IDG .com

NetworkWorld® Reprint

The leader in network knowledge ■ www.nwfusion.com March 28, 2005 ■ Volume 22, Number 12

CLEAR CHOICE TEST

VoIP analysis tools

Picking up VoIP-specific tools for the network management workbench

■ BY EDWIN MIER, DAVID MIER AND ROBERT TARPLEY, NETWORK WORLD LAB ALLIANCE

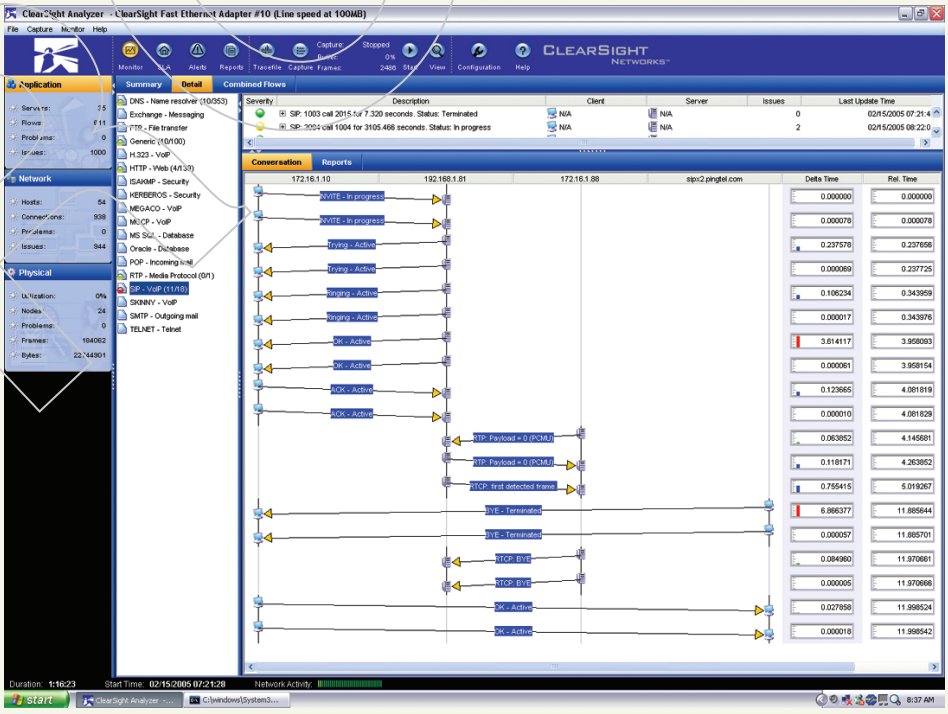
Some cavalierly refer to IP telephony as "just another application" that rides over your data network. But wait and see what happens if VoIP call quality starts eroding or, worse yet, if your organization's phone calls stop altogether.

In this Clear Choice Test, we evaluated a burgeoning class of new products, collectively called VoIP analysis tools. These wares help the VoIP network manager proactively monitor and troubleshoot the IP telephony environment to ensure call continuity.

Seven vendors accepted our invitation: Agilent Technologies, Brix Networks, ClearSight Networks, Fluke Networks, Touchstone Technologies, Viola Networks and WildPackets.

ClearSight's Analyzer garnered the Network World Clear Choice award for its extreme ease of use and its capability to analyze a range of VoIP protocols. Fluke's OptiView package made a strong second-place showing by capturing a substantial amount of information on the VoIP calls. However, it was a bit more tedious to use. There was a near-three-way tie for third place between Agilent, Touchstone and WildPackets, all of which provided much

VoIP SPECIAL REPORT



Driving ClearSight Networks' Analyzer: ClearSight gets high marks for its interface because all of its VoIP data and measurement can be accessed by applets from a single screen. VoIP streams are presented in log-type tables, with the ability to drill down for detail. A summary tab shows totals for bandwidth and flows and only a single click is needed to capture and playback any VoIP stream.

more complete analysis of VoIP traffic in the Session Initiation Protocol (SIP) environment than proprietary environments.

