pathSolutions

WHITE PAPER

Root Cause VoIP Troubleshooting

How to Identify and Resolve the Root-Causes of VoIP Call Quality Problems

(877) 748-1777
Sales@PathSolutions.com
www.PathSolutions.com

Contents

(877) 748-1777
Sales@PathSolutions.com
www.PathSolutions.com

Root-Cause Troubleshooting Key to Successful VoIP Deployments

Over the past five years, VoIP has become the preferred method for business voice communications. However, how you implement, deploy, and maintain a VoIP system will determine whether it's a success, failure, or simply riddled with ongoing issues that are never fully resolved.

Dealing with VoIP problems incur resource costs and wasted time while lowering IT and UC teams' customer satisfaction rates. In addition, poor quality calls can have a direct impact on a company's financial bottom line as the phone remains the main tool for conducting business. To avoid embarrassing and potentially career limiting VoIP deployments, IT and UC teams must identify and resolve the root-cause of VoIP call quality problems. This will determine customers' perceptions of service as well as how efficient IT is at addressing network issues.

The key to root-cause troubleshooting is the difference between *problem identification* and *problem resolution*: While it is much easier to identify a problem, the difficulty lies in how to resolve it. For example, a user notifies IT they have a problem and IT uses a tool to quickly confirm it. In this case, confirmation is relatively easy but that same tool may not be able to troubleshoot the root-cause of the problem.

This white paper describes a typical VoIP call quality problem, evaluates the tools used by organizations to solve it, and provides best practices for successful root-cause troubleshooting.

Case Study: "I Can't Hear You—Can You Hear Me?"

A VP, Dave, has just spoken with the IT Director about a call quality problem he experienced two hours ago. While the connection seemed okay, as the call progressed Dave could not hear everything the caller said to him—words seemed to be dropping in and out. Since that call, Dave has made several more and in all cases, the connection was good. But Dave wants to know if the original problem can be found and fixed so it won't happen again.

IT is now working against the clock: How quickly they are able to identify and resolve the problem may either impress Dave or cause him to walk away wondering why the IT budget is so high while the results seem so low. After all, how hard can it be to figure out what went wrong?

Networks are by nature, complex making it difficult to easily troubleshoot issues that may appear and then disappear. VoIP adds to that complexity as performance requirements for call quality are far more rigorous than data. But users don't care about how difficult it is to troubleshoot a problem; they just want the problem fixed.

Many times, IT professionals will pick up the wrong tool to try to identify and correct the problem. After all, there are many VoIP troubleshooting tools available on the market, each with a specific purpose. Selecting the wrong tool can lead to an incorrect diagnosis and thousands of dollars spent on unneeded repairs or upgrades. What's worse, the underlying issues that led to the poor VoIP quality call remain.

The following sections evaluate some of the most commonly-used tools and detail how Dave's problem might be addressed with those tools.

Packet Analyzer Tools (Wireshark)

A packet analyzer is a program that observes data packets as they flow across the network. It is typically used to confirm that a bottleneck is occurring on the network and is particularly handy for confirming packet loss during data transfers. Wireshark is a free, open source packet capture and analysis solution. The tool can either be set up on an analyzer port on a switch or via a wire-tap to look at packets that cross one particular link in the network.

To use Wireshark effectively, it's important to know which link to look at. As there are thousands of links on a given network, time may be wasted moving the analyzer around before finding the appropriate one. Once it is in the right location, Wireshark can be set up to start capturing packets. However, if the problem does not occur while Wireshark is capturing packets, the tool will be unable to identify the network issue that led to Dave's bad VoIP call.

