

VoIP and Network Management for the Mid-Market

A VoIP Primer

July 2008

- 3 Overview / Background
- 3 VoIP Crosses Networks and Networks Cross Vendors
- 3 Fear is Rational
- 4 A Word on VoIP Security, or "Just Because You're Paranoid, Doesn't Mean You Shouldn't Be Worried"
- 4 QoS for VoIP, or: "Could You Repeat That Please? I Didn't Catch That Last Packet..."
- 5 Premise vs. Hosted PBX
- 6 MOS and VoIP Monitoring on the Network
- 7 Network Optimization for VoIP, or When Lower is Higher
- 7 Network Monitoring, Network Management and VoIP



PacketTrap Networks

118 2nd Street, 6th FL

San Francisco, CA 94105

1-866-My-pt360 (1-866-697-8360)

LEGAL NOTICE AND ACKNOWLEDGEMENTS

Copyright © 2008 PACKETTRAP NETWORKS

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

The product and company names used in this whitepaper are for identification purposes only. Cisco is a registered trademark of Cisco Corporation. PacketTrapPerspective and PacketTrap are registered trademark of PacketTrap Networks, Inc.



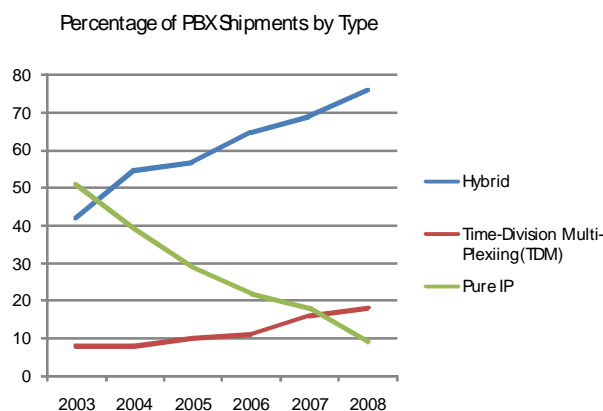
Corporate Headquarters
118 2nd Street, 6TH FL
San Francisco, CA 94105
1-866-My-pt360 (1-866-697-8360)
www.PacketTrap.com

Overview / Background

If you manage a mid-market IT network, your network will likely start streaming data for your company phone system sometime in the next few years; assuming of course, it hasn't started already. Originally driven by savings incentives and the promise of more efficient "unified communications" for business, the transition to VoIP has gone from the volitional to the inevitable. How do we know? Consider these facts:

- The IP PBX Market has continued to grow 52% per year in the last few years
- In 2005 more IP Phone systems were shipped than traditional PBX phones
- In 2008 major vendors will cease to support their own non-IP phone systems

In the last couple of years, the landscape and the analysis have changed. The industry is moving away from circuit-based voice solutions. End of life and end of support notices for time-division multiplexing (TDM) private branch exchanges (PBXs) and spare parts availability are prompting enterprises to re-evaluate their voice solutions. The Radicati Group, a telecommunications market research firm, predicts that 74 percent of all corporate telephony lines will be IP-based by 2009. Reasons companies give for implementing VoIP include ease of integration, cost savings, flexibility, productivity, consolidated network management, and the robust features that VoIP offers to both users and IT operational staff. Enterprises realize that rapid acceptance of VoIP standards and applications are making installations far easier than traditional voice installations. International market research firm Infonetics Research projects that worldwide revenue from IP-capable PBX equipment will reach \$10.2B in 2008, up 300% over the last five years. Because companies see their fully depreciated PBX systems as roadblocks to the cost savings and enhanced applications that IP telephony provide, some vendors are offering hybrid systems and upgrade paths that combine the capability of a traditional PBX and the enhanced feature set of an Internet protocol (IP) PBX. Over the next several years, VoIP adoption will continue to flourish, as installation of hybrid VoIP systems continue to grow faster than either traditional TDM or pure IP systems. However, a concern of some IT departments is that they are simply replacing one vertical telephony system with a newer vertical voice solution based on IP.