Protocols matter

We found — and users also need to keep in mind — that VoIP analysis tools are oriented toward particular VoIP protocol environments. Interpreting different call-control-protocol sequences is difficult because the messages vary considerably with the particular protocol used.

We tested each package in four different VoIP environments over a two-month period (see "How we did it," page 3). Using this methodology, we tested the packages against three proprietary protocols and with two SIP-based implementations.

The tools tested dramatically differ in their abilities to monitor and track SIP standards-based VoIP activity compared to how they work in proprietary protocol environments. Only two of the products, ClearSight's Analyzer and Fluke's OptiView package, did a good job tracking all VoIP activity in both standard-based SIP and proprietary-protocol VoIP environments.

But other products tested — such as Agilent's combination of Distributed Network Analyzer MX (DNA MX) probe and Telephony Network Analyzer (TNA) software and WildPackets' EtherPeek VX — still can view parts of VoIP phone traffic in different protocol environments. This is because actual VoIP conversations follow a fairly standard format across protocol environments. They comprise bidirectional Real-Time Transport Protocol (RTP) over User Datagram Protocol (UDP) streams, which are fairly easy to spot and decipher using tools that recognize RTP streams even if the IP PBX uses a proprietary signaling protocol.

Plugging in

The tools we tested mostly are specialty PC-based software applications. Many are add-ons to the vendors' network data analyzer, which provide the ability to recognize and process IP-telephony call control and VoIP conversations.

Long-time test-and-monitor vendor Agilent addresses VoIP monitoring through Real-Time Transport Control Protocol and RTP monitor applications that integrate with its popular Network Analyzer package. Its VoIP analysis package can be based on a laptop, run off a mirrored switch port or run on a probe appliance inserted in-line in key backbone network segments. We tested Agilent's 100M bit/sec capacity DNA MX probe that can fit with almost any network interface type, handle Gigabit links at wire speed and be accessed remotely from anywhere on the network. We ran the TNA software on a separate PC that communicated with the DNA MX over the network.

We ran ClearSight's software-only Analyzer on a Windows XP laptop. It sniffs passing traffic and captures all the packets traveling on the network, then analyzes them for VoIP traffic and associates the VoIP packets with the proper conversation. The network analyst's laptop usually is situated on a mirrored switch port to watch traffic that's copied and redirected from key traffic

Net Results

ClearSight Analyzer 4.0

OVERALL RATING **4.7**

Company: ClearSight Networks, www.clearsight.com. **Cost:** $8,000 for all software. **Pros:** Supports standard and proprietary VoIP call-control protocols; best layout and easiest to use; displays both overall VoIP bandwidth and specific call bandwidth; excellent RTP replay capability. **Con:** Summary stats of VoIP activity could be improved.

NetworkWorld CLEAR CHOICE

OptiView VoIP, Protocol Expert Plus and Link Analyzer 6.1

OVERALL RATING **3.9**

Company: Fluke Networks, www.flukenetworks.com. **Cost:** From $6,700 for software; $21,795 for Gigabit-capacity probe appliance. **Pros:** Supports many deployment topologies; effectively monitors proprietary VoIP protocols. **Cons:** Tedious interface; easy to confuse monitor and capture modes, which yield different stats.

EtherPeek VX 1.0

OVERALL RATING **3.65**

Company: WildPackets, www.wildpackets.com. **Cost:** $10,000 for software. **Pros:** Super peer map features shows all active VoIP connections; clear breakdown of active vs. closed VoIP calls. **Cons:** Sees only SIP and H.323-based VoIP activity; displays are generally clear but static, not customizable.

DNA MX and TNA software 4.5

OVERALL RATING **3.55**

Company: Agilent Technologies, www.agilent.com. **Cost:** $20,000 for central server; $7,700 for TNA software. **Pros:** Supports many LAN/WAN interfaces; scales well across multiple sites, distributed topologies. **Cons:** Hard to maneuver around main VoIP table; poor online help; hard to interpret date in some instances.

