AN OVERVIEW OF VOICE OVER INTERNET PROTOCOL (VOIP)

Ajay Kumar*
Graduate student, M.S. in Computer Science Program, Rivier College

Keywords: *Internet, VoIP, SIP, PBX, Jitter*

Abstract

The primary purpose of this article is to discuss the main issues of Voice over Internet Protocol (VoIP), particularly the security issues and challenges, as well as to analyze an example case study. This project also reviews the VoIP basics and advantages and disadvantages of this protocol.

1 Introduction

Because of the prevalence of the Internet, and because IP is the protocol connecting almost all devices, VoIP is a powerful service platform for next-generation application**.**

Voice over IP (VoIP) uses the Internet Protocol (IP) to transmit voice as packets over an IP network. Therefore, VoIP can be achieved on any data network that uses IP, like the Internet, Intranets and Local Area Networks (LAN). Here the voice signal is digitized, compressed and converted to IP packets and then transmitted over the IP network. Signaling protocols are used to set up and tear down calls [1], carry information required to locate users, and negotiate capabilities.

VoIP introduces the actual method of transmitting voice over an IP network and IP telephone. It describes telephony devices that use IP as the native transport for voice and call signaling. IP telephony needs VoIP to send calls over the network

2 Purpose

The purpose of this article is to discuss the security issues of VoIP, the business cases for VoIP, and potential benefits that a converged network provides and uses them as the factor in the Return–On-Investment (ROI) calculations. The following topics will be covered:

- VoIP protocols
- Security issues
- Case study
- Potential Benefits of the Converged Network.

3 VoIP Protocols

There are a number of protocols that may be employed in order to provide the VoIP communication services. In this section, we focus on most common aspects for the majority of the devices already deployed or being deployed today.

Virtually every device in the world uses a standard called Real-Time Protocol (RTP) for transmitting audio and video packets between communicating computers. RTP is defined by the Internet Engineering Task Force (IETF) in the *Request For Comments* (RFC) 3550. The payload formats for a

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

number of CODECs are defined in RFC 3551, though payload format specifications are defined in various ITU documents and in other IETF RFCs. RTP also addresses the issues like a packet order and provides mechanisms (via the Real-Time Control Protocol, or RTCP, defined in RFC 3550) to help address delay and jitter.

The H.323 Protocol and Session Initiation Protocol (SIP) both have their origins in 1995 as researchers looked to solve the problem of how two computers can initiate communication in order to exchange audio and video media streams. H.323 enjoyed the first commercial success, due to the fact that those working on the protocol in the ITU worked quickly to publish the first standard in early 1996. SIP, on the other hand, progressed much more slowly in the IETF, with the first draft published in 1996, but the first recognized "standard" published later in 1999. SIP was revised over the years and re-published in 2002 as RFC 3261, which is the currently recognized standard for SIP. These delays in the standards process resulted in delays in market adoption of the SIP protocol.

Today, H.323 still commands the bulk of the VoIP [2] deployments in the service provider market for voice transit, especially for transporting voice calls internationally. H.323 is also widely used in room-based video conferencing systems and is the main protocol for IP-based video systems. SIP has, most recently, become more popular for use in instant messaging systems.

3.1 Session Initiation Protocol

The Session Initiation Protocol (SIP) is an application-layer signaling-control protocol used to establish, maintain, and terminate multimedia sessions. Multimedia sessions include VOIP, conferences and other similar applications involving such media as audio, video and data.

SIP, on which the RFC 2543 is based, is a text-based protocol that is a part of the overall Internet Engineering Task Force (IETF) multimedia architecture. The IETF architecture also includes the Resource Reservation Protocol (RSVP; RFC 2205), Real-Time Transport Protocol (RTTP; RFC1889), and Session Description Protocol (SDP; RFC 2327). However, the SIP's functions are independent of any functions of these protocols [1]. It is important to note that SIP can operate in conjunction with other signaling protocols, such as H.323.

3.2 Overview of SIP operations

Callers and callees are identified by the SIP addresses. When making a SIP call, a caller first needs to locate the appropriate server and send it a request. The caller can either directly reach the callee or indirectly through the redirect servers. The Call ID field in the SIP message header uniquely identifies the calls. Below is the brief explanation of how the protocol performs its operations (RFC 2543).

