



**UNIFIED
COMMUNICATIONS
STRATEGIES**



SIP Trunking: How the NET UX2000 Helps Balance Risk and Reward

Russell Bennett

UC Insights

www.ucinsights.com

russell@ucinsights.com

Introduction

Unified communications (UC) holds out the promise of rich, multi-modal, presence-driven collaboration to enhance business productivity and speed decision making within the enterprise. However, no enterprise can reasonably invest in unified communications (UC) if it has no connectivity with the outside world. Although much business communication is conducted over email, landline/mobile telephony is the default real-time modality for 99+% of business communications; so any UC system must be connected to the PSTN. However, as we all know, the PSTN uses a completely different set of protocols that are wholly incompatible with those of a UC system. So the UC Architect is faced with 3 choices:

1. Connect the UC system to a traditional PBX which connects to the PSTN via a PRI Trunk;
2. Connect the UC system to a traditional PRI Trunk via an IP-PSTN gateway;
3. Connect the UC system to the PSTN via a SIP Trunk service.

The third method, SIP Trunking, arose as a mechanism for overcoming the limitations of the PRI trunk, specifically:

- The 23/30 channel limit;
- The fixed (64k) bandwidth per channel;
- Being tied into telephony toll rate plans for even inter-branch calls.

SIP Trunks use the same protocols as the UC system, and present an open market for the provision of PSTN origination and termination service via the Internet; so option 3 makes the most sense. However, scratching below the shiny surface of SIP Trunking reveals a series of challenges and complications.

SIP Trunking standards – or lack thereof

The SIP standards defined within a number of [IETF](#) RFCs contain certain ambiguities through the use of words such as ‘SHOULD’, ‘MAY’, ‘RECOMMENDED’ etc. in specifying implementation requirements¹. Where the standards are quite clear, some implementers of SIP technology have applied their own interpretations, for reasons best known to them, which create interoperability challenges. This is never more true than with SIP Trunking.

I recently wrote [a paper on SIP Trunking standards](#) regarding the [SIP Forum](#)’s recent ratification of its [SIPconnect 1.1 Technical Recommendation](#). Whether this standard is widely acknowledged, adopted or implemented by SIP Trunk service providers and UC vendors, in any given time frame, remains to be seen. In the meantime, the implementations of SIP Trunk interfaces run the gamut of possibilities in terms of the overall structure of the SIP messages, the choices of SIP transport and the use of voice codecs. For example:

- The service provider only supports UDP as a SIP transport, but the UC vendor recommends the use of TCP/TLS for security;
- The service provider requires the G.729 voice codec, but the UC vendor only supports G.711;
- The service provider places calls ‘on hold’ using “a=recvonly” in the SDP body, but the UC vendor uses “a=inactive”.

So unless your UC equipment vendor has certified its SIP Trunk interface against that of your service provider, it is almost certain that the two implementations do not match. I ran the Microsoft SIP Trunk certification program for 3 years and experienced the diversity of implementations at first hand. Absent a SIP Trunk standard, achieving bilateral interoperability between every SIP Trunk implementer is probably the modern equivalent of the Twelve Labors of Hercules.

By far the simplest solution to this situation is to deploy a [UX2000](#), from Network Equipment Technologies (NET). These devices can be configured to adapt to the various UC vendor and service provider implementations and can transcode voice codecs as required. The UX2000 ships with pre-tested configurations for the major UC vendors and SIP Trunk service providers. If your UC vendor or service provider are not in the pre-configured list, NET will provide consulting support to assist in configuring the device. Transcoding (i.e. converting, say, G.711 to G.729) is done at very high scale in hardware, using specialized Digital Signaling Processors (i.e. codecs baked into silicon).

The major telephony service providers will often support the ‘SIP message tweaking’ and transcoding functions in a DMZ-resident integrated services router that they provide with their MPLS service. Of course, these devices only connect to their service, which is strategically priced to minimize the cannibalization of their PRI revenues. In order to get the best rate for PSTN origination/termination, enterprises should examine the Internet-based SIP Trunk services that are not affiliated with the local Internet Service Provider or PSTN carrier. Using several service providers, both nationally and internationally, will probably provide the most flexibility and will allow optimization of various pricing structures. The ability to connect to different service providers, and the ‘least cost routing’ logic that will facilitate this, is a key feature of the UX2000.

¹ Most SIP RFCs refer to [RFC 2119](#): “Key words for use in RFCs to Indicate Requirement Levels”

Preventing Network Intrusion

As described above, the great thing about SIP Trunking is gaining access to Internet-based providers of PSTN termination and origination. The bad thing about SIP Trunking is that those providers reside in the Internet, along with the hackers, virus writers, fraudsters and sundry other malcontents. Therefore, it goes without saying that deploying a SIP Trunk interface at the enterprise network edge requires robust security.