VoIP Crosses Networks and Networks Cross Vendors

PacketTrap Networks appreciates the importance of VoIP, and has added VoIP QoS monitoring to the rest of the network monitoring capabilities of its solutions. For many companies investigating VoIP quality issues PacketTrap Perspective may be the first and least expensive step towards getting a handle on VoIP, starting with network discovery to gauge the readiness of your network for VoIP Deployment right on through first-level QoS monitoring. As we shall see, maintenance and management of the whole network, across many network products from many vendors, is key. Thus network management tools provided by your individual point product vendors alone are bound to be inadequate.

No doubt PacketTrap solutions will also be just part of the process. Professional expertise from a qualified consulting firm will probably be necessary, because the issues are complex and your current IT staff is already busy. So, in order even to begin planning for the retention of suitable expertise, all levels of a company need to understand VoIP issues at a basic level. Let's take a look at them.

Fear is Rational

There is a reason why the words "dial tone" are used metaphorically to denote services considered basic to a business, services for which the standard expectation is that they will be there when needed, which is to say always, except in extreme disasters. For business, and even private homes, phone systems have been just that in developed parts of the world for years, and for most businesses phones are a sine qua non. Without them basic functions, productivity and revenue come to a halt.

Anyone who has ever heard the words “the server is down” or “we lost the Internet” will understand the fear that arises in management at the thought of phones being tied to the network and run by the IT Department. For instance, many sales managers have encountered situations where email is down, but they can say to their staff, “you can still make phone calls.” The thought of the phones going down at the same time is frightening.

This fear is rational, but reliability, availability and maximizing uptime to the 99.99% “dial tone” level considered standard for basic business phone service are all realistic goals for mid-market networks. What is required is fail-over redundancy, preferably at multiple sites, built into the plan. The good news is that the ROI for moving to VoIP is usually high enough to absorb the cost of network infrastructure upgrades. The reliability of the whole network—for all functions—may benefit at the same time.

Unfortunately corporate management may not even know the half of all the potential choices and worries when it comes to VoIP implementation. This paper is here to help the IT Department think through concerns in advance so they can be dealt with, but it is also meant to be provided to your company management as a readable introduction to VoIP issues.

A Word on VoIP Security, or “Just Because You’re Paranoid, Doesn’t Mean You Shouldn’t Be Worried”

When Corey Elinburg, a VoIP security architect at Cisco Systems was interviewed (VOIP-NEWS 2/15/07) his most essential points on VoIP Security were that:

- VoIP security is a real concern, but
- VoIP can be secured adequately, and
- VoIP’s advantages are worth the trouble.

It should be remembered that all phone technologies have been vulnerable to penetration and attack of some sort. IP is not exceptional in this regard. The VoIP vulnerability relevant to most of us is a potential denial of service attack rather than an intercepted call, but both are real possibilities on an unprotected system. For those who like to mull over futuristic threat scenarios, there is also a lot of talk about “SPIT” (Spam over Internet Telephony) looming on the horizon, but not many actual reports of it yet.

How can VoIP be secured? The single most often repeated piece of advice on VoIP security is to put all VoIP traffic on distinct and separate V-LANs using standard private network RFC 1918 addressing. V-LANs (Virtual Local Area Networks) use the same pipes that carry the other network data, but treat the data within them as completely separate, thus making them impenetrable, if properly configured. Outside access from any PC with internet connection to the VoIP V-LAN should be prevented at all costs, or if that wall is breached, it should be with a clear understanding of the risks involved. Properly implemented with appropriate protections for the V-LAN, this configuration should stop most outside attacks,

Before considering the lengths to which an organization can go to prevent inside theft of calls, it should be recalled that it has always been possible to break into a physical phone line and intercept a call using inexpensive equipment. It may be true that IP offers a would-be intra-company eavesdropper the ability to do so a little more subtly than alligator clips in the phone room, so if an organization is determined to prevent this, the answer is in encryption in the phones and at the gateway PSTN access point. Most vendors now support encryption of some kind and, with careful management of the tendency to cause latency on the WAN, this solution offers high security and acceptable service levels in many organizations.