3.2.1 SIP Addressing

The SIP hosts are identified by a SIP URL, which is of the form `sip:username@host`. A SIP address can either designate an individual or a whole group.

3.2.2 Locating a SIP server

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

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

3.2.3 SIP Transaction

Once the host part of the Request URI has been resolved to a SIP server, the client can send requests to that server. A request together with the responses triggered by that request makes up a SIP transaction. The requests can be sent through reliable TCP or through unreliable UDP [1].

3.2.4 SIP Invitation

A successful SIP invitation consists of two requests: an `INVITE` followed by `ACK`. The `INVITE` request asks the callee to join a particular conference or establish a two party conversation. After the callee has agreed to participate in the call, the caller confirms that it has received that response by sending an ACK request. The `INVITE` request contains a session description that provides the called party with enough information to join the session [1]. If the callee wishes to accept the call, it responds to the invitation by returning a similar session description.

3.2.5 Locating a User

A callee may keep changing its position with time. These locations can be dynamically registered with the SIP server. When the SIP server is queried about the location of a callee, it returns a list of possible locations. A Location Server in the SIP system actually generates the list and passes it to the SIP server.

3.2.6 Changing an Existing Session

Sometimes we may need to change the parameters of an existing session. This is done by re-issuing the `INVITE` message using the same Call ID, but a new body to convey the new information.

3.2.7 The hop server

After the User Agent Server (UAS) has been reached, it sends a response back to the proxy server. The proxy server in-turn sends back a response to the client. The client then confirms that it has received the response by sending an `ACK`. In this case, we had assumed that the client's `INVITE` request was forwarded to the proxy server. However, if it had been forwarded to a redirect server, then the redirect server returns the IP address of the next hop server to the client then directly communicates with the UAS.

4 VoIP Technology

4.1 VOIP Benefits

The main advantage of VoIP is the cheaper option for the phone calls [10]. Another key advantage is being able to combine phone calls with business data. It means you can adopt call-centre style technology with each incoming call triggering on-screen pop ups with customer details. Or you can add a ‘Click to call’ button on your website.

When you consider that the average employee spends hundreds of hours a year on the telephone, it’s easy to see why VoIP is attracting a lot of attention. Many large organizations from banks to retail companies are using it for voice calls.

As the cost of high-speed Internet access (such as Broadband) comes down, VoIP is now within reach of small businesses. Some telecommunication companies and Internet Service Providers (ISPs) are now offering Voice over IP deals targeted at the small business sector.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

Traditional phone calls work by allocating an entire phone line to each call. With VoIP, voice data is compressed, and with VoIP on your computer network you can add telephones and increase call capacity without running additional cabling.

4.1.1 Scalability

Traditional PBX (Private Branch Exchange) phone systems have a set number of ports for telephones to plug in to. VoIP systems provide greater flexibility as you can run a number of 'virtual users' through each network socket.

4.1.2 Reduce operating costs

Because a VoIP-enabled system is based on software rather than hardware, it is easier to manage and maintain the system.

4.1.3 Improve productivity

VoIP treats voice as if it were any other kind of data, so users can attach documents to voice messages or participate in virtual meetings using shared data and videoconferencing.

4.1.4 Wireless-compatible

With a wireless LAN in place, mobile devices like PDAs and smart-phones can use your VoIP system. If you install a wireless LAN, you need to make sure you have appropriate security ensures in place, such as a firewall or encryption.

4.1.5 Enhanced customer service

By adding a 'Click to talk' button to a website, a VoIP-enabled enterprise can put web users in touch with customer service staff. You could also look at implementing customer relationship management software (CRM). Incoming calls could automatically trigger screen pops with customer account information and contact history.

4.1.6 Dependable call management

Voice-related services, such as follow-me roaming, caller-ID, call forwarding and broadcast messaging, become simpler to maintain and can be updated as needed by your employees.

4.1.7 Flexibility

A Virtual Private Network (VPN) is an allocated amount of bandwidth on the public internet where public access is prevented through encryption. If your company has its own VPN and combines it with VoIP, you can set up a fully functioning office where there is a broadband connection. Green-field sites can be up and running in minutes not weeks

5 VOIP Analysis

To create a proper network design it is important to know all the caveats and inner workings of networking technology [10]. This section explains many of the issues facing Voice over IP.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

5.1 Delay/Latency

VoIP delay or latency is characterized as the amount of time for speech to exit the speaker's mouth and reach the listener's ear.

