



# Service Visibility Solution Suite

## Data Sheet



**NetSocket**  
Real-time IP Service Assurance

# Service Visibility Solution Suite

## Data Sheet

### Overview

---

NetSocket's patented Session2Topology™ correlation engine gives network operators in both Enterprise and Service Provider markets real-time visibility and understanding of the IP traffic carried through their network. NetSocket's first-ever, real-time IP service assurance solution correlates previously unrelated information from across multiple planes of information into a single, coherent form that is vastly more useful than data from the individual layers.

---

### Product components

NetSocket's Service Visibility Solution Suite has three associated components: the Service Visibility Manager (SVM), the Service Visibility Point (SVP), and an optional Service Visibility Analyzer (SVA).

The SVM is an element manager and contains a web server for GUI access to the system using industry-standard web browsers. It supports standard SNMP interfaces to the NMS/OSS layer for simple integration into existing operational architectures.

The SVP relies on patented Session2Topology correlation and service/session analysis technologies to provide

visibility into the IP network, giving enterprises the power to understand how sessions traverse their networks on a hop-by-hop basis. With this understanding, network operators can quickly identify and rectify issues, increase operational efficiency, and improve the end-user experience. The Session2Topology correlation engine provides an understanding of IP traffic dynamics that is invaluable and unprecedented for real-time monitoring, management, and control of the network.

The SVA processes RTP/RTCP packets to perform media analysis for voice and video services.

### Real-time visibility into end-user experience

The SVA collects and analyzes session media packets (i.e., RTP packets) to provide real-time visibility to the end user's quality of experience (e.g., MOS, R-factor, packet loss, jitter, delay, echo, signal-to-noise ratio, etc.) for the real-time IP services monitored. The SVA unobtrusively monitors the media packets via passive taps or span ports (port mirrors), and uses technology licensed from Telchemy, Inc. and Opticom, GmbH to perform the media packet analysis.

The SVP collects and automatically correlates both session and topology information to provide real-time visibility to the end-to-end session for the real-time IP

services monitored. The SVP unobtrusively learns network topologies and the status of available network resources by using standard IP routing protocols. It obtains session information by listening to control traffic or by interacting with application servers and session control nodes, and incorporates the media analysis performed by the SVA into this correlated view.

The process of collecting and correlating session data to the specific IP network path used through the network is called Session2Topology correlation. This correlation allows for instant identification of specific users impacted by any events in any part of the network.

The SVP analyzes the correlated control, media, and topology information to provide key performance indicators (KPIs) and key quality indicators (KQIs) through interactive dashboards and executive-level visualization

at the SVM to track, manage, and improve the end-user experience. These KPI/KQI are stored for up to 90 days on the SVP.