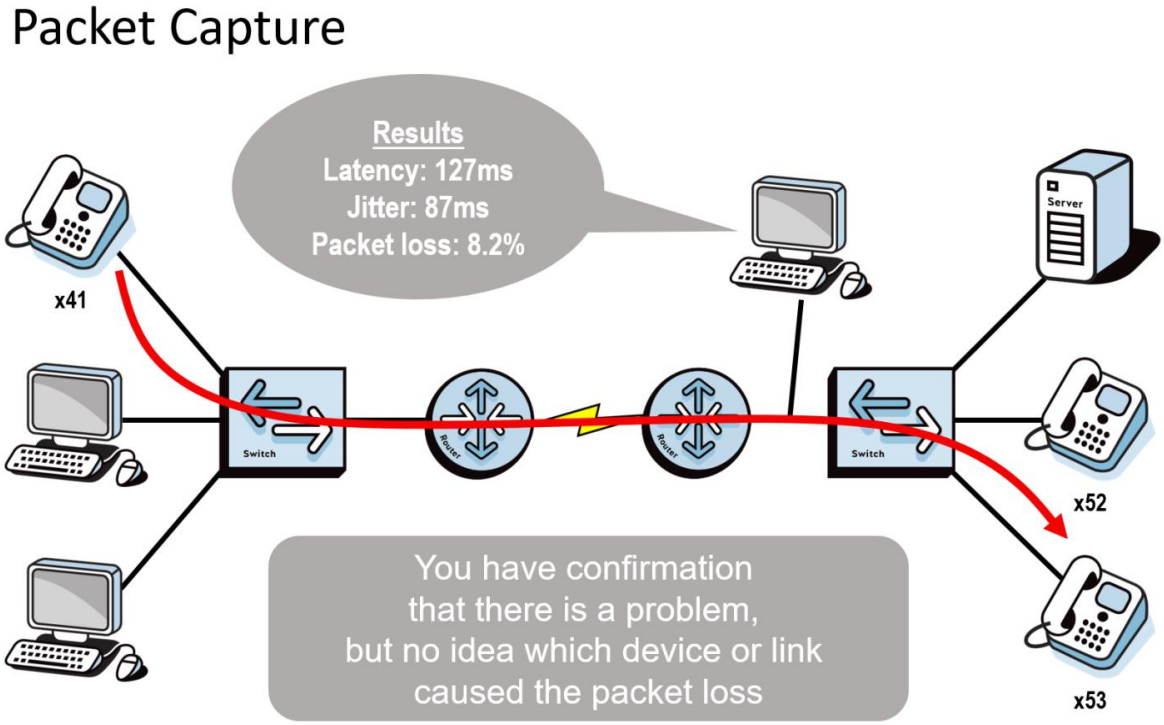
> ***Note:*** *Wireshark saves all of the captured packets it sees to a computer's local hard disk. These capture files can grow to be quite large depending on how long they are set to capture packets. To help reduce the size, put a capture filter in place telling Wireshark to only capture VoIP traffic to and from a certain phone's IP address.*

Since Dave's problem is intermittent and did not occur when Wireshark was set up, IT would be unable to determine which link dropped packets. In this case, Dave would have to wait until the problem happens again and notify the team. In general, this is an inefficient use of time and resources as users may not call IT or enter a help desk ticket when the problem happens and it may be a day or two until the problem occurs again. Keep in mind that throughout that time period, Wireshark is still capturing packets.

Once IT is notified the problem has resurfaced and knows the exact time sequence, it can stop the capture and start analyzing the packets for that period. IT can then verify the following:

- Packets were missing in the conversation.
- Packets had too high jitter or latency.
- Packets were out of order.

As the following figure shows, Dave's poor quality VoIP call was the result of jitter, latency, and packet loss. Unfortunately, since tools like Wireshark merely *confirm* the problem, IT cannot yet identify *where* or *why* the problem is happening.



What Packet Analyzers Are Good For

Packet analyzers are typically used to confirm packet loss during data transfers. They can also confirm that there are issues related to the contents of a packet (like missing QoS tags) or an application; for example, using an analyzer to gain feedback about session ports as well as possible issues with the source and destination of an IP address.

What Packet Analyzers Are Bad For

Packet analyzers, by definition, only give you a high level view of a problem—they can confirm that there is a problem but provide little insight into the root cause of it. For example, packet analyzers do not report issues in the physical, data-link, or network layers or provide any feedback related to bandwidth or device limitations.