There are three types of delay.

5.1.1 Propagation Delay

Propagation delay is caused by the speed of light in fiber or copper-based networks.

5.1.2 Processing delay

Processing delay defines many different caused of delay and is caused by devices that forward the frame through network.

5.1.2 Serialization delay

Serialization delay is the amount of time it takes to actually place a bit or byte onto an interface.

5.2 Jitter

Jitter is the variation of packet inter-arrival time. Jitter is one issue that exists only in packet-based networks. While in a packet voice environment the sender is expected to reliably transmit voice packets at a regular interval. These voice packets can be delayed throughout the packet network and not arrive at the same regular interval at the receiving station

If the data network is engineered well and the proper precautions are taken [10], then jitter is not usually a major problem, and the buffer does not significantly contribute to the total end-to-end delay.

The jitter buffer found within Cisco software is considered a dynamic queue. This queue can grow or shrink exponentially depending on the inter-arrival time of the RTP packets.

5.3 Voice Compression

Two basic variations of 64-kbps Pulse Code Modulation (PCM) are commonly used: μ-law and α-law. These methods are similar. They both use logarithmic compression to achieve 12-13 bits of linear PCM quality in 8 bits, but they are different in relatively minor compressions details. It is important to note that when making a long distance call, any required conversion is the responsibility of the converting country.

5.4 Echo

Echo is normally caused by a mismatch in impedance from the four-wire network switch conversion to the two-wire local loop. Echo can be loud, and it can be long. The louder and longer the echo, the more annoying the echo becomes. To understand how echo cancellers work, it is best to first understand where the echo comes from.

Echo cancellers are limited by the total amount of time they wait for the reflected speech to be received, a phenomenon known as echo tail.

It is important to configure the appropriate amount of echo cancellation when initially installing VoIP equipment. If it is not configured properly callers will hear echo during the phone call.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

5.5 Packet Loss

Packet loss in data networks is both common and expected. Many data protocols, in fact, use packet loss. The protocols identify the condition of the network and can reduce the number of packet loss in that network.

When putting voice on data networks, it is important to build a network that can successfully transport voice in a reliable and timely manner. Also it is helpful when a mechanism can be used to make the voice somewhat resistant to periodic packet loss.

5.6 Voice Activity Detection

In normal conversations, some one speaks and someone else listens. Modern network contains a bi-directional, 64,000 bit-per-second channel, regardless of anyone is speaking. This means that in a normal conversation at least 50% of total bandwidth is wasted.

By using VoIP, this wasted bandwidth can be utilized for other purposes when voice activity detection (VAD) is enabled. Typically, when the VAD detects a drop-off of speech amplitude, it waits a fixed amount of time before it stops putting speech frames in packets. This fixed amount of time is known as *handover* and is typically 200 ms.

5.7 Digital-to-Analog Conversion

Digital-to-Analog conversion issues also currently plague toll networks. Each time a conversion occurs from digital to analog and back, the speech or waveform becomes less true. Although modern toll networks can handle at lease seven D/A conversion before voice quality is affected, compressed speech is less robust in the face of these conversions

It is important to note that D/A conversion must be tightly managed in a compressed speech environment [10]. The only way to manage D/A conversion is to have the network designer design VoIP environments with as few D/A conversion as possible. Although D/A conversion affect all voice networks, VoIP networks using PCM CODEC are just as resilient to problems caused by D/A conversions as modern telephony networks.

5.8 Tandem Encoding

The circuit switches are organized in a hierarchical model in which switches higher in the hierarchy are called *tandem switches*. If the TDM switches compress voice and the tandem switch must decompress and recompress the voice, the voice quality can be drastically affected. Voice degradation occurs when there is more than one compression/decompression cycle for each phone call.

5.9 Dial-plan Design

One of the areas that causes the largest amount of problems when designing a VoIP network is the dial plan. The causes of these issues might be due to the complex issues of integrating disparate networks. Many of these disparate networks were not designed for the integration. Most of the companies must decide on their dial-plan design based on the plans for growth, cost of the leased circuits or Virtual Private Networks (VPNs), cost of additional equipment for packet voice, number of overlaps, and call-flows.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

6 Case Study

VoIP might well be in the "TO DO" list for many companies. Therefore, if a company is considering VoIP or expanding the use of VoIP applications, it is very important to revisit the company's existing network and find out if the network can support high-quality voice transmissions. This article outlines what are the main factors to be considered when assessing for VoIP readiness.

