

# Peerless VoIP Peering

By: Richard “Zippy” Grigonis

In the long migration to VoIP, network operators and service providers have discovered the need to efficiently and securely (not to mention inexpensively) exchange traffic in a native IP format without having it dive in and out of the PSTN. This is where VoIP Peering comes in, a general term describing service solutions that can connect carriers or, in another form, enterprise and consumer customers.

Stealth Communications is a company that gradually evolved into a preeminent position in the VoIP Peering world. Starting in 1995 as a provider of dedicated Internet access services to the mid-size and large enterprises in New York, it expanded in 1997 into the financial sector via its “the Financial Medium”, a low-latency, Ethernet-based interconnection service directly linking financial institutions with their trading partners. From there it was only a hop, skip and a jump to 2001, when they entered the service provider market with the world’s second largest native IPv6 exchange, NY6IX, later renamed the Big Apple Peering Exchange (Big APE) with added IPv4 support. Finally, in 2003, service providers the world over began to clamor to hook up with Stealth’s Voice Peering Fabric (VPF), based on a “Route at Layer-2” service model enabling buyers and sellers of minutes and telephony-related services to trade without a broker or counter-party, and route traffic completely within the IP domain, bypassing both the PSTN and the public Internet. VPF is one of the VoIP Peering industry’s great success stories, handling about 900 million minutes on a daily basis or over 300 billion minutes annually.

It may seem a bit strange to have LANs of various companies (as well as an increasing number of university campuses) connect at the VPF facilities at 60 Hudson in New York City, 700 South Federal in Chicago or Beijing, China. Calls are routed through the VPF and then to your LAN, IP PBX and/or desktop IP Phone, with no PSTN interworking or unnecessary routing hops around the Internet. Strange or not, it does simplify things and saves money. Of course, in many cases, some transcoding is still necessary at network borders, and some companies have taken devices such as the Dialogic IMG (Integrated Media Gateway) and have developed transcoding services.

Still, VoIP Peering was an immediate hit among the more forward-looking operators. For example, when LatiNode (a wholesale carrier serving the U.S., Central and South America) decided to be one of the first carriers to exchange voice traffic with other operators, its annual traffic rose from 31 million minutes in fiscal year 2001/2002 to 500 million minutes in the period ending June 2004 (fiscal year 2003/2004). Its customer and supplier interconnects also increased from 20 to 120.

In 2005 Eli Katz and some top venture capitalists (Venrock and Accel) founded a major VoIP Peering powerhouse, XConnect, which specializes in “Plug and Peer” VoIP federation-based interconnection services that connect IP-enabled carriers and services providers with rich multimedia end-to-end IP communications services. It operates peering solutions as either a managed service or on a hosted basis. It has headquarters in London with offices and facilities in U.S., Europe and Asia. XConnect deftly handles protocol interoperability, ENUM



directory services, and security/policy management. Teamed with its strategic technical partner Kayote Networks (makers of the hosted VoIP Traffic Manager, or VTM, that allows carriers and wholesalers to route and manage their VoIP traffic), XConnect provides ENUM and peering services to over 400 operators in more than 35 countries, including the Netherlands’ first nation-wide VoIP peering solution. It also recently acquired the European carrier ENUM exchange, e164.info and IPeerX.

Katz, now XConnect’s CEO, says, “There are some core aspects to the way the industry has evolved over the past six months. First, a new connection paradigm is emerging as the interconnection paradigm across the IP communications space, whether you’re looking at it from the point of view of voice-over-broadband operators, or the mobile IMS-based operators, or the fixed-line next-gen network. The connection paradigm that’s emerging is converging on the federation model, which we at XConnect have been developing over the past three years. The core components of a federation model consist, first, of some kind of IP connectivity. Then you have the registry function which provides the most efficient routing mechanism possible by being able to route a session, whether it’s a voice session or video, or push-to-talk or SMS or whatever new IP feature exists, to identify the correct routing, based upon the number or identifier that has been dialed or called.”

“Then there’s the signaling function that says, ‘Okay, the registry function has enabled me to identify to which service provider or entity I must route this call and possibly even identify the actual egress point in that customer’s network.’ Now you need to enable the signaling to go from service provider A to service provider B. And we see the role of a federation-based approach to signaling, which is to say that having a signaling hub to enable all of the different flavors of the signaling management to take place, whether that’s multi-protocol, or multiple versions or multiple instantiations, all of the underlying protocols dealing with a signaling hub essentially will enable you to have a scalable interconnection.”

“The next area we see that gets attention is security,” says Katz. “That refers to the additional requirements that are above and beyond your pure network-type of security. This relates to security that is more appropriate at the communication level. It involves things such as Spam over Internet Telephony [SPIT] protection, voice phishing, identity preservation and management, which is crucial when enabling a scalable interconnection. All of that fits into the security layer.”

“The top layer is the commercial layer,” says Katz. “There’s a choice of different commercial models in terms of how as a service provider you want to indicate what you are in comparison with other providers and you can choose to go down the route of, say, an assessment-based commercial approach, which is a classic ‘you-pay-me-for-every-minute-that-comes-into-my-network – and I will do the same for you’. There are newer models such as the settlement-free bill-and-keep model, which is a managed, settlement-free-based accounting mechanism set up between providers. Of course as an originator and a terminator of call traffic, you may have different commercial models when dealing with different service providers.”

“So all of these functions and models can occur in a federation or hub-type approach to scalable interconnection,” says Katz. “The federation approach is driven by the desire to effectively have as close an interconnection as possible between a service provider you deal with as well as all the other service providers called by your customers. Without that capability, you lose the ability to deliver new IP services and you start introducing unnecessary transit elements that have an effect both on the quality of the call or multimedia session as well as its actual cost.”

“All of this points to the question of how do we deliver a scalable, multilateral, hub-type approach to ‘I-want-to-interconnect 1,000 other service providers but I don’t have the capability or infrastructure to support 1,000 different bi-lateral interconnects’,” says Katz. “The federation or hub approach that’s emerging today is the exciting new paradigm for interconnection amongst all IP communications service providers.”

“One additional element in this new paradigm I haven’t yet mentioned – the standards bodies,” says Katz. “What are they up to regarding the enablement of this federation model? From a global standards perspective, you have the IETF responsible for all Internet protocols such as SIP [Session Initiation Protocol]. The IETF has two fundamental working groups, SPEERMINT and a new one called PEPPERMINT. SPEERMINT has to do with SIP-based peering, and the interconnection between service providers using the federated pipe model approach. PEPPERMINT deals with the private ENUM registry component. PEPPERMINT handles how you provision data into these scalable ENUM registry-type sources and services. You can appreciate how this model is beginning to gain ground by seeing how much development work occurs at the IETF on a ongoing basis.”

“In terms of actual instantiations,” says Katz, “many things have been happening over the past six months. First, take the GSMA, the association of all GSM wireless operators, one of the largest industry bodies in all of telecom. Over the past year – and much more so in pilot trials over the past few months – they’ve developed the registry component, the NRS [Number Resolution System] a global registry system to be used by GSM operators for optimized routing through the appropriate service provider across multiple services. That’s the pure registry component. That together with the signaling component is what they call the GSMA IPX, or IP Exchange, which is essentially a federation entity supporting a hub-based approach to the signaling and elements of security and ele-

ments of the commercial layer as well, as they have defined the commercial structures between service providers. The GSMA approach is what I described previously, the NRS and the IPX. In the past the trials on the NRS are now in the pilot phase. The IPX has already been in trials for a year-and-a-half, and is approaching commercial launch.”

“The GSM operators are concerned with how to enable the new services to be delivered on the most efficient routing basis possible,” says Katz, “and how we can enable the mass-market to partake of these new services in such a way that we enable transparency, feature-preservation and minimize unnecessary transit elements that disrupt these as well as increase cost.”

It is with increasing frequency that organizations need to contract out jobs to third parties. As such, many enter into arrangements where they have temps, sub-contractors and consultants of various types using their facilities on a non-permanent basis. Obviously, these on-site workers — whether they are there for the long or short haul — need network access.

Giant VoIP peering service providers such as Stealth’s VPF and XConnect run ‘federations’ of VoIP service providers that agree to exchange traffic under mutual agreed-upon rules. There are other forms of peering, of course. At a lower level, enterprises can set up networks to peer with their partners, suppliers and even customers.

In such cases, as more third-parties (partners, customers, suppliers) gain access to such increasingly vulnerable unified/converged corporate networks, IT departments will be investing in more network access solutions that allow for customized access, such as deciding who has permission to access what, on a group and/or individual basis, and for a set period of time.

One company that’s well-known in the Network Access Control (NAC) area is Great Bay Software and its Sponsored Guest Access (SGA) security application that lets IT administrators configure and monitor network security parameters for guest users, contract employees, and devices requiring temporary or specialized access in NAC or 802.1X networks. It’s interoperable with major NAC vendor solutions, including those of Cisco, ID Engines, Juniper and Symantec. Authorized company employees can create guest accounts, including the ability to manage time and user permissions. SGA also allows for the implementation of an Acceptable Use Policy. Coupling SGA with Great Bay’s Beacon Endpoint Profiler network management solution, NAC Appliance and 802.1X administrators can get reports on guest user network behavior, along with an ongoing contextual inventory of all appliances and ports, including non-Windows and non-NAC/EAP devices. **IT**

*Richard Grigonis is Executive Editor of TMC’s IP Communications Group.*

#### The following companies were mentioned in this article:

**Great Bay Software**  
[www.greatbaysoftware.com](http://www.greatbaysoftware.com)

**Voice Peering Fabric**  
[www.thevpf.com](http://www.thevpf.com)

**Kayote Networks**  
[www.kayote.com](http://www.kayote.com)

**XConnect**  
[www.xconnect.net](http://www.xconnect.net)

**Stealth Communications**  
[www.stealth.net](http://www.stealth.net)