.pdf&ei=rmMIUtitO6TgyQHkpIHIAg&usg=AFQjCNEfgJBFi09qxIuVfnPn2pVtbMU_pA&sig2=g1HG1qEMN

SIP (SESSION INITIATION PROTOCOL)

3.1 Introduction

SIP (Session Initiation protocol) is a signaling protocol, widely used for setting up, connecting and disconnecting communication sessions. The session can typically be voice or video calls over the Internet. SIP is standardized protocol which uses TCP or UDP in most cases. Protocol can be used for setting up, modifying and terminating two users (unicast) or multiple users (multicast) sessions of one or more media streams.

SIP is an Internet Engineering Task Force (IETF) standard used in Voice over IP (VoIP). Current version of SIP is SIP/2.0 and codified as RFC 3261. It is a signaling protocol which initiates, co-ordinates and ends the communication session between the two endpoints. Comparing SIP to traditional telephone, ringing the phone, busy tone and ending the call functions are done by SIP. SIP is used in IP Multimedia Subsystems (IMS) which provides media services in third generation.

SIP defines the following components,

- UA (User agent) - Logical network end point used to create or receive SIP messages.
- UAC (User agent client) - Client in the terminal initiates the SIP signaling.
- UAS (User agent server) - Server in the terminal responds to the SIP signaling received from UAC.
- Proxy Server- Receives connection request from UA and Proxy server routes the request to the targeted user.
- Redirect server- Receives the connection request and send the details about destination to the requester.
- Location Server: Receives registration request from the UA and updates the terminal database with them.

All servers mentioned above are available on a single physical machine called Proxy server, which is responsible for client database maintenance, connection establishing, maintenance, termination and call directing.

3.2 RTP

RTP is used for real time transportation of data. In VoIP, it is used to transmit voice and video. Combining SIP and RTP, VoIP calls can be established. VoIP call between two peer uses SIP protocol for signaling and RTP for transmission of voice data.

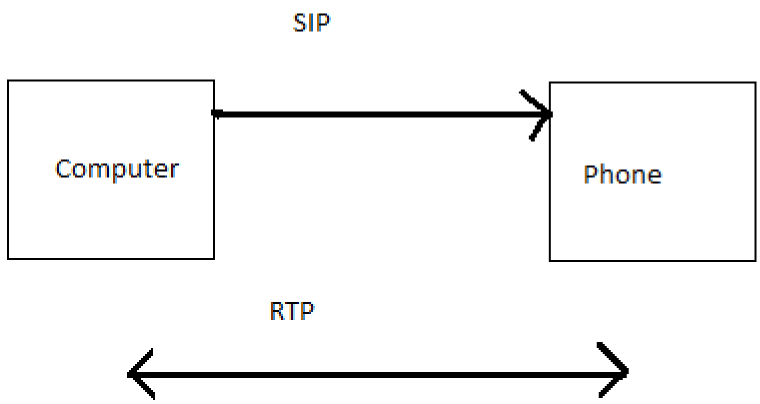


Fig 3.1: RTP Communication

3.3How implementation separates between User agent and proxies

What is User agent?

User Agent is a logical network end-point used to create or receive SIP messages and thereby manage SIP session. It performs the role of User agent client (UAC), which sends SIP request and User agent server (UAS), which receives the request and returns as SIP response.

SIP Proxy Server

Proxy server is used to perform call processing, setup calls between SIP devices, controlling call routing, etc. It makes a request on behalf of other clients; hence it acts as both server and client. Main purpose of proxy server is routing and makes sure that request is sent to another entity, close to targeted user.

SIP proxy is comparable to mail server or web server and as mentioned above user agents are client applications or terminals separated by end users. The architecture is similar to Internet mail, the end user device may frequently change its IP address or user may use different devices or device might be turned off, but SIP proxy provides a constant location, which is always on and waits for the incoming call and routes it to the particular recipient. Once the connection is made through SIP protocol, RTP connection will be created between the two end points with no intermediate server. SIP protocol is a lightweight protocol and SIP proxy can easily service millions of calls per second.

3.4 Initiating a SIP call

Redirected Server:

The server receives the request from a client and replies back to the client with current location of the particular user is called Redirected server

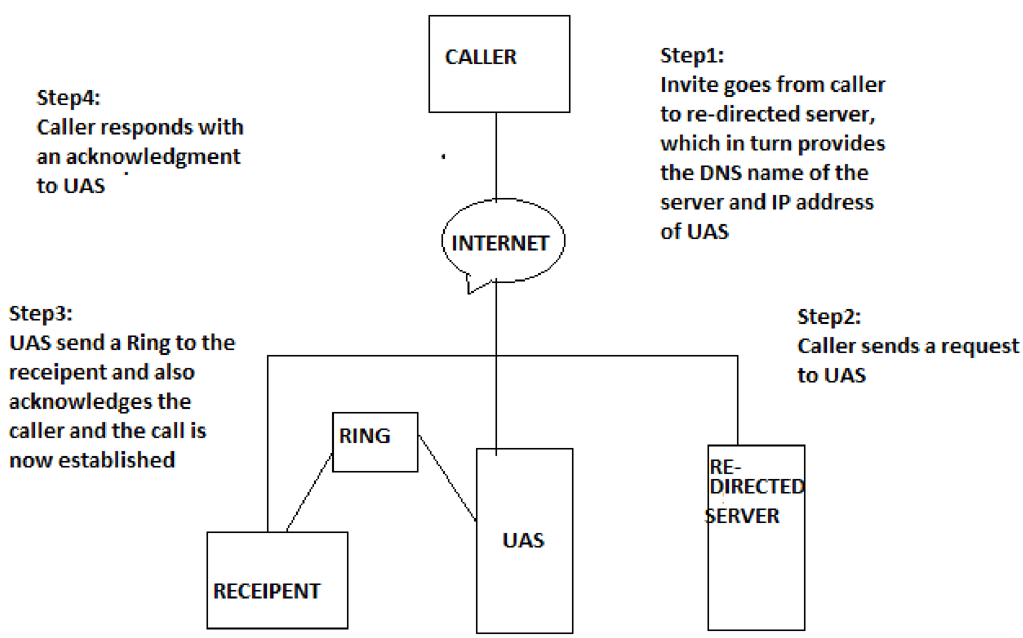


Fig 3.2: SIP Interface

3.5 Message sent in SIP

- INVITE – Connection establishing request
- ACK- Acknowledgement

- BYE- Connection termination
- CANCEL- Cancellation of non-established connection
- REGISTER- UA registration in SIP proxy
- OPTIONS- Inquiry of server options

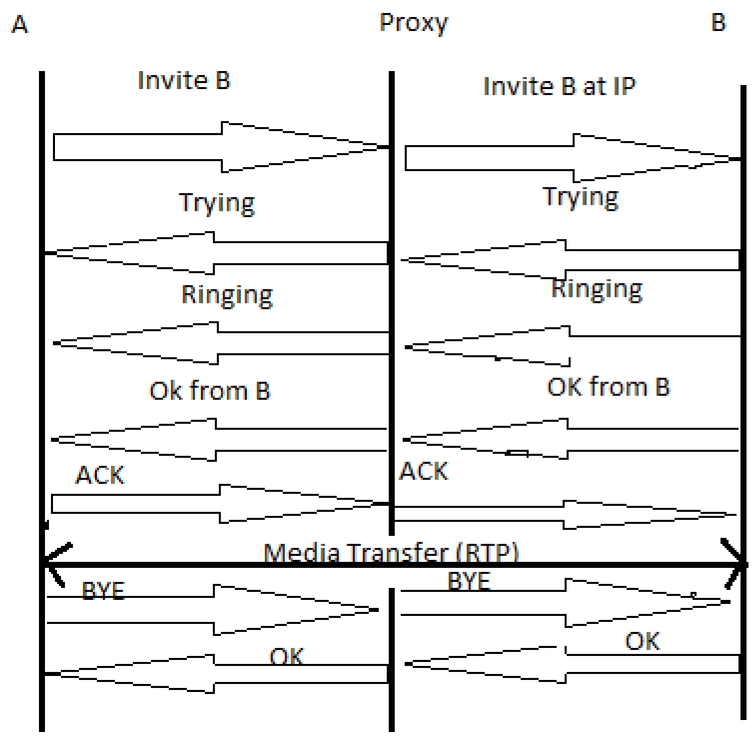


Fig 3.2: SIP Message handshake

Two Main features that differentiate SIP are: Splitting / Forking:

SIP provides ability to split an incoming call so that several extensions ring at the same time from the same single originating call. The extension which answers first gets the call. Once it is answered by any one extension, other extension stops ringing. This is useful if the called person is identified as being in one of several locations.

3.7Problems in SIP

- **Firewalls**: Due to firewalls, there are possible chances for two endpoints to receive incoming RTP traffic. Firewall allows incoming UDP packets from an IP address if the endpoint behind the firewall has sent UDP packets to that address. In such cases there is no problem. Some RTP packets might get lost; if both are sending traffic they will also be able to receive traffic. In that case firewall will block the traffic, which in turn needs middle server to route the traffic between the two endpoints.
- **NAT (Native Address Translation):**

For instance, computer in a local network try to access Internet. For Internet connection computer is connected to modem through Router. The Router acts as a Firewall and provides a single external IP address for all computers connected to the local network.

When one of the computers in a local network tries to connected to server. The IP packet that reaches the server appears like it has come from external IP address. The router every time changes the IP address and port number and substitutes it own external IP address and sends it to server. Server sends packets to external IP address, thinking that is the IP address of the computer. Once the router gets the packet it changes the IP address and Port on the packet and sends it to desire computer. This might lead to connection fail if either endpoint is behind NAT.

- Emergency calls cannot be made using SIP. This is still under discussion.
- Interactive Voice Response (IVR) is too difficult for SIP.

3.8 H.323

H.323 is published by ITU-T. This is a protocol like SIP which provides audio-visual communication session on any packet network. H.323 addresses bandwidth control to point to point and multi point conferences, call signaling, multimedia transport and control. This was originally designed for video conferencing and LAN telephony.

H.323 designed for video conferencing and LAN telephony. SIP is designed for multimedia Internet communication. Both SIP and H.323 addresses call signaling, media control, supplementary services, capabilities exchange. The advantage of SIP is that it is backed by IETF. Advantage of H.323 is that much larger piece of the current market.

3.9 Comparing SIP and H.323

- SIP defines only 37 headers while H.323 defines hundreds of elements.
- SIP encodes message as text while H.323 uses a binary representation of the message.
- SIP is simpler than H.323 and easier to support than H.323
- SIP provides more features than H.323 such as it can send JPEG image, business card so that the called user can know who is phoning. But these features are not available in H.323.
- H.323 is limited to loop detection in complex multi-domain. SIP uses a loop detection method by checking the history of message in the header fields and can be done in stateless manner.

3.10 SIP conclusion

SIP is simple, open protocol that can be deployed in carrier and enterprise networks. It provides multimedia applications in voice, data and video. This replaces H.323 in many areas.

References:

http://www.voipmechanic.com/sip-basics.htm
http://openlife.cc/system/files/FSWC%20Henrik%20Ingo%20Article%20SIP,%20VoIP%20and%20FLOSS.pdf
http://web.uct.ac.za/depts/commnetwork/eee5026/note/eee526-06-640sip_introduction.pdf
https://www.cs.columbia.edu/~smb/classes/f06/l13.pdf

VEHICULAR AD HOC NETWORK

4.1 Introduction

Taking into account of increasing demand for car safety, there are numerous vehicular network introduced, which provides critical safety application. Due to the demand, devices have tend to research on self organize and self healing networks without interference with centralized or pre-established infrastructures. One of such networks which have received a lot of interest is VANET. It has tremendous potential to provide improved vehicle and road safety, traffic efficiency, comfort to both drivers and passengers.

Vehicular Ad hoc Networks is subclass of Mobile ad hoc Networks (MANETs). VANET helps vehicle drivers to communicate and co-ordinate with each other to avoid any road accidents, traffic jams, speed control, free passage of emergency vehicles etc. Apart from this VANET also provides applications such as weather information and other multimedia applications and know applications include ADASE2 (Advance Drive Assistance Systems, Crash Avoidance Matrices Partnership (CAMP) etc.

Main features of VANET Architecture,

- Low latency required for safety application.
- Extension growth of multimedia and interactive application.
- Increase in security concerns.

4.2 Network Architecture of VANET

VANET is categorized into three namely, pure cellular/ WLAN, Pure ad hoc and hybrid. In pure cellular/ WLAN architecture the network uses wireless access points and cellular gateway to connect to Internet. Communication with Internet while driving is either by cellular tower or wireless access point. There is limitation with pure cellular as cellular towers and access points are not available everywhere. Nodes may also engage in communication with each other.

In Pure ad hoc network, nodes communicate with each other and this network has no infrastructure .When the vehicles are equipped with wireless networking devices, they use cellular tower and access point to communicate with each other.