WinEyeQ 1.3.5

OVERALL RATING **3.4**

Company: Touchstone Technologies, www.touchstone-inc.com. **Cost:** From $6,500 for all software. **Pros:** Excellent alerting; easy to set up, use; VoIP screens are well organized. **Con:** Sees only SIP and H.323-based VoIP activity.

BrixMon 2.1

OVERALL RATING **2.7**

Company: Brix Networks, www.brixnet.com. **Cost:** $31,000 for central server package; $1,800 to $7,500 per probe/site. **Pros:** Best for long-term status monitoring in large networks; reports many telephony metrics that others don't. **Cons:** Most complex system to set up and tedious use; not oriented to assessing individual VoIP calls.

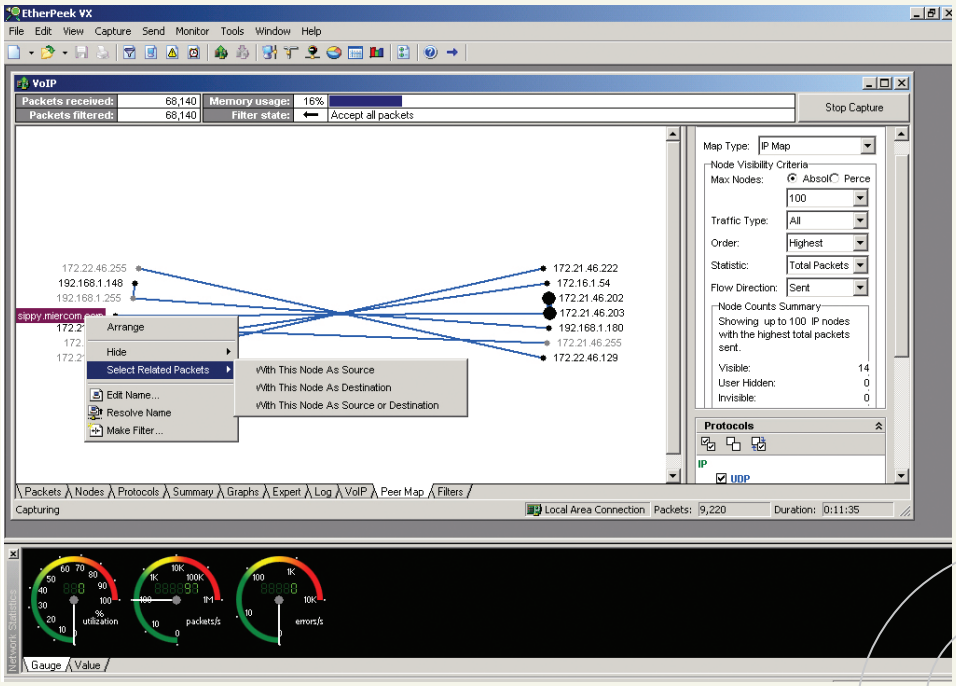
NetAlly RealTime and VoIP Assessment 4.0

OVERALL RATING **2.45**

Company: Viola Networks, www.violanetworks.com. **Cost:** $12,500 for base software with five agents. **Pros:** Special tool for Cisco VoIP reporting; very good for pre-VoIP deployment network analysis. **Con:** Doesn't monitor or assess real user VoIP traffic.

The breakdown	ClearSight Analyzer	Fluke OptiView VoIP, Protocol Expert Plus, and Link Analyzer	WildPackets EtherPeek VX	Agilent DNA MX and TNA	Touchstone WinEyeQ	Brix BrixMon	Viola NetAlly RealTime and VoIP assessment
Real-time VoIP monitoring 40%	5	4.5	3	3.5	3	2	1
Usability; data clarity, navigability 30%	5	3.5	4.5	3.5	4	3	3.5
Configuration and deployment 10%	4	4.5	4	4.5	4	2.5	4
Reporting (alerts, MOS) 10%	4	3	3.5	3.5	3.5	4	3
Special & unique features 10%	4	3	3.5	3	2.5	3.5	3
TOTAL SCORE	4.7	3.9	3.65	3.55	3.4	2.7	2.45

Scoring Key: **5:** Exceptional; **4:** Very good; **3:** Average; **2:** Below average; **1:** Consistently subpar



The window to WildPackets' EtherPeek VX VoIP Analysis: EtherPeek's interface does a great job distinguishing closed VoIP calls from active ones, which is useful in conducting diagnostics. WildPackets also serves up a peer-mapping feature, which is a dynamic representation of real-time flows and connections.

links.

