QUALITATIVE FACTORS THAT IMPACT REAL IMPLEMENTING VOIP IN PRIVATE NETWORKS

Peter CHOCHOL
Section of IT Development, Division of Information Technologies
Slovak Gas Industry, Mlynske nivy 44/a, 825 11 Bratislava, Slovak Republic

ABSTRACT

Integrating enterprise voice services on a data network can offer significant capital and operational cost reductions, and can enable new competitive services. However, if these business values are to be realized, customers must be won and retained by meeting their expectations for service quality. In networking, quality can mean many things. In VoIP, quality simply means being able to listen and speak in a clear and continuous voice, without unwanted noise. Quality depends mainly on the following factors: data loss, consistent delay characteristics (called jitter) and latency, leading to echo. QoS (Quality of Service) is more in demand on corporate LANs, private networks and intranets (private networks interconnecting parts of organizations) than on the Internet and ISP networks. QoS, reliability and security are an important tools for VoIP success. Call quality testing has traditionally been subjective: picking up a telephone and listening to the quality of the voice. The leading subjective measurement of voice quality is the MOS (mean opinion score) as described in the ITU (International Telecommunications Union) recommendation P.800. Considerable progress has been made in establishing objective measurements of call quality on example the E-model (ITU G.107).

Keywords: *VoIP, voice, quality, reliability, security, E-model, QoS measurement*

1. AN INTRODUCTION TO VOIP

Voice over internet protocol (VoIP) is a communications technology that uses the internet to transfer voice signals in the form of bits and bytes. It delivers these bits and bytes to a specified internet address rather than a telephone number. It's easier to think of it as being like sending e-mail from one computer to another, but in real time and using voice instead of text. The technology that most likely runs your existing switchboard and phones is a traditional public switched telephone network (PSTN) service. VoIP's advantage over this is its ability to combine several services, such as voice mail, video, e-mail and conferencing. This instantly increases your ability to collaborate and can result in higher productivity. But how can this benefit your company? Well, for starters, it's likely to lead to lower phone bills. And it could reduce the need to travel, too. If you have branch offices, they can be connected either through a dedicated lease line or virtual private network (VPN). Since all calls routed over the internet, irrespective of the network, are free, this leads to significant savings over existing voice services for inter-company communications and makes use of any under-utilised network capacity that you're paying for.

2. HOW VOIP CAN HELP YOUR BUSINESS

The days of businesses having to spend large amounts on communications due to a lack of affordable, flexible options are over. Voice over Internet Protocol (VoIP) and IP telephony allows the creation of appropriately scaled services to meet the requirements of businesses everywhere, especially multi-site ones. Advantages of migrating to VoIP include:

- Lower costs
- Improved control over technology
- Simpler system management
- Bundled services
- Improved network efficiency
- Potential for future application enhancement and development.

VoIP solutions offer businesses the chance to select a scaled-down system that does not rely on large volumes to provide better pricing, unlike wire-line public switched telephone networks (PSTNs). A company's network will be utilised to its full capacity. This offers improved efficiency in addition to standard features such as teleconferencing, integrated voice mail, e-mail, fax and messaging options, encryption and integrated information services. It also bypasses long-distance phone charges. And once a VoIP platform is in place, it's incredibly easy to add further applications or upgrade system settings.

3. QUALITY OF SERVICE

QoS (Quality of Service) means different things to different people. For most business customers, the term signifies getting the best possible VoIP service quality at the lowest possible cost. The quality of service (QoS) is defined in the ITU-T recommendation [1] to be „the collective effect of service performance which determines the degree of satisfaction of a user of the service". Particularly, the quality of VoIP service comprises overall voice quality, user comfort, additional services and so forth. A typical user is not concerned with how a particular service is implemented. However, the user is interested in comparing the same service offered by different providers in terms of universal, user-oriented performance parameters [2].

3.1. Key parameters impacting the user

- **Delay** - Delay manifests itself in a number of ways, including the time taken to establish a particular service from the initial user request and the time to receive specific information once the service is established. Delay has a very direct impact on user

satisfaction depending on the application, and includes delays in the terminal, network, and any servers. Note that from a user point of view, delay also takes into account the effect of other network parameters such as throughput.

- **Delay variation** - Delay variation is generally included as a performance parameter since it is very important at the transport layer in packetised data systems due to the inherent variability in arrival times of individual packets. However, services that are highly intolerant of delay variation will usually take steps to remove (or at least significantly reduce) the delay variation by means of buffering, effectively eliminating delay variation as perceived at the user level (although at the expense of adding additional fixed delay).
- **Information loss** - Information loss has a very direct effect on the quality of the information finally presented to the user, whether it be voice, image, video or data. In this context, information loss is not limited to the effects of bit errors or packet loss during transmission, but also includes the effects of any degradation introduced by media coding for more efficient transmission (e.g. the use of low bit-rate speech codecs for voice).