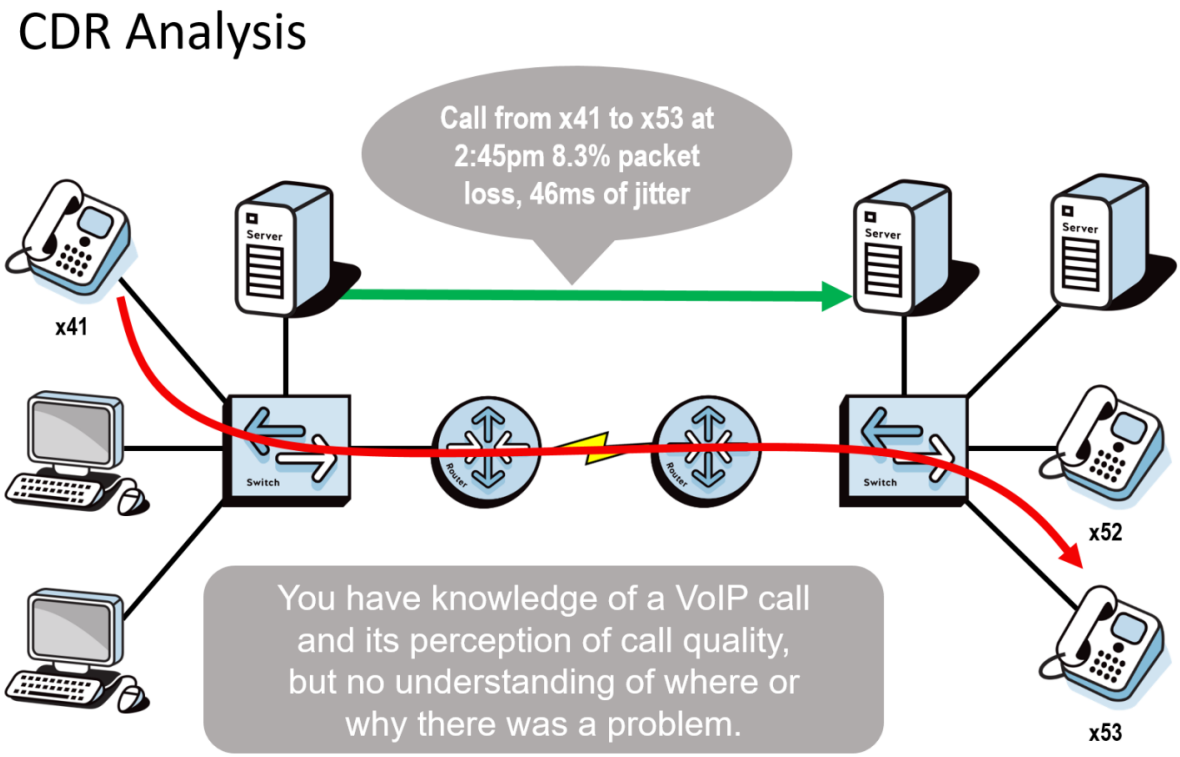
(877) 748-1777
Sales@PathSolutions.com
www.PathSolutions.com

Call Detail Record (CDR) Analysis Tool

Many VoIP phone systems store Call Detail Record (CDR) information on all calls made through the phone system, generally in a file or database. Often, that information includes call quality statistics like the loss and jitter seen during the call and other information that indicates how two phones are communicating over a network.

Typically, a third-party CDR analysis solution is needed to query and analyze these records. With this tool, information can immediately be accessed and viewed. In Dave's case, IT would be able to pull the data for the call that Dave was complaining about and verify the issue he was experiencing. However, IT would not be able to pinpoint the specific problem that caused the poor quality call and thus, would be unable to resolve it as these records only report what happened at a specific point in time.

As the following figure shows, Dave's poor quality VoIP call was the result of packet loss and jitter between phones x42 and x51. However, IT cannot identify *where* in the network the problem occurred or *why* it happened.



(877) 748-1777
Sales@PathSolutions.com
www.PathSolutions.com

What CDR Analyzers Are Good For

Like the majority of VoIP troubleshooting tools on the market, CDR analysis tools confirm that there is a problem on the network. They can also provide critical metrics that are often needed to justify performing system maintenance or upgrades.