There are four important factors to ensure the network is ready to handle the increased network load and ensure proper configuration so voice traffic will run efficiently. They are: Building a Network Inventory, Utilization Assessment, Bandwidth Modeling, and VoIP Quality Assessment.

6.1 Network Inventory

To do the network inventory, it is necessary to take into account for the entire infrastructure to support a VoIP deployment. Routers, Switches and links are configured to support the data network. VoIP traffic is extremely time-sensitive. Therefore, voice packets cannot be queued and must have priority over data information. If the network is not configured correctly, it will result into sound jittery. So this analyses will help the network administrator to assess whether any hardware upgrades or additional hardware upgrades is necessary to support the converged voice and data's network. It is very important to test each component of the converged network to ensure the support of voice and data and reduced the probability of jitter, packet loss, low latency, and clogged bandwidth.

6.2 Utilization Assessment

Firstly, it is an import requirement to find the network utilization of the network devices and links like gathering data on routers, switches and WAN links to find their capacity for carrying VoIP traffic looking for information of queuing and drops, bandwidth, CPU and memory.

6.2.1 Utilization Assessment tool

Collecting the data network utilization of the devices and links can be very time consuming. NetIQ solutions can not only automate the process, but also provide extensive reporting on the results. These reports provide guidelines to understand the performance of the applications and systems. Trend analysis reports will help to plan for system or application upgrades. The alert summary reports also collect information about the response times, which can be used to define any action to be taken.

6.2.2 Bandwidth Modeling

Four key parameters that provide the data necessary for a successful model are bandwidth capacity, utilization, number of calls, and type of CODEC used. When measuring bandwidth capacity and utilization, obtain the data from various times in the day and measure the number of calls as the total number of calls to support at any given moment.

Determine the correct CODEC is crucial to call quality and bandwidth used. CODECs that require 64-kbps rate provide a higher call quality but also require more bandwidth. One that requires a lower rate may allow more calls, but could lower the call quality.

Hence calculating the projected call volumes [14], CODEC selections and bandwidth requirements as input is the simple type of modeling. This determines the amount of bandwidth needed to support VoIP. It should be done on a very regular basis with different variables.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

6.3 VoIP Quality Assessment

VoIP quality assessment is a key component. Voice traffic places a new set of requirements on data networks with the goal being to provide excellent call quality, which is measured on the average means opinion score (MOS) assigned to the traffic. The MOS takes into account the calculations such as code, delay, lost data, and jitter buffer loss that can affect call quality. Higher MOS means higher call quality. Simulating voice traffic on the network is the best practices before installing the first IP phone to measure network's call quality. It should be measured at every location or call group that will be deployed. It should also test at various times and locations to establish a comprehensive assessment.

6.4 Example Case study Analysis

To do this analysis, let us consider a company that has about 60 users and has offices in Pittsburgh, PA (10 users), International Office in Montréal, Canada (60 users), London, UK (250 users), Singapore (6 users), Shanghai (2), and users in the United States that are connected to the U.S. office via VPNs.

Let us also assume that this company has three T-1 lines and one PRI line, and the company spends approximately $4200 a month. In addition, the company is looking for VoIP installation and doing an analysis on what are the *pros* and *cons* of it and what would be Return on Investment (ROI). The cost benefit will be estimated as well.

The following section discusses the example of VoIP installation analysis and the ROI estimation based on the Quintum calculation.

6.4.1 Calculation of the Return on Investment for Quintum VoIP installation

Let us consider the following scenario for the organization:

Average number of calls per hour:	100 calls
Average call duration in minutes:	5 minutes
Number of working hours per day:	8 hours
The number of working days per week:	5 days
The number of working weeks per month:	4 weeks
Total number of minutes per month:	80,000

Percentage of national calls – 70% @ $0.05 per minutes for calls over the PSTN
Percentage of international calls – 30% @ $0.10 per minute for calls over the PSTN
Total number of minutes (national) 56,000 @ $0.05, then the monthly charges is $2,800
Total number of minutes (international) 24,000 @ $0.10 then monthly charges is $2,400
Total PSTN charges per month without VoIP will be 5,200.