Fluke's OptiView package can run on a PC or on a special probe designed for in-line insertion on a backbone link and is based on packet-sniffing data capture and analysis. We tested it with a Gigabit-capacity in-line probe that cost about $21,800. We also ran it on a Windows 2000 laptop via a mirrored switch port. The VoIP analysis software was the same in both configurations, but the separate-probe approach is better suited to multi-site distributed environments.

Another implementation based on packet sniffing is Touchstone's software-only product, WinEyeQ, which we ran on a Win 2000 PC as it watched passing traffic on a mirrored switch port. WinEyeQ seems to be more focused on VoIP traffic than its packet-sniffing competitors because all of the screens in Touchstone's product were specifically designed for VoIP analysis.

WildPackets' EtherPeek VX is also Windows-based software and is a packet-sniffing monitor tool, which we ran on a Win 2000 PC, on a mirrored-switch-port connection.

Brix's BrixMon relies on hardware probes called verifiers that generate simulated VoIP traffic based on canned tests that you can tailor to your network. This test traffic is sent between verifiers. Brix says the system can monitor and report on real VoIP traffic, but we found it difficult to get this feature to work properly in the different scenarios.

Viola's NetAlly is a software-only package that also issues simulated streams of VoIP traffic sent between its distributed PC clients.

With simulated traffic there is no direct observation or monitoring of real user's VoIP traffic, therefore both BrixMon and NetAlly are indifferent to VoIP protocols. This can be useful if you plan to use the tool in a pre-deployment phase of an IP PBX system to assess if the current network infrastructure can perform adequately for VoIP traffic. But then, when real VoIP traffic is implemented on the network, you don't get the same level of VoIP-level protocol detail and real traffic analysis that the other packages provide.

In this category, our top marks went to Agilent and Fluke in large part because of the additional deployment topologies and options they support. The BrixMon system was notably much more difficult to deploy and get working properly.

Real-time VoIP monitoring

Our test is weighted heavily toward how well these products assist the process of real-time VoIP monitoring. Our assessment is based on whether information could accurately be reported in the following areas:

- VoIP call control (that is, call initiation and setup signaling).
- Status of current VoIP calls.
- Details about current VoIP calls (caller destination, vocoder used, etc.).
- Bandwidth consumption by current VoIP calls.
- IP addresses of key VoIP nodes and endpoints (call controller, gateways, IP phones).
- Latency, jitter and packet loss, for VoIP calls between two distributed sites.

The tools that offer real-time information turned in the best results, by far, when monitoring SIP-based VoIP activity. WildPackets did the best job, in part, because of its slick, graphical, state-based, SIP call-progress display. ClearSight was a close second, offering the same amount of real-time information. However, it wasn't as easy to determine which calls were completed. Agilent, Fluke and Touchstone all did a fairly good job tracking SIP-based call control.

Viola offers little in terms of in real-time monitoring and analysis of SIP or proprietary VoIP environments. Brix generates simulated VoIP protocols streams, too, like Viola, but also can monitor user VoIP streams to some extent.

When you turn to tracking proprietary call-control environments, ClearSight was the hands-down winner. In addition to the half-dozen VoIP protocols it formally supports, ClearSight categorized calls based on other proprietary protocols as generic call control. Fluke, which we placed second in this regard, did a good job tracking the proprietary call-control protocols, which classified them as "unknown" call control. ClearSight displayed the key VoIP parameters on one screen, where Fluke required additional windows to view all the parameters associated with a VoIP call.

How about tracking and reporting of VoIP calls? In the SIP environment, WildPackets had the best showing because you can click on a VoIP call and bring up a well laid-out display window showing a jitter graph, the server name, the IP addresses or the

endpoints, and other call information. Agilent's tool set was also noteworthy. It displayed the VoIP calls on a tabular screen with the call information spread across the columns of the table.