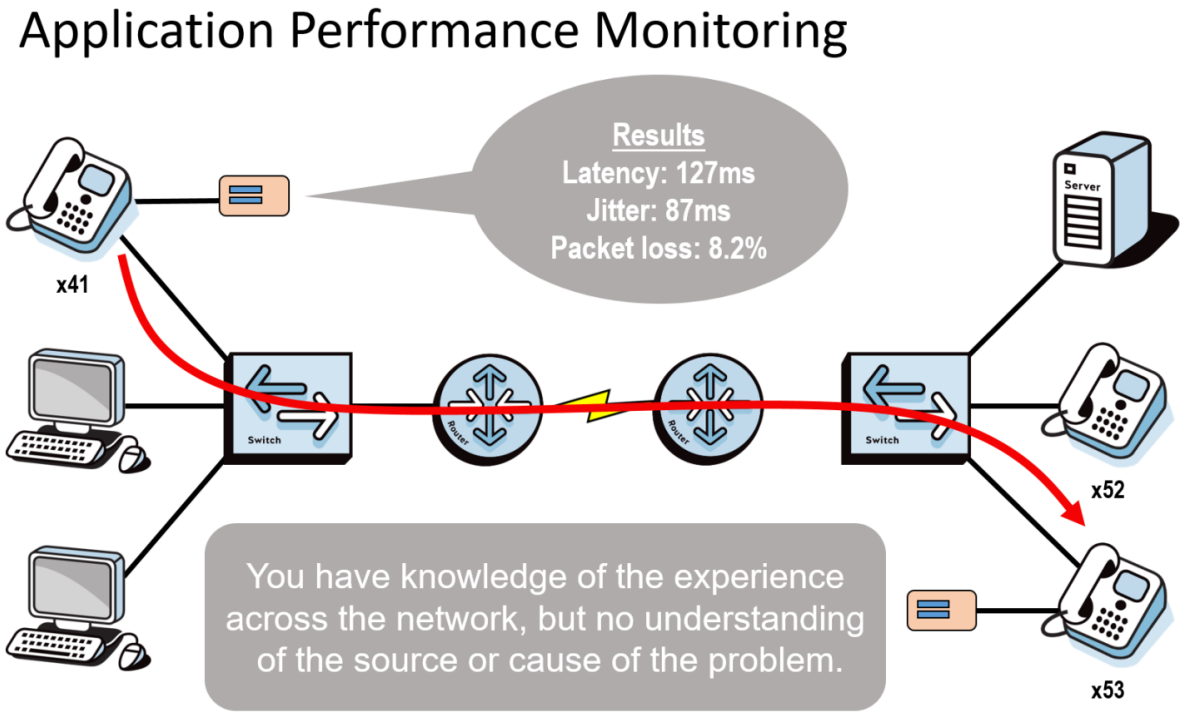
What CDR Analyzers Are Bad For

CDR analyzers are not troubleshooting tools. They can only confirm that there's a problem, they cannot identify where the problem is, what's causing it, or how to fix it.

Application Performance Monitoring (APM) Tools

Application performance monitoring—or call simulation—tools are used to determine the performance of a VoIP call. These types of tools operate as synthetic VoIP call generators, or call simulators, and test call quality around the network. APM tools require setting up two physical devices on the network and sending traffic between them, thus creating a synthetic voice call.

APM tools can identify call quality problems because they are constantly testing and measuring quality between two locations. In Dave's case, IT could set up an APM tool to monitor the performance between the two phones, x43 and x51, as the following figure shows. If the problem occurs again, the tool will be able to identify the problem but it will not be able to determine *where* or *why* the problem occurred.



What APM Tools Are Good For

APM tools are often used to measure the user experience across the network. If users are experiencing call quality problems, these tools confirm that problems like packet loss, latency, and jitter are occurring somewhere between the two endpoints.

What APM Tools Are Bad For

While APM tools can measure VoIP communications, they cannot pinpoint where the problem is occurring or the best way to fix it. Additionally, since these tools use network resources they have the potential of making actual VoIP calls worse by adding high-priority traffic to the network.

