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.

GL’s NetSurveyorWeb™ (PKV170), 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 currently supported protocols include 5G, 4G (LTE, IMS, Diameter), 3G UMTS (IuCS, IuPS), 2G (GSM, TRAU, MAP, CAMEL), VoIP (SIP, ED-137, SIGTRAN, H.323, MEGACO, MGCP), TDM (SS7, ISDN, CAS, GSM, TRAU) and Analog systems.

The central system comprises of a database engine, web server, and NetSurveyorWeb™ (PKV170), a web-based application, to facilitate data storage and retrieval through web browser clients. 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.

This surveillance system requires TDM and IP protocol analysis probes deployed at various physical locations. These probes can capture the data at high speed, store locally decode, and segregate the traffic to calls and forwards the CDRs, signaling frame details, and other statistics to the centralized database server.

GL also offers NetSurveyorWeb™ Lite (PKV169) a cost effective, simple plug and play connection, which is an integrated and simplified web-based system that is distributed at probe level.

For more information, please visit NetSurveyorWeb™ webpage.

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
Applications (Contd.)

- 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

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'

Call Detail Records

- Ability to customize column views with sorting capabilities for call detail records
- Provides End-to-End Call Flow analysis
- 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 formats
- Provides option to send the exported call flow or reports to the specified email address
- Ability to play voice files for the recorded calls
- Download the selected Call Trace in *.hdl and *.pcap formats
- 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 and 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)
- Voice Analysis (VBA)
- Signal level, Nosie Level, and Echo
- Delay Measurements (RTD, OWD)
- 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, and so on)
- Automatically alert users when “Calls of Interest” occur
- Set alarm conditions and generate alerts of different types such as 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
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, signaling and traffic parameters.

![System Architecture Diagram]

Figure: System Architecture
The real-time data view provides visibility into each individual call. Each call can be investigated based on call control, signaling and traffic parameters. Flexible filtering can help you organize and identify “Calls of Interest”. The CDR view includes:

**Frame Summary**
Frame summary view provides summary of signaling data along with the decodes in the form of Hexdump.

**Traffic Summary**
This option is currently available only for IP calls. Each call can be expanded to reveal per stream RTP statistics. The RTP/audio parameters such as payload type, total packet count, missing / duplicate / reordered / discarded packet count or %, MOS/R-Factor, cumulative packet loss, delay, and jitter values are displayed.

**Graph View for each call**
This call flow graph allows easy verification of the messages exchanged and the status of the call.

Users can also select any messages and observe the corresponding decode message details in the decode view.

**Merge View**
This feature display Ladder diagram and Decodes of the selected message in a single view. Hide/Show any of these views in order to easily view the information properly.

**Navigation and Search Tools**
Navigate through records easily using Previous and Next Hour, Day, Month, and Year options as required. A particular call of interest can be searched using one or more parameters in the Quick Search option.

**Whitelist**
User can configure the list of interested calling/called number to mark them as Whitelist and perform the action such as saving the trace file on the probe. This information is sent to the database and can view the Whitelisted calls separately in the NetSurveyorWeb™ and also download the trace file in *.hdl format.
Call Data Records (CDR) View (Contd.)

Quick View CDR

Quick CDR View 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 inter-operability 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 signaling decodes, thus providing visibility into complete end-to-end call flow.
Call Flow

The call flow provides visibility into each individual call. The call flow is depicted through graphical and tabular view which allows verification of the status and the messages exchanged in a call between the Called and the Calling numbers.

Selected Call Trace Download

The user can download the selected call trace in the *.hdl and *.pcap formats.
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.

**Figure: Alarm Settings and Email Alerts**
Graphs and 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.

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 |
| T1 E1 Layer 1 | • T1 E1 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 |
# Buyer’s Guide

<table>
<thead>
<tr>
<th>Item No</th>
<th>Product Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XX170</td>
<td>Network Surveillance Software with Centralized Database Engine and Client</td>
</tr>
<tr>
<td>PKV175</td>
<td>T1 E1 Physical Line Monitoring Option for Network Surveillance - requires PKV170</td>
</tr>
<tr>
<td>PKV172</td>
<td>ISDN Call Detail Record (CDR) Option for Network Surveillance - requires PKV170. requires OLV100 at the central site.</td>
</tr>
<tr>
<td>PKV092</td>
<td>CAS Call Detail Records (CDR) Option for Network Surveillance. requires OLV092 at the central site.</td>
</tr>
<tr>
<td>PKV173</td>
<td>SS7/SIGTRAN Call Detail Record (CDR) Option for Network Surveillance - requires OLV120 for SS7 and PKV106 for SIGTRAN at the central site.</td>
</tr>
<tr>
<td>PKV174</td>
<td>GSM (TDM or IP) and TRAU Call Detail Record (CDR) Option for Network Surveillance - requires OLV150 for GSM and OLV153 for TRAU at the central site.</td>
</tr>
<tr>
<td>PKV176</td>
<td>VoIP (SIP, MGCP, MEGACO etc.) Call Detail Record (CDR) Option for Network Surveillance - requires PKV101 at the central site.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item No</th>
<th>Related Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKV169</td>
<td>Network Surveillance Lite Software.</td>
</tr>
<tr>
<td>PKV171</td>
<td>Network Surveillance Agent Toolkit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item No</th>
<th>Related Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTE001</td>
<td>tProbe™ Dual T1 E1 Laptop Analyzer</td>
</tr>
<tr>
<td>XTE001</td>
<td>Dual T1 E1 Express (PCIe) Boards</td>
</tr>
<tr>
<td>TTE001</td>
<td>tScan16™ T1 E1 Boards</td>
</tr>
<tr>
<td>FTE001</td>
<td>QuadXpress T1 E1 Main Board</td>
</tr>
<tr>
<td>ETE001</td>
<td>OctalXpress T1 E1 Main Board plus Daughter Board</td>
</tr>
</tbody>
</table>

For more information, please visit [NetSurveyorWeb™](http://www.gl.com) webpage.