



# Securing Your VoIP Calls

By Wayne Scaggs

**O**ftentimes the solution to one problem is the introduction to another problem...and so it is with Voice over Internet Protocol (VoIP). VoIP is a marvelous new technology, propelling us into greater opportunities and bigger challenges. There are many benefits of VoIP; there are also security issues. Is your first response, "What security?" That was my first thought, and it is still on my mind. What do we need to do to ensure the integrity of our systems?

VoIP is the digitalization of analog voice, sent over a network. The network can be a LAN, WAN, or the Internet. The security issues for VoIP are the same as any other data that needs to be secured; however, there are some special conditions to deal with when it comes to voice data.

Unlike other data over a network, voice data has to be understood by the human ear. Therefore, in addition to speed of the data, we also have to be aware of the sequence of the data. When the data is slowed by security devices, the voice will sound choppy. When the data is out of sequence, it is unintelligible. Quality of Service (QoS) is the component needed to manage and organize the data.

The Internet provides free transportation for our data to travel. Along with this free transportation comes delay and insecurity, both of which can impede the use of VoIP over the Internet. VPN (Virtual Private Network) and SSL (Secure Sockets Layer) VoIP can provide a secure tunnel through the public Internet. As we address the security issues, keep in mind the requirements for an acceptable speed and bandwidth and the appropriate hardware to provide acceptable data flow throughput.

Your first line of defense is an above-average firewall; this can be hardware, software, or both, configured for your

optimal needs to prevent unauthorized access to your network. Your VoIP gateway should be behind your firewall for maximum protection. Placing your IP gateway behind the firewall helps insure authentication and prevents unauthorized use of your system, such as an intruder gaining access to your IP gateway and calling out on your switch.

Some VoIP gateways are configurable to only accept calls from predefined IP addresses, and the numbers must be registered in the gateway in order for the gateway to pass the IP call to your call center switch. If your gateway is not behind the firewall, you'll have to otherwise insure proper configuration and authentication of the data entering your network.

Let's put the pieces together:

- Start with a broadband connection to the Internet, preferably a data T1
- Add a firewall for your data and network protection
- Connect the IP gateway to the network and your call center switch
- Get a provider of IP calls
- Enable QoS on the router

This is just one configuration; there are variations to this configuration, in addition to other configurations. When it is time to add VoIP, remember that the voice data needs the same security levels as your other data as well as enough processing power to incorporate QoS in the network.

*Wayne Scaggs is president of Alston Tascom, Inc., which offers an end-to-end contact center solution using digital telephony. For further information, contact Alston Tascom at 909-548-7300, [info@alstontascom.com](mailto:info@alstontascom.com), or [www.alstontascom.com](http://www.alstontascom.com).*