www.itmag.com
INTERNET TELEPHONY®
VOLUME 10/NUMBER 7 JULY 2007 The IP Communications Authority Since 1998™

SIP Trunking: What Challenges Lie Ahead?

The allure of leveraging SIP trunking and eliminating the separate PSTN lines in enterprise deployments is very compelling. Initial deployments with SIP trunks to legacy PBX applications have shown early promise, delivering cost savings to enterprises while delivering equivalent features and quality to their legacy PSTN predecessors. However, a number of challenges await those that attempt to integrate end-to-end SIP solutions utilizing SIP Trunking carriers to connect enterprise SIP applications. This article will explore the issues that have slowed widespread adoption of SIP trunking with SIP applications.

The Promise of End to End SIP

A wide range of enterprises have jumped in and adopted Voice over IP (VoIP) and SIP within their enterprise as a way to consolidate facilities to an all-IP infrastructure, leveraging enhanced services and supporting a geographically dispersed workforce. Others have retained their existing Time Division Multiplexed (TDM) equipment, but leveraged SIP as a replacement for their legacy Public Switched Telephone Network (PSTN) trunking.

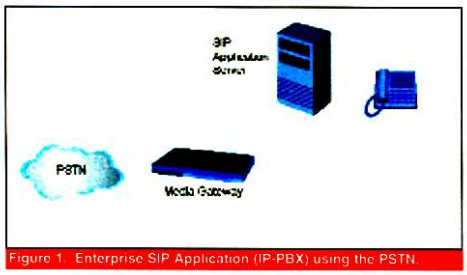

Figure 1. Enterprise SIP Application (IP-PBX) using the PSTN.

The feedback from those that have adopted VoIP ranges from very positive "we're glad we did it" to the tenuous "it sure was a lot of work and I hope this pays off". None-the-less, VoIP is here to stay as an increasingly larger percentage of IP-PBX, contact center, IVR, unified messaging and other new communications deployments are based purely on VoIP within the enterprise.

The vast majority of today's enterprise deployments are "SIP Islands", depend on traditional PSTN circuits to connect trunk circuits from their enterprise to the local carrier. This arrangement has allowed the enterprise to leverage SIP and migrate to new applications, while maintaining the well-established relationship with their "tried and true" local telephone carrier. (See Figure 1.)

Over the last few years a new collection of carriers has entered the market offering to replace those TDM circuits with SIP trunks - eliminating the separate TDM circuits and combine both the data and voice traffic for the enterprise into one consolidated broadband facility and significantly reduce costs. (See Figure 2.)

These end-to-end SIP applications are the focus of this discussion.

The Challenges

After a number of conversations with a wide range of end customers, Value Added Resellers (VARs) and integrators, a number of interesting and common issues seem to affect their ability to sell, install and service end-to-end SIP applications.

Interoperability

The first and most obvious issue is whether the enterprise SIP application is interoperable with the candidate SIP trunking carriers. One of the serious down-sides to SIP is there are many options that affect compatibility between systems.

One immediate example is the method for transporting DTMF: In-band (G.711), RFC-3261 or SIP INFO? Without both sides agreeing on a common transport method, the application and carrier will not be able to correctly relay DTMF key presses from the user to other applications like voicemail or IVR systems.

Beyond the DTMF compatibility issue, other more subtle but equally complex configuration settings include the following:

- Supported voice coders
- Fax Transport (G.711 or T.38?)
- Call Transfers
- Registration, frequency of re-registration and timeouts
- ISDN features including User to User Information transport
- Message waiting
- Etc.

Assuming all of the above configuration settings are figured out and the solution finally works correctly - the

result only means this one application will work with this one carrier. The testing needs to be repeated for each and every application and carrier!

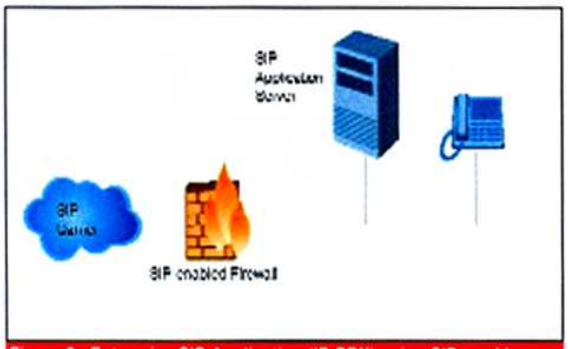

Figure 2. Enterprise SIP Application (IP-PBX) using SIP trunking.

"Carrier Lock"

Since no application vendor can possibly test with all possible SIP Trunking carriers, we are starting to see technical limitations or marketing agreements that would limit the choice of SIP carriers that could be used with each application.

Remember back to the Ma Bell thinking of the 70's that limited you to their company-provided black phones? History may be repeating itself.

Retesting

Okay, let's pretend for a minute that in some future date, every application somehow gets tested with every SIP carrier. Now imagine that one of the SIP carriers adds a feature or capability that would affect the interoperability to applications - now all those applications would have to be retested and re-certified with the carrier.

Now multiply this times the number of SIP carriers - does your head hurt yet?

Security

After interoperability, security is the second most discussed issue relating to SIP trunking. One of the side effects of using TDM circuits for trunking is that they are relatively secure and only carry voice traffic. It's virtually impossible to attack a data network through a TDM voice circuit.