Fluke and Touchstone reported similar information, but we felt it was more difficult to navigate the screens to view the data with these tools. ClearSight presented the VoIP statistics in a large table making it a bit tedious to find key VoIP parameters.

For call monitoring in proprietary-protocol environments, ClearSight and Fluke turned in good performances by still presenting all the VoIP call information. WildPackets and Agilent did an adequate job monitoring proprietary-protocol calls because of their general data-analysis capabilities, but none of the others could effectively display VoIP call information in proprietary environments.

The ability to report VoIP bandwidth consumption was also split along protocol lines. ClearSight did the best job accurately reporting VoIP bandwidth and other VoIP-activity details such as jitter, latency and packet loss in both the SIP and proprietary environments. Fluke was a close second here, effectively reporting VoIP details in all protocol environments but not as elegantly as ClearSight.

Based on SIP traffic only, Touchstone, Agilent and WildPackets all did an excellent job analyzing VoIP call control and reporting call performance statistics.

Across all protocols, Fluke did the best job monitoring and reporting key QoS conditions. ClearSight, Viola and Brix also did well monitoring QoS in all protocol environments, but there were some cases in which all information was not reported consistently. Brix and Viola reported QoS conditions based on their own generated traffic and were not sensitive to the actual VoIP control protocol used by the IP PBX.

In standard SIP-only environments, WildPackets and Fluke did the best job reporting network impairments and QoS-type conditions consistently and accurately. All other products displayed the QoS parameters, but, in some cases, the values were not reported consistently.

Clean and legible

It's not enough for a VoIP analysis tool to accurately track the information you seek, it must also let you readily locate the data, and view it in a clear, straightforward manner. In this critical area of usability and navigability, these products varied considerably.

ClearSight placed first. All its VoIP data and measurements come from applets launched from one screen. VoIP streams are shown in a log-type table. The user selects any one and drills down for more detail. The graphics are all clean and very legible. A summary tab shows totals for bandwidth and flows. There's a single click to capture and play back any VoIP stream.

WildPackets was close behind (see graphic, previous page). EtherPeek VX's interface does a great job distinguishing closed VoIP calls from active calls, which is useful in conducting diagnostics. It's easy to see who is on the phone in real time. Another WildPackets' plus is a very slick peer map feature, a dynamic, graphical representation of real-time flows and connections.

As long as you are working with either SIP or H. 323 protocol streams, Touchstone's interface is refreshingly simple to navigate. A single, well-organized VoIP screen provides seven tabs for individual applets. Everything is structured on a VoIP call-by-call basis; it is easy to capture, trace, record and delete calls.

Agilent's interface provides volumes of technical details, but finding only the data you want can be tedious. The main VoIP display is somewhat awkward to use, and on-screen help could be more, well, helpful.

Fluke's OptiView system can run in monitor or capture mode, and it's difficult to tell which is running at any time. However, the output is different depending on the mode and we found this a constant nuisance. Like Agilent, the wealth of captured data available to the user is impressive. It's just a little complex to find what you're after. The newer set of VoIP applications — including VoIP Properties, Call and Channel Details — are easier to use and navigate than the older data analyzer base of the system, such as Capture Views, Network Monitoring and

VoIP SPECIAL REPORT

How We Did It

Over a two-month period, the VoIP analysis tools were connected into our test bed made up of four IP PBX systems, which were:

- EADS Telecom's Nexspan L system, which uses a proprietary, stimulus-based VoIP call-control protocol.
- Mitel Networks' SX-200 ICP, which uses a proprietary message-based protocol called MINET for call control.
- NEC's Univerge 7000, which uses both a proprietary stimulus-based call-control protocol called PROTIMS and also supports Session Initiation Protocol-based endpoints via a separate SIP controller.
- PingTel's SIPxchange, which is based fully and exclusively on standard SIP VoIP call control.