Before we can really discuss ways to measure acceptable service, we need to understand what determines quality in the first place.

QoS for VoIP, or: “Could You Repeat That Please? I Didn’t Catch That Last Packet...”

Packet Loss: For many uses of data traveling over the LAN and WAN, a certain degree of packet loss is both expected and manageable and is dealt with in the very common Transmission Control Protocol (TCP) by simply resending lost packets until all are received and compiled into a complete copy of the sent data. Because immediacy of data as measured in milliseconds is not normally an issue for functions like email or database entries, this slight potential for delay is acceptable. We will not notice that portion of a second, or even the whole second, it might take to resend and reprocess those lost packets (and often the subsequent packets as well) using TCP.

For voice and a few other functions (such as online gaming) immediacy is a requirement for successful and useful transmission. We cannot wait for our phone to compile a speaker's last sentence before we listen to it and respond, so lost packets must be dealt with differently. Thus, most VoIP systems employ the User Datagram Protocol (UDP). For these functions it is better to sacrifice some reasonable measure of lost packets in the interests of immediacy, and that is exactly what UDP does.

Obviously, if too many packets are lost, quality will suffer. In fact, the tinny, muffled sound many of us associate with a "bad phone connection" is the direct result of some form of information loss during transmission. If the phone connection is IP, then packet loss is the culprit.

Latency: If packet loss delivers voice with annoying artificial tones, then latency delivers voice after a delay. In fact to measure latency is to measure the delay of packets between nodes. The International Telecommunications Union defines unacceptable packet delay as more than 150ms in one direction. More generally, delay of more than 250ms in both directions becomes unacceptable.

Jitter: The difference between Latency and Jitter is that in the latter case delay for some packets is greater than for others. If one thinks about it for a minute it is pretty clear how that would create echo and other distorted "quavering" sound qualities. Ordinary echo is when a portion of the vibratory information traveling through air takes a longer route (by bouncing against a far away wall, for instance) and returns later than another portion.

Quality of Service (QoS): Substandard quality is often more noticeable to the human mind than superior quality, and QoS for VoIP is no exception: If we have a really, really "bad connection" we will have to wait some annoying interval (caused by Latency) to finally hear that tinny, muffled voice (caused by Packet Loss) and when we do it will have a quavering quality that opens out into a full blown echo (caused by Jitter). The goal of all VoIP monitoring and QoS programs is to measure these factors. The goal of proper vendor selection and network design is to eliminate them, or at least reduce them to imperceptible levels.

- Control over QoS: From the point of view of your organization's control over call quality, there are essentially three main matrices through which data will travel and these will determine overall QoS:
- Your own network (LAN and WAN) and phones;
- The matrix between your network and your call's destination outside the network; (in other words your service provider, the Internet, various Public Switching Phone Networks and your destination's carrier);
- Your destination's phone system, in those cases in which that is other than your own.

Of all three you have the most control over the first, so most of the rest of this paper will be an overview of the issues surrounding network management and optimization for effective VoIP monitoring. Your control over the second essentially boils down to the choice of a reliable service provider, one that offers good QoS statistics and reputation. Your only control over the third is in your choice of whom to call.

Premise vs. Hosted PBX

Like any company Phone system, VoIP requires a PBX, a switching facility to manage and transfer calls inside the company, so there is one more major decision to deal with before a discussion of network optimization for VoIP: Whether to host VoIP PBX software on your own network, or to subscribe to an offsite PBX hosting service. No matter what choice your company makes voice packets will travel over your own network, so proper design and network monitoring for VoIP optimization will still be a priority.