After the implementation of VoIP, let us consider we still use PSTN 10% only, and then we will have the following estimations:

Percentage of completion over IP 90% @ 0.000, then monthly charges is $0.00
Percentage of calls completed over PSTN; 7% National calls @ $0.05 is $280
Percentage of calls completed over PSTN: 3% International calls over PSTN: $240
Total PSNT call charges $520
Monthly cost of IP usage for VoIP is: $100.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

The saving for PSTN call charges per month with VoIP is: $4580.00

Cost of the Quitum VoIP equipment is $8800.

Time taken to recoup the cost is 1.92 months.

Therefore, just in 1.92-month period our case-study company can recoup the saving and can be up to $4500 per month.

7 Advantages and Disadvantages of VoIP networks

7.1 Advantages of VoIP networks

The advantages include the reduction of costs. VoIP is relatively inexpensive**.** This is the biggest advantage to most companies. VoIP is technically free. Typically, companies pay their normal high-speed Internet provider and in return receive VoIP free [12]. These companies can connect with almost anyone and at almost anytime.

VoIP creates a phone system that eliminates many problems. One example is that VoIP allows a company to route telephone calls to one location instead of several. The advantage of this is that the companies do not have to keep as many employees on staff. This fact saves money, and the companies are able to reroute the calls to the appropriate person or place with very little effort and can do this within or outside of multiple buildings in multiple cities.

The second major advantage of VoIP is that it is mobile. It means that any employee can take it with them on business trips, vacations, etc. All you have to have is a high-speed Internet connection to use this from anywhere. You can check in at the office while on vacation or you can use it to call your office for hundreds of reasons while on business trips. This is particularly nice for people who want to work from home. With VoIP, people are able to complete their work from the comfort of their own couch. Today, people can sit at home, take care of their children, and still earn a decent paycheck via VoIP.

7.2 Disadvantages of VoIP networks

The major problem with Voice over IP for companies and customers is that there are some reliability problems. If the customer runs too many programs at one time, there are risks of getting disconnected. This has to be aggravating, because what are the chances of redialing and getting the same person? Slim to none. This means that you have to sit on hold again, repeat everything you told that person, etc. It is a nightmare depending on who you were calling.

Companies have problems with Voice over IP in many of the same ways [12]. They have too many employees on too many applications and, using Voice over IP, they have dropped calls and sometimes full system shut-downs. While this is not as common within companies, it is still happening.

The other major problem with Voice over IP is the call quality. Sometimes there is static or echo, when you are using an Internet connection to complete the call. Turning down the volume on the headset, microphone, and/or speakers should help tone down the problem, if it does not get rid of the problem completely.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

While there are several other smaller problems that are associated with Voice over IP, there are hundreds of developers improving these services everyday. The developers are currently creating built-in generator systems in case the electricity goes out, improving all of the problem areas, and enforcing the new government law stating that any provider has to offer 911 services.

8. Voice-over-IP Implementation Options

While the VoIP market continues to evolve, the current universe of VoIP implementation options can be segmented into four broad categories (PBX-based gateway, Router-based gateway, PC-based gateway, and intelligent multi-path switching gateway). Each of these has its own advantages and disadvantages.

8.1 PBX-based gateways

The leading manufacturers of PBX equipment are all introducing their own solutions to the VoIP challenge. With their significant market-share and mind-share among corporate telecom managers, these companies are well-positioned to capture a sizable piece of the early VoIP market. From a technical point of view, these companies can effectively integrate the management of VoIP functionality with the existing corporate voice communications platform. They also have many years of experience building hardware and software that meets the reliability standards of the voice market.

The downside is that these vendors have minimal experience in IP-centric data networking. Without strong expertise in the vagaries of connectionless, non-determinate protocols, it is unclear how well they will be able to address the issues of voice signal quality in the IP world. And, as strong as their market position may be among telecom buyers and distribution channels, it is extremely weak on the data communications side of the equation. This may hamper PBX vendors' long-term ability to achieve dominance in a world dominated by IP innovators.

Perhaps the biggest drawback to the PBX-based approach is that this class of solution is tied so directly to highly proprietary PBX platforms. The leading PBX vendors have no demonstrable track record in either defining or adopting the types of open technical standards that have accelerated adoption of the Internet over the past decade. Without this commitment to standards-based technology, PBX vendors' VoIP solutions won't be a very good bet for companies seeking broad interoperability and flexible migration paths.

