# Making VoIP Perform as Advertised

The promise of lower cost has motivated many enterprises to move their voice traffic to the enterprise IP wide area network (WAN). Many have discovered, however, that Voice over IP (VoIP) quality does not always meet business use standards.

In addition, as VoIP is introduced to the network, the performance of other business-critical applications -- already at risk given growing Web/Internet traffic -- begins to deteriorate. The challenge is to assure the performance of real-time VoIP calls while protecting business data that requires immediate response times, in a manner that optimizes the efficiency of the WAN.

The growth in real-time and interactive business traffic that requires immediate response mandates a layer of application-aware control that intelligently links the performance requirements of a growing mix of converged data, VoIP and video applications with available network resources in a manner that assures an optimal user experience.

This application-aware, traffic-management solution should work with the existing IP network, and should assure the performance of individual VoIP calls and application flows. Policies should be accurate and application-aware, and tuning performance in both the inbound and outbound directions should be possible to ensure the integrity of each user connection.

Users should first know what is currently running on their network so that they can proactively manage the WAN to assure business-critical data and VoIP performance. Traffic should be actively monitored, classified and then assigned policies that assure the required level of performance in the most efficient manner possible.

Intelligent traffic-management policies can be applied to assure the performance of existing business-critical applications (e.g., CRM, SAP), while non-critical traffic is limited in the most efficient manner possible. In most cases, traffic-management policies that specifically guarantee bandwidth and response time for each application session and/or flow are required.

VoIP-specific controls should be applied to assure real-time VoIP call performance (e.g., latency, jitter, bandwidth) on a call-by-call basis. This requires granular and accurate enforcement of bandwidth policies and priority control for each individual call. Given that a VoIP call is a two-way exchange, these policies should be enforced in both the inbound and outbound direction.

In addition, because a VoIP session consists of multiple flows (e.g., call setup, call control and call media) each flow should be individually protected to guarantee the integrity of the call. This means the traffic-management solution should be session aware and enforced on a per-flow basis. For example, if the call control information for a single call is compromised by the media traffic, calls may be dropped midstream.

While proactive traffic management provides a first level of control against other applications running on the network, techniques such as packet size optimization and burst control are necessary to manage the impact at a packet level. These are not available when a router alone is used to perform the traffic-management functions.

Call admission control is needed to protect VoIP calls already in progress. This should be network aware (knowledgeable about calls running on the network), with policies that establish directives on what to do when the next call is placed. In addition, the policy-management process should be kept simple, using VoIP-aware defaults that apply policies dynamically based on the VoIP protocol, the codec and the number of concurrent calls to be supported.



## About the Author

For further information contact: David Cowgill VoIP Blog Founder http://www.aboutvoip.org