Hybrid architecture is combination of cellular/ WLAN and ad hoc network, which provides rich content and greater flexibility in content sharing. Similar to MANET nodes, VANET are self-organize without a centralized authority. This type of network, nodes acts as a server and client thereby exchanging and sharing information with each other. VANETs have a few distinguishing characteristics which makes it a challenging class of MANETs

4.3 Characteristics of VANET

- **Node**: Provides high number of nodes in a link.
- **High mobility and frequency topology changes**: Changes the topology according to the nodes and provides high mobility.
- **Data Delivery**: Main purpose of VANET is to provide safety and the data has to be delivery on time without any delay.
- **No confidential of safety information**: Safety information is delivered right away and no confidential of safety information.

- **Privacy**: A communication capability in vehicles reveals the information about the users such as speed, identification, mobility pattern. In spite of non-repudiation of safety messages, privacy of users should be respected.

4.4 Routing Protocols

There are three Routing Protocols used namely:

- Proactive routing protocol
- Reactive routing protocol
- Position- based routing protocol

4.4.1 Proactive routing protocol

Routing protocol employ DSDV (Distance Sequenced Distance Vector), OLSR (Optimized Link State Routing Protocol). The protocol keeps updating information about the routing among all the nodes of a network. It updates the routes even if that particular route is not currently used. Updates are done periodically regardless of network load, bandwidth constraints and network size.

4.4.2 Reactive routing protocol

This protocol overcomes the Proactive routing protocol. It updates and maintains the routing information only for the active routes and reduces the burden on the network. Dynamic Source Routing (DSR) and ad hoc on-demand Distance vector (AODV) are the reactive routing protocols used.

4.4.3 Position based routing

This protocol needs the physical position of the nodes available to provide service. Sender requests the position of the receiver by means of location server. Depending upon the position, the packet is sent to receiver by its neighbor nodes. Greedy Perimeter Stateless Routing (GPSR) and Distance Routing Effect Algorithm for Mobility (DREAM) is position based routing algorithm.

4.5 Types of Communication in VANET

Inter vehicle Communication:

Configuration of Inter Vehicle uses multi-hop to transmit traffic information to group of receivers. In intelligent transportation systems are worried only about the activity of road ahead and not behind.

Types of message forwarding:

- Naive broadcasting
- Intelligent broadcasting

Naive broadcasting:

Broadcasting in Naive broadcast is done periodically and at regular intervals. Vehicle ignores the message, if it receives the message from a vehicle behind it. This means all the vehicles moving in the forward direction receives all the messages broadcast.

Limitation of Naive broadcasting:

It generates numbers of broadcast messages, which leads to message collision, resulting in less message delivery and increased delivery time.

Intelligent Broadcasting:

This resolves the problems of Naive broadcasting by limiting the numbers of message broadcast for an emergency event. Concept is, if the vehicles receives the message from vehicle behind, it assumes that at least one vehicle at the back has received it and ceases the broadcasting. The vehicle behind will be responsible for sending it to rest of the vehicles. If the vehicle receives it from more than one source, it acts according to the first message received.

4.6 AD Hoc Network

Ad hoc is decentralized wireless network. It doesn’t depend on pre-existing infrastructure such as access points or routers in wireless networks; instead each node acts as router and forward data to other nodes. Depending on the network connectivity the forwarding node is determined. It also uses flooding for forwarding data. Ad hoc is made of multiple nodes which are connected by links. The links are influenced by signal loss, interference, noise and reliability. Link is connected or disconnected any time; network must be able to dynamically restructure the links. Network allows two nodes to communicate by relaying the information via other nodes. Decentralized nature of wireless ad hoc network makes it suitable for a variety of networks.

4.7 Classification of Ad hoc network

- MANET
- Wireless Sensor Network
- Wireless mesh Network

MANET:

MANET is self- configuring network, in which devices are connected by wireless links. MANET has routing network environment on top of link layer ad hoc network. Each device in MANET is free to move in any direction and the link changes accordingly. VANET is a subgroup of MANET.

Wireless sensor network:

It consists of spatial distribution of autonomous sensors which monitor physical and environmental condition such as temperature, sound, pollution, pressure, etc. Modern network are bi-directional and also enables control of sensor activity.

WMN:

It provides delivery of Internet broadband, wireless LAN, network connectivity for both operators and customers at low price. WMN allows users to be connected to Internet always by connecting them to wireless mesh routers. Mesh routers have bridge functionality to connect WMN with cellular, wireless sensors, Wi-Fi and WiMax.

4.8 Application of Ad hoc network:

- Area Monitoring
- Visitor Tracking system

- Air pollution detection
- Green house monitoring
- Forest fire detection
- Agriculture

4.9 ITS (Intelligent Transportation Systems)

It is an information and communication technology applied to transport infrastructure and vehicles. It improves transport safety, transport productivity, travel reliability etc.

4.9.1 Wireless communication technology

Radio Modem communication:

It is a private radio network, which is used in industrial critical application were real time data is need. They are independent of telecommunication or satellite network. They use licensed frequencies in either UHF or VHF. Frequency range of UHF and VHF are 300MHz-3GHz and 30MHz-300MHz respectively.

Short Range Communication:

Its uses Dedicated short range communication for active safety of vehicular to vehicular communication (V2V) and vehicular to interface communication (V2I). Short range communication offers latency, accuracy and reliability.

Long range communication:

It is purposed with infrastructure network such as Wi-Fi, WiMax, GSM, and 3G. Unlike short range, long range requires expensive infrastructure deployment.

4.11 Application of ITS

Emergency vehicle notification system:

In-vehicle e-call is emergency call generator which connects to nearest emergency point automatically. In-vehicle sensors are activated after an accident or by manually making a call. It can carry both data and voice. The voice call enables the user to talk to a trained e-call operator and minimum set of data which contains information about time, precise location of accident, vehicle identification are sent to nearest emergency point.

Auto road enforcement:

Traffic enforcement camera system consists of camera and vehicle monitoring device which detects the vehicles exceeding the speed limit at that particular area. When the vehicle exceeds the limit the camera takes the pictures of the license plate number and the device generates the ticket and it's sent through e-mail.

4.12 VANET in ITS

Transport systems are made more intelligent by bringing VANET in ITS. Main feature of ITS is providing safety application. VANET enables ITS to provide better safety application, as VANET provides information about the road curves, traffic, congestion update etc. Apart from traffic, it also supports electronic toll collection, Internet access, weather updates, etc. ITS provides a better service with VANET.

Research in VANET field: VANET is technology that significantly improves the quality of transportation systems. There are several research projects in VANET fields are developed.

References:

http://www.google.ca/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CC4QFjAA&url=http%3A%2F%2Fscholar.sun.ac.za%2Fbitstream%2Fhandle%2F10019.1%2F17881%2Fmojela_on_2011.pdf%3Fsequence%3D2&ei=e1gIUvfLEqP8yAH5x4GgAQ&usg=AFQjCNGmq1nNxr5rOn8G75ajxgEwlPVubA&sig2=SmRHa-o1r_vslAC3uUJSTg

VOIP OVER VANET

5.1 Introduction

VoIP provides a good service over VANET. In this project VoIP over VANET is implemented real time. For this, various voice codec and their voice quality will be analyzed focusing on inner-vehicular voice communication. Vehicular traffic generator provides information about roads and this mobility information is used to achieve good results.

Mobile ad hoc networks are independent networks which consist of mobile nodes equipped with wireless communication, network capabilities. Nodes communicated without any network infrastructure. This network opens the way for emergency networks, wireless sensor and vehicular ad hoc networks (VANET) etc.

VANET are specific class of MANETs providing information that helps drivers to have a safe and comfort driving. VANET have several constraints such as high mobility, frequently changing and unpredictable topology, hard delay, which distinguishes VANET from other mobile ad hoc networks.

VoIP over Internet Protocol is a technology that allows making voice calls using an Internet connection instead of regular phone line. To provide better quality of service, VoIP should be limited to end to end delay and packet loss rate. Quality of service also depends on the type of voice codec used. CODEC performs analog to digital voice conversion and digital compression.

5.1.1 VANET

Vehicular ad hoc network supports intelligent inter- vehicle communication to have a safe and secure driving. VANET are categorized into vehicle to infrastructure (v2I) and vehicle to vehicle communication (V2V).

5.1.2 Application issues

VANET applications can be characterized into two groups. First group focuses on enabling the delivery of messages and file to the target receiver. This group is time sensitive. Second group focuses on connecting Internet using roadside beacons or through inter vehicular communications.

5.1.3 Network issues

Network layer provides wireless multi-hop communications. Routing protocol such as unicast, multicast, broadcast, geocast match most of the aspect, but they don't provide high-speed mobility and high nature of unpredictability of VANETs. Most of the routing protocol need to de used or it should be redesigned to behave unique depending on VANETs characteristics and needs.

5.1.4 Mac and PHY protocol issues

MAC protocol was purposed to efficiently share the medium in VANETs networks. Dedicated short-range communication (DSRC), called also IEEE802.11p is used as MAC protocol. This helps in rapid changing of vehicular network environments. IEEE802.11p uses Enhanced Distributed Channel Access mechanism which was originally provided by IEEE802.11e. In the physical layer, IEEE802.11p operates at 5.9GHz band and 5.8GHz band with 75MHz bandwidth divided into seven channels each with 10 MHz frequency band. The center channel is control channel and rest is service channel.

5.1.5 Mobility issues

VANETs vehicular environment presents different requirements such as varying vehicle speed, mobility, traffic lights, obstacles, traffic congestion, driver's behavior, etc. Hence MANET mobility model cannot be used in VANETs; currently there are many road traffic generators to provide realistic simulation of mobility models.

5.2 VOIP OVER VANETs (VOVAN)

The speech source alternates between talking and silence period, which considers to be exponentially distributed. The speech is digitalized by sampling, quantization and encoding.

The speech which encoded is made into packets of equal size and transmitted through Internet Protocol.

In receiver side, encoded speech will be comprised by the payload for a certain duration depending upon the codec used and then reverse processes is performed. The packets are de-packetized and decoded.

5.3 CODEC

CODEC encodes and decodes the packet. Primary function is to convert the analog voice signal to digital and compress the digital signal in order to obtain lowest rate. This is done without degrading the voice quality. CODEC generate constant bit-rate audio frames consisting of 40 bytes IP/UDP/RTP headers followed by payload. CODEC adds additional that will influence the speech quality.

CODEC	Bit rate (Kbps)	Sample Size(Bytes)	Packets per second	Payload Size (bytes)
G.711	64	80	50	160
G.723.1	6.3	24	34	20
G.726.A	32	20	34	80
GSM	13.2	20	50	33

Table 5.1: CODECs Comparison

Primary challenge in designing VOVAN is to provide a good delay performance under constraints of vehicular speeds and unreliable connectivity and fast topological changes. Voice quality is mainly influenced by CODECs. Set of simulations are done to test VOVAN with different voice CODECs.

Reference:

http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6208691&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D620869

ASTERISK

6.1 Introduction

Asterisk is open source, where communication happens in software instead of hardware. This allows new features to be added with less effort and changes can be made according to the needs.

Asterisk was originally written by Mark of Digium, Inc. It is PABX and lot more. It is reliable, free software that turns an ordinary PC which has Linux operating system into a powerful telephone system. It is an open source tool for telephony application and also acts as call processing server.

6.1.1 What is Asterisk?

Asterisk is software that can make a PC with Linux to act as a Telephony server. Asterisk supports high density, redundant applications. It’s an intermediate connecting the Internet and telephony technologies with Internet and telephony applications. It can provide service to any phone, phone line or packet voice connection to another interface or services. Asterisk supports VoIP, SIP, H.323, IAX and BGCP. It can inter-operate with all standards- based telephony equipment. Traditional telephone technologies such as ISDN, PRI and T-carrier are supported by Asterisk.

6.1.2 Why Asterisk?

- **Cost Reduction**: Asterisk can be installed with half the cost needed for an installation of traditional system. For large scale systems the saving can be even greater.
- **Control**: Asterisk allows a business to take control of their entire phone calls. It provides them better and cheaper communication.
- **Integration**: Asterisk can be integrated with Microsoft outlook, CRM and ERP systems. It helps in integrating business systems directly with phone system.
- **VoIP**: Asterisk was basically designed to handle VoIP calls. Provides a Voice calls over IP with free of cost.

- **Reduced Cabling Cost**: Asterisk can also be made to make calls within the office using the existing LAN lines. Hence there is considerable saving of wires as only few set of cables need to be laid.

6.1.3 PABX

Asterisk is software implementation of PABX (Private Automatic Branch Exchange). It is less expensive to use PBX instead of using separate lines for each user in a company. It means, with PABX lines from Telephone Company can be shared among users, instead of providing them each separate line. It provides a place for multiple phone lines to be terminated at company. It services the company by switching calls between company users on local lines and shares the external phone lines. It provides the feature that is not available with Public Switch Telephone Network (PSTN). It provides features like

- Voice mail
- Interactive Voice Response
- Call Waiting
- Conference
- Paging
- Transferring calls etc.,

6.2 Role of Asterisk in Home Office

Consider there is a company at New York and employee works for the northwest region as sales representative and lives in a different location. Employee has a DSL line coming to the home office. The head office has an Asterisk server and high-speed Internet. Caller contacts the New York office by dialing toll-free telephone number of the head office. If caller wants to talk to sales representative at northwest region, the Asterisk server in New York calls the employee. The call is connected through Internet and there are no chargers for long distance communication. If the employee didn't answer the call, the caller can leave message for the employee or can be redirected to sales department.

