SteelCentral Packet Analyzer Plus

High-speed packet analysis software that works with SteelCentral AppResponse to diagnose problems fast

The Business Challenge

Having the right tool to continuously analyze terabytes of packet data traversing your enterprise network, and to quickly make sense of them is a critical step in network monitoring and troubleshooting. But you don’t want to transfer these large packet files across the network, and risk slowing down other important transactions and applications.

Instead, analyze the data where it is stored locally using special indexing that can help you drill down quickly to isolate a problem without wasting time. Having such a tool can streamline the process of diagnosing complex network issues in minutes, not hours or days.

SteelCentral Packet Analyzer Plus

Riverbed® SteelCentral™ Packet Analyzer Plus is a packet analysis and reporting solution that works with Riverbed® SteelCentral™ AppResponse network-based application performance management. It has an intuitive graphical user interface that streamlines packet analysis.

Simply drag and drop preconfigured “Views” onto a group of virtual interfaces (VIFGs) or a packet trace file, and see the results immediately.

By rapidly isolating the specific packets needed to diagnose and troubleshoot complex performance issues, you can quickly analyze multi-terabyte packet recordings on remote SteelCentral AppResponse appliances, a SteelCentral AppResponse Virtual Editions, or SteelCentral AppResponse Cloud without having to transfer large packet captures files across the network or cloud. SteelCentral Packet Analyzer Plus also fully, and seamlessly integrates with:

- Wireshark®, the leading open source protocol analyzer, for deep packet analysis and decoding.

- Riverbed® SteelCentral™ Transaction Analyzer, to facilitate the flow of network traffic data between the two products and streamline transaction troubleshooting help identify issues when millions of packets need to be analyzed. Then seamlessly analyze a particular transaction of interest via a simple right-click drill down from PA+ to TA.

These workflows allow you to get to the right level of detail needed to diagnose root cause of end-user, and transaction problems quickly and easily.
Key Benefits

- Speed and simplify problem identification using packet analysis
- Eliminate the need to transfer large trace files over the network
- Streamline diagnosis of remote problems without on-site assistance

Figure 1
This is an example of a series of “views” that have been dropped on a local trace file or packets on a SteelCentral AppResponse and the resulting analysis in SteelCentral Packet Analyzer Plus. Because of the smart indexing that occurs at the time the packets are captured, the analysis happens almost instantaneously.

Figure 2
The conversation ring shows traffic between two nodes and displays it as a bidirectional stream; users can select either direction or both for analysis.
Key Features

Drilldown for in-depth analysis
- Easily isolate traffic of interest using drag-and-drop multi-level drilldown and an extensive collection of network analysis views
- Display the details of any chart selection and quickly hone in on specific packets to isolate anomalous network behavior
- Microbursts can saturate a gigabit network and cause significant damage. Zoom into a 100 microsecond view of the network and identify these utilization spikes or “microbursts”.

Broad selection of views
- With an extensive number of network analysis views you’ll easily drill down and discover the root cause of any issue
- Views include: LAN and network, bandwidth usage, talkers and conversations, performance and errors, user activity, and more
- Conversation ring traffic between two nodes is displayed as a bidirectional stream; users can select either direction or both of them
- Enhanced view search with autofill

Time control
- Easily move through view metrics over extended periods of time with just a few mouse clicks using “back-in-time” functionality
- Enhance visual presentation with sub-sampling and data aggregation techniques

Automation
- Create triggers and alerts on virtually any view metric, such as high bandwidth, slow server response time, and high TCP round-trip time
- Actions executed include event logging, sending an email alert, and packet capture

Reporting
- Create professional reports directly from screen views in a variety of formats including PDF, Word, and Excel

Dynamic visualization
- Present information accurately with a complete collection of interactive charts
- Customize views or build new ones with the View Editor

Wireshark integration
- Use SteelCentral Packet Analyzer as a “searchlight” to help you identify issues buried within millions of packets. Once identified, you can choose to send the selected traffic to Wireshark directly for deeper individual packet inspection and decoding
- Take advantage of Wireshark capture and display filters and expansive dissector library for deep packet analysis through the “Send to Wireshark” button
- Supports both pcap and pcap-ng files (default format) for Wireshark nanosecond granularity

Remote management and control
- Configure remote SteelCentral AppResponse appliances for easy to manage branch office troubleshooting without having to send remote technicians offsite or to deploy additional hardware
- Packet Analyzer Plus uses the ViFG concept defined in AppResponse. ViFGs can monitor physical or VLAN interfaces
- Role-based access controls for remote capture files; users are now able to share a remote capture file with all the users belonging to the same role
Integration with Riverbed Products

SteelCentral Packet Analyzer Plus is integrated with all variations of SteelCentral AppResponse for easier, more efficient packet analysis. It also streamlines the transfer of packets between AppResponse and SteelCentral Transaction Analyzer. Use SteelCentral Packet Analyzer Plus as a searchlight to help you identify issues when millions of packets need to be analyzed. Then seamlessly analyze a particular transaction of interest via a simple right-click drill down from Packet Analyzer Plus to Transaction Analyzer.

System Requirements

SteelCentral Packet Analyzer Plus requires at a minimum the following:

<table>
<thead>
<tr>
<th>SteelCentral Packet Analyzer Plus</th>
<th>Operating Systems</th>
<th>Suggested Hardware Platform</th>
<th>Memory</th>
<th>Disk Space</th>
<th>Graphics Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Microsoft Windows 7 (SP1), Windows 8 or Windows 10*</td>
<td>A Dual-core 2.0 GHz CPU or better</td>
<td>2 GB or more of system memory</td>
<td>300 MB of disk space for a base installation; additional space is required to store generated reports or trace files</td>
<td>Graphics card with minimum resolution of 1024 x 768</td>
</tr>
</tbody>
</table>

*Also note: Local System Live Interfaces are not supported in Windows 10 currently.

Table 1: System requirement for running SteelCentral Packet Analyzer Plus.

Gartner Magic Quadrant Recognition

Riverbed is a five-time leader in the Gartner Network Performance Monitoring and Diagnostics (NPMD) magic quadrant.*

*Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.