Security on Voice over Internet Protocol from Spoofing Attacks

Neha Kapoor, Yash Kumar,Mona Sharma

Student,ECE,DCE,Gurgaon, India

EMAIL:neha04263@gmail.com, yashguptaip@gmail.com,monasharma1194@gmail.com

ABSTRACT:-

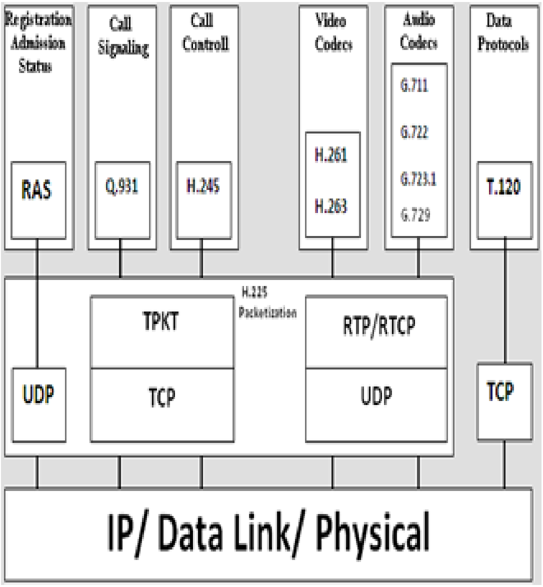
Voice over Internet protocol (VoIP), there is an existing way of communication over any network. Using this technology the users can make telephone calls over IP network. This paper will describe Voice over Internet protocols (VoIP) to a level that allow discussion of security issues and concerns. There are two spoofing attacks are possible, one is IP spoofing attack and another is URI spoofing attack, which are designate in this paper. The implementation of VoIP concerned by businesses, components of a VOIP system, and related security issues. The business apprehensions will be those which are used to affect the Quality of Service (QoS). The network components gateways, call processors and two of the more mutualdesignsapprehended by VoIP.

Keywords:-VoIP, MGCP, H.323, SIP, Spoofing attacks, QoS.

1.INTRODUCTION: - Voice over Internet protocol (VoIP) is a form of communication that allows the end-user to make telephone calls over a broadband internet connection. Basically VoIP is revolutionizing the world of communication. VoIP technology is used to transmit voice message over a data network using IP. Such data network may be the internet or a corporate intranet or managed networks which are specially used by long distance and local service traditional providers and ISPs (Internet Service Providers).Interconnected VoIP services are also permitting you to make and receive call to and from old-style landline numbers, usually for a service fee. Other services allow to end-users to use own landline phone, it is used to replace VoIP calls. All these patterns are held by a special adapter.

The history of VoIP originated with conversations by a few computer users over the internet. Initially, VoIP required a headset to plug into the computer, and the members could only communicate with other who had a alike or related set-up. In November 1977, the IETF published the ‘specifications for the NVP (network voice protocol). In the introduction to this document, the purpose for the research were explained as the growth and complaint of the feasibilityof secure, full-duplex1,real time, high-quality, low-bandwidth, digital voice communications over packet switched computer communication network.

In its early periods, the VoIP technology was not enough mature. There was a big gap between the technological reality and the marketing structure. In the mid-90s, IP networks were rising, the technology had improved and the use of personal computers had grown broadly. The communications network providers are used



To adopt IP in their infrastructure, enterprises are adopting IP for private corporate networks. The communication between employees facilitate by using this technique whether working at home, travelling or at corporate locations. VoIP can also enlargecommercialefficiencies.

2.IMPLEMENTATION OF VoIP: - in this section basically we discuss three things, first one is VoIP protocols and after that how data process in VoIP and at the last we will discuss Quality of Services (QoS) in Voice over Internet protocol.

a. Protocols

In VoIP implementation three types of protocols which are widely used the (MGCP) media gateway controller protocol, the Session Initiation Protocol, and the H.323 family of protocols

- *H.323 family of protocols*

  H.323 is contains family of protocols and a set of endorsements from the (ITU) international Telecommunication Union that are used for many functions related to calls like setup a call , its registration, authentications, also call termination function and similar other functions. These protocols convey from one place to another over TCP or UDP protocols. The figure 1 shows the various H.323 protocols with their moving mechanisms. The H.225 consists by H.323 family of protocols are used for call signaling, admission, and registration purpose. To establish and control the media sessions H.225 is used. T.120 is used for conferencing applications in which a shared white board application is used. The G.7xx series by H.323 is defined the audio codec and H.26x series of specifications is defined the video codec. For media transport H.323 uses RTP and the purpose of controlling RTP sessions RTCP is used. The figure 2 and 3 shows the call-setup process and H.323 architecture.

