Overview

GL’s Network Surveillance System is based on a scalable and flexible architecture and is used in conjunction with GL’s Protocol Analyzer probes to non-intrusively monitor from one or many testing locations.

The NetSurveyorWeb™ client application remotely or locally facilitates to view database using a simple web browser application. It includes database to store real-time and/or historic data.

GL’s NetSurveyorWeb™ (PKV170), is a web-based client that facilitates display of call data records and call summary using a web interface by connecting to T1 E1 / T3 E3 / OC-3 STM-1/ OC-12 STM-4 / IP probes through a web server for monitoring physical layer, signaling, and traffic. Supported protocols include SIP, SS7, ISDN, VoIP (SIGTRAN, SIP, H.323), GSM, GSM A, TRAU, MAP, IuCS, CAMEL, IuPS, and LTE.


Main Features

Web Based UI

- Access real-time and historic data remotely via browser based clients.
- Interfaces with Oracle database.
- Web administration features to monitor the connected probe status, database loader status, alarms, and perform database maintenance
- Multi-user support.
- Modular and distributed architecture is capable of theoretically ‘infinite capacity’.

(contd...)
Main Features (Contd...)  

Call Detail Records
- Ability to customize column views with sorting capabilities for call detail records.
- Easy navigation of records to display Previous or Next Hour, Day, Month, Year through navigation tool.
- Ability to export the call detail records displayed based on time filter or record index as PDF and CSV.
- Ability to play voice files for GSM and TRAU protocols.
- Decode SMS in different languages for GSM CDRs.
- Provides options to view CDR, Ladder Diagram, and Protocol Decodes of a selected frame in a single view.

Filter & Search Calls of Interest
- Drill-down to calls of interest with filter and/or search options.
- Customize Filters (Date, Time, and other call control parameters).
- Apply single or multiple filters for data analysis; use logical operators between filters.

Key Performance Indicators (KPI’s)
- Voice Quality (MOS, R-Factor)
- Signal level, Nosie Level, and Echo.
- Delay Measurements (RTD, OWPD).
- Signaling Messages and Traffic Types.
- Call Duration and Call Volume.
- Call Status (Completed, Busy, Success, Failure).

Physical Layer Monitoring
- Physical Layer Alarms (Link Status, Carries Loss, Sync Loss, ...).
- Automatically alert users when “Calls of Interest” occur.
- Set alarm conditions and generate alerts of different types like email alert, visual alert, audible alert, or even log into tables for future analysis.
- Provides database query methods to gather status, statistics, events, and results.

Alerts and Indicators
- Automatically alert users when “Calls of Interest” occur.
- Set alarm conditions and generate alerts of different types like email alert, visual alert, audible alert, or even log into tables for future analysis.
- Provides database query methods to gather status, statistics, events, and results.

Typical Applications
- Comprehensive analysis from overall network health to detailed protocol monitoring.
- Call Detail Records, fraud detection and location, remote protocol analysis and troubleshooting, real-time signaling monitor, traffic optimization engineering, and statistics.
- Determine actual call signaling routes to verify network functionality under all situations including congestion and loss of SS7 nodes.
- Revenue and billing verification, alarm monitoring, intrusive testing.
- Quality of service measurements, call trace and recording.

System Architecture
GL’s NetSurveyorWeb™ has a three tier architecture. The first layer consists of GL’s Protocol Analyzer Probes which are capable of tapping into live call traffic and non-intrusively capture signaling message summary and build CDRs. The second layer is the Data Layer where the captured data is stored into a database. This layer consists of a listener, and a SQL DBMS (such as Oracle) components. Listener will listen to the connected probes, receives data, and feeds the data to DB. The last layer is the Data Access Layer controlled by Web Server and Client application where the data presentation logic is contained.

Users can log into the central system locally or remotely to view the collected real-time and historic data including call parameters, layer 1 status display, as well as layer 2 and 3 analysis. Also available is the ability to filter the call records using a variety of filtering mechanisms including time/date, signalling and traffic parameters.

Figure: System Architecture
Quick View CDR
Quick View CDR is a combination of Custom Filters and Column View, user can create their own Quick View groups and add the required columns in the created group to be displayed on the Data View. Default Quick CDR View is provided for all the protocols such as All Calls, Failed Calls, Passed Calls, VoLTE Enabled Calls, CS Fallback, Poor LMOS, Good LMOS, Longer Duration Calls, and more.

Multi-protocol call flow
This feature is useful in testing interoperability of different types of networks, say for example SIP-to-SS7. The Multi-protocol Call Flow provides the flow of messages exchanged between different nodes in the form of a ladder diagram along with the ability to display respective signalling decodes, thus providing visibility into complete end-to-end call flow.