Table 1 Indication of suitable performance target for VoIP applications

Medium	Audio	
Application	Conversational voice	
Degree of symmetry	Two-way	
Typical data rates	4-64 kbit/s	
Key performance parameters and target values	One-way delay	< 150 ms preferred < 400 ms limit
	Delay variation	< 1 ms
	Information loss	< 3% packet loss ratio

4. DEFINITION OF CATEGORIES OF SPEECH TRANSMISSION QUALITY

The mean of opinion (MOS) scores, i.e., of the values on a predefined scale that subjects assign to their opinion of the performance of the telephone transmission system used either for conversation or for listening to spoken material. The abbreviation MOS (Mean Opinion Score) is defined in ITU-T Rec. P.10/G.100 [4]. A MOS can range from 5 down to 1.

While the parameters mentioned above describe the individual factors affecting speech transmission quality, it is the combined effect of all parameters together which leads to the overall level of speech transmission quality as perceived by the user. For transmission planning purposes, the E-model ITU-T G.107 [5] is a useful tool for assessing the combined effect of all parameters and hence differentiating between categories of speech transmission quality.

The primary output of the E-model is the Transmission Rating Factor, R. Table 2 gives the definitions of the categories of speech transmission quality in terms of ranges of Transmission Rating Factor R provided by Recommendation G.107. Also provided are descriptions of "User satisfaction" for each category.

Table 2 ITU-T G.107 – Provisional guide for the relation between R-value and user satisfaction

***R*-value (lower limit)**	**MOS_{CQE} (lower limit)**	**User satisfaction**
90	4.34	Very satisfied
80	4.03	Satisfied
70	3.60	Some users dissatisfied
60	3.10	Many users dissatisfied
50	2.58	Nearly all users dissatisfied

It is very important to fully understand the principle recommended in this Recommendation. The R-value is a measure of a quality perception to be expected by the average user when communicating via the connection under consideration: quality is a subjective judgement such that assignments cannot be made to an exact boundary between different ranges of the whole quality scale.

5. END – TO – END QOS MEASUREMENT

The complexity of modern networks requires that for transmission planning the many transmission parameters are not only considered individually but also that their combination effects are taken into account. This can be done by "expert, informed guessing," but a more systematic approach is desirable, such as by using a computational model. The output from the model described here is a scalar quality rating value, R, which varies directly with the overall conversational quality.

The E-model is based on the equipment impairment factor method, following previous transmission rating models. It was developed by an ETSI ad hoc group called "Voice Transmission Quality from Mouth to Ear".

The reference connection, as shown in Figure 1, is split into a send side and in a receive side. The model estimates the conversational quality from mouth to ear as perceived by the user at the receive side, both as listener and talker.

Speech transmission quality is an important aspect of quality-of-service for many user applications of many telecommunications services. Recommendation ITU-T P.11 [3] identifies the key speech quality parameters and gives the subjective effects of variations in the parameters. Examples of speech quality parameters are speech level, attenuation distortion, transmission delay, echo path loss and delay, circuit noise, background noise, nonlinear distortion (such as the effects of low bit-rate speech codecs, packet loss, etc) and terminal characteristics.

The transmission parameters used as an input to the computation model are shown in Figure 1. Values for room noise and for the D-factors are handled separately in the algorithm for send side and receive side and may be of different amounts. The parameters SLR, RLR and circuit noise Nc are referred to a defined 0 dBr point. All other input parameters are either considered as values for the

overall connection such as OLR (in any case the sum of SLR and RLR), number of qdu, equipment impairment factors Ie and advantage factor A, or referred only to the receive side, such as STMR, LSTR, WEPL (for calculation of Listener Echo) and TELR.

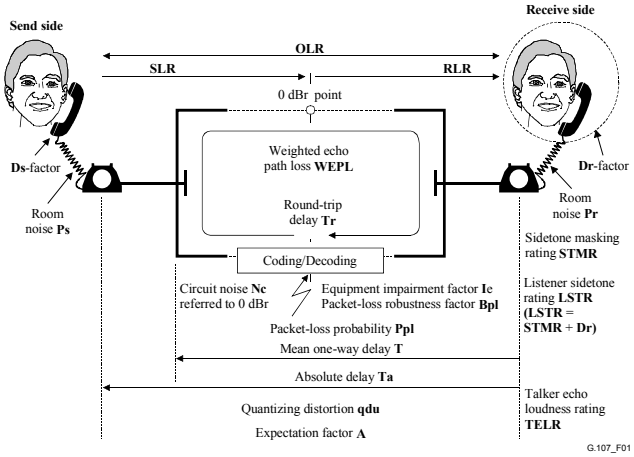

Fig. 1 ITU-T G.107 – Reference connection of the E-model

There are three different parameters associated with transmission time. The absolute delay Ta represents the total one-way delay between send side and receive side and is used to estimate the impairment due to too-long delay. The parameter mean one-way delay T represents the delay between the receive side (in talking state) and the point in a connection where a signal coupling occurs as a source of echo. The round-trip delay Tr only represents the delay in a 4-wire loop, where the "double reflected" signal will cause impairments due to Listener Echo.