Once you bring a data circuit into the picture, everything changes. Now you need to worry about a whole host of possible attacks, including:

- Denial of Service
- Trojan horses
- Spoofing and Man-in-the-middle
- Unauthorized recording and eavesdropping
- Call Detail Capturing (tracking who you call and for how long)
- Theft of services (unauthorized use of your network)
- Unsolicited incoming calling (SPIT)
- And more.

No sane IT manager would open their enterprise data network up to an IP Service Provider without some form of network protection. Many IT managers hope to use their existing firewalls to protect their SIP-based voice traffic, but standard firewalls don't understand the relationship between SIP and the RTP streams needed to pass voice conversations. Even "SIP Aware" firewalls have a limited ability to verify the origin of the incoming requests and open the appropriate pin-holes in the firewall for the RTP streams that carry the voice. Very few of these devices fully validate the SIP

call control and inspect every RTP packet to ensure the payload is valid and that the data rate demands of each call match the validated active calls.

Trust

While a few of the major carriers have jumped into the SIP trunking market, most of the carriers offering services to enterprises are smaller pure-IP carriers that are using the offering to compete with the majors. These pure-IP carriers are typically much younger organizations that in many cases don't own the broadband facilities or the staff used to install the services to the end customer. These smaller carriers contract with local broadband service providers who contract with installation technicians to activate the service. In some extreme cases, the services may be passed over the customer's existing broadband IP facilities with little or no coordination with the broadband service provider - creating a "parasitic" relationship.

These varied and complex business relationships many times result in serious support issues between the enterprise and the SIP carrier. If there is poor voice quality or dropped calls, who do I call?

It makes sense to leverage the expertise of the data security experts and stay focused on your business.

The result of these issues has yielded a newly coined Telecom cliché:

"Nobody ever got fired for using TDM trunking"

Figure 3: Enterprise SIP Application (IP-PBX) using Enterprise Session Border Controller.

However, the writing is on the wall and it is clear that the customer demand will eventually push the SIP carriers and equipment manufactures to solve these issues in the near future.

Enterprise Security/Interoperability Solution

It's clear that the key to solving many of the above issues is an intermediary that can play both the role of security agent and interoperability expert.

This is the role of the enterprise Session Border Controller (eSBC). Unlike the larger carrier-to-carrier Session Border Controllers (SBC) on the market, the eSBC sits at the enterprise premise and fits between the enterprise and the SIP carrier, mitigating many of the protocol and media incompatibilities while providing carefully managed security. (See Figure 3.)

Required security capabilities of the enterprise Session Border Controller (eSBC):

- Authentication
- Public/Private Network Address Normalization
- NAT Traversal
- Topology Hiding
- Session Admission Control
- Session-based Firewalling
- Encryption/Decryption
- Service Level Agreement (SLA) assurance
- Rouge RTP Detection and Deep Packet Inspection

In addition to the security issues, the eSBC will also provide a number of important features in solving or isolating the interoperability incompatibilities:

- Protocol conversion (H.323 to SIP, or SIP to SIP)
- Protocol variant interoperability
- Media transcoding (voice, video, fax and DTMF conversion)

Ownership

Today many of the SIP Trunking carriers are providing security devices for the enterprise premise along with their service. However, these devices are provided at their convenience, not based on the level of security required by the enterprise. Ask yourself: Would you let your Internet Service Provider (ISP) install and manage your firewall? Doubtful. In the end, it seems that the eSBC will be owned and managed by the enterprise - just as today the firewall for data traffic is typically owned by the enterprise.

Role of the Supplier

Enterprises and application developers have to focus on their applications - not becoming security experts and trying to keep up with the latest intrusion techniques. That's why virtually all enterprises have already partnered with a vendor to support their data security software or devices. It makes sense to leverage the expertise of the data security experts and stay focused on your business.

Expect the same will occur with SIP trunking and delivery of services over IP. Enterprises will eventually choose a technology partner to secure their voice and video interface to the outside world and depend on leading-edge technology and expertise to protect their enterprise from the "bad guys".

Getting in the Game

In the end, it seems that only a handfull of vendors will be able to step up and play a role in solving the security and interoperability challenges created by greater penetration of SIP Trunking. The keys to holding one of these positions will be:

1. An demonstrated history of the related VoIP transport and media technologies
2. A range of established interoperability relationships
3. A deep understanding of the security challenges and solutions
4. Established OEM or channel relationships needed to deliver product to the market

Final Words

The promise of SIP Trunking is within sight and based on some early adoption rates, there is strong interest for secure, interoperable and reliable connectivity. The issue is whether the SIP trunking carriers and their technology partners are up to the challenge. If you do take the jump to SIP Trunking, choose your partners well - as the cliché goes, your career may depend on it.

Alan Percy is Director of Business Development at AudioCodes, (news - alert) a leading provider of Voice over IP and Session Border Controller-enabling technology. In this role, Mr. Percy is responsible for identifying market trends and building relationships to foster new business opportunities. Mr. Percy joined AudioCodes in 2001 and brings over 20 years of experience in the telecommunications, networking and wireless equipment industries. Mr. Percy holds a BA in Computer Science from the University of Buffalo, has had a number of papers published in various telecom technical journals. Percy is a frequent speaker at industry conferences and was recently named to the 100 Top Voices of IP Communications by Internet Telephony magazine. He can be reached at alan.percy@audiocodes.com