- *Session Initiation Protocol (SIP)*

  The SIP is a text-based protocols, it is an alternative to the complex H.323 protocols and similar to HTTP. The IETE which is used for modification and termination session between two and more participants is defined by the (SIP) Session Internet Protocol.This type of protocol becomes more popular in comparison to H.323family of protocol because it is more similar than it. The following figure 4. Shows the SIP architecture and figure 5 Shows the call-setup and tear down process.

Fig.1 H.323 Protocol family

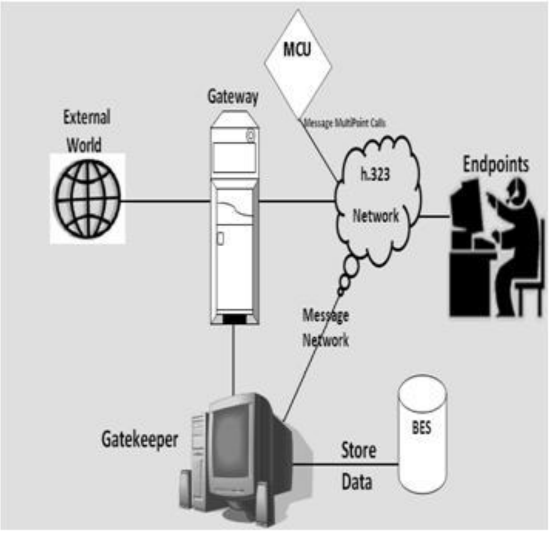


Fig.2 H.323 Architecture [2]

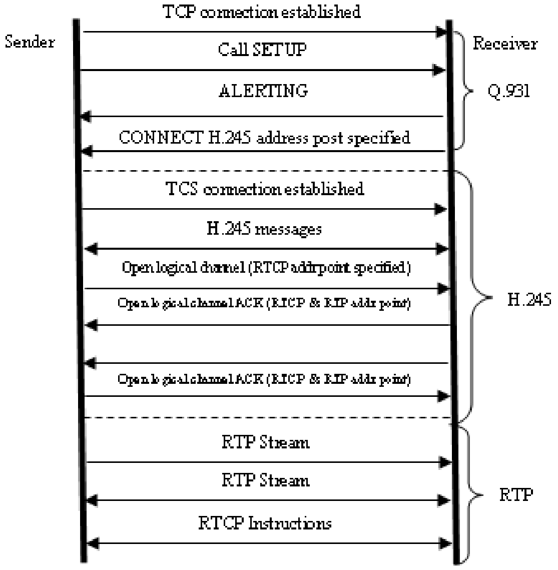

Sender
Receiver
TCP connection established
Call SETUP
ALERTING
Q.931
CONNECT H.245 address post specified
TCS connection established
H.245 messages
Open logical channel (RTCP addrpoint specified)
Open logical channel ACK (RTCP & RTP addr point)
H.245
Open logical channel ACK (RTCP & RTP addr point)
RTP Stream
RTP Stream
RTP
RTCP Instructions

Fig.3 H.323 call setup process

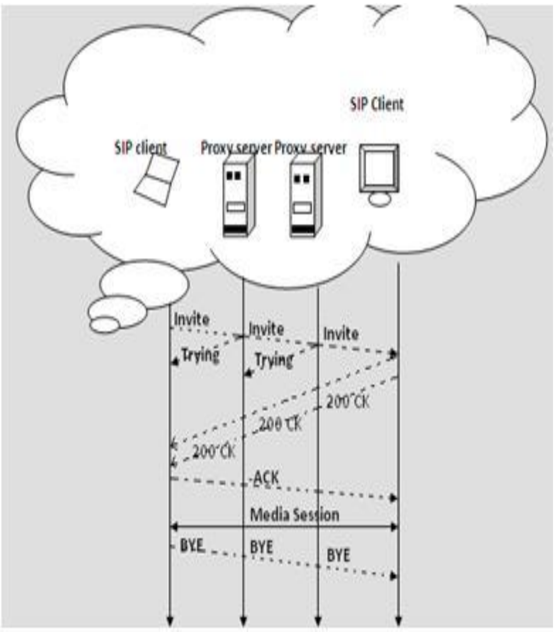


Fig.4 SIP Network Architecture

- Media Gateway Control Protocol (MGCP)