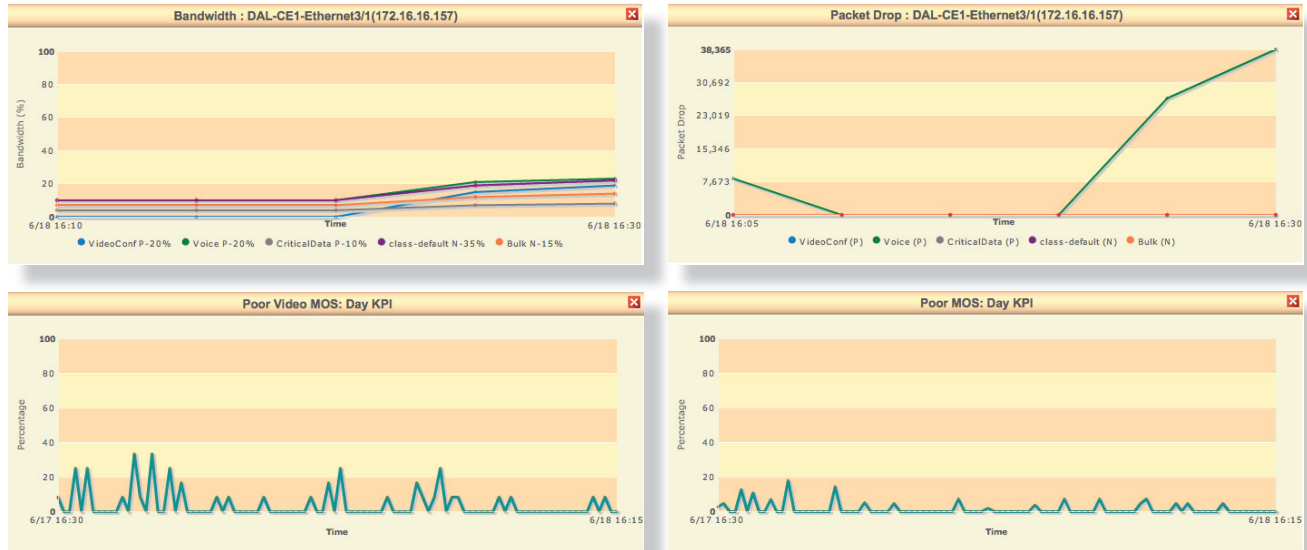


FIGURE 1: NETSOCKET SVP MANAGER – SAMPLE GRAPHS

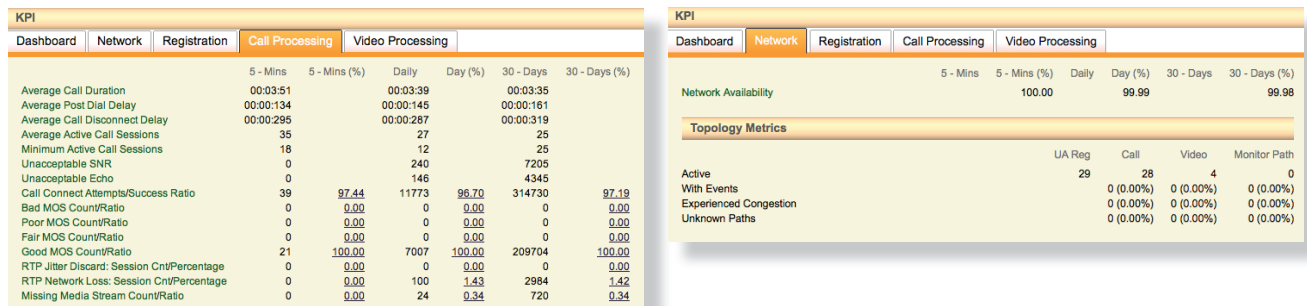


FIGURE 2: NETSOCKET SVP MANAGER – SAMPLE KPIS

In addition to numerous KPI/KQI metrics, the SVP automatically records and stores a “.pcap” file for every failed session. The benefit of this feature is that it avoids the need to deploy probes in various parts of the network, and collect session packets over a long period of time, after a customer incident. Instead of waiting for the problem to re-occur, which increases time and expenses, issue resolution can begin immediately.

For each session, Quality of Session Records (QSRs) detail the hop-by-hop IP network path along with any

changes to this path, any network events that have occurred along this path, and the associated end-user experience metrics (e.g., MOS, R-factor, packet loss, jitter, delay, echo, SNR, etc.). If session metrics deviate outside the expected range, the SVP notifies operations teams of potential problems or trends and provides a list of affected sessions. In other words, the operations team gets the information it needs to succeed—instantly, and all in one place.

Further, the SVM can be queried to reveal the specific user sessions traversing any link in the IP network. This is enabled by NetSocket's unique Session2Topology

correlation engine. An example of the query result is shown below.