A small PC will serve many telephone users and with Asterisk telephone system can be easily built for small or large enterprise.

6.3 Connecting Office Telephone System to the Internet

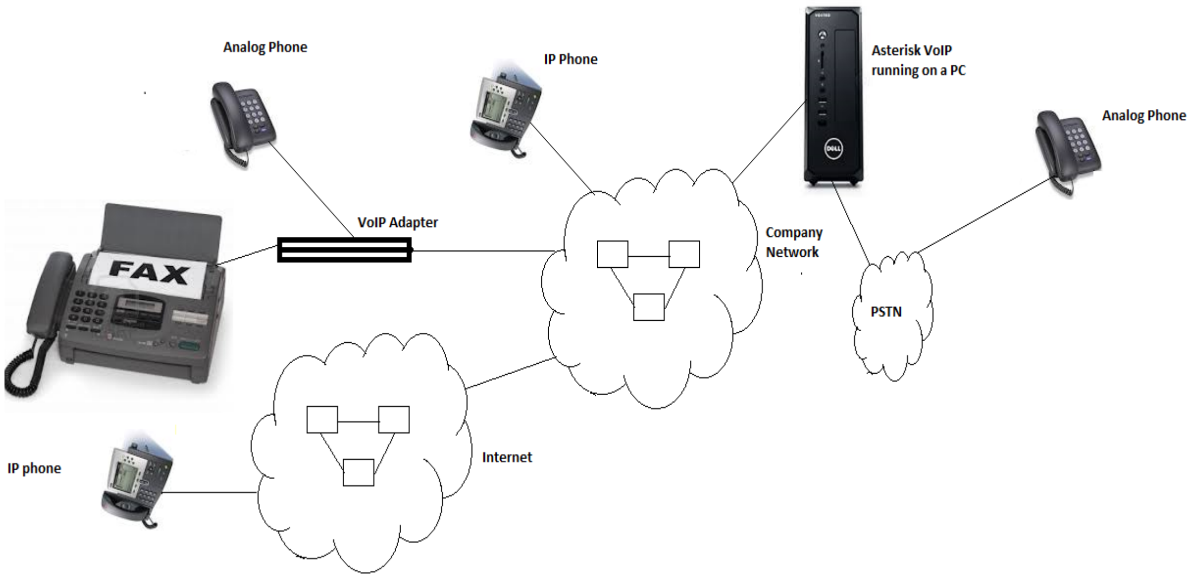


Fig 6.1: Connecting Office Telephone System to the Internet

As shown in the figure, IP phone can be directly connected to the Internet. To connect analog phone or Fax to Internet, it has to be connected through VoIP adapter. Once the Asterisk system is connected to the Internet, any VoIP enabled phone will be able to connect to the Asterisk system and call can be made from Asterisk system to other VOIP or analog phone controlled by the Asterisk system.

Asterisk server connected to local area network can control the phones in that particular network. The phones can call each other through the Asterisk server. Asterisk server can also control the phones of other networks or Interwork, even if the Asterisk server is behind the network. Using Digium FXS interface cards Asterisk can control the analog telephones. T- Carrier and FXO interface boards from Digium can connect Asterisk server with PSTN and Calls can be made to and from PSTN.

6.3.1 Interface and channels:

A call arrives or leaves an Asterisk server through an interface, such as SIP, Zaptel, and IAX. Every call is placed or received over an interface on its own distinct channel. A Channel can be connected to physical channel, like POTS line or logical channel such as IAX or SIP channel.

When a call arrives on a channel, dial plan has to decide what has to be done. It has to decide whether the call has to be answered, connected or forwarded or directed to voice mail.

Applications (e.g. Voice mail) of Asterisk are available to dial plan while processing the incoming call. Dial plan and the application selected determine what Asterisk will do.

SIP channel are used to route calls in and out of an Asterisk server over IP with SIP (Session Initiation Protocol). The call comes in and leaves the Asterisk server through SIP channel.

6.3.2 Inter-Asterisk Exchange (IAX):

IAX is standardized VoIP protocol for Asterisk networking. It provides transparent interoperability with NAT and PAT firewalls. IAX provides call placing, receiving and transferring calls and call registration. Connecting a phone server anywhere on the Internet and registering with home PBX, instant routing of calls can be done.

IAX supports authentication of incoming and outgoing calls. With IAX dial plan polling, dial plan for PBX's can be centralized. Each PBX only needs to know its local extension and if it needs further information, it has to query central PBX.

6.3.3 Session Initiation Protocol (SIP):

SIP is IETF standard for VoIP. SIP control syntax is similar to SMTP, HTTP, FTP and other IETF protocols. SIP is emerging standard in VoIP as it is simple compared to other protocols like H.323 and human readable. Asterisk and SIP inter-operates successfully with multiple vendors such as Cisco, SNOM, and H.323.

6.3.4 Benefits of using Asterisk:

- Provides cheapest call rates
- Cost savings on long distance calls
- Saving on line costs
- Cheap Land line to mobile calls
- Unified messaging such as Fax, Voicemail and E-mail.

References:

http://cdn.oreilly.com/books/9780596510480.pdf
http://www.asterisk.org/sites/asterisk/files/mce_files/documents/asterisk_quick_start_guide.pdf
Voip-Info.org. 2003-2010. Asterisk config sip.conf. HTML at Voip-Info.org.

RASPBERRY PI

7.1 What is Raspberry Pi?

Raspberry Pi is credit card sized single board computer which can run servers, capable of offering basic office computing, Internet, e-mail access, low-level gaming, software tools for programming and many other regular features expected from a computer.

7.1.1 History about Raspberry pi:

Raspberry Pi was developed by Raspberry Pi Foundation and it was released on 29th of February 2012. It is single board computer type and operates on Linux (Raspbian, Debian GNU/Linux, Fedora and Arch Linux ARM), RISC OS, FreeBSD, NetBSD, and Plan 9. There are two types of Raspberry Pi Model A and Model B, which operates in 2.5W and 3.5W respectively. Storage capacity depends upon the SD card used. It has a SD card slot and storage capacity can be changed depending upon the need. Memory of model A, model B revision 1 and model B revision 2 are 256MByte, 512MByte, 256MByte respectively. Graphics used is broadband Video core IV.

7.1.2 What can be done with Raspberry pi?

Raspberry Pi has powerful multimedia and 3D graphics capabilities; hence has the potential to be used as games platform. It's a small general purpose computer, but has better potential than regular PC at some things. Raspberry pi exposes GPIO which gets you to work straight away with Robotics projects unlike home PCs.

7.1.3 Size of Raspberry Pi

Raspberry Pi board size is 3.370 inch X 2.125 inch and 15mm deep. Raspberry Pi without case weighs 1.6oz.

7.1.4 Raspberry Pi Board Description

Raspberry Pi system is a Broadcom BCM2835 System on chip (SOC) multimedia processor, which means system's components, including central and graphics processing units long with audio and communications hardware are built in on single component. Instruction set Architecture used in BCM2835 is ARMING. Generation of ARM's processor design is ARM11. Advanced RISC Machine (ARM) is a processor, which is based on 32-bit reduced instruction set (RISC) architecture. Popular ARM-based processors include ARM7, ARM9, ARM11 and cortex based architecture is not common in Desktops, but every mobile has at least one ARM based processing core.

ARM Features:

- Load/store- based architecture
- Single-cycle instruction execution
- Consistent 16x32 bit register file
- Link register
- Easy decoding and pipelining
- Power-indexed addressing modes
- Fixed 32 bit instruction set

ARM-based BCM2835 is the reason that Raspberry Pi is able to operate in 5V 1A power supply and there is no heat sinks problem as it operates in low power.

7.2Why Linux

The majority of desktop and laptop computers available today run either on Microsoft windows or Apple operating systems. Both the platforms are closed source. Raspberry pi is designed to operate in GNU/Linux OS. Unlike windows, Linux is open source. Source code for entire operating system can be downloaded and changes can also be made. Changes made can be viewed by everyone. This open source development ethos has allowed Linux to be quickly altered to run on Pi and the process is known as porting. There are several versions of Linux are ported to Raspberry Pi's BCM2835 which includes Debian, Fedora Remix and Arch Linux. Each version is for different needs, but they are compatible with each other, Debian system will perfectly run on Arch Linux and vice versa.

7.2.1 Pros of Raspberry Pi

- Home PCs lacks in GPIO, which is major drawback in getting started with Robotics projects, but Raspberry pi exposes GPIO which gets you to work straight away.
- Raspberry pi is not compatible with Traditional PC software. Software for desktops and laptops is built with X86 instruction set architecture, which is not supported by Raspberry Pi.
- User doesn't require any extension programming experience since it was introduced for younger generation to learn about programming.
- Python is the programming language that is used the Pi. It is less complex than other languages available. Hence it provides better coding reliability.
- By changing the SD card, it allows you to change the function of the device easily instead of spending time in re-installing the software.
- Raspberry pi is perfect for adaptive technology. It displays at 1080p high definition resolution to build systems such as digital jukeboxes or prototyping embedded systems. Its helps in building complex product at cheaper price.
- Raspberry pi is energy efficient and provides a greener ethical alternative to small business. Since it is a palm sized product, it is easy to recycle and carbon dioxide emitted by this very less, unlike servers which require lots of energy and extension cooling systems.
- According to Nick Heath, Raspberry pi is low cost board which can be used for testing any products for software developers and network engineers to test firewall designs.

7.2.2 Cons of Raspberry Pi

- Processor is not fast and it is time consuming. It can't do any complex multi-tasking.
- There are currently 1.3 Billion Windows users around the world, but Raspberry Pi is not compatible with Windows operating systems.

- Raspberry pi is not compatible with Traditional PC software. Software for desktops and laptops is built with X86 instruction set architecture, which is not supported by Raspberry Pi

7.3 Difference between Model A and Model B:

Title	Model A	Model B
Chip	Broadband BCM2835 SOC multimedia processor	Broadband BCM2835 SOC multimedia processor
CPU	ARM1176JZF-S	ARM1176JZ-F
GPU	DualCore VideoCore IV Multimedia Co-Processor.	DualCore VideoCoreIV Multimedia Co-Processor
Ethernet	None	Ethernet RJ45 jack
USB 2.0	None	onboard 10/100 Ethernet RJ45 jack
Operating system	Linux	Linux
Onboard storage	SDIO slot, MMC and SD	SDIO slot, MMC and SD

Audio output	HDMI	HDMI
Video Output	HDMI	HDMI
Memory	SDRAM of 256 MB memory	SDRAM of 512MB memory
Dimensions	8.6cm x 5.4cm x 1.5cm	8.6cmx4cmx 1.7cm

Table 5.1: Raspberry Pi Comparison

7.4 Picture of Raspberry Pi

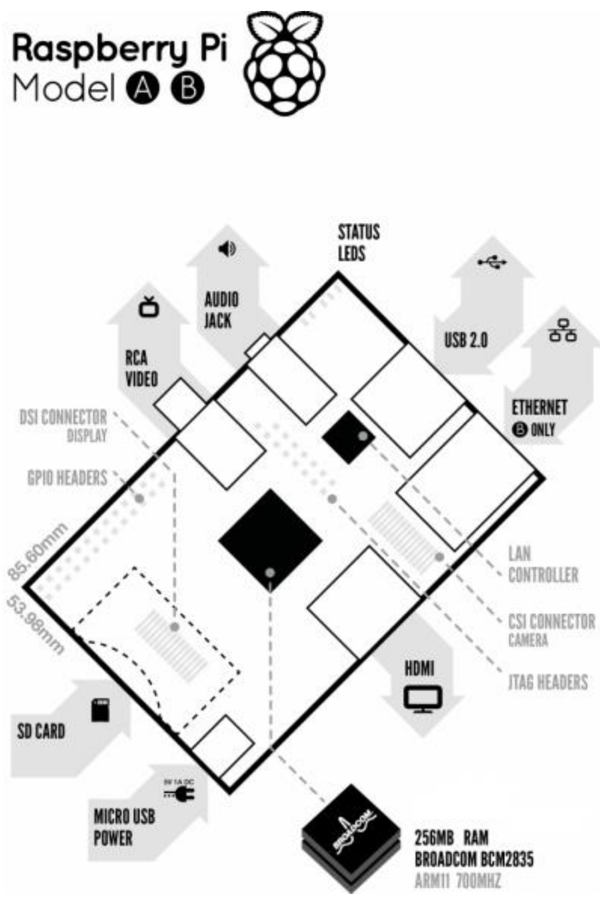


Fig 7.1: Picture of Raspberry Pi

7.5 Hardware Description

7.5.1 Connecting Display

Raspberry Pi has to be connected to a display to get started. Pi supports Composite Video, HDMI Video and DSI Video. Composite Video and HDMI Video are accessible to the end user, but DSI video requires some specialized hardware.