It is a complementary protocol to H.323 and SIP. The process of communication between the separate components of a decomposed VoIP gateway is done by Media Gateway Control Protocol. When we are using these servers MGCP and MGP, 'Call agent' is compulsory and manage conferences and calls that shown in (figure 6). The Media Gateway endpoint is not responsible for calls and conferences. It does not maintain call states.

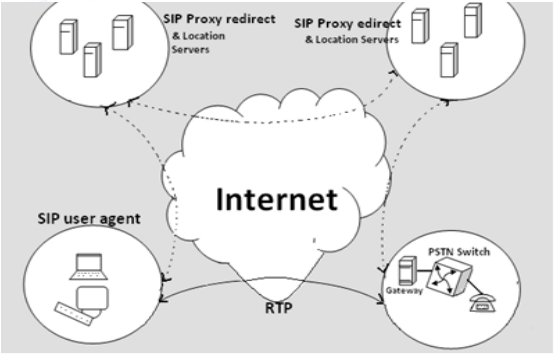


Fig.5 Call setup and Tear down in SIP

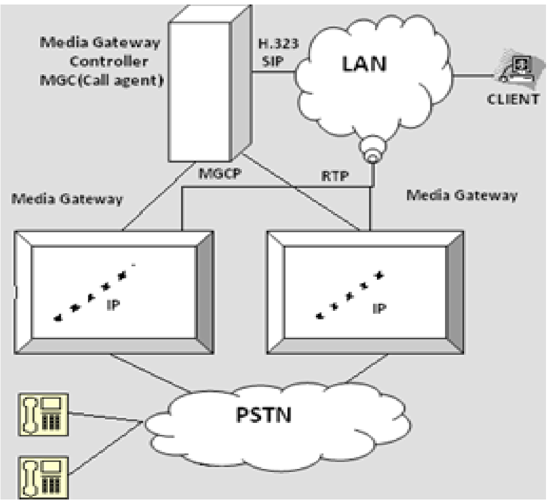


Fig.6 MGCP Architecture

The command which is sent by the MGC call agent is executed by MGs. MGCP assumes that call agents will synchronize with each other sending coherent commands to MGs under their control. The mechanism for synchronizing call agents does not define by MGCP. MGCP is a master/slave protocol with a closely coupling between the endpoint and server.

b. *Data Processing in VoIP Systems*

There are three types of needed components in VoIP. CODEC, Packetizer, and playout buffer. At the sender’s side the analog voice signals are converted into digital voice signals, after that these digital signals are compressed and then encoded into a predetermined format via voice codec. The Telecommunication Union Telecommunication (ITU-I) developed and standardized various voice codec such as G.729, G.723, and G.711 etc. The packetization process is performed by distributing fragmented encoded voice into equal size of packets.

Furthermore, in each and every packet, selected protocol headers from different layers are committed to encoded voice. Which Protocols headers added to voice packets are of real-time transport protocol (RTP), Internet Protocol (IT), and User Datagram Protocol (UDP) as well as Data Link Layer header. The RTCP and RTP were designed to support real-time applications at the Application layer. The UDP protocol is more suitable for VoIP applications and it cannot be applied to VoIP technology.

Then the packets are sent to its destination over IP network, where the reverse process of decoding and depacketizing of the received packet is carried out. A play out buffer is used at the receiver end to transfer the packets without any interruption. Fig.7 shows end-to-end transmission of voice in VoIP system.

The signaling protocol of VoIP namely Session Initiation Protocol (SIP) and H.323 are required to establish VoIP calls and at the end to close the media streams between the clients.