Essentially, Hosted PBX is a SaaS model. (The PacketTrap Whitepaper on SaaS could be helpful at this point in your research.) In light of the phenomenal success of SaaS in the mid-market for CRM and some other services, it might be an important trend to adopt this approach to phone service also. Obviously, the factors involved in this decision are complex and will vary greatly according to the company making the decision. They include:

Upfront Cost vs. Cost per Call Hosted PBX will cost less to set up, but will cost more per call over the long run

Size and the Sophistication of IT Department: For companies who prefer to keep IT Departments small and all focus on core business, hosted PBX might justify a possible greater cost per call over time.

Control vs. Flexibility There is great flexibility with hosted PBX. Rapid expansion at multiple extended locations is virtually instantaneous. But with that flexibility comes the concern that a necessary business function is now in the hands of a vendor who may go bankrupt, be acquired or simply fail to perform. The ability to sue a vendor for failure to meet minimal Service Level Agreement standards is not very helpful to a company that is losing money on inadequate phone coverage.

It is clear that as a company grows in size and sophistication, so does the likelihood of premise based PBX. For the purposes of this paper, it is important to realize that, whatever your decision on the Premise vs. Hosted PBX question, as long as packets containing voice data are traveling over your network, QoS will be determined to a great extent by your own ability to do effective network monitoring and network management on your WAN and LAN, and your organization will benefit from a design that allows for VoIP performance monitoring such as that provided by PacketTrap.

One thing is for certain, when the phones are down or quality drops, the inevitable complaints will land in the IT Department first. Even if the problem lies with a vendor, if IT Administration has no visibility into what is happening on the immediate network, the ability to troubleshoot will suffer as well. The best defense is VoIP monitoring and high QoS, to eliminate complaints before they arise.

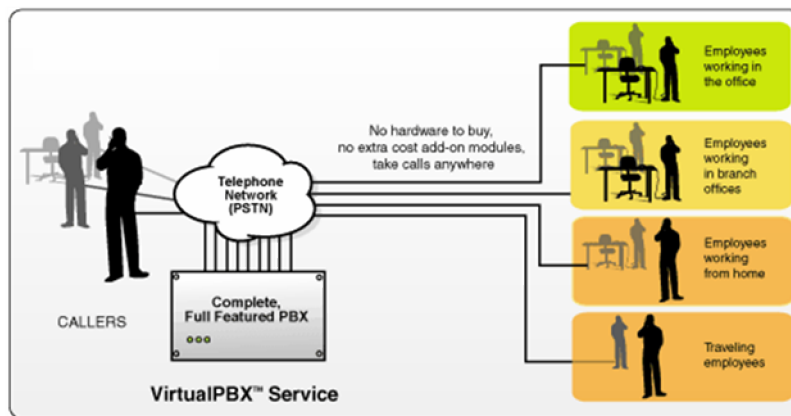


Figure 1: Example Hosted PBX

MOS and VoIP Monitoring on the Network

We learned in Section 3 that VoIP uses UDP because it does not spend precious time on the replacement of lost packets. At the same time if a certain number of packets are lost, quality suffers. It follows that there is a maximum level of acceptable packet loss during transmission. Go beyond that and service drops to unacceptable levels.

In order to measure QoS then we need to be able to measure rates of packet loss, and packet delay (which essentially covers both latency and jitter). The most common way to do this is by leveraging capabilities that are present in most of the routers used in the mid-market. Both Cisco and Juniper, for instance, build certain packet measuring capabilities into their routers. Cisco's Internetworks Operating System (IOS) is the best known of these.

The ability to read the information given off by a router with QoS measurement capabilities is the first line of VoIP monitoring defense and is the capability PacketTrap provides in Perspective. To understand how it works, we need to look at codecs, simulated codecs and IP SLAs.