7.5.2 Composite Video

Composite video is available through yellow and silver port at the top of the Pi. The ports helps connect Pi to older display devices and the port is called as RCA phono connector. The connector creates composite colors found within the image (red, green and blue) and sends it to display device. Quality of Composite video is not good. There is interference, lack clarity and runs at limited resolution.

7.5.3 HDMI Video

Better quality than composite video can be achieved through HDMI Video. This is the only port found at the bottom of the Pi. HDMI port can display images at Full HD 1920x1080 resolution. Unlike Composite video it provides a high-speed digital connection for pixel-perfect pictures. Digital signals present in the HDMI cable can be displayed on a computer monitor by using HDMI-DVI cable.

7.5.4 DSI Video

This video output slot on the Pi can be found above the SD card slot. It's a small ribbon connector protected by layer of plastic. It is known as Display Serial Interface (DSI), which is used in the flat-panel displays of tablets and smart phones.

7.5.5 Connecting Audio

Raspberry Pi's HDMI port audio is simple. If HDMI is properly configured it can carry both video and audio signals. In DVI-D monitors, audio will not be available because DVI can't carry audio signals unlike HDMI. For DVI-D monitors and Composite video there is a 3.5mm audio jack located next to yellow phone connector which provides analog audio signals.

7.5.6 Connecting to Keyboard and Mouse

Keyboard and mouse are connected to USB port of the Raspberry Pi Model B. It has two slots for connecting keyboard and mouse. In Model A, USB hub has to be purchased in order to use both devices simultaneously since it has only one USB port. Wireless Keyboard and mouse can be used by connecting dongle to the USB port.

7.5.7 Connecting Power

Raspberry pi is powered by using micro-USB connector and slot for it can be found on lower left side of the circuit board. This connector is similar to Smartphone connectors and tablet devices. Pi needs power of 700mA, but some chargers supplies only 500mA, which might cause intermittent problems during operation. There is no power button on the device, it will start working as soon as the power is connected to the device and turns off by unplugging the power.

7.5.8 GPU

Like CPU, GPU is a single-chip processor, which is used to primarily for computing effects, object transformations and 3D motion. GPU is occasionally called visual processing unit (VPU), is a specialized board designed to manipulate and alter memory to accelerate the creation of images in a frame buffer. GPU are used in embedded systems, PCs, mobile phone and work stations. In a personal computer, a GPU can be present on a video card or can be on the mother board.

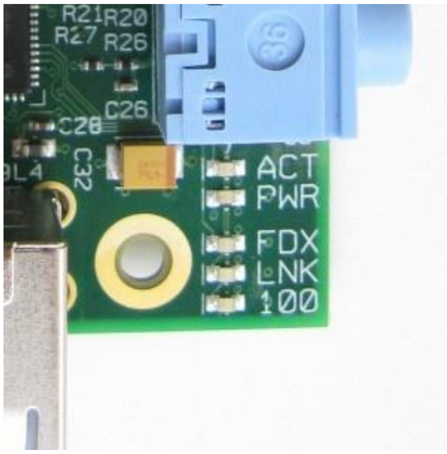


Fig 7.2: Picture of GPU

7.5.9 PICTURE OF LED

All Raspberry Pi boards have LEDs positioned next to audio jack and USB ports. Model B has 5 status LEDs and Model A has 2 status LEDs

7.5.9.1 Meaning of LEDs

- ACT – D5 (Green) – SD Card Access
- PWR – D6 (Red) – 3.3 V Power is present
- FDX – D7 (Green) – Full Duplex (LAN) connected
- LNK – D8 (Green) – Link/Activity (LAN)
- 100 – D9 (Yellow) – 100Mbit (LAN) connected

PWR LED is directly connected to power supply rail and FDX, 100, LNK LEDs are directly connected to USB/Ethernet chip, which is control them using Hardware. ACT LED is connected to GPIO pin on the SOC.

7.5.10 GPIO pin

GPIO has twenty six pins in which three are power supply pins,

- 1: 3V3 (3.3V)
- 2: 5V0 (5.0V)
- 3: GND (0V)
- 4: 6 of DNC (Do not connect) Pins
- 5: 17 of GPIO pins

GPIO pin can be set high by connecting it to a voltage supply or set low by connecting it to ground. Raspberry Pi can take either values, it can take it as input and as well output.

7.5.11 Role of Raspberry Pi in the project

Raspberry is used as a server in this project to provide real time communication. It acts as a wireless access point and provides the Wi-Fi connection to the vehicles under Local Area Network. The board gets Internet access through Ethernet and it translates that as a Wi-Fi access point through Wi-Fi Dongle. The vehicles get registered with server to start communication between them.

7.6 Flashing from SD card

To use the SD with Raspberry Pi, Operating system has to be flashed into SD card. There are various Linux Distributions. Everything has its own advantage and disadvantage and Operating system used in this project is Wheezy and the OS can be changed later if it is not compatible as SD can be flashed again with new operating system at any point.

The most updated list of Linux releases, which are compatible with Raspberry Pi, can be downloaded from Raspberry Pi official website.

Software is required to flash the OS into SD card. Win32Diskimager is the software which has to be used by Windows user to flash the OS. SD card has to be formatted, if it doesn't have enough space. Formatting tool software can be used to format the SD and if it is a new SD card there won't be a need of formatting it.

7.7Flashing from Windows

If the PC used for Flashing is running on Windows, some third-party software is required to get the image file flashed on to the SD card.

Latest version of Image writer can be found at the official website of Image Writer. The steps presented below helps in getting the SD card ready.

1: Download the image writer zip file and extract it to a folder on your computer.

2: Plug the SD card into the card reader slot of the computer

3: Double click on the image file writer software to open the program and click the blue folder icon to open a file browser.

4: Browse the extracted image file and open it.

5: click write button on the Win32diskimager window, to write the OS on to SD card.

6: once the OS is flashed, there will be a message saying that it was successfully done.

References:

http://www.myraspberry-pi.org/wp-content/uploads/2013/02/Raspberry.Pi_.User_.Guide_.pdf

http://www.raspberrypi.org/wp-content/uploads/2012/12/quick-start-guide-v1.1.pdf http://www.engadget.com/2012/09/04/raspberry-pi-getting-started-guide-how-to/

http://www.raspberrypi.org/

http://downloads.element14.com/raspberryPi1.html

http://www.raspberrypi.org/faqshttp://www.makeuseof.com/pages/great-things-small-package-your-unofficial-raspberry-pi-manual

RESULTS AND CONCLUSION

8.0 Testing:

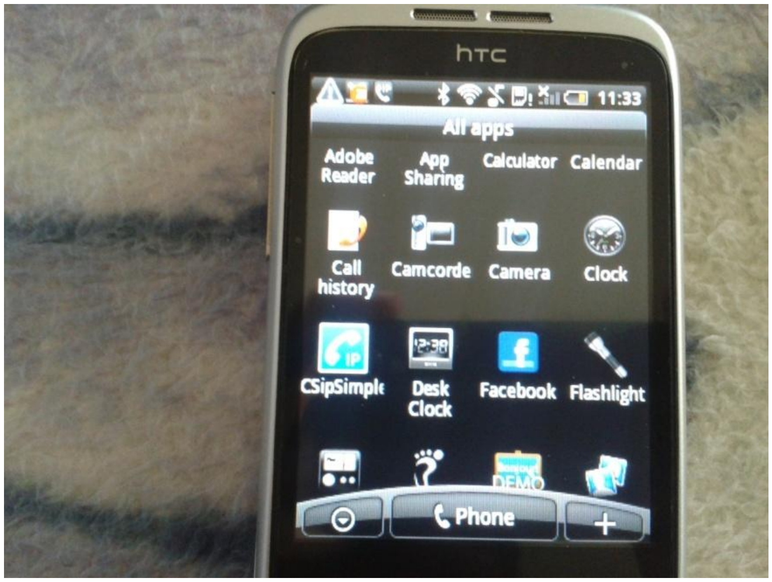
Totally three cell phones were used to test the VANET connectivity and first phone was in basement of my house and second phone was in first floor and the third phone was in first floor as well. The distances between the three phones were more than 100 meters. Connected the first phone to Home Wi-Fi and connected second and third phone to Server. Disconnecting the first device from home Wi-Fi, it gets automatically connected to the nearby VANET device. Each call was tested about 10 minutes and I tried testing with three different CODECs namely Speex, G.729 and G.711. G.711 had poor network efficiency and there was a lack of voice. Using G.729, the speech quality of voice decreased marginally. Comparing G.729, G.711 and Speex, Speex had a better quality than the other two CODECs.

Performance order of speech Codec:

Speex
G.729
G.711

8.1 OUTPUTS:

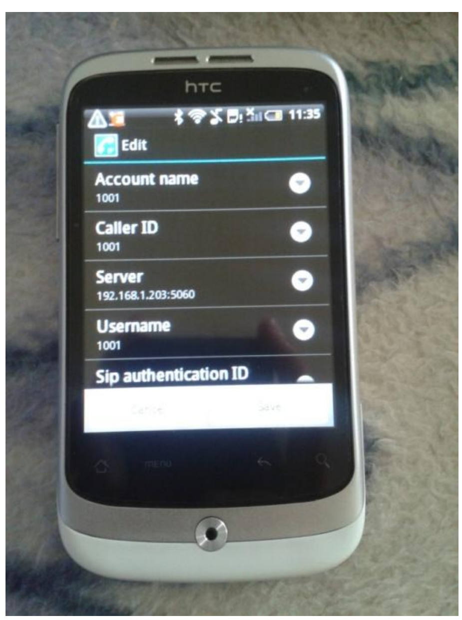
Download CSIPSimple software in Android phones to make audio calls

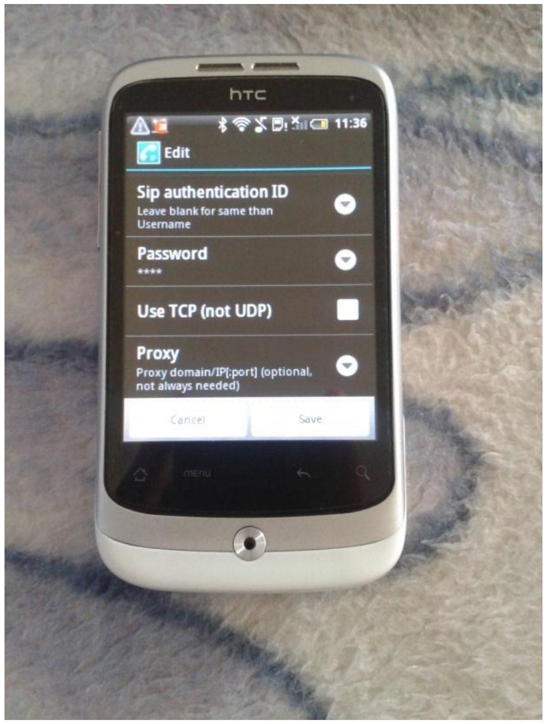


After downloading, the phone has to be registered with server (Raspberry Pi)

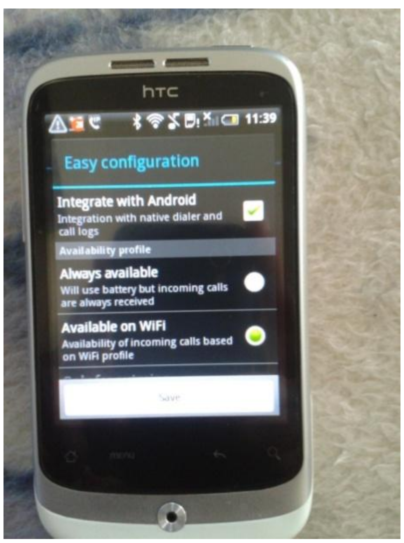
Steps to register the phone:

Create a CSIPSimple account by entering the Account name, caller ID, Server IP address and Password.

