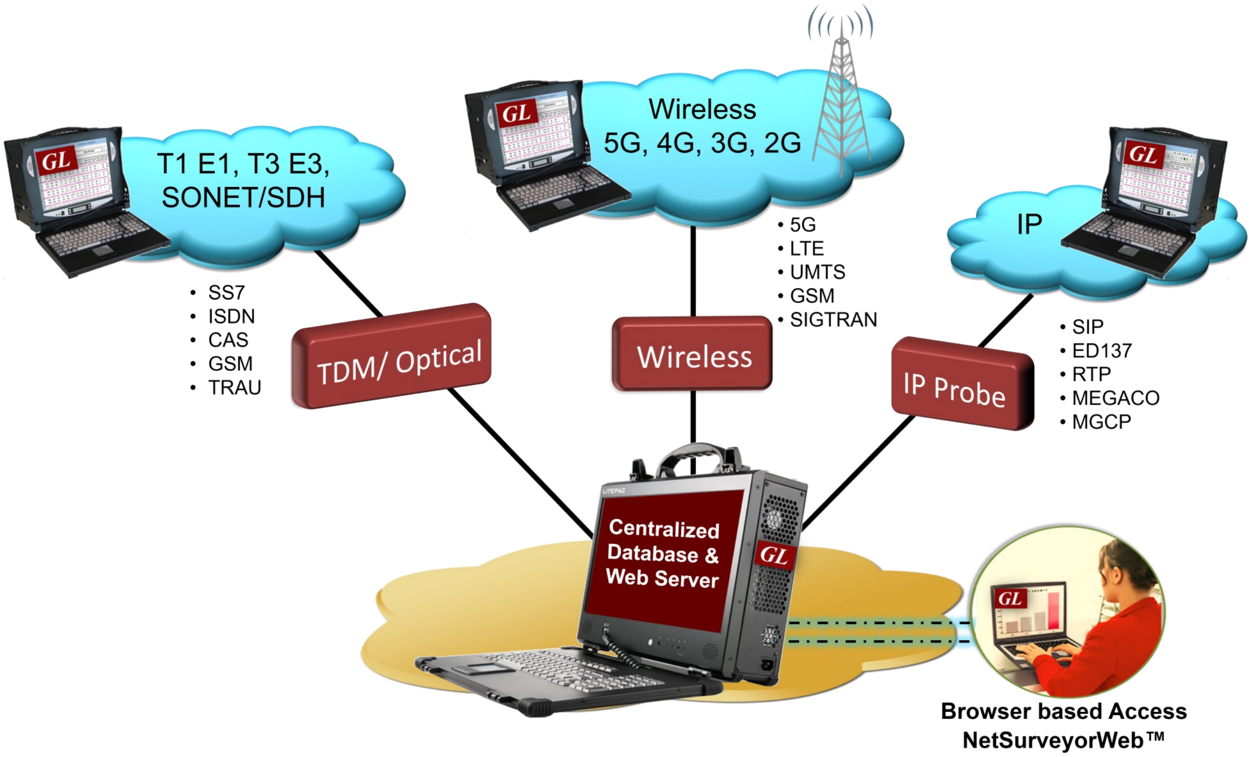
NetSurveyorWeb™

(Centralized network surveillance system for TDM / Wireless/ IP Networks)



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)**, 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 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.

The system relies on protocol analysis probes placed at different physical sites. These probes capture, decode and organize traffic into calls, sending CDRs, signaling frame details, and other statistics to the central database server. The probes capture data locally on high-speed networks and come equipped with protocol analysis software for convenient field analysis. The probes can be customized to capture legacy interfaces (T1, E1, Analog) or Ethernet and SONET / SDH networks.

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.