8.2 Router-based gateways

Manufacturers of routers and other data networking hardware are also attacking the VoIP market, albeit from the other direction. Like their PBX counterparts, these suppliers have healthy market-share and mind-share among an entrenched constituency – in this case, data communications managers and networking equipment resellers. Their expertise in IP technology should also stand them in good stead, especially when it comes to solving voice quality problems using the IP quality-of-service (QoS) techniques they have been developing for some time.

Unfortunately, router vendors' vulnerabilities mirror those of PBX vendors. Their unfamiliarity with voice technology and call management continues to hamper their ability to deliver corporate-class telephony solutions. And continuing failure to raise to the reliability standards that have been perfected among telephony vendors over the past several decades essentially disqualifies them from serious consideration when it comes to corporate voice infrastructure.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

Finally, it must be noted that the standards-based approach that has characterized recent advances in data networking is beginning to show signs of unraveling. In their pursuit of competitive advantages, many networking vendors are introducing an increasing – though subtle – element of proprietary flow control mechanisms. More and more, they are steering their customers to so-called "end-to-end" solutions – which is really a code-phrase for requiring a single manufacturer’s equipment across the edge, access and core strata of the network. This, again, represents the type of lock-in that most technology managers would prefer to avoid at this early stage of their VoIP plans.

8.3 PC-based gateways

Several vendors are bringing stand-alone gateways to market. These products offer a router- and PBX-independent solution, since they are not tied to a particular manufacturer’s platform. These smaller, more nimble vendors exhibit a greater ability to rapidly adopt – and even help define – emerging standards.

However, stand-alone gateways are also typically based on a PC platform, which calls into question their inherent reliability. Also, these vendors do not have access to the type of manufacturing scale that lends itself to cost-efficiency. It is doubtful that expensive, unstable products will find broad acceptance among buyers and distributors of corporate voice equipment.

8.4 Intelligent Multi-path Switching Gateways

A fourth alternative to the above categories has recently appeared on the VoIP scene: the multi-path switch. These devices are specifically designed to address the issues unanswered by the product categories described above – including voice quality, network reliability, and vendor independence. It is this type of solution that the following section focuses on in further depth.

9 Security

The convergence of voice and data networks complicates the security issues [15]. Until now most attacks have targeted data networks, but, as voice applications become even more strategic on IP network, they too can be exposed (94 registered attacks in November 2005) to many of the same vulnerabilities that plague data networks, including denial or service (DoS), application layer attacks. Critical flaws in one vendor’s IP telephony software could allow hackers to gain control and shutdown voice systems, redirect phone calls, eavesdrop, or gain access to other computers running the vendor’s telephony. All IP telephony platforms in the market do not share the architecture, hence vulnerability in one are likely to be absent in another. Most communication vendors provide solid security solutions. It is very important to recognize that security in a converged world does not have a simple one-step, one-layer, or one-vendor solution.

The first step is to know what can be done. Following are the key principles for defending converged networks, ensuring that voice applications remain secure and protecting an enterprise’s global communications.

9.1 Protect communications flow at every level of a Multi-vendor Network

It is very important for an organization to identify the needs to be able to defend itself from attack at every vulnerable point and application (e.g., denial of service). Providing protection only at the network

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

infrastructure layer (e.g., at the router) can pose major problem, if an intruder gets into the network and most attacks happen within the network. Ignoring the DoS protection within the server at gateways and end-points can make a business less secure.

The best strategy is to provide layers of protection all the ways from the network infrastructure through the application level to the user device. Organizations can make it harder for attackers by increasing the number and types of hurdles they have to pass through up and down the communication stack.

9.2 Use Open rather than Proprietary Solutions

The major benefit of the open standards is that vendors and users alike are able to build on what is already been accomplished to solve security problems. Therefore, the level of protection is constantly improving.

In a proprietary implementation, businesses rely on a vendor's claims of the security being provided, which could put a company at risk if those claims have not been tested and certified. Whereas the open standards let customers choose the best, most cost-effective security solutions that make the most sense for their particular business.