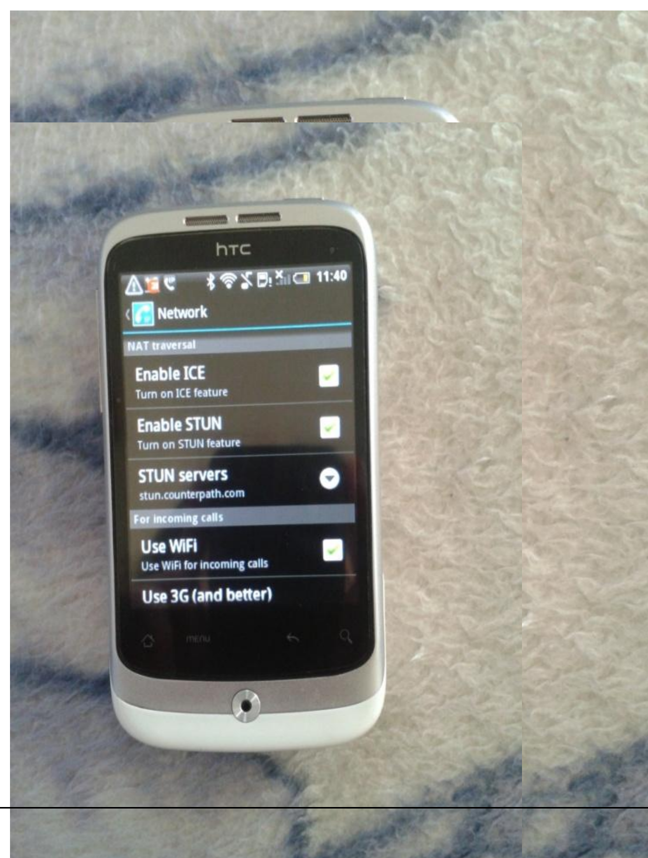


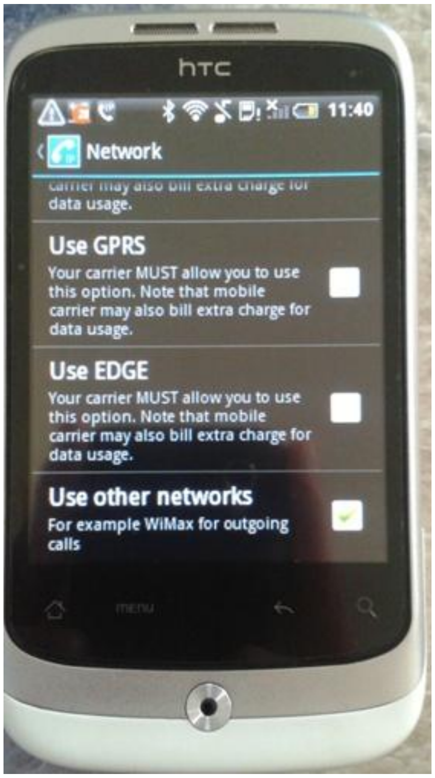


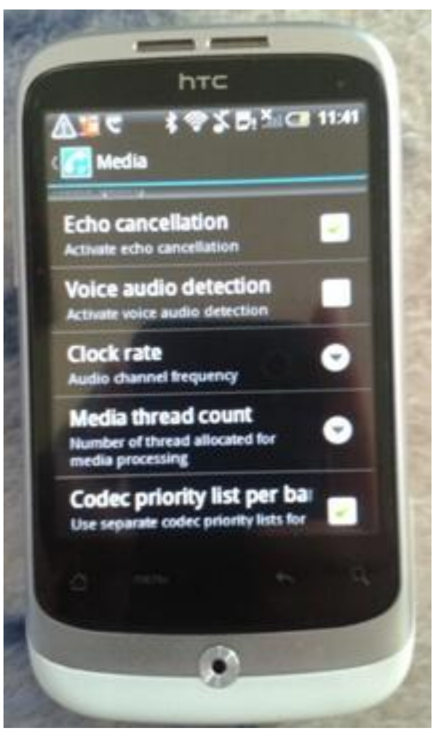
Above pictures shows how an account have to be created

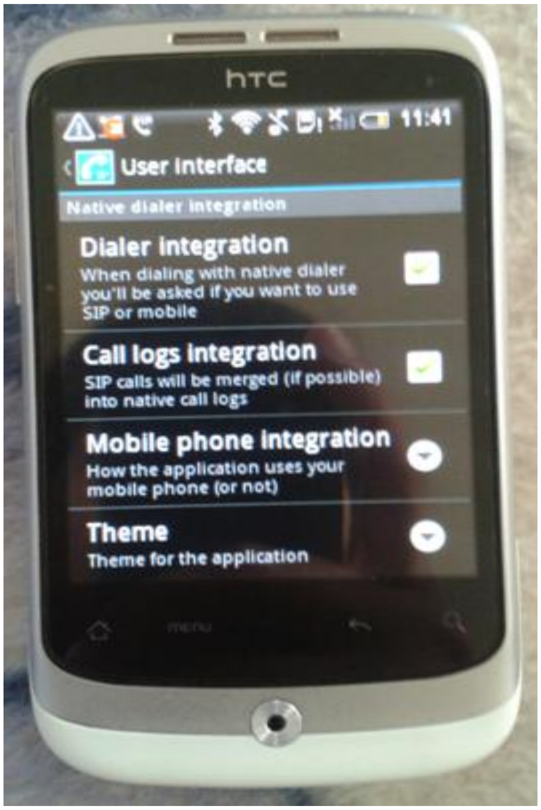


Enabling Setting configurations:

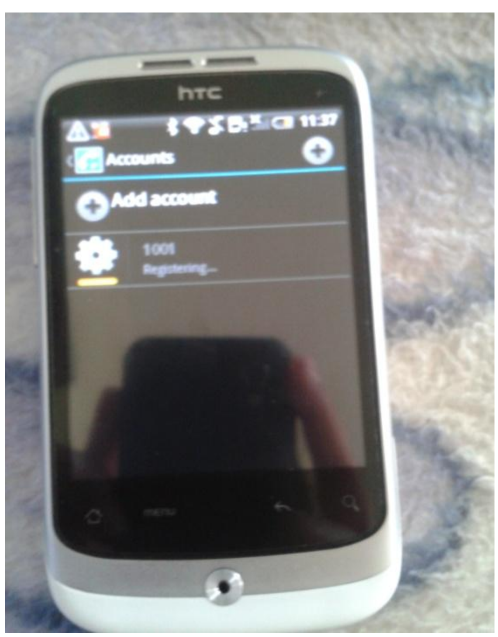



htc
11:40
Network
data usage.
Use GPRS
Your carrier MUST allow you to use this option. Note that mobile carrier may also bill extra charge for data usage.
Use EDGE
Your carrier MUST allow you to use this option. Note that mobile carrier may also bill extra charge for data usage.
Use other networks
For example WiMax for outgoing calls

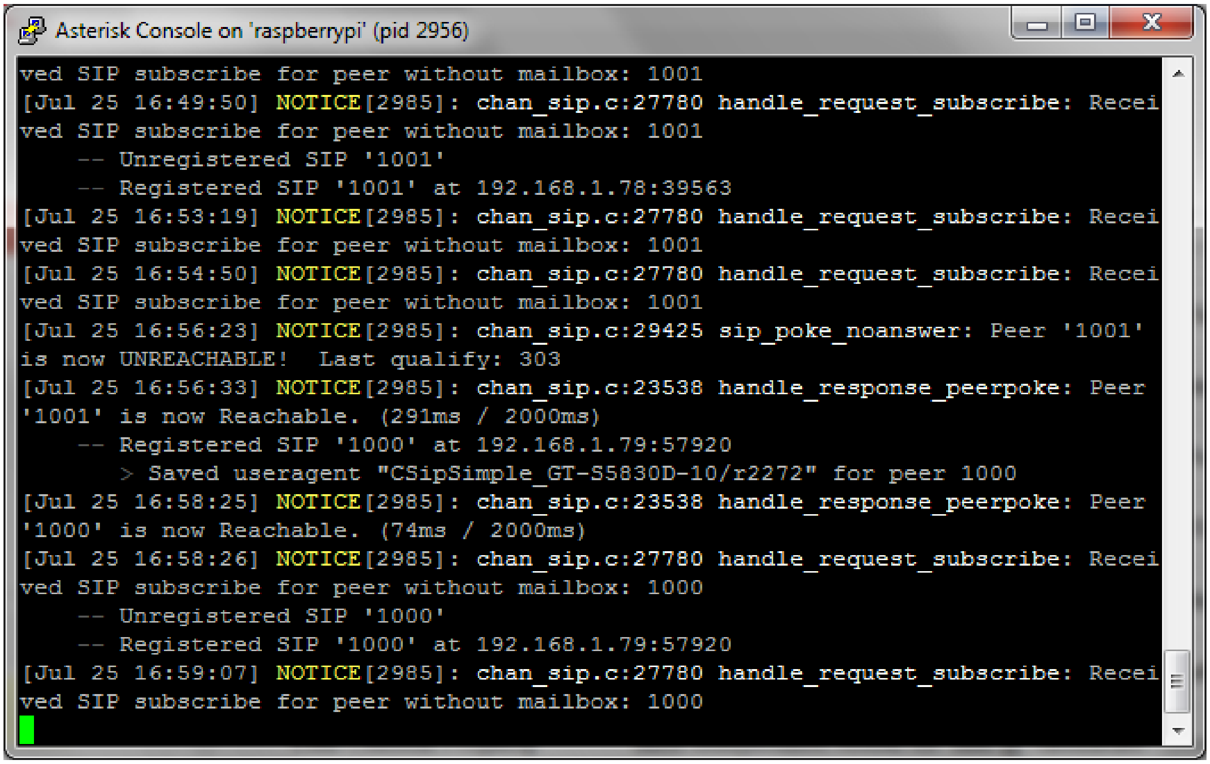

htc
11:41
Media
Echo cancellation
Activate echo cancellation
Voice audio detection
Activate voice audio detection
Clock rate
Audio channel frequency
Media thread count
Number of thread allocated for media processing
Codec priority list per ba
Use separate codec priority lists for

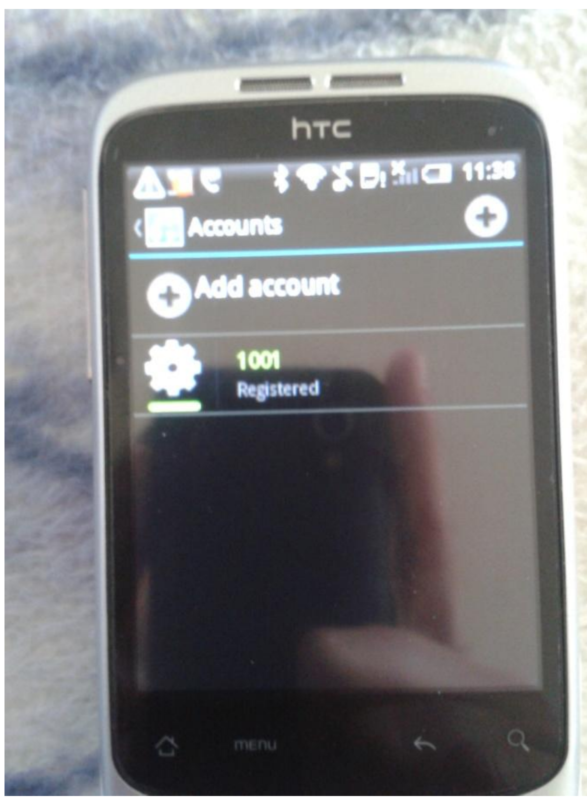


Register SIP phones with the server:



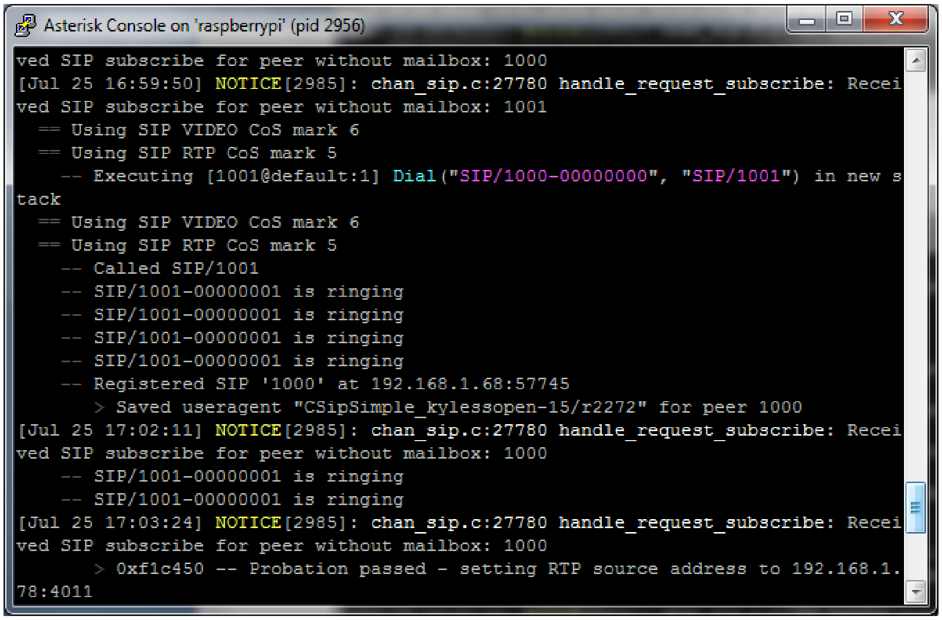
Phone getting registered with Server

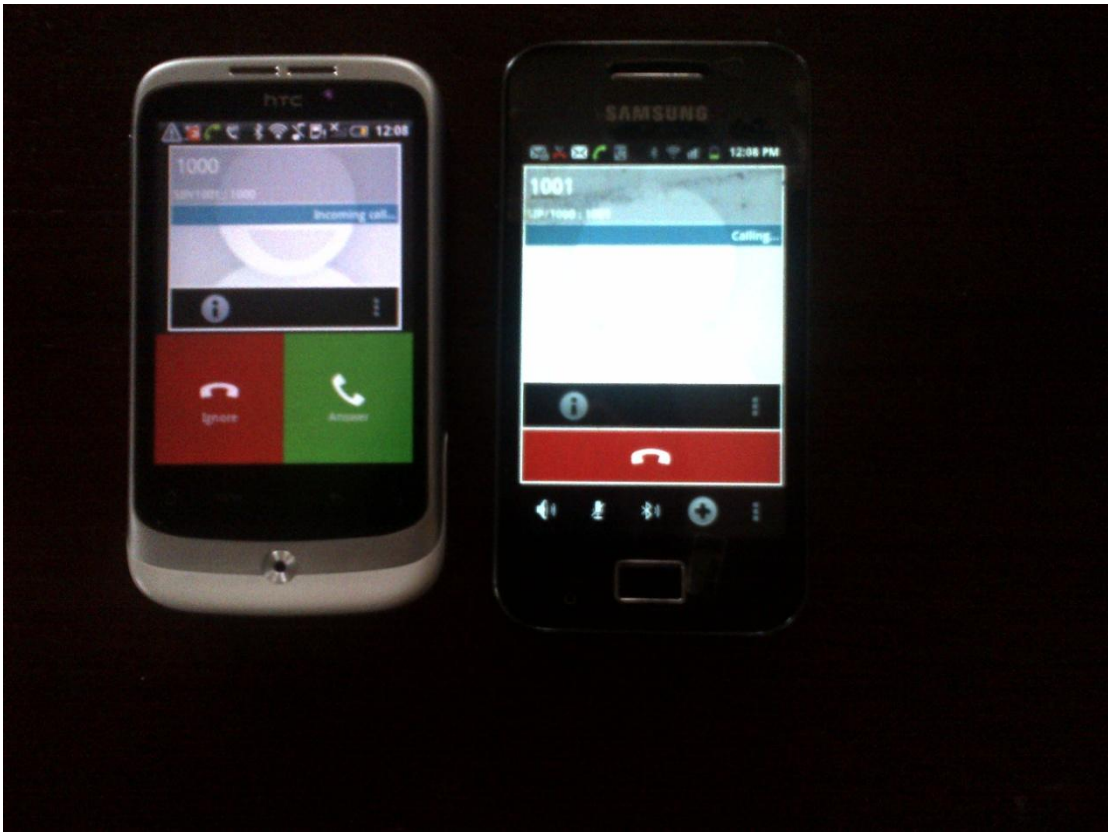




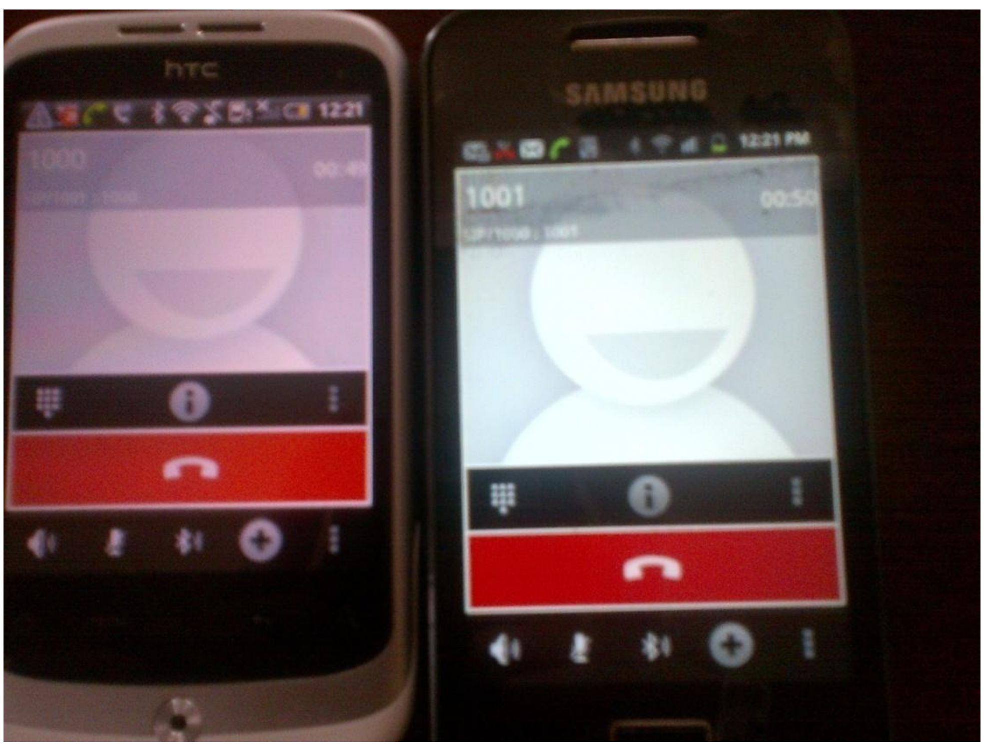
Once the phone gets registered with the server, it prompts a message saying that the phone is registered.

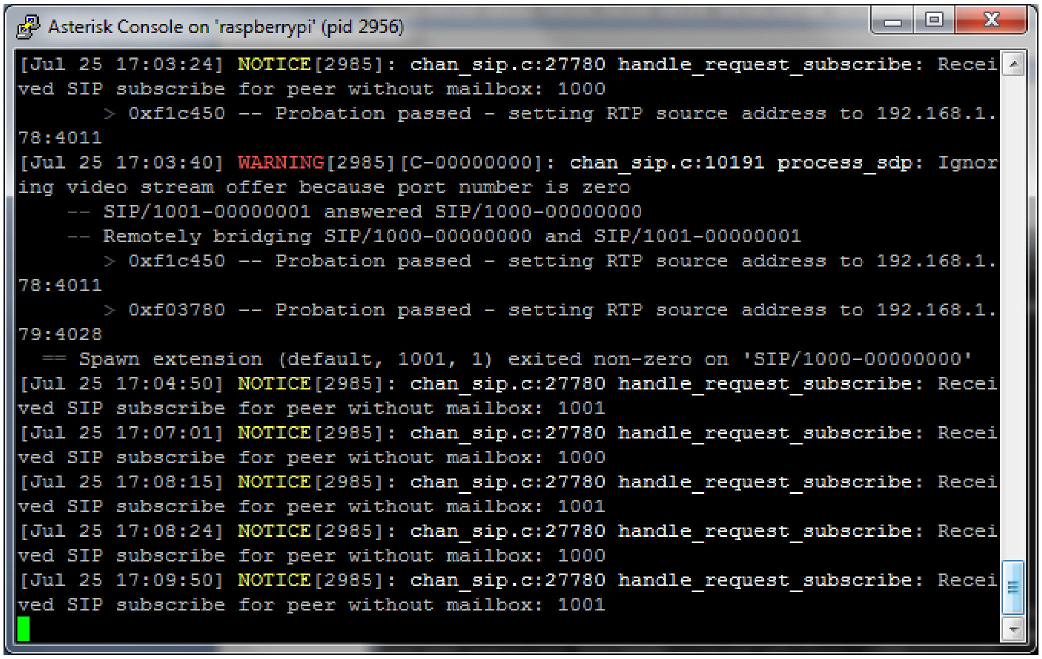
Once the phone is registered, call can be made to another phone which is also registered with server.





In above picture, phone 1001 calls 1000





Once the phone gets registered with the server, the communication happens between the peers through Wi-Fi. For instance, vehicle1 is connected to different Wi-Fi and vehicle2 near by the vehicle1 is connected to the server (Raspberry Pi). If the vehicle1 gets disconnected, it will automatically be connected to the vehicle2 Wi-Fi. Vehicle2 then acts as a server for the vehicle1 and provides the service.

References:

- Madsen L, Smith J, Sokol S. 2003. The Hitchhiker's Guide to Asterisk. HTML at MicroAlcarria, PDF at DynX Services.
- Meggelen van J, Madsen L, Smith J. 2007. Asterisk, the Future of Telephony. Second Edition. O'Reilly & Associates, Inc. ISBN-13: 978-0-596-51048-0. 574 pp. HTML at the Asterisk Documentation Project, PDF at O'Reilly Media, Inc.
- Voip-Info.org. 2003-2010. Asterisk config sip.conf. HTML at Voip-Info.org

CHAPTER- 9

Vehicle changes its location constantly; therefore there is a constant demand for information on current location. Taking into account of increasing demand for car safety, there are numerous vehicular network introduced, to provide critical safety application. Due to the demand, devices have tend to research on self organize and self healing networks without interference with centralized or pre-established infrastructures. One of such networks which have received a lot of interest is VANET. It has tremendous potential to provide

- Improved vehicle
- Road safety
- Traffic efficiency
- High mobility
- Comfort to both drivers and passengers have increased the demand for it.

Feasibility of application in VANET not only relies on characteristics of vehicular network, but also on the communication medium. In this project, Wi-Fi used for vehicle to vehicle communication or vehicle to roadside communication is found to provide reliable and high throughput, when the vehicles are connected. Applications such as file sharing, HD video transferring was easily possible through high data rate of Wi-Fi. This setup is particularly designed for delay tolerant applications and streaming of audio, video and conferencing using V2V2I setup. Since VANETs are high dynamic networks, CODECs used must be able to deal with delay and packet loss. There are several research projects going on regarding inter-vehicle communication in VANET environment.

FUTURE WORK

10.1 Future Work

- Quality of service can be designed for VOVAN, to adapt the CODECs with VANET environment.
- In Vehicular networks only two nodes communicate with each other, hence there is no collision with each other. Research can be done on multi-node communication.
- There is multiple wireless communication technologies used in VANET. Technologies are needed to be managed. Future work can be done in implication of using multiple wireless networks.
- Nodes in VANET have high mobility, therefore addressing for Internet access is challenging. Investigations can be done in increasing the potential to change the Internet gateway.

Appendix

Download debian Operating system for Raspberry pi from this link

http://downloads.raspberrypi.org/images/raspbian/2013-07-26-wheezy-raspbian/2013-07-26-wheezy-raspbian.zip.torrent

Download Wi-Fi USB Dongle driver

https://github.com/jenssegers/RTL8188-hostapd/archive/v1.1.tar.gz

To update and download Asterisk:

To start with, update the system and install the required components by copying the command below:

sudo apt-get update

sudo apt-get -y install make gcc g++ libxml2 libxml2-dev ssh libncurses5 libncursesw5 libncurses5-dev libncursesw5-dev linux-libc-dev sqlite libnewt-dev libusb-dev zlib1g-dev libmysqlclient15-dev libsqlite0 libsqlite0-dev bison openssl libssl-dev libeditline0 libeditline-dev libedit-dev mc sox libedit2 libedit-dev curl libcurl4-gnutls-dev apache2 libapache2-mod-php5 php-pear openssh-server build-essential openssh-client zlib1g zlib1g-dev libtiff4 libtiff4-dev libnet-telnet-perl mime-construct libipc-signal-perl libmime-types-perl libproc-waitstat-perl mpg123 libiksemel-dev php5 php5-cli mysql-server php5-mysql php-db libapache2-mod-php5 php5-gd php5-curl mysql-client vim

Download and Extract Asterisk:

To Download and Extract asterisk, enter the commands as below:

cd /usr/src
sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-1.8-current.tar.gz

Sudo tar xvfz asterisk-1.8-current.tar.gz

cd asterisk-1.8*

8.4 Compile and Install Asterisk
Using the following commands:

sudo ./configure

sudo make
sudo make install
sudo make samples
sudo make config

Finally, restart the PI by typing the following command:
sudo init 6

Asterisk is now installed.

Compile Wi-Fi USB dongle driver

tar -zxvf v1.1.tar.gz

make

Install Wi-Fi USB tangle driver

make install

cd RTL8188-hostapd-1.1/hostapd

sudo make

sudo make install

Start Wi-Fi USB dongle driver Service

sudo service hostapd restart

[ok] Stopping advanced IEEE 802.11 management: hostapd.

[ok] Starting advanced IEEE 802.11 management: hostapd

Install DHCP Server Support

sudo apt-get install hostapd udhcpd

Configure DHCP. Edit the file /etc/udhcpd.conf and configure it like this:

start 192.168.1.2 # This is the range of IPs that the hostspot will give to client devices.

end 192.168.1.254

interface wlan0 # The device uDHCP listens on.

remaining yes

opt dns 8.8.8.8 4.2.2.2 # The DNS servers client devices will use.

opt subnet 255.255.255.0

opt router 192.168.42.1 # The Pi's IP address on wlan0 which we will set up shortly.

opt lease 864000 # 10 day DHCP lease time in seconds

Edit the file /etc/default/udhcpd and change the line:

DHCPD_ENABLED="no" to #DHCPD_ENABLED="no"

Configure DHCP

Edit the file /etc/udhcpd.conf and configure as below:

sudo ifconfig wlan0 192.168.1.204

Edit the file /etc/network/interfaces and replace the line "iface wlan0 inet dhcp" to set static IP:

iface wlan0 inet static

address 192.168.1.204

netmask 255.255.255.0

If the line "iface wlan0 inet dhcp" is not present, add the above lines to the bottom of the file.

allow-hotplug wlan0

wpa-roam /etc/wpa_supplicant/wpa_supplicant.conf

iface default inet manual to: #allow-hotplug wlan0

wpa-roam /etc/wpa_supplicant/wpa_supplicant.conf

iface default inet dhcp

Edit the file /etc/hostapd/hostapd.conf (create it if it doesn't exist) and add the following lines:

interface=wlan0

driver=nl80211

ssid=My_AP

hw_mode=g

channel=6

macaddr_acl=0

auth_algs=1

ignore_broadcast_ssid=0

wpa=2

wpa_passphrase=My_Passphrase

wpa_key_mgmt=WPA-PSK

wpa_pairwise=TKIP

rsn_pairwise=CCMP

If you would like to create an open network:

/etc/hostapd/hostapd.conf:

interface=wlan0

ssid=My_AP

hw_mode=g

channel=6

auth_algs=1

wmm_enabled=0

Change ssid= and channel= to values of your choice. Note that anyone will be able to connect to your network, which is generally not a good idea. Also, some regions will hold an access point's owner responsible for any traffic that passes through an open wireless network, regardless of who actually caused that traffic.