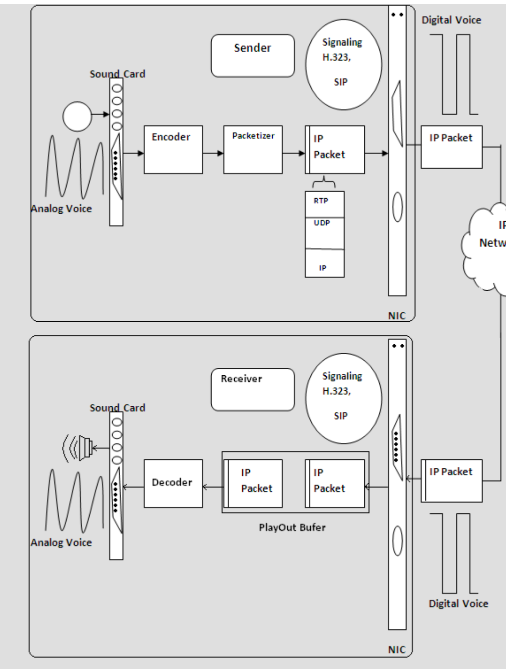


Fig.7 End-to-End voice transmission

c. Quality of Service (QoS) in VoIP

It can be defined as the network ability to provide good services that satisfy its customers. And we can say QoS is used for measurements of the degree of user satisfactions. If degree of satisfaction is higher that means the QoS is also higher

QoS are briefly described as given below:

- Delay

  Delay can be categorized into three categories: delay at the receiver, delay at the source and network delay. It can be defined as the total time it take since a person, communicating another person, speaks words and hearing them at the another end.

- Jitter

  IP network does not guarantee of packet delivery time which introduce variation in transmission delay. This variation is known as Jitter and it has more negative effects on voice quality.

- Throughput

  The throughput may be defined as the maximum number of bits received out of the total number of bits sent during an interval of time.

- Echo

  Echo is the term of the reflections of the sent voice signals by the distant end. In PSTN network uses echo signals could be electrical echo.

3.CONFIGURATION OF VoIP:-

Dedicated router

These devices allow any user to use its own traditional phone to place VoIP calls. They are connected to cable and allow any user to attach an ordinary telephone. Once these routers are configured with an appropriate VoIP provider and service plan, there is no necessity for special software with a computer. In fact, there is only need to pick up your phone and dial a number at the dial tone. You can also bring your own adapter with you when you travel and make calls wherever broadband internet access is available.

Adapter (USB)

They usually come in the form of USB adapters that are slightly larger than the typical thumb drive. It also allows you to use a traditional phone to place VoIP calls.

Software-controlled VoIP applications: "softphones"

There are many softphones that allow you to place VoIP phone calls directly from an ordinary computer with a microphone, headset and sound card. Software-based VoIP applications are quite attractive to consumers because they often already have most of the components necessary to get started at little to no cost.

Dedicated VoIP phones

A VoIP phones looks like an ordinary cordless and corded telephone, and it attaches directly to a PC network rather than a traditional phone line. A dedicated VoIP phone may consists of a base station and phone that connect to the internet. Similar to adapter, dedicated VoIP phones also require aprovider as well as a required service plan.

4.VoIP ATTACKS:-

Malformed Message attacks

Malformed Message Attacks is one of the most representative cases using the vulnerabilities of text-based protocols. These attackers are cause malfunctions of proxy server by manipulating SIP headers. For instance, overflow-null, overflow-space, specific header detection and using non-ASCII code are involved in these malformed message attacks.

SIP Flooding Attacks

IP phones generate request or responses to send to a specific UA, called by the target. Asoutcome, a single UA is overcome by receiving extreme SIP messages within a short duration of time, so that the UA cannot provide usual services. INVITE flooding is one of the most archetypal attacks. Essentially, the issue of IP layer is flooding attack. In case of INVITE flooding, after all, it could be higher annoying attack for the VoIP user because the one should see many call requests at the same time and hear ringing of calls.

Spoofing attack

This type of attacks can take a variety of different forms; For instance, an attacker can change in the protocols which are used as the IP. Spoofing can be done when an attacker search to be someone else in order gain access to restricted resources or steal information. Also, an attacker may send fraudulent emails and set up fake website in order to capture user's account information like –user's passwords and login names. A phishing attack is any fake email and website. Another type of spoofing involves setting up a fake wireless access point and tricking victims into connecting to them through unauthorized connections.