Figure: Ladder Diagram and Protocol Decodes
**Alarm Settings**

Trigger alarms and alerts whenever calls-of-interest occur, a network link failure is detected, or regularly at scheduled intervals. Directly access the pre-configured filter profiles or the KPI profiles to trigger alarms and alerts either when the custom filters conditions are passed, or send the pre-defined KPI report hourly, daily, monthly or yearly. Alert actions can be defined based on the output of the alarm conditions such as like email alert, visual alert, audible alert, SMS alerts, exporting data, setting alarm severity, or even log into tables for future analysis. Alarm Severity type can be set as Minor, Major, or Critical.

Flexible options are provided to save alarm filters as profiles, add, edit or delete the existing alarms, selection of user KPIs, and selection of Custom filters. Schedule alarms and alerts for hourly, daily, monthly, or yearly.

**Graphs & Reports**

Report provide an overall summary of the captured signaling, and traffic over the entire network with the help of useful graphs. Graphs are available in the form of Bar Graph, Pie Chart, Dot Graph, along with the data in tabular format for each of the plotted graph. Reports can be generated for all calls or filtered records only.

**Report Configuration**

NetSurveyorWeb™ allows users to add new KPIs and customize the reports based on SQL Queries using Report Configuration feature. The Add / Import KPI feature allows user to Add / Import the required KPI to the existing KPI group. This will avoid the user from creating the new KPI if it is readily available. Also, with the add option, the KPI profiles will be automatically updates whenever the user who created this KPI does any modification. The import option will give full permission to the user to edit the KPIs as required.

---

![Alarm Settings and Email Alerts](image1)

![Report Configuration](image2)

---

**Figure: Alarm Settings and Email Alerts**

**Figure: Report Configuration**
### Supported KPIs

<table>
<thead>
<tr>
<th>Protocol Type</th>
<th>Basic KPIs</th>
</tr>
</thead>
</table>
| **VoIP SIP** (SIP and H.323) | • Answer Call  
• Call Duration  
• Listening MOS  
• Conversational MOS  
• Session Request Delay (Successful Calls)  
• Session Request Delay (Unsuccessful Calls)  
• Session Disconnect Delay  
• Failure Cause  
• Average Packet Loss |
| **SS7** | • Call Completion  
• Disposition Count  
• Billing Duration  
• Message Counters  
• Link_MessageCounters |
| **T1E1 Layer 1** | • T1E1 Events |
| **ISDN** | • Call Completion  
• Call Types |
| **GSM** | • Mapped Vs UnMapped  
• SMS  
• Top 5 SMS  
• Total CDRs on different links  
• Total SMS on different links |
| **GSM A** | • Answer Call  
• Call Duration  
• Listening MOS  
• Conversational MOS  
• Failure Cause  
• Average Packet Loss % |
| **TRAU** | • Call Duration |
| **IuCS** | • Answer Call  
• Call Duration  
• Listening MOS  
• Conversational MOS  
• Failure Cause  
• Average Packet Loss |
| **IuPS** | • Answer Call  
• Call Duration  
• Failure Cause  
• Session Request Delay (Successful Calls)  
• Session Request Delay (Unsuccessful Calls)  
• Session Disconnect Delay |
| **VoIP SIGTRAN** | • Call Types  
• Billing Duration  
• Message Counters |

### Buyers Guide

**XX170** – Network Surveillance Software with Centralized Database Engine and Client

**PKV175** – T1 E1 Physical Line Monitoring Option for Network Surveillance - requires PKV170

**PKV172** – ISDN Call Detail Record (CDR) Option for Network Surveillance - requires PKV170. requires OLV100 at the central site.

**PKV092** – CAS Call Detail Records (CDR) Option for Network Surveillance. requires OLV092 at the central site.

**PKV173** – SS7/SIGTRAN Call Detail Record (CDR) Option for Network Surveillance - requires OLV120 for SS7 and PKV106 for SIGTRAN at the central site.

**PKV174** – GSM (TDM or IP) & TRAU Call Detail Record (CDR) Option for Network Surveillance - requires OLV150 for GSM and OLV153 for TRAU at the central site.

**PKV176** – VoIP (SIP, MGCP, Megaco etc.) Call Detail Record (CDR) Option for Network Surveillance - requires PKV101 at the central site.

### Related Software

- **PKV169** – Network Surveillance Lite Software.
- **PKV171** – Network Surveillance Agent Toolkit

### Related Hardware

- **PTE001** – tProbe™ Dual T1 E1 Laptop Analyzer
- **XTE001** – Dual T1 E1 Express (PCIe) Boards
- **TTE001** – tScan16™ T1 E1 Boards
- **FTE001** – QuadXpress T1E1 Main Board
- **ETE001** – OctalXpress T1E1 Main Board plus Daughter Board
- **UTE001** – Portable USB based Dual T1 E1 Laptop Analyzer
- **HTE001** – Universal HD T1 E1 PCI Cards