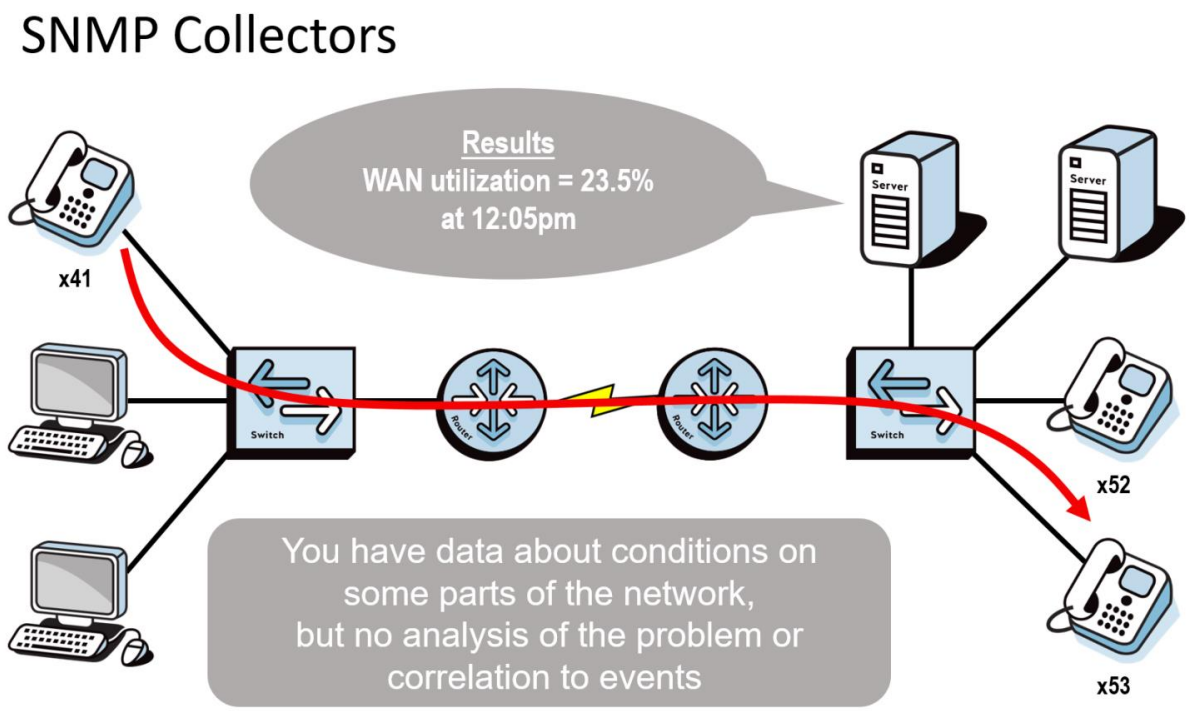
Simple Network Management Protocol (SNMP) Collector Tools

Most organizations employ some form of network performance monitoring on a network. An SNMP collector is a probe that finds and collects data from switches and routers on the network. This tool is used to measure performance related to specific conditions that are

occurring on individual network components. By analyzing this information, IT can gain a better understanding of important metrics like WAN utilization rates, resource limitations, and packet loss.

Typically, SNMP collectors require an administrator to have empirical knowledge about the network, the devices that exist, and the information available on the different devices. This may result in thousands of engineering-hours of effort spent downloading SNMP MIB files for network equipment, compiling them into the tool, and then configuring the tool to query specific data elements (OIDs) from the network equipment. Correlation of this data needs to be done manually and then interpreted by an expert.

SNMP collectors are difficult to configure and are not designed to report on the breadth or depth of the network. As a result these types of tools are not useful for troubleshooting problems. Additionally, SNMP collectors usually look at only one or two error counters—this is not enough information to identify and potentially diagnose VoIP call quality issues. In the following figure, all an SNMP collector can tell IT is that during Dave's call, the WAN link was overloaded at 2:35 pm. So while the SNMP collector identifies that a problem occurred during the call, it cannot determine whether the WAN link issue was the cause of Dave's poor call.



(877) 748-1777
Sales@PathSolutions.com
www.PathSolutions.com

What SNMP Collectors Are Good For

SNMP collectors provide targeted insight into a specific device. These tools can be used to confirm whether a device is working or not working.

What SNMP Collectors Are Bad For

While SNMP collectors can provide advanced insight into how devices are performing, these tools are not able to correlate that data with other devices on the network. Additionally, these tools tend to look at only a few error counters so it's possible that a device is identified as "healthy" may be throwing packets away due to a number of other error conditions the tool does not track.

Root-Cause Troubleshooting: A Better Way to Identify and Resolve VoIP Issues

While there are many tools available on the market today that provide some visibility into network problems, most are specialty solutions designed for specific uses. The tools described in the preceding sections fulfill a type of *guess-and-check* style of network troubleshooting. Worse, these tools may not even correctly identify where and why a problem occurred. A root-cause troubleshooting solution, however, takes a much more holistic approach: examining the root-cause of a problem, identifying the exact location of the error, and providing instructions on how to fix it.