9.3 Trust Vendors who Approach to Security and Collaborate with the Industry

Security conscious vendors take a multifaceted approach to delivering secure products and solutions. Media encryption is one example. It is just not offered on high-end elements, those requiring third-party adjuncts. Some vendors also offer key services that can enhance the security of converged networks. A serious vendor can help in the initial architectural planning of a secure converged network. It is very important for modern leading vendors to work with groups like the VoIP Security Alliance of the VoIP and security communities, focused on increasing vendor and customer awareness of threats to IP communications. As an industry, where every business network and the applications on it are completely not safe from malicious attacks, network threats can be real, but steps can be taken to reinforce and protect business communications against attacks. Open standards-based, multi-vendor solutions and services, combined with industry best practices, are the path to greater integrity in an increasingly hostile communications environment.

10 Conclusion

In a VoIP network, voice quality is only as good as the quality of the weakest network link. Packet loss, delay and delay variation all contribute to degraded voice quality. Additionally, because network congestion (or more accurately, instantaneous buffer congestion) can occur at any time in any portion of the network, network quality is an end-to-end design issue. The QoS tools discussed in this project are a set of mechanisms to increase voice quality on data networks by decreasing dropped voice packets during times off network congestion and minimizing both the fixed and variable delays encountered in a given voice connection.

11 Acknowledgements

I would like to take this opportunity and thank the Department of Mathematics and Computer Science at the Rivier College for giving me the opportunity to write a paper on this interesting topic. Finally, I

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

would like to give special thanks to Dr. Vladimir V. Riabov, Ph.D., associate professor of Computer Science, for all the support and help.

References

[1] Voice over IP : Protocols and Standards. Retrieved October 17, 2005, from http://www.voip-voice-over-ip.com/internet-phone/protocols.htm

[2] Understanding Voice Over Internet Protocol. Packetizer, 2005. Retrieved October 19, 2005 from http://www.packetizer.com/voip/papers/understanding_voip/voip_protocols.html

[3] SGCP Simple Gateway Control Protocol. Telcardia Technologies, 2004. Retrieved October 20, 2005 from http://www.argreenhouse.com/SGCP/sgcp-slides.pdf

[4] David Gurle and Olivier Hersent. Media Gateway to Media Controller Protocols, 2003. Retrieved October 17, 2005 from http://www.awprofessional.com/articles/article.asp?p=99707&seqNum=3

[5] H. Schulzrinne and J. Rosenberg. A Comparison of SIP and H.323 for Internet Telephony. Retrieved October 17, 2005 from http://www.cs.columbia.edu/~hgs/papers/Schu9807_Comparison.pdf

[6] IT Guru Academic Edition. OPNET Technologies, 2005. Retrieved October 20, 2005 from http://www.opnet.com/services/university/itguru_academic_edition.html

[7] The world's Leading Network Modeling and Simulation Environment. OPNET Technologies, 2004. Retrieved October 20, 2005 from http://www.opnet.com/products/modeler/home.html

[8] William Stallings. Data and Computer Communications, 7th Edition. Pearson Education, 2005.

[9] Larry L. Pearson and Bruce S. Davie. Computer Networks: A System Approach, 3rd Edition. Morgan Kaufmann, 2005.

[10] Jonathan Davidson. A Systematic Approach to Understanding the Basics of VOIP, Cisco Press, 2005.

[11] American Metal Bulletin, 2006. Retrieved April 4, 2006 from http://www.metalbulletin.plc.uk/amm.asp

[12] VoIP Services Guide. Retrieved April 6, 2006 from http://www.voip-service-guide.net/voip-advantages.html

[13] Voice-over-IP Implementation Options. Retrieved April 5, 2006 from http://www.techland.co.uk/index/quintum_risk_reward

[14] Randy Rosenbaum. Internet Telephony. Planning for VoIP. Vol. 9, January 2006.

[15] Joseph Curcio. Internet Telephone Securing Voice in an IP World. Vol. 8, November 2005.

---

* **AJAY KUMAR** was born in Bangalore, India. He received his B.S. in Mathematics, Physics and Chemistry from Bangalore University in India in 1991. After emigration to the United States in 1996, he worked as a consultant and software developer for Unisys Corporation. Ajay is currently a computer programmer/analyst at TradePoint Systems in Nashua. He passed the Oracle Certified Associate exams. Ajay is pursuing a M.S. in Computer Science at Rivier College.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).