Edit the file /etc/default/hostapd and change the line:

DAEMON_CONF="" to: DAEMON_CONF="/etc/hostapd/hostapd.conf" sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"

To set this up automatically on boot, edit the file /etc/sysctl.conf and add the following line to the bottom of the file:

net.ipv4.ip_forward=1

S## To enable NAT in the kernel, run the following commands:

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j ACCEPT

sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT

sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"

##Now edit the file /etc/network/interfaces and add the following line to the bottom of the file:

up iptables-restore < /etc/iptables.ipv4.nat

##Fire it up! Run the following commands to start the access point:

sudo service hostapd start

sudo service udhcpd start

sudo update-rc.d hostapd enable

sudo update-rc.d udhcpd enable

apt-get update
apt-get upgrade
apt-get install build-essential libtool automake subversion git-core libsrtp0-dev libssl-dev libspeexdsp-dev yasm libvpx-dev libgsm1-dev libxml2-dev libx264-dev screen pkg-config

Download FFMPEG through this link

apt-get remove libavutil51
cd /usr/local/src
wget -c http://ffmpeg.org/releases/ffmpeg-1.0.2.tar.gz
tar zxvf ffmpeg-1.0.2.tar.gz
cd ffmpeg

Configure FFMPEG

```
./configure --extra-cflags="-fPIC" --extra-ldflags="-lpthread" --enable-pic --enable-memalign-hack --enable-shared --disable-static --disable-network --disable-protocols --disable-pthreads --disable-devices --disable-filters --disable-bsfs --disable-muxers --disable-demuxers --disable-parsers  --disable-hwaccels --disable-ffmpeg --disable-ffplay --disable-ffserver  --disable-encoders --disable-decoders --disable-zlib --enable-gpl --disable-debug  --enable-encoder=h263 --enable-encoder=h263p --enable-decoder=h263 --enable-encoder=mpeg4 --enable-decoder=mpeg4 --enable-libx264  --enable-encoder=libx264 --enable-decoder=h264
```

Compile FFMPEG

```
make -j `getconf _NPROCESSORS_ONLN`
```

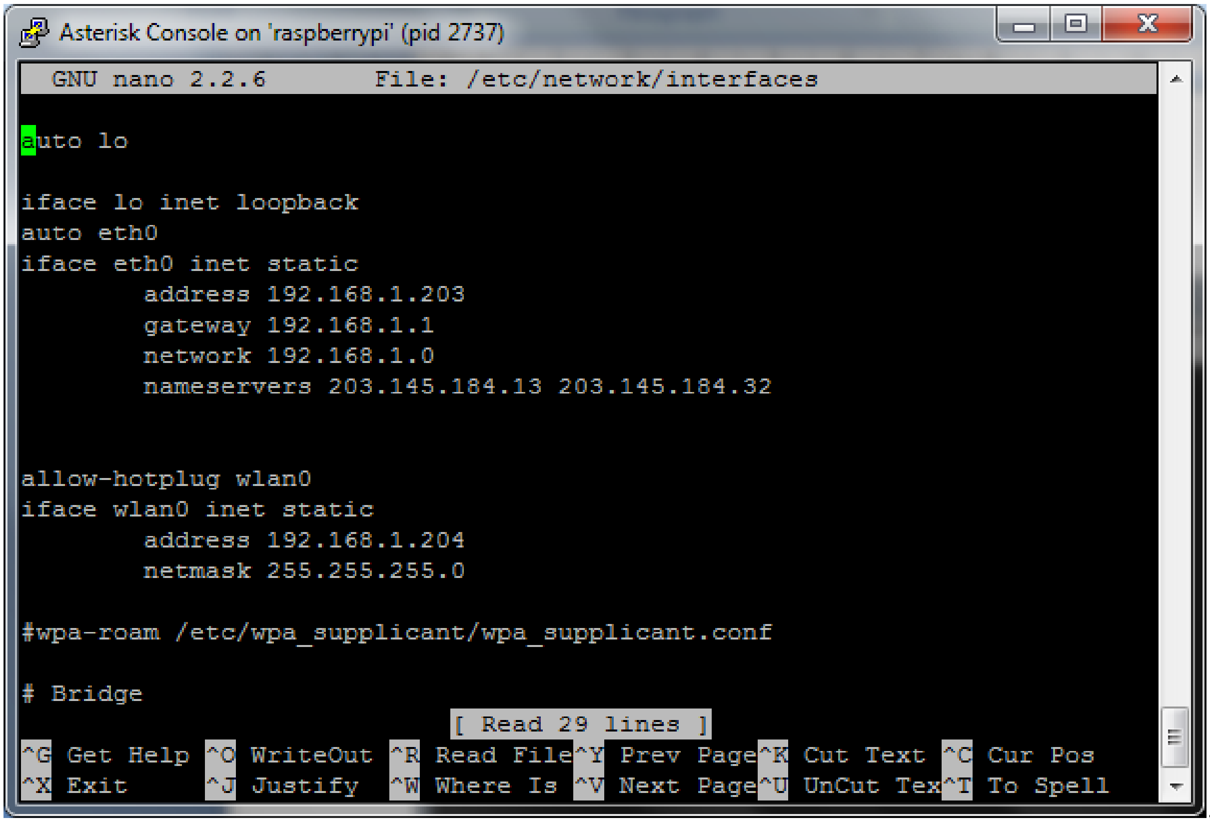
Install FFMPEG

```
make install
```

Configure FFMPEG

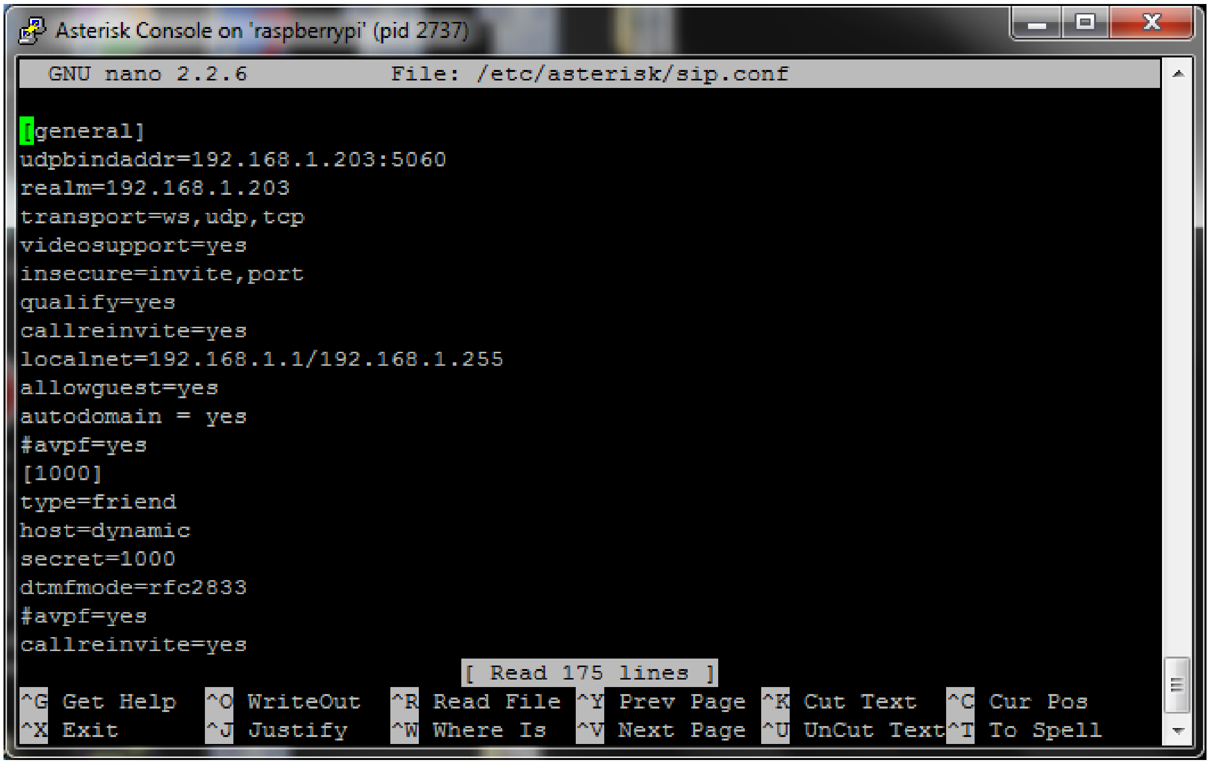
```
ldconfig
```

Screen shots:

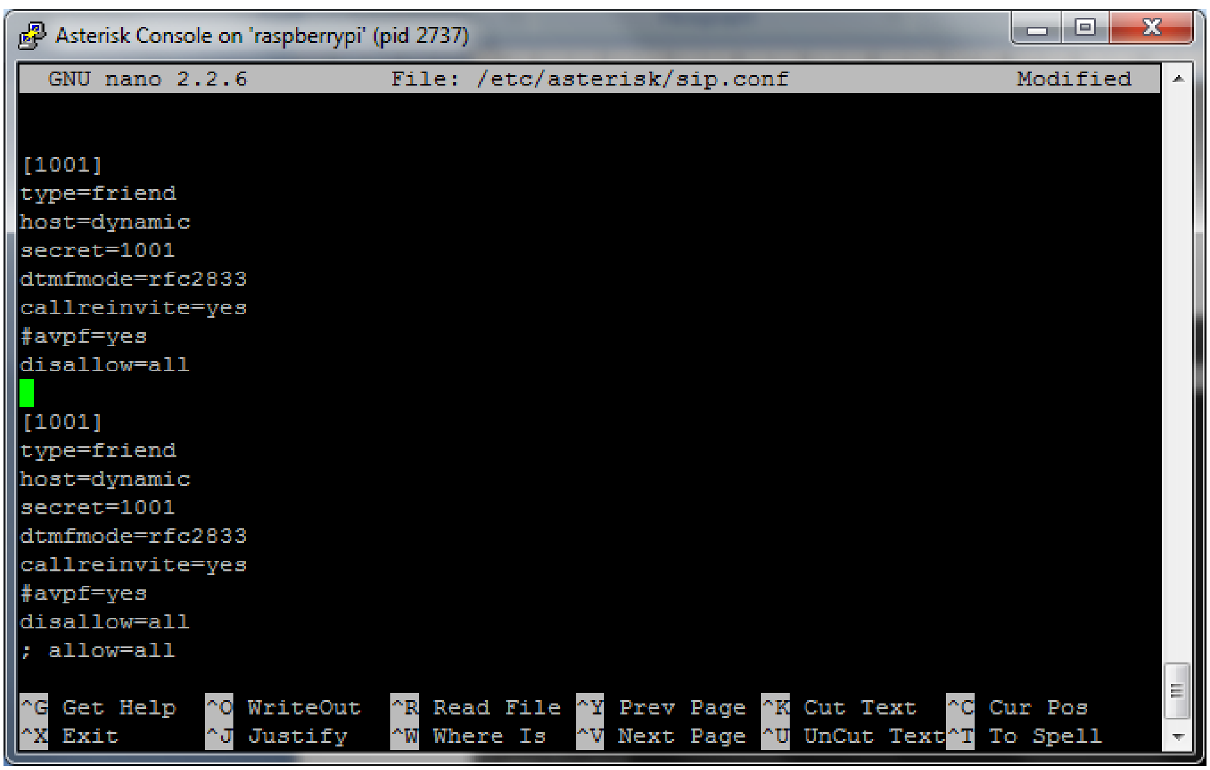


```
192.168.1.203 - PuTTY

  GNU nano 2.2.6           File: /etc/network/interfaces


allow-hotplug wlan0
iface wlan0 inet static
        address 192.168.1.204
        netmask 255.255.255.0

#wpa-roam /etc/wpa_supplicant/wpa_supplicant.conf

# Bridge

auto br0
iface br0 inet static
    address 192.168.1.203
    network 192.168.0.1
    netmask 255.255.255.0
    broadcast 192.168.1.255
    bridge-ports wlan0 eth0

up iptables-restore < /etc/iptables.ipv4.nat

^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

```
Asterisk Console on 'raspberrypi' (pid 2737)