"Codec" is usually said to stand for coder/decoder and in its modern usage refers to a program which encodes a stream or signal digitally for compression, possible encryption and transmission. The term has broad application, but as applied to telephony it usually refers to a particular codec, most often for the standard G.711 or G.729. G.711 has, among other ordinary functions, a built-in packet loss concealment algorithm which helps to minimize the effects of lost packets on voice quality.

A "Simulated Codec" is, then, a pre-set relay of encoded digital information with precise and known parameters. By measuring the changes in the information from transmission at one router to reception at another, together with the time lapsed in transmission, the three primary modes of poor QoS, packet loss, latency and jitter, can be measured and relayed elsewhere for display and diagnosis of network efficiency issues.

MOS or "Mean Opinion Score" is the best known overall measurement of QoS for VoIP. Taking the measurements of packet loss and delay as applied to a particular codec an algorithm can be applied to calculate a number between one and five inclusive; with one representing the lowest level of satisfaction and five the highest. (Does that mean that our subjective experience will always correlate with MOS scores? Unfortunately, it is not as simple as that and there is a great deal of art in setting up VoIP in such a way that subjective quality can be aligned with MOS and managed effectively.)

Internet Protocol Service Level Agreements (IP SLAs) are agreed upon levels of service for data transmission, in this case of VoIP packets. They can act as part of the contractual agreement between a vendor and user, and also provide a reference point by which issues can be discussed.

The purpose of measuring simulated codecs against agreed upon MOSs and SLAs and aligning those measurements with subjective quality assessment, is to ensure that network optimization for VoIP accomplishes its goals.

Network Optimization for VoIP, or When Lower is Higher

Obviously there are many fine points to network optimization, such as equipment choice and degree of redundancy vs. cost, which lie outside the scope of this paper. We do want to draw attention to a common piece of advice that can get a VoIP installation in trouble.

It sounds logical. If phones are the most important business service on the networks and if they are also the most sensitive to packet loss, latency and jitter, then VoIP packets should be given priority over other network traffic. Right?

Not so fast. Some of the packets moving across the network are part of the processes by which your network is managed and optimized, such as routing updates. If you favor the VoIP packets over these basic network optimization functions it will actually hurt voice quality. Thus to make VoIP your first priority, you must make it your second priority, after those basic system optimization functions.

Network Monitoring, Network Management and VoIP

VoIP can only work as well as your network as a whole. From the time when you first inventory your network with VoIP installation in mind, to the day when VoIP is running on your network and you need constant polling MOS scores and SLA performance statistics carefully calibrated against other of multi-vendor network measurements (and subjective experience) for network optimization, your success will depend on network discovery, network monitoring and network management.

Network management systems can range from freeware to elaborate systems costing hundreds of thousands of dollars. Probably, like most serious companies, you were thinking of something in between. The first step in VoIP is always to inventory your network and when you do, if you are like most companies, you will find that your network is heterogeneous to the extent that for best practices in network management, you cannot rely solely on the management systems which come with one vendor's equipment. For one thing, these systems are often thrown in as an afterthought to provide a little leverage in what is primarily a hardware sales process. For another, support for competitive products is usually not given high priority in these systems for obvious reasons.

As you plan for the upgrade and "VoIP-ification" of your network, one very inexpensive way to get a handle on it is to download the PacketTrap Perspective solution and configure the network discovery, network monitoring and network analysis tools there, some of which are free. Others, part of the Professional version, include the ability to monitor routers, hubs and switches for packet loss, latency jitter and other MOS and QoS statistics from appropriate and properly configured elements on your network.

Finally, PacketTrap works with many reputable IT consultants and resellers, whose expertise is in VoIP and Network Management in the Mid-market. We are happy to refer you to a consultation.

PacketTrap Networks

Corporate Headquarters
118 2nd Street, 6th FL
San Francisco, CA 94105
1-866-My-pt360 (1-866-697-8360)
www.PacketTrap.com

Learn more about network management solutions at www.PacketTrap.com.