Two kind of spoofing attacks are possible: IP spoofing attack and URI spoofing attack. IP spoofing attack is to make a way for IP source addresses in order to feign a trusted user and IP spoofing having the intrinsic security problem in TCP/IP protocol suites and it is not in the scope of our study in VoIP security. The URI spoofing attack is a particular case in malformed message attacks. The attacker who takes hostage SIP messages between the UAs forges their URI field, so the attacker can hide himself from trace backs. If spoofed BYE requests are sent to victims then the call is terminating by this attacker.

Threats / risks

Many of the threats associated with VoIP are similar to the threats inherent to any internet application. The operators which are use are aware with the difficulties of email abuse in the mode of spam. VoIP opens yet additional pathway for these exasperations, which can lead to SPIT, spoofing and identity theft.

Spam over internet telephony (SPIT)

VoIP spam is nonessential, automatically dialed, pre-recorded phone calls using VoIP and it is similar to E-mail spam.

Spoofing

IT is technically possible for an attacker to masquerade as another VoIP caller. For example, an attacker could conceivably inject a bogus caller ID into an ordinary VoIP call so that the receiver believes the call to be coming from a trusted and identified source. The receiver, mislead by the electronic identification of the caller, may place unjustified trust in the person at the other termination. In such an conversation, the receiver may be tricked into disclosing personal information like-account numbers, social security numbers, or secondary verification factor: a mother's first name, for example. This scheme is necessarily the VoIP version of outdated phishing, where operator follows links in an unwanted email and is tricked into providing personal information on a false website. Aggressors may usage these bits and pieces of personal information to complete partial identity record of victims of identity theft.

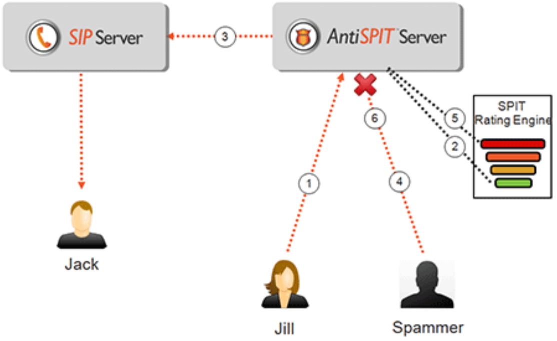


Fig.8 SIP and SIPT server

Confidentiality concerns

The concern is that VoIP data sometimes travels encrypted over the internet. Thus it is officially possible for someone to collect VoIP data and attempt to reconstruct a discussion. Although it is veryproblematic to attain, some software program are designed to piece together bits and piece of VoIP data in an effort to reconstruct discussions. Although such activity is nowinfrequent, you should be conscious of this opportunity as it may increase as VoIP become more widespread.

5.HOW TO PROTECT AGAINST RISKS:-

The "voice VLAN" is a special access port feature of Ethernet switches which allow IP phones to configure automatically and easily associated to a logically separate VLAN. This feature allows a PC to be daisy chained to an IP phone and connection for both phone and PC to be trunked through the same physical Ethernet cable. This feature provides various benefits, but the one important benefit is when the voice VLAN is enabled on a switch port that is also enabled to allow simultaneous access for a regular PC.

Enabling voice VLAN raises the complexity to properly secure these Ethernet port. Enabling without the proper security controls in place can increase the risk to an organization.

There are several types of principle as well as practices for safe VoIP usages are the same. However, you may already practice with other internet applications. For good personal computing these are the key practices:

- We can use anti-virus and anti-spyware programs.
- We can also use a firewall.
- Back-up, identify, and secure your data like- personal and financial.
- Use and maintain a strong password.
- We can update and patches our application software.
- Be careful about opening files attached to instant messages or Email messages.
- Always verify the authenticity and security of new software and downloaded files.
- Securely configure your web browser(s).
- Do not reveal personal information to persons to whom you don't know individuality.

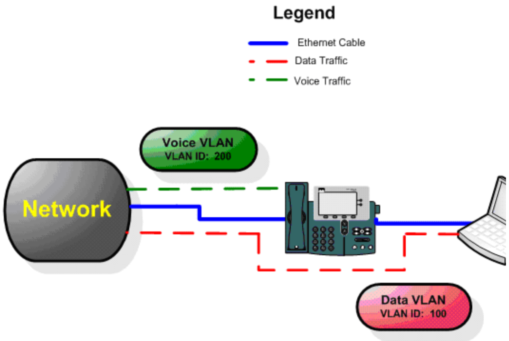


Fig.9 A typical VoIP scenario

6.REQUIREMENTS, AVAILIBILITY AND SERVICE LIMITATIONS:-

If you want to consider about VoIP services you should not assume its features, options and functionality. These will equal to those traditional landlines. You should be familiar with these availability, requirements and possible service limitation of VoIP service before switching to VoIP as either a primary means of communication or an enhancement to your current service.