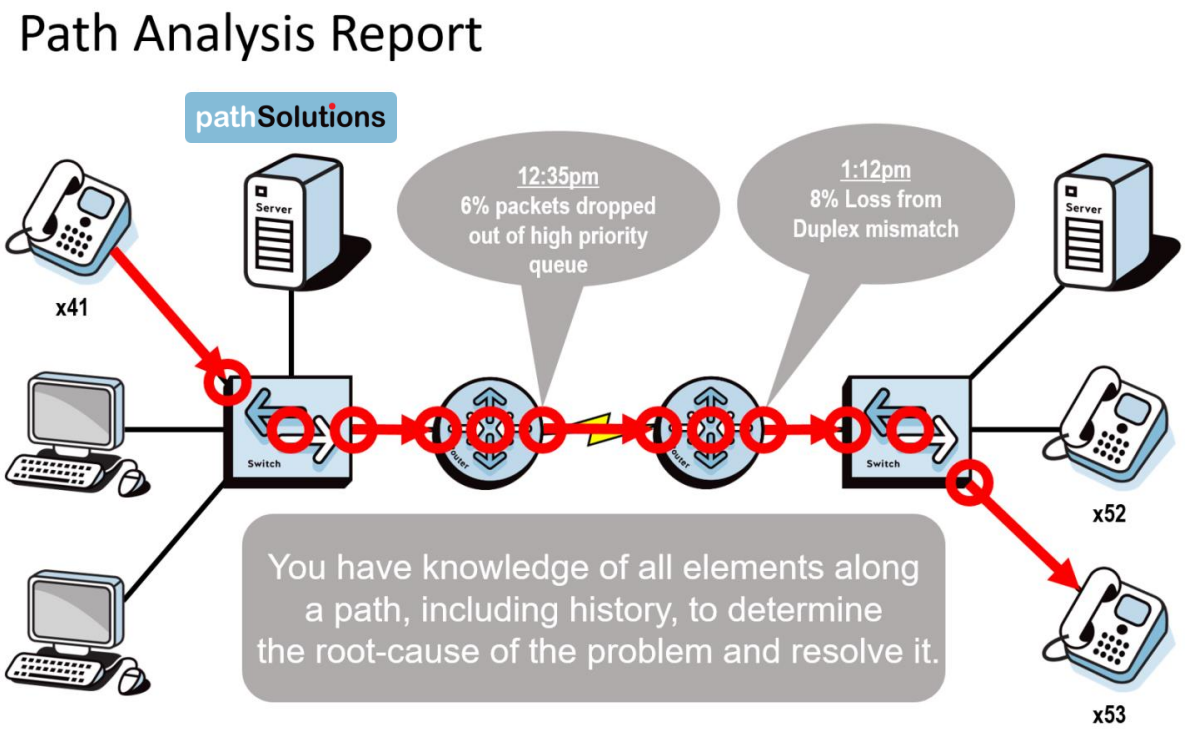
For example, it would be much easier to identify and resolve Dave's call quality problem if IT could identify what switches or routers were dropping or delaying packets along the path that the specific call took, at the time the call was made. If there was a plain-English description of the problem and how to resolve it, Dave's intermittent call problem could have been fixed in a matter of minutes.

PathSolutions TotalView for VoIP networks is a root-cause troubleshooting tool. Unlike other tools, TotalView queries all routers, switches, and gateways in the entire infrastructure for error counters on every link in specific time intervals, such as every five minutes. To prevent overloading links and devices, TotalView executes the query in an efficient manner. Its heuristic engine interprets the error counters and generates a plain-English prescription of discovered problems, like:

> *"This interface has a duplex mismatch."*

Finally, to support VoIP systems, TotalView produces a layer-1, layer-2, and layer-3 path-map between all VoIP phones so that all the involved links, switches, and routers used by a VoIP

phone call through the network are mapped and that information is then mapped to the error counters. In addition, it is able to automatically analyze Class-based QoS queues to show how QoS queuing is working on critical MPLS links (with TotalView QueueVision). As the following figure shows, IT is able to resolve Dave's problem using TotalView.



TotalView displays how Dave's call traversed the network and what happened between the two phones, including historic usage and error information. Besides reporting what happened along the path between the two phones, TotalView's drill-down capabilities provide the root-cause plain-English answer for Dave within a minute:

> *"The VoIP phone call that you made 2 hours ago was poor because the Finance switch trunk port was dropping 6% of its packets due to a cabling fault."*

In this case, IT is finally able to identify where the problem occurred and why it happened. And although Dave's problem was intermittent, since TotalView is always on, the root-cause problem is fixed right away—no need to wait for the problem to reoccur.

Additional Resource:

Webinar: Troubleshooting VoIP Call Quality Problems, Quick & Dirty Secrets to Resolution

(877) 748-1777
Sales@PathSolutions.com
www.PathSolutions.com