5.1. Calculation of the transmission rating factor, R

The result of any calculation with the E-model in a first step is a transmission rating factor R, which combines all transmission parameters relevant for the considered connection. This rating factor R is composed of:

$$R = Ro - Is - Id - Ie\text{-}eff + A \quad (1)$$

Ro represents in principle the basic signal-to-noise ratio, including noise sources such as circuit noise and room noise. The factor Is is a combination of all impairments which occur more or less simultaneously with the voice signal. Factor Id represents the impairments caused by delay and the effective equipment impairment factor Ie-eff represents impairments caused by low bit-rate codecs. It also includes impairment due to packet-losses of random distribution. The advantage factor A allows for compensation of impairment factors when there are other advantages of access to the user. The term Ro and the Is and Id values are subdivided into further specific impairment values. The following clauses give the formulae used in the E-model.

6. RELIABILITY

Corporate voice-over-Internet Protocol networks need much improvement if they are to approach the reliability of traditional phone systems. They must incorporate a degree of redundancy, but that's not the whole story.

Redundancy is a very common way to increase the reliability of an organization's network infrastructure. In the traditional voice world, we often hear about the "five 9s reliability," meaning that the telephone network is available 99.999 percent of the time. This translates to just over five minutes of downtime throughout an entire year. Because users have extremely high expectations for the performance of their telephone networks, there is a great deal of concern in relying on the data network to carry voice communications. This is especially the case in environments where voice is a mission-critical application (like revenue-based contact centres).

The same concern holds true for many other applications. Building security and surveillance systems, devices that monitor medical equipment and other mission-critical data applications carry similar requirements for high-availability networks. Converged network design should consider all such applications when assessing reliability needs [6].

Unfortunately, "five 9s reliability" is difficult to achieve in data networks. Complete redundancy would certainly increase the reliability of a network, but is usually cost-prohibitive; the degree of reliability "appropriate" to a company, therefore, usually becomes a financial decision. But while complete redundancy may not be feasible, certain applications simply require high-availability networks. It is therefore important to consider a variety of methods, in addition to redundant systems, to ensure high availability of the telephone system.

Most IP telephony environments are moving toward centralization of the call processing intelligence in a main location, usually the company's corporate office. Remote sites are commonly handled as sets of extensions managed by the main system, especially when those remote sites are relatively small. Redundancy takes several appropriate forms here.

- A redundant server, co-resident or hosted in a separate location.
- Backup servers (or "survivable gateways") can be located in regional offices.
- Redundant networking equipment is important too.

Beyond redundancy, though, there are other important considerations.

- In the case of a local network outage in which the LAN becomes unavailable, each site must maintain a limited number of digital phones connected to the local public switched telephone network (PSTN).
- A greater vulnerability, often beyond the company's control, is WAN access. The lines joining the customer's premises to the network service provider (NSP) can be severed without warning, so mission-critical operations require the establishment of alternate access routes into the NSP.
- At each location, some amount of backup power is important. Extending emergency power to a limited number of phones at each site is also

important, but does not necessarily have to be extended to every telephone.

Identify a limited number of phones at each location that would require the backup, perhaps based on the demands of certain roles (like senior management and workgroup coordinators) and logical locations (like reception desks, evacuation rooms and security department) in each facility.

7. SECURITY

"VoIP security," a term that is widely used by the trade press, vendors and even standards bodies, is misleading and generates much confusion. For example, it makes good sense to say "quality of service (QoS) is an essential component for Internet Protocol (IP) telephony security," but it makes no sense to say "QoS is an essential component for VoIP security." What if your VoIP traffic travels over the Internet, where QoS is non-existent? Similarly, the risks from peer-to-peer, Internet-based solutions like Skype are very different to the risks from intranet-based IP-PBX solutions — yet "VoIP security" is often used to characterize both scenarios. Because of the versatility of VoIP, we need a taxonomy to more accurately reflect threat scenarios. Common Threats:

- **Network-based denial of service (DoS)**. These attacks are especially problematic in a VoIP environment, because the network congestion that they introduce can make conversations unintelligible. In LANs and WANs, the threat can be mitigated by creating a separate virtual LAN for voice traffic and protecting it (via bandwidth reservation, for example) from malicious traffic that could overrun it. VoIP over the Internet remains a riskier proposition, due to the lack of QoS in Internet backbone networks.
- **Eavesdropping**. This threat has received a lot of attention due to the understandable fear that malicious people can listen in on our conversations. Packet capturing, or "eavesdropping," is technically an issue within LANs, WANs and the Internet, although this risk is generally overhyped. The same eavesdropping techniques apply whether the intent is to capture data packets or voice ones. Therefore, the same precautions that organizations implement to protect data traffic against eavesdropping also apply to voice traffic.
- **Signaling protocols**. These are used to establish communication sessions between two or more endpoints. Among the standards-based protocols, Session Initiation Protocol (SIP) is becoming the most widely deployed solution. But it is a relatively new protocol, and is just beginning to receive the detailed security analysis and scrutiny that will enhance its resistance to attack. By manipulating signaling protocols, hackers can steal services, disrupt sessions or launch other malicious attacks.

Organizations can protect themselves from these and other threats by implementing the following best practices recommendations:

7.1. Protect the IP-PBX Server

- **Firewalls**. The behavior of voice over IP (VoIP) signaling protocols dictate the need for firewalls that are "IP telephony-aware." For example, SIP and H.323 use ports that are allocated dynamically during call set up. The firewall must scan VoIP messages and open ports dynamically only for calls approved by the call control server. At call disconnection, the firewall must close the session as well as any open ports. Since most IP-PBXs use proprietary protocols (most are based on versions of H.323) to speak with their family of IP phones, organizations must use firewalls that provide explicit support for that proprietary protocol.
- **Network-based intrusion prevention**. To complement firewalls, use a network-based intrusion prevention system (IPS) to protect the IP-PBX against DoS and other attacks. The IPS solution should be able to block signaling protocol attacks (for example, recognize anomalous behavior in the signaling protocol).
- **Host-based Intrusion Prevention (IPS)**. Protect the underlying operating system of the IP-PBX via host IPS.

7.2. Protect the Network

- **VLANs**. Separate voice traffic from data traffic using virtual LANs (VLANs). This is only possible when using IP telephony handsets. With Windows-based softphones, voice and data traffic is tagged with the same VLAN identifier, due to Window's inability to support 802.1Q VLAN tagging. Thus, traffic originating from softphones is more susceptible to DoS attacks than traffic originating from IP telephony handsets.
- **Quality of service**. Prioritize traffic in the voice VLAN to be sure that it cannot be "overrun" via bandwidth utilization spikes from malicious data traffic. Include the ability to lower the priority of unknown traffic or filter traffic that matches the profile of known attacks.

7.3. Protect the IP Phones

- **IP telephony handsets**. Endpoint security is presently not necessary for IP telephony handsets, nor does independent agent-based software exist for these devices. Most end users do not use their IP phones to surf the Internet or to download executables, so the risk to IP telephony handsets is negligible.
- **Softphones**. Use best practice laptop security configurations and endpoint security solutions. Currently, this is centrally managed personal firewalls and antivirus software.

8. CONCLUSIONS

Voice over IP is quickly becoming readily available across much of the world, however many problems still remain. For the time being transmission networks involve too much latency or drop too many packets, this effects quality of service sometimes severely deteriorating the quality of the call. Also VoIP contains many security risks, sending out packets that any person may intercept. Although VoIP may offer cheaper solutions for many the PSTN offers a high QoS and greater security that makes up for its higher prices. Quality, reliability and security are key factors for success VoIP implementation in private networks. That's why is necessary to understand, analyze, describe and measure this parameters before and after implementation and on this basis to guarantee the success solution.

REFERENCES

[1] ITU-T: Recommendation E.800: Terms and definitions related to quality of service and network performance including dependability, 2008

[2] ITU-T: Recommendation G.1010: End-user multimedia QoS categories, 2001

[3] ITU-T: Recommendation P.11: Telephone transmission quality, 1993

[4] ITU-T: Recommendation P.800.1: Mean Opinion Score (MOS) terminology, 2006

[5] ITU-T: Recommendation G.107: The E-model, a computational model for use in transmission planning, 2008

[6] Snyder J.: How IT Managers Can Make VoIP Networks More Reliable, Gartner, 2005

[7] Halpern J.: IP Telephony Security in Depth, Cisco, 2003

[8] Hardy W.C.: VoIP service quality, ISBN 0-07-141076-7, 2003

[9] Marsan M., Corazza G., Listanti M., Roveri A.: Quality of Service in Multiservice IP Networks, ISBN 3-540-00604-4, 2003

Received Jun 21, 2009, accepted November 11, 2009

BIOGRAPHY

Peter Chochol is Director of IT Development in Slovak Gas Industry. He holds degree in Engineering from the Technical University of Košice and a Master's in Electronics and Multimedia Communications. During his 22 years working in IT departments in Slovak and Czech Gas Industries has been led a lot of IT projects.