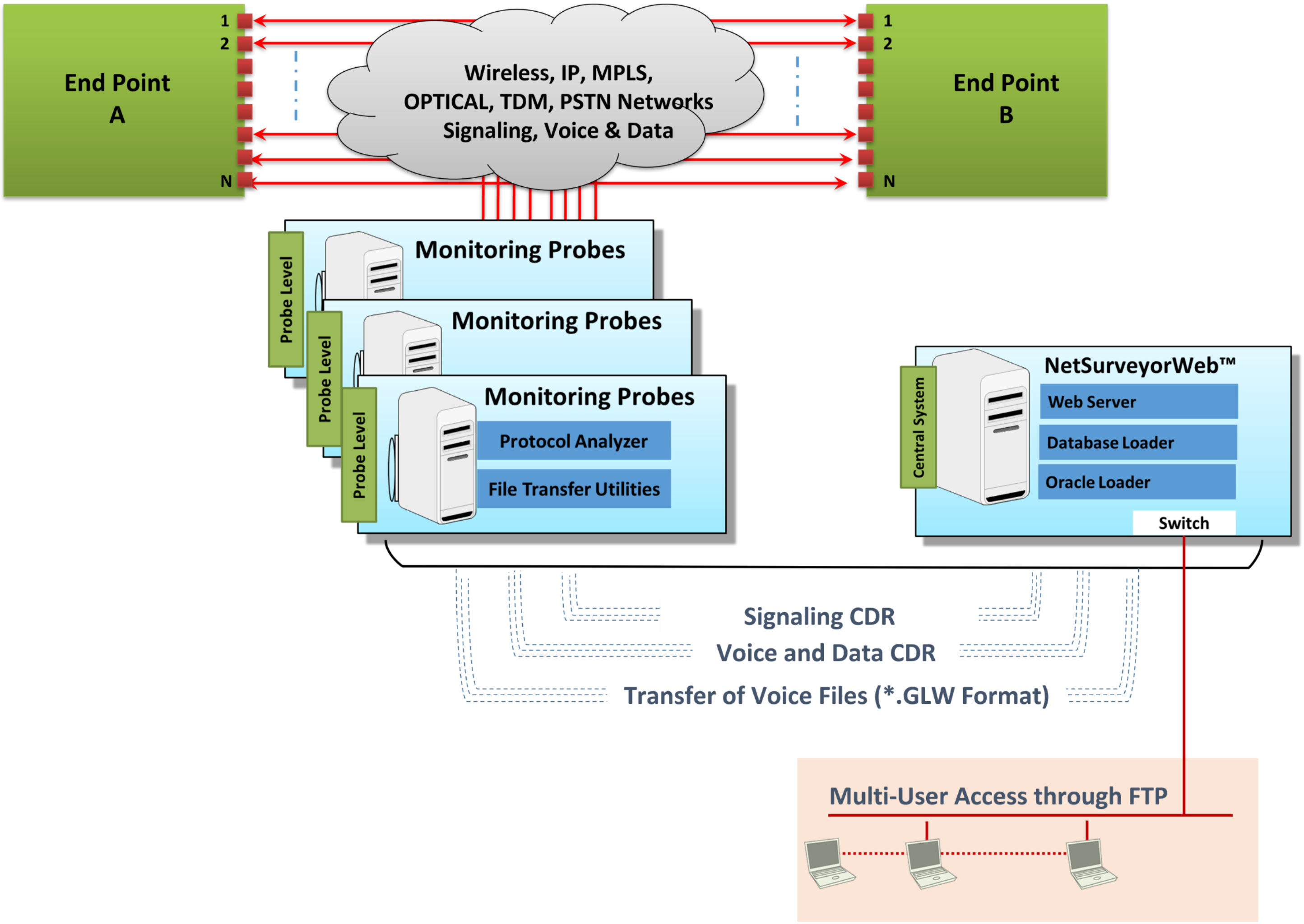
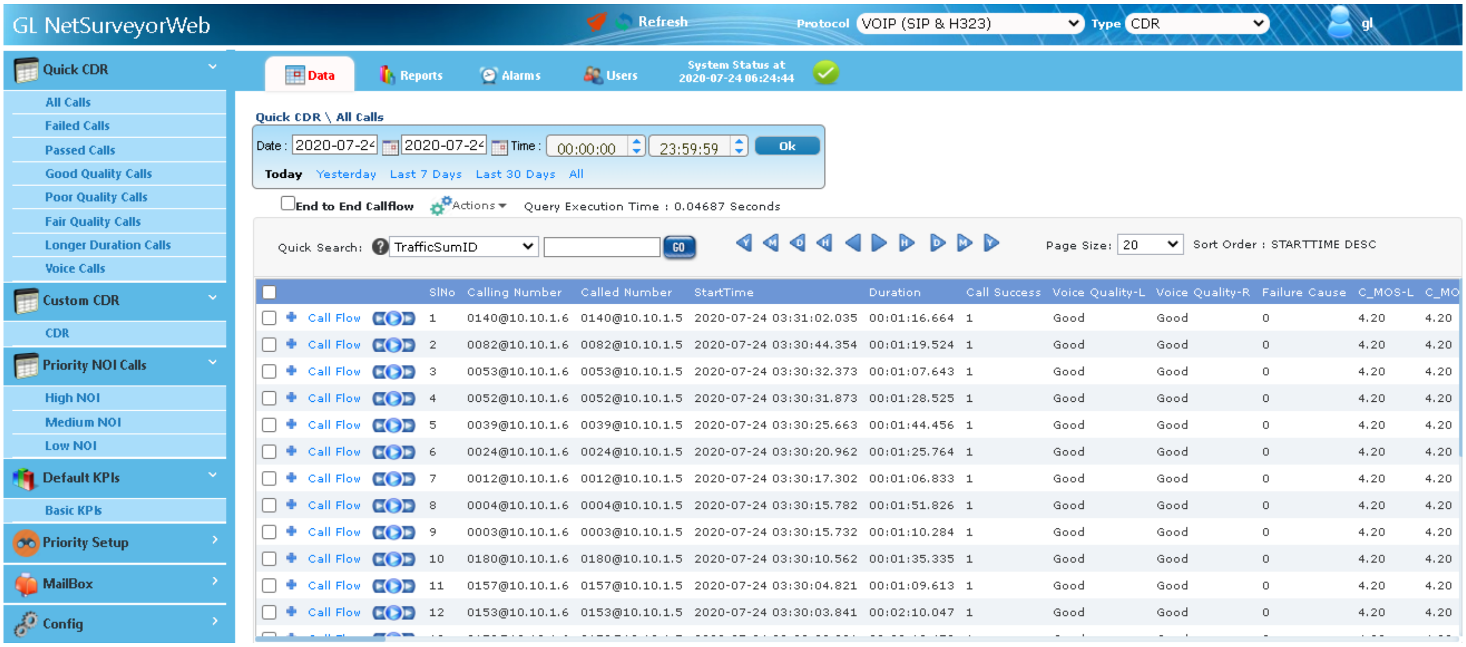