The test bed was configured with two subnets simulating a headquarters and a branch location. The two subnets were interconnected using Cisco routers and Extreme Networks switches. The WAN connection was simulated using a Hurricane IP Network Emulator from PacketStorm Communications. The PacketStorm Emulator let us vary our network environment simulating various impairments including latency, jitter and packet loss.

A mirrored port was configured on the headquarter subnet for the VoIP analysis tools. Five of the seven tools were connected using this port, but the Brix and the Viola products had connections on both sides of our WAN. These two products can generate simulated traffic between their own endpoints to assess the performance of the connecting link.

We used more than eight IP phones to generate real VoIP call traffic between the headquarters and branch subnets. Additionally, some calls were made locally on only the headquarter subnet. Up to four separate VoIP phone calls were placed concurrently, as were conference calls. Before, during and after the calls, the VoIP tools were used to examine the characteristics of the call flows. We used the tools to display call initiation and setup, signaling and any performance statistics relating to the actual VoIP conversation itself.

Expert Views.

The interface and data displays for Viola's NetAlly — while limited to information collected in its simulated tests — are all clean and clear. Brix's package is focused on generating simulated VoIP streams as part of programmed tests, akin to Viola. The Brix user interface is consistent for the various tests, but it takes time to become familiar with the screen navigation techniques using hyperlinks and various buttons.

Reporting

Besides real-time VoIP monitoring, we set aside some test criteria to address any additional, useful reporting capabilities.

Included in this category is the ability to automatically assess the relative quality of selected VoIP calls. The products report VoIP call quality to varying degrees using a confusing mix of different metrics and scales. These range from widely recognized Mean Opinion Score equivalent ratings, which assign a value from 1 to 5, to new and more esoteric scales including Network R factor, E Model, per ITU G.107, and some proprietary methods.

We didn't intend to test which of these techniques is most accurate or best conveys relative VoIP call quality. What we did do is compare the call quality rating of VoIP calls with no impairments, with similar VoIP calls over a network with fairly major impairments. We found that in most cases, the call quality assessment was reduced, to an appropriate extent, by the added impairments.

All the ratings in this category were close with Brix and ClearSight at the higher end, and with Viola and Fluke at the lower end. Brix offers a number of unique telephony-oriented measurements among its test repertoire, such as post dial delay, which is the elapsed time after you dial, until the destination phone rings. ClearSight's package includes some canned, long-term trend reports, which would be useful in service level agreement-monitoring environments. Agilent's package can generate call detail records (CDR) on VoIP calls that it observes. Touchstone similarly can generate CDRs, while Viola says it can interrogate Cisco CallManager CDR records for VoIP call analysis.

Special features

Several of these products offer unique capabilities that the other portion of our methodology did not address.

ClearSight includes the ability to directly decode VoIP calls traversing Wi-Fi wireless networks. It also offers fairly comprehensive monitoring and analysis of video traffic. The ClearSight software can be set up to issue simulated call setup sequences to a VoIP call controller to monitor its uptime and availability. Brix and Viola also support similar call setup simulation and monitoring features.

WildPackets has a feature that lets the user vary network jitter in the playback of a VoIP call, to see the effect on call quality. Fluke offers the ability to deploy and centrally interrogate multiple distributed probes. And Touchstone has a special utility for analyzing VoIP-based DTMF tones, to aid analysis of interactive voice response systems.

In our overall assessment, we found considerable variety in capability and performance based on the VoIP call-control protocol environment. Until SIP emerges as the ubiquitous VoIP standard — and most agree that's likely over the next two years — users need to correctly mate tools such as these with their particular protocols, IP PBX systems and/or other major VoIP applications.

Edwin Mier is president of Miercom, a network-product test center based in East Windsor, N.J. Dave Mier is manager of lab testing, and Tarpley is senior lab tester at Miercom. They can be reached at ed@miercom.com, dmier@miercom.com or rtarpley@miercom.com, respectively.

NW Lab Alliance

Miercom also is a member of the Network World Lab Alliance, a cooperative of the premier testers in the network industry, each bringing to bear years of practical experience on every test. For more Lab Alliance information, including what it takes to become a partner, go to www.nwfusion.com/alliance.

ClearSight
Networks™