5 Reasons Why Troubleshooting VoIP Problems with Wireshark Doesn't Work

Wireshark and other packet capture solutions are beneficial tools when investigating application layer problems because they can show you the contents of the packets and thus, identify application configuration problems. However, analyzers fail when they try to solve VoIP problems because of tool limitations. Here are 5 reasons why analyzers won't work:

1) **Can't solve packet loss problems.** If a capture confirmed that packets were missing in a conversation, you could not detect where or why the packets were missing: an analyzer only confirms that they were *not seen* in the capture. To find and solve the actual problem, routers and switches must be interrogated for error counters and misconfigurations.

2) **Single point of view.** If packets are lost upstream from where the capture is performed, the capture might look perfectly healthy. To narrow down where the problem might be occurring, the analyzer must be moved around the network to different locations.

3) **Can't track latency.** Analyzers don't capture how long packets have taken to reach their destination, or even the capture point: It may be a few milliseconds or it could be much longer.

4) **SPAN ports might make things worse.** If a SPAN port on a switch is used for the capture, it may not send all the packets to the analyzer. A switch's primary responsibility is to forward frames normally. Frames get copied to the SPAN port only if the switch has additional resources available. During microbursts, the switch may skip copying some packets to the SPAN port, making the capture incomplete. As a result, you may think that packets were lost when they weren't.

5) **Can't identify queueing problems.** Queueing is critically important for VoIP call quality. But an analyzer has no ability to see how, or if, queueing is configured properly.

PathSolutions TotalView addresses all of these situations, ensuring the best operating environment for VoIP and Video services.