**Topology Query Result**  
59 Records Found.

Table Options  
Result Graph

<< first < prev 1 2 3 next > last >>

From ID	To ID	Start Time Stamp	Duration	MOS	Termination Reason	pcap	RTP pcap	Congestion	Path Changes	Jitter Discard	Network Loss	SNR	Echo
2102743504@2.0.0.3	7133455205@4.0.0.3	JUL 26, 2011 4:05:06 PM	00:04:01	4.19/4	Normal	Y	Y	Y	N	0	267	33	None
2109875663@2.0.0.3	7133455204@4.0.0.3	JUL 26, 2011 4:05:05 PM	00:04:01	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
2108974624@2.0.0.3	7133455203@4.0.0.3	JUL 26, 2011 4:05:04 PM	00:04:01	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
2106486535@2.0.0.3	7133455202@4.0.0.3	JUL 26, 2011 4:05:04 PM	00:04:00	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
2105379654@2.0.0.3	7133455201@4.0.0.3	JUL 26, 2011 4:05:02 PM	00:04:01	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
5125873004@1.0.0.3	7133452010@3.0.0.3	JUL 26, 2011 4:04:12 PM	00:03:00	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
5125876872@1.0.0.3	7133452009@3.0.0.3	JUL 26, 2011 4:04:11 PM	00:03:00	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
5125878976@1.0.0.3	7133452008@3.0.0.3	JUL 26, 2011 4:04:10 PM	00:03:00	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
5125876586@1.0.0.3	7133452007@3.0.0.3	JUL 26, 2011 4:04:09 PM	00:03:00	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
5125876570@1.0.0.3	7133452006@3.0.0.3	JUL 26, 2011 4:04:08 PM	00:03:00	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
5125873484@1.0.0.3	7133452005@3.0.0.3	JUL 26, 2011 4:04:07 PM	00:03:00	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
5125878424@1.0.0.3	7133452004@3.0.0.3	JUL 26, 2011 4:04:06 PM	00:03:00	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
5125876542@1.0.0.3	7133452003@3.0.0.3	JUL 26, 2011 4:04:05 PM	00:03:00	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None
5125872567@1.0.0.3	7133452002@3.0.0.3	JUL 26, 2011 4:04:04 PM	00:03:00	4.19/4.13	Normal	Y	Y	Y	N	0	0	33	None

<< first < prev 1 2 3 next > last >>

FIGURE 3: NETSOCKET SVP MANAGER – SAMPLE TOPOLOGY QUERY & RESULT

Each session identified in the results window can be viewed to display the QSR for that session.

## Key Features

- Topology awareness: IPv4/v6, BGP, OSPF, IS-IS, EIGRP, Static routes, MPLS (LDP and RSVP-TE), BGP VPNs
- Control plane: SIP, H.323, UNISStim (Nortel/Avaya)
- Media plane: RTP/RTCP
- Configurable thresholds for VoIP and Video (desktop, conferencing, telepresence) metrics
- Presentation:
  - SNMP v1/v2c
  - Web-based GUI and CLI
  - Interactive topology map showing complete network monitored, network events, paths of sessions across the network; queries can be executed directly from within map
  - Graphical and tabular session performance and quality reports clearly identifying users/services impacted and root cause network events for specific time periods, or specific network locations, or specific users
- Color-coded icons to display service status
- Detailed alerts for any service-impacting event
- Automatic “.pcap” file capture for viewing in Wireshark™ and other standard tools
- Quality of Session Report (QSR) capturing all session information
- “Rewind the network” to know exact state of network at time of event – for up to 30 days
- Custom Key Performance/Quality Indicator (KPI/KQI) reports
- Offload of KPI/KQI reports on schedule or on-demand
- Threshold-driven alarms sent to NMS/OSS via SNMP; up to 4 thresholds per KPI

## Platform

The software platform includes a highly available Unix operating system and a full-featured, Tier-1 carrier-vetted routing protocol suite. The base hardware platform used is a commercial, off-the-shelf appliance with dual Intel

processors, CD R-RW/DVD ROM, four (4) 300 GB SAS HDD in RAID-10 configuration, multiple 1G or 10G port options, 12 GB of RAM, and both AC and DC power options.