Requirements

VoIP requires a connection to the internet through an ISP, a VoIP service to spread the reach to old-style landlines, and VoIP software to truly place calls. Plain old telephone services (POTS) requires none of these fundamentals. It is important to note that the DSL internet services use the traditional phone lines for your internet connection. For that case, you already have telephone service to begin with. You may wish to weight to expected benefits of VoIP against these cost. Thesecost are given to your current operating environment.

Availability due to bandwidth

VoIP services always require a high-speed internet connection to provide a reliable functionality. Even given typical broadband connection degradation of quality, service interruptions, speeds and though is possible due to high internet traffic. For example, if you are trying to place a VoIP call while other people are using a lot of bandwidth on the same internet connection, then the sound quality of your own VoIP call may also be affected.

7.CONCLUSIONS:-

Security for a VoIP system should begin with solid security on the internet network. It should be protected from the threats of attached hostile networks and the threats of the internet network. The security policy includes any specific VoIP requirements.

The load of the VoIP system should be housed

By the servers and network involved, confirming that proper resources are in place is present. A devoted VoIP phone may contains of a base station and phone that connected to internet or it may also operate on a local wireless network. Conducting a risk analysis of each component and process will identify the susceptibilities and threats.

This will offer the information needed to determine proper measures. There should be a proper valance balance between the security and business needs of the organization. It is the key to the success of any VoIP arrangement.

8.BIBLIOGRAPHY

[1]. H. Yong-feng, Z. Jiang-ling, "Implementation of ITU-T G.

729 speech codec in IP telephony gateway" Wuhan University
Journal of Natural Sciences, Volume 5, Number 2, June 2000.

[2]. M. Habib, N. Bulusu, "Improving QoS of VoIP over WLAN
(IQ-VW)", Project Research Paper, for CS522 Computer
Communications, University of Colorado at Colorado
Springs, December 2002.

[3]. P. M. Athina., A. T. Fouad and J. K. Mansour, "Assessing the
Quality of Voice Communications Over Internet Backbones",
IEEE/ACM Transactions on Networking, Vol. 11, No. 5, Oct.
2003.

[4]. Qiu, P.Q., Monkewich, O., and Probert, R.L., "SIP
Vulnerabilities Testing in Session Establishment and User
Registration" ICETE (2), 223-229., 2004.

[5]. J. B. Meisel, M. Needles, Voice over Internet protocol (VoIP)
development and public policy implications, Info 7, 2005.

[6]. Advisory Committee on International Communications and
Information Policy (ACICIP), 2005.

[7]. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, Security
Considerations for Voice over IP Systems, Recommendations
of the National Institute of Standards and Technology, NIST
Special Publication 800-58, 2005.

[8]. http://www.isoc.org/pubpolpillar/voip-paper.shtml
15.08.2006.
http://www.eyeball.com/spit-solution.htm.

[9]. K. M. McNeill, M. Liu and J. J. Rodriguez, "An Adaptive
Jitter Buffer PlayOut Scheme to Improve VoIP Quality in
Wireless Networks", IEEE Conf. on BAE Systems Network
Enabled Solutions, Washington, 2006.

[10]. C. Lin, X. Yang, S. Xuemin and W.M. Jon, "VoIP over
WLAN: Voice capacity, admission control, QoS, and MAC",
International Journal of communication Systems, Vol.19, No
4, pp. 491-508, May 2006.

[11]. L. Mintandjian, P.A. Naylor, "A Study Of Echo In Voip
Systems And Synchronous Convergence Of The μ-Law
Pnlms Algorithm", 14th European Signal Processing
Conference (EUSIPCO 2006), Florence, Italy, September 4-8,
2006.

[12]. Seedorf, J., "SIP Security: Status Quo and Future Issues",
Talk presented at 23rd Chaos Communication Congress,
2006.

[13]. Russel, T., "Session Initiation Protocol (sip) Controlling
Convergent Networks" McGrawHill Professional, 2008.