Figure: System Architecture

Call Data Records (CDR) View



Protocol VOIP (SIP & H323) Type CDR

System Status at 2020-07-24 06:24:44

Quick CDR \ All Calls

Date : 2020-07-24 2020-07-24 Time : 00:00:00 23:59:59

□ End to End Callflow Query Execution Time : 0.04687 Seconds

Quick Search: TrafficSumID Page Size: 20 Sort Order : STARTTIME DESC

□		SlNo	Calling Number	Called Number	StartTime	Duration	Call Success	Voice Quality-L	Voice Quality-R	Failure Cause	C_MOS-L	C_MO
□	Call Flow	1	0140@10.10.1.6	0140@10.10.1.5	2020-07-24 03:31:02.035	00:01:16.664	1	Good	Good	0	4.20	4.20
□	Call Flow	2	0082@10.10.1.6	0082@10.10.1.5	2020-07-24 03:30:44.354	00:01:19.524	1	Good	Good	0	4.20	4.20
□	Call Flow	3	0053@10.10.1.6	0053@10.10.1.5	2020-07-24 03:30:32.373	00:01:07.643	1	Good	Good	0	4.20	4.20
□	Call Flow	4	0052@10.10.1.6	0052@10.10.1.5	2020-07-24 03:30:31.873	00:01:28.525	1	Good	Good	0	4.20	4.20
□	Call Flow	5	0039@10.10.1.6	0039@10.10.1.5	2020-07-24 03:30:25.663	00:01:44.456	1	Good	Good	0	4.20	4.20
□	Call Flow	6	0024@10.10.1.6	0024@10.10.1.5	2020-07-24 03:30:20.962	00:01:25.764	1	Good	Good	0	4.20	4.20
□	Call Flow	7	0012@10.10.1.6	0012@10.10.1.5	2020-07-24 03:30:17.302	00:01:06.833	1	Good	Good	0	4.20	4.20
□	Call Flow	8	0004@10.10.1.6	0004@10.10.1.5	2020-07-24 03:30:15.782	00:01:51.826	1	Good	Good	0	4.20	4.20
□	Call Flow	9	0003@10.10.1.6	0003@10.10.1.5	2020-07-24 03:30:15.732	00:01:10.284	1	Good	Good	0	4.20	4.20
□	Call Flow	10	0180@10.10.1.6	0180@10.10.1.5	2020-07-24 03:30:10.562	00:01:35.335	1	Good	Good	0	4.20	4.20
□	Call Flow	11	0157@10.10.1.6	0157@10.10.1.5	2020-07-24 03:30:04.821	00:01:09.613	1	Good	Good	0	4.20	4.20
□	Call Flow	12	0153@10.10.1.6	0153@10.10.1.5	2020-07-24 03:30:03.841	00:02:10.047	1	Good	Good	0	4.20	4.20

Figure: Call Detail Records View

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

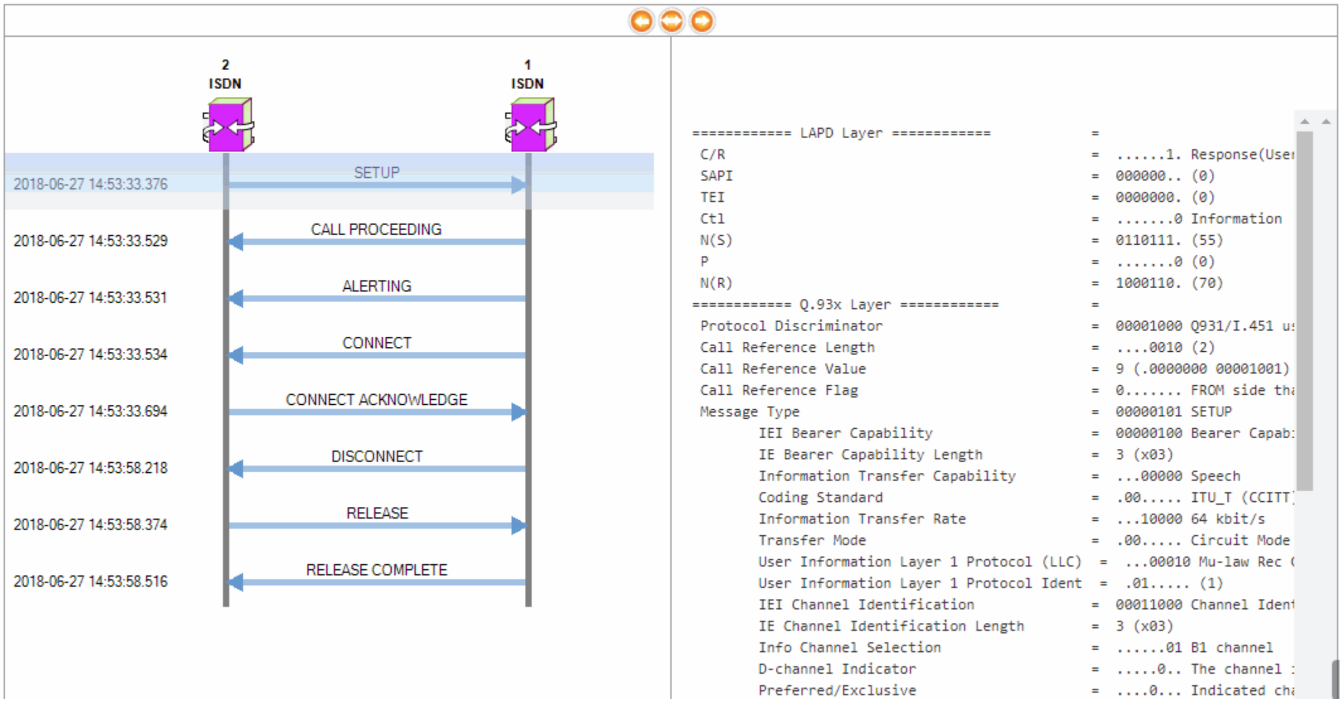
Quick CDR View is a combination of Custom Filters and Column View, user can create their own Quick View groups and add the required columns in the created group to be displayed on the Data View. Default Quick CDR View is provided for all the protocols such as All Calls, Failed Calls, Passed Calls, VoLTE 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.

End-to-End Call Flow

The stitched CDR data enables users to perform end-to-end analysis of communication sessions traversing the network. This analysis tracks the complete call flow, from its origination point to the destination, including any intermediate network devices along the path.



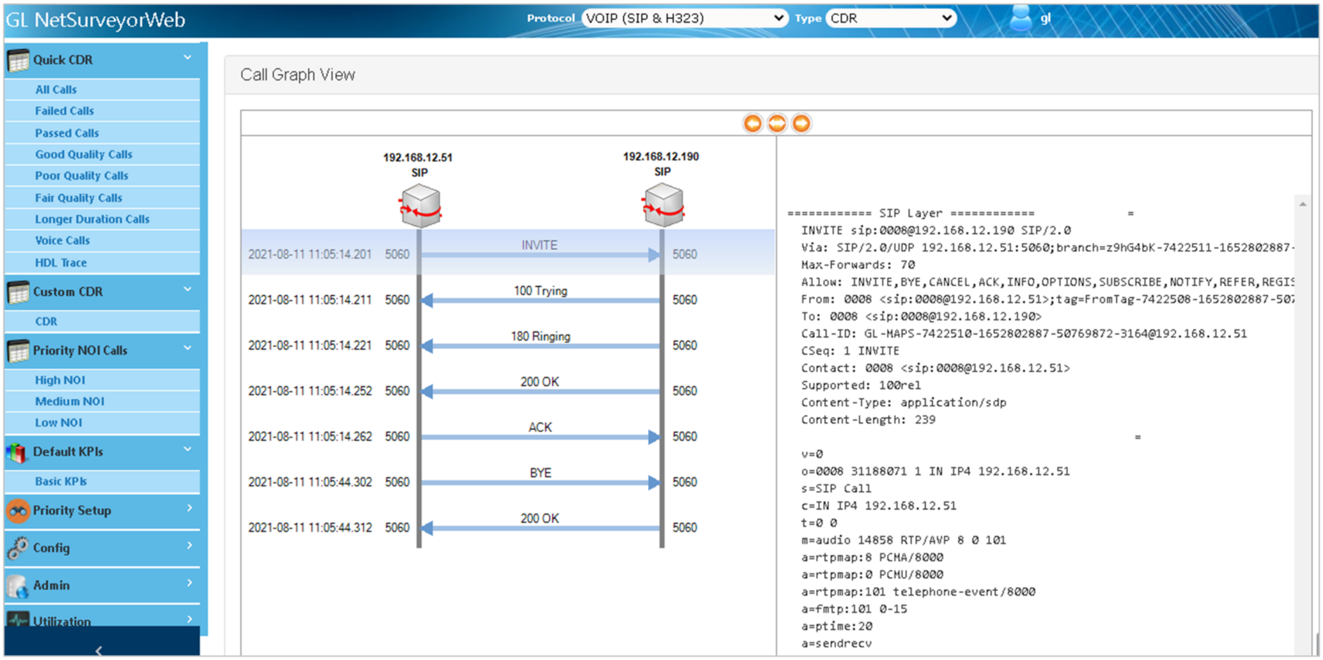
```
2018-06-27 14:53:33.376   SETUP
2018-06-27 14:53:33.529   CALL PROCEEDING
2018-06-27 14:53:33.531   ALERTING
2018-06-27 14:53:33.534   CONNECT
2018-06-27 14:53:33.694   CONNECT ACKNOWLEDGE
2018-06-27 14:53:58.218   DISCONNECT
2018-06-27 14:53:58.374   RELEASE
2018-06-27 14:53:58.516   RELEASE COMPLETE
```

```
============ LAPD Layer ============               =
 C/R                                              =  ......1. Response(User
 SAPI                                             =  000000.. (0)
 TEI                                              =  0000000. (0)
 Ctl                                              =  .......0 Information
 N(S)                                             =  0110111. (55)
 P                                                =  .......0 (0)
 N(R)                                             =  1000110. (70)
============ Q.93x Layer ============              =
 Protocol Discriminator                           =  00001000 Q931/I.451 us
 Call Reference Length                            =  ....0010 (2)
 Call Reference Value                             =  9 (.0000000 00001001)
 Call Reference Flag                              =  0....... FROM side tha
 Message Type                                     =  00000101 SETUP
        IEI Bearer Capability                     =  00000100 Bearer Capab:
        IE Bearer Capability Length               =  3 (x03)
        Information Transfer Capability           =  ...00000 Speech
        Coding Standard                           =  .00..... ITU_T (CCITT)
        Information Transfer Rate                 =  ...10000 64 kbit/s
        Transfer Mode                             =  .00..... Circuit Mode
        User Information Layer 1 Protocol (LLC)   =  ...00010 Mu-law Rec (
        User Information Layer 1 Protocol Ident   =  .01..... (1)
        IEI Channel Identification                =  00011000 Channel Ident
        IE Channel Identification Length          =  3 (x03)
        Info Channel Selection                    =  ......01 B1 channel
        D-channel Indicator                       =  .....0.. The channel :
        Preferred/Exclusive                       =  ....0... Indicated cha
```

Figure: Ladder Diagram and Protocol Decodes

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.



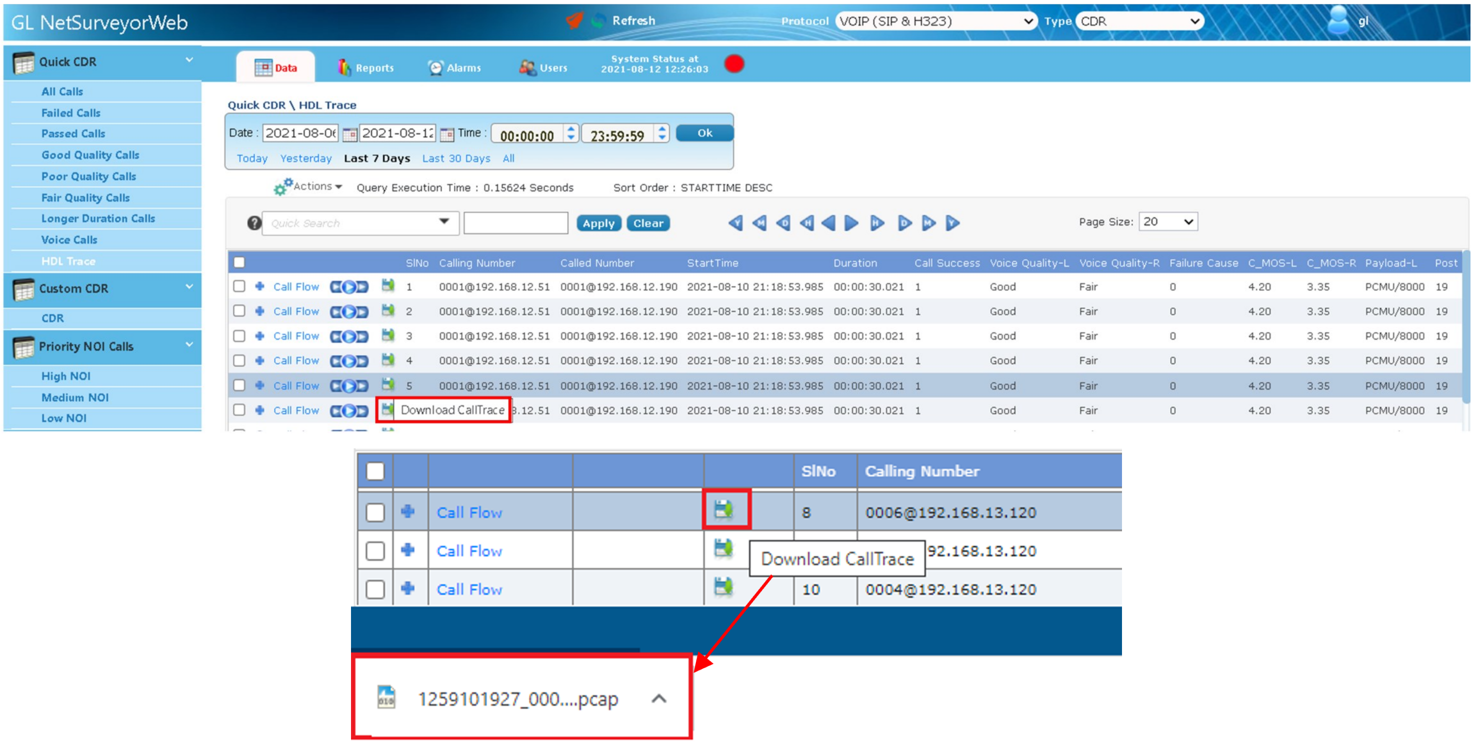
Time	Port	Message	Port
2021-08-11 11:05:14.201	5060	INVITE →	5060
2021-08-11 11:05:14.211	5060	← 100 Trying	5060
2021-08-11 11:05:14.221	5060	← 180 Ringing	5060
2021-08-11 11:05:14.252	5060	← 200 OK	5060
2021-08-11 11:05:14.262	5060	ACK →	5060
2021-08-11 11:05:44.302	5060	BYE →	5060
2021-08-11 11:05:44.312	5060	← 200 OK	5060

```
============ SIP Layer ============              =
  INVITE sip:0008@192.168.12.190 SIP/2.0
  Via: SIP/2.0/UDP 192.168.12.51:5060;branch=z9hG4bK-7422511-1652802887-
  Max-Forwards: 70
  Allow: INVITE,BYE,CANCEL,ACK,INFO,OPTIONS,SUBSCRIBE,NOTIFY,REFER,REGIS
  From: 0008 <sip:0008@192.168.12.51>;tag=FromTag-7422508-1652802887-507
  To: 0008 <sip:0008@192.168.12.190>
  Call-ID: GL-MAPS-7422510-1652802887-50769872-3164@192.168.12.51
  CSeq: 1 INVITE
  Contact: 0008 <sip:0008@192.168.12.51>
  Supported: 100rel
  Content-Type: application/sdp
  Content-Length: 239
                                                                =
  v=0
  o=0008 31188071 1 IN IP4 192.168.12.51
  s=SIP Call
  c=IN IP4 192.168.12.51
  t=0 0
  m=audio 14858 RTP/AVP 8 0 101
  a=rtpmap:8 PCMA/8000
  a=rtpmap:0 PCMU/8000
  a=rtpmap:101 telephone-event/8000
  a=fmtp:101 0-15
  a=ptime:20
  a=sendrecv
```

Figure: SIP Call Flow

Selected Call Trace Download

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



Date : 2021-08-0 2021-08-1 Time : 00:00:00 23:59:59

Query Execution Time : 0.15624 Seconds Sort Order : STARTTIME DESC

Page Size: 20

□				SlNo	Calling Number	Called Number	StartTime	Duration	Call Success	Voice Quality-L	Voice Quality-R	Failure Cause	C_MOS-L	C_MOS-R	Payload-L	Post
□	✚	Call Flow		1	0001@192.168.12.51	0001@192.168.12.190	2021-08-10 21:18:53.985	00:00:30.021	1	Good	Fair	0	4.20	3.35	PCMU/8000	19
□	✚	Call Flow		2	0001@192.168.12.51	0001@192.168.12.190	2021-08-10 21:18:53.985	00:00:30.021	1	Good	Fair	0	4.20	3.35	PCMU/8000	19
□	✚	Call Flow		3	0001@192.168.12.51	0001@192.168.12.190	2021-08-10 21:18:53.985	00:00:30.021	1	Good	Fair	0	4.20	3.35	PCMU/8000	19
□	✚	Call Flow		4	0001@192.168.12.51	0001@192.168.12.190	2021-08-10 21:18:53.985	00:00:30.021	1	Good	Fair	0	4.20	3.35	PCMU/8000	19
□	✚	Call Flow		5	0001@192.168.12.51	0001@192.168.12.190	2021-08-10 21:18:53.985	00:00:30.021	1	Good	Fair	0	4.20	3.35	PCMU/8000	19
□	✚	Call Flow	Download CallTrace		3.12.51	0001@192.168.12.190	2021-08-10 21:18:53.985	00:00:30.021	1	Good	Fair	0	4.20	3.35	PCMU/8000	19

□				SlNo	Calling Number
□	✚	Call Flow		8	0006@192.168.13.120
□	✚	Call Flow	Download CallTrace		92.168.13.120
□	✚	Call Flow		10	0004@192.168.13.120

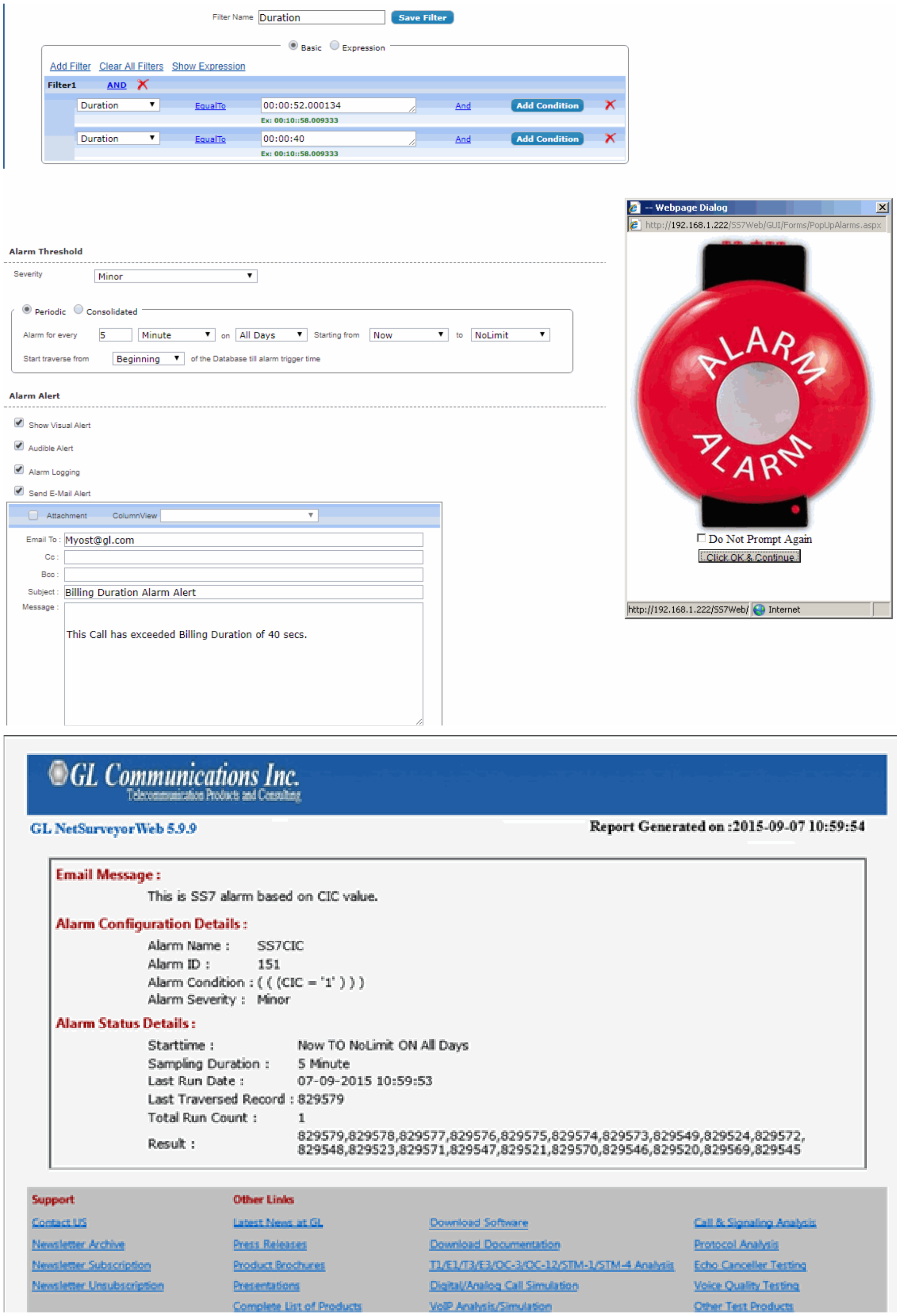
1259101927_000....pcap

Figure: Download the Selected Call Trace

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.



Filter Name: Duration

● Basic ○ Expression

Filter1 AND

Duration ▼ EqualTo 00:00:52.000134 And
Ex: 00:10::58.009333

Duration ▼ EqualTo 00:00:40 And
Ex: 00:10::58.009333

Alarm Threshold

Severity: Minor ▼

● Periodic ○ Consolidated

Alarm for every 5 Minute ▼ on All Days ▼ Starting from Now ▼ to NoLimit ▼

Start traverse from Beginning ▼ of the Database till alarm trigger time

Alarm Alert

☑ Show Visual Alert

☑ Audible Alert

☑ Alarm Logging

☑ Send E-Mail Alert

□ Attachment ColumnView ▼

Email To : Myost@gl.com
Cc :
Bcc :
Subject : Billing Duration Alarm Alert
Message : This Call has exceeded Billing Duration of 40 secs.

-- Webpage Dialog
http://192.168.1.222/SS7Web/GUI/Forms/PopUpAlarms.aspx

□ Do Not Prompt Again

Click OK & Continue

http://192.168.1.222/SS7Web/ Internet

GL Communications Inc.
Telecommunication Products and Consulting

GL NetSurveyorWeb 5.9.9

Report Generated on :2015-09-07 10:59:54

Email Message :
This is SS7 alarm based on CIC value.

Alarm Configuration Details :
Alarm Name : SS7CIC
Alarm ID : 151
Alarm Condition : (((CIC = '1')))
Alarm Severity : Minor

Alarm Status Details :
Starttime : Now TO NoLimit ON All Days
Sampling Duration : 5 Minute
Last Run Date : 07-09-2015 10:59:53
Last Traversed Record : 829579
Total Run Count : 1
Result : 829579,829578,829577,829576,829575,829574,829573,829549,829524,829572, 829548,829523,829571,829547,829521,829570,829546,829520,829569,829545

Support	Other Links		
Contact US	Latest News at GL	Download Software	Call & Signaling Analysis
Newsletter Archive	Press Releases	Download Documentation	Protocol Analysis
Newsletter Subscription	Product Brochures	T1/E1/T3/E3/OC-3/OC-12/STM-1/STM-4 Analysis	Echo Canceller Testing
Newsletter Unsubscription	Presentations	Digital/Analog Call Simulation	Voice Quality Testing
	Complete List of Products	VoIP Analysis/Simulation	Other Test Products

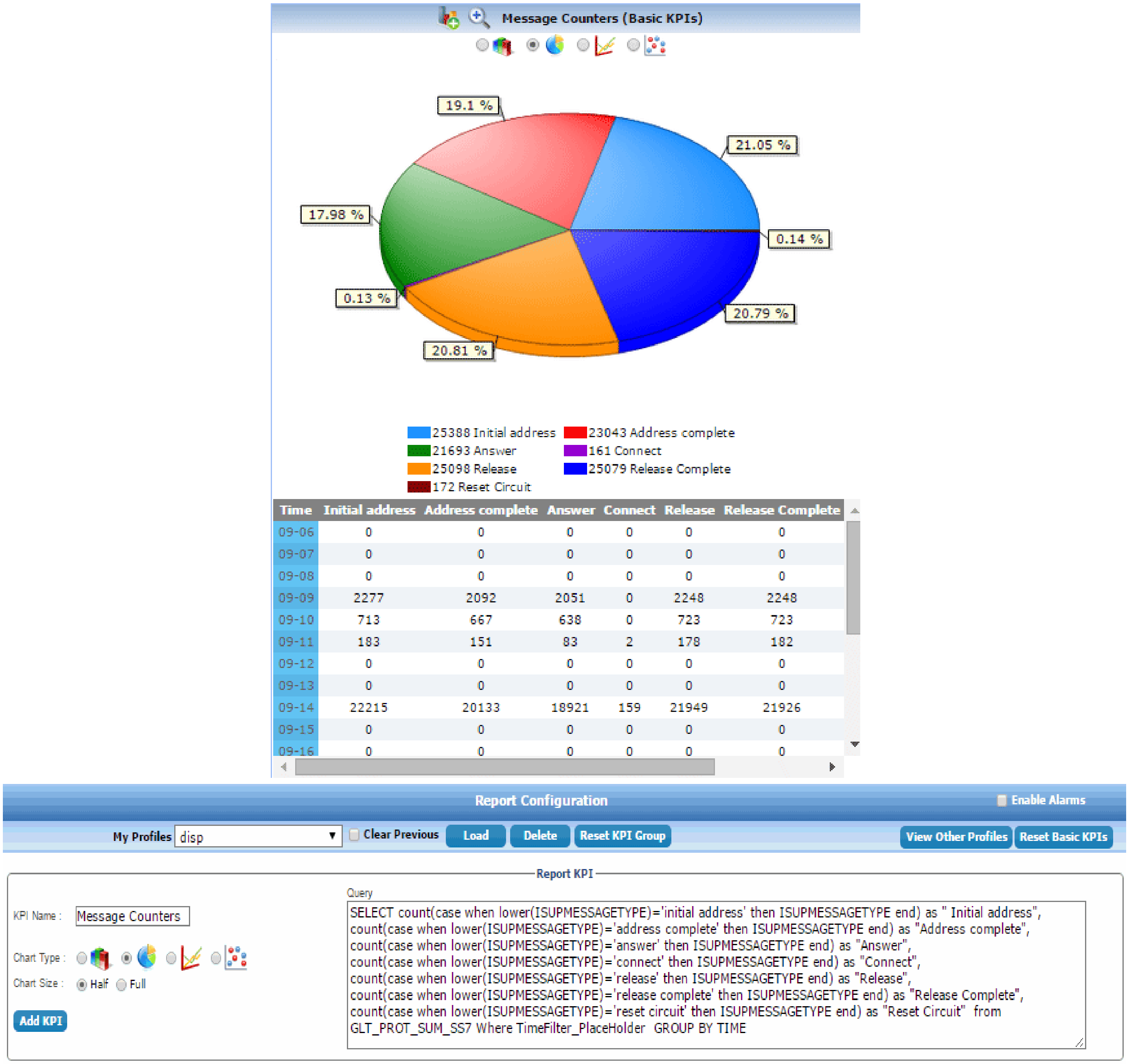
Figure: Alarm Settings and Email Alerts

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. Customized graphs for various metrics such as Call Completion Ratio, Answer Call Ratio, Answer-Seizure Ratio, and Call Duration

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.



🟦 25388 Initial address
🟥 23043 Address complete
🟩 21693 Answer
🟪 161 Connect
🟧 25098 Release
🟦 25079 Release Complete
🟥 172 Reset Circuit

Time	Initial address	Address complete	Answer	Connect	Release	Release Complete
09-06	0	0	0	0	0	0
09-07	0	0	0	0	0	0
09-08	0	0	0	0	0	0
09-09	2277	2092	2051	0	2248	2248
09-10	713	667	638	0	723	723
09-11	183	151	83	2	178	182
09-12	0	0	0	0	0	0
09-13	0	0	0	0	0	0
09-14	22215	20133	18921	159	21949	21926
09-15	0	0	0	0	0	0
09-16	0	0	0	0	0	0

Report Configuration

□ Enable Alarms

My Profiles: disp ▼ □ Clear Previous

Report KPI

KPI Name : Message Counters

Chart Type : ○ ● ○ ○

Chart Size : ● Half ○ Full

Query

```
SELECT count(case when lower(ISUPMESSAGETYPE)='initial address' then ISUPMESSAGETYPE end) as " Initial address",
count(case when lower(ISUPMESSAGETYPE)='address complete' then ISUPMESSAGETYPE end) as "Address complete",
count(case when lower(ISUPMESSAGETYPE)='answer' then ISUPMESSAGETYPE end) as "Answer",
count(case when lower(ISUPMESSAGETYPE)='connect' then ISUPMESSAGETYPE end) as "Connect",
count(case when lower(ISUPMESSAGETYPE)='release' then ISUPMESSAGETYPE end) as "Release",
count(case when lower(ISUPMESSAGETYPE)='release complete' then ISUPMESSAGETYPE end) as "Release Complete",
count(case when lower(ISUPMESSAGETYPE)='reset circuit' then ISUPMESSAGETYPE end) as "Reset Circuit"  from
GLT_PROT_SUM_SS7 Where TimeFilter_PlaceHolder  GROUP BY TIME
```

Figure: Report Configuration

Supported KPIs

Protocol Type	Basic KPIs
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

Item No	Product Description
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) and 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.

Item No	Related Software
PKV169	Network Surveillance Lite Software.
PKV171	Network Surveillance Agent Toolkit

Item No	Related Hardware
PTE001	tProbe™ Dual T1 E1 Laptop Analyzer
XTE001	Dual T1 E1 Express (PCIe) Boards
TTE001	tScan16™ T1 E1 Boards
FTE001	QuadXpress T1 E1 Main Board
ETE001	OctalXpress T1 E1 Main Board plus Daughter Board

For more information, please visit NetSurveyorWeb™ webpage.