The corporate networks are typically protected from unauthorized intrusion by 'firewalls'. These devices are deployed in the network DMZ and are designed to allow only validated traffic to pass to and from the core enterprise network. However, firewalls are primarily designed to cope with simple message-based traffic such as email (SMTP) and web page requests (HTTP), both of which are easy to inspect and validate. Therefore, most firewalls will block SIP Trunking traffic because they are unable to cope with the complexity and load:

- SIP messages are typically complex, with other protocols and message types embedded within them: so differentiating a valid and authorized SIP transaction from a 'Trojan Horse' is difficult;
- Voice codecs occupy significant bandwidth – so operating at scale requires specialized technology;
- SIP and real-time media should be encrypted to ensure privacy and security, but decrypting these data packets to ensure validity introduces latency into the call.

The inability of firewalls to deal with the complexity and load created by SIP Trunking means that network administrators have three choices:

1. Block SIP Trunk traffic from traversing the firewall (which will be the default action with most firewalls).
2. Open firewall ports to freely allow the traversal of SIP Trunk (and any other) traffic.
3. Deploy a SIP Trunk gateway with an embedded Enterprise Session Border Controller (E-SBC).

The first two options are non-starters, and the E-SBC function is a key feature of the [NET UX2000](#). In order to provide high scalability in tandem with high security, the UX2000 uses a range of technologies and techniques, including:

- Establishing encrypted tunnels using TLS, authenticated by an exchange of digital certificates, to carry the SIP sessions between the service provider and the UC system;
- The use of DSPs for transcoding, as described above;
- (Assuming no transcoding is required) After validating the SIP session, allowing encrypted (SRTP) media packets associated with that session to pass through the assigned port. This is done with almost zero-latency by inspecting the (unencrypted) packet header to ensure that it originates from and is destined for the IP addresses of the validated end-points.

The Viable Alternatives

Of course, NET isn't the only vendor of SIP Trunking gateways, and some competitors also ship an on-board E-SBC. When comparing UX2000 to this class of devices, you should compare their security features to those of NET, who is (I think) the only vendor with extensive certification for and deployment in Federal Government communications networks. You should also compare modularity and adaptability: two key attributes that will reduce cost by allowing you to configure each device for the requirements of each individual deployment.

Another alternative would be to evaluate a pure-play E-SBC. There are a number on the market and these devices are feature rich security elements that have adapted their security and session mediation features to accommodate SIP Trunking as an additional use case. Without doubt, E-SBCs are highly adaptable 'Swiss-army-knives' for the IP network edge and can perform a range of non-UC functions that the UX2000 is not designed to address, such as application session security (i.e. protecting web-sites). However, E-SBCs did not originate as communications devices and are missing the 'legacy PBX' connectivity that is critical to accommodate a phased migration plan from TDM to UC. Furthermore, these devices can be expensive and close attention should be paid to scale costs (i.e. call volume per \$) and their cost effectiveness in the branch office scenario.

If you are a deployer of Microsoft Lync, you will want to ensure that the Survivable Branch Appliance (SBA) is a feature of all devices that you evaluate for branch office deployments. A branch office can gain from a SIP Trunk service and provide access to the local PSTN connection for the entire corporate network. However, in an IP-outage scenario, having an SBA and a TDM gateway connection is the only way to maintain local business continuity.

Summary

For many, the complexity and risk of SIP Trunking may seem to outweigh the rewards. However, I contend that the most successful firms (and people) are those that deal with the world as they find it, rather than waiting for the world to conform to their expectations. So it goes with UC/PSTN connectivity:

- PRI trunks are expensive;
- SIP Trunk services are not yet standardized;
- No single SIP Trunk service provider will be able to support your needs across a range of geographies;
- The Internet is occupied by malcontents and fraudsters just waiting for you to drop your guard.

Dealing with the world of SIP Trunking as we find it means that the UC Architect should consider deploying a SIP Trunking gateway with an embedded E-SBC such as the innovative, highly scalable and highly adaptable NET UX2000. This device enables the enterprise to facilitate interoperability with various SIP Trunk services; to leverage least cost routing across a range of service providers as well as to defend the corporate network against unauthorized intrusion.

Copyright © 2011 UCStrategies. All rights reserved. Information in this document is subject to change without notice. UCStrategies assumes no responsibility for any errors that may appear in this document.

UCStrategies

St. Helena, CA 94574
Phone: (707) 963-9966
UCStrategies.com

NET

6900 Paseo Padre Parkway
Fremont, CA 94555
Toll Free: (800) 234-4638
Phone: (510) 713-7300
Fax: (510) 574-4000