  == Registered custom function 'QUEUE_MEMBER'
  == Registered custom function 'QUEUE_MEMBER_COUNT'
  == Registered custom function 'QUEUE_MEMBER_LIST'
  == Registered custom function 'QUEUE_WAITING_COUNT'
  == Registered custom function 'QUEUE_MEMBER_PENALTY'
 app_queue.so => (True Call Queueing)
  == Parsing '/etc/asterisk/cli_permissions.conf': Found
Asterisk Ready.
  == Parsing '/etc/asterisk/cli.conf': Found
*CLI> sip show peers
Name/username             Host                                    Dyn Forcerport
 ACL Port     Status      Description
1000                       (Unspecified)                           D    a
     0        UNKNOWN
1001                       (Unspecified)                           D    a
     0        UNKNOWN
1060/1060                  (Unspecified)                           D    a
     0        UNKNOWN
1061/1061                  (Unspecified)                           D    a
     0        UNKNOWN
8000                       (Unspecified)                           D    a
     0        UNKNOWN
5 sip peers [Monitored: 0 online, 5 offline Unmonitored: 0 online, 0 offline]
*CLI>
```



```
Asterisk Console on 'raspberrypi' (pid 2737)
  GNU nano 2.2.6              File: /etc/asterisk/sip.conf

[general]
udpbindaddr=192.168.1.203:5060
realm=192.168.1.203
transport=ws,udp,tcp
videosupport=yes
insecure=invite,port
qualify=yes
callreinvite=yes
localnet=192.168.1.1/192.168.1.255
allowguest=yes
autodomain = yes
#avpf=yes
[1000]
type=friend
host=dynamic
secret=1000
dtmfmode=rfc2833
#avpf=yes
callreinvite=yes
                              [ Read 175 lines ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```



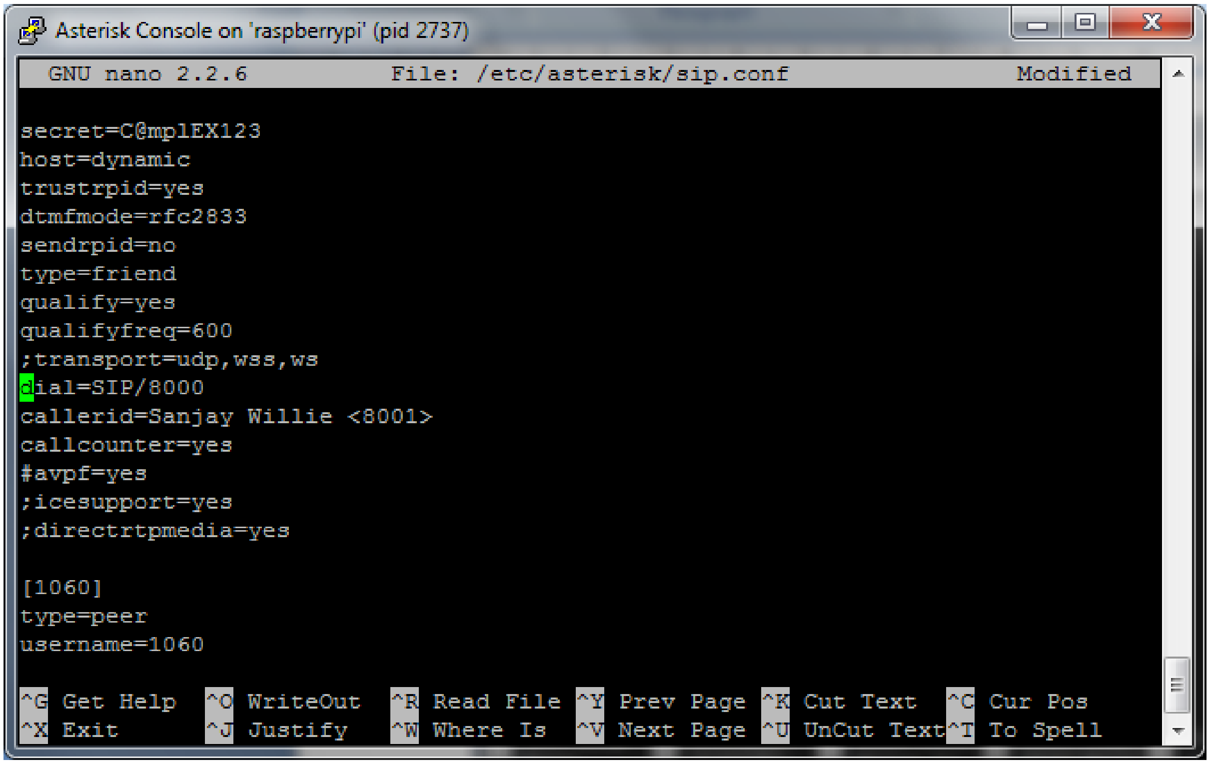
```
Asterisk Console on 'raspberrypi' (pid 2737)
  GNU nano 2.2.6              File: /etc/asterisk/sip.conf                Modified


[1001]
type=friend
host=dynamic
secret=1001
dtmfmode=rfc2833
callreinvite=yes
#avpf=yes
disallow=all

[1001]
type=friend
host=dynamic
secret=1001
dtmfmode=rfc2833
callreinvite=yes
#avpf=yes
disallow=all
; allow=all

^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

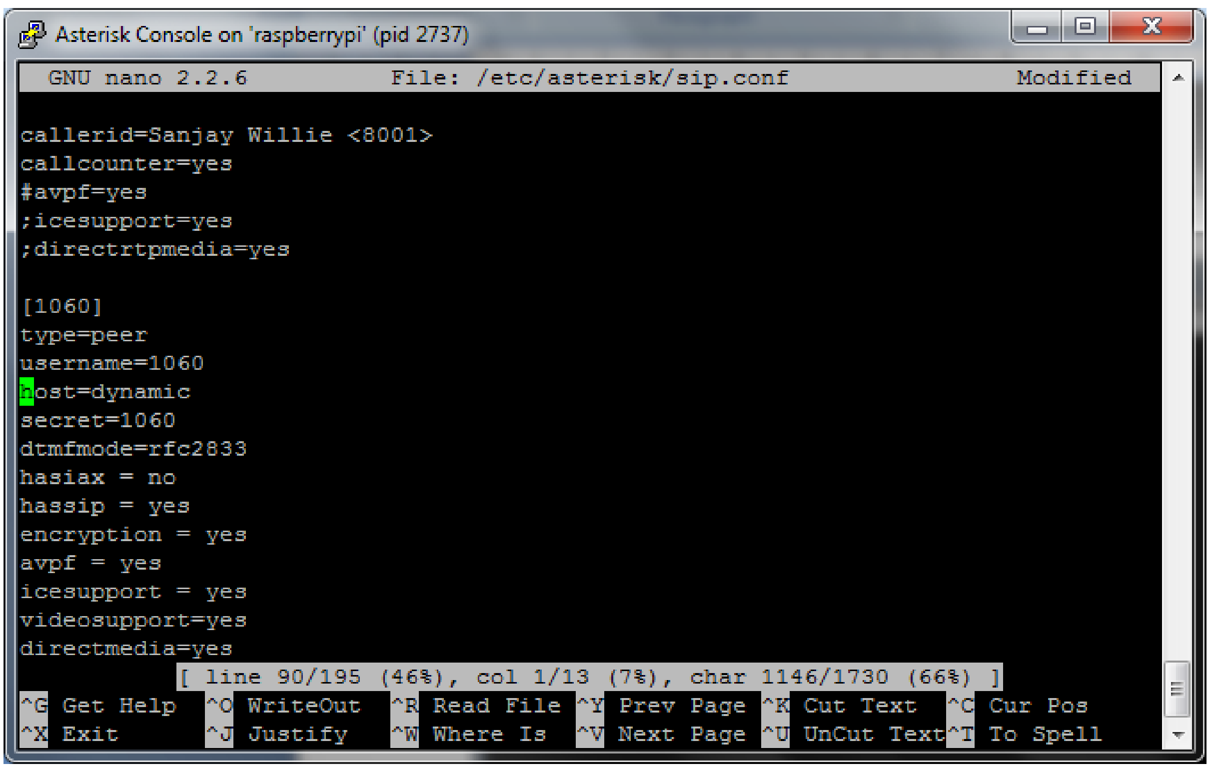
Asterisk Console on 'raspberrypi' (pid 2737)

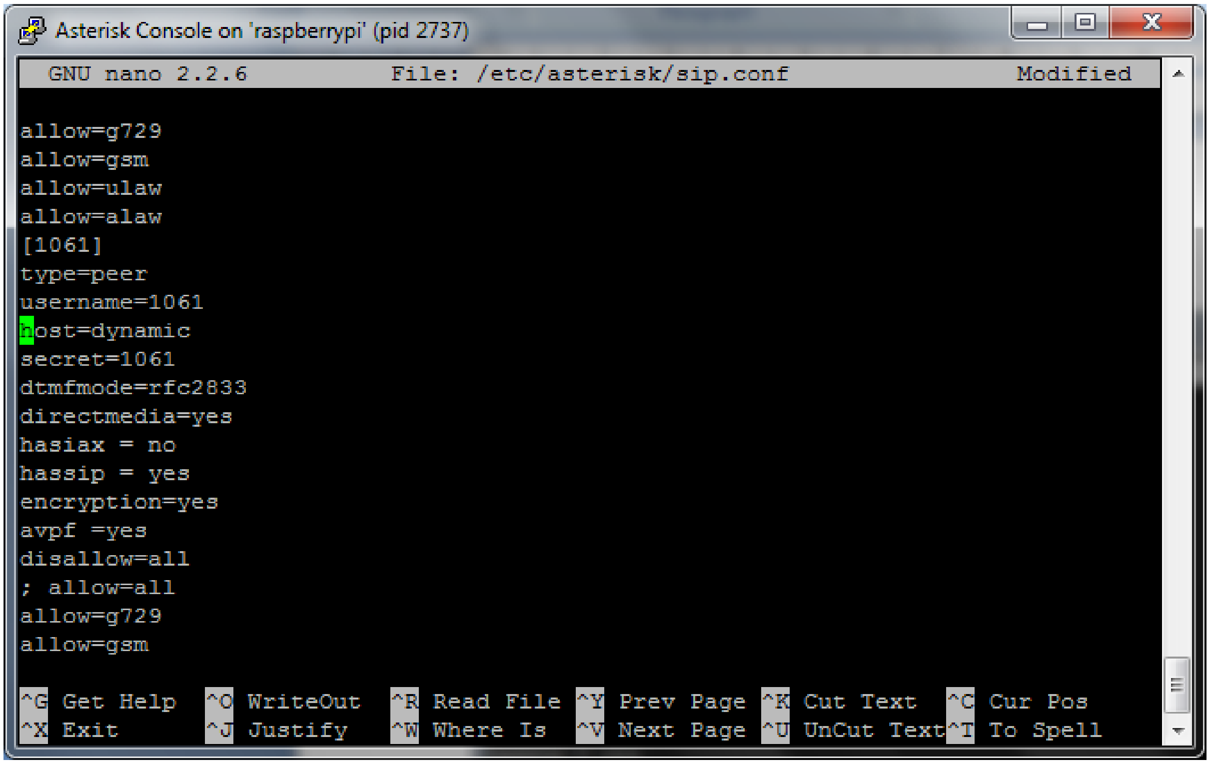
```
  GNU nano 2.2.6              File: /etc/asterisk/sip.conf                Modified

[1001]
type=friend
host=dynamic
secret=1001
dtmfmode=rfc2833
callreinvite=yes
#avpf=yes
disallow=all
; allow=all
allow=g729
allow=gsm
allow=ulaw
allow=alaw
allow=g711u
allow=h263p
allow=h263
allow=h261
allow=vp8

^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text^T To Spell
```

Asterisk Console on 'raspberrypi' (pid 2737)

```
  GNU nano 2.2.6              File: /etc/asterisk/sip.conf                Modified

allow=gsm
allow=ulaw
allow=alaw
allow=g711u
allow=h263p
allow=h263
allow=h261
allow=vp8

[8000]
secret=C@mplEX123
host=dynamic
trustrpid=yes
dtmfmode=rfc2833
sendrpid=no
type=friend
qualify=yes
qualifyfreq=600
;transport=udp,wss,ws

^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text^T To Spell
```


Asterisk Console on 'raspberrypi' (pid 2737)
GNU nano 2.2.6 File: /etc/asterisk/sip.conf Modified
secret=C@mplEX123
host=dynamic
trustrpid=yes
dtmfmode=rfc2833
sendrpid=no
type=friend
qualify=yes
qualifyfreq=600
;transport=udp,wss,ws
dial=SIP/8000
callerid=Sanjay Willie <8001>
callcounter=yes
#avpf=yes
;icesupport=yes
;directrtpmedia=yes
[1060]
type=peer
username=1060
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell


Asterisk Console on 'raspberrypi' (pid 2737)
GNU nano 2.2.6 File: /etc/asterisk/sip.conf Modified
callerid=Sanjay Willie <8001>
callcounter=yes
#avpf=yes
;icesupport=yes
;directrtpmedia=yes
[1060]
type=peer
username=1060
host=dynamic
secret=1060
dtmfmode=rfc2833
hasiax = no
hassip = yes
encryption = yes
avpf = yes
icesupport = yes
videosupport=yes
directmedia=yes
[line 90/195 (46%), col 1/13 (7%), char 1146/1730 (66%)]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell



8.6 Connectivity of Extension: