

VoIP Virtual Private Networks: Bringing the Benefits of Convergence to the Enterprise

By Robert VanSickle

Vice President Sales, Americas Region & Worldwide Sales Strategy

VocalTec Communications

www.vocaltec.com

Robert_VanSickle@vocaltec.com

Virtual private networks (VPNs) are not new to the enterprise environment. Large corporations, as well as small and medium-sized enterprises (SMEs), have been operating IP-based VPNs for many years to carry large volumes of data traffic. Voice traffic within the enterprise was traditionally carried over a separate leased line network. This has always been a costly service and typically reserved for the larger corporations. Today, Voice over IP (VoIP) technology enables enterprises large and small to leverage their existing IP VPNs to carry voice traffic as well. These VoIP VPN solutions, offered by several leading carriers, allow voice to be handled as another data application running over the IP network. This allows enterprises to run all of their voice, data and fax communications over a single network, managed and billed by one service provider. Given the savings involved, it is no wonder that nascent VoIP VPN services in the United States are expected to grow to \$1.4 billion by 2007 (Probe Research, April 2002).

Business Case

Over the last five years, long distance rates have dropped due to deregulation and increasing competition in the international and national long distance markets. As a result, the business case for international toll bypass in these competitive markets has become less compelling, as the main cost component for long distance calls has shifted to the last mile (local access). Carrier-provided Voice VPN solutions based on end-to-end VoIP connectivity circumvent the last mile and significantly reduce transport costs. These savings can be passed on to the enterprise, while still leaving the carrier with a better margin. For enterprises with offices in countries with high-cost international tariffs, international toll bypass is still a key business driver.

VoIP VPN can be thought of as an enhanced managed data VPN service. Thus, enterprises can leverage VoIP VPN to expand their data capacity while reducing their voice costs. Combining voice and data makes it easier to justify bandwidth required to connect SMEs to a service provider's POP, as voice savings can offset the pipe cost. As such, the SME market, traditionally neglected by global and incumbent carriers, represents a huge opportunity for alternative carriers.

Another key factor driving deployments of VoIP VPN is Quality of Service (QoS). As MPLS technology is rolled out in service provider IP backbones and backed up with SLAs, service providers can commit to the QoS levels required by enterprises.

Looking forward, VoIP VPNs provide carriers with a vehicle to ease customer transition to IP. Once the VoIP architecture is in place, carriers can offer enhanced revenue-generating IP services on top of the same infrastructure.

How does VoIP VPN Work?

VoIP VPN enables carriers to provide multiple corporate customers with cost-effective, private voice services over managed and unmanaged IP networks. These voice VPN services are managed and billed by the carrier and integrate seamlessly with the enterprise's existing corporate dialing plans, including support for abbreviated dialing, closed user groups, centralized management and advanced billing options. VoIP VPN services may include on-net and off-net calling services for maximum reduction of long distance costs. Robust security features control access to corporate network resources.

Carriers offer two types of VoIP VPN models: 1) CPE model based on dedicated customer premises equipment (CPE); and 2) hosted model based on shared gateways at the carrier's central office servicing multiple enterprises.

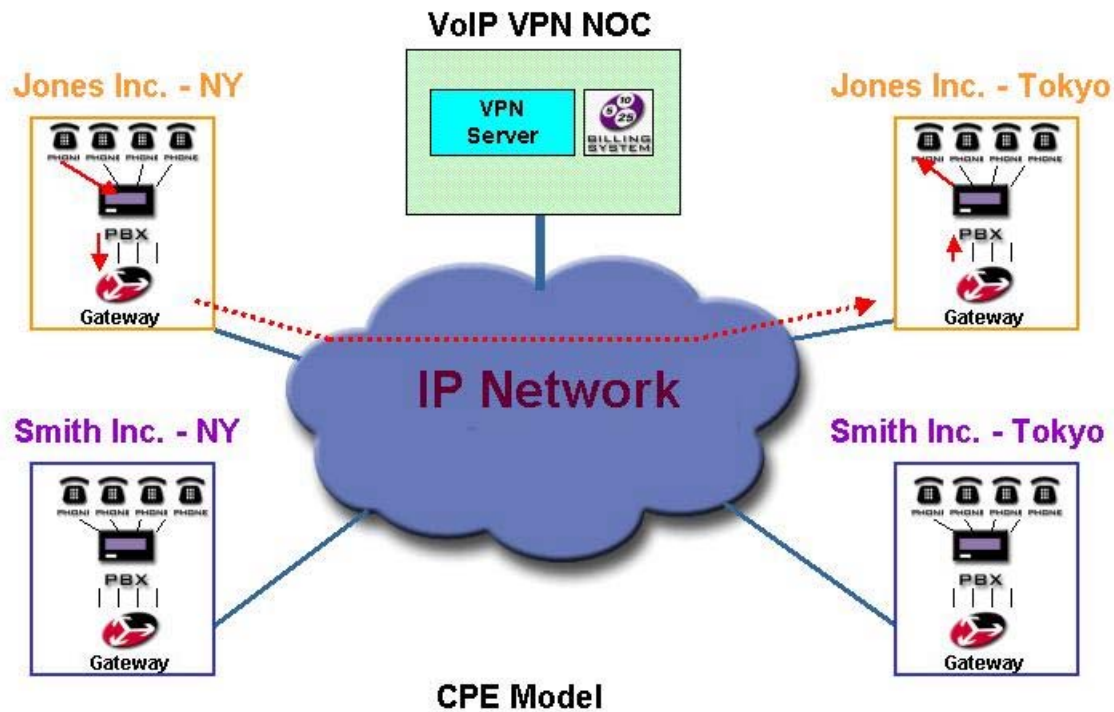
CPE Model

The CPE model deploys a VoIP gateway at each branch site and can be easily integrated within the enterprise's existing IP infrastructure. The CPE model reduces the service provider's cost of ownership as the enterprise purchases/leases the gateway. These gateways are installed and can be managed by the service provider.

In addition, Web-based self-management enables non-technical enterprise personnel to perform administrative and provisioning activities, while reducing the service provider's management costs.

In the following example, the Jones Corporation's offices are located in New York and Tokyo. In each office a VoIP gateway is used to interface with the PBX. The two may be connected using analog or digital interfaces and signaling. The gateway located at the customer's premises connects to the carrier's IP backbone. The customized dialing plan and dial-routes are configured on the carrier's centralized VPN server. When a user in New York dials the extension of a user in Tokyo, the PBX forwards the call to the voice gateway. The voice gateway in New York queries the VPN server for the destination gateway based on the dialed extension number. The VPN server searches its database of configured routes and customized dial plans and, based on the match found, returns the IP address of the gateway in Tokyo. The gateway in New York then places the call to the gateway in Tokyo.

In this way, the CPE model achieves end-to-end VoIP connectivity between the Jones Corporation's international offices, bypassing international tolls as well as last mile access charges.



Hosted Model

The hosted model is deployed within the service provider's existing network infrastructure to provide a quick, inexpensive and scalable VPN solution. It is particularly suited for carriers that do not have the mass deployment capabilities required for installing the CPEs (e.g., CLECs). The hosted model provides enterprises with the technical backing of a carrier, responsible for delivering a fully managed service and often acting as systems integrator.

VoIP equipment can be deployed within the carrier's infrastructure to accept VPN traffic from thousands of different VPN users. By identifying and routing the call to the appropriate VPN group based on the Automatic Number Identification (ANI), there is no need to pre-dedicate PSTN switch ports for each VPN customer.

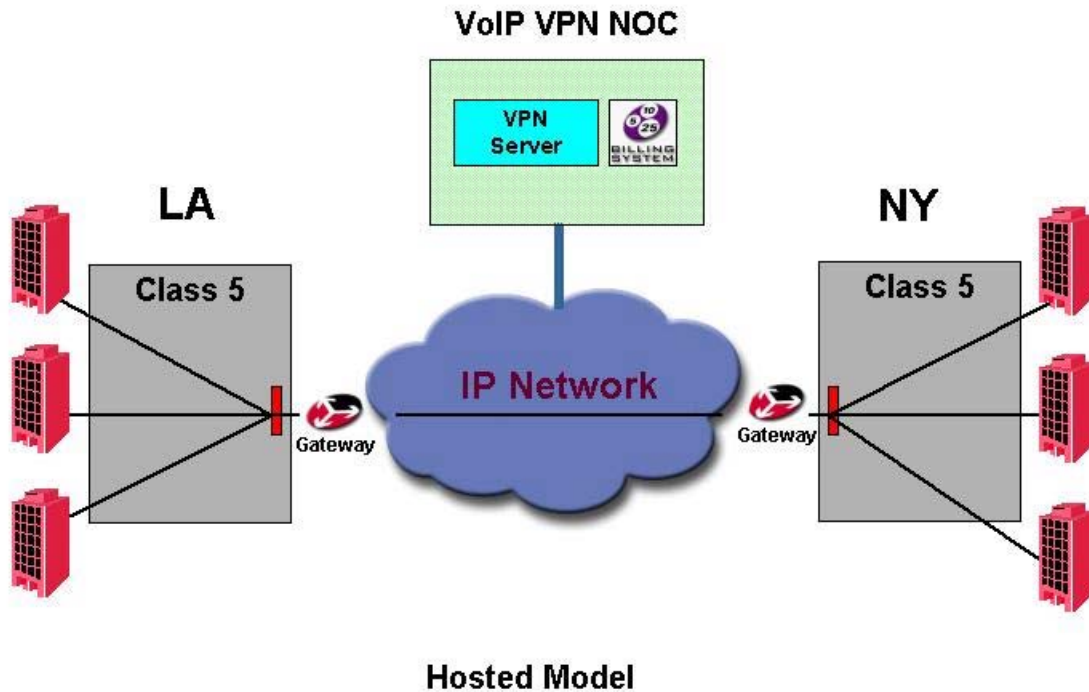
The hosted model is a radical departure from the CPE model. All equipment is located at the Central Office, a 24x7-manned location where rapid support and maintenance can be performed. There is no need to deploy staff to install and program CPE equipment, nor is costly training required for field personnel. Management of VPN service parameters is performed remotely from the carrier's Network Operations Center (NOC). Software-based provisioning allows for rapid deployment of new customers. Voice traffic can also be carried over the open Internet (enabling transport cost savings to the carrier), with assured voice quality and security using specially developed features. Additionally, the

need for redundant circuits is diminished due to the fully meshed, routed VoIP network, saving additional investment on backbone capacity.

Call Scenario

Let's say a caller in New York dials "5" for a VPN call and the 4-digit extension for a colleague in Los Angeles. The PBX then routes (based on the "5" prefix) the call to a trunk group, which the phone company's Class 5 switch identifies as a VPN call. Using existing technology, the Class 5 switch can be programmed to know which trunk group, which may be shared by multiple enterprises, the VPN call goes to. It then connects the call to the trunk group that terminates on a VoIP Gateway and passes the ANI in the call set up information.

The VoIP Gateway then asks the VPN service to assign the proper VPN dialing plan based on the ANI, and map the 4-digit extension to a fully qualified E.164 number. The VoIP architecture's intelligent routing capabilities select one or more potential Gateways in LA to terminate the call. This information is provided to the originating Gateway in New York, which in turn connects the call to the proper Gateway in LA. From the LA Gateway the call is then passed to the local switch for call termination.



Win-Win Proposition for carriers and enterprises

VoIP VPN represents a very strong value proposition for both carriers and enterprises:

Carrier benefits

- Cost-effective support of multiple VPNs using single shared infrastructure
- High scalability and flexibility using ANI-based routing
- Additional revenues from voice services vis-à-vis flat rate, low-price data services
- Convergence optimizes bandwidth utilization and works with existing PBX
- Differentiation by offering enterprises enhanced dialing capabilities in small branches
- Leveraging VoIP VPN platform for provision of enhanced IP-based services, such as unified messaging and voice mail with Web integration

Enterprise benefits

- Reduced costs
 - Save on intra office communications (on-net)
 - Save on off-net international/LD calls (toll bypass)
 - Eliminate expensive PBXs in small offices
 - Forced on-net, which routes PSTN dialed calls through the VoIP network when the dialed number belongs to the same VPN
- Single provider and single bill for voice and data services
- Billing by department for internal cost control
- Managed service with no support overhead
- VPN off-net originated calls for traveling users

Conclusion

Feature-rich VoIP VPN services allow carriers and service providers to address the immediate needs of the lucrative and growing enterprise market, which by 2007 will account for 36 percent of overall voice over packet traffic in the United States (Probe). Using CPE-based or hosted models, Voice VPN is a cost-effective, scalable solution for the carrier, while significantly cutting operational costs for multinational corporations and SMEs. The VoIP VPN solution can be deployed to run on top of enterprises' existing high-bandwidth data networks, serving as the basis for convergent IP-based services.