Polystar | ELISA INDUSTRIQ

OSIX MONITORING

PRODUCT DESCRIPTION

Release 14.1 V1.0

POLYSTARDOCUMENTATION@POLYSTAR.COM +46 8 50 600 600 WWW.ELISAINDUSTRIQ.COM/POLYSTAR

COPYRIGHT NOTICE

TRADEMARKS

ELISA POLYSTAR

Elisa Polystar Sweden AB ("Elisa Polystar") is part of the Elisa Oyj ("Elisa" or "Elisa Corporation") International Digital Services company group.

Contents

1 Introduction

Welcome to the OSIX Monitoring product description. This document aims to provide a brief description of the purpose and use of the OSIX Monitoring product.

The OSIX system is designed with high scalability and flexibility in mind, and can quickly be adapted to new demands and requirements. This also vouches for a long projected lifespan for the product.

The OSIX system has integrated solutions for various domains, from legacy SS7 to 5G SA and IMS, advanced alarm functionality, location tracking, handset tracking, customer/service/network statistics, SMS messaging, security detection, roaming management, etc.

1.1 Business value

In today's market environment, it is essential for operators to understand what their customers are using the network for and how they experience it. Smartphones and data usage have increased subscribers' demand for bandwidth and their expectations of service and performance.

To maintain a first-class customer experience, advanced real-time monitoring and troubleshooting capabilities are crucial to any organisation operating networks.

The OSIX system provides tools to:

- Perform detailed root-cause analysis on call, session and protocol levels using unique drill-down capabilities.
- Monitor network performance and Quality of Service (QoS).
- Generate real-time alarms on abnormal network behaviour; the alarms can be distributed via SNMP (v1, v2c, or v3) and/or email.
- Detect poor network performance and prevent customer-affecting service issues by providing fast and accurate error finding.
- Resolve network problems faster through an intuitive display of information.
- Gain access to all signalling data across any network technology for the network-wide troubleshooting and root-cause analysis in real-time or historically.
- View and analyse end-to-end QoS and correlate information from different sources on a multi-protocol level.
- Retrieve historical control signalling for analysis purposes

1.2 Business solutions

OSIX Monitoring is an important part of Elisa Polystar's solution portfolio, and the main source of information in the company customer experience assurance solution. OSIX provides operators with end-to-end real-time insights to network and service performance, as well as customer experience, and enables operators to proactively identify and resolve customer-impacting issues, regardless of whether they are using traditional network services or OTT applications.

Figure 1: Elisa Polystar's solution portfolio

At Elisa Polystar, our focus is to provide telecom operators with tools for future-ready, data-driven assurance and automation. OSIX is part of the Elisa Polystar platform that integrates with a wide range of data sources, including:

- Probe-based signaling and network node telemetry
- FM/PM-based OSS information
- CRM ticketing and inventory data
- Customer CRM details

This approach ensures a solution that is adaptable to future analytics needs, giving telecom operators the flexibility to meet their evolving requirements.

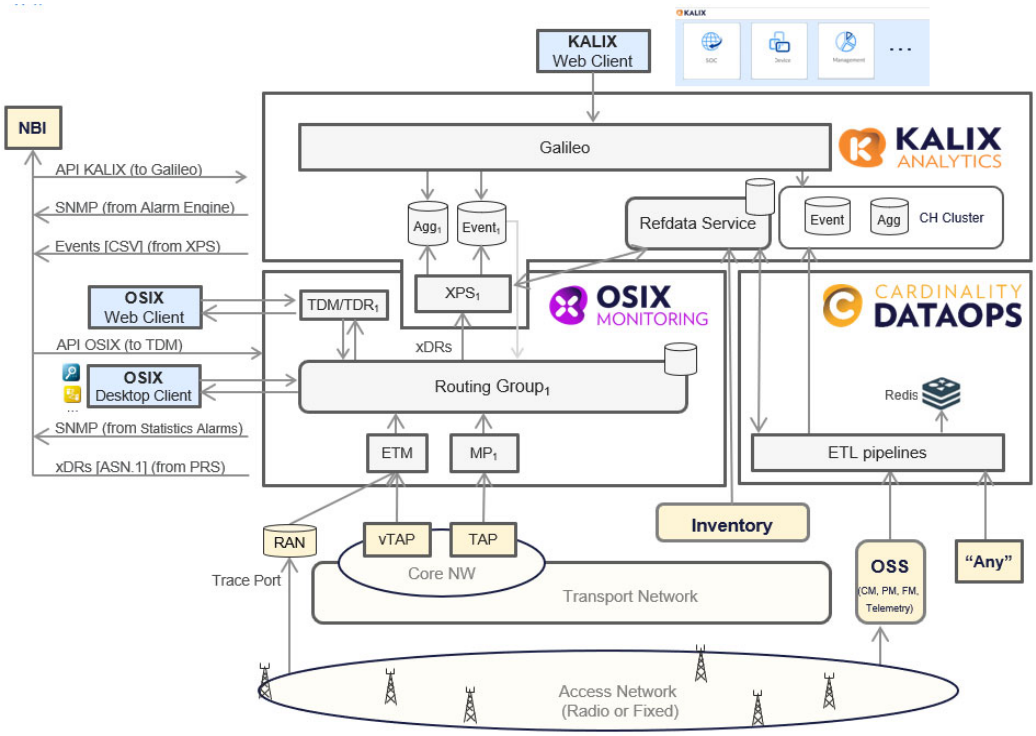


Figure 2: Elisa Polystar's product portfolio

1.3 Licensing

Certain functionalities that are described in this document require separate licences. To find out which functionalities are licensed in a particular system or offer, please contact your Elisa Polystar sales representative.

1.4 More information

The individual solutions are further described in separate documents, containing information about the included report packages and other options for the selected protocols and interfaces.

Contact an Elisa Polystar representative for more information about specific areas and offers.

2 System architecture

The OSIX Monitoring system is designed to provide flexibility, scalability and upgradability. It consists of different components in a layered architecture, where the capturing and processing layers handle the monitored traffic. The exposure layer is needed to use the OSIX Web client, and the system management layer manages the system itself.

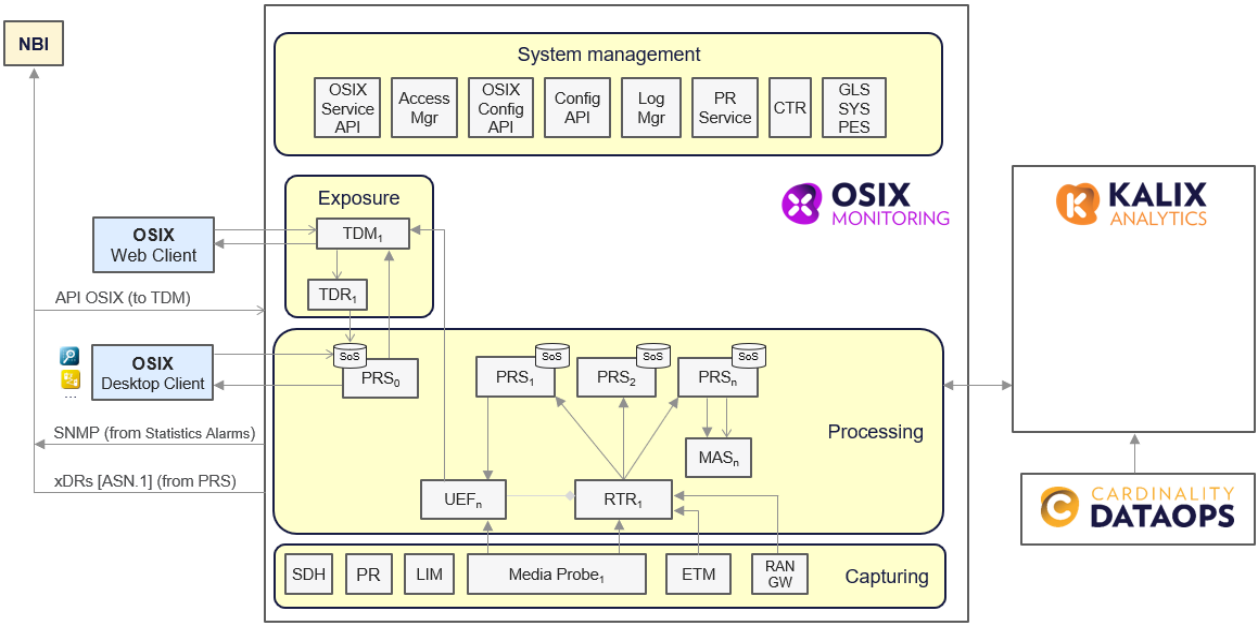


Figure 3: OSIX Monitoring system architecture

The figure above shows the main components of the OSIX Monitoring system and their relation to the other Elisa Polystar products.

To feed the capturing components, the monitored traffic needs to be mirrored out from the active network. Depending on the configuration of the active network, link aggregation and filtering may also be needed to achieve a traffic feed that is within the capacity of each capturing component. The aggregated and filtered traffic feeds are made available by equipment outside OSIX. Elisa Polystar can supply a filtering and link aggregation solution based on a packet broker product from vendors such as Cubro, Keysight, Gigamon, or other similar packet broker providers. Elisa Polystar additionally offers a switch-based load sharing solution, including link aggregation, for processing high volumes of user plane monitoring.

The components of the capturing layer collect and filter the traffic to pass it on to processing. Signalling is transferred transparently, whereas user plane traffic is aggregated in the capturing components due to its large volumes. The aggregates will be enriched with, for example, application and IMSI. RTP streams can also be aggregated. The Packet Recorder (PR) type of capturing unit can provide un-aggregated user plane traffic, for a limited number of individual users, transparently to the OSIX Web Client application. The External Tap Mediator (ETM) handles traffic, for example from vTAPs for 5G SA monitoring, The ETM can also be used to receive a feed from customer data fetched from Trace Port, but in some cases, this requires a RAN GW.

The processing layer implements functionality for tracing and monitoring. The data available in OSIX Monitoring can be sent from processing directly or be fetched historically. The data is sent either directly to the OSIX Desktop Client or via the exposure layer to the OSIX Web client. The processing layer also handles xDR export and SNMP.

The exposure layer in OSIX Monitoring contains the functions for the OSIX Web client, but also allows for northbound integration with third-party systems to access historical data from the processing layer.

Elisa Polystar handles third-party data sources (for example, PM Data) using the DataOps component.

2.1 Capturing

The capturing components provide filtering and separation of traffic. Different monitors can be defined to filter and send traffic from a certain set of links to the correct router in the processing layer. For user plane traffic, the capturing components perform aggregation before passing the traffic on to the processing layer.

Elisa Polystar provides different capturing nodes for different type of physical interface. See chapter *7 Deployment on hardware* and *8.1.1 VMs for the capturing layer* for more details about the different hardware solutions within the capturing layer.

2.2 Processing

In the processing layer, traffic is separated into different routing groups. One routing group (RG) is typically set up to monitor the traffic around one active network node, such as one MME or one AMF. All signalling messages going into the same state machine (that is, appearing as one row within the OSIX Call Trace or xTrace applications) must be captured in the same RG.

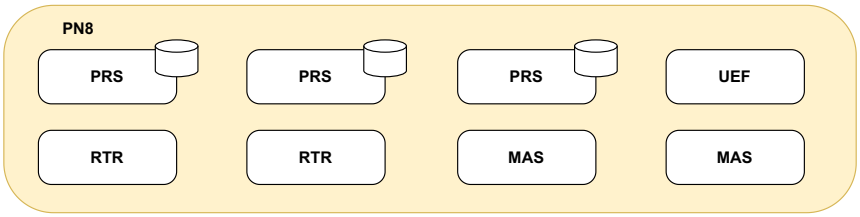


Figure 4: A routing group

To simplify filtering and assigning data access rights in OSIX applications, one or more routing groups are combined into traffic groups.

Within an RG, incoming traffic from the capturing layer is load balanced by the router (RTR) component and sent to a group of processing servers (PRSs). The RTR ensures that signalling messages belonging to the same state machine are sent to the same PRS. The RTR also provides other functionality, such as reassembly of fragmented packets on TCP and SCTP level (IP fragmentation is handled by the MediaProbe). (GCP is a proprietary Elisa Polystar message-based communication protocol running over TCP, encrypted using TLSv1.2, which is used for, but not limited to, communication with the GLS.)

Scaling of the system can be done by adding components to an existing RG, or, in case it is expanded to monitor new network nodes, by setting up new, complete routing groups.

The probe servers host the state machines by collecting related signalling messages into transactions known as “Calls”. These transactions are the basis for the OSIX Monitoring Call Trace application. The PRSs save the transaction data into several databases, of which Storage of Signals (SoS) is the most important. Through data from SoS, the OSIX clients can retrieve full binary signalling for historical calls. PRSs also save selected parameters from each transaction into the Call Search Engine (CSE), which speeds up SoS searches and provides longer retention times of historical data. The PRS also handles the Message Search

Engine (MSE) an optional historical storage of individual signalling messages, and binary storage. The binary storage implements a persistent storage of ongoing transactions on GTP, but will be phased out in the future when GTP will use an event-based type of monitoring.

If the OSIX Monitoring Performance Analyser or Mass Call applications are installed for the OSIX Desktop client, the PRS sends records for all relevant transactions to a performance server.

The PRS also sends xDRs for each transaction to the XPS (xDR Processing Server) in KALIX. These xDRs can also be exported to an external system via an NBI (northbound interface).

The mapping server (MAS) is used to share data needed by all PRSs (and rarely the RTR) within the routing group. Typically, these data are used for Control plane enrichment (for example, IMSI enrichment) and deciphering. The actual deciphering will be performed by the PRS in the case of ciphered Gb or S1-MME, but by the RTR in the case of Encapsulating Security Payload (ESP) ciphered SIP. Most routing groups contain a MAS.

The User Plane Enrichment Function (UEF) is used for enriching the User plane (UP) aggregates generated in the MediaProbe (MP). The UEF must be used in installations using the OSIX Web client, but is also a requirement when monitoring UP for 5G SA networks, as well as in legacy scenarios where CUPS (Control and User Plane Separation) multi-homing is active. The UEF receives the UP aggregates directly from the MP and enriches them with meta data (for example, IMSI) received from the PRS. The UEF sends the enriched information in xDRs to the XPS in KALIX. On request, these xDRs can be sent to the TDM (for OSIX Web) as well.

The UEF can also be used for legacy systems without CUPS, but in such a case the option to send the GTPv2 signalling and the UP aggregates to the same state machine in the same PRS exists. However, this solution requires a stateful RTR component.

When configuring event-based GTP state machines, a UEF is also needed. Today, event-based SMs can be configured for an IoT system, but tomorrow it will be the default configuration. All GTP SMs will be event-based in the future.

In systems with a packet recorder, the OSIX Desktop client can directly access the packet recorder to fetch user data. Setting up packet recorder streams, and optionally downloading recorded files, is made in the OSIX Packet Recorder application, which is implemented by the Packet Recorder Service.

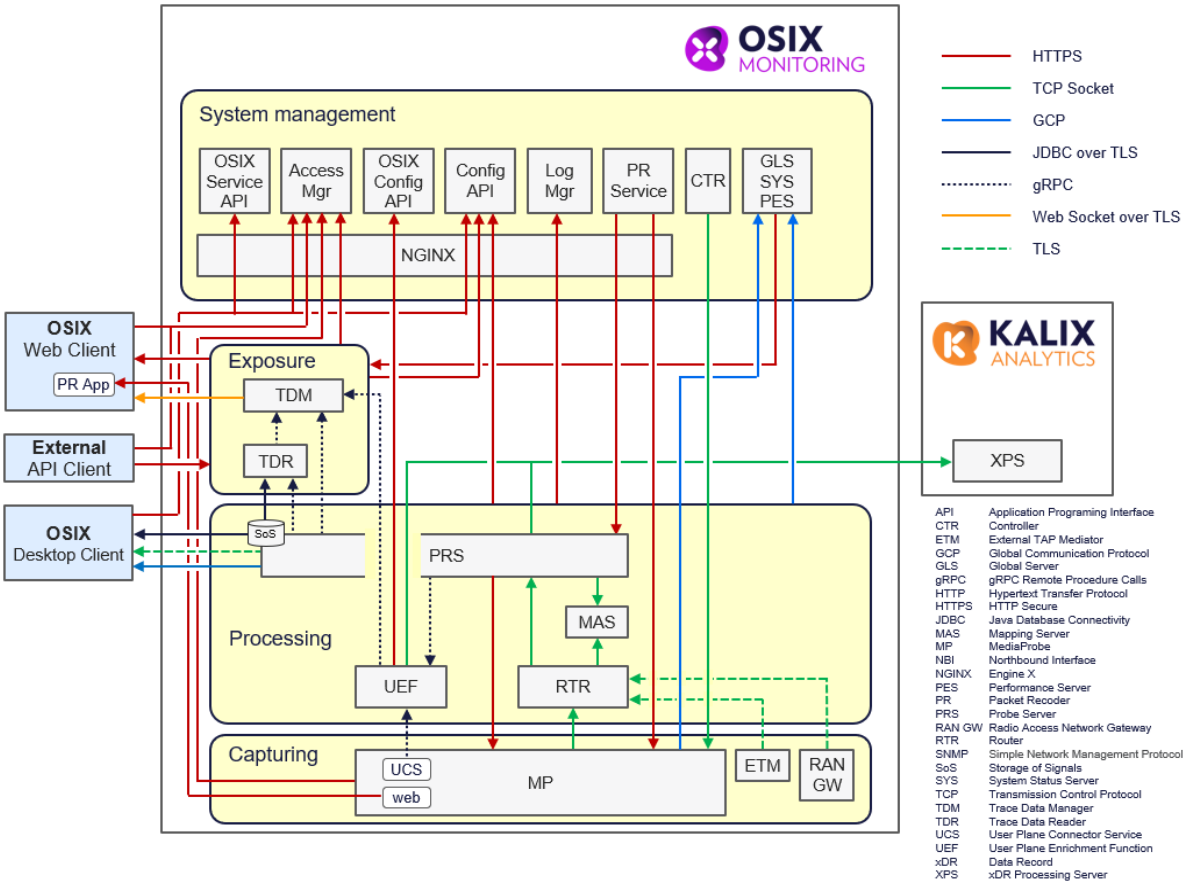


Figure 5: Detailed architecture

2.3 Exposure

The OSIX Web client can access trace level data in the processing layer using the TDM (Trace Data Manager) and TDR (Trace Data Reader) services implemented in the exposure layer. TDM is the interface between the OSIX Web client and OSIX Web backend services. The TDM serves as a mediator of data and provides security and filtering capabilities. The TDR is the primary provider of historical data from the processing layer and communicates directly with SoS storage as well as the PRSs, and can perform filtering on binary historical data.

2.4 System management

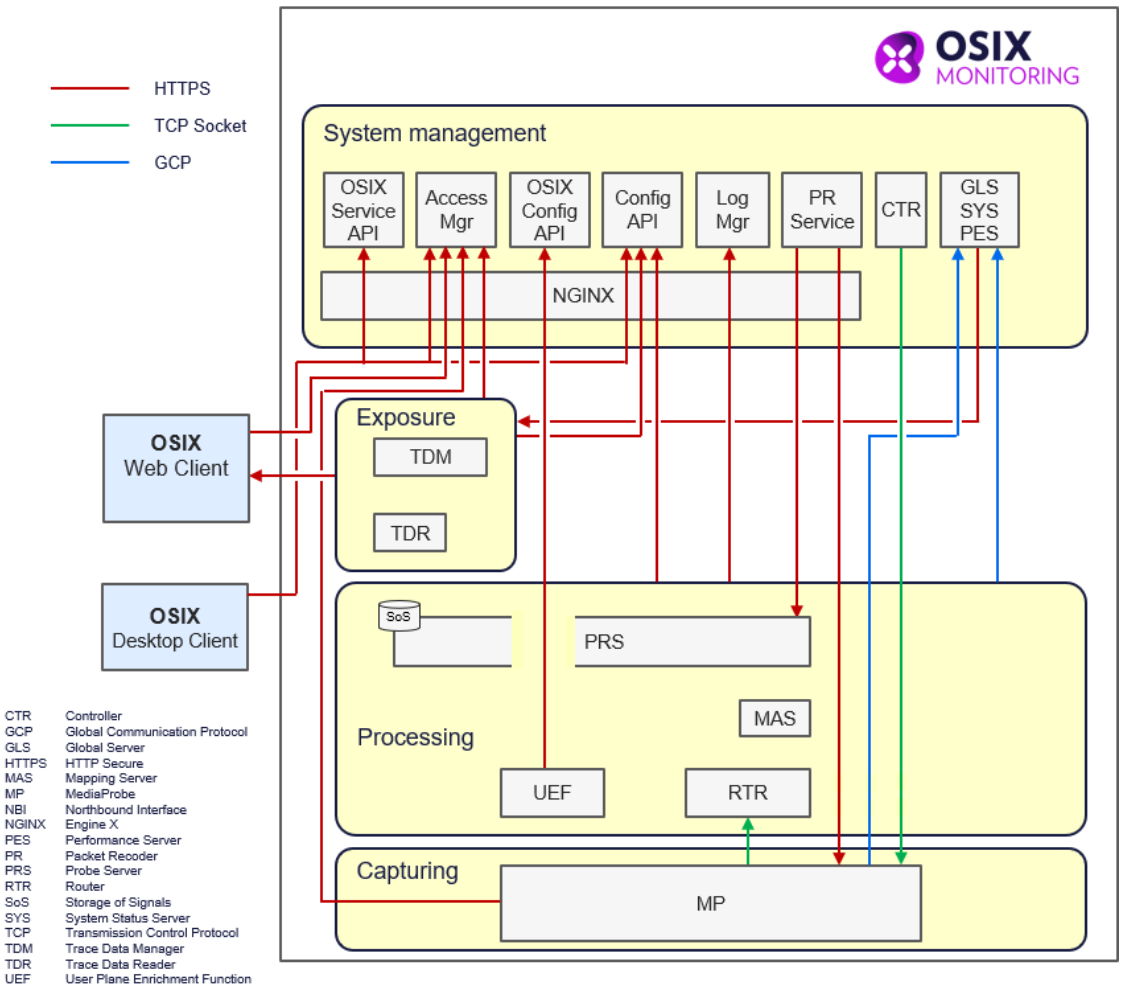


Figure 6: System management

2.4.1 System configuration

Most system configuration parameters are controlled by the Global Server (GLS) and stored in any of its databases. A system administrator can change the configuration through the Configuration Manager application within an OSIX client. Most components communicate directly with the GLS or its databases to retrieve their configuration. For the capturing components, the Controller (CTR) provides translation of GLS configuration data into a format supported by these components.

The MediaProbe cluster controller is needed if multiple MediaProbe instances are run on the same hardware, which is the case for the 40GMP, 80GMP, and 100GMP MediaProbes.

2.4.2 Authentication and authorisation

Using any of the recommended authentication models (Polystar authentication or Active directory authentication, see *5.5 User management*), authentication is handled through the Access Manager component.

For the desktop client, the user profiles and authorisation information reside in the GLS. At login, the GLS verifies the credentials supplied by the user towards the Access Manager.

User Manager is the front-end application used to configure users, permissions, and roles within Access Manager.

2.4.3 Personal System Accounts

For improved auditing, Personal System Accounts are implemented in the system. This means that instead of common accounts being used when logging into servers, users with the proper permissions can use their normal OSIX personal accounts for Linux level login.

Who should have access to this feature is controlled from User Manager, the frontend for Access Manager. A service called Gatekeeper runs on all servers in the system and syncs public ssh keys from the Global Function to allow for password-less ssh to any server (between other servers not involving the GF still requires the user's password).

Authentication via password is handled by contacting the LDAP server integrated into Access Manager via the SSSD service on the server the user logs into. If the account is managed by an external Active Directory, the LDAP BIND request is forwarded to the Active Directory, which handles the user authentication.

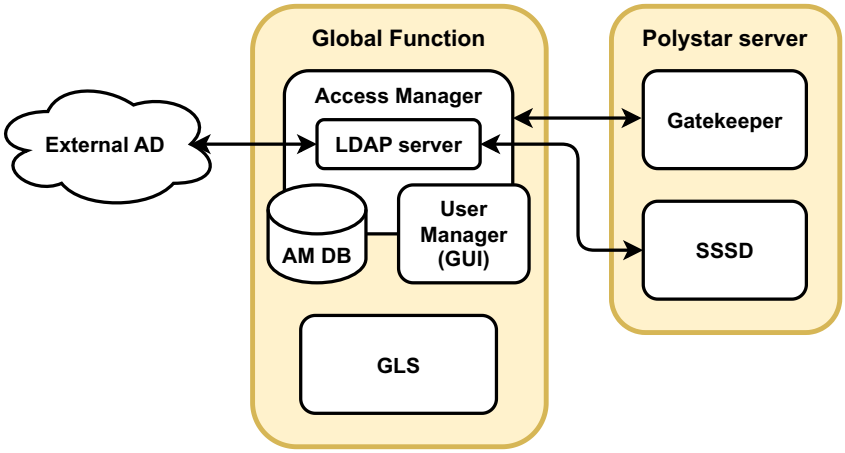


Figure 7: Personal System Accounts

2.5 Geographical deployment

This section describes where the OSIX Monitoring and KALIX Analytics components are deployed geographically.

2.5.1 Typical deployment

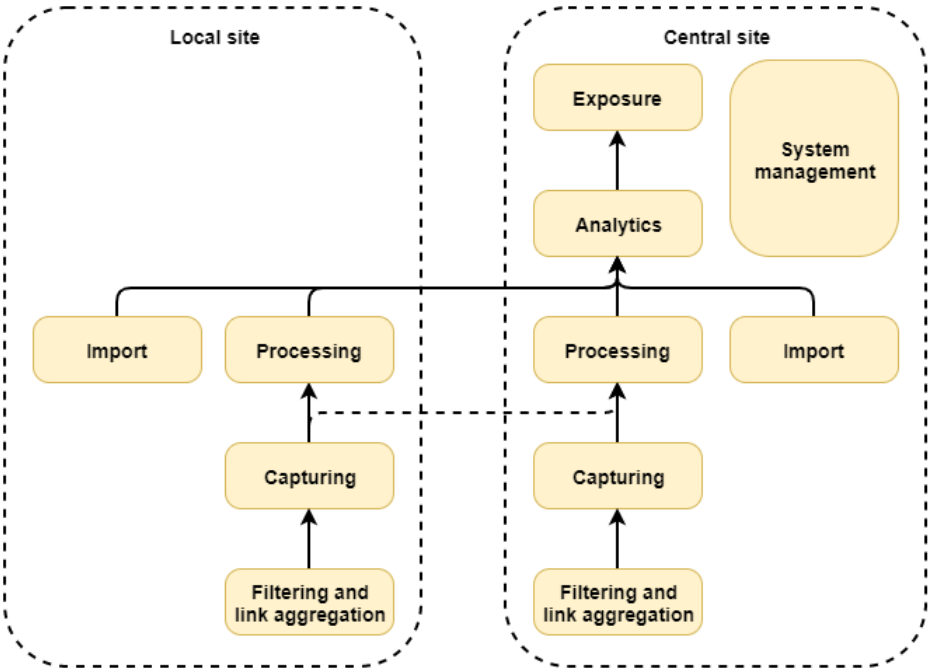


Figure 8: Typical deployment of OSIX, KALIX, and DataOps

In a typical deployment, capturing and processing is implemented on the geographical sites of the monitored nodes. This deployment strategy ensures low latency between monitored nodes and the Elisa Polystar components within the capturing and processing layers, which is vital for enrichment and deciphering. An exception is the routing groups for IMS core and STP traffic, which need to cover the entire monitored system, and therefore are implemented on a central site.

The analytics layer (found in the KALIX product) and the exposure layer (OSIX and KALIX) are typically deployed in one central location since their components correlate and aggregate traffic system wide.

The import is handled by the DataOps product.

2.5.2 Deployment with centralised processing

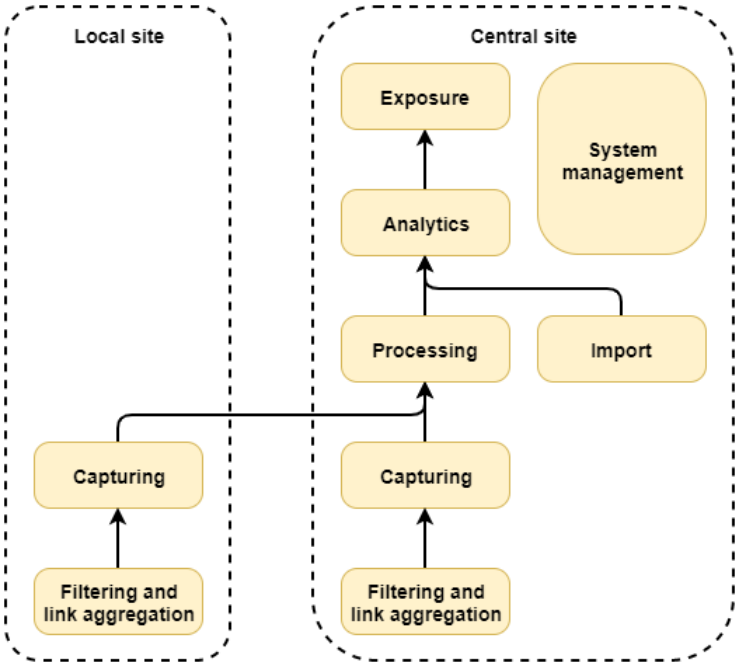


Figure 9: Deployment with centralised processing

Under certain circumstances, it is possible to locate all processing on a central site. This could be beneficial for system dimensioning when there is fail-over of traffic between monitored nodes on different sites. However, central distribution of processing nodes puts high requirements on network infrastructure and is only possible in certain traffic scenarios. Please contact your Elisa Polystar representative to determine whether central location of processing nodes is supported for your network.

2.6 Domain Name System

The OSIX Monitoring System is set up with a local DNS server and DNS zone. The DNS server is located on the Global Function.

When new servers are configured in the system, they are automatically added/ updated to the local DNS server. This ensures that all servers have the correct DNS lookup. This DNS configuration is used to generate the `/etc/ansible/hosts` file, which in turn is used by automated scripts to perform various actions on the servers.

As a technical strategy, Elisa Polystar has started using the `.osix` domain for inter-server/service communication. For example, when the Global Function (GF) needs to perform an action on the PRS, the code in the GF will use `prs42.osix` as a name lookup. This has also been tied to TLS certificates—all inter-server communication uses a TLS certificate issued to the `.osix` domain. The strategy is that `.osix` should never be used outside of the Elisa Polystar servers. The external DNS should also not be aware of the `.osix` domain.

The host name (without an FQDN, i.e. `prs42` above), can be assigned according to any RFC-compliant scheme decided by the customer with one exception, which is that the GF must have the host name `gls`.

In addition to using the `.osix` domain, all Elisa Polystar servers are also part of the `.polystar.net` domain. This is implemented in Bind so that both domains point to the same zone file. The `.polystar.net` domain is indented for when an external server wants to connect to an Elisa Polystar server.

The system can be reconfigured for the servers to respond with a customer domain (and a customer-signed TLS certificate) instead of `.polystar.net`.

The local DNS can be configured to perform a recursive/forwarding lookup that points to an external DNS, which makes it possible for custom software on an Elisa Polystar server to look up a host name such as `server.customer-domain.com`.

3 Capabilities

3.1 Network monitoring

The OSIX system provides passive monitoring of a wide range of networks, interfaces, and protocols. The products are continuously enhanced and support for new technologies is added.

A complete listing of supported interfaces and protocols is available in a separate document—*Supported protocols and interfaces*.

3.2 User data aggregation

Elisa Polystar offers user plane analytics where the complete volume of user data is fully monitored. The analytics provided falls under three main categories; Mobile PS, Mobile CS, and Fixed broadband user plane. To offload the processing and presentation layers the data is aggregated, resulting in the most value-generating KPIs in this domain of analytics.

This is the most efficient way of monitoring huge data volumes, which is crucial to managing continuously increasing bandwidth requirements. In the Mobile PS and Fixed broadband domains, the data carried over the IP layer is presented by a large number of application and transport KPIs. In the Mobile CS domain aggregation of RTP user data provides voice quality records that indicate the end users' call experience.

3.2.1 Mobile PS user data

Elisa Polystar captures the full GTP user data by monitoring the mobile core user plane nodes, and performs activity-based aggregation per mobile subscriber for the presentation layer. The aggregation is activity-based, where the main aggregation keys are the User Identity and the user data Application identified from deep packet inspection (DPI). The resulting aggregates present important service metrics such as data volume, throughput speed, round-trip time (RTT), internet server details, TCP statistics, DNS, Application details, and more.

The activity aggregation combines multiple bi-directional data flows for the same application, leading to accurate DPI classification that may be combined with a large number of network and user dimensions.

In the resulting analytics, detailed information is provided related to applications and protocols, transport layer measures, as well as throughput and data volumes. For a network perspective, the user plane analytics can be combined with APNs, network node identifiers, or Radio access types. To get the user perspective, the analytics may be combined with IMSIs or any related user identifier, or device types to see trends between handheld models.

3.2.2 Fixed broadband user data

Elisa Polystar captures the full fixed broadband network user data by monitoring the broadband network gateways (BNG), and performs activity-based aggregation per customer premises equipment (CPE) for the presentation layer. The aggregation is activity-based, where the main aggregation keys are the User Identity, and the user data Application identified from deep packet inspection (DPI). The resulting aggregates present important service metrics such as data volume, throughput speed, round-trip time (RTT), internet server details, TCP statistics, DNS, Application details, and more.

The activity aggregation combines multiple bi-directional data flows for the same application, leading to accurate DPI classification that may be combined with a large number of network and user dimensions.

In the resulting analytics, detailed information is provided related to applications and protocols, transport layer measures, as well as throughput and data volumes. For a network perspective, the user plane analytics can be combined with access node identifiers and vendor types. To get the user perspective, the analytics may be combined with Subscriber identifiers and Subscription rates.

3.2.3 DPI enrichment

The monitored GTP user data and Fixed broadband user data flows are enriched with DPI information. Elisa Polystar uses a third-party software called Qosmos ixEngine® by ENEA for DPI enrichment. The ixEngine® DPI library contains a vast number of application signatures that are continuously maintained, and new popular applications are continuously added. The DPI enrichment is available in the OSIX and KALIX products.

3.2.3.1 Local applications

DPI information for user plane analytics is customisable in order to complement the current application library from Qosmos. Host names from HTTP and HTTPS server name indication (SNI) field are used to create rules for classifying user data records, either to new or existing applications. This means that customers with strong interest in any specific unsupported application can create a pattern matching for in a local library. It can also be used for recently launched applications that have not yet been added to the DPI library. Server IP addresses can also be used to add applications to a local DPI library. However, it is recommended to only translate IP addresses where the relation to an application or a service is known.

3.2.4 OTT Video Analytics

The feature Over The Top Video Analytics is a tool to monitor video streaming experience and network performance for mobile devices. Video analytics are offered as part of the Mobile PS analytics solutions.

Data volumes for video streaming keep growing, with special focus on on-demand video streaming that uses services like YouTube, Netflix, Amazon Prime, HBO, TikTok, Meta, and similar. Delivering such services consumes network bandwidth, and ensuring a positive end user experience is becoming more important. OTT Video Analytics provides measurements to understand the User Experince, Audio and Video Quality, and Transport Network Throughput. In addition, a set of measurements are available to perform deep analysis throughout the full ecosystem, including Access Network, Service Providers, Operating Systems, Application Providers, and Devices.

3.2.5 Mobile CS user data

3.2.5.1 Aggregated RTP Voice quality analysis

Many VoIP calls traverse multiple networks, and the service quality is often affected by circumstances outside the control of the service provider. This makes VoIP performance management and service quality monitoring critically important. The voice quality calculation is made in the MediaProbe by analysing the RTP (Real-Time Transport Protocol). Values like MOS (Mean Opinion Score), Jitter, delay, echo, and packet loss are forwarded to the Probe Server, and enters the related State Machine (for example, SIP). A MOS value is given for conversation and listening. It is also calculated every 30 seconds (configurable) and at the end of each call. The RTCP (RTP Control Protocol) sends quality report for an RTP stream from the end points/nodes. RTCP reports are taken into account if present in the

monitored traffic. These values are presented in OSIX Call Trace/xTrace in a separate column.

3.2.5.2 MediaProbe for RTP

By integrating a third-party library into the MediaProbe for RTP, Elisa Polystar has created a voice quality analysis implementation that is P.564 class 1-compliant. It allows network managers to see call quality problems in real time and identify the root cause of the problem on active or even completed calls.

3.2.5.3 VoIP call quality monitoring

VoIP call quality can be affected by packet loss, discards due to jitter, delay, echo, and other problems. Some of these problems, notably packet loss and jitter, are time-varying in nature as they are usually caused by congestion on the IP path. The MediaProbe can provide call quality metrics for RTP, including listening and conversational quality scores, and detailed information on the severity and distribution of packet loss and discards (due to jitter). The columns for Aggregated RTP are available in both Call Trace, Protocol Analyser, and xTrace. Supported protocols are SIP, SIP-T, H.323, MGCP, and MEGAGO.

3.3 Deciphering

The OSIX system supports deciphering of the following protocols and interfaces:

- 5G-NAS over NGAP on N1
- 4G-NAS over S1AP on S1-MME
- SIP on Gm
- BSSGP on Gb

Deciphering of NAS over NGAP on N1 is supported for keys exchanged on HTTP/2 over N12 and on GTPv2 over N26/S10. Supported encryption algorithms are 5G-EA0, 5G-EA1, 5G-EA2, and 5G-EA3. In most cases at least 98% of ciphered 5G-NAS messages can be deciphered.

Deciphering of NAS over S1AP on S1-MME is supported for keys exchanged by Diameter over S6a, by GTPv1-C on Gn (SGSN Context Request), by GTPv2 on S10, and by MAP over Gr (in case of a co-located SGSN/MME). Supported encryption algorithms are EEA1, EEA2, and EEA3. Deciphering capabilities can vary depending on the interfaces monitored, specific network elements configuration like re-use of 2G keys in 4G procedures, and actual monitoring devices, such as IoT devices that have established PDP connections prior to monitoring them and capturing their keys. Even considering the above, in most cases at least 95% of ciphered NAS messages can be deciphered.

Deciphering of Gm is supported for keys exchanged over SIP on Mw interface between P-CSCF and I/S-CSCF. If SIP is not possible to monitor due to co-located CSCF nodes, fetching keys from Diameter on Cx interface between S-CSCF and HSS is supported. Supported protocol for deciphering is ESP with algorithm AES-CBC and DES-EDE3-CBC. Normally, 99% of ciphered messages on Gm can be deciphered.

Deciphering of Gb is supported for keys exchanged on MAP over Gr and for keys exchanged on Diameter over S6a. Supported encryption algorithms are GEA1, GEA2, and GEA3. The OSIX Data Processing system can normally decipher over 90% of the signalling for Gb.

3.4 IMSI enrichment

OSIX Data Processing enriches transactions where IMSI is not present in signalling for the following interfaces and procedures:

- S1-MME
- Sxa/Sxb session establishment, session deletion, and usage report
- Gm
- Rx
- Iu-CS/A interface
- SIP/ISUP interconnect roaming MT calls
- GTP-U
- Iu-PS
- GTPv1-c
- GTPv2-c
- N1/N2
- N4
- HTTPv2 (5G core)

Typical IMSI enrichment rates are 99% for SIP Gm, 99% for Rx, 99% for N1/N2, and 97% for S1-MME.

3.5 Scalability and system expansions

The OSIX Monitoring system is designed for scalability. While offering cost-efficient solutions for monitoring small networks with limited amounts of traffic, the system can also easily be expanded. New PRSs can be added to existing routing groups, and new XPSs can be added to existing XPS groups is case traffic volumes grow.

Most expansion scenarios can be handled without traffic loss, and, in some cases, without any system downtime. For example, monitoring of new links can be added to existing routing groups without any interruption in the monitoring of existing links. New processing nodes that host new routing groups can be added without interruption of existing routing groups, for example when monitoring of a new geographical site is added to the system. In case of configuration changes in the Analytics and Exposure layer, the disk buffering capabilities of the PRS ensure there is no loss in analytics and exposure data.

3.6 System upgrade

3.6.1 OSIX upgrade

Elisa Polystar uses a phased upgrade approach to minimise system downtime and risk. In the OSIX upgrade the Capturing, Probes, and System Management components are upgraded. This is followed by a verification phase. If a critical regression should be detected, roll-back is supported.

The OSIX upgrade process rests on the assumption that the system is kept upgraded to the current major release or any of the two previous major releases. Hence, upgrading the system with an annual or higher frequency is strongly recommended.

The table below describes the end user consequences and time spans associated with an OSIX and KALIX upgrade. The information in the table can be used to plan upgrade time windows and manage end user information about the upgrades in the best possible way. The information is only valid if annual or more frequent upgrades are performed. A less than annual upgrade frequency necessitates a more complex multi-step upgrade approach with longer system down time.

Upgrade stage	Description	OSIX end user consequences	KALIX end user consequences	Time interval
Upgrade preparation	Preparation steps, such as downloading SW, etc.	None	None	N/A
OSIX upgrade downtime	Time during which the OSIX system is brought down.	■ Not possible to login ■ Data loss (not recovered)	■ Not possible to login ■ Data loss (not recovered)	1-2h from start of OSIX upgrade
OSIX verification and roll-back window	Time for verification and potential roll-back of OSIX.	None, except in the unlikely event a roll-back must be performed.	None, except in the unlikely event a roll-back must be performed.	2-8h from start of OSIX upgrade.
OSIX data inaccuracy time	Time during which some functions affecting data accuracy are recovering from the downtime.	■ Degraded S1-MME deciphering rate (up to 48h) ■ Degraded Gb deciphering rate (acceptable level after up to 48h, fully recovered after up to 120h) ■ Degraded ESP deciphering rate (up to 8h) ■ Degraded Gm IMSI enrichment (up to 8h) ■ Degraded A-interface IMSI enrichment (typically 12h) ■ Degraded CP enrichment of UP data (up to 48h) ■ Incomplete state information on long sessions on GTP and Diameter (network dependent)	■ Inaccuracy in measures based on ciphered protocols (see OSIX for details) ■ Not finding all events in IMSI-based searches, for example, Customer Analysis ■ Data volume graphs show too low values (up to 48h)	Different for different functions. System fully recovered except minor Gb deciphering degradation after 48h.
KALIX upgrade downtime	Time during which the KALIX system is brought down.	None	Not possible to login.	1-4h from start of KALIX upgrade.
KALIX data processing delays	Time during which KALIX reads data buffered during the KALIX upgrade downtime.	None	■ Real-time data not available ■ Alarms not available ■ Scheduled reports not available ■ Inaccuracy in Silent roaming measures.	Up to 24h from start of KALIX upgrade.

Table 1: System upgrade process stages

3.6.2 Platform upgrade

A platform upgrade is the process of upgrading platform RPMs outside the OSIX applications, in order to get access to security-related fixes and other OS-level enhancements. Elisa Polystar packages and verifies OS- and third-party RPMs in so-called OS channel releases, named after their respective AlmaLinux/RHEL snapshot date. The platform upgrade process upgrades between minor versions of the OS.

A yearly platform upgrade is mandatory and included in the standard support contract. All releases made available during a certain year, starting with the first major release of that year, requires the OS to be updated to the first OS channel release of that year. More frequent platform upgrades are available subject to the applicable support agreement.

Like the general OSIX upgrade process, the platform upgrade process is designed based on the assumption of annual or more frequent upgrades. The OSIX and KALIX software must be on the current major release or any of the two previous major releases for platform upgrade to be supported.

The table below describes the end user consequences and time spans associated with a platform upgrade.

Upgrade stage	Description	End user consequences	Time interval
Platform upgrade preparation	Preparation steps including channels or yum repository content transfer and setup, running check scripts, etc.	None	N/A
Platform upgrade installation	Installation and the reboot of servers after successful installation. This step is dependent on a successful execution of the Platform upgrade preparation step described above.	■ Not possible to login ■ Data loss (not recovered)	Typically less than 30 minutes, but in some cases up to 8h (for servers that need to perform a System File Check).

Table 2: Platform upgrade process stages

3.7 Multiple Network Support

Multiple Network Support (MNS) means the ability to operate on two logically/ physically isolated networks in a customer network.

The "Networks" are isolated between the user application layer (OSIX clients - User Network) and the signalling traffic, that is, the Backbone Network. This is achieved by using physically separated Ethernet ports on GN, PN, XN, and MP as illustrated in the figure below:

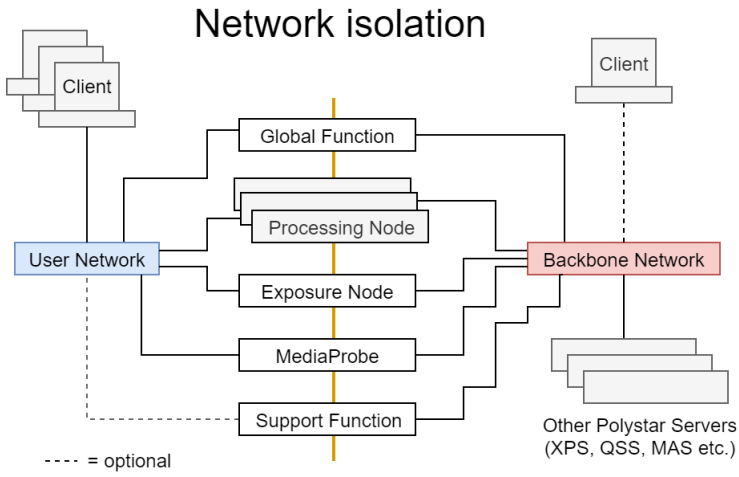


Figure 10: Network separation

Monitored traffic is processed in the backbone network, and client-requested traffic is provided in the user network.

In addition to already mandatory IPs in the backbone network, additional IPs for the user network is required for this purpose, that is, one IP address per JVM component per network inherence.

3.8 Redundancy

3.8.1 Secondary Global Function

Deploying a Secondary Global Function component minimises downtime and increases availability for client access in the event a Global Node/System Management Node (the node the Global Function component is hosted on) should suffer any malfunction or be degraded for any reason. If there is a problem with the primary Global Function component, clients connect to the secondary Global Function component.

The following functionality is served by the secondary Global Function component and is hence available after malfunction/degradation of the primary Global Node/ System Management Node: system configuration; OSIX reference data; OSIX Licence configuration; OSIX and common User authentication and authorisation configuration; OSIX profiles and OSIX Performance Analyser configuration.

The Secondary Global Function component does not support moving of active alarms in the system, the alarm log, link status information, statistics alarms, or historical system status information.

The secondary Global Function component is deployed on an additional Global Node/System Management Node or as a VM in the customer data centre.

If a second SMN is added to the system design, this also ensures that all nodes in the system, including the first SMN, can be re-staged if a need to do a full OS update occurs. In a system with only one SMN, re-staging of the SMN will require that the vStaging VM is installed in the customer data centre.

3.8.2 Secondary Support Function (SF)

Deploying a secondary SF minimises the general downtime and increases the availability for the Elisa Polystar support team to access the system and reduce response times in the event the System Management Node should suffer a malfunction or be degraded for any reason. If there is a problem with the primary support function (SF), the Elisa Polystar support team will connect to the secondary support function.

The secondary support function is deployed on an additional System Management Node or as a VM in the customer's data centre.

3.9 Backup/restore

The OSIX system supports backup and restore of configuration data. Remote storage of backup files can be configured. The default setting is that a backup is made automatically once a day.

The following configuration data is included in a backup:

- OSIX system configuration
- OSIX reference data
- OSIX Licence configuration
- OSIX Alarms configuration
- OSIX and common User authentication and authorisation configuration
- OSIX profiles
- OSIX Performance Analyser configuration
- OSIX xDR/CSV export configuration

3.10 System health

The OSIX system includes a built-in system monitoring application called System Status, which is realised as a KALIX portal dedicated to monitoring the OSIX system, and which summarises the most important information about the system in eight pre-defined sections:

- Overview
- Capturing
- Traffic flow
- Deciphering and enrichment
- Analytics
- KALIX
- Hosts
- Services

Additional custom views can be created using the Ad hoc analysis feature in KALIX, using predefined System Status datasets, measures, and dimensions.

The System Status application can handle alarms based on best-practice system KPIs, either from within the application itself or from an external alarm management system via SNMP and/or email, and, likewise, the System Status data can be scheduled and distributed via email.

3.10.1 Polystar Element Manager (PEM)

The Polystar Element Manager (PEM) is a service for management of system resources. It is a self-healing service for JVMs (RTR, PRS, MAS, UEF) in routing groups. The PEM also reports if RTR/PRS threshold values reach above the stated capacity. The PEM is Elisa Polystar's Element Management System (EMS) that manages network elements (NE)* in the OSIX monitoring system.

The PEM service is implemented as a self-contained container service on the (v)GF.

4 Clients

This chapter describes the various OSIX clients that are available in the OSIX Monitoring system. The OSIX client is available in two different deployments—desktop and web.

4.1 OSIX desktop applications

Currently, seven different OSIX applications can be included in the OSIX system:

- Protocol Analyser
- Call Trace
- Performance Analyser
- Mass Call
- Real Time Statistics
- Network Status
- Statistics Alarm
- Packet Recorder

4.1.1 Protocol Analyser

The Protocol Analyser (PA) application monitors protocol messages. These messages can be viewed in real time or historically, reading from the SoS (Storage of Signals). Included in the application are advanced filtering functionalities, and comprehensive tools for adapting the user interface. You also have quick access to detailed information within the protocol messages down to each individual bit and byte of the signalling.

This application will help you solve network problems at a deeper level, and find reasons for erroneous transactions, by filtering on specific protocol messages, etc.

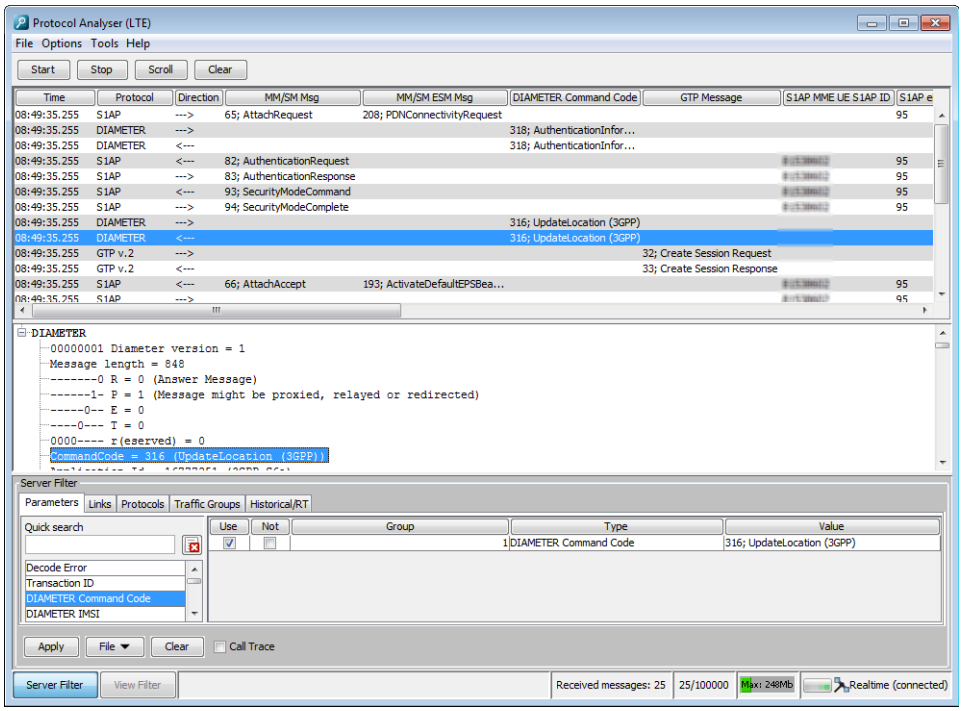


Figure 11: Protocol Analyser main window

In Protocol Analyser you will see the bits and bytes of all signalling messages and the decode of all layers of the used protocols, for example:

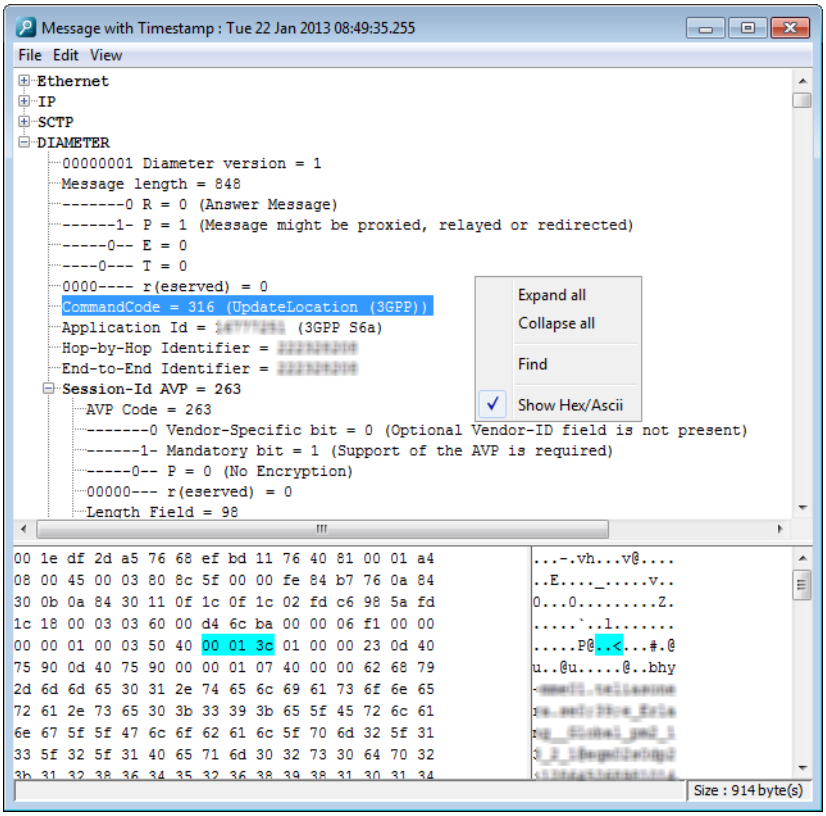


Figure 12: A message in Protocol Analyser

All protocols supported in OSIX Monitoring are available in Protocol Analyser with a huge set of predefined parameters available for filtering. See chapter *15 Protocol parameters* for available parameters.

4.1.1.1 Customising the interface

You can customise each window to display the information you are interested in, with the representation, order, and sorting of your choice, by using the Columns and Customise dialog boxes.

4.1.1.1.1 Columns dialog box

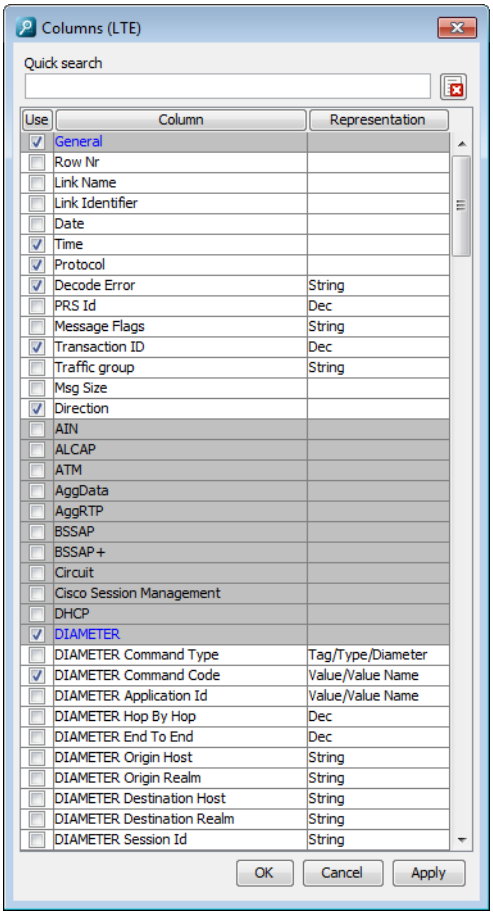


Figure 13: Columns dialog box

4.1.1.2 Filters

There are five different types of filters for Protocol Analyser and Call Trace:

- **Traffic Groups** - The links in your network are divided into one or more traffic groups, and you must select at least one traffic group before you can start monitoring messages. Each traffic group is composed of a number of routing groups.
- **Historical/RT** - You can switch between historical and real time search mode. The historical filter is used for viewing calling processes historically, that is, from a certain time interval and with a certain duration. A historical search will filter out all messages that do not fit in the time period selected in the search filter.
- **Parameters** - You can set a filter on any parameter value visible in the main window. The quickest way to do this is to right-click the value and add to the filter. This filter type also allows you to exclude messages with specific values.
- **Links** - You can choose to only view messages being sent on one or more specific links. A link is related to how the capturing is done and is related to a filter in the MediaProbe.
- **Protocols** - If you are running more than one protocol, you can easily select to only view messages of a certain protocol type.

4.1.1.2.1 Server filter and view filter

The parameter, link, and protocol filters can be set both as a server filter and as a view filter. A server filter determines which messages should be sent from the probe servers to the desktop client, minimising the load on the LAN/WAN, while the view filter searches through the messages sent to the client computer and displays messages passing the filter criteria, and can thus be turned on or off.

4.1.1.2.2 Combining filter criteria

Filters can be set to display either messages where a certain parameter equals a certain value, or messages where a certain parameter does NOT equal a certain value. The set filter criteria can then be combined with AND/OR functionality.

4.1.1.3 Available parameters

For available protocol parameters for Protocol Analyser, see *15.3 Protocol Analyser*.

4.1.2 Call Trace

The Call Trace application groups messages into “Calls”. Calls can be view in real time or historically using the Storage of Signals (SoS) database. Included in the application are advanced filtering functionalities, and comprehensive tools for adapting the user interface. You also have quick access to detailed information about the processes, and all the messages sent during the processes.

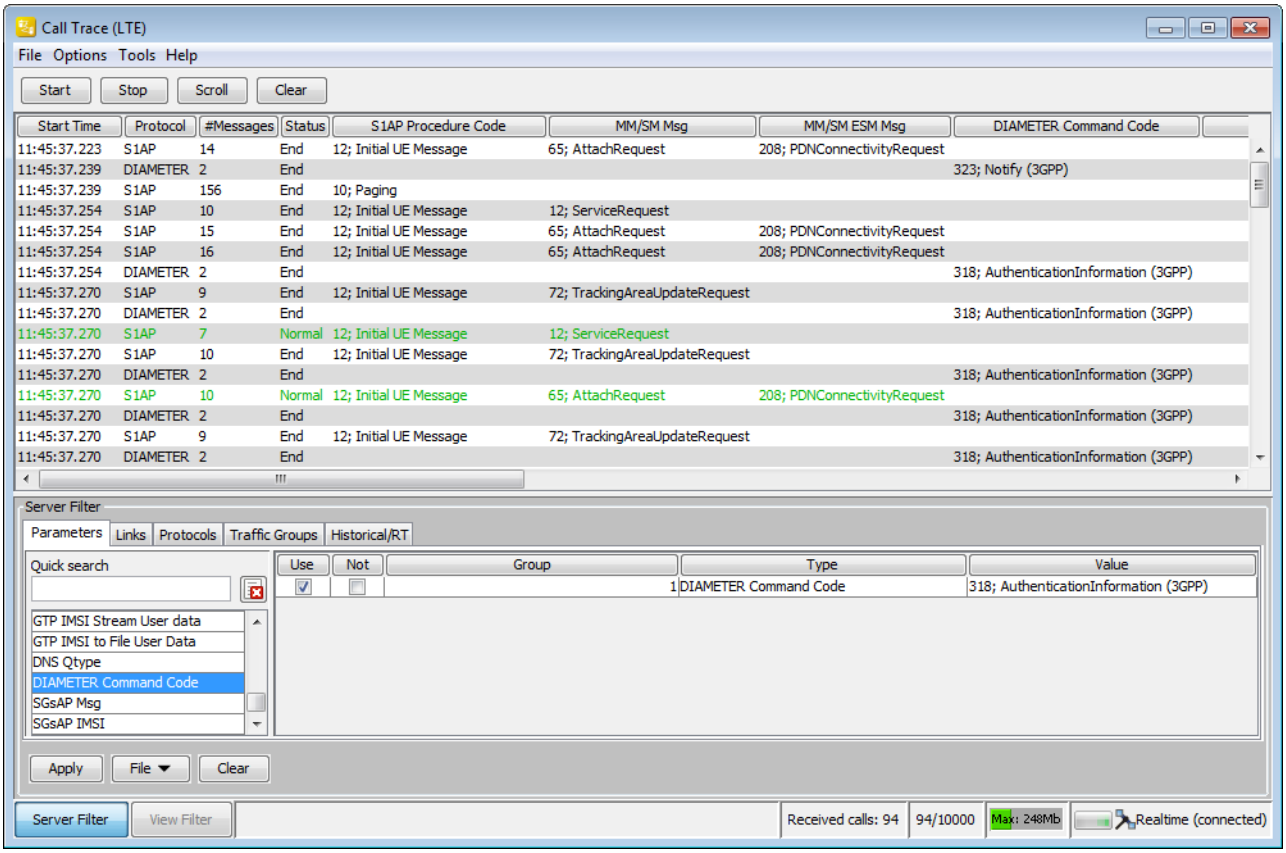


Figure 14: Call Trace main window

The comprehensive Client Correlation functionality allows you to find and view all messages, end-to-end, for all the different transactions that are parts of the logical transactions, for example, all the transactions relevant for a mobile call, an SMS transaction, or a VoIP call.

The Call Flow view, that displays how the messages are sent between different nodes, is available for both single transactions and correlated transactions.

The Call Trace application will help the customer support staff to give top class service to your subscribers with a complete overview of all the calling processes. You will also be able to find reasons for poor statistical values detected in Performance Analyser, or see if there were any disturbances during an alarm in Network Status, etc. Signalling technicians will have access to all the bits and bytes in every calling process and protocol message for deep analysis as well.

A Client Correlation example for the Mobile Packet correlation engine is shown in the following figure:

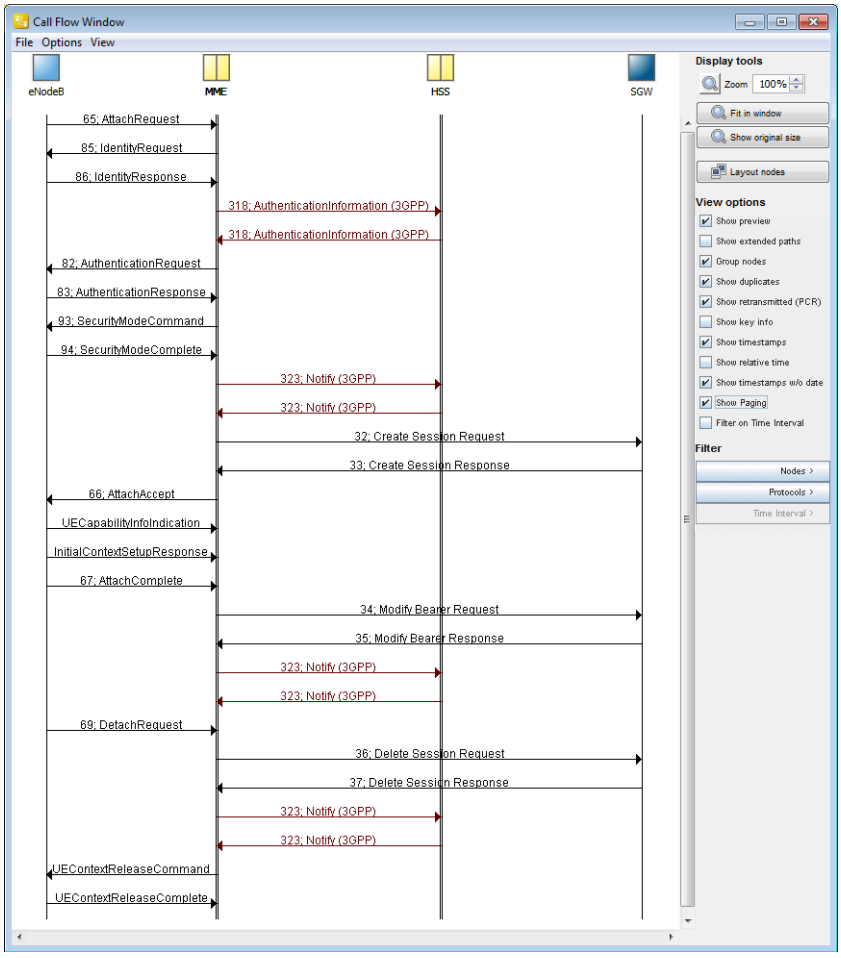


Figure 15: The Call Flow Window for Mobile Packet

The Call Trace application supports numerous protocols for fixed, mobile, IMS, VoIP, and intelligent networks.

4.1.2.1 Customising the interface

The customisation of the interface for Call Trace is the same as for Protocol Analyser. See *4.1.1.1 Customising the interface*.

4.1.2.2 Available parameters

For available protocol parameters for Call Trace, see *15.2 Call Trace*.

4.1.3 Performance Analyser

The Performance Analyser application monitors Key Performance Indicators (KPI) for different transaction groups in real time, which will show you the performance in your network.

For each KPI alarm, thresholds can be set per transaction group.

The following predefined protocol-specific KPIs are available:

- **ASR (Answer Seizure Ratio)** - displays the number of successful call attempts (answered or terminated with a normal release cause) out of the total number of call attempts in per cent. Alarms are generated when the current levels go below the set alarm thresholds. (For ISUP, IUP, BICC, ISDN, SIP, and Iu-CS.)
- **NER (Network Efficiency Ratio)** - displays the number of calls terminated with a normal release cause, user busy, or no answer, out of the total number of call attempts in per cent. Alarms are generated when the current levels go below the set alarm thresholds. (For ISUP, IUP, BICC, ISDN, SIP, and Iu-CS.)
- **NOSC (Number Of Short Calls)** - displays the number of calls with unusually short conversations times out of the total number of call attempts in per cent. Alarms are generated when the current levels go above the set alarm thresholds. (For ISUP, IUP, BICC, ISDN, SIP, and Iu-CS.)
- **Invite performance** - displays the number of invites that have not required any message to be resent out of the total number of invites in per cent. Alarms are generated when the current levels go below the set alarm thresholds. (For SIP.)
- **Register success** - displays the number of successful registrations out of the total number of registrations in per cent. Alarms are generated when the current levels go below the set alarm thresholds. (For SIP.)
- **Register performance** - displays the number of registrations that have not required any message to be resent out of the total number of registrations in per cent. Alarms are generated when the current levels go below the set thresholds. (For SIP.)
- **SMS** - displays the number of successful SMS transactions out the total number of SMS transactions in per cent. Alarms are generated when the current levels go below the set thresholds. (For Iu-CS.)
- **Attach accepts** - displays the number of accepted attach requests out of the total number of attach requests in per cent. Alarms are generated when the current levels go below the set thresholds. (For GPRS and Iu-PS.)
- **PDP activations** - displays the number of PDP activations terminated with Session Management cause 36 (Regular deactivation) out of the total number of PDP activations in per cent. Alarms are generated when the current levels go below the set thresholds. (For GPRS and Iu-PS.)
- **Successful transactions** - displays the number of transactions that have reached end state without any error codes out of the total number of transactions in per cent. Alarms are generated when the current levels go below the set thresholds. (For INAP/CAP.)
- **T1** - displays the number of transactions with a maximum time, defined as T1 by the system administrator, between the Begin message and the Continue, End, or Abort message out of the total number of transactions in per cent. Alarms are generated when the current levels go below the set thresholds. (For INAP/CAP.)
- **T2** - displays the number of transactions with a maximum time, defined as T2 by the system administrator, between the Begin message and the Continue, End, or Abort message out of the total number of transactions in per cent. Alarms are generated when the current levels go below the set thresholds. (For INAP/CAP.)

- **Frequency** - displays the average number of INAP transactions per second. Alarms are generated when the current levels go above the set max levels or below the set min levels. (For INAP/CAP.)
- **Invoke Frequency** - displays the average number of Invokes per second. Alarms are generated when the current levels go above the set levels. (For INAP/CAP.)
- **Time out Frequency** - displays the average number of timeouts per second. Alarms are generated when the current levels go above the set levels. (For INAP/CAP.)
- **Average response time** - displays the average response time between the Begin message and the Continue, End, or Abort message in milliseconds. Alarms are generated when the current response times go below the set thresholds. (For INAP/CAP, MAP and IS-41.)
- **Successful SCCP transactions** - displays the number of transactions that have reached end state without any error codes out of the total number of transactions in per cent. Alarms are generated when the current levels go below the set thresholds. (For MAP and IS-41.)
- **Successful TCAP states** - displays the number of TCAP transactions that do not have any aborts or timeouts out of the total number of successful SCCP transactions above in per cent. Alarms are generated when the current levels go below the set thresholds. (For MAP and IS-41.)
- **Successful TCAP transactions** - displays the number of TCAP transactions that have reached end state without any error codes out of the total number of successful TCAP states above in per cent. Alarms are generated when the current levels go below the set thresholds. (For MAP and IS-41.)
- **Transaction Success Rate**- displays the GTP transaction success rate in per cent. Alarms are generated when the current levels go below the set thresholds. (For GTP.)
- **Response Delay** - displays the delay between a request and a response, for example between a Create PDP request and a Create PDP response, in per cent and in milliseconds. The control signalling affects the value, not the user data. Alarms are generated when the current levels go above the set levels.(For GTP.)
- **User Data Throughput** - displays the min/max throughput downlink (for example when a user is browsing a web page), in per cent and in milliseconds, and uplink (for example when a user is sharing a file), in per cent and in milliseconds. (For GTP.)

The transaction groups can consist of many different parameters, enabling you to pin-point and monitor statistics for an exact type of transaction, originating at certain places, terminating at certain places, containing specific numbers, etc.

Performance Analyser will help you increase your quality of service, since you can instantly see in which areas the performance is going down. This information allows you to reroute the calls, without affecting the customers, while solving the problem.

You also have instant access to the Call Trace and Protocol Analyser applications where filters are automatically set on the parameters the selected group is based on. You can then see if and how the traffic was affected by the alarms.

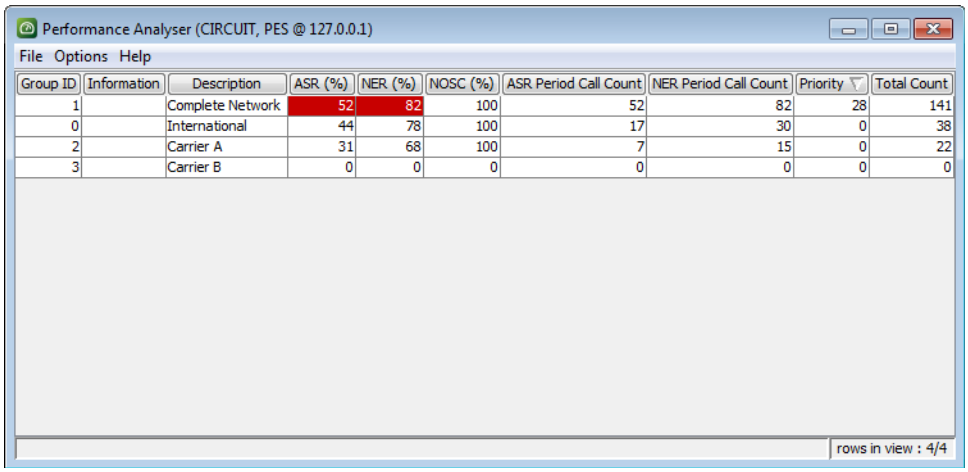


Figure 16: Performance Analyser main window

This application will help you detect problems quickly, and decrease the time required for problem solving. The application is typically displayed on the NOC wall. Alarms can be sent to an internal alarm application, or to third-party alarm management systems using SNMP traps, or as an email message to email receivers.

4.1.4 Mass Call

In the Mass Call application (PSTN only) you can monitor either the number of call attempts made to specific numbers, or made by specific numbers. ISUP, IUP and BICC protocols are supported.

4.1.4.1 Mass Call B Number

Monitoring call attempts to specific numbers will help you see if you need to reroute the traffic, or activate call gapping, for example, when there are massive amounts of call attempts for a TV vote, or to a booking centre for newly released theatre tickets, etc. You will also be able to find errors in routing tables which results in calls that are looping around the network.

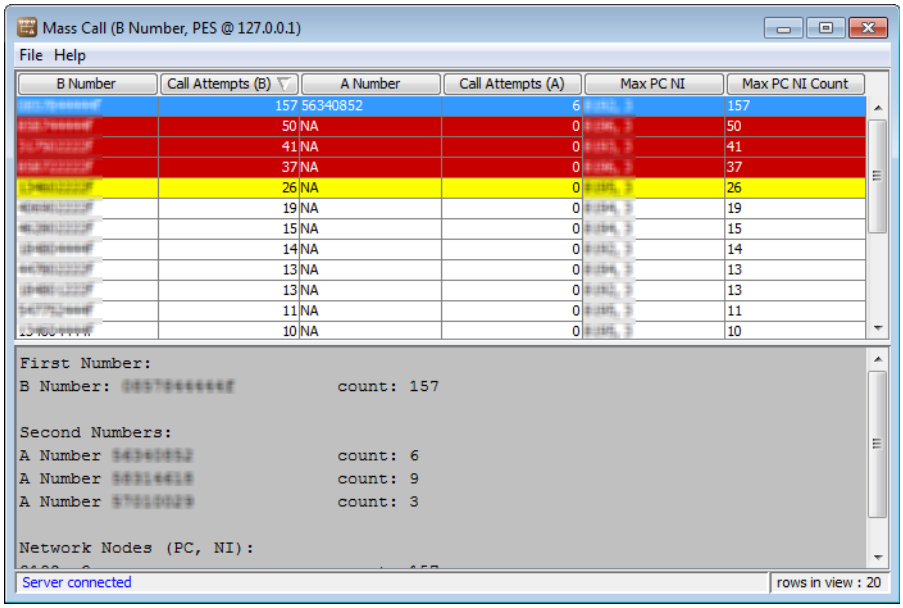


Figure 17: Mass Call B Number

4.1.4.2 Mass Call A Number

Monitoring call attempts made by specific numbers will help you find subscribers that have strange calling patterns, for example, if a dialer has been connected to automatically find free extensions in a corporate switchboard.

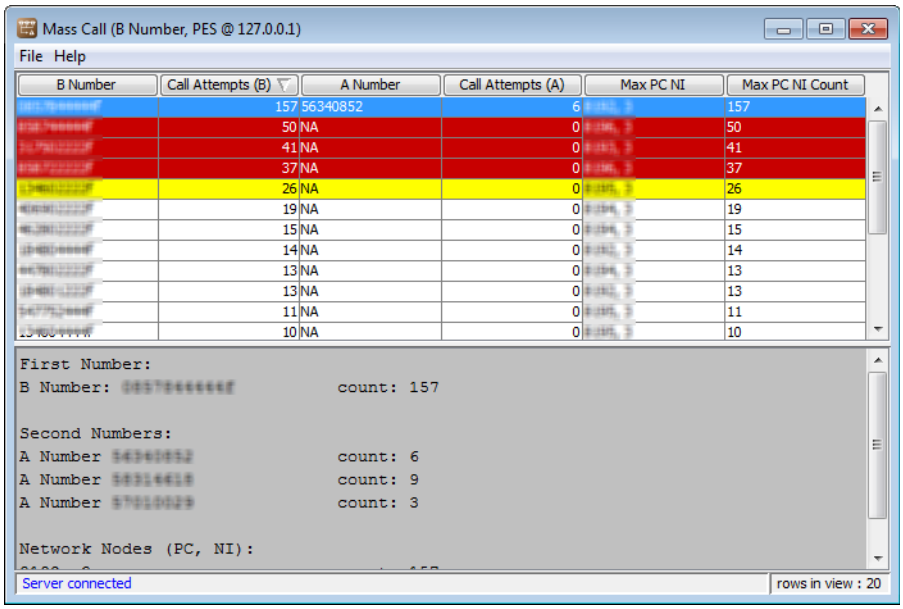


Figure 18: Mass Call A Number

4.1.4.3 Common features

You have instant access to the Call Trace and Protocol Analyser applications where filters are automatically set on selected numbers and/or second numbers/PC NI combinations. You can then see if and how the traffic was affected by the alarms.

This application helps you solve problems before customers are affected by overloaded switches, and stop fraudulent subscriber behaviour. See *10.6 Mass Call* for more information.

4.1.4.4 Specific alarm levels

If there are specific numbers or number sequences that frequently have large amounts of call attempts, specific alarm levels can be applied, which will reduce the number of alarms for these numbers or number sequences.

4.1.5 Real Time Statistics

With the Real Time Statistics application you can set up and view diagrams, or statistical information in table format, over certain types of messages and/or calls in your network in real time. This allows you to immediately detect drops or peaks in the traffic, which need further attention.

Different filter criteria can be set up for the different graphs, based on either protocol messages or calls. Several graphs can also be combined in the same diagram, where each graph has its own designated colour for easier identification.

When setting up the diagrams, you select if you wish the graph to be based on messages or calls, and then you can apply different filter settings:

- **Traffic group filter** – Messages/calls passing the links in the selected traffic group(s) will be counted.
- **Protocol filter** – Messages/calls for the selected protocol(s) will be counted.
- **Link filter** – Messages/calls for the selected link(s) will be counted.
- **Parameter filters** – Messages/calls matching the set parameter values (settings for wildcards, ranges, non-existent parameters, etc., can be used) will be counted.

You can also select to open filters that you have saved in the Protocol Analyser or Call Trace applications and re-use them in the Real Time Statistics application, which also means that all the parameters available for filtering in Protocol Analyser and Call Trace, are also available for filtering in Real Time Statistics.

Once the filters are set, and you select to view the diagram, the graphs will display the number of messages/calls passing the filter settings in real time. The graphs are updated with the time resolution of your choice.

All filter settings can also be saved and used at a later time, or shared between colleagues.

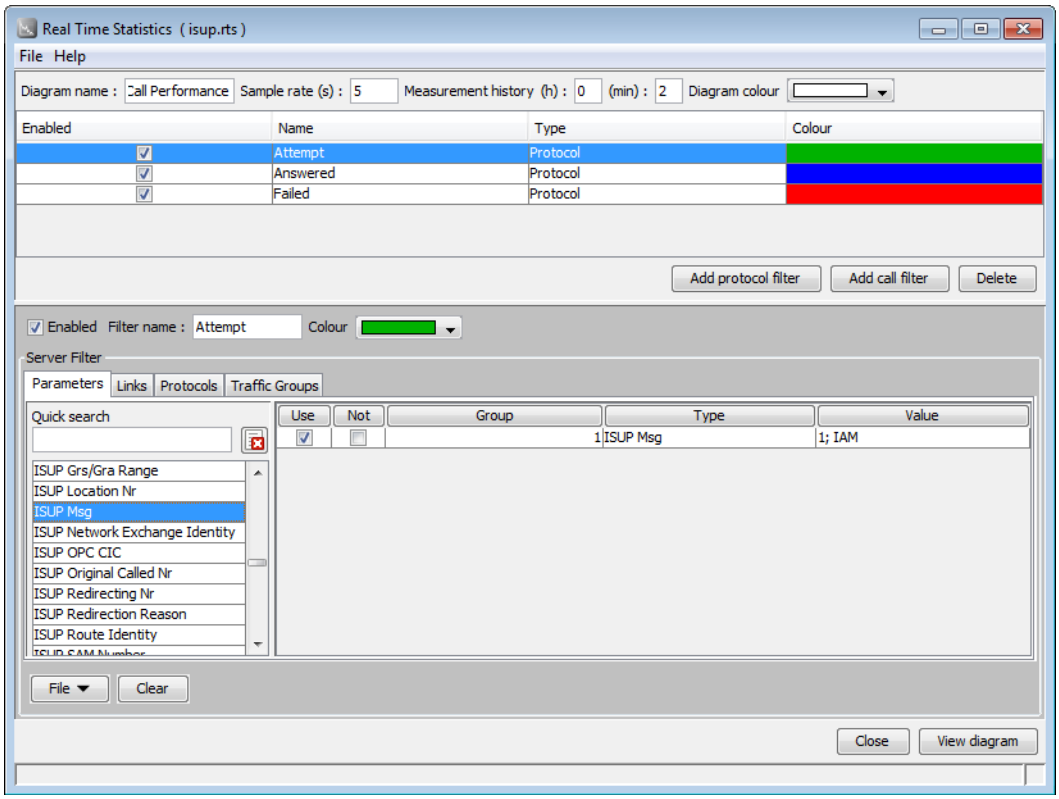


Figure 19: Real Time Statistics main window

An example of a diagram in Real Time Statistics is shown in the following figure:

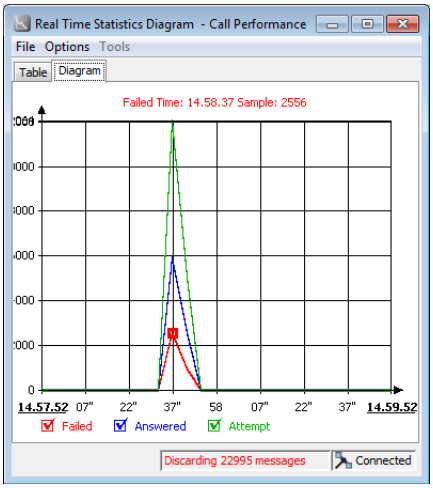


Figure 20: Diagram example in Real Time Statistics

4.1.6 Network Status

The Network Status application monitors alarms on MTP1 level, MTP2 level, MTP3 level, and on high link load, poor performance, large amounts of call attempts, and alarms generated by certain types of messages or transactions, and displays them in a user interface, which allows you to acknowledge and clear the alarms, as well as search for similar alarms throughout your network.

You also have quick access to the Call Trace and Protocol Analyser applications, where you can then see if your subscribers were affected in any way by the alarms.

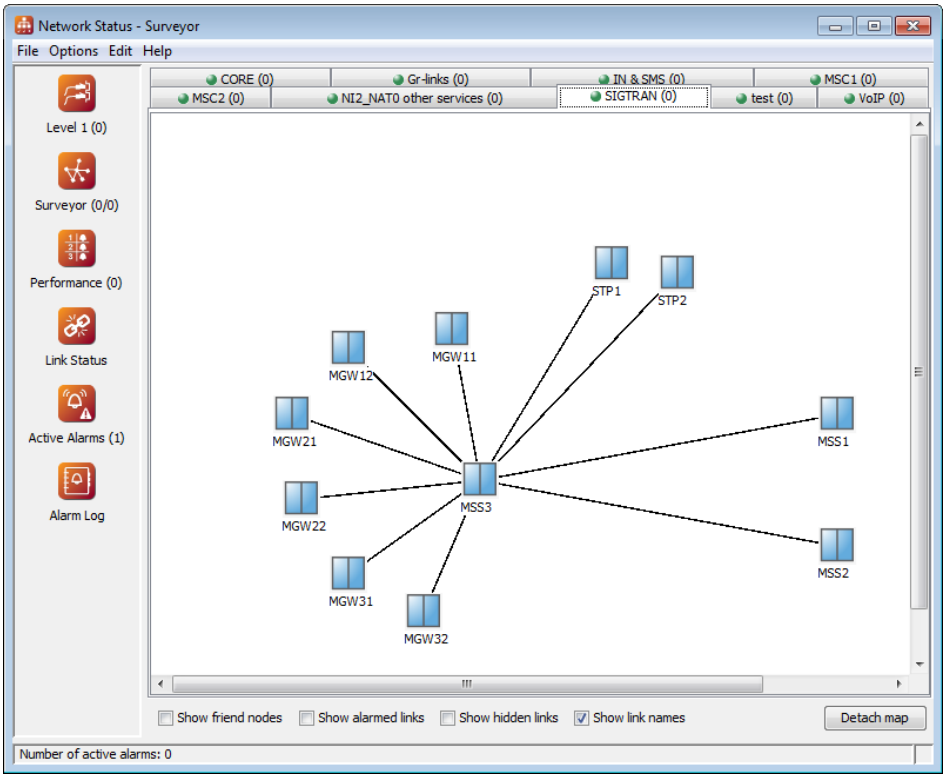


Figure 21: Network Status Surveyor view

This application will help you detect problems quickly, and decrease the times for problem solving.

4.1.7 Statistics Alarm

In the Statistics Alarm application you can set up different filter criteria which will generate alarms if they are met. For example, you can set up a filter on B Number equals 555 55 55. As soon as a protocol message, or call, with B Number 555 55 55 is detected, an alarm is generated. You can also set filters to generate alarms when you have calls with a certain duration, or if you have more than 500 IAM messages per minute, etc. All filter options included in the Protocol Analyser and Call Trace applications are available.

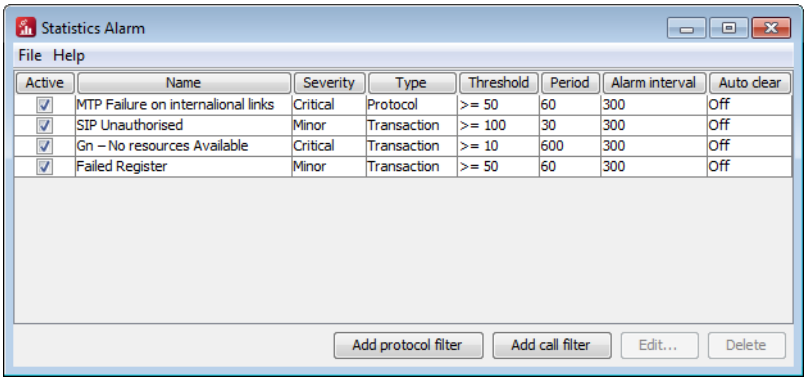


Figure 22: Statistics Alarm main window

4.1.8 Packet Recorder

The Packet Recorder application offers the ability to record all user data for any given subscriber and/or interface, be it packet data sessions in the mobile core or RTP streams in the IMS or CS network. This enables troubleshooting of complex network or subscriber problems that require the full content of the user plane data to be analysed, in addition to the control signalling.

The Packet Recorder application is run in a web GUI that supports Chromium. Packet streams are stored locally on a MediaProbe based on a capture filter defined by the user. Streams can be set to capture a fixed volume of data or as sliding window storage, where the oldest data is continuously replaced by newer data. The data can be exported in PCAP format for offline processing or decoding in Wireshark.

The application is available in two versions:

- Packet Recorder – GTP

  GTP-U data based on an IMSI filter. The following interfaces are supported:

  - S1U
  - S5
  - S8
  - Gn
  - Gp
  - N3
  - N9

- Packet Recorder – RTP

  RTP data based on an IMSI and/or MSISDN filter. The following interfaces are supported:

  - A
  - Iu-CS
  - Gm (VoLTE access)

4.2 OSIX web client

The OSIX web client uses the same data as the desktop client.

The benefits of the OSIX web client is a simplified centralised deployment, which makes for smoother update and maintenance handling. Also, no specific user software is required apart from a compatible browser.

4.2.1 OSIX xTrace

In the web client, the Call Trace and Protocol Analyser applications have been merged into one application called OSIX xTrace. In OSIX xTrace, the user can easily transition between session and message searches by changing mode.

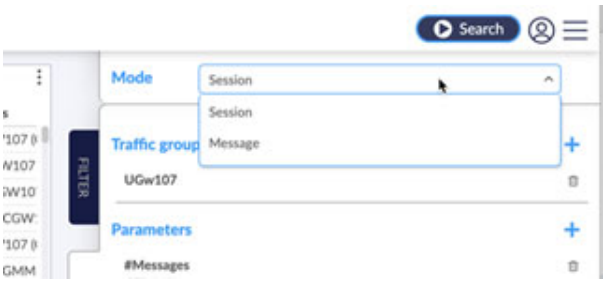


Figure 23: Modes

As in the desktop client, the user can search and filter on data, and view binary data and flow charts. Client correlation is also available.

The applied filters and settings are stored in the web application for easy access and sharing with colleagues.

4.2.1.1 Layout

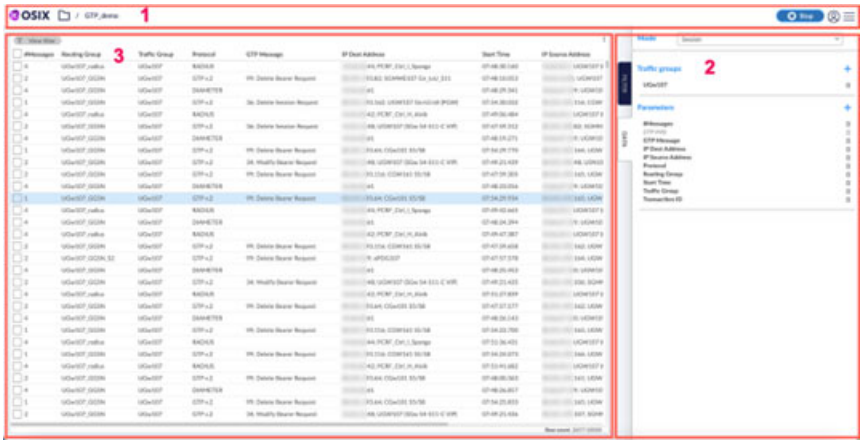


Figure 24: Layout

- Top bar (1)

Use the top bar to select templates, initiate searches, display user information, and navigate.

- Settings tabs (2)

With the tabs on the right-hand side, the user can define which data to search for by applying filters and selecting a desired time window. By clicking the tabs, the user can navigate between the settings, and by clicking the active tab hide the right-hand section, giving more space to view the data.

- Data window (3)

This area displays the data widgets, where the user can interact with the data and refine/filter it further. From here, the user can also drill deeper into the details.

One difference between the desktop and web clients is that for the latter, only the data displayed in the table is fetched from the OSIX Processing layer. The advantage of this is, that the fetching of data is quite fast and does not exhaust the client memory. On the other hand, when drilling down to details, the relevant data must be fetched again. This means that the user must define which parameters to view before fetching the data to the table, as adding additional parameters requires fetching all the data again.

4.2.1.2 Filters

There are five different types of filter:

- **Traffic Groups** and **File** – The network links are divided into one or more traffic groups, and at least one traffic group must be selected before you can start monitoring messages. It is also possible to import a msgs file by selecting File.
- **Historical/Relative** and **Reatime** –The historical filter is used for viewing calling processes historically, that is, from a certain time interval and with a certain duration. An historical search will filter out all messages that do not fit in the time period selected in the search filter. Realtime, on the other hand, will stream new data from the time the trace is started.
- **Parameters** – You can set a filter on any parameter value visible in the main window. The quickest way to do this is to right-click the value and add it to the filter. This filter type also allows you to exclude messages with specific values.
- **Protocols** – If more than one protocol is running, you can easily choose to only view messages of a certain protocol type.
- **Duration** – You can filter on *Total duration* or *Conversation duration*.

4.2.1.3 Data filter and view filter

Another difference between the desktop and web clients is that in the web client, the parameters defined on the data tab can be applied when building data filters, that is, the filter applied when fetching data from the OSIX processing layer. Multiple data filters can be created and stored in the same template, and later edited and renamed, if necessary. The filters are applied individually—simply select the desired filter in the drop-down menu. (As more filters are created, the list will grow.)

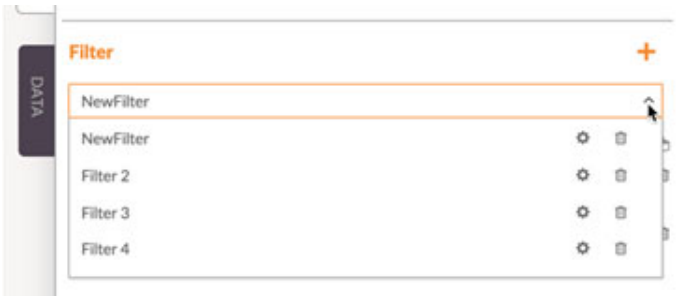


Figure 25: Filters

A view filter is a filter that is based on the data already loaded to the web client, that is, it requires no new query to be executed. A view filter can also be transferred to the data filter setting and saved for later use. But if only applied as view filter it will not be saved to the template.

4.2.1.3.1 Setting parameters manually

The user can manually add filters by clicking the + icon. A new row is added where the user can select parameters and enter the desired values. By adding multiple rows, several filter values can be set. Make sure the toggle button is set to edit mode (the pen icon) to enable editing of the filter parameters, values, and operands.

Figure 26: Manual parameters

4.2.1.3.2 Setting parameters using the data table

If data is present in the table, the user can also apply the value directly to the data or view filter using the click menu.

Figure 27: Data table parameters

4.2.1.4 Session and message details

When a session or message has been identified, the corresponding messages and details can be reviewed by simply clicking the desired session or message. The same work flow applies when opening a single message. Multiple messages can be opened and reviewed in the same window, by selecting their respective check boxes.

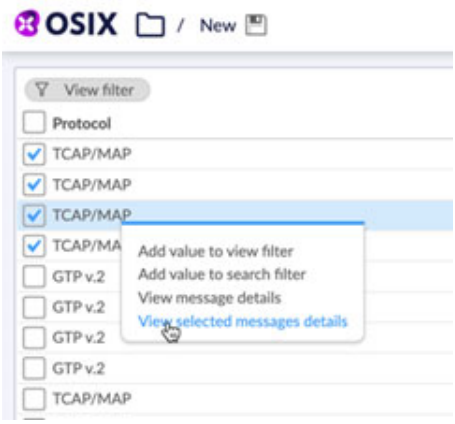


Figure 28: Session details

The detail view opens in a new browser tab. The user can easily toggle between the table and flow chart views. Currently, hex and ASCII data representations are not available.

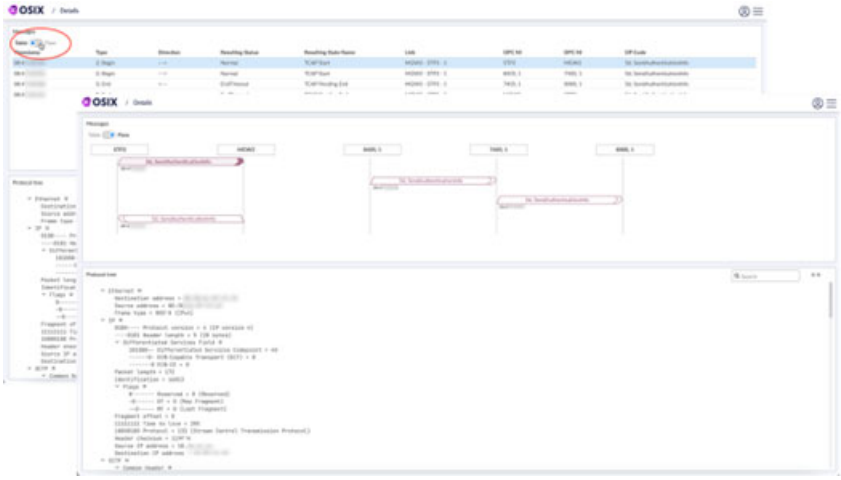


Figure 29: New tab

When viewing a session(s) or message detail, there is a feature available to compare messages (up to three at a time) with one-another. In this feature, there is also a diff function included.

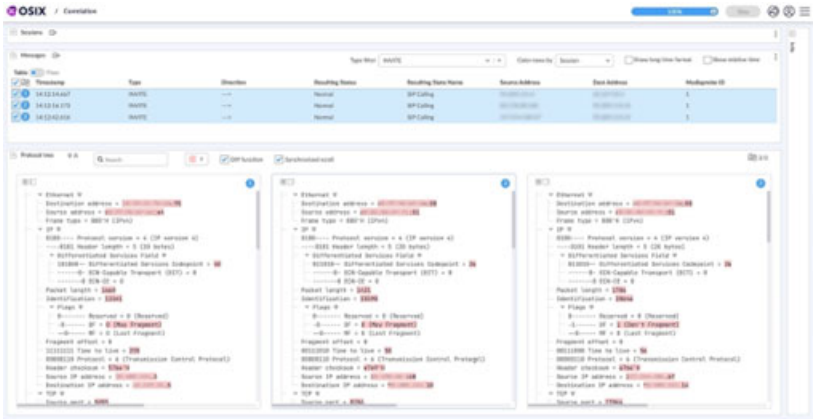


Figure 30: Comparing messages

Sessions that contain RTP aggregates will also allow users to visualise the MOS score (LQ and CQ) throughout a call in both directions. This can be found on the RTP Media tab. After a point in time is selected, the summary of the corresponding aggregates are presented on the right-hand side. The user can then identify which of the aggregates is of interest, and the detailed data will be presented in the protocol tree. (The data of this feature are highly dependent on the sampling frequency.)

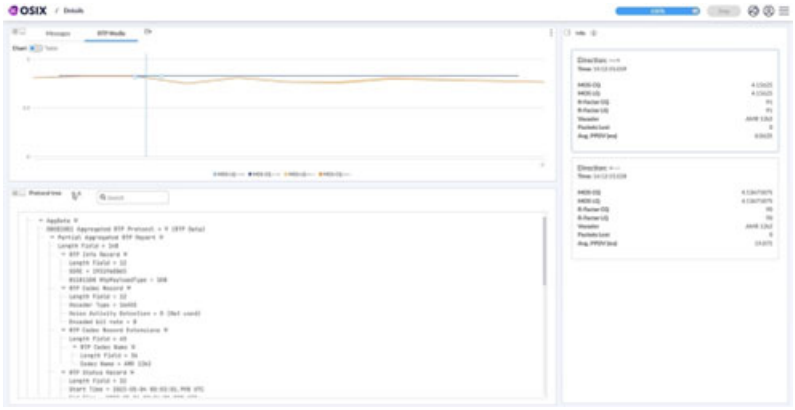


Figure 31: RTP media plotting

4.2.1.5 Call correlation

The user can perform call correlations in the same way the desktop client performs client correlations. Currently, four correlation options are available, where the Combine option corresponds to the Manual correlation option in the desktop client. In the web client, a session representation is included, enabling the user to select or deselect sessions to review.

Note that the call correlation for the web client takes place in the TDM/TDR, and not in the actual client, as is the case for the client correlations in the desktop client.

The correlation result is opened in a new browser tab that displays the sessions (1), a list/flow chart of messages related to the selected sessions (2), and the protocol tree (3).

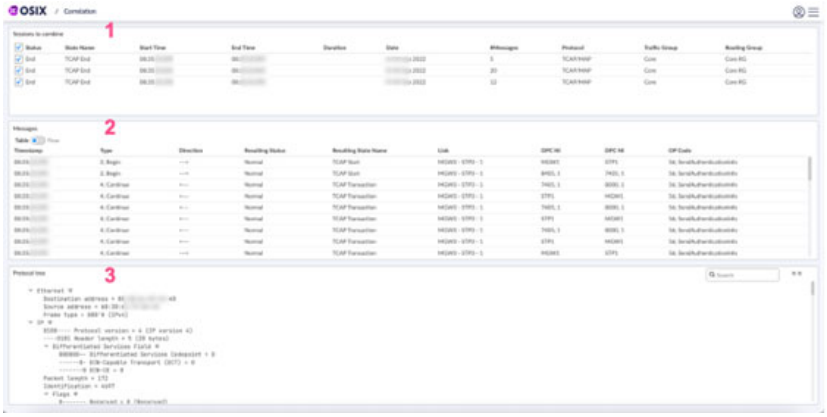


Figure 32: Correlation

4.2.1.6 Templates

The OSIX web application stores user settings and filters in templates. This enables the user to quickly pick up and continue work at a later time, and also share the work with colleagues. The user can select whether a template should be private (only viewable for the specific user) or public (accessible by all). Only the template creator or a template admin can delete public templates.

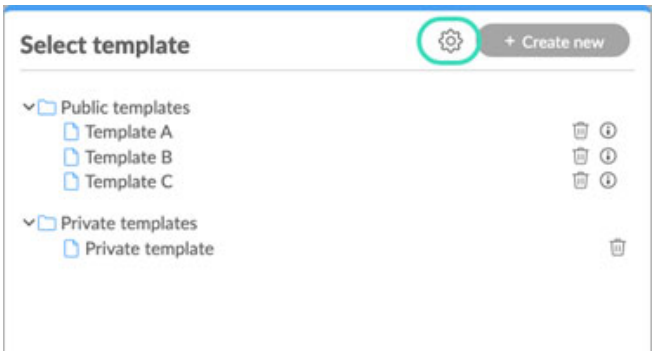


Figure 33: Templates

For template administrators, there is a specific template management view.

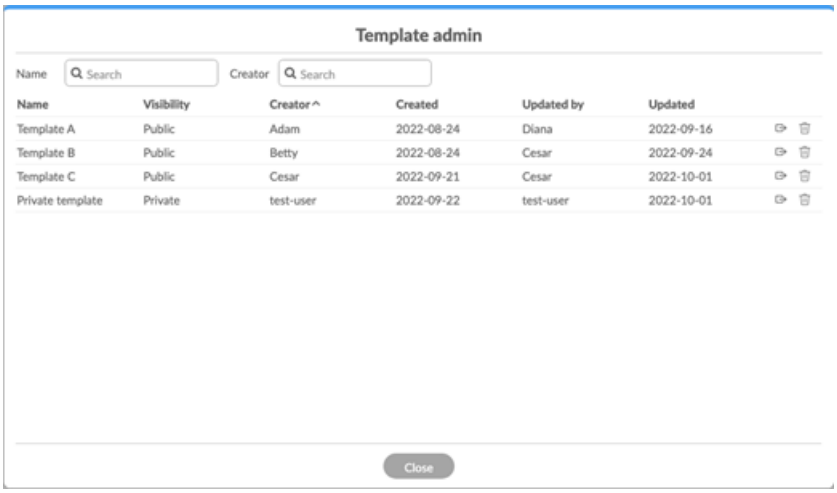


Figure 34: Template management

4.2.1.7 xTrace Live Graph

A similar feature that is available in the desktop client is called Realtime Statistics, where the user can include the Live Graph widget in a template. This allows for realtime volume measurement based on one or more filters. In OSIX xTrace, one template can host several Live Graph widgets. Each widget can be controlled independently or via the global Play button.

From the Live Graph widget, users can open corresponding trace data and fetch the underlying data for a deviating value.

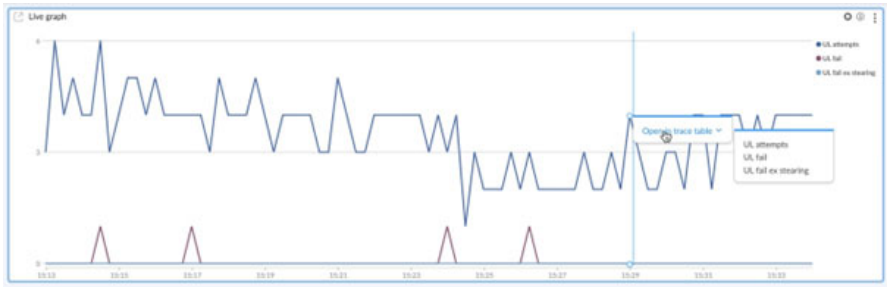


Figure 35: xTrace live graph plotting

4.3 SOS (Storage of signals)

With the SOS functionality you can view calling transactions and protocol messages historically.

Each Probe Server (PRS) has an SOS database which stores all the signalling data tied to a call. The storage time is very flexible, and can be configured per PRS and protocol. The number of days you store data in SOS is freely configurable. However, you must have enough servers to handle the amount of data.

In SOS, all messages in the full calls as seen in Call Trace are stored in binary format. To speed up the search, the Call Search Engine (CSE) is used. The CSE contains a number of columns for parameters that links to the calls stored in SOS. A column in CSE guarantees a quick search of the data stored in SOS.

When data is cleared from SOS, the CSE columns can still be stored to display transaction entries with limited information. See chapter *16 SOS columns*, for available parameters that are supported for CSE.

During an historical search, the client selects a time interval from which to view calling transactions or protocol messages. The data is then fetched by the client from the SOS databases on each PRS and displayed in the Call Trace and Protocol Analyser applications. The transactions and messages are displayed in the same way as when running the applications in real time, with the same filtering functionality, quick access to details, etc.

4.4 xDR generator

The PRS generates xDRs, used internally and/or externally. An xDR is generated when the call closes, but can also be generated during a call (partial xDR). These xDRs can be exported in true real time to, for example, your Fraud Management System. This means that you can detect fraud even prior to connection, and you are not limited to the static and restricted xDRs from the network elements.

The OSIX system always delivers 100% of the xDRs in whichever formats and states you desire, while the xDRs delivered by the network elements often might be incomplete.

In the system, you can configure several different xDR generators, with different formats and filters (that is, you can decide to generate xDRs when certain filter criteria are met) and send them to different ports on different IP addresses.

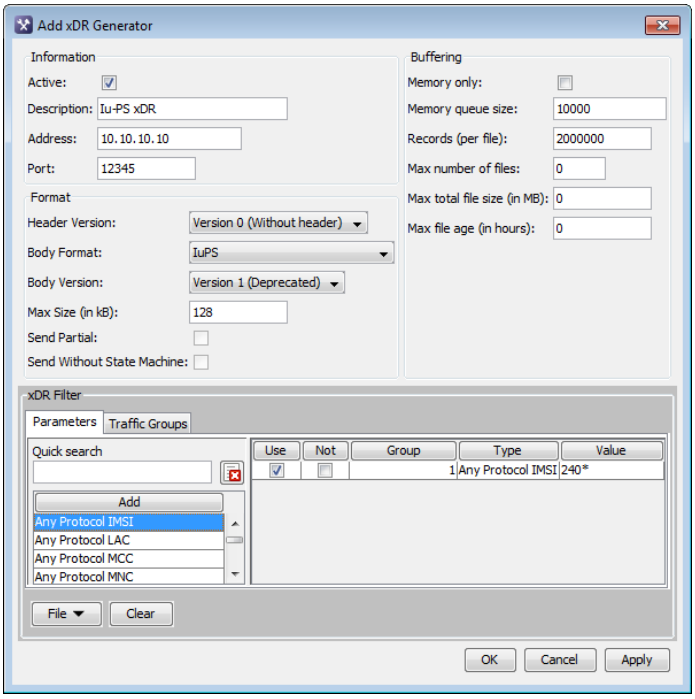


Figure 36: xDR Generator example

4.4.1 xDR interfaces

The xDR generation has three main interfaces towards third-party systems: pure socket (real time), file server (near real time), and database (near real time).

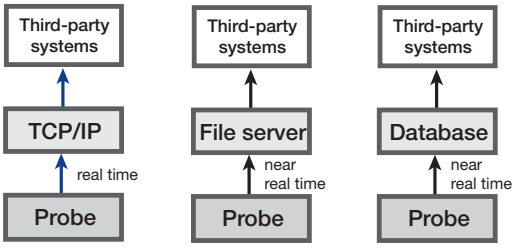


Figure 37: Interfaces to third-party systems

4.4.1.1 Pure socket

xDRs are sent in a binary stream according to the specified xDR format. The third-party system must be able to read data from the socket at the same speed as OSIX sends data. If the third-party system is too slow, or disconnects, a backup functionality is activated.

4.4.1.2 File server

With the file server interface, OSIX uses a disk saver application that saves xDRs to disk according to the specified format. xDRs are stored in sequence, and there is no extra header inserted between the xDRs.

4.4.1.3 Formats

The xDRs can be delivered in several different formats, and for several different purposes and protocols simultaneously.

4.5 SNMP

The OSIX system provides SNMP functionality which can be used to send network alarms to other systems, for example Network Management Systems.

Currently, the following events can trigger SNMP traps to be sent.

Note: The listing follows the Configuration Manager Category ID order.):

Layer 1 OK	ICMP Source Quench	Statistic Alarm (clearable)
Loss Of Signal	ICMP Time Exceeded	Probe Connection OK
Loss Of Frame Alignment	ICMP Parameter Problem	Probe Connection Broken
Loss Of Multi Frame Alignment	Diameter Disconnect-Peer	Sigtran Destination Unavailable
Remote Alarm Indication	Diameter CE Error	Sigtran Destination Available
Alarm Indication Signal	Diameter CE Success	Sigtran Signalling Congestion
Severe Error Handling	Diameter CE Timeout	Sigtran Destination User Part Unavailable
Remote Defect Indication	Diameter DW Error	Sigtran Application Server Up
Loss Of Pointer	Diameter DW Timeout	Sigtran Application Server Down
Out-of-Cell Declination	Circuit ASR Alarm	Sigtran Heartbeat failure
Loss-of-Cell Declination	Circuit NER Alarm	Sigtran Heartbeat failure clear
In Service	Circuit NOSC Alarm	Sigtran SCTP link inactive
Out Of Service	Mass Call Alarm	Sigtran SCTP link inactive clear
Processor Outage	Gprs Attach Alarm	Sigtran M2UA link release
Congestion	Gprs PdpActivate Alarm	Sigtran M2UA link release clear
No Signal Units	INAP Successful Transactions Alarm	Sigtran M2UA link congestion
Link Limit Exceeded	INAP T1 Alarm	Sigtran M2UA link congestion clear
Link Limit Exceeded Cleared	INAP T2 Alarm	Sigtran Signalling Congestion clear
Transfer controlled	INAP Min Transactions Alarm	Sigtran M2PA link in service
Transfer prohibited	INAP Max Transactions Alarm	Sigtran M2PA link out of service
Transfer restricted	INAP Invoke Frequency Alarm	Sigtran M2PA link processor outage
Transfer allowed	INAP Timeout Frequency Alarm	Sigtran M2PA link congestion
Route-Set-Test Timeout	MAP SCCP Alarm	Sigtran M2PA link congestion clear
Link inhibit	MAP TCAP State Alarm	Point codes Not Monitored
Link uninhibit	MAP TCAP Success Alarm	Disk usage high
Linkset available	MAP Response Time Alarm	Disk usage high (clear)
Linkset unavailable	IS41 SCCP Alarm	Disk usage turned off
Node available	IS41 TCAP State Alarm	Disk usage turned on
Node unavailable	IS41 TCAP Success Alarm	Gemini Cell Rate Limit
Subsystem allowed	IS41 Response Time Alarm	Gemini Cell Rate Limit Cleared
Subsystem prohibited	SIP ASR Alarm	Gemini Drop Rate Limit
Subsystem congested	SIP NER Alarm	Gemini Drop Rate Limit Cleared

Gprs Traffic Unavailable	SIP NOSC Alarm	Gemini Mem High Limit
Gprs Traffic Available	SIP Invite Performance Alarm	Gemini Mem High Limit Cleared
Gprs BVC Unavailable	SIP Register Success Alarm	Gemini Mem Low Limit
Gprs BVC (0) Unavailable	SIP Register Performance Alarm	Gemini Mem Low Limit Cleared
Gprs BVC Available	Iu CS ASR Alarm	Gemini Load High
Gprs Linkset available	Iu CS NER Alarm	Gemini Load High Cleared
Gprs Linkset unavailable	Iu CS NOSC Alarm	MediaProbe Memory In Use High
Gprs BVC (0) Available	Iu CS SMS Alarm	MediaProbe Memory In Use High Cleared
Gprs NSVC Blocked	Iu PS Attach Alarm	MediaProbe Disk Usage High
Gprs NSVC Unblocked	Iu PS PDP Activate Alarm	MediaProbe Disk Usage High Cleared
Gprs NS Reset	GTP Min Throughput Down Alarm	MediaProbe Dir Usage High
Gprs NS Reset Clear	GTP Min Throughput Up Alarm	MediaProbe Dir Usage High Cleared
Gprs NSEI Unavailable	GTP Max Throughput Down Alarm	MediaProbe Received Packaged
Gprs NSEI Available	GTP Max Throughput Up Alarm	MediaProbe Received Packaged Cleared
Gprs NSVC Unavailable	GTP Response Delay Alarm	MediaProbe Received kB
Gprs NSVC Available	GTP Success Level Alarm	MediaProbe Received kB Cleared
ICMP Destination Unreachable	Statistic Alarm (single)	
ICMP Redirect	Statistic Alarm (counter)	

5 Security

A service assurance solution must be designed to reduce risk and protect from the cyber security threats facing the industry. While OSIX must always be deployed behind firewalls and never be exposed to the internet, it is designed following defence in depth principles. As an integrated part of the development process, a design for security guideline is applied. The guideline is based on best practices from the OWASP and ensures that prevention is implemented against threats such as those listed in the OWASP top 10.

5.1 Operating system and hardening

All servers in the OSIX system are provisioned with the AlmaLinux or RHEL operating system. Please note that Elisa Polystar does not support a delivery model where the operating system is provided by the CSP.

All OS installation is performed from a version-controlled staging environment, which ensures consistent quality and configuration across the installed base.

To reduce vulnerability to an ever increasing amount of cyber attacks, services and servers need to be hardened. Hardening is a unique security task that aims to reach a high level of security defence. As part of the deployment process, Elisa Polystar performs hardening scans for every major release, using a battle-test security tool for hardening the Linux OS. Elisa Polystar performs an extensive health scan and compliance testing against security best practices, such as CIS benchmarks, NIST and NSA, thus identifying current deviation and gaps. Elisa Polystar uses the CIS benchmarks as reference and a source for hardening to comply with regulations and common standards on the market.

Hosts/VMs in the OSIX system are continuously updated with strengthened hardening, based on deviation results along with other improvements and recommendations identified, at every upgrade occasion of the OSIX system.

OSIX servers are hardened using security hardening. Security hardening is applied on new servers before shipment to the customer and on servers in the field, through the standard OSIX upgrade process.

The following changes are done in a security hardening configuration:

- **Audit**
  - Set auditd buffer to 8192
  - Track sudo usage with -S execve -F euid=0
  - Watch the /etc/group, /etc/passwd, /etc/gshadow, /etc/shadow, /etc/security/opasswd, /etc/issue, /etc/issue.net, /etc/hosts, /etc/hostname, /etc/sudoers (and .d folder) files
  - Watch unsuccessful attempts to control permission modification
  - Watch unsuccessful file access
  - Watch deleted files and programs
  - Make auditd configuration immutable
  - Enrich the logs to add in user names
  - Set auditd to be lossless
- **Authentication**
  - Enable logging of failed login attempts
- **Banner**
  - Legal banner added for login prompt (/etc/issue & /etc/issue.net)

- **Disabling use of the following file systems**
  - sqashfs
  - udf
  - cramfs
  - hfs
  - freevxfs
  - jffs2
  - hfsplus
- **DNS (named service)**
  - Hide BIND version
  - Zone transfer disabled
- **Firewall**
  - Firewall is ensured to be up to date
  - A whitelist port list of both UDP and TCP ports (ports needed for product to work with possibility to add customer specific ports)
  - ICMP echo and reply is allowed
  - Disable ZoneDrifting
  - If traffic does not match the rules, the traffic will be dropped
- **Fstab**
  - Hardened /dev/shm with options "nodev, nosuid, noexec"
  - Hardened /boot with options "nodev, nosuid, noexec"
  - Hardened /proc with option "hidepid=0"
- **iLO**
  - In the case of a physical HP server, IPMI over LAN gets disabled
- **NTP service**
  - Restrict queries over ipv4 with "restrict default kod nomodify notrap nopeer noquery"
  - Restrict queries over ipv6 with "restrict -6 default kod nomodify notrap nopeer noquery"
  - Disable monitor
- **Postfix**
  - Removed disclosure of sensitive information in the SMTP banner
- **Reboot**
  - Reboot through ctrl+alt+delete is disabled
- **sshd config**
  - Disable root login via ssh
  - Instruct ssh client to perform client alive check after 36 hours
  - Instruct ssh client alive check to terminate session without sending alive message to client
  - Set AllowAgentForwarding to "no"
  - Set MaxAuthTries to "3"
  - Set UseDNS to "no"
  - Limit ssh acceptance to protocol version 2
  - Disable CBC ciphering
  - Limit Kex algorithms
  - Limit MAC algorithms
- **Storage**
  - Disable use of usb storage for all users
  - Disable use of firewire for all users
- **sysctl config**
  - Set kernel.dmesg_restrict to "1"
  - Set net.ipv6.conf.all.accept_redirects to "0" if possible
  - Set net.ipv6.conf.default.accept_redirects to "0" if possible
- **USBGuard**
  - Default policy is applied to USBGuard (USBGuard is installed from staging 6.5.0)

- **Mount options**
  - /var/log has nodev, nosuid, noexec and acl flags
- **Privilege escalation**
  - su binary is blocked through pam configuration
- **sysctl**
  - ICMP redirects are blocked
- **SSH**
  - MaxStartups has been set to 10:30:60

5.2 Platform update strategy

Security-related maintenance of servers in production is handled through OS channel releases, which are separated from releases of OSIX. OS channel releases are based on the latest snapshot from RedHat or AlmaLinux communities. The releases are published according to a pre-defined schedule three times per year, with additional releases in case of critical vulnerabilities. The availability of the OS channel releases is subject to the respective support agreement and to the Polystar Premium Security Service (PPSS).

5.3 Application security

Several prevention mechanisms against typical cyber security threats are implemented in the Elisa Polystar applications.

OSIX uses prepared statements for SQL injection prevention. In this way, user input can never translate to an SQL statement that causes unwanted reading or modification of database contents. OSIX further uses the Angular framework and its built-in protection against cross-site scripting, based on input sanitisation and HTML escaping.

Session tokens are handled in a way that offers full CSRF and XSRF protection. No cookies are used for tracking purposes.

URLs never contain sensitive information or session IDs, and never show data in clear. Transfer of sensitive data is always performed via the HTTP POST method. Secret URL parameters that cause specific behaviour or elevated privileges are never used.

ActiveX controls and applets are not used.

The policy mechanism HTTP Strict Transport Security (HSTS) is enabled in the OSIX web interface.

Service usage is limited to only the subset of clients where it should be used. For example, the DNS used by the Global Function responds only to clients included in its predefined ACL.

5.4 Encryption of data in transit and TLS certificates

The interface between the OSIX web client and the server is encrypted using HTTPS/TLS 1.2. TLS 1.2 is also used to protect some sensitive internal interfaces within the OSIX system. Accepted cipher suites are those using AES encryption with GCM from the "Intermediate" configuration according to Mozilla's recommended configurations for servers using TLS. All these ciphers use SHA-256 or SHA-384. The key exchange method ECDH (with 256 bit key length) is preferred, but any method is accepted. However, if DH is used, the key exchange setting is set to 2048 bits. TLS 1.0/1.1 and SSLv3 are completely disabled. Data sent over TLS is not compressed. Truncated HMAC extension is not used. Session resumption is supported.

See the *System architecture* chapter for more information about encryption on internal interfaces.

For the OSIX web interface, a trusted certificate is used. OSIX is shipped with a certificate for the `polystar.net` domain, which can be used as a local domain within the CSP network. As an alternative, the CSP can deploy OSIX on a domain of its choice, installing its own certificate.

For internal interfaces, internally trusted certificates are used. These are generated using our private CA, located on the Global Function. The root certificates are unique per installed system. All certificates can be regenerated in case of suspected compromise.

5.5 User management

Elisa Polystar has two recommended authentication models, referred to as Polystar authentication and Active Directory authentication. With either of these options, a user can log in to any product with the same password, which is stored in one place. This also means that the user only needs to change the password in one place. Another benefit of this feature is that functionality that spans multiple products, for example Drill Down to Call Trace, will not suffer from a potential mismatch of passwords between products.

The information in the following sections is valid for systems configured to use Polystar authentication or Active Directory authentication.

5.5.1 Polystar authentication, password policy and management

Using Polystar authentication, the user database resides within the OSIX system and the Access Manager component. Passwords are handled within Access Manager. The following password policy is implemented:

- Password must be between 8 and 50 characters long.
- Password must not be the same as the user name.
- Password may contain any combination of UTF-8 characters.
- Incremental timeout at repeated failed login attempts is implemented.
- Sessions are automatically expired after 12 hours.
- Change of password requires the user to repeat the current password.
- Pasting of password is permitted in order to support vault solutions and automatic password completion.
- Users can optionally be required to change their password before logging in the first time.

Stored passwords are salted and encrypted according to the "Password Based Key Derivation Function" using HmacSHA512.

5.5.2 Active Directory authentication

With Active Directory authentication, the Access Manager component is integrated with a CSP's Active Directory. Microsoft Active Directory for MS Server 2008 and 2012 R2 are supported. Standard LDAP (plain text) and LDAPS (encrypted) are supported. Permissions for OSIX and OSIX Data NBI API can be assigned from the Active Directory on user or group level. Active Directory authentication and Polystar authentication can coexist in the same system for different user groups. Both Azure Entra and Active Directory integration cannot be enabled simultaneously.

5.5.3 Azure Entra authentication

With Azure Entra authentication, the Access Manager component is integrated with a CSP's Azure Entra tenant, hosted by Microsoft. This enables Single Sign-On (SSO) in OSIX Web. Permissions for OSIX Web can be assigned on group level (user level integration is not supported). Azure Entra authentication and Polystar authentication can coexist in the same system for different user groups. Azure Entra and Active Directory integration cannot both be enabled simultaneously.

5.5.4 Access control

OSIX and OSIX Data NBI API use role-based access control. A number of pre-defined roles are included and custom roles can be defined based on individual permissions. The design follows the principle of least privilege. New users and roles are per default given no permissions.

5.5.5 Personal system accounts

Personal system accounts are mandatory starting from release 10.0. This means that authentication and access control for OS-level and database access needed by system administrators is also controlled by Polystar or Active Directory authentication.

If the system goes through partial hardening process, the base users of the system get locked down so they cannot be used normally. This is done by removing /bin/bash as a shell for those users.

5.5.6 Locked MySQL shell

The default behaviour of certain packages has been modified from the standard base configuration. Specifically, the shell has been removed for the MySQL user on servers where MariaDB server is installed.

5.5.7 OSIX product level authentication

Using OSIX product level authentication, OSIX user accounts are handled independently. For such accounts, a configurable password expiry timer is supported. Password policy settings such as minimum length, uppercase/ lowercase letters etc. are supported. It is possible to block the login of users after a configurable number of failed login attempts. Session supervision is supported in the form of a configurable user inactivity timer and the ability for a system administrator to log off users.

The stored passwords are encrypted with the SHA-1 algorithm.

5.5.8 OSIX Radius authentication

Radius is a protocol to authenticate remote users to a dial-in access server. OSIX sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the link-layer protocol. In turn, the NAS sends a Radius Access Request message to the Radius server, requesting authentication to grant access via the Radius protocol.

OSIX has the ability to interrogate one or more RADIUS servers and use local authentication if RADIUS fails.

5.5.9 Inactivity timer

An optional timer can be activated that will automatically log out users that are inactive in the system for too long. By default, this timer is turned off. This feature is only available in xTrace.

5.6 Audit logging

OSIX is designed to protect the privacy and personal data of the subscribers in the monitored networks. A key component in this design is audit logging. Through audit logging, all actions of users of the OSIX system are logged, so that any illegal access to personal data can be detected and handled.

The audit logging solution is based on the assumption that the customer has a centralised logging system, to which logs are sent directly from the applications and OS components. This architecture avoids risks related to tampering of local log files and miscellaneous vulnerability exploits.

Two kinds of audit logs exist. Application logs contain user activities within the Elisa Polystar applications. OS logs contain user activities on OS level. The OSIX systems can send audit logs in a number of formats. For application logs, the following formats and transport protocols are supported:

Format	Transport protocol
syslog	UDP, TCP, TCP/TLS
gelf	HTTP, HTTPS over TCP
splunk	HTTP, HTTPS over TCP

For OS logs, the following formats and transport protocols are supported:

Format	Transport protocol
syslog	UDP, TCP

OS logs are based on the 30-stig.rules configuration provided by RHEL/AlmaLinux. This rule set is designed to meet the requirements set by Security Technical Implementation Guides (STIG). Some Elisa Polystar customisation of the 30-stig.rules has been made to avoid too extensive logging due to the usage of ntpd service -x switch.

5.6.1 Generic log elements

5.6.1.1 Non-field log elements

These are generic information elements that different logging formats will handle in a format-specific way. The element identification/name cannot typically be mapped to an identifying string that is the same for all logging formats.

Time/timestamp
: The point in time when the user performed an action that triggered the log event. Because of network delays/buffering this is typically a time before the logging event is received by the log management system.

  The format of the timestamp is determined by the logging format. For example, GELF uses the number of seconds since Epoc with decimals, but Syslog uses a ISO-8601 formatted string. The format is typically converted/represented in a user-friendly style by the graphical interface of the log management system (the web browser)

Message	The main message that will give information about the action that triggered the log event. The format of the message is determined by the logging format. For example, GELF has a limit on the number of characters for the message (but has an additional full_message field where the uncropped message can be found).
Host/Source	The name of the host that sent this log message. It will be the set to the IP/host of the server running the service that sent the log message. Most log management systems will honour this and show it to the end user. Some log management systems may override this and set it to the IP/host of the incoming socket. Some may override it to a custom source string.
Level	Normally used to indicate the severity of the logging message. Not used by Polystar application logging. Logging formats that require this to be set will have it set to “informational” log message.
Facility	In Syslog used to indicate program that is logging the message. Not used in Polystar application logging. Is always set to local0 (number 16) for Syslog.

5.6.1.2 Generic fields

These are generic fields that are used by most or all Polystar applications.

application_name	Originating service/application. For example: galileo, osix, packetrecorder or access-manager.
user	Identification of the user that performed the action. For example, polylesc. For internal triggered actions the special string [local server user] is used.
user_ip	The IP number of the machine the user used to trigger the action.
user_host	The host of user_ip (best effort resolution). Typically resolved with a reverse DNS lookup. May sometimes be resolved to the same as IP number. Not always present.
filter	Human readable filter used to filter the traffic. Different applications may use different formats. Not fully indented for machine parsing because the format may change in future releases.

5.6.2 OSIX logging

5.6.2.1 Logged actions in OSIX

- Login/Log out.
- Password change (using a close-to-database format where the password is omitted).
- Elevation of privileges (both failed attempts and successes).
- Opening of a specific application within OSIX. For example, Statistics Alarm.
- Editing of a setting within Configuration Manager. The log message will contain a close-to-database format of what has been changed.

- Setting a filter (server or view) in Protocol Analyser, Call Trace or Real Time Statistics.
- Start steaming (realtime) or start searching (historical) using Protocol Analyser or Call Trace.
- Export of message data (message file, text, HTML or PCAP) in Protocol Analyser or Call trace.
- Call Trace Event Search.
- User entered text in “search logging dialogue” when using Protocol Analyser or Call Trace (when that setting is enabled for the user group).

5.6.2.2 OSIX-specific fields

mode	Used to indicate search modes (Realtime/Historical) in Protocol Analyser, Call Trace and Real Time Statistics.
traffic_groups	Comma separated list of used traffic groups.
filter_type	If Server filter or View filter is used in Protocol Analyser or Call Trace.
group	The user group tried to the user. Only used with OSIX application (because only OSIX has a one-to-one relationship between user and group).
user_pid	Process identifier of the process that the user is using to trigger the action. Typically, the Windows process ID of OSIX.exe.
osix_application	The name of the specific application within OSIX. For example, Call Trace

5.6.3 Galileo (KALIX) logging

5.6.3.1 Logged actions in Galileo

- Fetching/searching data from Galileo via the HTTP REST API. Typically triggered by KALIX or Call Trace Event Search. May also be triggered by services (for example kalix_scheduler).
- Failed Galileo search due to that the user does not have permission to use a specific filter. Typically triggered when the user searches on a sensitive parameter that the user does not have permission to view.

5.6.3.2 Galileo-specific fields

request_id	The UUID for the request the user made. Typically never shown to the end user.
search_start	Time stamp of the start of the search interval (ISO-8601 formatted string).
search_end	Time stamp of the end of the search interval (ISO-8601 formatted string).
datasets	Comma separated list of datasets that user searched. Typically maps to a view in KALIX or Call Trace Event Search Event Type.

Sensitive parameter (one field per parameter)	The name of this field will be set to the ID of the sensitive (maskable) dimensions listed in Polystar User Manager. The name listed in User Manager is a pretty name, for example “IMSI”. The ID used in logging may for example be “imsi”. The value of this field will be a comma separated list of the values the user has set a filter on. If the user has set a filter for the same value multiple times it will only be listed once. The list has no specific internal order and no ordering should be assumed.
portal_name	Name of the KALIX portal the user used. Only present for normal KALIX usage. Since 6.5.2
view_name	Name of the view inside a KALIX portal the user used. Only present for normal KALIX usage. Since 6.5.2

5.6.4 User Manager (access-manager) logging

Note: The actual password used is never logged.

5.6.4.1 Logged actions in Access Manager

- Create token (normal login of a user)
- Authentication failure during token creation (typically wrong username/ password)
- User changing own password
- Management: Add/remove masked dimension
- Management: Add permission to role
- Management: Add portal permissions
- Management: Assign/unassign external entity (external LDAP authentication)
- Management: Change another user password
- Management: Store/Delete user
- Management: Post/remove certificates
- Management: Store/remove privacy profile
- Management: Store/remove role
- Management: Store Integration Settings (external LDAP authentication)
- Management: Upload config file (batch upload of users, roles etc)

5.6.4.2 Access Manager-specific fields

account_name	Added/edited account name
account_display_name	Added/edited accound pretty name (typically user first name and last name)
account_email	Added/edited account e-mail address
account_privacy_profile	Added/edited account privacy profile
account_roles	Added/edited account roles (comma separated)

role_name	Added/edited role name
role_category	Added/edited role category (Kalix feture or Kalix portal)
role_permissions	Added/edited role permissions (comma separated)
privacy_profile_name	Added/edited privacy profile name
privacy_profile_excluded_maskings	Added/edited privacy profile excluded maskings (comma separated). All dimensions that should be visible for this privacy profile.
privacy_profile_excluded_extradata	Added/edited privacy profile excluded Extra data maskings (comma separated). All additional Extra data dimensions that should be visible for this privacy profile.
added_masked_dimension	Added masked dimension name (user defined)
privacy_profiles_added	Added masked dimension applied privacy profiles (comma separated). All privacy profiles that this newly added dimension should be masked for.

5.6.5 Packet Recorder logging

5.6.5.1 Logged actions in Packet Recorder

- Create stream
- Delete stream
- Stop stream
- Download of stream data from Packet Recorder web GUI.
- Loading of user data from Packet Recorder into OSIX Call Trace

5.6.5.2 Packet Recorder-specific fields

No specific fields are implemented for Packet Recorder. Fields are implemented inside the main log message.

5.6.6 Voice Media Service logging

5.6.6.1 Logged actions in Voice Media service (RTP Playback)

- Downloaded wav file

No specific fields are implemented for Voice Media Service (RTP Playback). Fields are implemented inside the main log message.

5.6.7 Trace data manager (OSIX web) logging

5.6.7.1 Logged actions in Trace Data Manager

- Streaming of data from Trace data manager. Triggered typically by the osix web UI session trace view, but can also be triggered by other things as the export API.
- Fetching of session details data from Trace data manager, Triggered typically by the osix web UI session details view, but can also be triggered by other things as the export API.

- Failed searches due to that the user does not have permission to use a specific filter. Typically triggered when the user searches on a sensitive parameter that the user does not have permission to view.
- Performing an OSIX API request to export data.

5.6.7.2 Trace Data Manager-specific fields

request_id	The UUID for the request the user made. Typically never shown to the end user.
search_start	Timestamp of the start of the search interval (ISO-8601 formatted string).
search_end	Timestamp of the end of the search interval (ISO-8601 formatted string).
traffic_groups	Comma separated list of traffic groups that user searched for. May be empty.
routing_groups	Comma separated list of routing groups that user searched for. May be empty.
links	Comma separated list of links that user searched for. May be empty.
Sensitive parameter (one field per parameter)	The name of this field will be set to the name (with ID in parenthesis) of the sensitive (maskable) dimensions listed in Polystar User Manager. The name listed in User Manager is a pretty name, for example “IMSI”. The ID used in logging may for example be “imsi”. The value of this field will be a comma-separated list of the values the user has set a filter on. If the user has set a filter for the same value multiple times it will only be listed once. The list has no specific internal order and no ordering should be assumed.

5.6.7.3 OSIX API-specific fields (Request builder)

request_id	The UUID for the request the user made. Typically never shown to the end user.
request_builder_id	The stored UUID for the template that was built in request builder.
export_format	The chosen output format (msgs, pcap, pcapng).

Note: Elisa Polystar does not provide the central log management system. As a fallback for deployments without any central log management, it is possible to configure the system to save audit logs on the local discs of the various nodes within OSIX. These log files must not be sent to a central log management system nor machine parsed, as their format is not specified and may change. Any integration with central log management systems must be based on logs sent directly from the applications, as described above.

5.7 iLO security

5.7.1 iLO password handling

By default, HPE servers come with a pre-configured user name and password for the iLO (Integrated Lights-Out) interface, which is used by the system to monitor the health of the server. If desired, the customer can change this default password and/

or user name to their own. However, please note that a valid user name and password are required for this functionality.

5.7.2 Customer CA for host-monitor

By default, each customer system uses its own self-signed certificate authority (CA) and certificates. However, if the customer prefers to use their own certificates for the iLO instead of the self-signed certificates generated by Elisa Polystar, they may do so. In this case, the customer will need to provide their CA to the Elisa Polystar services department.

6 System requirements

6.1 Client hardware

Minimum desktop client PC requirements:

- Windows (32 bit)/Windows (64 bit)/Linux (64 bit)/Mac OS X
- 400 megahertz (MHz) processor or faster
- 4 GB RAM of system memory (whereof 2 GB free for the OSIX application)
- 400 MB of free hard disk space

6.2 Site requirements

See the site requirement documentation for more information.

7 Deployment on hardware

Elisa Polystar has used HPE servers equipped with HPE ancillaries exclusively for more than 20 years. For HPE Gen11 servers, AMD processors are used. Over these years, Elisa Polystar has developed a well-functioning system based on the best price/performance model by selecting the appropriate HPE parts for each component in the system using CTO (Configure To Order), including server chassis form factor, choice of CPU (clock frequency, number of CPUs and cores), amount of RAM, and storage, to provide the optimum price and performance per component.

Hardware deployment of OSIX Monitoring uses HPE ProLiant DL/BL servers. The physical servers are all configured with different RAID configurations, which prevents data loss in case of hardware failure.

For complete specifications of hardware nodes, please refer to *OSIX Hardware Specification*.

7.1 Capturing nodes for E1/T1 monitoring

The LIM 3.0 extracts signalling from E1 and T1 G.703 PCM links in fixed, GSM, and 3G networks. It connects to E1/T1 links, decodes layer 1 and layer 2 of the protocol stack, and then forwards the monitored data to the Router (RTR) over TCP/IP.

Each LIM 3.0 provides 64 E1/T1 receivers in 1U of a 19” rack, that is, a possibility to monitor 32 E1/T1 links. The LIM is controlled by an external application through an OS- and language-neutral text-over-TCP/IP/Ethernet API, and is capable of decoding SS7 MTP-2, ATM (AAL5 and AAL2), frame relay or LAPD.

The average link load is limited to 0.4 Erlang. However, peak loads can be up to 1 Erlang.

7.1.1 Capacity matrix LIM 3.0

32 E1s	Pro	Basic	Comment
MTP-2 low speed links (LSL)	120	8	
MTP-2 high speed links / timeslots (HSL)	4/240	-	Annex A
ISDN LAPD links	200	160	
Frame Relay channels / timeslots	96/1488	16/496	Gb
HSSL (ATM AAL5)	8	2	ATM over E1

Table 3: Capacity matrix LIM 3.0

Please note that one LIM is only able to process one layer 2 decoding algorithm at a time.

7.1.2 Hardware features

- 19” x 1U rack-mounted chassis, 482 x 144 x 42mm.
- E1/T1 receivers have software-selectable E1(2 Mbit/s) or T1 (1.5 Mbit/s) mode 75/100/120 ohm termination, and are compatible with standard -20dB (G.772) and also -30dB monitor points.
- Dual 10/100 Mbit/s Ethernet, both supporting Power over Ethernet (PoE).
- Power consumption less than 10W per chassis. Dual 48VDC power inputs and dual PoE.
- No moving parts, passively cooled.
- Measured MTBF: 130 module-years between failures

Figure 38: LIM 3.0 - front

7.1.3 Electrical independence—hot swapping

The power converters in each probe chassis accept two separate, polarity-independent input voltages of 38-60VDC. This makes the probe extremely resistant to variations in power supply.

7.1.4 Software independence

All real-time critical issues are handled by the hardware, and the software is easily upgradeable. Upgrades can also be handled remotely.

7.1.5 Synchronisation

The OSIX system uses the NTP protocol for time synchronisation. When the capturing nodes have been synchronised, they use the PCM links as the timing source, that is, the system runs at the same pace as the switching system. This assures very accurate time stamps.

The NTP time adjustment is continuously monitored and typically lies within fractions of a millisecond.

7.1.6 Carrier class-approved

Each component of the OSIX system is thoroughly tested and approved in accordance with requirements for CE and EMC carrier class levels.

The capturing nodes and LIMs are separately approved for electrical safety, for example regarding electrostatic discharge and surge resistibility according to ITU-T.

7.2 Capturing nodes for STM-1

7.2.1 STM-1

The capturing nodes consist of 1U 19" rack-mounted chassis (482mm x 144mm x 42mm) with room for one or three independent sub-modules. Each sub-module is equipped with the following interfaces:

- Two SFP sockets for STM-1 SFP modules. Multi-mode and single-mode fibres, different wavelengths and connectors are selected by the added SFP module.
- Two 10/100 Mbit/s Ethernet with RJ-45 connector.
- Status LEDs.

The units can be equipped as follows:

- SDH 3.0-1 - equipped with one (1) SDH sub-module.

Note: This version is not expandable, which means that you need to replace the whole chassis if you need to increase with additional sub-modules.

- SDH 3.0-2 - equipped with three (3) SDH sub-modules. This version is HW prepared with three sub-modules, and can be upgraded to SDH 3.0-3.
- SDH 3.0-3 - equipped with three (3) SDH sub-modules.

Figure 39: SDH 3.0-3 front

A chassis provides two or six SFP sockets in total and can thereby monitor both directions of up to three SDH links.

Each SDH 3.0 sub-module can monitor two simplex SDH links. The SDH Layer 1 configuration supported is STM-1->AU-4->TU-12. Each sub-module is capable of monitoring 68 MTP-2 duplex links.

7.2.2 Capacity matrix SDH 3.0

Signalling Monitoring Performance, per (sub)module	Pro	Basic	Comment
MTP-2 low speed links (LSL)	120	8	
MTP-2 high speed links / timeslots (HSL)*b	4/240	-	Annex A
ISDN LAPD links	200	160	
Frame Relay channels / timeslots	96/1488	16/496	
HSSL (ATM AAL5)*a	8	4	

Table 4: Capacity matrix SDH 3.0

* Not supported in OSIX software. However, support can be provided by contract.

[a] An ATM-based HSSL channel is “always” (that is, the standard says so) 30 timeslots wide on E1. SDH allows narrower channels, too.

[b] HSL according to MTP2 itu96 Annex A.

7.3 Capturing nodes for Ethernet

7.3.1 MediaProbe

The MediaProbe is Elisa Polystar's solution and platform for Ethernet monitoring and analysis of control and user plane data in high-capacity data networks. The MediaProbe offers real time user plane quality analysis, load balancing, traffic aggregation, and sophisticated filtering features, and delivers performance metrics for troubleshooting and for ensuring the quality and high performance of the service.

7.3.2 Connection

The MediaProbe is strategically placed at the various points within the network and network gateways that allows it to non-intrusively collects the full network data, promising an uptime of 99.99%.

The actual connection to the customer network can be made inline using fibre splitters, or using aggregated mirror ports. Either way, the MediaProbe is a passive probe and does not interfere with the customer network. The only information sent back from the MediaProbe to the network are ARP responses when requested by the network in order to establish a consumer feed to the MediaProbe.

7.3.3 Hardware configuration

The MediaProbe offers fantastic flexibility and power as it can be deployed in a network of any size, from the smallest to the largest, that supports 1Gb, 10Gb and 100Gb connections.

A prerequisite for any hardware configuration when monitoring GTP-U user plane traffic, is that all user plane traffic for one user session is received on the same MediaProbe. To offer such a flexibility, the MediaProbe comes in a wide range of hardware configurations, including switch-based load sharing, as described in chapter 4 of the *OSIX Hardware Specification*.

7.3.4 Switch-based load sharing

With the Elisa Polystar proprietary switch-based load sharing solution, the possibility to process very high throughput speeds of user plane monitoring is enabled at competitive prices. Activity aggregation of user data requires that the complete uplink and downlink traffic related to one device and one application is processed in one single probe device. In the situation that throughput speeds of a monitored network node exceed the processing capacity of one single probe, the traffic must be split up and load balanced without breaking aggregate completeness.

This highly efficient and affordable load sharing solution delivers complete aggregates for the analytics layer by utilizing:

- MP100M MediaProbes
- 1 x HPE Aruba Networking CX 8325P 32-port Switch

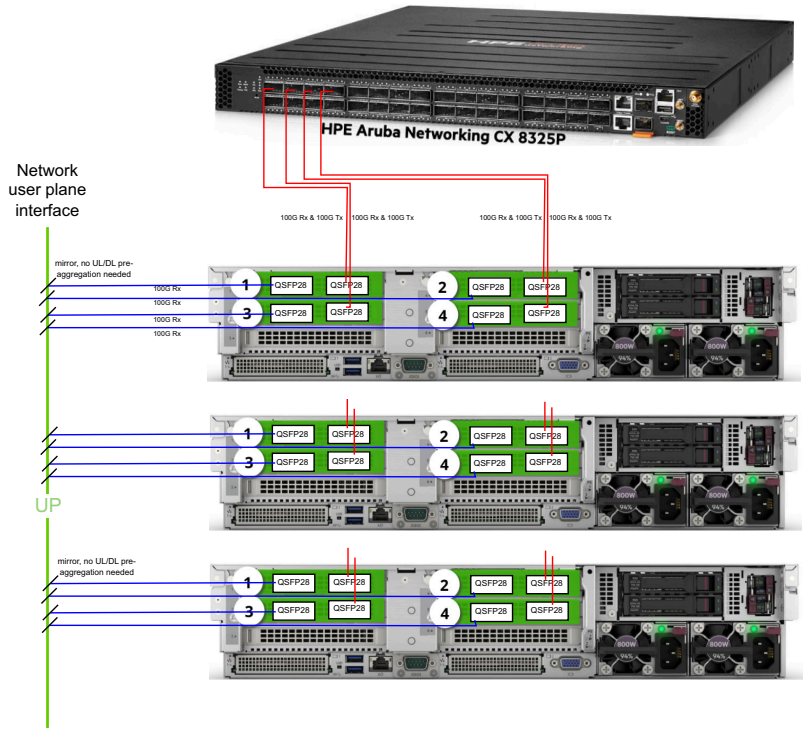


Figure 40: Load-sharing solution

7.4 Capturing nodes for virtual taps

7.4.1 ETM

When using virtual taps, mainly in 5G Core, Elisa Polystar has developed the External Tap Mediator (ETM). The ETM handles various virtual tapping solutions and enables monitoring where eth monitoring and physical taps are not feasible. The ETM also handles load balancing and traffic filtering.

Even though signalling data may differ in format between virtual tapping solutions, the ETM streamlines the data into a format that is recognisable within the rest of Elisa Polystar's systems.

The ETM is used for monitoring all 5G SA vTAPs, except the Ericsson vTAP where the MediaProbe still is used.

In a hardware deployment, the ETM is deployed on a Processing Node (PN).

7.4.2 MediaProbe

In the case of using Ericsson vTAPs for traffic monitoring, the MediaProbe is used as a consumer of that feed. The MediaProbe is configured in a customised way to be able to interpret the payload that it receives, which is dependent on consumer-related configuration in the Ericsson vTAP itself. The MediaProbe is able to provide the vTAP with its identity when requested, but is otherwise a passive probing device.

7.5 System Management Node

The System Management Node (SMN) is an OpenStack-based platform and includes miscellaneous supporting functions, deployed as virtual machines (VMs).

The System Management Node (SMN) requires eight (8) IP addresses in total (for future needs).

The host itself requires one (1) IP address plus one (1) IP address for the ILO in addition to the VMs deployed, which require one (1) IP address each.

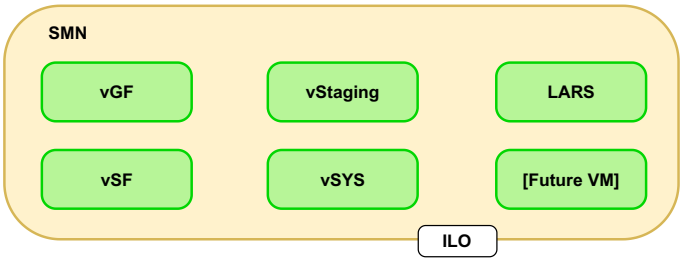


Figure 41: System Management Node (SMN)

The System Management Node (SMN) replaces the former Global Node (GN).

For more information about the virtual components, see chapter *8 Deployment in a virtualised environment*.

7.6 Processing Node

The processing node can host eight or fourteen components in any combination, and a routing group can consist of components from several different processing nodes.

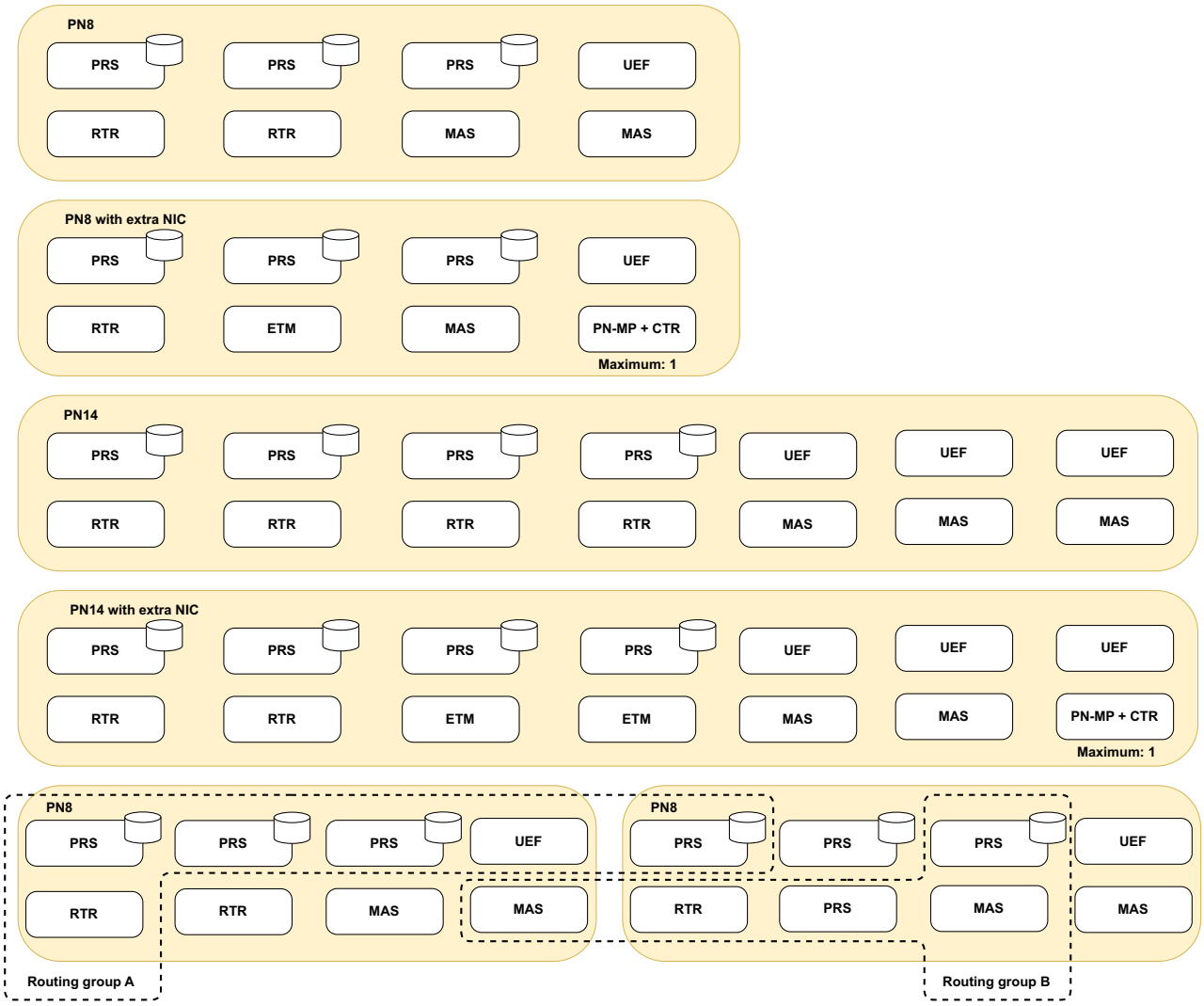


Figure 42: Processing node and routing group examples

7.7 Polystar Cloud Node (PCN)

The Polystar Cloud Node (PCN) is a one-host OpenStack platform which can host a combination of different types of VMs, as long as the host resources are not exceeded. To calculate the total usage, please use the attached Excel spreadsheet.

The PCN is suitable for small operators, test environments, PoCs etc. with a limited amount of traffic. General dimension rules apply according to the Dimensioning rules.

The Polystar Cloud Node (PCN) requires one (1) IP address for the host itself, one (1) IP for the ILO, and one (1) IP address for the internal DHCP server, in addition to deployed instances, which all require one (1) IP address each.

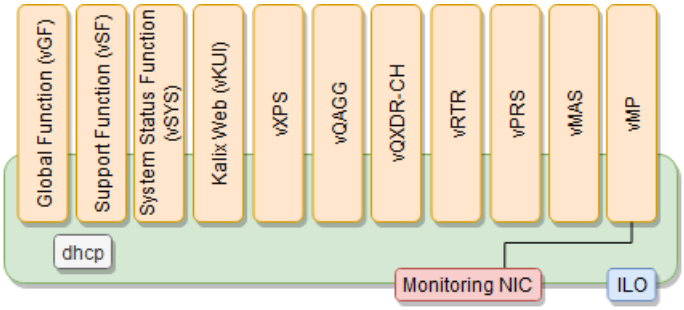


Figure 43: Polystar Cloud Node

For more information about the virtual components, see chapter *8 Deployment in a virtualised environment*.

7.8 Polystar Pod Node (PPN)

The Polystar Pod Node is a Podman-based container node that can host a combination of different containers as long as the host resources are not exceeded. For example, the TDM/TDR nodes used by the OSIX web client is implemented on PPN, as well as the RAN Gateway.

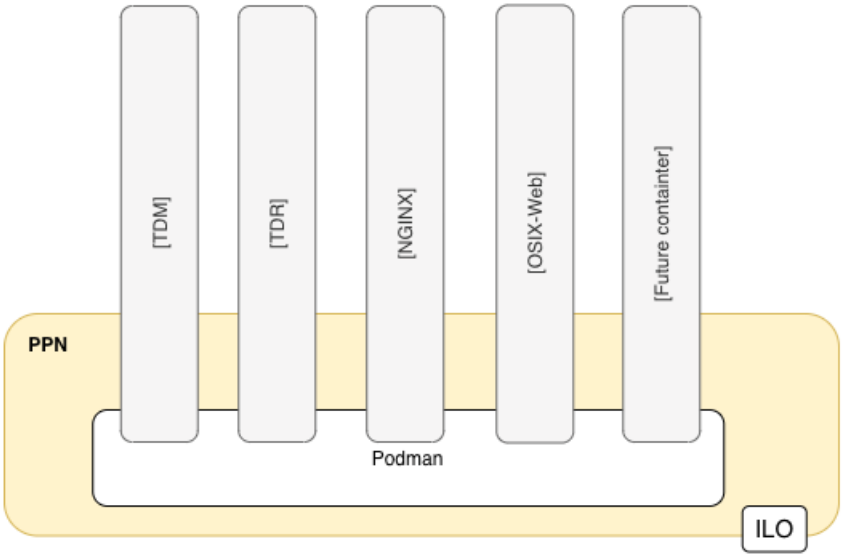


Figure 44: Polystar Pod Node

8 Deployment in a virtualised environment

As part of the Elisa Polystar product strategy, OSIX Monitoring components are available as virtual machines for deployment in a customer's data centre environment.

The driver behind data centre deployments can also be linked to the evolution of Network Function Virtualisation (NFV) and Software Defined Networking (SDN). However, this chapter does not address solutions on how monitoring of NFV/SDN type networks can be achieved.

Elisa Polystar supports the vSphere ESXi (VMware) and Openstack platforms (hypervisors).

Please note that Elisa Polystar does not provide the actual hypervisor, only the virtual image. The sourcing and management of the hypervisor component and its associated management tools is the responsibility of the customer.

The Virtual Machine images are provided as either an OVA file for VMware and RHV, or as a compressed tar ball containing a cqow2 file for OpenStack deployment.

The VM is delivered as one integrated image that contains the guest OS and the application software. Elisa Polystar does not support a delivery model where the guest OS is provided by the operator.

Deployment of individual VMs is supported both to new green-field systems, as well as expansions to existing legacy systems.

Example: An expansion to a legacy system can be made using a combination of legacy hardware functions and virtual machines. Please note, however, depending on traffic distribution, individual routing groups should not be split over both legacy hardware and virtual machines.ps should not be split over both legacy hardware and virtual machines.

8.1 Virtual images

The components of the OSIX Monitoring system are deployed in virtual images according to the following.

8.1.1 VMs for the capturing layer

It is possible to deploy the MediaProde on a VM. However, the capacity of a Virtual MediaProbe (vMP) is much less than the capacity of a physical MP, why the vMP only can handle control plane traffic. Even if we can deploy many vMPs in parallel, all user plane (UP) flows must come to the same MP/vMP. The only UP traffic allowed using vMPs is RTP. For non-RTP user plane monitoring, a physical MediaProbe is required, but for control plane only installations the vMP can be an attractive choice.

Note that SR-IOV support is required for the vMP to comply to the capacity in our dimensioning guidelines.

8.1.2 VMs for the processing layer

The Virtual Probe Server (vPRS), Virtual Router Server (vRTR), Virtual Mapping Server (vMAS), and Virtual User plane Enrichment Function (vUEF) host the PRS, RTR, MAS, and UEF components, respectively. Note that each virtual image contains exactly one instance of the PRS, RTR, MAS, or UEF component.

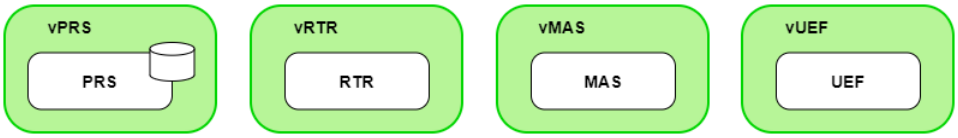


Figure 45: vPRS, vRTR, vMAS, vUEF

8.1.3 VMs for system management

8.1.3.1 vGF

The virtual Global Function (vGF) replaces what was previously known as the Global Node/GLS Server. The vGF includes all components/services that are part of the system management subsystem.

Depending on the size of the data processing system, the vGF can be scaled up. The vGF is deployed on the System Management Node (SMN) or in the customer data centre.

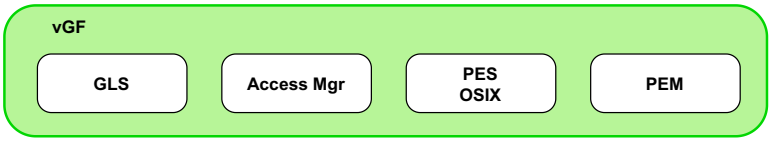


Figure 46: vGF

8.1.3.2 vSYS

The vSYS is the preferred implementation option for system status. (There are alternative installation options for hardware-based legacy systems.) The vSYS includes all components needed to process and store system status data in databases and to expose it through a KALIX-based UI. The vSYS is deployed on the SMN or in the customer data centre.

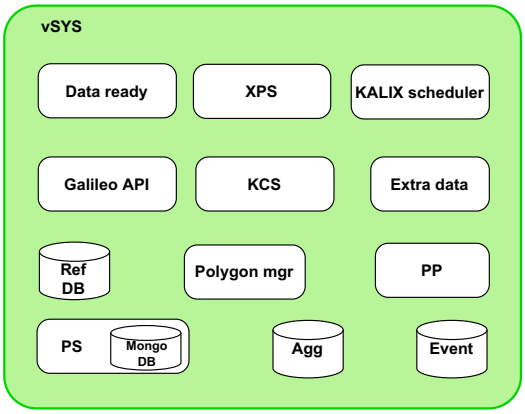


Figure 47: vSYS

8.1.4 VMs for the exposure layer

The TDM/TDR components are deployed within a single virtual image, corresponding to the Exposure Node in a hardware deployment.

8.1.5 VMs for container deployment

The Elisa Polystar Pod VM includes Podman as container runtime and can be used to deploy a combination of different containers as long as the host resources are not exceeded.

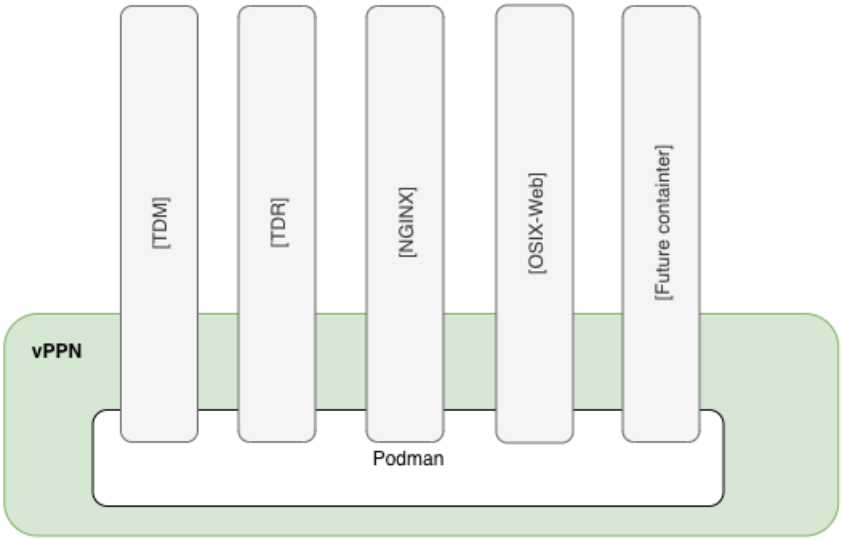


Figure 48: VMs for container deployment

8.1.6 VMs for O&M

vSF is used by Elisa Polystar support as a jumping host to access the system.

vStaging is used in case of OS reinstallation.

9 Cloud-native deployment

In parallel to hardware- and VM-based deployment, OSIX Monitoring can also be deployed in a cloud-native environment. For customers providing a Kubernetes-based data centre, a container-based deployment of OSIX Monitoring is available.

At present, a cloud-native deployment of OSIX Monitoring and KALIX Analytics takes the form of a hybrid system, mixing container-based and either (or both) VM-based and HW-based deployment. This provides a natural transition path, where an existing installation can gradually be moved to cloud-native. Typically, needs for OSIX Monitoring capacity expansions are handled by gradually moving routing groups from HW-based Processing Node or VM based components to a cloud-native deployment on Kubernetes.

9.1 Hybrid deployment

This chapter describes what can be deployed on Kubernetes and what must be deployed outside Kubernetes, as VMs or on HW, in a hybrid deployment.

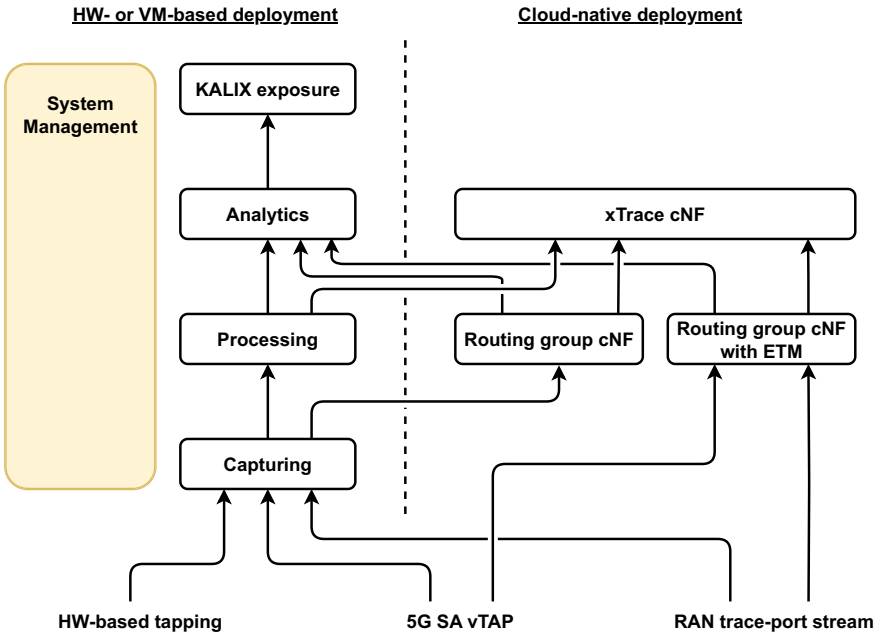


Figure 49: Hybrid deployment

The capturing layer is deployed on VMs or hardware. Specifically, for generic DPI-based user plane monitoring of Gn-U, S1-U, and N3 interfaces, only hardware-based deployment of the Capturing layer is feasible, due to the high data volumes. Virtualised MediaProbe is available for control plane monitoring and limited volumes of RTP. Generally, the capturing layer is deployed outside the Elisa Polystar Kubernetes cluster.

However, in the case of vTAP monitoring for 5G SA, and in the case of trace-port stream integration for RAN monitoring, no external hardware- or VM-based component is needed. Instead, an External Tap Mediator (ETM) from Elisa Polystar is deployed as part of the cNFs within the Kubernetes cluster.

The components within the Processing layer can be deployed either within or outside the Kubernetes cluster. This choice is made on a per routing group basis, meaning that each node in the active network has its monitoring deployed either completely inside or completely outside the cluster. At present, cloud-native deployment inside the cluster is supported for all types of monitoring, except monitoring of GGSN, SGW, PGW, and UPF. That specific monitoring will be

refactored to support cloud-native deployment in a future release. A transition path where monitoring of other node types is first moved to cloud-native deployment is recommended.

The OSIX web client Exposure components, TDM and TDR, are deployed within the Kubernetes cluster. In a hybrid system, there are no OSIX web client Exposure components deployed on hardware or VMs outside the cluster.

Likewise, system management functions such as Global Function, Access Manager and Logging and Repository Server are deployed outside the Kubernetes cluster. In this way, system status reporting as well as centralised logging provides a unified view covering components deployed inside as well as outside the Kubernetes cluster.

9.2 OSIX clients in a hybrid system

The OSIX web client is the only allowed client for cloud-native deployments of OSIX Monitoring. It is built on the latest technology and avoiding lengthy native client verification and installation procedures. It is ideal for the more agile approach that comes with moving services to the cloud. The OSIX web client Exposure components are deployed inside the cluster, giving seamless visibility into all traffic, regardless of whether the routing group components handling the traffic are deployed inside or outside the cluster.

In a hybrid system, the OSIX desktop applications such as Call Trace and Protocol Analyser can only access the subset of the traffic handled outside the Kubernetes cluster. Note however, that the OSIX desktop application Configuration Manager can still be used for configuration, in case configuration APIs are not yet fully utilised.

9.3 Full cloud-native deployment

In general, Elisa Polystar's strategy is to offer cloud-native deployment of all software. KALIX, including the analytics layer and system management functions, will be offered as cNFs for deployment on Kubernetes in a future release. Elisa Polystar recommends starting the transitioning towards cloud-native deployment by introducing a hybrid deployment model as described above, with the long-term ambition of moving all parts eventually. The capturing layer for DPI-based monitoring of user plane will come last in this transition path, due to high data volumes and dependencies on advanced load-sharing technology.

9.4 Containerised network functions

Looking more closely on the cloud-native OSIX Monitoring deployment, it consists of three types of cNFs—the routing group cNF(s), the xTrace cNF, and the logging and monitoring cNF.

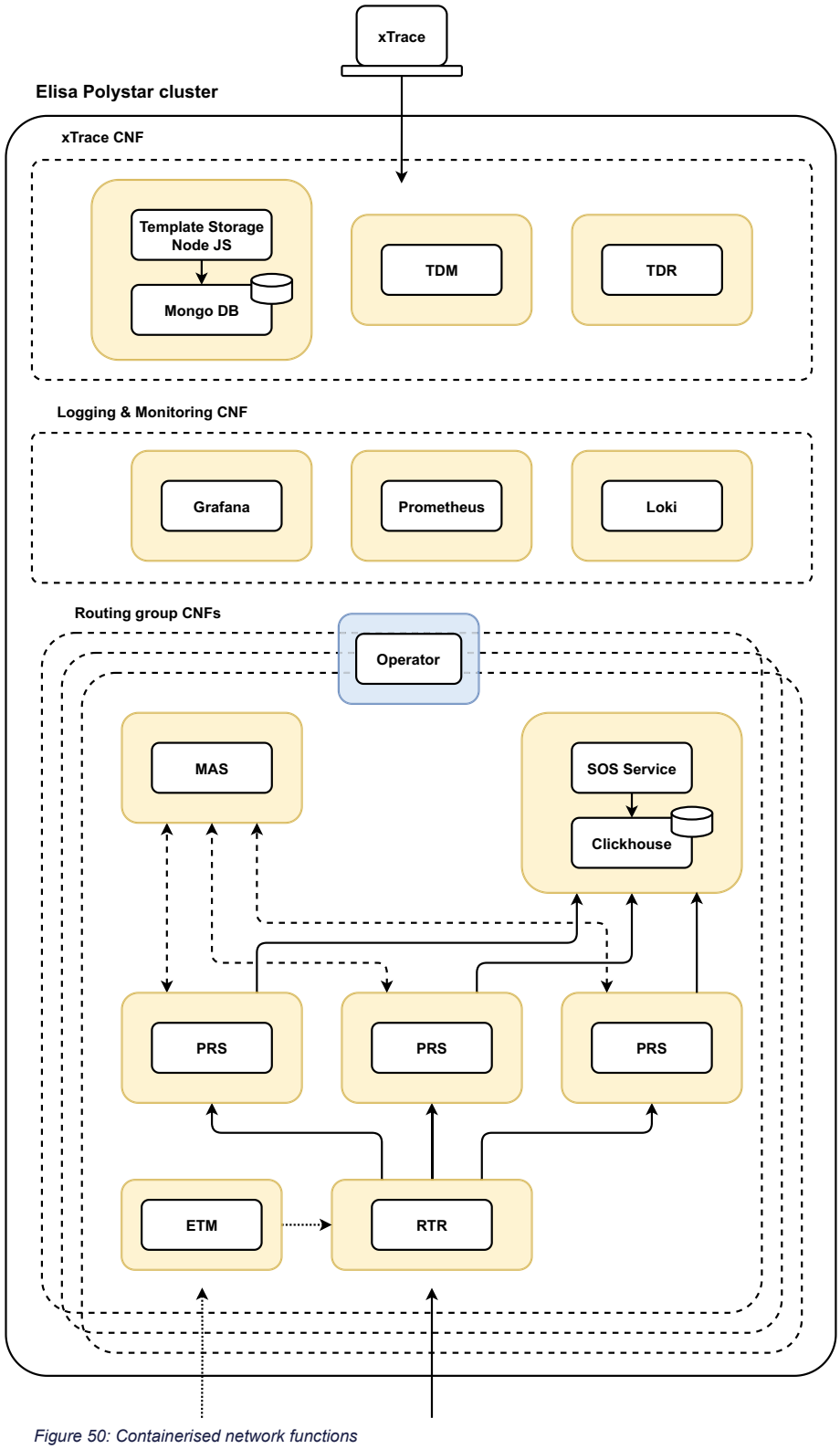


Figure 50: Containerised network functions

The routing group cNF contains, for example, RTR, PRS, and MAS components, that is, the same set of components that are deployed on a processing node in a hardware-based deployment. In a later release, the routing group cNF will also be capable of hosting the User Plane Enrichment Function (UEF) component. One key difference to hardware- and VM-based deployment is the separation between computing and storage. In a cloud-native deployment, storage is not attached to each PRS instance. Instead, there is an SOS service which centralises the storage per routing group. This architecture enables elasticity by making the PRS more stateless. In addition, improved database technology also provides a reduced storage volume compared to hardware- or VM-based deployment.

The routing group operator is our software extension that automates tasks beyond what Kubernetes provides. The operator reads the configuration from the GF database and automatically creates required pods for the routing group(s). It also handles the deployment of computing and storage resources, including the capability to scale up resources.

The routing group cNF may optionally contain the External Tap Mediator (ETM). This component is used to terminate a stream either from a 5G SA vTAP or from a RAN trace port.

An ingress is set up to receive traffic into the routing group cNF. If there is an ETM, the traffic is sent directly from the network equipment vTAP implementation or trace port. In case of traditional tapping, an Elisa Polystar MediaProbe or other capturing device outside the Kubernetes cluster is used, and traffic is sent from it to the routing group cNF.

The xTrace cNF implements the backend components needed for xTrace—the OSIX web-based user interface. The xTrace cNF can handle traffic from routing groups both within and outside the Kubernetes cluster, meaning that the user of OSIX xTrace gets the complete end-to-end view also in a hybrid solution.

The logging and monitoring cNF add the capability to supervise performance and statistics for deployed pods in the Kubernetes cluster. However, this is only an addition to the system status application and the logging functionality deployed in legacy for centralised management and enhanced monitoring capabilities. The logging and monitoring cNF consists of Grafana, Loki, and Prometheus.

9.5 Delivered artefacts and compatibility

Elisa Polystar’s strategy is to rely on the standard Kubernetes toolset to avoid lock-in to any specific cloud providers. With limited adaptions, it is therefore possible to deploy OSIX Monitoring in any Kubernetes-compatible cloud environment. Elisa Polystar has extensive experience of integrating with different orchestration frameworks to achieve automated onboarding and configuration.

Elisa Polystar's application is certified with the 'VMware Ready for Telco Cloud' logo. That is, the cloud-native applications are available in CSAR format with all associated manifests and artefacts.

9.6 Container security and compliance

All Elisa Polystar container images and deliverables are signed for authenticity and integrity.

Privilege escalation is not permitted within containers. Containers run as non-root users, and the file system is mounted as read-only for added security.

Elisa Polystar performs regular container scans to mitigate risks and maintain system security.

Security contexts are implemented to enforce container security policies, and Linux kernel capabilities within containers are restricted to reduce the attack surface.

The application manages its own data backup and restore, and supports in-line pod upgrades for minimal downtime.

Privileged pods are not allowed, and additional container capabilities are restricted to maintain compliance with Kubernetes baseline security standards.

9.7 Data integrity and protection

Images from external registries are validated before deployment, and connections to registries are encrypted to protect data during transmission.

All third-party software is sourced from trusted repositories and verified for integrity to prevent tampering.

9.8 Access control and monitoring

Sufficient mechanisms are in place to control access, ensuring only authorised users can access sensitive information and resources.

Stored data is safeguarded against unauthorised access, modification, and deletion. Data transmission is also secured to prevent interception or modification.

9.9 Configuration management and continuous integration and deployment

Automated onboarding of CNFs is ensured through the customer's CI/CD pipeline. Required artefacts are uploaded to the customer's preferred repository. Configuration changes are managed through various methods, including Operators, Netconf, Helm Upgrade, Configmap, and/or Rest APIs.

10 OSIX Monitoring for PSTN networks

The OSIX Monitoring system extracts information from signalling networks, and includes applications for monitoring and troubleshooting, xDR/SNMP trap generation, email messaging, and OSS (Operation Support System) applications. The following sections show a few examples for PSTN networks.

10.1 Protocols and links

All major protocols and links used within PSTN networks are supported by the OSIX system. For information about supported protocols, see the OSIX Supported Protocols document.

All supported protocols have a large set of predefined parameters available for filtering. For information about protocol parameters, see chapter *15 Protocol parameters*.

10.2 PSTN network features

- Support for all major interfaces and protocols, including several ISUP dialects.
- Real-time KPI measurements for ISUP/BICC/IUP and INAP, for example, ASR and NER.
- Automatic detection of SS7 links and point codes with map view and included alarming and status functionality.
- Monitoring call attempts to specific numbers will help you see if you need to reroute the traffic, or activate call gapping.

10.3 Protocol Analyser

10.3.1 User interface

In the Protocol Analyser main window you can monitor the protocol messages, either in real time or historically with SOS. You can also set different filters or search for specific messages. You can have a maximum of four different Protocol Analyser windows with different settings open at the same time.

Example:

The figure shows different cause values for ISUP. For example, the cause value 34 indicates that there is no appropriate circuit/channel presently available to handle the call, which means that the call cannot be connected.

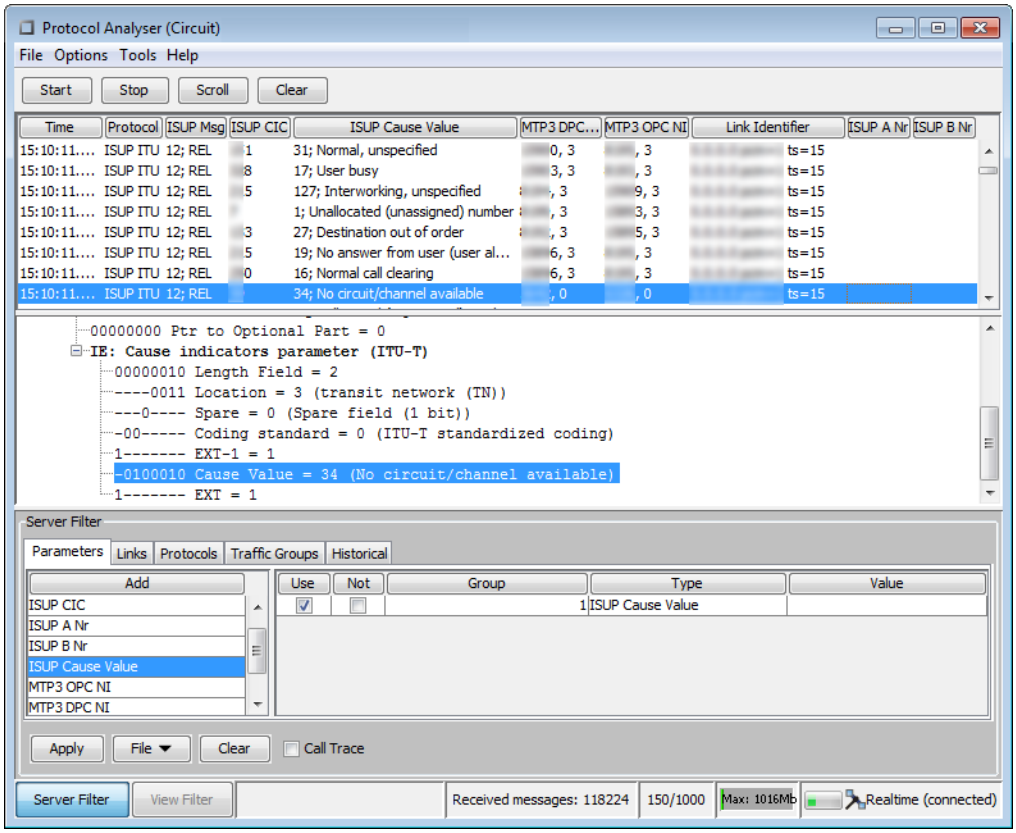


Figure 51: Protocol Analyser main window - Cause value examples

10.3.1.1 Message details

The window is divided into several parts—one displaying the different protocol messages, one displaying a preview of the message, one showing the hexadecimal code, one showing ASCII code, and finally the filter section. You can also choose to open a separate Message Viewer with the contents of the entire message.

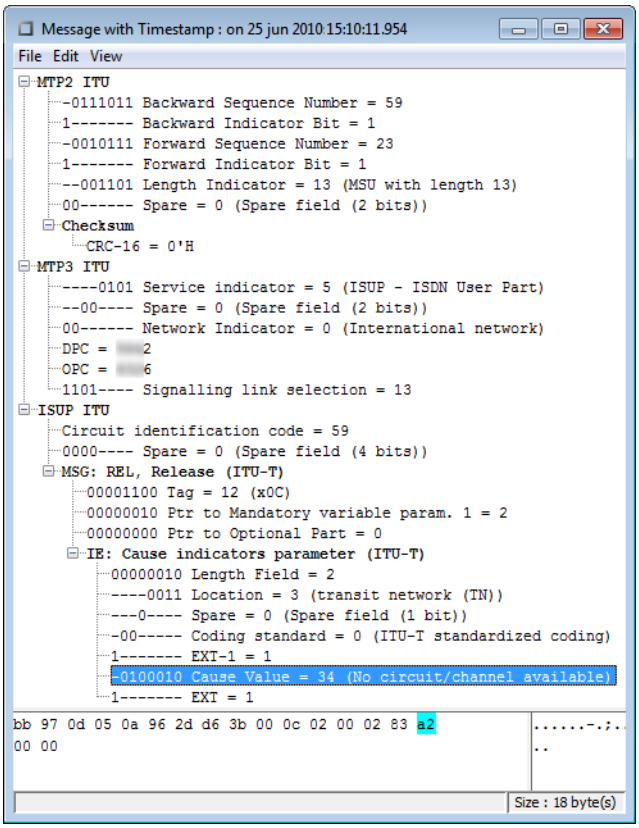


Figure 52: Message viewed in Protocol Analyser

10.4 Call Trace

10.4.1 User interface

In the main window you can monitor the calls, either in real time or historically with SOS. You can also set different filters or search for specific calls. You can have four different Call Trace windows with different settings open at the same time.

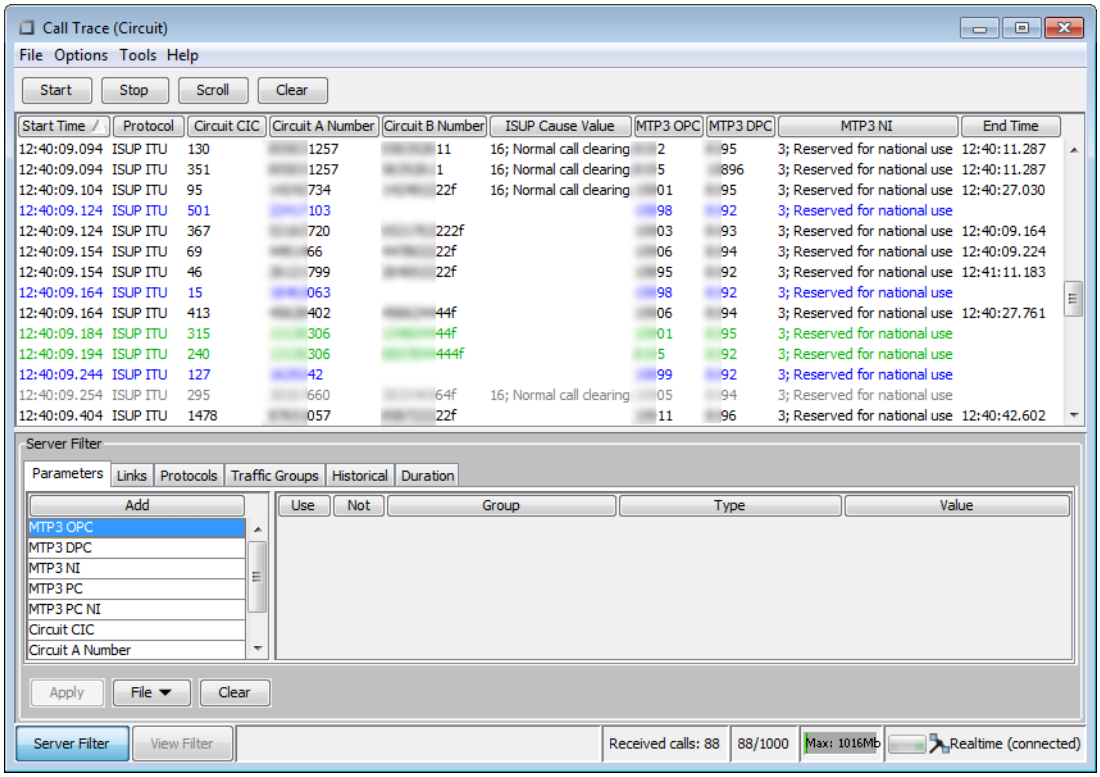


Figure 53: Call Trace main window

10.4.1.1 Call details

If you want to take a closer look at a call, you can double-click it to open the Call window. The window is divided into several parts, or panes—one displaying the different protocol messages sent referring to the selected call, one displaying a preview of the message, one showing the hexadecimal code, one showing ASCII code, and finally one pane displaying different parameters for the call. You can also choose to open a separate Message Viewer with the contents of the entire message.

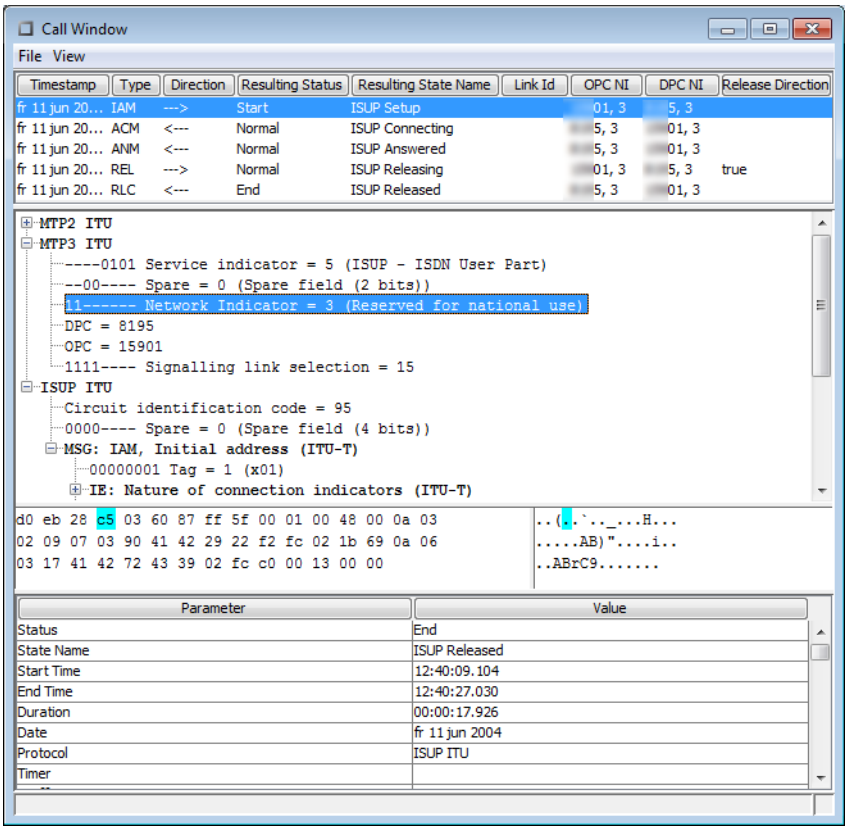


Figure 54: Call window

10.4.1.2 Call flow

When viewing the call details, you can also choose to view the call flow in a graphical representation, where the nodes are visible and the different messages are represented with arrows.

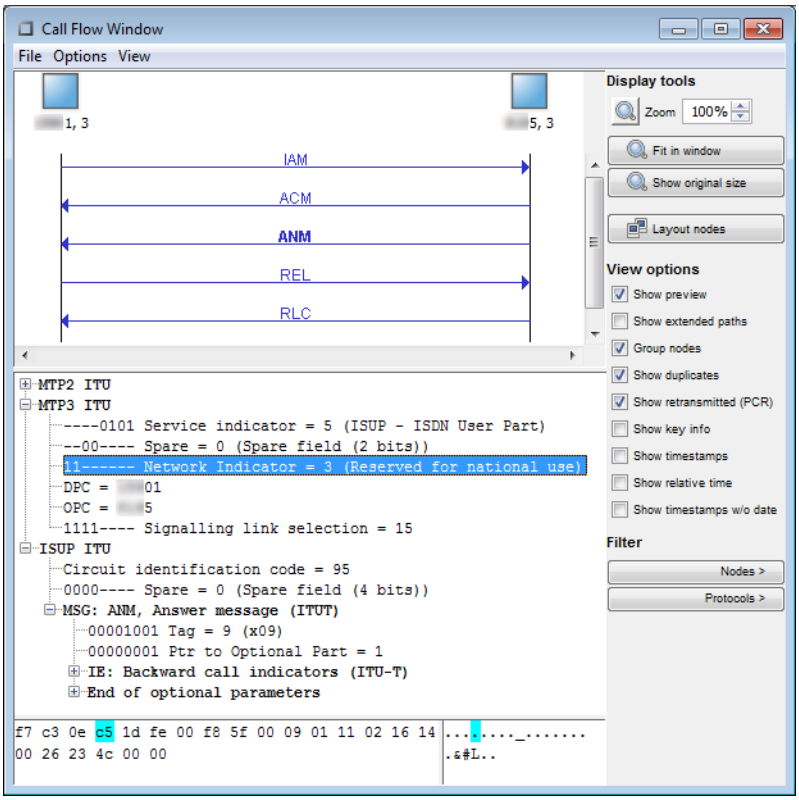


Figure 55: Call flow window

10.4.1.3 Client correlation

The client correlation is done between all messages relating to the same call/ transaction, regardless of where in the network the messages are sent. All messages relating to the process are presented in the Call window.

For PSTN networks, client correlation is available for:

- PSTN ISUP-INAP transactions.
- IMS and Voice over IP transactions

10.4.1.3.1 Client correlation example for PSTN ISUP-INAP

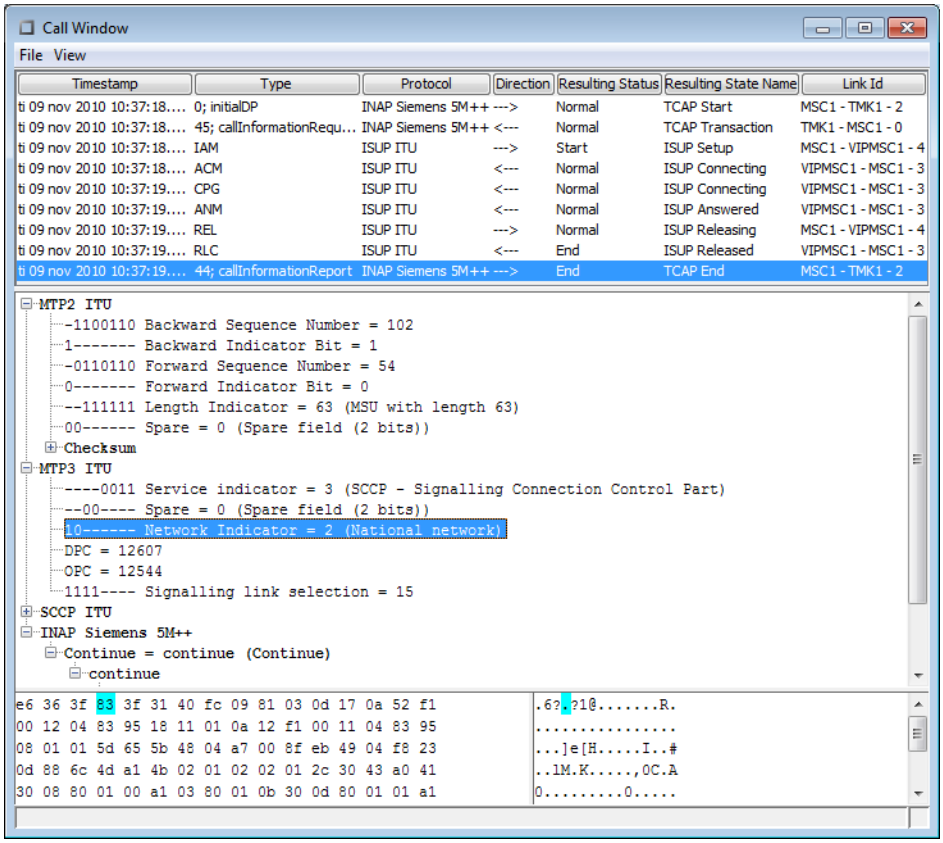


Figure 56: Call window for PSTN ISUP-INAP

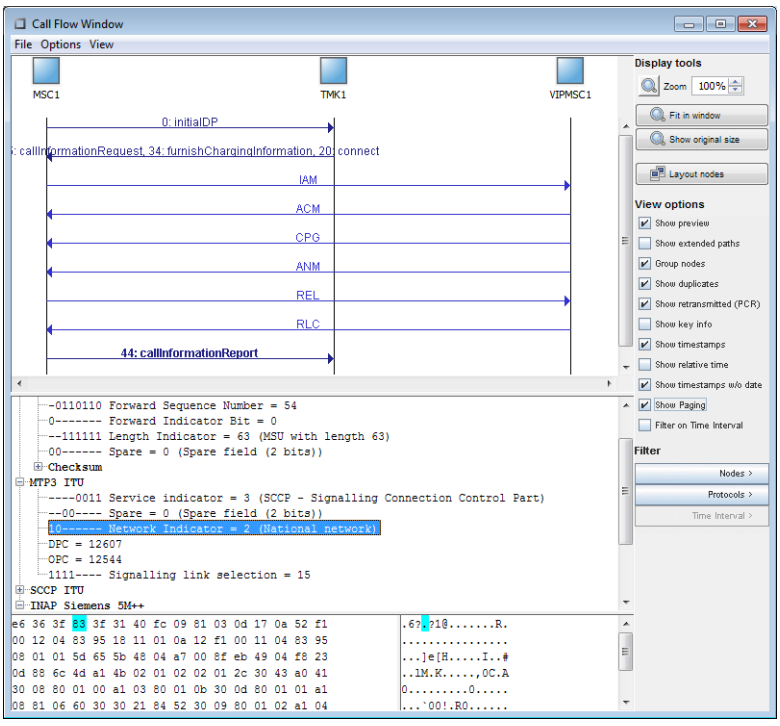


Figure 57: Call flow window for PSTN ISUP-INAP

10.5 Performance Analyser

The Performance Analyser application monitors different Key Performance Indicators (KPIs) for different protocols. For PSTN networks, Performance Analyser is available for circuit-switched protocols (ISUP, IUP, BICC), which have been grouped together, ISDN, and INAP.

The user interface for the circuit-switched protocols and ISDN are very similar. The user interface for INAP, however, is quite different.

10.5.1 User interface

10.5.1.1 Main window

The main window displays the KPIs for the call groups in real time. You can have one window open per protocol, plus one additional window, and the information is updated every ten seconds by default (this is configurable per client).

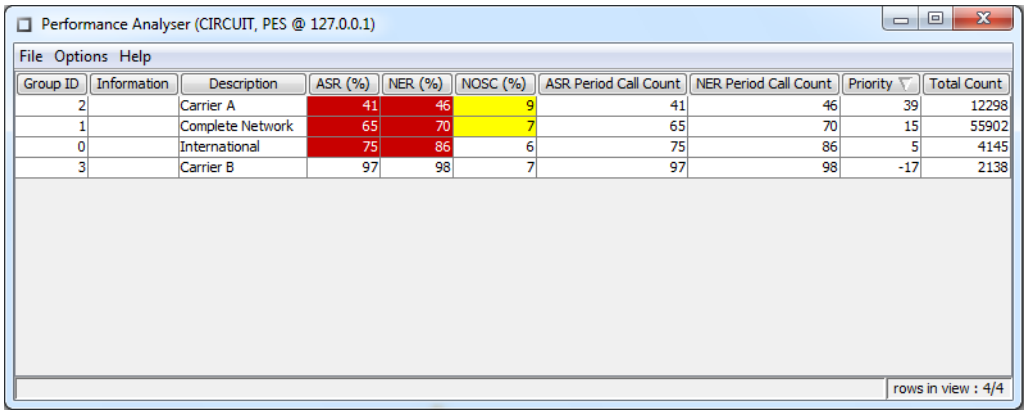


Figure 58: Performance Analyser main window for Circuit

10.5.1.2 Columns

The following columns are available in the main window:

Group ID	Displays the individual group's unique number. (Circuit, ISDN, INAP)
Information	If the KPIs for the group have been measured by OSIX and set automatically, this column displays the results from the last evaluation. (Circuit, ISDN, INAP)
Description	If the group has been automatically generated by OSIX, this column will display which parameter values the group consists of, otherwise the system administrator can set an appropriate name for this column. (Circuit, ISDN, INAP)
ASR	Answer Seizure Ratio displays the number of answered calls out of the total number of call attempts, in per cent. (Circuit, ISDN)
ASR Period Call Count	Answer Seizure Ratio Period Call Count displays the number of successful call attempts that the ASR % value is based on. (Circuit, ISDN)
NER	Network Efficiency Ratio displays the number of calls terminated with normal release causes (defined by the system administrator) out of the total number of call attempts, in per cent. (Circuit, ISDN)
NER Period Call Count	Network Efficiency Ratio Period Call Count displays the number of successful call attempts that the NER % value is based on. (Circuit, ISDN)

Table 5: Main window columns

NOSC	Number of Short Calls displays the number calls with a conversation time shorter than a certain time interval (defined by the system administrator) out of the total number of call attempts, in per cent. (Circuit, ISDN)
Success	Displays the number of successful INAP transactions, that is, transactions reaching End state without any error codes, out of the total number of transactions.
Avg Resp Time	Displays the average time between the first and the second message in the INAP transactions.
T1	Displays the number of INAP transactions with less than the set T1 interval (default 300 milliseconds) between the first and the second message, out of the total number of INAP transactions.
T2	Displays the number of INAP transactions with less than the set T2 interval (default 1.000 milliseconds) between the first and the second message, out of the total number of INAP transactions.
Frequency	Displays the average number of INAP transactions per second within each group.
Invoke Frequency	Displays the average number of Invokes per second within each group.
Timeout Frequency	Displays the average number of timeouts per second within each group.
Priority	Displays a priority value calculated by OSIX, based on the deviation between current value and set alarm value, and the set buffer size. (Circuit, ISDN, INAP)
Total Count	Displays the total amount of call attempts counted in the group since the counters were last reset. (Circuit, ISDN, INAP)

Table 5: Main window columns (Continued)

10.5.1.3 Call group information

If you want to view detailed information about the call group and/or start Call Trace or Protocol Analyser with an automatic filter for the call group, double-click the group to open the Call Group Information dialog box.

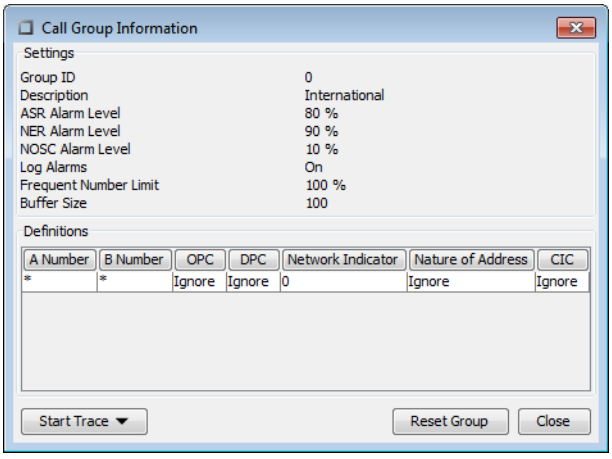


Figure 59: Call Group Information dialog box for Circuit

The available parameters are:

A Number	Displays the calling number (Circuit, ISDN, INAP)
B Number	Displays the called number (Circuit, ISDN, INAP)
OPC	Displays the originating point code (Circuit, ISDN, INAP)

Table 6: Call Group parameters

DPC	Displays the destination point code (Circuit, ISDN, INAP)
NI	Displays the network indicator (Circuit, ISDN)
NoA	Displays the nature of address (Circuit, ISDN)
CIC	Displays the circuit identification code (Circuit, ISDN)
Destination Route Address	Displays the destination route address (INAP)
Called BCD	Displays the called BCD number (INAP)
S Key	Displays the Service Key (INAP)
Called SSN	Displays the called subsystem number (INAP)
Calling SSN	Displays the calling subsystem number (INAP)

Table 6: Call Group parameters (Continued)

10.5.2 Server configuration

The server configuration is very similar for the circuit-switched protocols and for ISDN. For INAP, however, the settings are completely different.

10.5.2.1 Main settings

When configuring the Performance Analyser application for Circuit and ISDN, you have a vast number of options on how to set up the call groups, the alarm levels you want each group to have, which release causes should be counted as successful, the maximum number of seconds for a short call, etc. You can also select to not have alarms sent if a certain number is involved in a major part of the call attempts by using the Frequent number functionality.

When configuring the Performance Analyser application for INAP, you have a vast number of options on how to set up the transaction groups, the alarm levels you want each group to have, the time interval in T1 and T2 measuring, frequency settings, buffer size, etc.

- **T1**

  The number of transactions with a maximum time, defined as T1 by your system administrator, between the start message and the second message out of the total number of transactions in percent.

- **T2**

  The number of transactions with a maximum time, defined as T2 by your system administrator, between the start message and the second message out of the total number of transactions in percent.

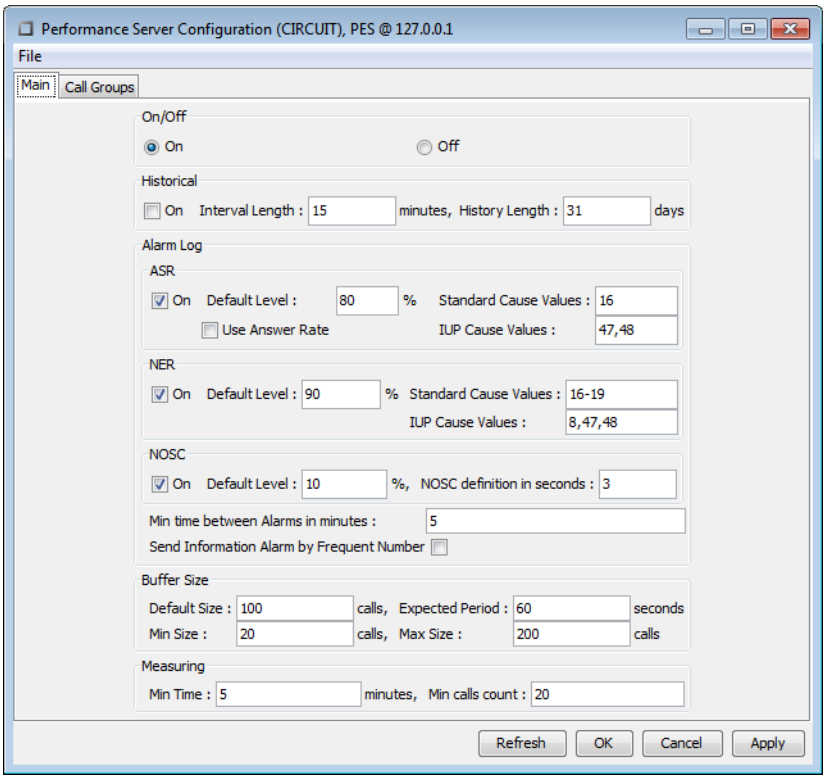


Figure 60: Performance Analyser server configuration Main tab for Circuit

10.5.2.2 Call group settings

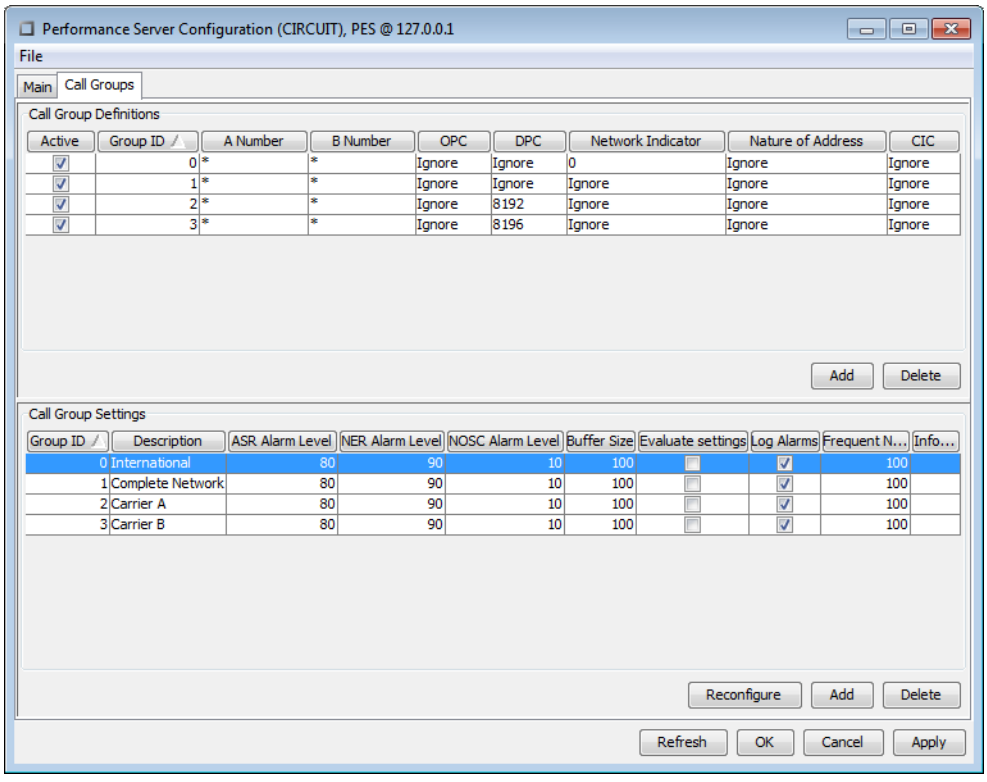


Figure 61: Performance Analyser server configuration Call Groups tab for Circuit

10.5.3 Call groups/Transaction groups

10.5.3.1 Circuit

The call groups can consist of any combination of A Number, B Number, OPC, DPC, Network Indicator, Nature of Address, and CIC. For A Numbers and B Numbers, wild cards can be used, and a plus sign can be used for a “catch all” group. Nature of Address is not applicable for call groups for IUP.

10.5.3.2 ISDN

The call groups can consist of any combination of Link, Direction, A Number, A Number Type, B Number, and B Number Type. For A Numbers and B Numbers, wild cards can be used, and a plus sign can be used for a “catch all” group.

10.5.3.3 INAP

The transaction groups can consist of any combination of A Number, B Number, Destination Route Address, Called BCD Number, OPC, DPC, Service Key, Called SSN, and Calling SSN. For A Numbers, B Numbers, Destination Route Addresses, Called BCD Numbers, and Service Keys, wild cards can be used, and a plus sign can be used for “catch all” groups. For Service Keys, you also can enter regular expressions with different types of wild cards.

10.5.4 Automatic group generation

If you are unsure about how to configure the call groups, OSIX can automatically generate groups based on different parameters.

10.5.4.1 Available parameters for Circuit

- OPC
- DPC
- Network Indicator
- Nature of Address (not for IUP traffic)
- CIC

10.5.4.2 Available parameters for ISDN

- Link
- Direction
- A Number Type
- B Number Type

10.5.4.3 Available parameters for INAP

- OPC
- DPC
- Service Key
- Called SSN
- Calling SSN

Setting one or more of these parameters to All will allow OSIX to automatically generate a new group for each new value, or combination of values, it finds.

10.5.5 Intelligent alarm settings

Setting appropriate alarm levels can be difficult the first time the application is used in your network. To give you a hint, OSIX can measure the KPI values for the call groups/transaction groups, and calculate appropriate alarm settings for you, called “intelligent alarm settings”. You can also select to not have alarms sent if a certain number is involved in a major part of the call attempts by using the Frequent number functionality. However, this possibility is not available for INAP Frequency alarms.

10.5.6 Export

If you want to save your settings, or edit them in another environment than in the Performance Analyser server configuration, you can export your group settings, open them in Excel, and import them back into Performance Analyser later.

10.6 Mass Call

The Mass Call Application monitors call attempts made to/from specific B numbers/ A numbers for the ISUP, IUP, and BICC protocols. There are two main windows with different focus; calls made to specific B numbers, calls made by specific A numbers.

10.6.1 User interface

In the Mass Call B Number window, you can detect large amounts of call attempts made to certain numbers, which enables you to reroute calls before congestion occurs, or detect looping calls. The window displays information about the B numbers to which the call attempts are made, the A numbers placing the calls, and the DPC/NIs involved in the call setup.

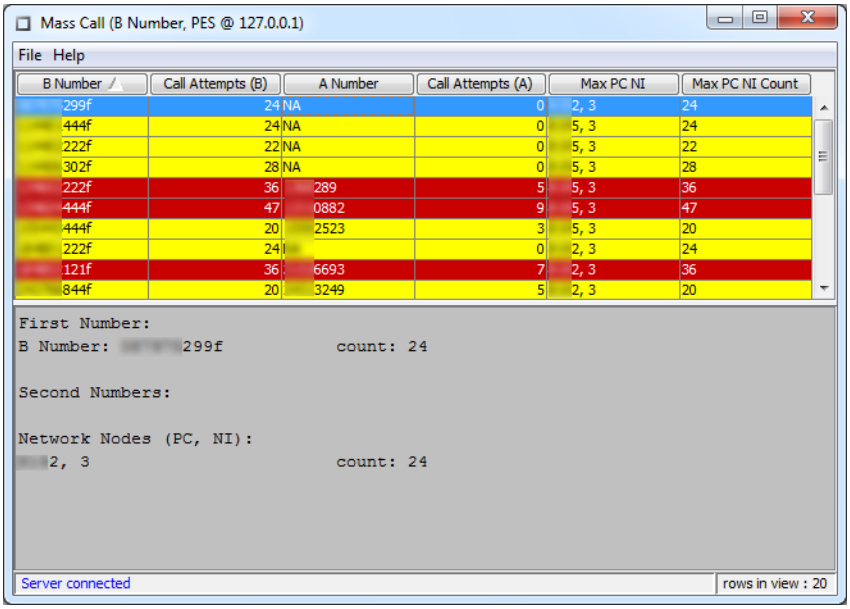


Figure 62: Mass Call B Number main window

In the Mass Call A Number window, you can detect numbers that make large amounts of call attempts, thus identifying fraudulent behaviour. For example, if a certain A number places a large amount of call attempts to different B numbers in sequence, you may suspect that a dialler is being used to hack a switch. The window displays information about the B numbers to which the call attempts are made, the A numbers placing the calls, and the OPC/NIs involved in the call setup.

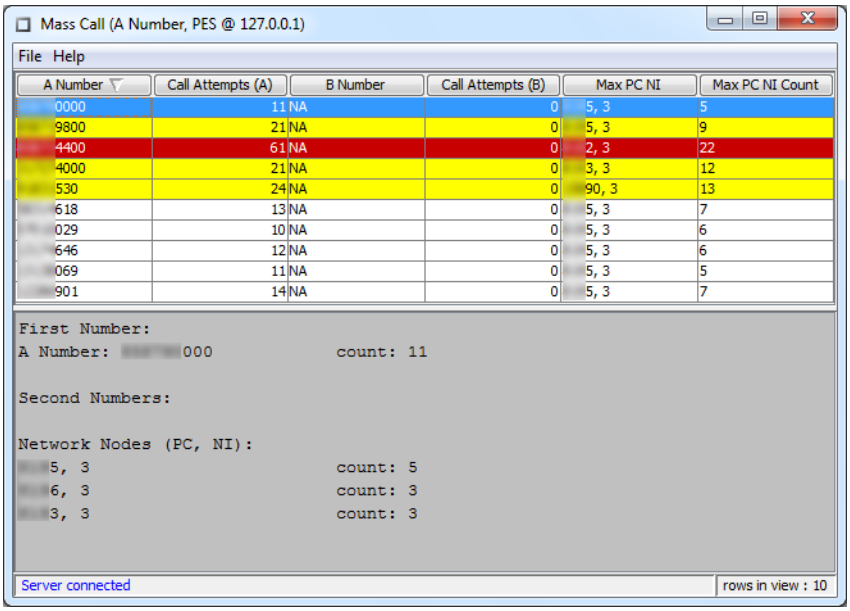


Figure 63: Mass Call A Number main window

The configuration of the Mass Call application is very easy, and enables you to set thresholds for the number of call attempts that have to be made before a number appears in the main window, as well as set the amount of unique numbers you wish to see in the main window. You can also set specific alarm levels for numbers, or number sequences that frequently have high amounts of call attempts.

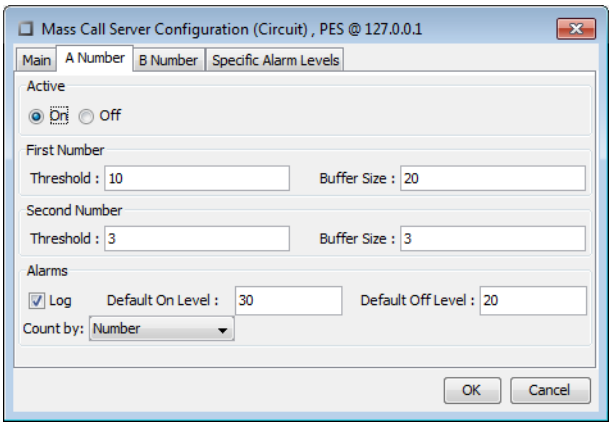


Figure 64: Mass Call Server Configuration window

10.7 Real Time Statistics

10.7.1 User interface

The main window in the Real Time Statistics application displays the different settings for your diagrams, with the top half displaying general settings for sampling rate, measure history, etc., and the bottom half the filter settings that determine which messages/transactions should be counted in the diagram.

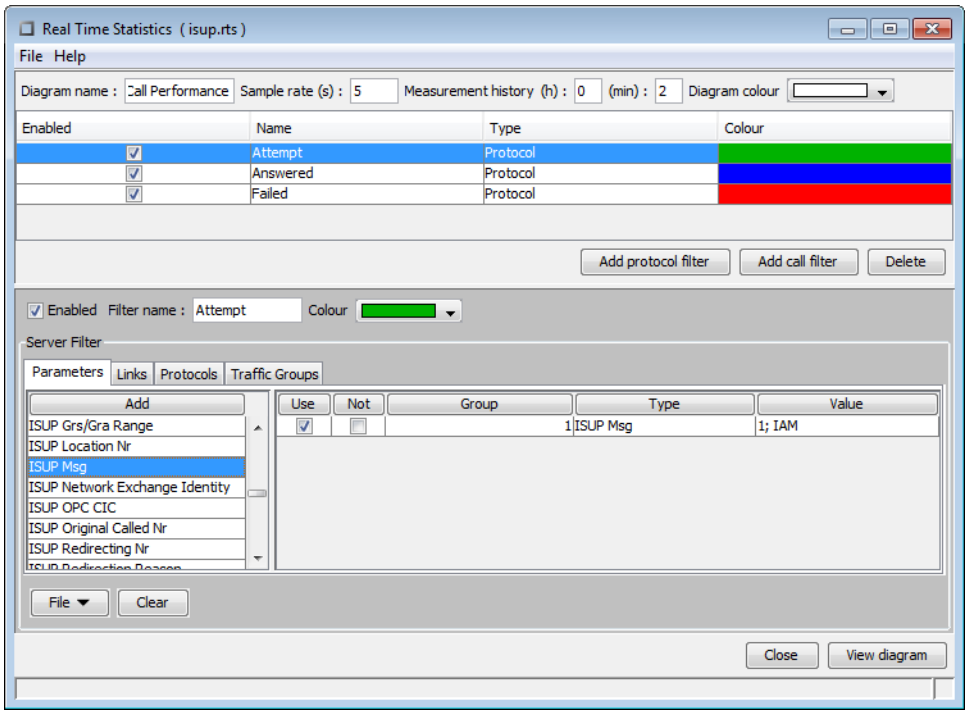


Figure 65: Real Time Statistics main window

10.7.2 Statistical Information

When you are finished with the diagram settings, the statistical information can be viewed either in table format, or in diagram format in real time.

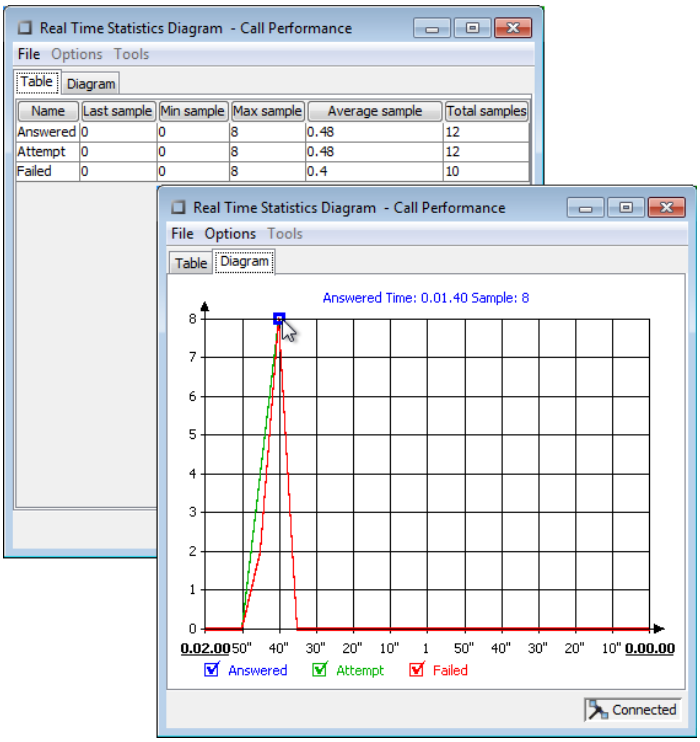


Figure 66: The Real Time Statistics Diagram

In this view you can also select to save the information as a comma-separated file, which can then be opened in a word processing or spreadsheet application.

10.7.3 Filters

There are four different types of filter:

- **Traffic groups** - The links in your network are divided into one or more traffic groups, and you must select at least one traffic group before you can start monitoring statistical information over messages/transactions in real time.
- **Parameters** - You can set a filter on any parameter value visible in the main window. This filter type also allows you to exclude messages/transactions with specific values from your statistical information.
- **Links** - You can select to only view statistical information about messages/transactions that are sent on one or more specific links.
- **Protocols** - If you are running more than one protocol, you can easily choose to only view statistical information about messages/transactions in a certain protocol type.

10.7.3.1 Combining filter criteria

Filters can be set to display either messages where a certain parameter equals a certain value, or messages where a certain parameter does NOT equal a certain value. The set filter criteria can then be combined with AND/OR functionality.

10.7.3.2 Saved filters

Any filters you have previously created and saved in either Call Trace or Protocol Analyser can be opened and used in the Real Time Statistics application.

10.8 Network Status

10.8.1 User interface

The main window in the Network Status application has four different views:

- **Level 1** – displays alarms detected on the links connected to the LIMs
- **Surveyor** – displays different maps over the network and any alarms on level 2 or 3
- **Performance** – displays the number of alarms detected by the Performance Analyser and Mass Call applications
- **Link Status** – displays the current status on all different links

and two different dialog boxes:

- **Active Alarms** – displays all the currently active alarms on all the different levels
- **Alarm Log** – displays all alarms that have been cleared

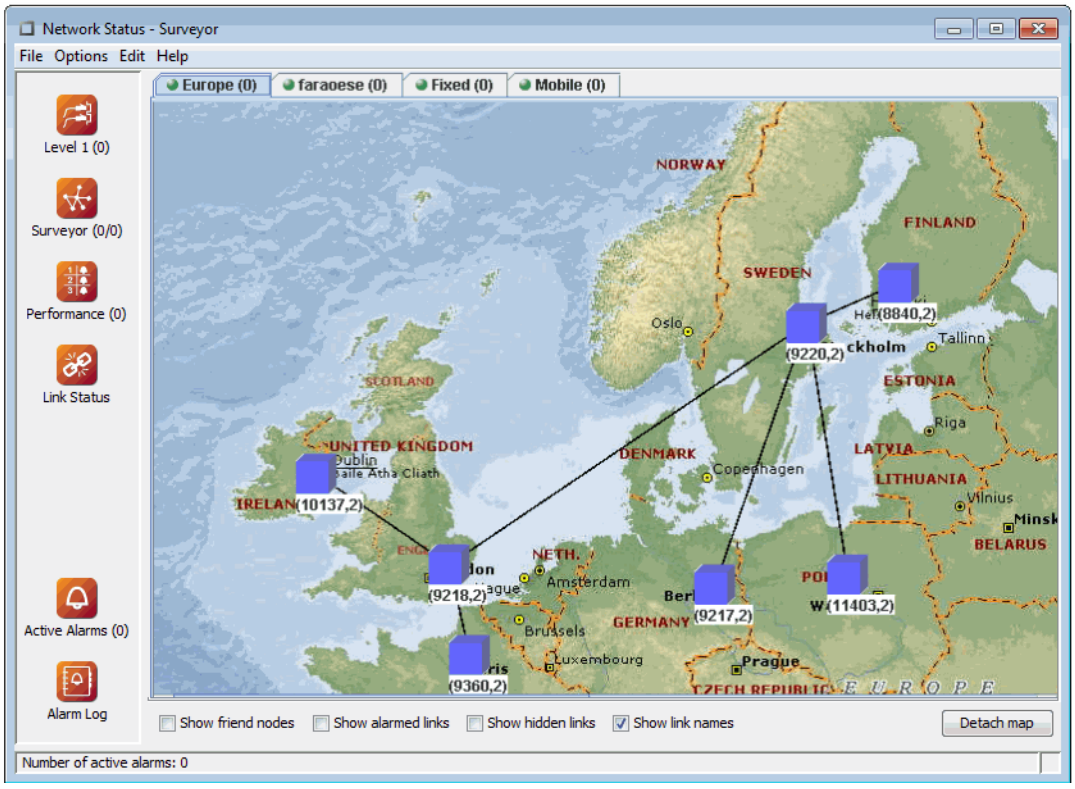


Figure 67: Network Status main window map view

SS7 links and nodes (PCs) connected to the system are automatically detected, and as soon as network problems occur, for example Transfer Prohibited, the corresponding link and/or node will start blinking and an alarm will be registered in the Active Alarms dialog box.

The Active Alarms dialog box contains information about all the alarms currently active, and the Alarm Log contains information about historical alarms.

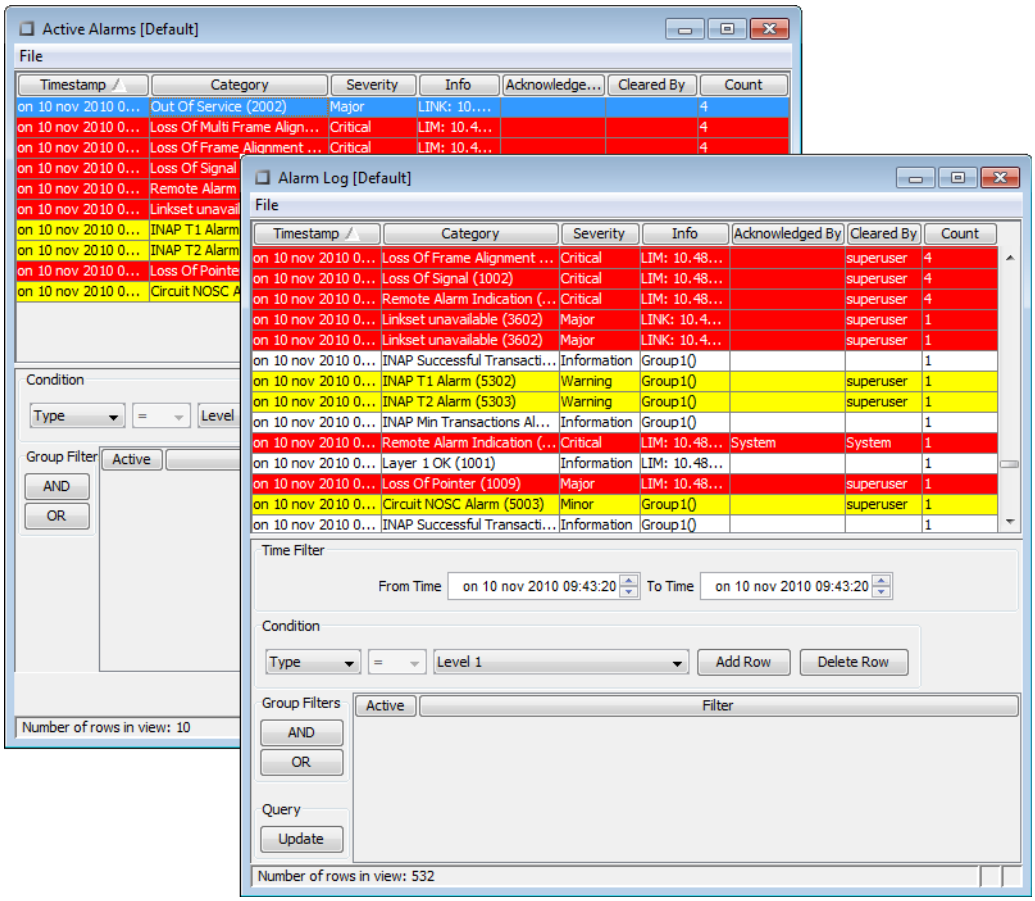


Figure 68: Active Alarms and Alarm Log dialog boxes

Both of these dialog boxes contain comprehensive filter functionality for viewing the specific events that are of interest. All alarms are also available as SNMP traps and/or as email messages.

10.9 Statistics Alarm

With the Statistics Alarm application you can set up alarms to be generated when certain filter criteria for protocol messages or calls/transactions are met.

10.9.0.1 Easy-to-Use GUI

The GUI (Graphical User Interface) allows you to easily set up alarms based on either protocol messages or calls/transactions.

10.9.1 User interface

The main window in Statistics Alarm consists of an overview over the different alarms that have been set up, with four buttons at the bottom of the window.

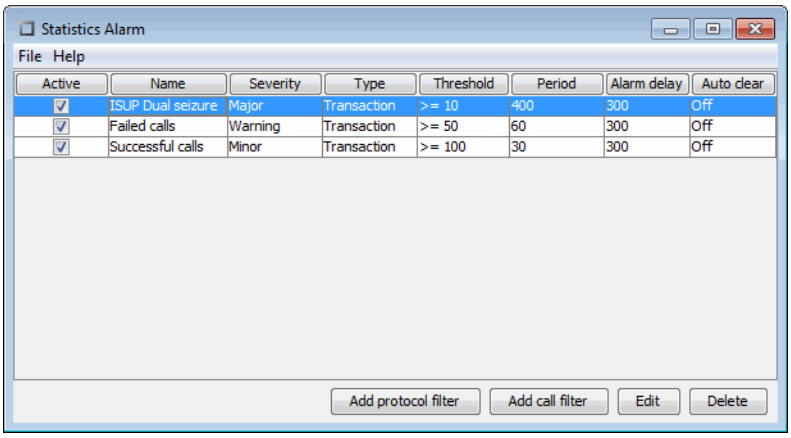


Figure 69: Statistics Alarm main window

Changing the size of the main window will also dynamically adjust and resize the columns to give the best fit in the available space.

10.9.2 Alarm settings

Alarms are set up based either on protocol messages and their contents, or based on calls/transactions and their contents.The alarm settings allows you to set up alarms to be generated either at first occurrence, or at a certain number of occurrences over a certain period of time. You can also set up the alarms to be automatically cleared or not.

You can activate/deactivate alarms settings that you have created, as well as edit and delete existing alarm settings.

10.9.2.1 Protocol filter settings

The protocol filter setting will generate an alarm when there are protocol messages passing the filter, or when the number of messages passing the filter exceeds the set threshold during the set time interval.

The alarms will be sent to the Network Status application and to any third-party applications of your choice.

When making protocol filter settings, you can use the following filter types: Parameter filters, Link filters, Protocol filters, and Traffic group filters.

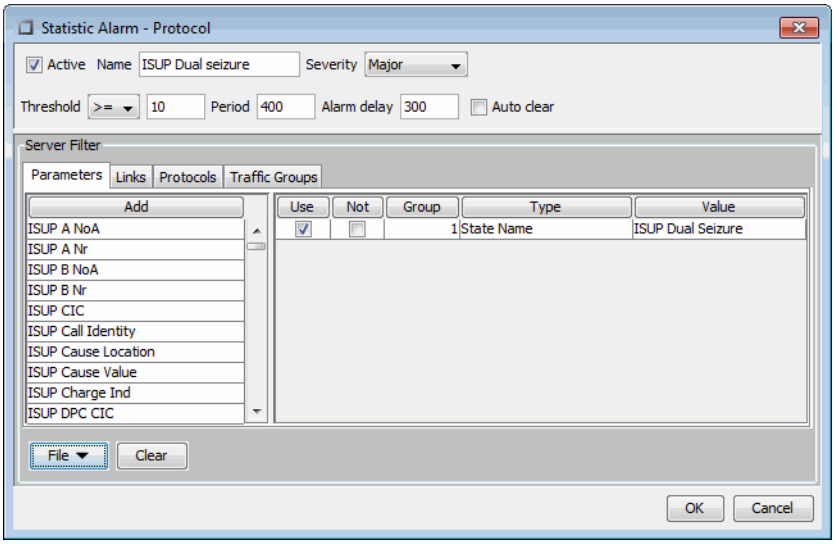


Figure 70: Parameters tab sample for protocol filter settings

10.9.2.2 Transaction filter settings

The transaction filter setting will generate an alarm when there are calls/ transactions passing the filter, or when the number of calls/transactions passing the filter exceeds the set threshold during the set time interval.

The alarms will be sent to the Network Status application and to any third-party applications of your choice.

When making transaction filter settings, you can use the following filter types: Parameter filters, Link filters, Protocol filters, Traffic group filters, and Duration filters.

10.9.3 Filter settings management

Filter settings are fully editable and can also be saved for later use.

If you want to keep a filter setting but not use it at the moment, you can select to deactivate the filter setting, and then activate it again when you want to use it.

To delete a filter setting, select it in the main window and click the Delete button.

11 OSIX Monitoring for mobile networks

OSIX Monitoring extracts information from signalling networks and includes applications for monitoring and troubleshooting, xDR generation/SNMP trap generation, email messaging, and OSS (Operation Support System) applications. The following sections show a few examples for mobile networks.

11.1 Protocols and interfaces

OSIX Monitoring supports all major telecommunication technologies within 2G, 3G, 4G, and 5G. The system supports a wide range of interfaces and protocols and supports legacy and state-of-the-art technology; for example, both legacy Gb and 5G SA. In a majority of installations, several network topologies are monitored in the same system simultaneously.

For protocol compliance, see the *OSIX Supported Protocols* document.

All supported protocols have a large set of predefined parameters available for filtering. For information about protocol parameters, see chapter *15 Protocol parameters*.

11.2 Mobile network features

- Support for all major GSM/GPRS/UMTS/4G and 5G interfaces, including different vTAP dialects.
- Real-time deciphering of Gb, EMM/ESM, SIP over ESP, and 5G NAS.
- Real-time mapping of TMSI/P-TMSI/GUTI to IMSI.
- User-plane handling of GTP-U with different levels of aggregation. This offers an effective approach for monitoring huge data volumes. Flow aggregation enables troubleshooting on individual TCP/UDP flows, including user data application protocols, for example HTTP, DNS, SMTP, FTP, and RTSP. Session aggregation gives a lower hardware footprint, focusing on key summary information from user-plane signalling
- Multi-protocol Client Correlation for voice, text and ongoing/closed data sessions.
- Real-time KPI measurements for Iu-CS/Iu-PS/Gb and Gn.
- Support for full 10GbE Monitoring.
- Automatic detection of SCTP associations/endpoints with map view and included alarming and status functionality.

11.2.1 Mobile Data Monitoring (MDM)

The OSIX system architecture is specially developed to handle mobile data. The architectural changes are applied to the GTP protocols as of now, but will be deprecated in future releases

The features are summarised below:

- Persistent system components - RTR and PRS components can keep the state of sessions on restarts.
- Binary message data handled on disk instead of server memory - enables components to handle a higher number of simultaneous transactions.
- Searchability for ongoing calls in Call Trace both in real-time and historical mode.

- Multi-protocol correlation for both ongoing and closed sessions.
- User Plane troubleshooting functionality in Call Trace, which allows better visibility and more dynamic filtering.

11.3 Protocol Analyser

11.3.1 User interface

In the Protocol Analyser main window you can monitor the protocol messages, either in real time or historically. You can also set different filters, or search for specific messages. You can have four different Protocol Analyser windows with different settings open at the same time.

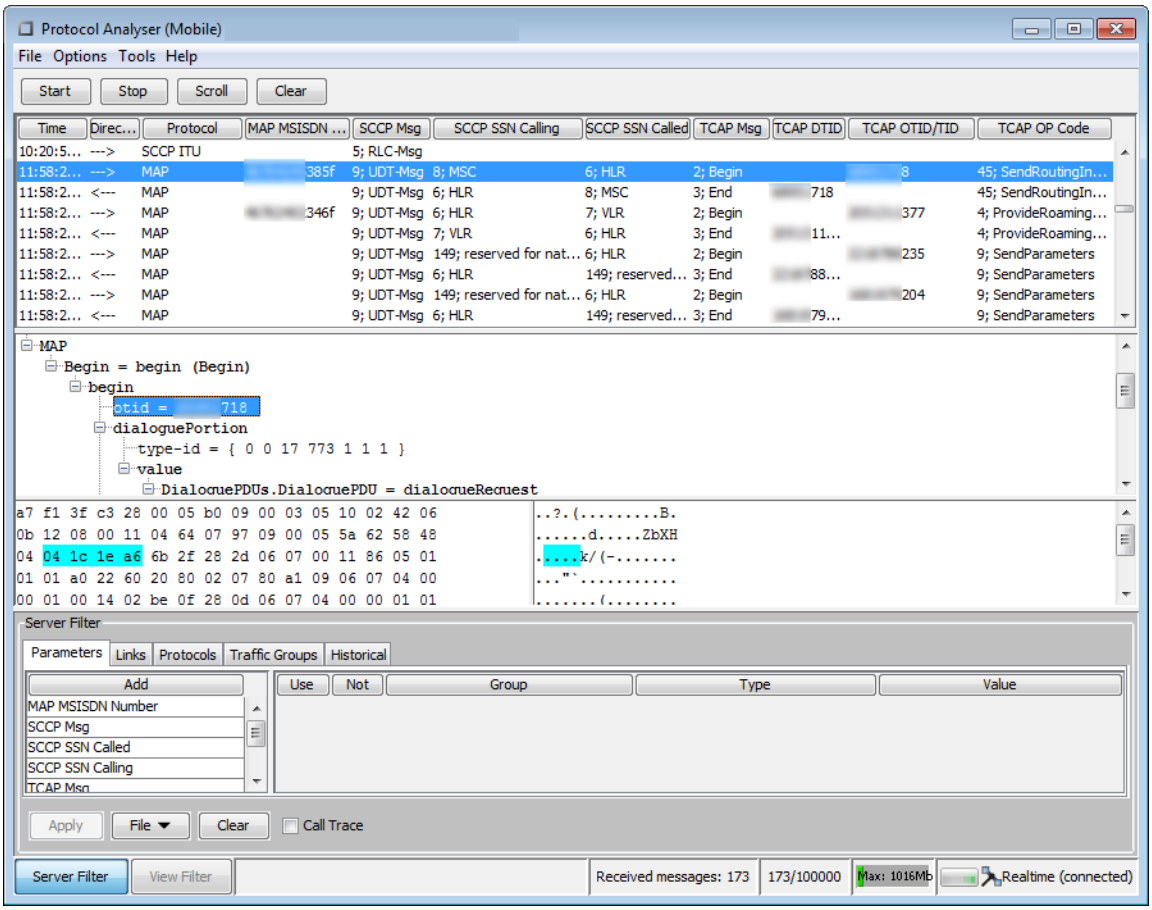


Figure 71: Protocol Analyser main window

11.3.1.1 Message details

The window is divided into several parts—one displaying the different protocol messages, one displaying a preview of the message, one showing the hexadecimal code, one showing ASCII code, and finally the filter section. You can also choose to open a separate Message Viewer with the contents of the entire message.

Example:

The figure shows a response to the MAP operation update GPRS location with the error code “Unknown subscriber” (no such subscription exists). The error code indicates that the user failed to update the current location.

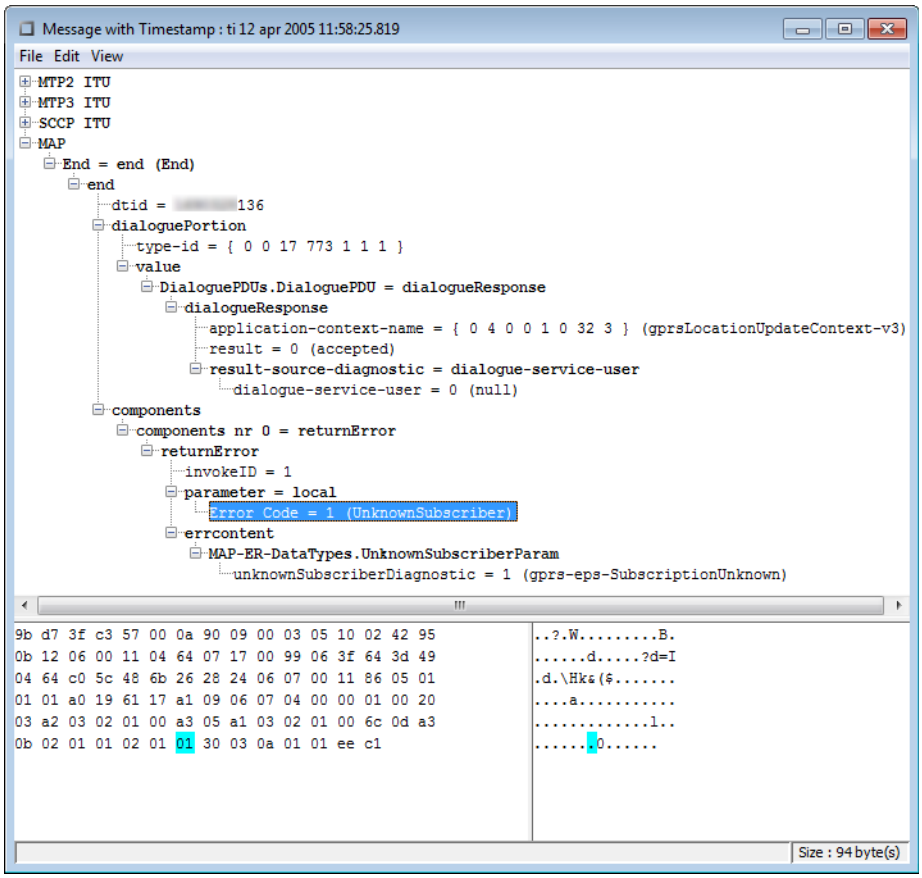


Figure 72: Message showing error code “Unknown subscriber”

11.4 Call Trace

11.4.1 User interface

In the Call Trace main window you can monitor transactions, either in real time or historically. You can also set different filters, or search for specific calls. You can have a maximum of four different Call Trace windows with different settings open at the same time.

Example:

The figure shows an example of a problem subscribers may have trying to attach through GPRS Gb if the services are not included in their subscription.

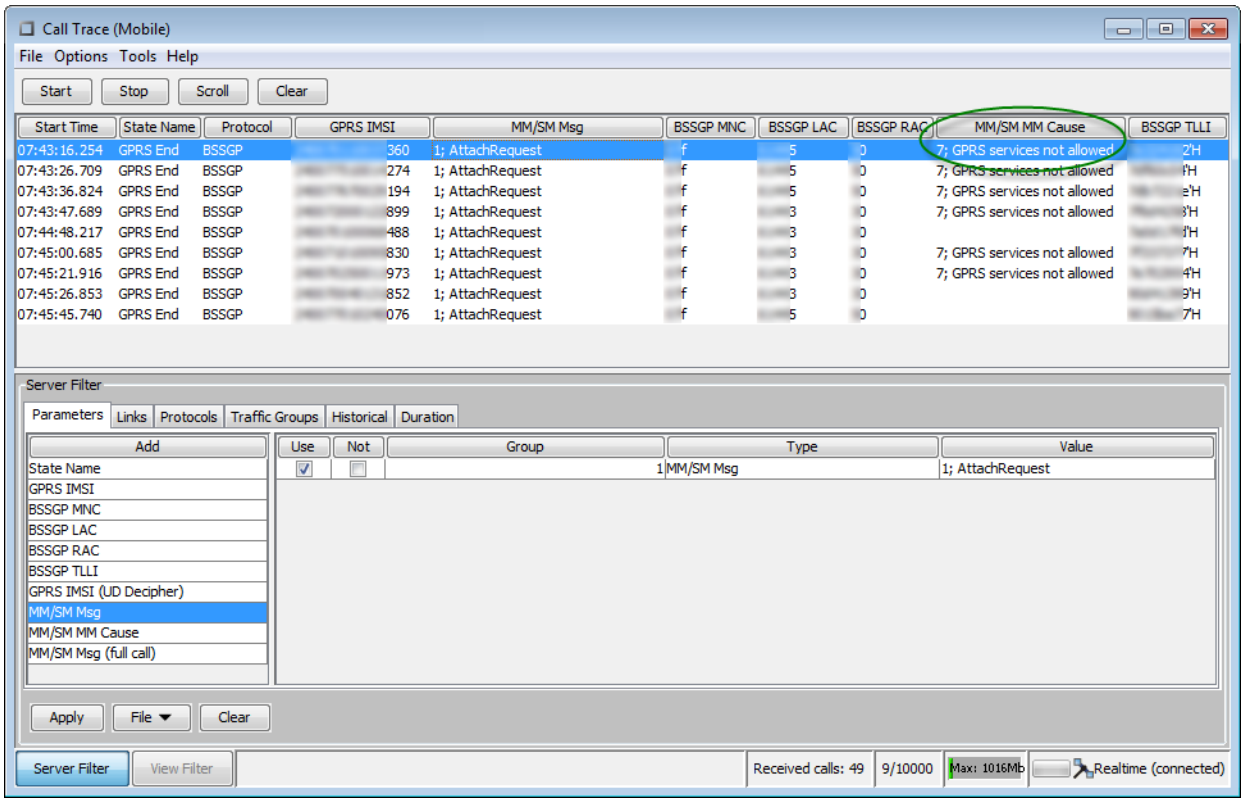


Figure 73: Call Trace main window - GPRS troubleshooting

11.4.1.1 Call details

If you want to take a closer look at a call, you can double-click a call to open the Call Window. The window is divided into several parts, or panes—one displaying the different protocol messages sent referring to the selected call, one displaying a preview of the message, one showing the hexadecimal code, one showing ASCII code, and finally one pane displaying different parameters for the call (this pane is not present in the following figure). You can also choose to open a separate Message Viewer with the contents of the entire message.

Example:

The figure shows an unsuccessful PDP connection on the Gn interface with the cause “No resources available”. This indicates that the user was not able to initiate a data session, because not enough resources were available within the network to allow the PDP Context to be created.

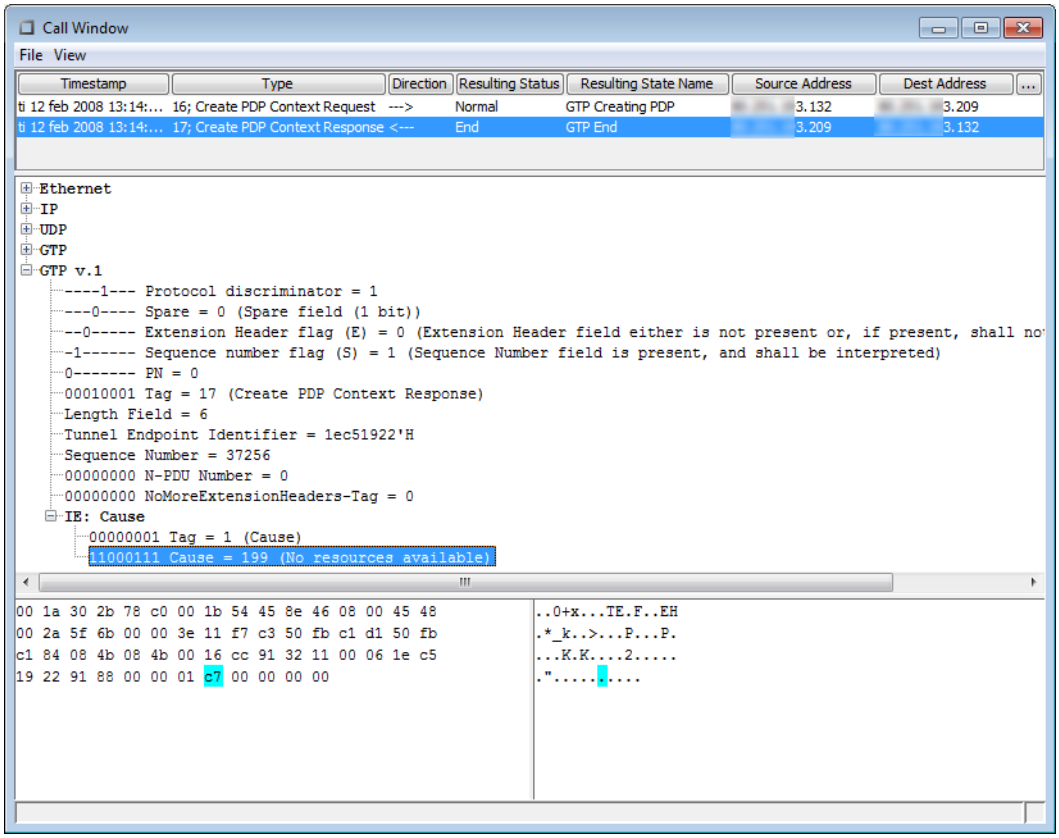


Figure 74: Call Window with cause “No resources available”

11.4.1.2 Call flow window

When viewing the call details you can also select to view the call flow in a graphical representation, where the nodes are visible and the different messages are represented with arrows.

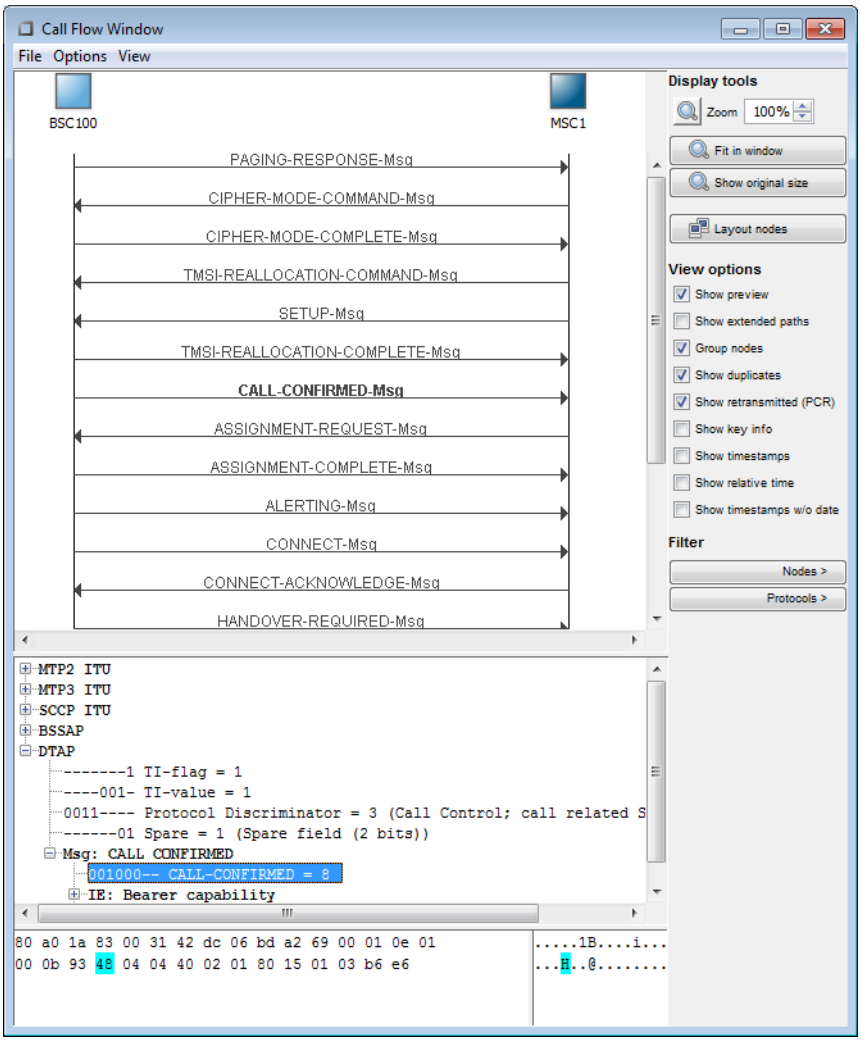
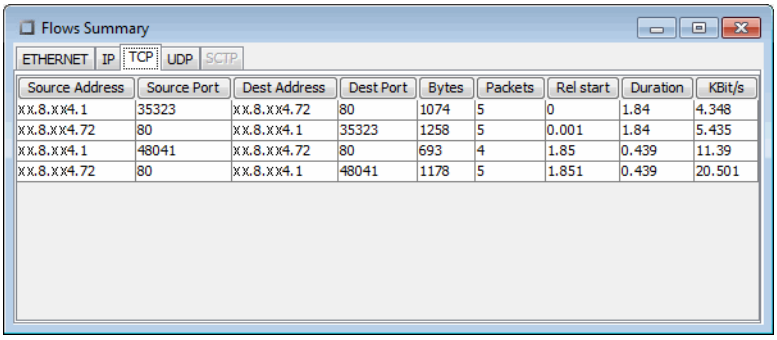


Figure 75: Call flow window

11.4.1.3 Flows summary

In the Flows Summary window, the flows between involved end points are visualised, giving a summary of Ethernet, IP, TCP, UDP and SCTP flows. Flows Summary is only supported for IP-based traffic.



Source Address	Source Port	Dest Address	Dest Port	Bytes	Packets	Rel start	Duration	KBit/s
xx.8.xx4.1	35323	xx.8.xx4.72	80	1074	5	0	1.84	4.348
xx.8.xx4.72	80	xx.8.xx4.1	35323	1258	5	0.001	1.84	5.435
xx.8.xx4.1	48041	xx.8.xx4.72	80	693	4	1.85	0.439	11.39
xx.8.xx4.72	80	xx.8.xx4.1	48041	1178	5	1.851	0.439	20.501

Figure 76: Flows Summary window

11.4.2 Client correlation

Call correlation is done between all messages with operation codes relating to the same procedure, regardless of where in the network the messages are sent. All messages relating to the same procedure are presented in the Call window and the Call Flow window.

There is also correlation available for certain protocols, parameters, and procedures, where all messages relating to the entire process are presented in the Call window. For mobile networks, correlation is available for:

- Mobile Transactions (calls, SMSs, USSD)

  Protocols: ISUP, BICC, MAP, IS-41, BSSAP, RANAP, INAP/CAP, ALCAP, BSSAP+, MEGACO

- Mobile Packet - (Iu-PS, Gb, S1-MME, S6a, SGs, Gn/Gp, S11, S5/S8, Gi RADIUS, Ut HTTP, Gx, Gy, Rx, Sxa, Sxb)

  Protocols: GTP, RANAP, GPRS Gb, RADIUS, DIAMETER, S1AP, MAP, SGSAP, HTTP, INAP, RRC

- IMS and Mobile

  Protocols: ISUP, SIP, BICC, MGCP, H.248, H.225, ISDN, INAP/CAP, DNS, DIAMETER, MAP, RANAP, BSSAP, SGsAP, S1AP, GTP, LDAP, HTTP, HTTP/2, PFCP, NGAP, SMPP

- End-to-end - a combination of Mobile Packet and IMS & Mobile

See the *OSIX Call Trace User Guide* for more information about recommended client correlations per domain.

11.4.2.1 Client correlation examples for mobile transactions

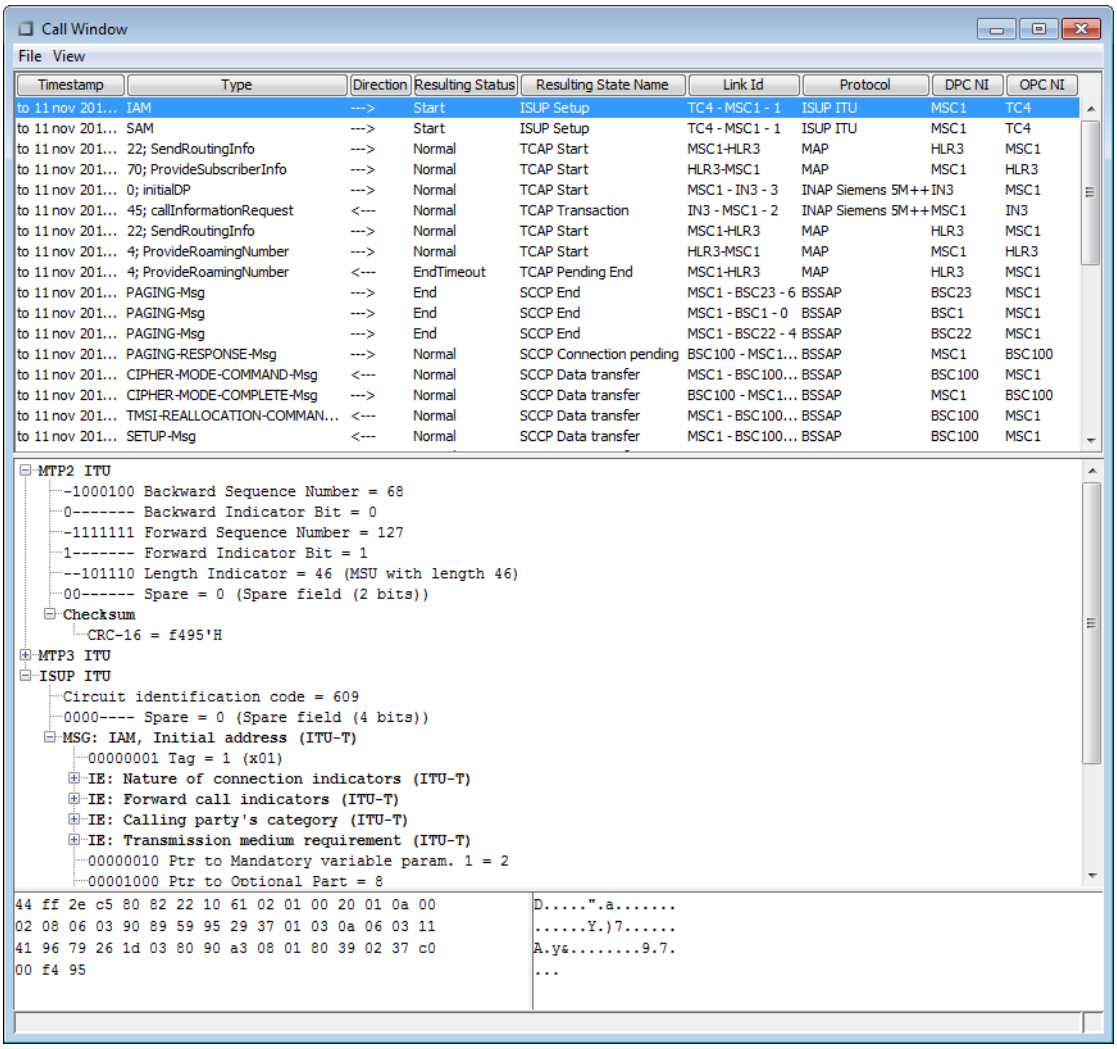


Figure 77: Call window for mobile transactions

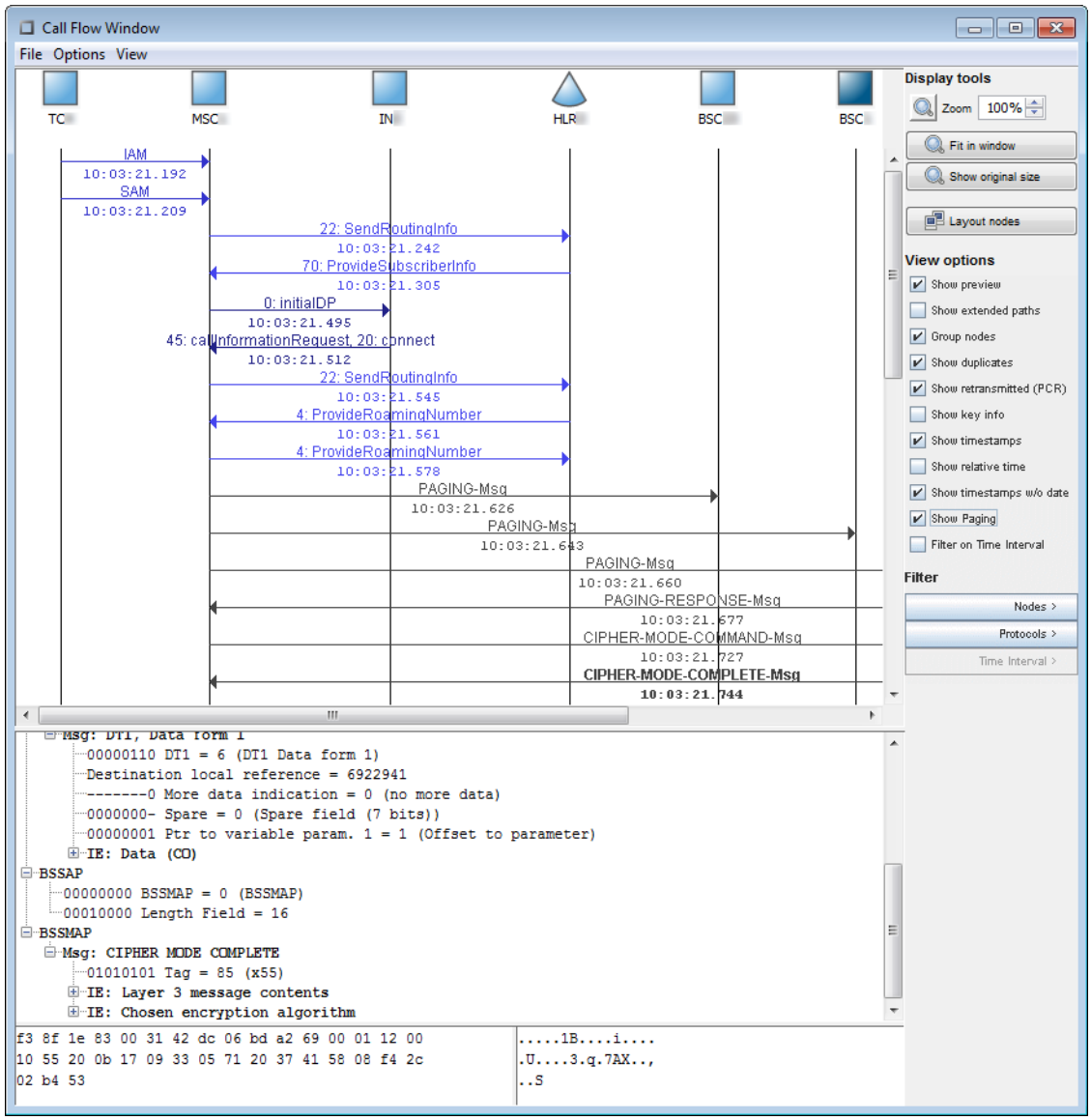


Figure 78: Call flow window for mobile transactions

11.5 Performance Analyser

The Performance Analyser application monitors Key Performance Indicators (KPIs) for different call groups in real time, which will inform you about the performance in your network. For mobile networks, Performance Analyser is available for MAP, IS-41, GPRS, GTP, CAP, Iu-CS, Iu-PS, and CIRCUIT (ISUP, BICC).

11.5.1 User interface

The Performance Analyser main window displays the call group KPIs in real time. You can have one window open per protocol, and the information is updated every ten seconds by default (this is configurable per client).

Example:

The figure illustrates verification of a new SM-SC. It shows that the average response time for sending a text message is over two seconds. These statistics can be investigated further on cause codes in Real Time Statistics or through built-in drill-down to Call Trace or Protocol Analyser.

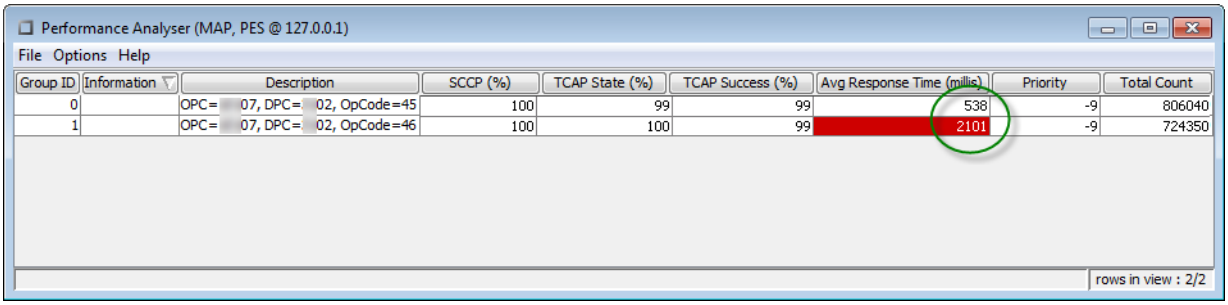


Figure 79: The Performance Analyser Main Window for MAP

The Avg Response Time (mills) column indicates serious problems. It can, for example, indicate under-dimensioned nodes and/or high traffic load.

TCAP KPIs can, for example, indicate that the application layer in an SM-SC is down.

11.5.1.1 Columns

The following columns are available in the main window:

Group ID	Displays the individual group's unique number.
Information	If the KPIs for the group have been measured by OSIX, and set automatically, this column displays the results from the last evaluation.
Description	If the group has been automatically generated by OSIX, this column will display what parameter values the group consists of, otherwise the system administrator can set an appropriate name for this column.
SCCP %	Displays the number of SCCP transactions that have not received any unspecified return causes, out of the total number of SCCP transactions, in per cent. (MAP, IS-41)
TCAP State %	Displays the number of TCAP transactions that have not timed out or aborted, out of the total number of TCAP transactions, in per cent. (MAP, IS-41)

Table 7: Main window columns

TCAP Success %	Displays the number of TCAP transactions that have not received any unspecified error codes, out of the total number of TCAP transactions, in per cent. (MAP, IS-41)
Avg Response Time	Displays the average response time (time between the Begin message and the first Continue message) for the number of transactions specified in the groups' buffer. (MAP, IS-41)
Attach %	Displays the number of attach accepts, out of the total number of attach requests, in per cent. (GPRS, Iu-PS)
Attach Count	Displays the total amount of attach requests counted in the group since the counters were last reset. (GPRS, Iu-PS)
PDP Activate %	Displays the number of PDP activations terminated with the session management causes (SM cause 36 by default), defined by the system administrator, out of the total number of PDP activations, in per cent. (GPRS, Iu-PS)
PDP Activate Count	Displays the total amount of PDP activations counted in the group since the counters were last reset. (GPRS, Iu-PS)
ASR %	Displays the Answer Seizure Ratio, that is, the number of answered calls, out of the total number of call attempts, in per cent. (Iu-CS)
NER %	Displays the Network Efficiency Ratio, that is, the number of calls terminated with specified release causes, out of the total number of call attempts, in per cent. (Iu-CS)
NOSC %	Displays the number of calls with a conversation of time of less than the specified time interval (3 sec by default), out of the total number of calls, in per cent. (Iu-CS)
Call Count	Displays the total amount of call attempts counted in the group since the counters were last reset. (Iu-CS)
SMS %	Displays the number of successful SMS transactions, out of the total number of transactions, in per cent. (Iu-CS)
SMS Count	Displays the total amount of SMS transactions counted in the group since the counters were last reset. (Iu-CS)
Transaction Success (%)	Displays the transaction success rate in per cent. The default GTP success release cause is 128. (GTP)
Response Delay (%)	Displays the delay between a request and a response, for example between a Create PDP request and a Create PDP response in per cent. The control signalling affects the value, not the user data. (GTP)
Avg. Response Delay (ms)	Displays the delay between a request and a response, for example between a Create PDP request and a Create PDP response, in milliseconds. The control signalling affects the value, not the user data. (GTP)
Min Throughput Downlink (%)	Displays the minimum throughput downlink (for example when a user is browsing a web page) in per cent. (The number of transactions below a threshold value set by the System Administrator.) (GTP)
Min Throughput Uplink (%)	Displays the minimum throughput uplink (for example when a user is sharing a file) in per cent. (The number of transactions below a threshold value set by the System Administrator.) (GTP)
Max Throughput Downlink (%)	Displays the maximum throughput downlink (for example when a user is browsing a web page) in per cent. (The number of transactions below a threshold value set by the System Administrator.) (GTP)

Table 7: Main window columns (Continued)

Max Throughput Uplink (%)	Displays the maximum throughput uplink (for example when a user is sharing a file) in per cent. (The number of transactions below a threshold value set by the System Administrator.) (GTP)
Avg. Throughput Downlink (kbit/s)	Displays an average value of the buffered throughput downlink (kbit/s). This value is only for information and it is not alarm-based. (The number of transactions below a threshold value set by the System Administrator.) (GTP)
Avg. Throughput Uplink (kbit/s)	Displays an average value of the buffered throughput uplink (kbit/s). This value is only for information and it is not alarm-based. (The number of transactions below a threshold value set by the System Administrator.) (GTP)
Priority	Displays the group's priority based on a combination of the discrepancy between the group's actual statistical value and alarm value, and the group's buffer size. The groups are sorted by this column by default in order for you to easier detect the groups with the largest discrepancies. (GTP)
Total Count	Displays the total number of transactions made within each group since the last server configuration, or since you last reset the group. (GTP)

Table 7: Main window columns (Continued)

11.5.1.2 Call Group Information dialog box

If you want to view detailed information about a transaction group and/or start Call Trace or Protocol Analyser with an automatic filter for the transaction group, double-click the group to open the Call Group Information dialog box.

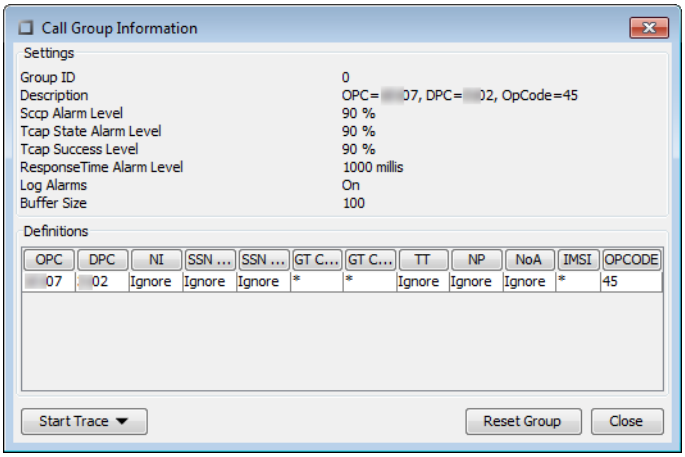


Figure 80: Call Group Information dialog box for MAP

The following parameters are available:

OPC	Displays the originating point code. (MAP, IS-41, Iu-CS, Iu-PS)
DPC	Displays the destination point code. (MAP, IS-41, Iu-CS, Iu-PS)
SSN	Displays the subsystem number. (MAP, IS-41)
GT Called	Displays the called global title. (MAP, IS-41)
GT Calling	Displays the calling global title. (MAP, IS-41)
Called GT TT	Displays the translation type for the calling global title. (MAP, IS-41)
Called GT NP	Displays the numbering plan for the calling global title. (MAP, IS-41)

Table 8: Call Group parameters

Called GT NoA	Displays the nature of address for the calling global title. (MAP, IS-41)
IMSI	Displays the international mobile subscriber identity. (MAP, IS-41, GPRS, Iu-CS, Iu-PS)
Op Code	Displays the operation code. (MAP, IS-41)
MCC	Displays the mobile country code. (GPRS)
MNC	Displays the mobile network code. (GPRS)
LAC	Displays the location area code. (GPRS, Iu-CS, Iu-PS)
RAC	Displays the routing area code. (GPRS, Iu-CS, Iu-PS)
CI	Displays the cell identifier. (GPRS)
APN	Displays the access point name. (GPRS, Iu-PS)
Calling number	Displays the calling number. (Iu-CS)
Called number	Displays the called number. (Iu-CS)
NI	Displays the network indicator. (Iu-CS, Iu-PS)
SAC	Displays the service area code. (Iu-CS, Iu-PS)
APN	Displays the Access Point Name. (GTP)
SGSN	Displays the Serving GPRS Support Node. (GTP)
GGSN	Displays the Gateway GPRS Support Node. (GTP)
Transaction Type	Displays the Transaction Type for Create PDP, Delete PDP, Update PDP and SGSN Context. (GTP)

Table 8: Call Group parameters (Continued)

11.5.2 Server Configuration

The server configuration for GPRS and Iu-PS are quite similar, while the server configuration for MAP and Iu-CS are a bit different. The server configuration for MAP and IS-41 are almost identical.

11.5.2.1 Main settings

When configuring the Performance Analyser application you have a vast number of options on how to set up the transaction groups, the alarm levels you want to have, which cause values, time intervals, buffer size, etc.

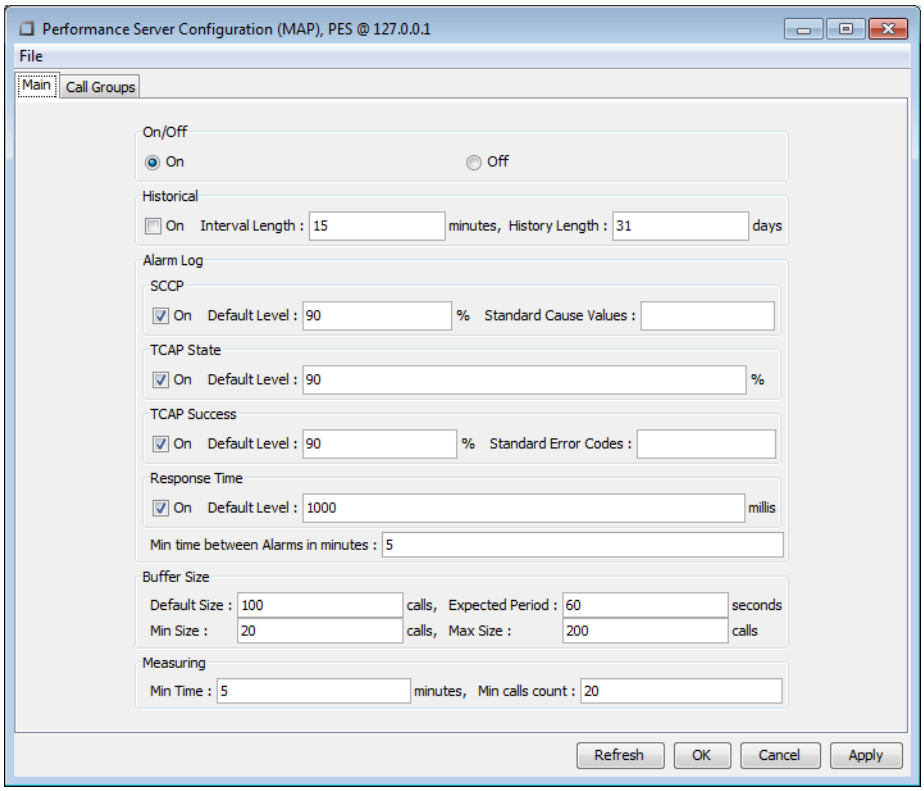


Figure 81: Performance Analyser server configuration for MAP – Main tab

11.5.2.2 Call Group settings in Server Configuration dialog box

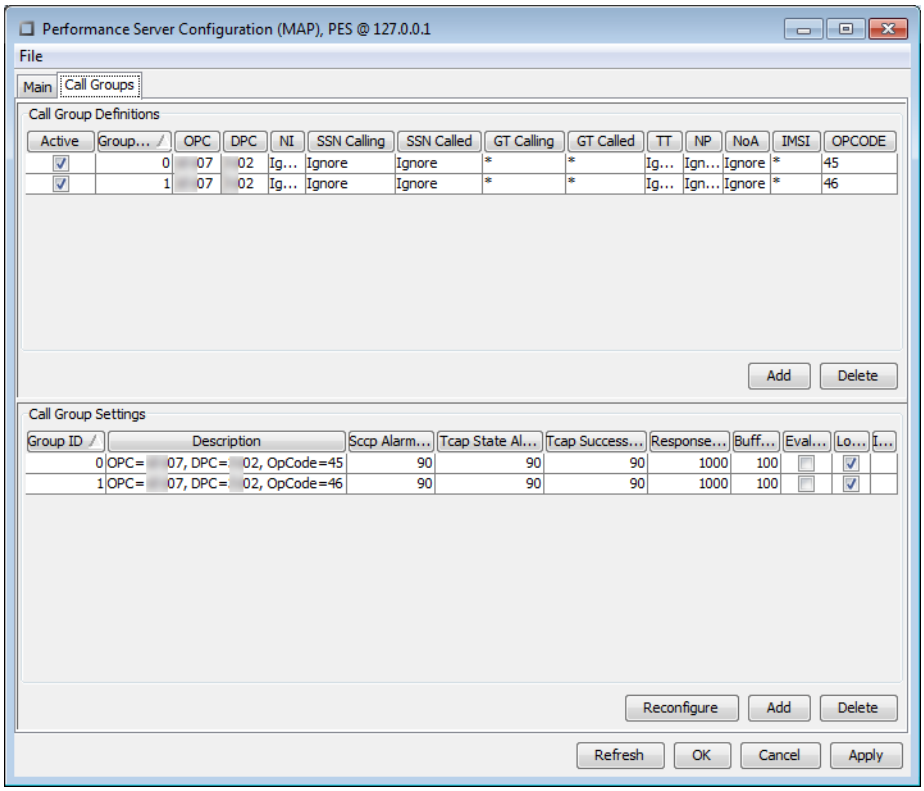


Figure 82: The Performance Analyser server configuration for MAP – Call Groups tab

11.5.3 Transaction groups

The transaction groups can consist of any combination of the parameters listed in the Call Group Definitions section. For IMSI, called and calling numbers can use wild cards, and for access point names you can enter regular expressions with different types of wild cards.

11.5.4 Automatic group generation

If you are unsure about how to configure the transaction groups, you can set one or more of the parameters with an All/Ignore drop-down list to All, which will allow OSIX to automatically generate a new group for each new value, or combination of values, it finds.

11.5.5 Intelligent alarm settings

Setting appropriate alarm levels can be difficult the first time the application is used. To give you a hint, OSIX can measure the percentages for the different KPIs, and calculate appropriate alarm settings for you, called “intelligent alarm settings”.

11.5.6 Export

If you want to save your settings, or edit them in another environment than in the Performance Analyser server configuration, you can export the group settings, open them in Excel, and import them back into Performance Analyser later.

11.5.7 Performance Analyser for GTP

For mobile networks, the latest Performance Analyser application is for GTP. It monitors the following KPIs:

- Transaction Success Rate
- Response Delay
- User Data Throughput
- Total Count
- Period Count

The following figure shows the main window for GTP.

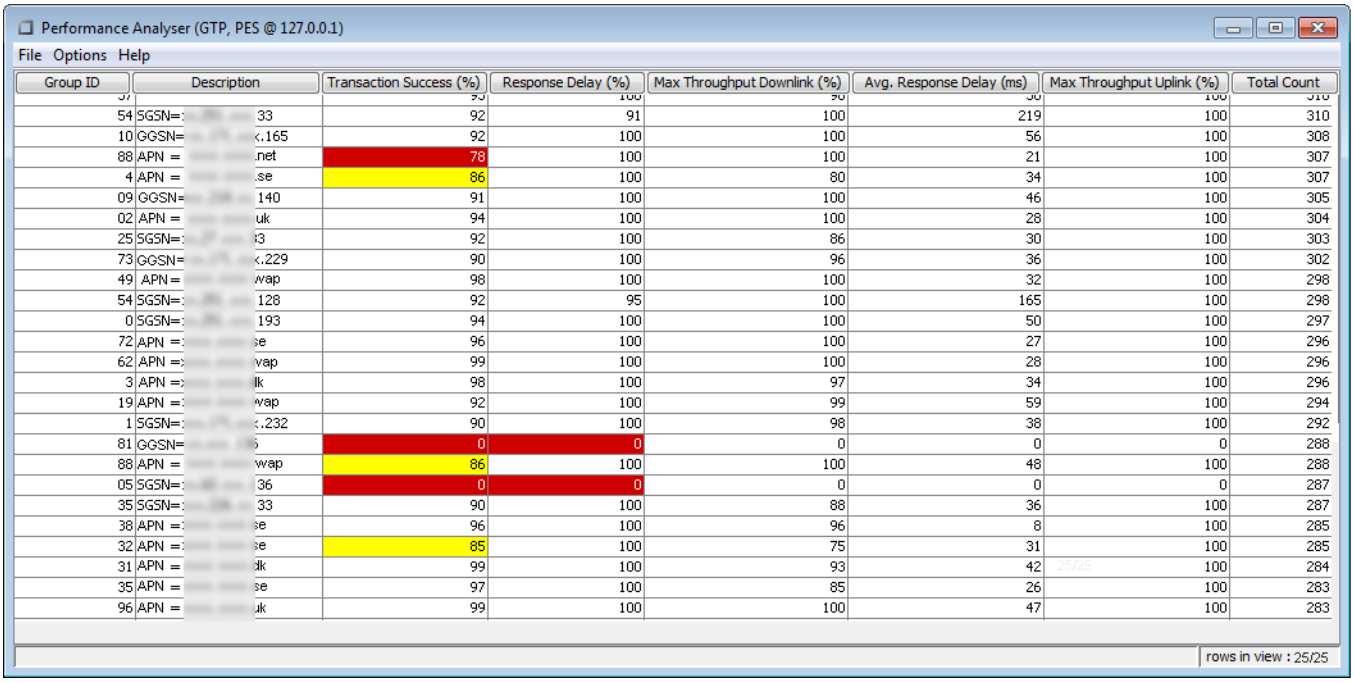


Figure 83: Performance Analyser GTP main window

The call groups consist of a combination of:

- APN
- SGSN
- GGSN
- Transaction Type for Create PDP
- Transaction Type for Delete PDP
- Transaction Type for Update PDP
- Transaction Type for SGSN Context

The following figure shows the Call Group Information window for GTP.

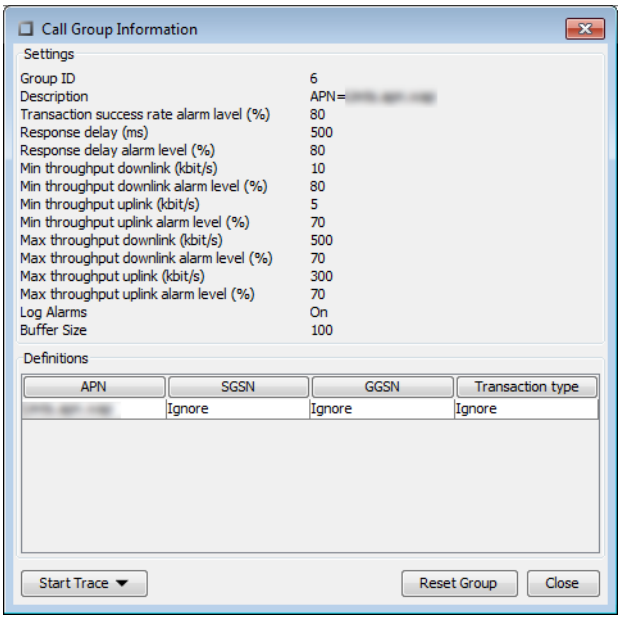


Figure 84: Performance Analyser GTP Call Group Information window

11.6 Real Time Statistics

11.6.1 User interface

The Real Time Statistics main window displays different settings for your diagrams, with the top half displaying the general settings for sampling rate, measure history, etc., and the bottom half containing the filter settings that determine which messages/transactions should be counted in the diagram.

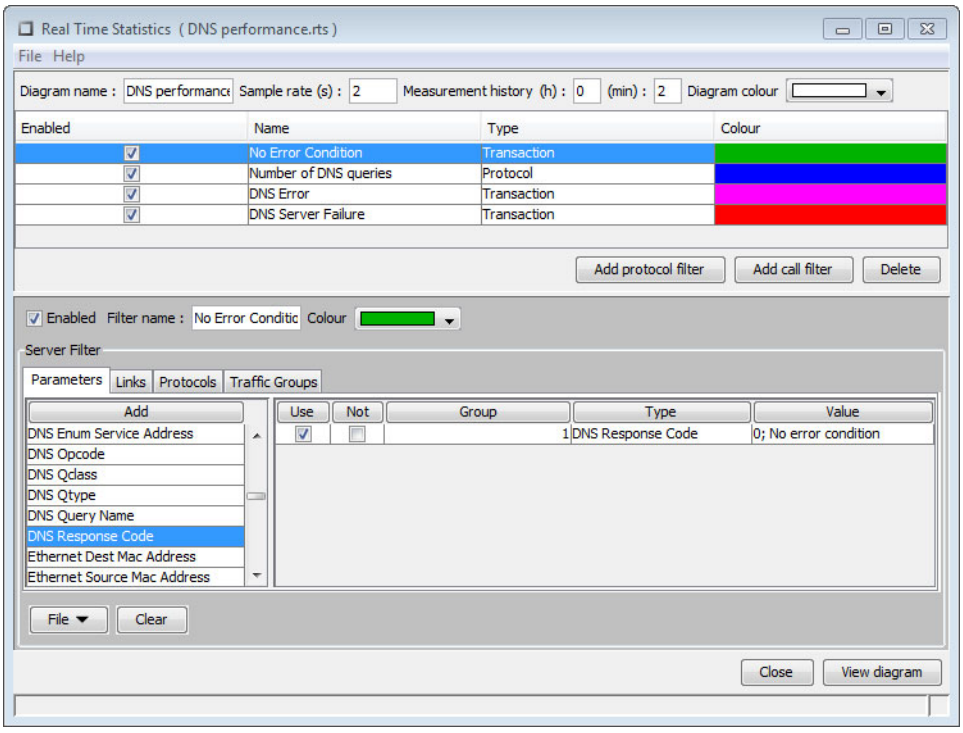


Figure 85: Real Time Statistics main window

11.6.2 Statistical Information

When you are finished with your diagram settings, the statistical information can be viewed either in a table format, or in a diagram format, in real time.

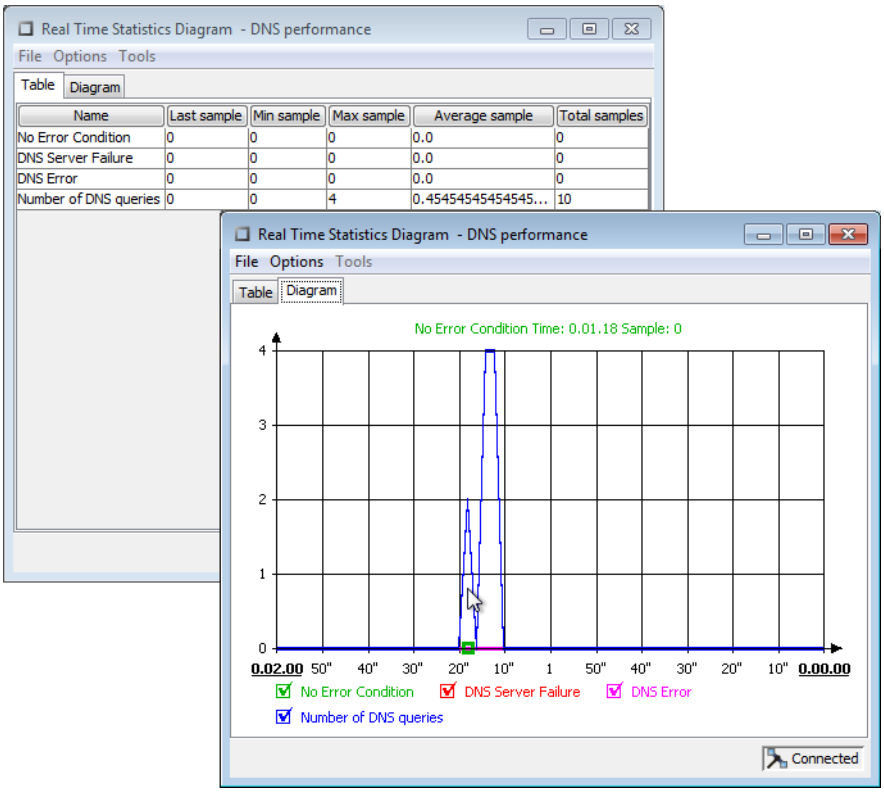


Figure 86: The Real Time table/diagram view

In this view you can also select to save the information as a comma-separated file, which can then be opened in a word processing or spreadsheet application.

11.6.3 Filters

There are four different types of filter:

- **Traffic Groups** - The links in your network are divided into one or more traffic groups, and you must select at least one traffic group before you can start monitoring statistical information over messages/transactions in real time.
- **Parameters** - You can set a filter on any parameter value visible in the main window. This filter type also allows you to exclude messages/transactions with specific values from your statistical information.
- **Links** - You can select to only view statistical information about messages/ transactions that are sent on one or more specific links.
- **Protocols** - If you are running more than one protocol, you can easily select to only view statistical information about messages/transactions in a certain protocol type.

11.6.3.1 Combining filter criteria

Filters can be set to display either messages where a certain parameter equals a certain value, or messages where a certain parameter does NOT equal a certain value. The set filter criteria can then be combined with AND/OR functionality.

11.6.3.2 Saved filters

Any filters you have previously created and saved in either Call Trace or Protocol Analyser can be opened and used in the Real Time Statistics application.

11.7 Network Status

11.7.1 User interface

The Network Status main window displays four different views:

- **Level 1** – which displays alarms detected on the links connected to the LIMs
- **Surveyor** – which displays different maps over the network and any alarms on level 2 or 3
- **Performance** – which displays the number of alarms detected by the Performance Analyser and Mass Call applications
- **Link Status** – which displays the current status on all the different links, and two different dialog boxes:
- **Active Alarms** – which displays all the currently active alarms on all the different levels
- **Alarm Log** – which displays all historical alarms that have been cleared

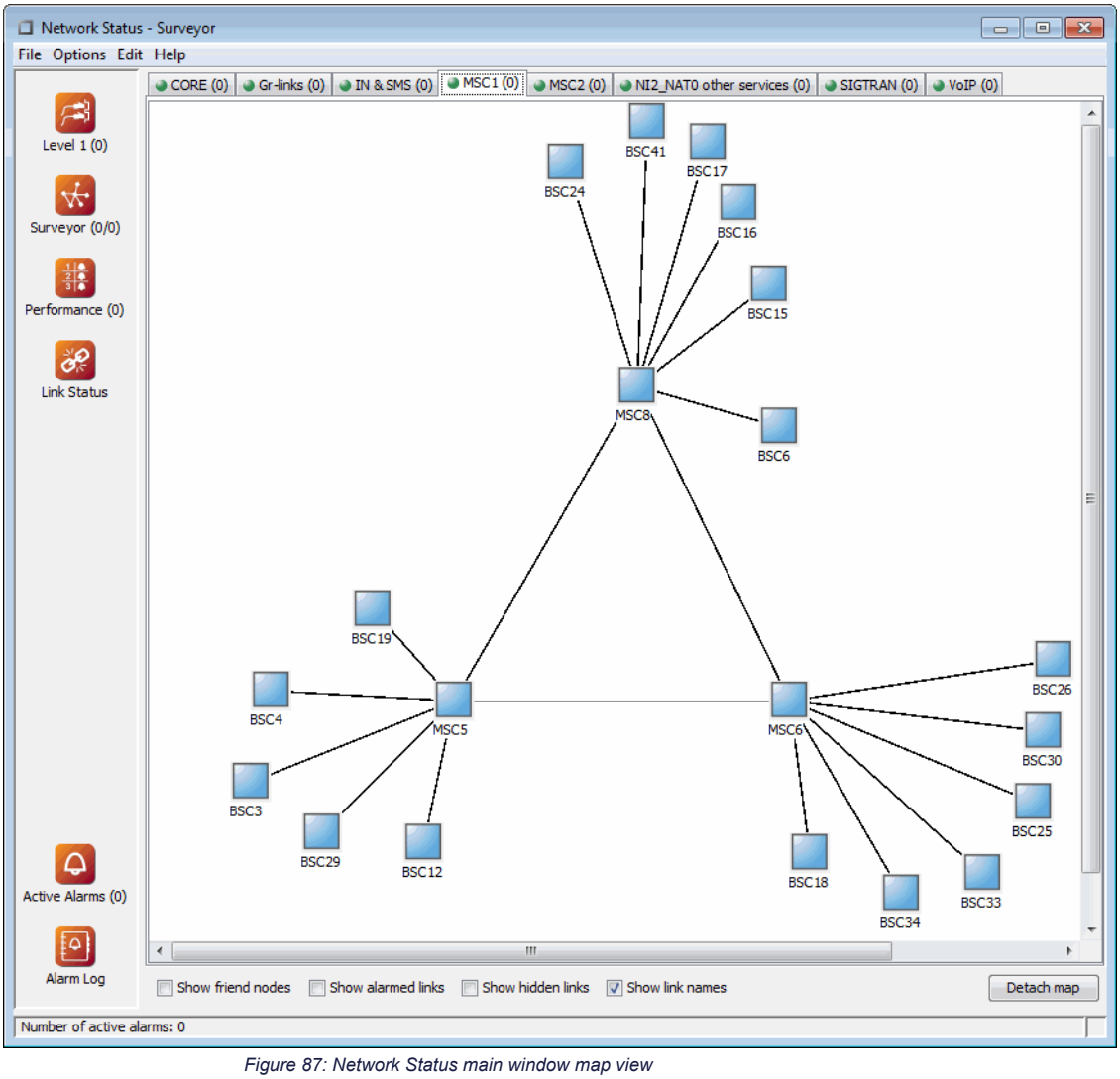


Figure 87: Network Status main window map view

SS7 links and SIGTRAN associations (together with neighbouring PCs and SCTP endpoints) are automatically detected by the OSIX system. Maps are easily created by drag and drop, and as soon as network problems occur, for example Transfer Prohibited, the corresponding link and/or node will start blinking and an alarm will be registered in the Active Alarms dialog box.

The Active Alarms dialog box contains information about all the alarms currently active, and the Alarm Log contains information about historical alarms.

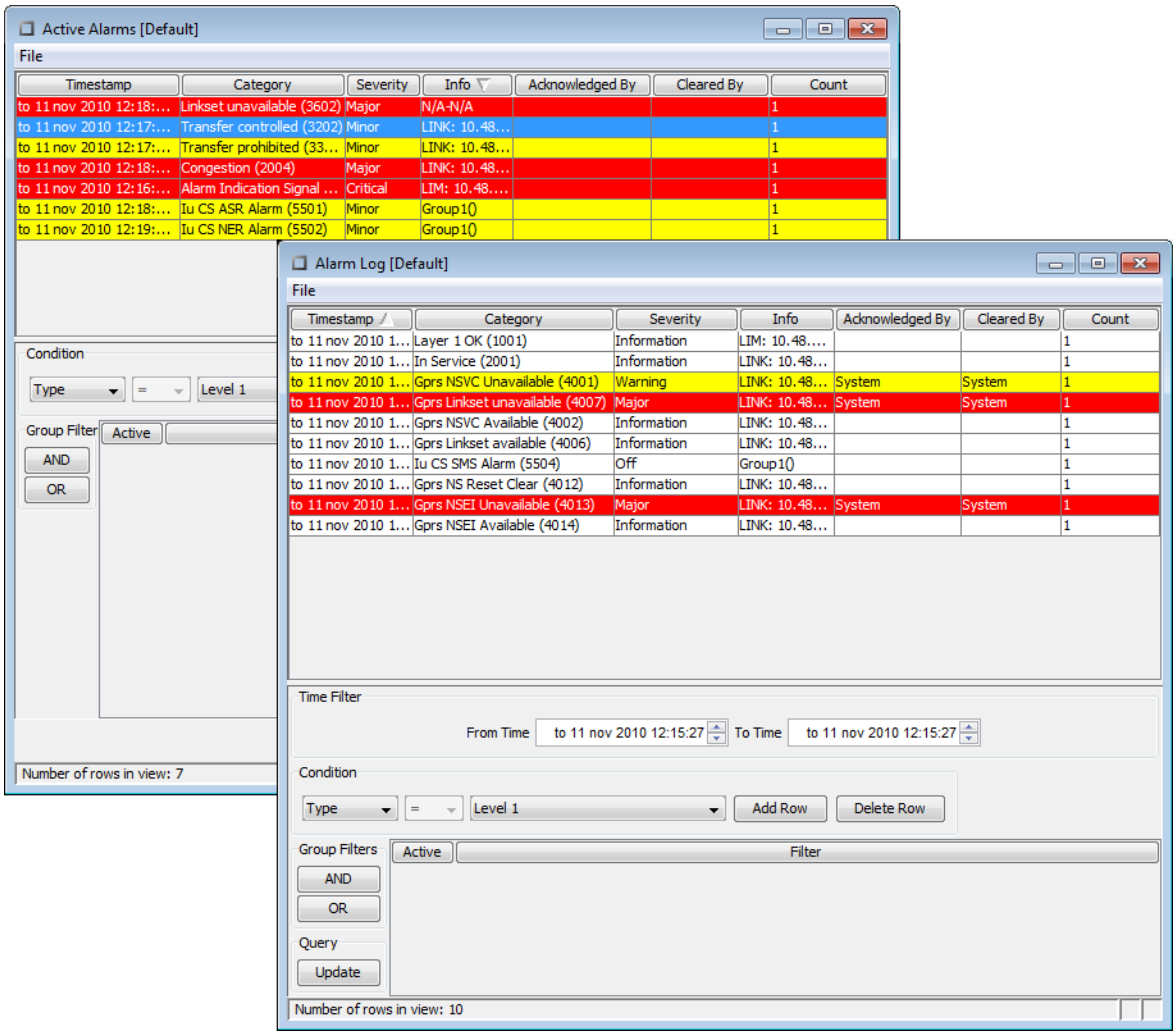


Figure 88: Active Alarms and Alarm Log dialog boxes

Both of these dialog boxes contain comprehensive filter functionality for viewing the specific events that are of interest. All alarms are also available as SNMP traps and/or as email messages.

11.8 Statistics Alarm

With the Statistics Alarm application you can set up alarms to be generated when certain filter criteria for protocol messages or calls/transactions are met.

11.8.0.1 Easy-to-Use GUI

The GUI (Graphical User Interface) allows you to easily set up alarms based on either protocol messages or calls/transactions.

11.8.0.1.1 Alarm Settings

The alarm settings allows you to set up alarms to be generated either at first occurrence, or at a certain number of occurrences over a certain period of time. You can also set up the alarms to be automatically cleared or not.

11.8.1 User interface

The Statistics Alarm main window consists of an overview over the different alarms that have been set up, and four buttons at the bottom of the window.

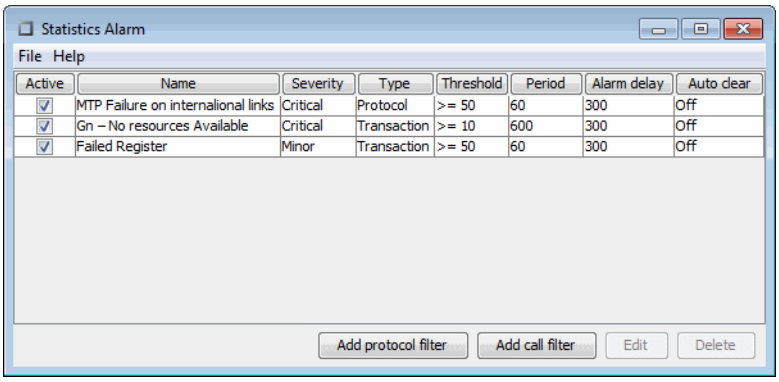


Figure 89: Statistics Alarm main window

Changing the size of the main window will also dynamically adjust and resize the columns to give the best fit in the available space.

11.8.2 Alarm settings

Alarms are set up based either on protocol messages and their contents, or on calls/transactions and their contents.

You can activate/deactivate alarms settings that you have created, as well as edit and delete existing alarm settings.

11.8.2.1 Protocol filter settings

The protocol filter setting will generate an alarm when there are protocol messages passing the filter, or when the number of messages passing the filter exceeds the set threshold during the set time interval.

The alarms will be sent to the Network Status application and to any third-party applications of your choice.

When making protocol filter settings, you can use the following filter types: Traffic group filters, Parameter filters, and Link filters.

11.8.2.2 Transaction filter settings

The transaction filter setting will generate an alarm when there are calls/ transactions passing the filter, or when the number of calls/transactions passing the filter exceeds the set threshold during the set time interval.

The alarms will be sent to the Network Status application and to any third-party applications of your choice.

When making transaction filter settings, you can use the following filter types: Traffic group filters, Parameter filters, Link filters, and Duration filters.

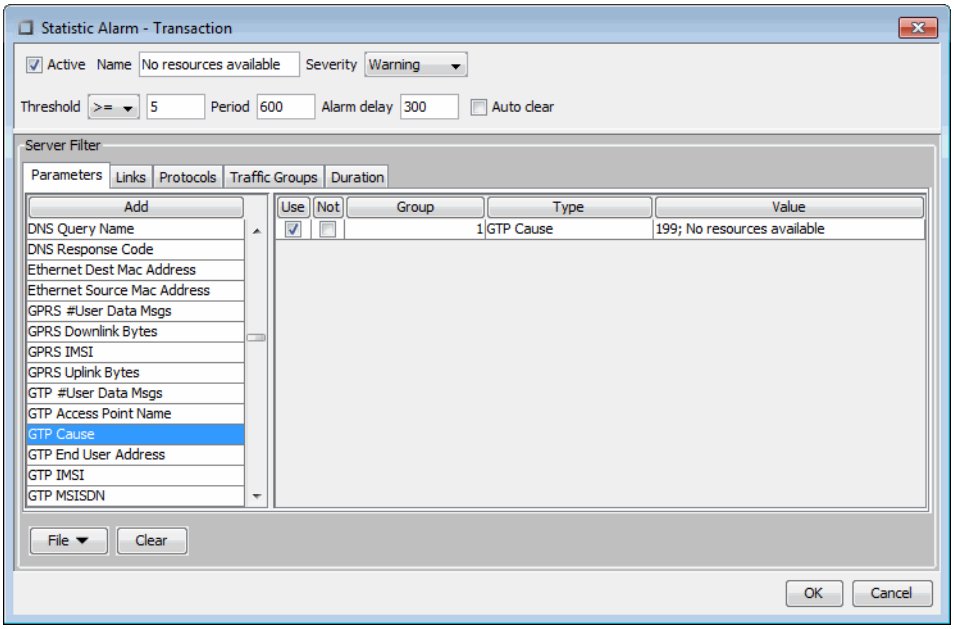


Figure 90: Parameters tab sample for transaction filter settings

11.8.3 Filter settings management

Filter settings are fully editable and can also be saved for later use.

If you want to keep a filter setting but not use it at the moment, you can select to deactivate the filter setting, and then activate it again when you want to use it.

To delete a filter setting, select it in the main window and click the Delete button.

12 OSIX Monitoring for IMS and VoIP networks

OSIX extracts information from signalling networks and includes applications for monitoring and troubleshooting, xDR generation/SNMP trap generation, email messaging, and OSS (Operation Support System) applications. The following sections show a few examples for IMS and VoIP networks.

12.1 IMS/VoIP protocols and interfaces

In a pure IMS environment, there are four main protocols: SIP, RTP, Diameter and DNS. SIP is used for the establishment of multimedia sessions, and Diameter is used for database communication. DNS is used to find other IMS nodes, but also for conversion between telephone numbers and IMS URIs. The user plane is carried by the RTP protocol, handled in OSIX by creating aggregations of the streams, partially during the session (partial) and also when the session ends (final).

When IMS/VoIP is interworking with legacy networks, other protocols like H.248 (Megaco) and BICC are used.

The OSIX Monitoring system supports all the major protocols; SIP, Megaco/H.248, RTP and DNS as they are used on a majority of the IMS/NGN interfaces.

All major protocols and links/interfaces used within VoIP networks are supported by the OSIX Monitoring system.

For information about supported protocols, see the *OSIX Supported Protocols* document.

All supported protocols have a large set of pre-defined parameters available for filtering. For information about protocol parameters, see chapter *15 Protocol parameters*.

12.2 IMS/VoIP network features

- Support for all major interfaces and protocols including extensions, for example DNS NAPTR.
- Multi-protocol client correlation with support for matching of for example ICID, SDP values, and A/B numbers.
- RTP quality analysis, including MOS score and real-time correlation to subscriber (SIP dialog).
- Real-time KPI measurements for SIP.
- Flexible storage of signalling with individual storage length per protocol and SIP method. That is, INVITE can, for example, be stored for a longer time than REGISTER.

12.3 Protocol Analyser

12.3.1 User interface

In the Protocol Analyser main window you can monitor the protocol messages, either in real time or historically. You can also set different filters or search for specific messages. You can have a maximum of four different Protocol Analyser windows with different settings open at the same time.

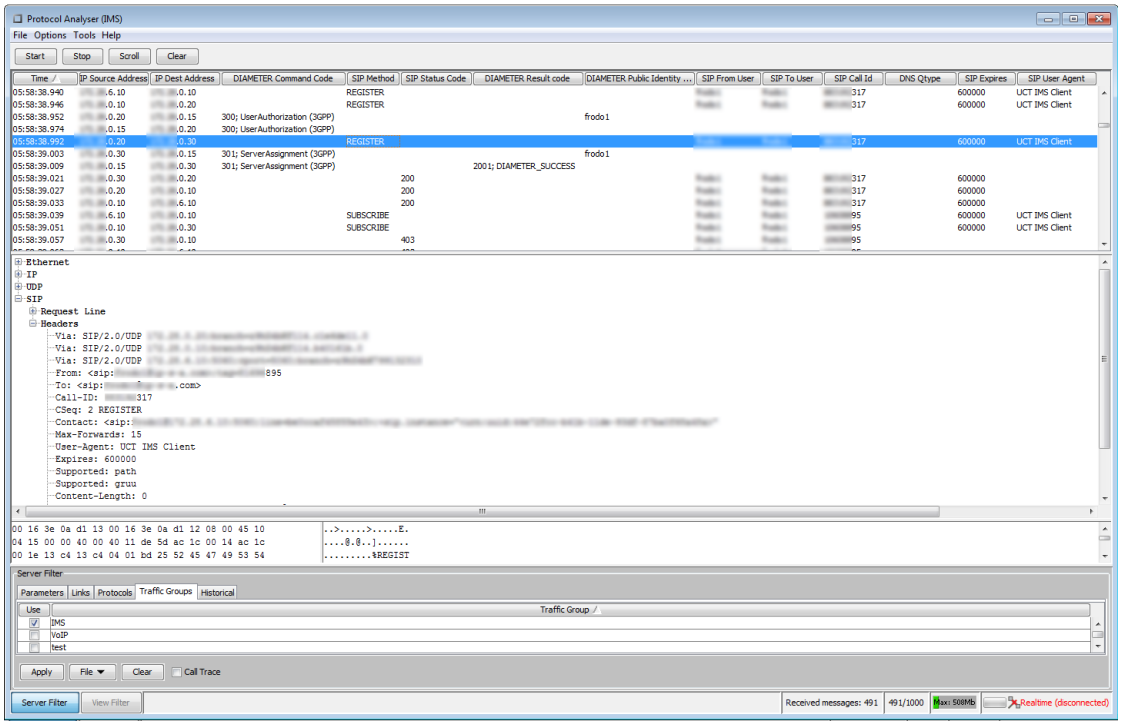


Figure 91: Protocol Analyser main window

12.3.1.1 Message details

The message window is divided into several parts—one displaying the different protocol messages, one displaying a preview of the message, one showing the hexadecimal code, one showing ASCII code, and finally the filter section. You can also open a separate Message Viewer with the contents of the entire message.

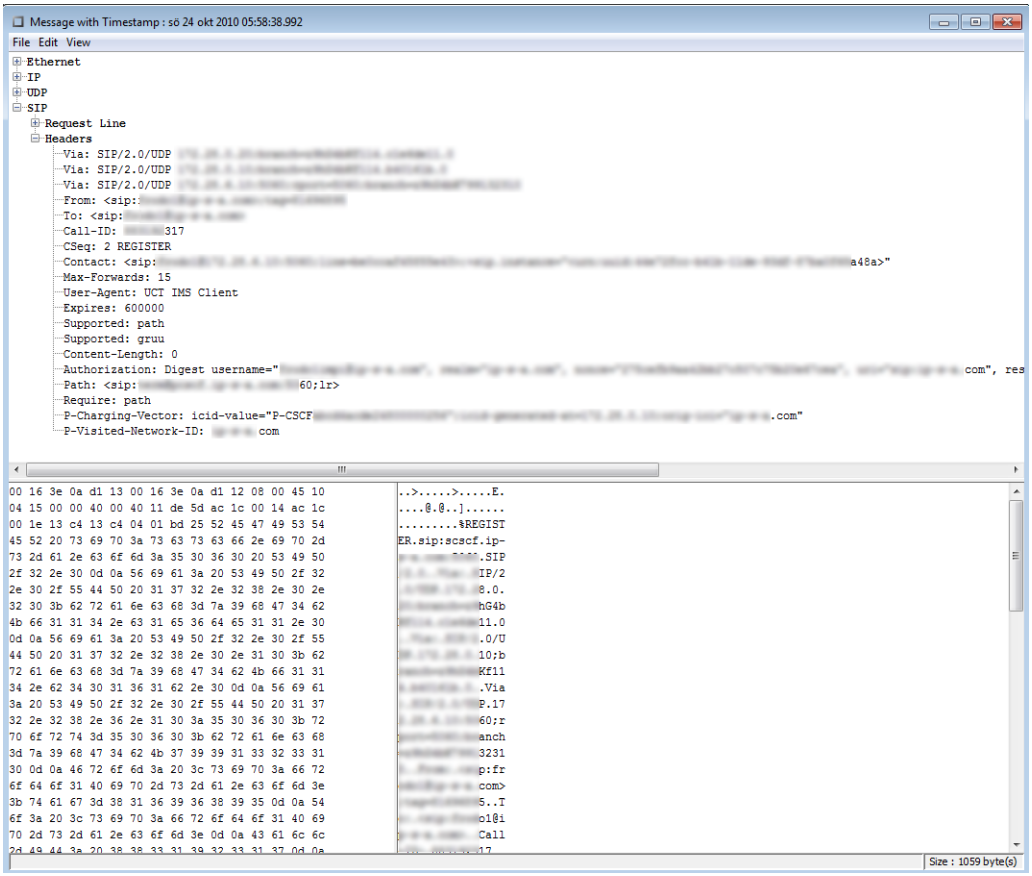


Figure 92: Protocol Analyser message window

12.4 Call Trace

12.4.1 User interface

In the Call Trace main window you can monitor the calls, either in real time or historically. You can also set different filters, or search for specific calls. You can have a maximum of four different Call Trace windows with different settings open at the same time.

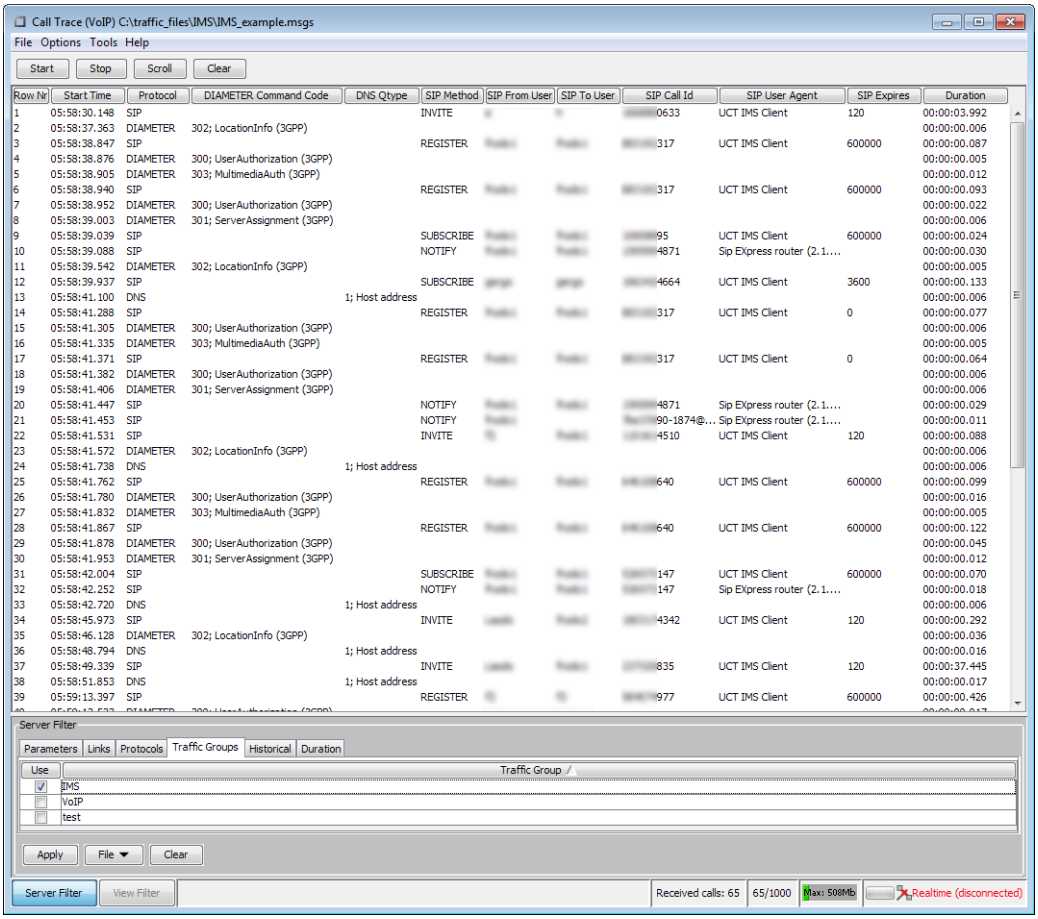


Figure 93: Call Trace main window

12.4.1.1 Call details

If you want to take a closer look at a call, you can double-click a call to open the Call window. The window is divided into several parts or panes—one displaying the different protocol messages sent referring to the selected call, one displaying a preview of the message, one showing the hexadecimal code, one showing ASCII code, and finally one pane displaying different parameters for the call (this pane is not present in the figure below). You can also open a separate Message Viewer with the contents of the entire message.

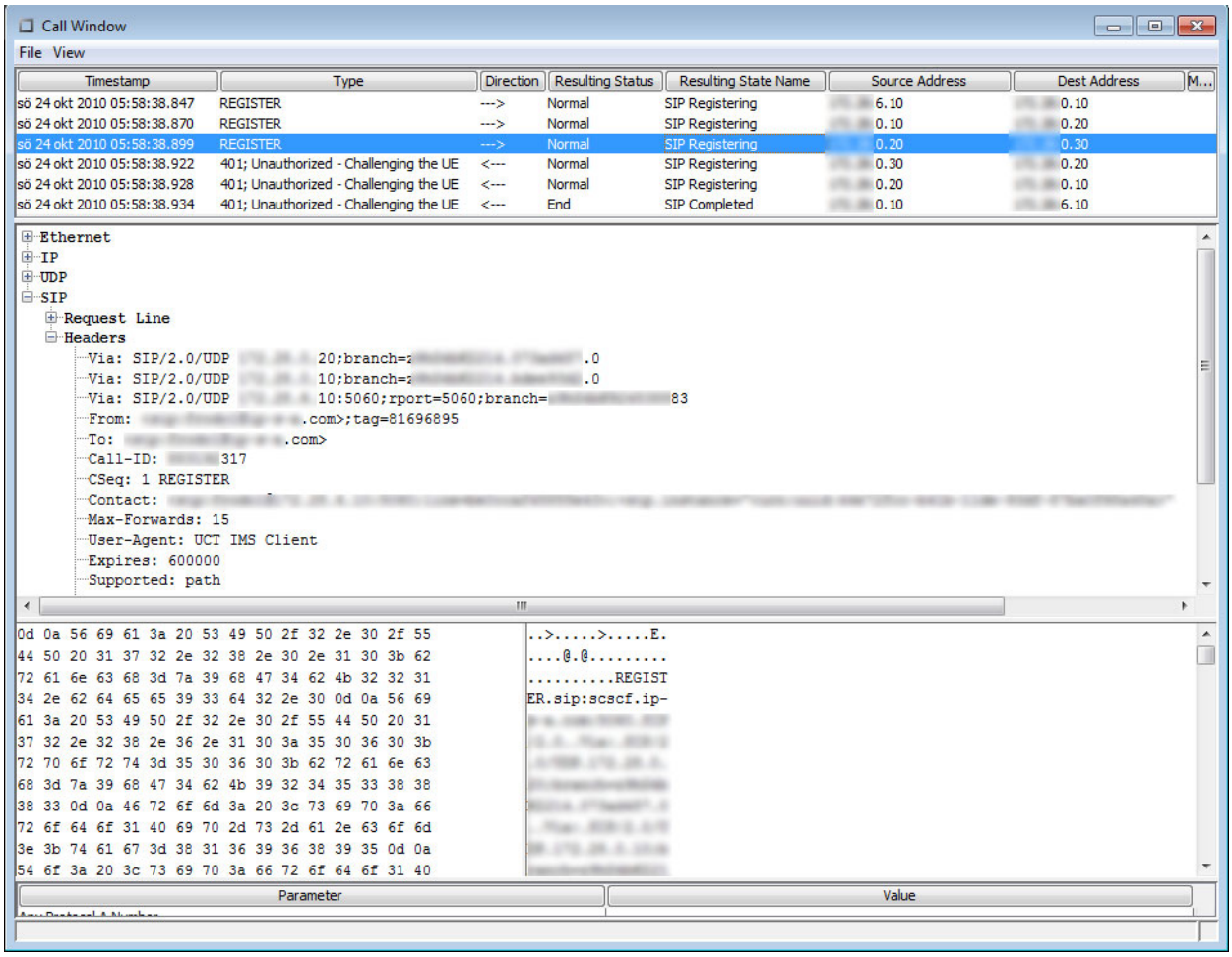


Figure 94: Call Trace Call window

12.4.1.2 Call flow

When viewing the call details, you can also choose to view the call flow in a graphical representation, where the nodes are visible and the different messages are represented with arrows.

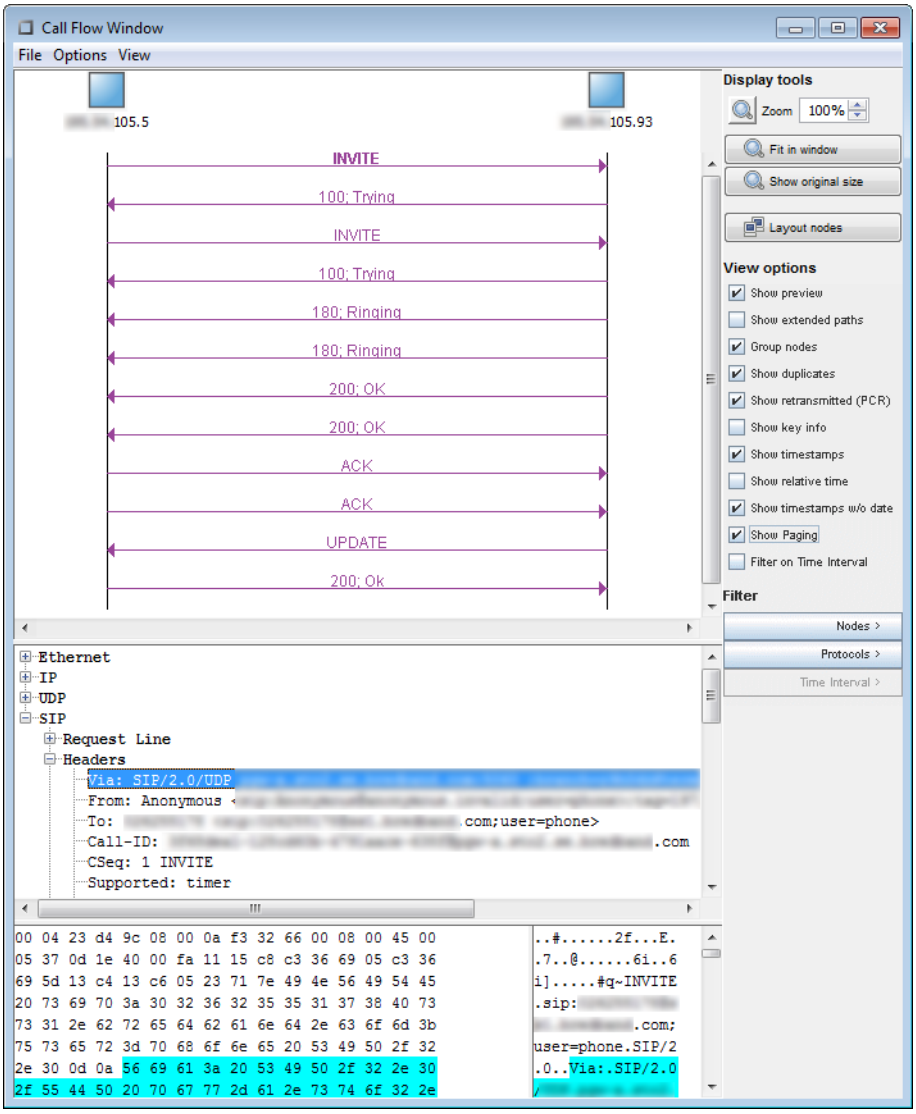


Figure 95: Call Trace Call Flow window

12.4.2 Client correlation

Client correlation is done between all messages that relate to the same call/ transaction, regardless of to where in the network the messages are sent. All messages that relate to the process are presented in the Call window.

For IMS and VoIP networks, the recommended client correlation engine is “IMS & Mobile”.

The following protocols are supported for IMS & Mobile: ISUP, SIP, MEGACO, INAP/CAP, BICC, MGCP, H.225, ISDN, DNS, Diameter, MAP, RANAP, S1AP, SGsAP, LDAP, HTTP, HTTP/2, PFCP, NGAP, SMPP and BSSAP.

12.4.2.1 Client correlation example for IMS & Mobile

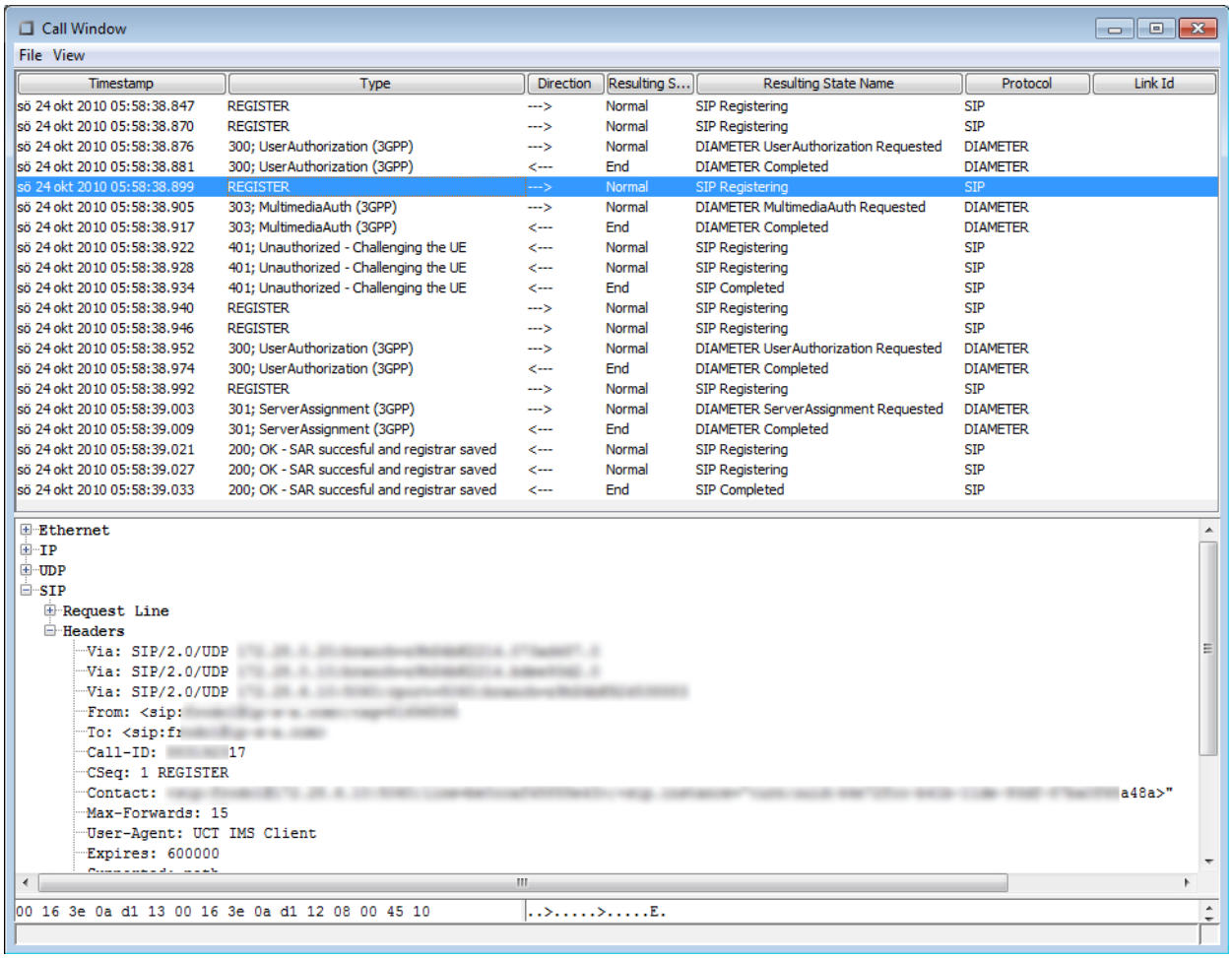


Figure 96: Call Trace Call window for IMS & Mobile client correlation

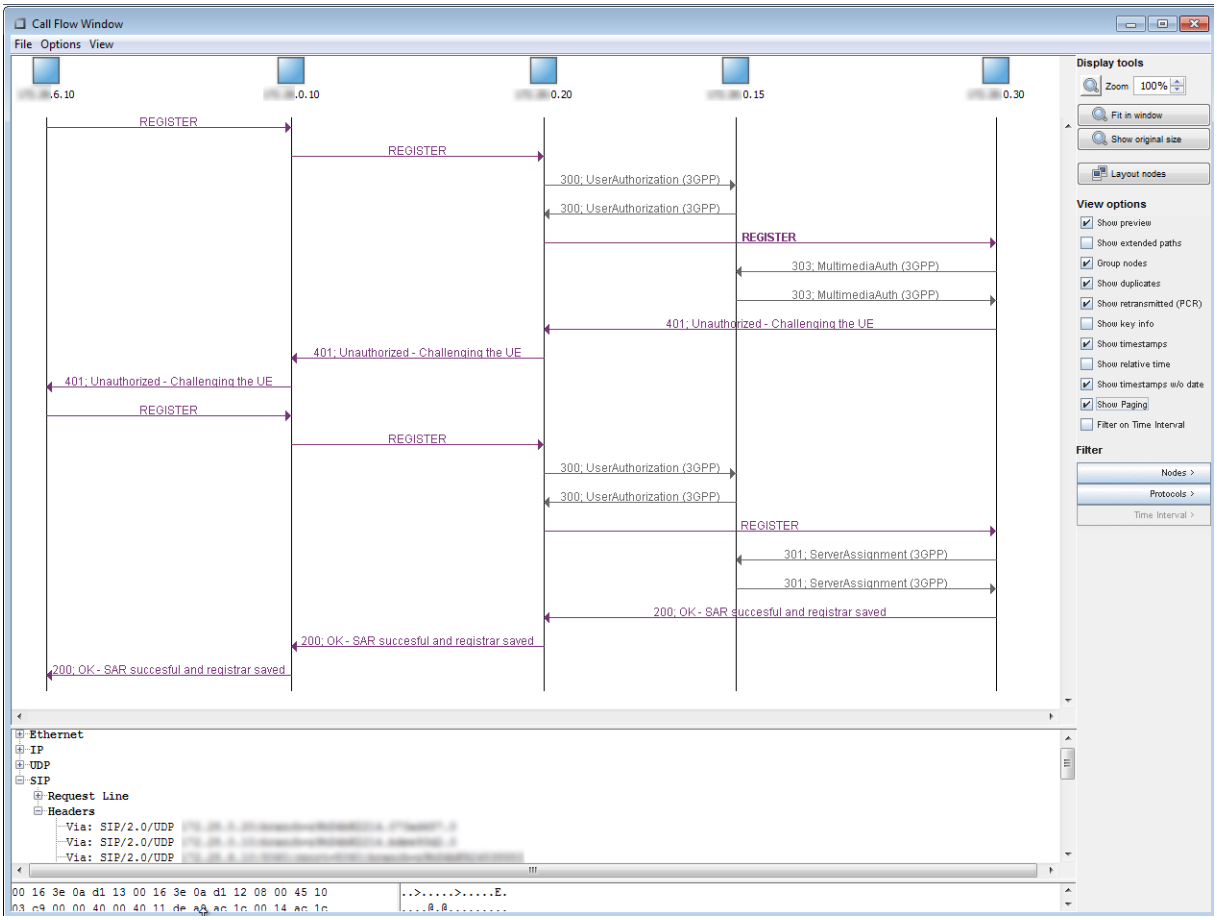


Figure 97: Call Trace Call Flow window for IMS & Mobile

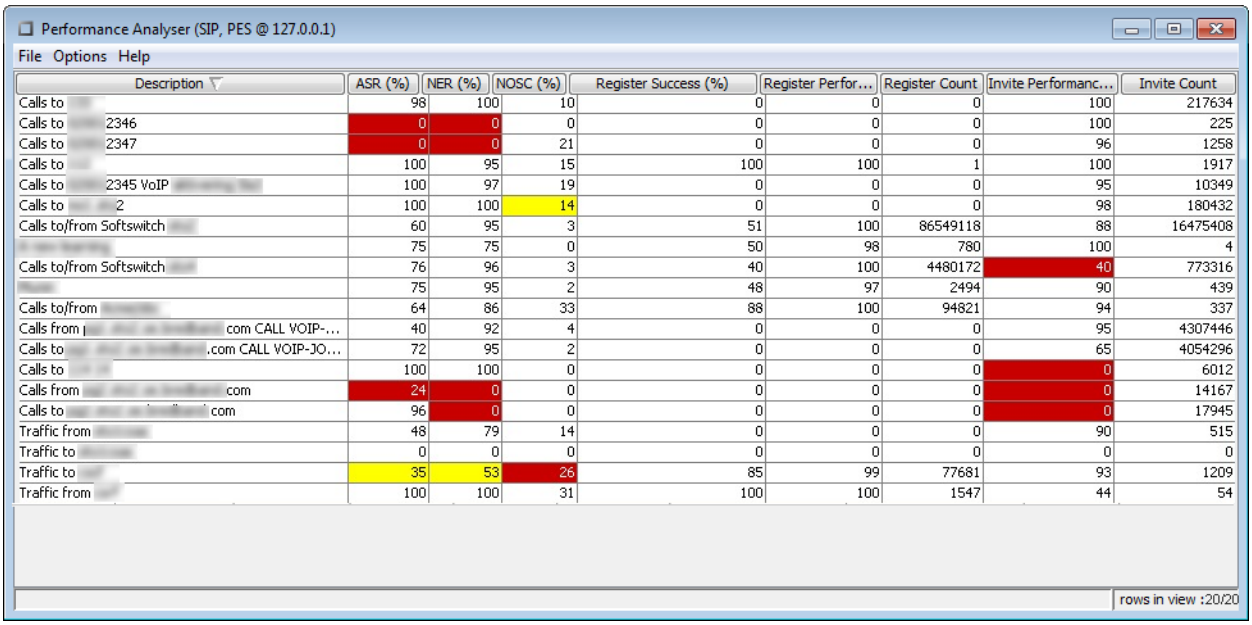
12.5 Performance Analyser

12.5.1 User interface

The Performance Analyser main window displays the calling statistics for the call groups in real time.

Example:

In addition to monitoring specific partners, other traffic groups can be defined and monitored. The figure shows traffic to/from a particular soft switch or emergency calls.



Description	ASR (%)	NER (%)	NOSC (%)	Register Success (%)	Register Perfor...	Register Count	Invite Performanc...	Invite Count
Calls to	98	100	10	0	0	0	100	217634
Calls to 2346	0	0	0	0	0	0	100	225
Calls to 2347	0	0	21	0	0	0	96	1258
Calls to	100	95	15	100	100	1	100	1917
Calls to 2345 VoIP	100	97	19	0	0	0	95	10349
Calls to 2	100	100	14	0	0	0	98	180432
Calls to/from Softswitch	60	95	3	51	100	86549118	88	16475408
	75	75	0	50	98	780	100	4
Calls to/from Softswitch	76	96	3	40	100	4480172	40	773316
	75	95	2	48	97	2494	90	439
Calls to/from	64	86	33	88	100	94821	94	337
Calls from com CALL VOIP-...	40	92	4	0	0	0	95	4307446
Calls to .com CALL VOIP-JO...	72	95	2	0	0	0	65	4054296
Calls to	100	100	0	0	0	0	0	6012
Calls from com	24	0	0	0	0	0	0	14167
Calls to com	96	0	0	0	0	0	0	17945
Traffic from	48	79	14	0	0	0	90	515
Traffic to	0	0	0	0	0	0	0	0
Traffic to	35	53	26	85	99	77681	93	1209
Traffic from	100	100	31	100	100	1547	44	54

Figure 98: Performance Analyser main window for SIP

12.5.2 Columns

The following columns are available in the main window:

Group ID	Displays the individual group's unique number.
Information	If the KPIs for the group have been measured by OSIX and set automatically, this column displays the results from the last evaluation.
Description	If the group has been automatically generated by OSIX, this column will display what parameter values the group consists of, otherwise the system administrator can set any appropriate name for this column.
ASR (%)	Answer Seizure Ratio displays the number of answered calls out of the total number of call attempts, in per cent.
NER (%)	Network Efficiency Ratio displays the number of calls terminated with normal release causes (defined by the system administrator) out of the total number of call attempts, in per cent.

Table 9: Performance Analyser main window columns

NOSC (%)	Number of Short Calls displays the number calls with a conversation time shorter than a certain time interval (defined by the system administrator) out of the total number of call attempts, in per cent.
Invite Performance (%)	Displays the number of successful Invite transactions, that is, Invites where no message has been retransmitted, out of the total number of Invites. This KPI will help you detect problems on IP level.
Invite Count	Displays the total amount of Invites counted in the group since the counters were last reset.
Register Success (%)	Displays the number of successful Registrations out of the total number of registration attempts.
Register Performance (%)	Displays the number of successful Register transactions, that is, Registrations where no message has been retransmitted, out of the total number of Registrations. This KPI will help you detect problems on IP level.
Register Count	Displays the total amount of Registrations counted in the group since the counters were last reset.
Priority	Displays a priority value calculated by OSIX based on the largest deviation between current value and set alarm value and the set buffer size.
Total Count	Displays the total amount of SIP transactions counted in the group since the counters were last reset.

Table 9: Performance Analyser main window columns (Continued)

12.5.2.1 Call group information

If you want to view detailed information about the call group and/or start Call Trace or Protocol Analyser with an automatic filter for the transaction group, double-click the group to open the Call Group Information dialog box.

Example:

The figure shows a call group that gives statistics for a group of three destination IP addresses.

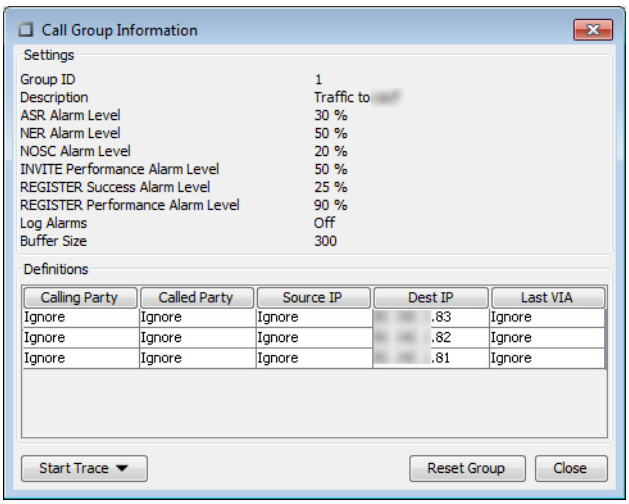


Figure 99: Call Group Information dialog box for SIP

The following parameters are available:

Calling Party	Displays the calling party number
Called Party	Displays the called party number
Source IP	Displays the source IP address
Dest IP	Displays the destination IP address

Table 10: Call group parameters

12.5.3 Server configuration

When configuring the Performance Analyser application you have a vast number of options on how to set up the call groups, the alarm levels you want each group to have, which release causes should be counted, the maximum number of seconds for a short call, etc.

12.5.3.1 Main settings

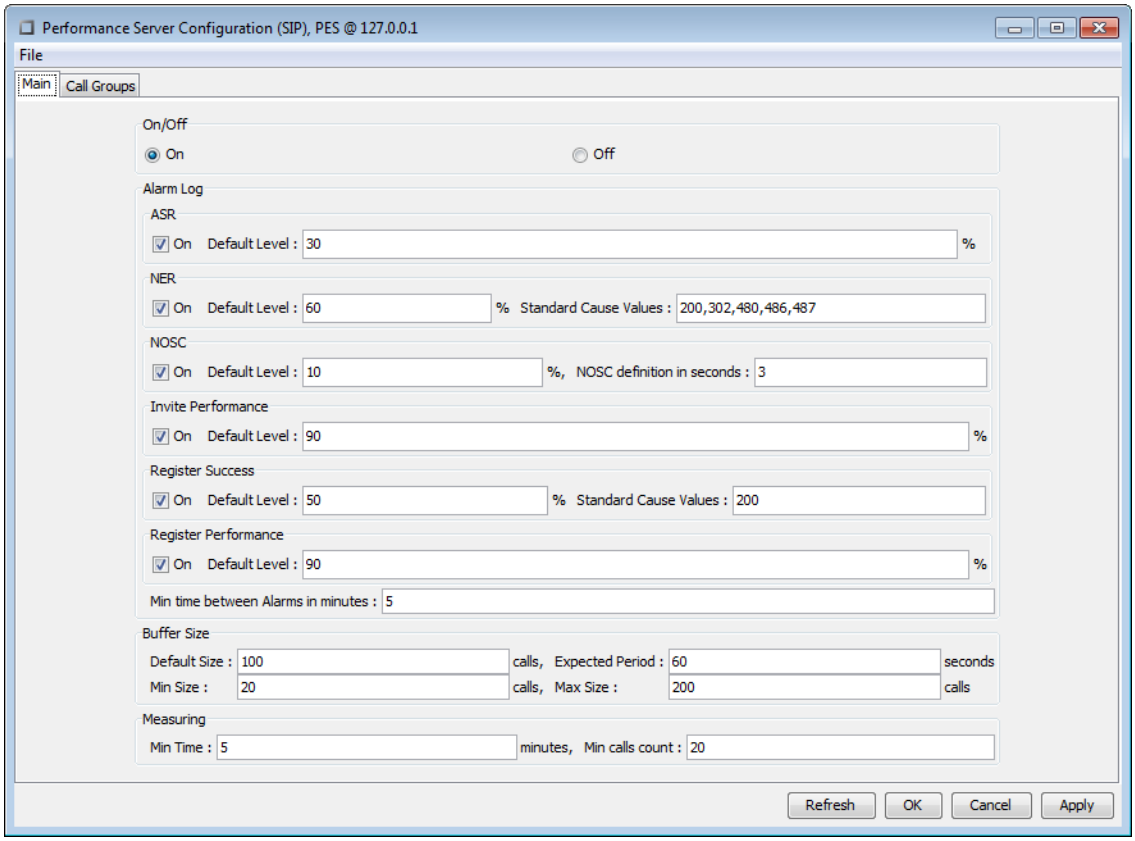


Figure 100: Server configuration Main tab

12.5.3.2 Call group settings

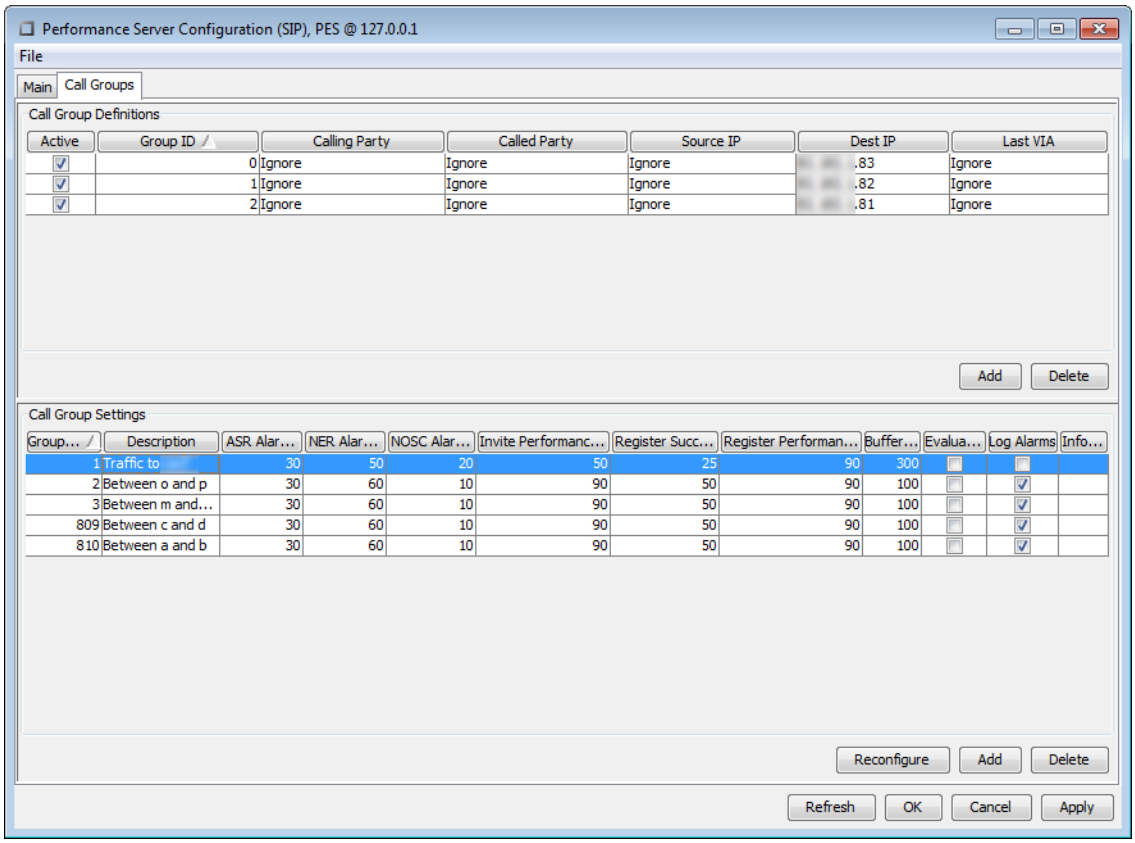


Figure 101: Server configuration Call Groups tab

12.5.4 Call groups

The call groups can consist of any combination of Calling Party Number, Called Party Number, Source IP, Destination IP, Last VIA, and VLAN ID. For A numbers and B numbers, wild cards can be used, and a plus sign can be used for a catch all group. You can also enter regular expressions with different types of wild cards for all the parameters.

12.5.5 Automatic group generation

If you are unsure about how to configure the call groups, OSIX can automatically generate groups based on the Source IP and Destination IP parameters.

12.5.6 Intelligent alarm settings

Setting appropriate alarm levels can be difficult the first time the application is used. OSIX can measure the ASR, NER, NOSC, Invite Performance, Register Success, and Register Performance values for the call groups, and calculate appropriate alarm settings for you, called “intelligent alarm settings”.

12.5.7 Export

If you want to save the settings or edit them in another environment than in the Performance Analyser server configuration, you can export them, open them in Excel, and import them back into Performance Analyser later.

12.6 Real Time Statistics

12.6.1 User interface

The Real Time Statistics main window displays the different settings for your diagrams, with the top half displaying the general settings for sampling rate, measure history, etc., and the bottom half the filter settings that determine which messages/transactions should be counted in the diagram.

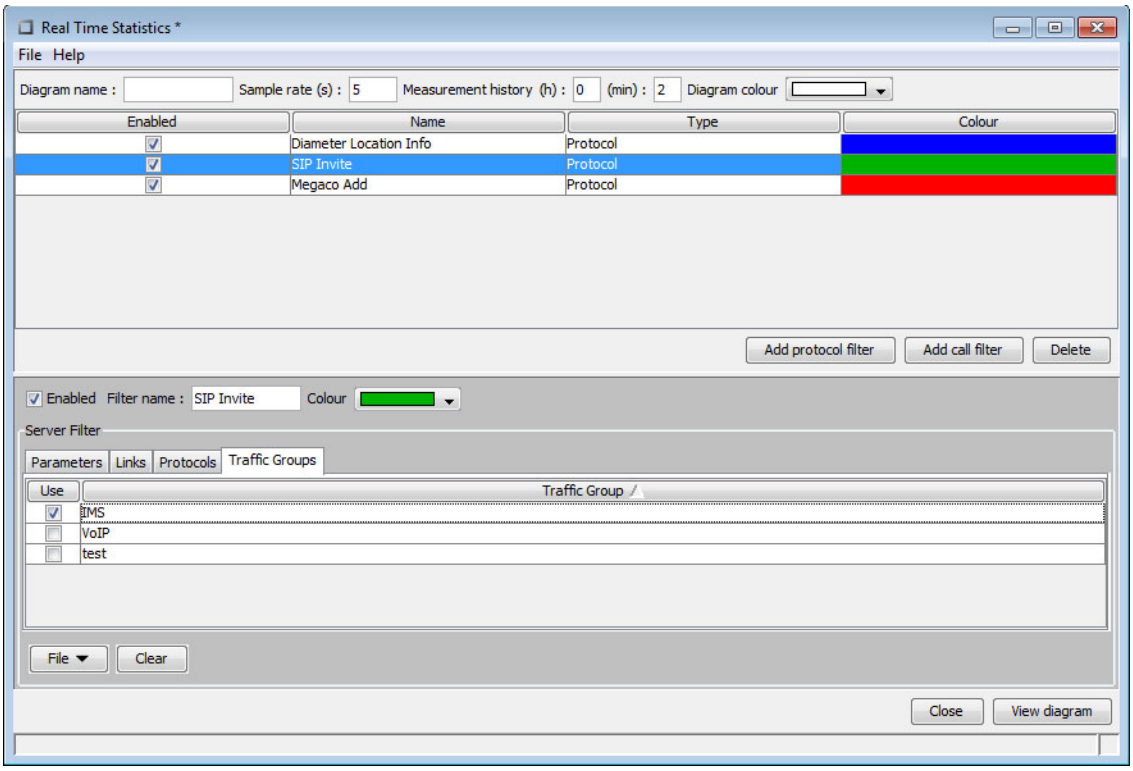


Figure 102: Real Time Statistics main window

12.6.2 Statistical information

When you are finished with the diagram settings, the statistical information can be viewed either in a table format or in a diagram format, in real time.

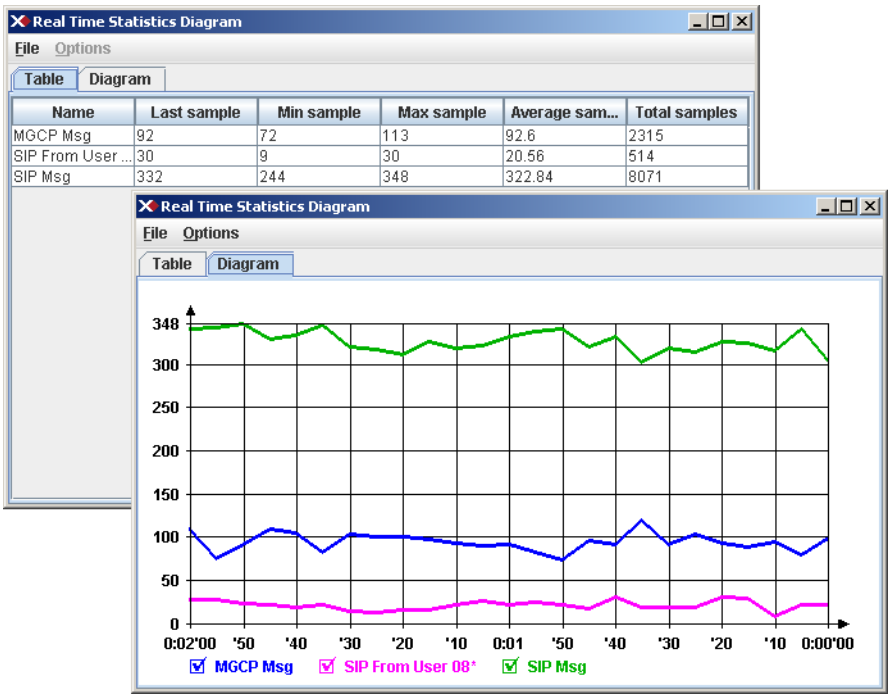


Figure 103: Real time table/diagram view

In this view you can also select to save the information as a comma-separated file, which can then be opened in a word processing or spreadsheet application.

12.6.3 Filters

There are four different types of filter:

- **Traffic groups** - The links in your network are divided into one or more traffic groups, and you must select at least one traffic group before you can start monitoring statistical information over messages/transactions in real time.
- **Parameters** - You can set a filter on any parameter value visible in the main window. This filter type also allows you to exclude messages /transactions with specific values from your statistical information.
- **Links** - You can select to only view statistical information about messages/ transactions that are sent on one or more specific links.
- **Protocols** - If you are running more than one protocol, you can easily select to only view statistical information about messages/transactions in a certain protocol type.

12.6.3.1 Combining filter criteria

Filters can be set to display either messages where a certain parameter equals a certain value, or messages where a certain parameter does NOT equal a certain value. The set filter criteria can then be combined with AND/OR functionality.

12.6.3.2 Saved filters

Any filters you have previously created and saved in either Call Trace or Protocol Analyser can be opened and used in the Real Time Statistics application.

12.7 Network Status

12.7.1 User interface

The Network Status main window displays four different views:

- **Layer 1**, which displays alarms detected on the links connected to the LIMs.
- **Map**, which displays different maps over the network and any alarms on level 2 or 3.
- **Performance**, which displays the number of alarms detected by the Performance Analyser application.
- **Link Status**, which displays the current status on all the different links.
- and two different dialog boxes:
- **Active Alarms**, which displays all the currently active alarms on all the different levels.
- **Alarm Log**, which displays all alarms that have been cleared.

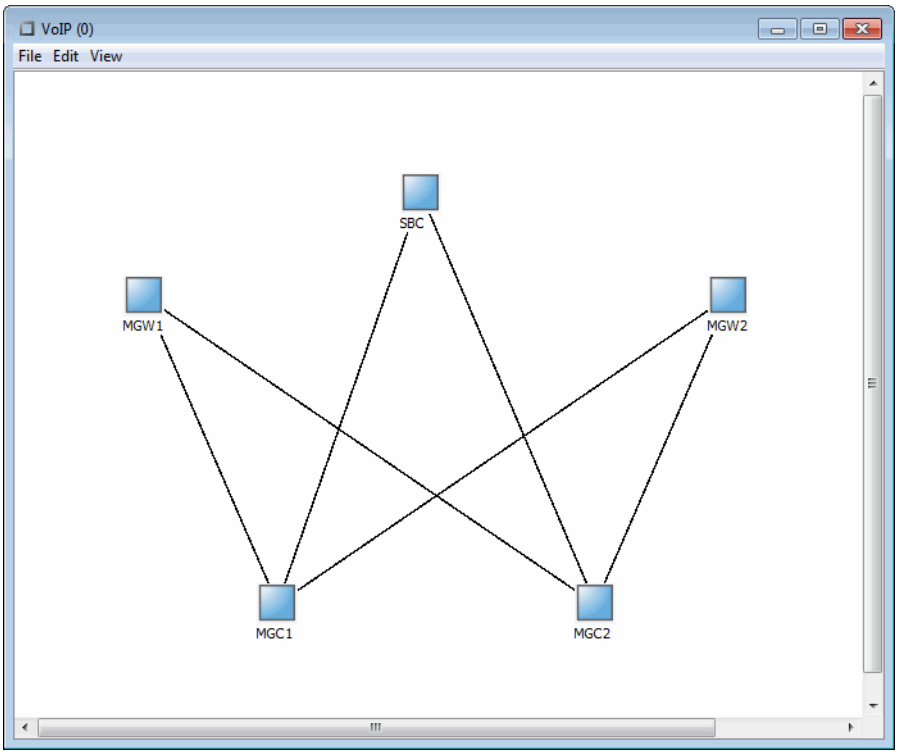


Figure 104: Network Status main wWindow, Map view (detached)

The **Active Alarms** dialog box contains information about all the alarms currently active, and the Alarm Log contains information about historical alarms.

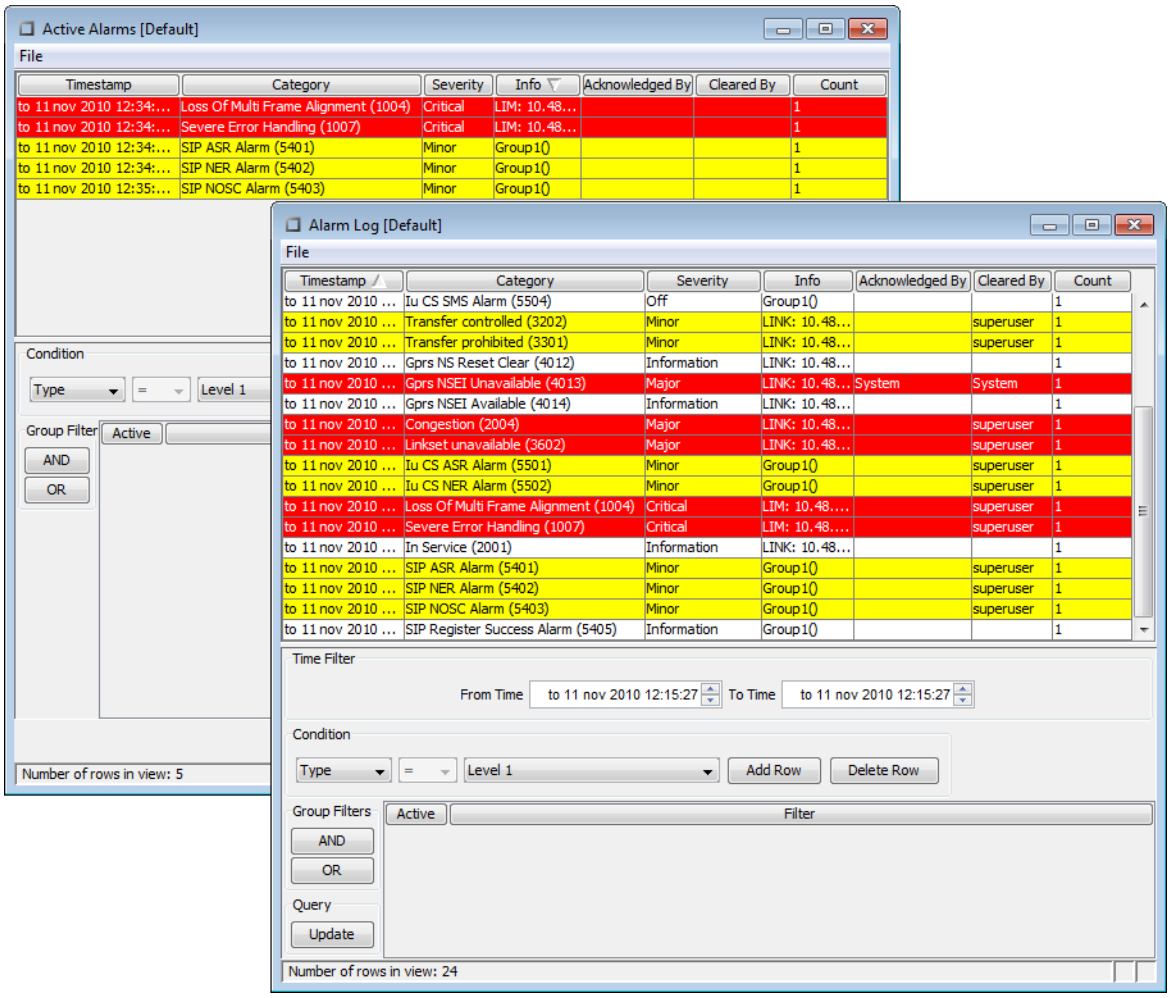


Figure 105: Active Alarms and Alarm Log dialog boxes

Both dialog boxes contain comprehensive filter functionality for viewing the specific events that are of interest.

12.8 Statistics Alarm

With the Statistics Alarm application you can set up alarms to be generated when certain filter criteria for protocol messages or calls/transactions are met.

12.8.0.1 Easy-to-use GUI

The GUI (Graphical User Interface) allows you to easily set up alarms based on either protocol messages or calls/transactions.

12.8.0.1.1 Alarm settings

The alarm settings allow you to set up alarms to be generated either at first occurrence, or at a certain number of occurrences over a certain period of time. You can also set up the alarms to be automatically cleared or not.

12.8.1 User interface

The Statistics Alarm main window consists of an overview over the different alarms that have been set up, and four buttons at the bottom of the window.

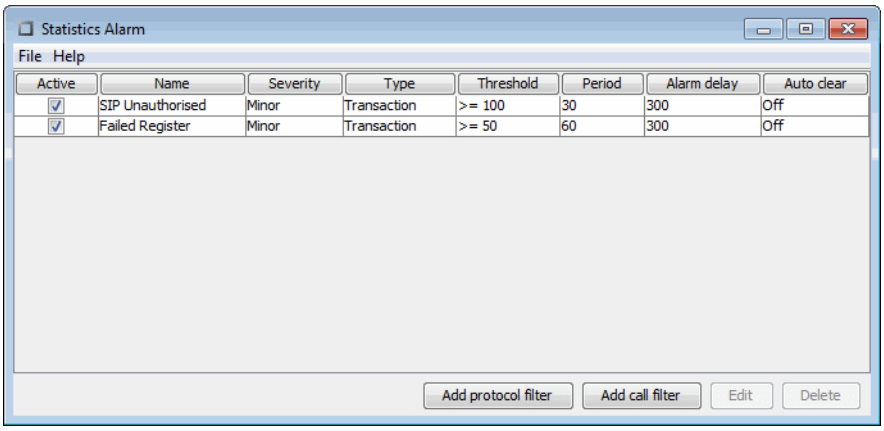


Figure 106: Statistics Alarm Main window

Changing the size of the main window will also dynamically adjust and resize the columns to give the best fit in the available space.

12.8.2 Alarm settings

Alarms are set up based either on protocol messages and their contents, or on calls/transactions and their contents. You can activate/deactivate alarms settings that you have created, as well as edit and delete existing alarm settings.

12.8.2.1 Protocol filter settings

The protocol filter setting will generate an alarm when there are protocol messages passing the filter, or when the number of messages passing the filter exceeds the set threshold during the set time interval.

The alarms will be sent to the Network Status application and to any third-party applications of your choice. When making protocol filter settings, you can use the following filter types: Traffic group filters, Parameter filters, and Link filters.

12.8.2.2 Transaction filter settings

The transaction filter setting will generate an alarm when there are calls/ transactions passing the filter, or when the number of calls/transactions passing the filter exceeds the set threshold during the set time interval.

The alarms will be sent to the Network Status application and to any third-party applications of your choice.

When making transaction filter settings, you can use the following filter types: Traffic group filters, Parameter filters, Link filters, and Duration filters.

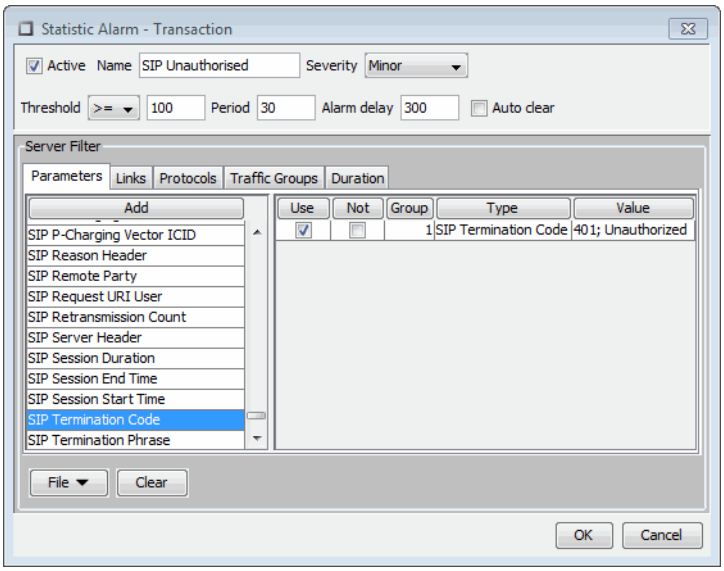


Figure 107: Parameters tab sample for transaction filter settings

12.8.3 Filter settings management

Filter settings are fully editable and can also be saved for later use.

If you want to keep a filter setting but not use it at the moment, you can select to deactivate it, and then activate it again when you want to use it.

To delete a filter setting, select it in the main window and click the Delete button.

13 OSIX Monitoring for 5G SA

The 5G Stand Alone (5G SA) networks, as specified by 3GPP, build on the successful 4G networks but comes with some new architecture enhancements. The access protocols (5G-NAS/NGAP) are similar to the legacy protocols (4G-NAS/S1AP) and the PFCP protocol is used in both 4G and in 5G SA.

However, the communication between the core network nodes uses a Service Based Architecture (SBA) based on RESTful APIs using the HTTP/2 protocol. The core components are known as Network Functions (NF) and are in general realised in a Kubernetes environment.

When monitoring a 5G SA network, there are some additional challenges beyond just adding support for new protocols and parameters. These challenges are related to how to extract the signalling from the 5G SA core network. Security requirements (TLS 1.3) and implementation specifics (K8) leads to that the traditional physical tapping of signalling Elisa Polystar traditionally uses will not be possible when monitoring a 5G SA core network.

Fortunately, the 5G SA core vendors have realised that this is an issue for the CSPs and they offer a possibility to access an uncyphered feed from each NF. The less fortunate part is, that there is no standard for how this tapping is done, and each vendor is doing this in different ways.

13.1 Summary of features for 5G SA in OSIX Monitoring

- OSIX Call Trace and Protocol Analyser support for all relevant protocols and reference points
- IMSI enrichment of 5G-NAS/NGAP, HTTP/2, GTPv2-C, and PFCP
- Client correlation E2E support for the added protocols
- Real-time deciphering of 5G-NAS
- Support for vTAP integration with many different vendors, for example, Ericsson, Nokia, Mavenir, Affirmed, etc.
- Identification of 5GC nodes based on enrichment and meta data

13.2 High-level system architecture

The External TAP Mediator (ETM) is introduced to handle the interaction with different vendors vTAPs. It terminates different feeds (for example, gRPC, HEP3, AVRO) and reads the meta data to normalise the signalling for consumption of the OSIX Monitoring components.

In some cases, the MediaProbe (MP) can still be used also for 5G SA core signalling. However, since the MP is a passive component and many vendors vTAP solutions requires an active counterpart, the ETM must be used in many cases. The MP is currently used for the Ericsson vTAP and for scenarios with a physical feed.

The following figure shows different ways for OSIX Monitoring to consume 5G SA signalling:

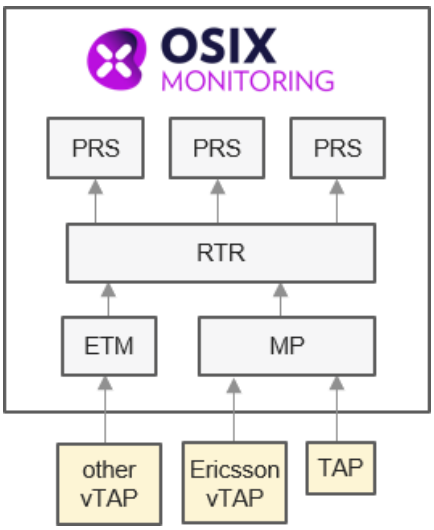


Figure 108: 5G SA signalling to OSIX Monitoring

13.3 vTAP support

The different vendors different vTAPs provides third-party systems like OSIX with unciphered data, either directly from the NF, or from an intermediate SCP (Service Communication Proxy). This is often the only way to get a full picture of all the signalling in a 5G SA network. However, there are some challenges. One challenge is to identify the actual NF itself. The traditional way to identify nodes in a core network is based on IP addresses. In 5G SA the destination IP will often still be okay, but the sending NF will normally only know its own internal IP. Instead, we must use NF names and FQDNs to identify the involved nodes. This information (and similar) will be send to us by meta data. These meta data are sent in different ways, and look quite different depending on the vTAP used.

There are many different vTAP vendors, all with their own specific solutions. Elisa Polystar adds support for these vendors when any of our customers implements them in their network.

13.3.1 Supported vTAP vendors

Currently, the following vendors and vTAPs are supported, but more are added continuously:

13.3.1.1 Ericsson vTAP

Ericsson dual-mode architecture comes with a Packet Core Controller (PCC) containing two vTAPs for 5G SA, one for the AMF and one for the SMF. The connection between Ericsson and third-party systems is based on GRE tunnels. The two different vTAPs above use different tunnels, dynamically set up by meta data. The meta data consumed by OSIX Monitoring for the PCC vTAPs is found in GRE and pcapng but also in the JSON layer.

The other ten Ericsson NFs in the dual-mode core are found in six different products (CCSM, CCDM, CCPC, CCRC, CCES, and SC) and also use GRE as above. The meta data is sent in GRE and pcapng as above, but there is no meta data in the JSON layer.

For the Ericsson vTAPs, the MediaProbe is used to terminate the GRE tunnels. The twelve vTAPs above will slightly differ from each other, but all are supported by the OSIX Monitoring system. To handle the variety of vTAPs, the MediaProbe must be configured with application-specific information.

13.3.1.2 Nokia vTAP

The Nokia vTAP comes in three different flavours—CMG, CMM, and Mobile Core. Meta data is sent to us via the Homer Encapsulation Protocol v3 (HEP3), and the ETM terminates this stream and extracts the necessary meta data, including it in either fields in the protocols stack of the message or in internal messages.

13.3.1.3 Mavenir vTAP

The Mavenir vTAP sends us the signalling and meta data using Avro schemas. The receiving node is the ETM, and it extracts the signalling and aligns it for consumption of other OSIX components.

13.3.1.4 gRPC vTAPs

OSIX also supports to receive signalling using gRPC (gRPC Remote Procedure Calls). The receiving node is the ETM, and it extracts the signalling and aligns it for consumption of the other OSIX components. Today, we support Affirmed vTAP and BroadSoft vTAP this way.

14 OSIX Monitoring for radio networks

Radio Access Network (RAN) monitoring extends the visibility of OSIX from the core network to the RAN Radio Resource Control (RRC) interface, which is critical since the radio interface greatly influences performance and quality of the services being provided to users.

By monitoring RAN RRC, service providers can proactively identify and resolve issues before they become service-affecting, ensuring that their customers receive reliable and high-quality service. Additionally, RAN RRC monitoring enables service providers to optimise their network performance, which can improve overall customer satisfaction and reduce churn.

14.1 Summary of features for RAN monitoring

14.1.1 OSIX Monitoring

- OSIX Call Trace and Protocol Analyser RRC support
- OSIX columns for RRC
- Client correlation E2E, for example with S1AP and GTP
- IMSI enrichment RRC calls
- Timing advance information
- RAN GW node for integration towards RAN data source
  - Files
  - Streaming

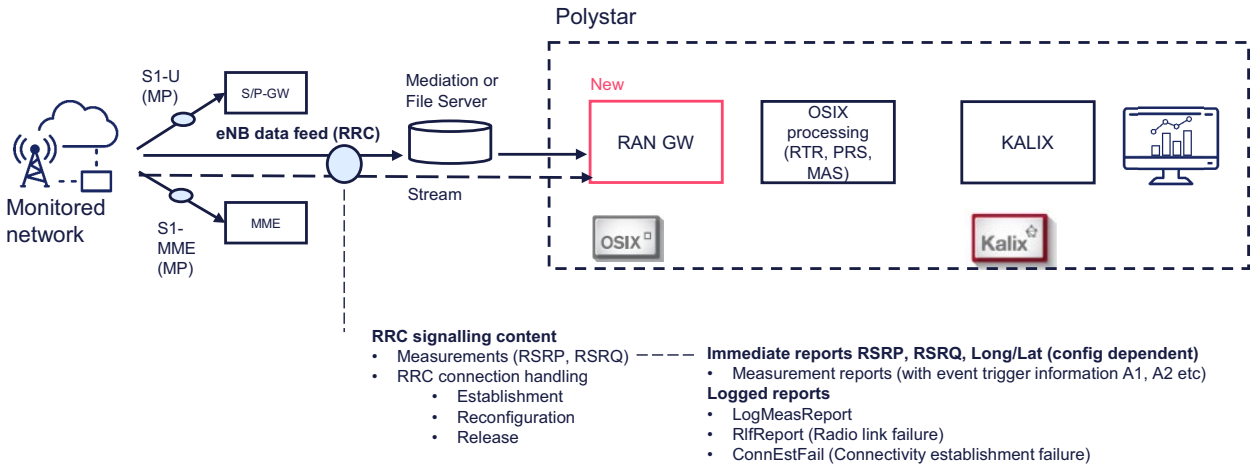
14.2 High level system architecture

RAN Gateway (RAN GW) is a new component that is introduced to the OSIX Monitoring architecture in order to receive, handle, and correlate radio RRC messages with existing core messages.

The RAN GW node acts as an interface between the RAN network and the existing processing nodes of the system. The RAN GW can handle file collection or TCP/IP sockets to collect the RAN data. Data is collected from eNodeBs through trace files or streams. Different ways of transferring the source data to the RAN GW are possible, for example, via an intermediate trace file server.

The trace data content provided by the eNodeBs are control plane protocols of the three surrounding interfaces—Uu, S1-MME, and X2. The main interest is the RRC protocol signalling, which is collected from Uu. The RRC protocol is responsible for the setup, reconfiguration, and release of the radio interface connection. The UE also uses RRC to report a set of various measurements (including RSRP and RSRQ) to the eNodeB. Some of these measurement reports can trigger handovers, and RRC is used in all of these mobility procedures.

The following figure highlights a generic implementation scenario:



14.3 RAN data collection

Collecting the RAN trace files from LTE cells typically requires access to the corresponding network management system. These systems provide a way to remotely collect and manage trace files from the LTE cells.

In general, the operator needs to have the proper software licenses and the hardware elements required by its corresponding RAN vendor in order to generate those files.

The following sections outline the general steps to collect RAN trace files from LTE cells.

14.3.1 RAN vendor-related requirements

Note: The specific steps to collect RAN trace files from LTE cells may vary depending on the network management system being used, as well as the specific LTE cell hardware and software. It is best to consult with the corresponding RAN vendor engineers to determine the best way to get these data.

14.3.1.1 Huawei RAN

Elisa Polystar will collect trace files from the Huawei trace server, which is part of the Huawei U2000 deployment and represents a unified system of collection for all trace files from different cells. RAN trace servers are usually generated and sent per cell every five minutes and have a predefined size which is configured by the Huawei NMS. Elisa Polystar requires access to at least the .SIG and .LOG files.

14.3.1.2 Nokia RAN

The new Data Collection and Analytics Platform (DCAP) solution for LTE/5G networks is the Nokia solution for collecting data from the eNodeB and make it available for third-party northbound interfaces using a real-time TCP/IP socket which supports both IPv4 and IPv6. The operator needs to configure the DCAP to forward LTE cell traffic to the receiving system. The receiving system, in this case Elisa Polystar, must have the appropriate decoders to decode the TCP stream into data.

14.3.1.3 Ericsson RAN

There are two ways to get the Ericsson LTE cell trace files. The first, and preferred, method is streaming mode or copying cell trace files from a storage location in the Ericsson ENM system. CTR is the file type that is typically used. The operator, with the help of Ericsson engineers, needs to make sure that all generic non-proprietary parameters required for RRC and MR monitoring are enabled in the CTR file feed.

14.4 MDT (Minimisation of Drive Test)

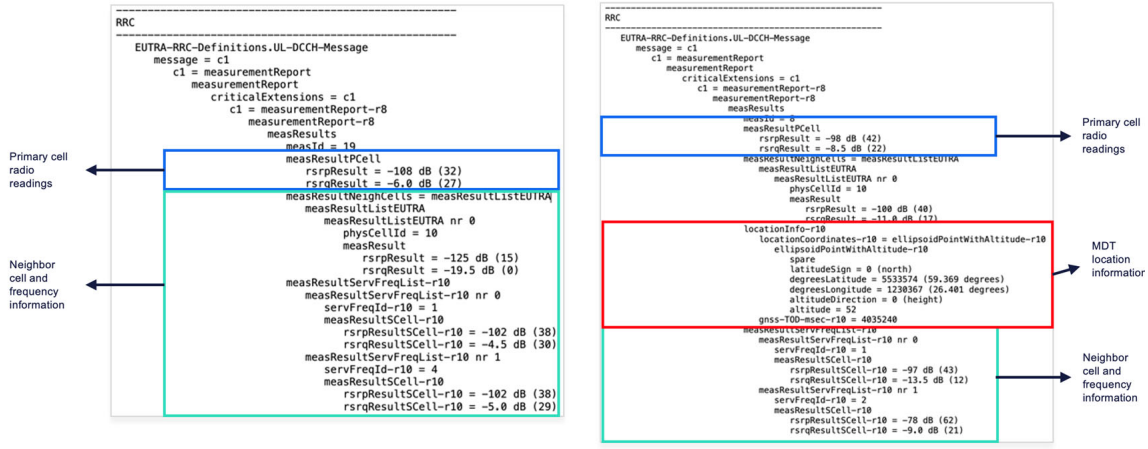
Minimisation of Drive Test (MDT) is a technique used in cellular networks to reduce the amount of drive tests required to optimise network performance. Drive tests involve physically driving around an area with a measurement device to collect data on network performance.

MDT allows network operators to collect performance data without the need for drive tests. This is achieved by using data already available in the network to determine the quality of service being delivered to users. This data is then used to identify areas of the network that require optimisation, such as areas with poor coverage or high congestion. MDT relies on measurements taken by user equipment, such as signal strength, signal quality, and connection drops. These measurements are sent to the network, where they are used to generate performance statistics. The statistics are then analysed to identify areas where performance is poor, and optimisation is required.

MDT is an important tool for network operators as it enables them to optimise their networks more efficiently and cost-effectively. It can help to improve network performance and increase user satisfaction. Elisa Polystar is introducing MDT support in its RAN monitoring solution to allow the operator to use KALIX advanced map visualisation to pinpoint where network radio performance is degrading, and drill down to individual XDRs per customer or event to OSIX Call Trace for an end-to-end call trace ladder diagram.

14.4.1 MDT in OSIX

OSIX Call Trace can show MDT-enriched measurement reports in the RRC measurement report message. The following figure illustrates the difference between an MDT-enriched measurement report and a regular measurement report message.



On the left, a normal measurement report message shows primary cell information and neighbour cell information, while on the right, another measurement report also shows primary and neighbour cell information with MDT-enriched data.

14.5 Geolocation

Geolocation is an OSIX feature that enriches RAN measurement reports with estimated GPS coordinates for each UE. The enrichment is done in real time using a machine learning (ML) model that estimates latitude and longitude from radio-level measurements obtained from UE measurements reports. For training the model, a feed of MDT measurement reports that include the UE GPS locations is required.

The need for the Geolocation feature comes from the fact that in many networks the proportion of measurement reports containing UE GPS locations is very small (sometimes as little as 1 percent). Hence, it is beneficial to be able to enrich the rest of the measurement reports with estimated location information to provide more a comprehensive geographic view of the data.

Geolocated RAN data that can be accurately represented on a geographical map is of great value for optimising network performance and operations, such as performance monitoring, traffic management, or capacity planning. Such views are available in KALIX.

14.5.1 Data requirements

To enable robust ML geolocation, comprehensive training data availability is necessary. The solution requires a set of data inputs collected from MDT measurement reports that include the GPS location of the UE devices, and another set of inputs from network reference data. Briefly, the following types of data input are needed:

- MDT-enriched measurement reports
  - Serving cell measurements: RSRP, RSRQ, Timing Advance
  - Neighbouring cell measurements: RSRP, RSRQ
  - UE location: Latitude, longitude
- Reference data (for serving and neighbouring cells)
  - Location: Latitude, longitude
  - Bearing, antenna height, antenna tilt, transmit power, frequency

The dataset also needs to have the following characteristics:

- Substantial history (at least 30 days)
- Good geographical coverage

14.5.2 Geolocation accuracy

The accuracy of the Geolocation model can be measured by comparing the estimated locations to the real locations for those MDT-enriched measurement reports that include UE GPS locations. Another way would be through conducting drive tests.

The achievable accuracy depends on the environment (network density) and the number of training samples available in that area. It also depends on the quality and diversity of those training samples, but that is harder to quantify. In practice, when there is a lot of training data from an area, the estimated locations tend to be highly accurate. On the other hand, if there are very few training samples collected from an area, or none at all, the model cannot adapt to the specifics of that area, and is thus effectively falling back to a more generalised and less accurate prediction based on network geometry.

15 Protocol parameters

All parameters in a supported protocol are decoded in Call Trace and Protocol Analyser. To make searching efficient, a selection of the most interesting parameters are searchable. These protocol parameters are listed in this chapter.

15.1 Supported protocols

The OSIX protocol library currently supports a large number of different protocols, with different dialects for PSTN, mobile, IMS, VoIP, NGN, and LTE networks. New protocols for emerging technologies are continuously added.

See the *OSIX Supported Protocols* document for more information.

15.2 Call Trace

The protocol parameters listed are available for searching in Call Trace.

15.2.1 General

In Call Trace, the following General parameters are currently available:

Status	Protocol	#Messages
State Name	Timer	Routing Group
Start Time	Traffic Group	PRS ID
End Time	Reloaded	PRS IP
Duration	Transaction ID	HEP3 Correlation ID
Date	Row Nr	

Table 11: General parameters in Call Trace

15.2.2 5GC

In Call Trace, the following parameters for 5GC are currently available:

5GC Service	5GC Service Operation	5GC N2 Info
5GC Request Cause	5GC Cause	5GC Title
5GC IMSI	5GC IMEI(SV)	5GC MSISDN
5GC RAT	5GC MCC	5GC MNC
5GC TAC	5GC NCI	5GC ECI
5GC AMF Region	5GC AMF Set	5GC AMF Pointer
5GC DNN	5GC S-NSSAI SST	5GC S-NSSAI SD
5GC PDU Session Type	5GC PDU Session ID	5GC 5QI
5GC EPS Interworking Indication	5GC UE IPv4 address	5GC EIR Status
5GC HO State	5GC Source NF Instance ID	5GC Source FQDN
5GC Source NF Type	5GC Source NF	5GC Destination FQDN
5GC Destination NF	5GC Target FQDN	5GC Target NF Type
5GC Target NF	5GC 3gpp-sbi-target-apiroot	5GC next-hop-authority
5GC Session AMBR DL (Mbps)	5GC Session AMBR UL (Mbps)	5GC Charging Characteristics
5GC Rating Group	5GC Used Total Volume	5GC Used Uplink Volume
5GC Used Downlink Volume	5GC Result Code	

Table 12: 5GC parameters in Call Trace

15.2.3 5G NAS

In Call Trace, the following parameters for 5G NAS are currently available:

5GMM Msg	5GMM Registration Type	5GMM Type of Security Context
5GMM KSI	5GMM IMEISV	5GMM IMSI
5GMM 5G-TMSI	5GMM Old 5G-TMSI	5GMM Additional 5G-TMSI
5GMM TAC	5GMM Cause	5GMM PDU Session Status
5GMM Deciphered	5GMM Integrity Algorithm	5GMM Ciphering Algorithm
5GMM SUCI MCC	5GMM SUCI MNC	5GMM NSSAI Requested
5GMM NSSAI Allowed	5GMM NSSAI Rejected	5GSM Msg
5GSM Cause	5GSM DNN	5GSM S-NSSAI SST
5GSM S-NSSAI SD	5GSM SSC Mode	5GSM Session AMBR DL (Mbps)
5GSM Session AMBR UL (Mbps)	5GS NAS MM Msg	5GS NAS MM Registration type
5GS NAS MM Type of Security Context	5GS NAS MM KSI	5GS NAS MM IMSI
5GS NAS SM SSC Mode	5GS NAS MM IMEISV	5GS NAS UE Policy Msg Type
5GS NAS UE Policy UPSC Indicated	5GS NAS UE Policy UPSC Added/Updated	5GS NAS UE Policy Removed

Table 13: 5G NAS parameters in Call Trace

15.2.4 AggData

In Call Trace, the following parameters for AggData are currently available:

AggData User Protocol	AggData HTTP Url	AggData HTTP Host
AggData HTTP Cause	AggData HTTP Referer	AggData HTTP User Agent
AggData DNS Query Name	AggData DNS Response Code	AggData MMS Message Type
AggData MMS From	AggData MMS To	AggData MMS User Agent
AggData MMS Response Status	AggData RTSP Url	AggData RTSP User Agent
AggData RTSP Status	AggData FTP User Name	AggData FTP request First Error Reason
AggData IMAP User Name	AggData SMTP User Name	AggData POP3 User Name
AggData Stack	AggData Application	AggData UL Packets
AggData DL Packets	AggData UL Bytes	AggData DL Bytes
AggData UL Throughput (kbit/s)	AggData DL Throughput (kbit/s)	AggData # User Data Msgs
AggData UL Peak Throughput (kbit/s)	AggData DL Peak Throughput (kbit/s)	

Table 14: AggData parameters in Call Trace

Note: In **Call Trace**, “A/B” is added for each stream for AggRTP parameters.

15.2.5 AggMSRP

In Call Trace, the following parameters for AggMSRP are currently available:

AggMSRP Source IP	AggMSRP Destination IP	AggMSRP Source Port
AggMSRP Destination Port		

Table 15: AggMSRP parameters in Call Trace

15.2.6 AggRTP - End Point Descriptor

In Call Trace, the following parameters for AggRTP - End Point Descriptor are currently available:

AggRTP UDP Source Address	AggRTP UDP Dest Address
AggRTP UDP Source Port	AggRTP UDP Dest Port

Table 16: AggRTP - End Point Descriptor parameters in Call Trace

15.2.7 AggRTP - Codec Metrics

In Call Trace, the following parameters for AggRTP - Codec Metrics are currently available:

AggRTP Vocoder Type	AggRTP Payload Type

Table 17: AggRTP - Codec Metrics parameters in Call Trace

15.2.8 AggRTP - Packet Transport Record

In Call Trace, the following parameters for AggRTP - Packet Transport Record are currently available:

AggRTP Packets Received	AggRTP Packets Discarded	AggRTP Avg. Packet Loss (%)
AggRTP Packets Lost	AggRTP Packets Duplicated	

Table 18: AggRTP - Packet Transport Record parameters in Call Trace

15.2.9 AggRTP - Jitter Record (RFC 3550)

In Call Trace, the following parameters for AggRTP - Jitter Records are currently available:

AggRTP Max. PPDV (ms)	AggRTP Avg. PPDV (ms)

Table 19: AggRTP - Jitter Records parameters in Call Trace

15.2.10 AggRTP - RTCP Delay Record

In Call Trace, the following parameters for AggRTP - RTCP Delay Record are currently available:

AggRTP RTCP Avg. Round-trip Network Delay (ms)	AggRTP RTCP Avg. One-way Delay (ms)
AggRTP RTCP Max. Round-trip Network Delay (ms)	AggRTP RTCP Max. One-way Delay (ms)

Table 20: AggRTP - RTCP Delay Record parameters in Call Trace

15.2.11 AggRTP - Quality Record (G. 107)

In Call Trace, the following parameters for AggRTP - Quality Records (G. 107) are currently available:

AggRTP R-Factor Listening Quality	AggRTP MOS Listening Quality
AggRTP R-Factor Conversational Quality	AggRTP MOS Conversational Quality

Table 21: AggRTP - Quality Records. 107) parameters in Call Trace

15.2.12 AggRTP - Degradation Metrics

In Call Trace, the following parameters for AggRTP - Degradation Metrics are currently available:

AggRTP Loss Degr.	AggRTP Delay Degr.	AggRTP Echo Level Degr.
AggRTP Discard Degr.	AggRTP Signal Level Degr.	AggRTP Recency Degr.
AggRTP CODEC Degr.	AggRTP Noise Level Degr.	

Table 22: AggRTP - Degradation Metrics parameters in Call Trace

15.2.13 AggRTP - RTCP End System Delay Record

In Call Trace, the following parameters for AggRTP - RTCP End System Delay Record are currently available:

AggRTP RTCP Avg. Orig. End-System Delay (ms)	AggRTP RTCP Avg. Term. End-System Delay (ms)
AggRTP RTCP Max. Orig. End-System Delay (ms)	AggRTP RTCP Max. Term. End-System Delay (ms)

Table 23: AggRTP - RTCP End System Delay Record parameters in Call Trace

15.2.14 AggRTP - Voice Jitter Records (G. 1020)

In Call Trace, the following parameters for AggRTP - Voice Jitter Records (G. 1020) are currently available:

AggRTP Avg. Mean-Absolute Packet Delay Variation (PDV)	AggRTP Max. Mean-Absolute Packet Delay Variation (PDV)

Table 24: AggRTP - Voice Jitter Records (G. 1020) parameters in Call Trace

15.2.15 AggRTP - RTCP-XR Record

In Call Trace, the following parameters for AggRTP - RTCP-XR Record are currently available:

AggRTP RTCP-XR Loss Rate (%)	AggRTP RTCP-XR RT Delay (ms)	AggRTP RTCP-XR R-factor
AggRTP RTCP-XR Discard Rate (%)	AggRTP RTCP-XR End Sys. Delay (ms)	AggRTP RTCP-XR Ext. R-factor
AggRTP RTCP-XR Avg Burst Density(%)	AggRTP RTCP-XR Signal Lvl. (dBm)	AggRTP RTCP-XR MOS-LQ
AggRTP RTCP-XR Avg Gap Density (%)	AggRTP RTCP-XR Noise Lvl. (dBm)	AggRTP RTCP-XR MOS-CQ

Table 25: AggRTP - RTCP-XR Record parameters in Call Trace

AggRTP RTCP-XR Avg Burst Duration (ms)	AggRTP RTCP-XR Residual ERL (dB)	AggRTP RTCP-XR RX Config
AggRTP RTCP-XR Avg Gap Duration (ms)	AggRTP RTCP-XR Gap Size (# of packets)	

Table 25: AggRTP - RTCP-XR Record parameters in Call Trace (Continued)

15.2.16 AggRTP - RTCP SR Record

In Call Trace, the following parameters for AggRTP - RTCP SR Record are currently available:

AggRTP RTCP-SR # of RTP Packets	AggRTP RTCP-SR # of RR Reports	AggRTP RTCP-SR # of Octets

Table 26: AggRTP - RTCP SR Record parameters in Call Trace

15.2.17 AggRTP - RTCP RR Record

In Call Trace, the following parameters for AggRTP - RTCP RR Record are currently available:

AggRTP RTCP-RR Packets Lost	AggRTP RTCP-RR DLSR	AggRTP RTCP-RR Inter Arrival Jitter

Table 27: AggRTP - RTCP RR Record parameters in Call Trace

15.2.18 AggRTP - RTCP SS/RR-based QoE Metrics

In Call Trace, the following parameters for AggRTP - RTCP SS/RR-based QoE Metrics are currently available:

AggRTP RTCP-SR/RR MOS-LQ	AggRTP RTCP-SR/RR MOS-CQ

Table 28: AggRTP - RTCP SS/RR-based QoE Metrics parameters in Call Trace

15.2.19 AggRTP - Gap 500 Delay Record

In Call Trace, the following parameters for AggRTP - Gap 500 Delay Record are currently available:

AggRTP Gap 500 Delay (ms)	AggRTP Gap 500 Delay Ratio (%)

Table 29: AggRTP - Gap 500 Delay Record parameters in Call Trace

15.2.20 AggRTP - DTMF Record

In Call Trace, the following parameters for AggRTP - DTMF Record are currently available:

AggRTP DTMF Packets Out Of Order	AggRTP DTMF Packets Lost	AggRTP DTMF Events Discarded
AggRTP DTMF Very Low Volume	AggRTP DTMF Very High Volume	AggRTP DTMF High Quality Sequence
AggRTP DTMF Digits		

Table 30: AggRTP - DTMF Record parameters in Call Trace

15.2.21 AggRTP - Voice Quality

In Call Trace, the following parameters for AggRTP - Voice Quality are currently available:

AggRTP Lowest MOS CQ	AggRTP Lowest MOS LQ	AggRTP Packet Loss (%) at lowest MOS
AggRTP Lowest MOS Time	AggRTP Number of Final Aggs	AggRTP Gap Between Aggs

Table 31: AggRTP - Voice Quality parameters in Call Trace

15.2.22 AIN

In Call Trace, the following parameters for AIN are currently available:

AIN Calling Number	AIN Called Number	AIN Routing Number

Table 32: AIN parameters in Call Trace

15.2.23 ALCAP

In Call Trace, the following parameters for ALCAP are currently available:

ALCAP Cause	ALCAP Dest SAI	ALCAP Aal2 Path Id
ALCAP Orig SAI	ALCAP SUGR	ALCAP CID

Table 33: ALCAP parameters in Call Trace

15.2.24 Any Protocol

In Call Trace, the following parameters for Any Protocol are currently available:

Any Protocol A Number	Any Protocol B Number	Any Protocol IMSI
Any Protocol CI	Any Protocol LAC	Any Protocol RAC
Any Protocol SAC	Any Protocol Conversation Duration	Any Protocol IMEI(SV)
Any Protocol MNC	Any Protocol MCC	Any Protocol APN/DNN

Table 34: Any Protocol parameters in Call Trace

15.2.25 ATM

In Call Trace, the following parameters for ATM are currently available:

ATM Path ID	ATM VCI
ATM VPI	ATM CID

Table 35: ATM parameters in Call Trace

15.2.26 BSSAP

In Call Trace, the following parameters for BSSAP are currently available:

BSSAP Layer 3 Msg	BSSAP LCS Cause	BSSAP Redir Num
BSSAP BSSMAP Cause	BSSAP MCC	BSSAP DTAP CC Cause
BSSAP Assignment Failure Cause	BSSAP MNC	BSSAP IMSI
BSSAP Handover Failure Cause	BSSAP LAC	BSSAP Incoming HO Cmd
BSSAP Handover Required Reject Cause	BSSAP CI	BSSAP Outgoing HO Cmd
BSSAP Handover Required Cause	BSSAP Last CI	BSSAP Firts HO Ref
BSSAP BSSMAP Last Cause	BSSAP CIC	BSSAP Latest HO Ref

Table 36: BSSAP parameters in Call Trace

BSSAP BSSMAP Transport Layer Address MSC	BSSAP Called Num	BSSAP Answer Time
BSSAP BSSMAP Transport Layer Address BSC	BSSAP Calling Num	BSSAP Release Time
BSSAP RR Cause	BSSAP Connected Num	BSSAP Conversation Duration

Table 36: BSSAP parameters in Call Trace (Continued)

15.2.27 BSSAP+

In Call Trace, the following parameters for BSSAP+ are currently available:

BSSAP+ Msg	BSSAP+ IMSI Detach Non GPRS	BSSAP+ Cell Global ID RAC
BSSAP+ IMSI	BSSAP+ Gs Cause	BSSAP+ LAI LAC
BSSAP+ SGSN Number	BSSAP+ Reject Cause	BSSAP+ TMSI
BSSAP+ IMSI Detach GPRS	BSSAP+ Cell Global ID LAC	BSSAP+ NRI

Table 37: BSSAP+ parameters in Call Trace

15.2.28 Circuit

In Call Trace, the following parameters for Circuit are currently available:

Circuit CIC	Circuit B Number	Circuit A NoA
Circuit A Number	Circuit B NoA	

Table 38: Circuit parameters in Call Trace

15.2.29 Circuit - ISUP

In Call Trace, the following parameters for ISUP are currently available:

ISUP Cause Value	ISUP DPC CIC	ISUP Answer Time
ISUP ACM Cause Value	ISUP Releasing OPC	ISUP Release Time
ISUP Location Nr	ISUP TMR	ISUP Conversation Duration
ISUP Redirecting Nr	ISUP Route Identity	ISUP ACM Time
ISUP Original Called Nr	ISUP Redirection Reason	ISUP Setup Time
ISUP Generic Number	ISUP Call Identity	ISUP Address Presentation Restricted Indicator
ISUP Charge Ind	ISUP Network Exchange Identity	ISUP Echo Flag
ISUP OPC CIC	ISUP Cause Location	ISUP Correlation id

Table 39: ISUP parameters in Call Trace

15.2.30 Circuit - IUP

In Call Trace, the following parameters for IUP are currently available:

IUP Called Nbr	IUP Line Id NAI	IUP Answer Time
IUP Calling Nbr	IUP Calling NAI	IUP Release Time
IUP Line ID	IUP Full Calling Line ID	IUP Conversation Duration
IUP Reason	IUP Full Calling NAI	IUP Setup Time
IUP Line Id Type	IUP CNA Reason	

Table 40: IUP parameters in Call Trace

15.2.31 Circuit - BICC

In Call Trace, the following parameters for BICC are currently available:

BICC Cause Value	BICC Action Indicator	BICC Release Time
BICC Location Nr	BICC TMR	BICC Conversation Duration
BICC Redirecting Nr	BICC Transport Layer Address	BICC Setup Time
BICC Original Called Nr	BICC Backbone Network Id	
BICC Charge Ind	BICC Answer Time	

Table 41: BICC parameters in Call Trace

15.2.32 DHCP

In Call Trace, the following parameters for DHCP are currently available:

DHCP Bootp Msg	DHCP Domain Name	DHCP First DNS Address
DHCP Transaction ID	DHCP Lease Time	DHCP Relay Agent Info Type
DHCP Client MAC	DHCP Server ID	DHCP Relay Agent Circuit ID
DHCP Client IP	DHCP Renewal Time	DHCP Relay Agent Remote ID
DHCP Your IP	DHCP Rebinding Time	DHCP Relay Agent Subscriber ID
DHCP Relay agent IP	DHCP Vendor Class ID	DHCP First Classless Static Route
DHCP Subnet Mask	DHCP Client ID	
DHCP Host Name	DHCP First Router Address	

Table 42: DHCP parameters in Call Trace

15.2.33 DIAMETER

In Call Trace, the following parameters for DIAMETER are currently available:

DIAMETER Command Code	DIAMETER Application Id	DIAMETER Origin Host
DIAMETER Origin Realm	DIAMETER Destination Host	DIAMETER Destination Realm
DIAMETER Session Id	DIAMETER IMSI	DIAMETER MSISDN Number
DIAMETER Calling party address	DIAMETER Called party address	DIAMETER Public Identity
DIAMETER Multiple Services CC Result	DIAMETER Multiple Services CC Service Id	DIAMETER Multiple Services CC Rating group
DIAMETER Used Input Octets	DIAMETER Used Output Octets	DIAMETER Used Total Octets
DIAMETER Framed IP	DIAMETER Called Station	DIAMETER SGSN IP
DIAMETER GGSN IP	DIAMETER Last Hop Dest IP	DIAMETER Charging Characteristics
DIAMETER Radio Access Type 2G/3G	DIAMETER ICID	DIAMETER User Name
DIAMETER SIP Method	DIAMETER Cause Code	DIAMETER Result Code
DIAMETER Experimental result code	DIAMETER SGSN MCC	DIAMETER SGSN MNC
DIAMETER Charging rule name	DIAMETER Charging rule base name	DIAMETER Event trigger
DIAMETER Priority level	DIAMETER Preemption capability	DIAMETER Preemption vulnerability
DIAMETER Disconnect cause	DIAMETER MCC	DIAMETER MNC

Table 43: DIAMETER parameters in Call Trace

DIAMETER LAC	DIAMETER SAC/CI	DIAMETER IMEI(SV)
DIAMETER Framed IPv6 prefix	DIAMETER QCI	DIAMETER Max Response Time
DIAMETER Subscription Id	DIAMETER Subscription Type	DIAMETER Server Assignment Type
DIAMETER User Authorization Type	DIAMETER User Data Already Available	DIAMETER UE SRVCC Capability
DIAMETER ECI	DIAMETER Data Reference	DIAMETER IPCAN Type
DIAMETER NIDD Used	DIAMETER NIDD Delivery	DIAMETER PDN Continuity
DIAMETER Operation Mode	DIAMETER 5GS Interworking	DIAMETER DRMP
DIAMETER NBIFOM	DIAMETER eDRX RAT	DIAMETER Additional APN
DIAMETER SCEF Realm	DIAMETER eDRX Cycle	DIAMETER Paging Window
DIAMETER UE Usage Type	DIAMETER ULR Flags	DIAMETER Access Restriction Data
DIAMETER Subscription Data Flags	DIAMETER Preferred Data Mode	DIAMETER V2X Permission
DIAMETER Core Network Restrictions	DIAMETER Ext Max Requested BW DL (kbps)	DIAMETER Ext Max Requested BW UL (kbps)
DIAMETER Ext APN AMBR DL (kbps)	DIAMETER Ext APN AMBR UL (kbps)	DIAMETER Ext GBR DL (kbps)
DIAMETER Ext GBR UL (kbps)	DIAMETER Service selection	DIAMETER 2nd RAT
DIAMETER Abort Cause	DIAMETER Termination cause	DIAMETER Ext BW NR
DIAMETER V2X Allowed	DIAMETER Visited NW Identifier	DIAMETER TAC
DIAMETER Equipment Status	DIAMETER CC Request Type	DIAMETER Accounting Record Type
DIAMETER RFSP	DIAMETER Rx Request Type	DIAMETER Rx Media Type

Table 43: DIAMETER parameters in Call Trace (Continued)

15.2.34 DNS

In Call Trace, the following parameters for DNS are currently available:

DNS Opcode	DNS Response Code	DNS Called Number
DNS Query Name	DNS Answer Address	DNS Enum Service Address
DNS Qtype	DNS Answer Count	DNS ID
DNS Qclass	DNS Answer Result	

Table 44: DNS parameters in Call Trace

15.2.35 EMI

In Call Trace, the following parameters for EMI are currently available:

EMI Operation Type	EMI Response Type	EMI Error Code
EMI Source Address	EMI Destination Address	EMI PID
EMI Message Type	EMI DCS	

Table 45: EMI parameters in Call Trace

15.2.36 EMPP

In Call Trace, the following parameters for EMPP are currently available:

EMPP Method	EMPP Response Status	EMPP CSeq
EMPP Message Type	EMPP A Number	EMPP B Number
EMPP Source IMSI	EMPP Destination IMSI	EMPP Charge IMSI
EMPP Charge MSISDN	EMPP Operation Result	

Table 46: EMPP parameters in Call Trace

15.2.37 ESP

In Call Trace, the following parameters for ESP (IP Encapsulating Security Payload) are available:

Security Parameters Index (SPI) Sequence Number

Table 47: ESP parameters in Call Trace

15.2.38 Ethernet

In Call Trace, the following parameters for Ethernet are currently available:

VLAN Priority	VLAN ID	Ethernet Dest Mac Address
VLAN CFI	Ethernet Source Mac Address	

Table 48: Ethernet parameters in Call Trace

15.2.39 GPRS Gb

In Call Trace, the following parameters for GPRS Gb are currently available:

GPRS IMSI	BSSGP PDU*	BSSGP Cause
BSSGP Radio Cause	BSSGP MCC	BSSGP MNC
BSSGP LAC	BSSGP RAC	BSSGP CI
BSSGP TLLI	BSSGP NRI	GPRS Uplink Bytes
GPRS Downlink Bytes	GPRS # User Data Messages	BSSGP Last LAC
BSSGP Last RAC	BSSGP Last CI	

Table 49: GPRS GB parameters in Call Trace

15.2.40 GTP

In Call Trace, the following parameters for GTP are currently available:

GTP Message*	GTP Version	GTP IMSI
GTP MSISDN	GTP End User Address	GTP End User Address IPv6
GTP APN	GTP Cause	GTP Request Cause
GTP Tunnelled Source Address	GTP Tunnelled Dest Address	GTP Charging Characteristics
GTP IMEI(SV)	GTP RADIO MCC	GTP RADIO MNC
GTP RADIO LAC	GTP CORE MCC	GTP CORE MNC
GTP CORE LAC	GTP TAC	GTP DTI
GTP NSAPI	GTP Multiple NSAPI	GTP EBI
GTP RAN address for user traffic	GTP RAC	GTP SAC

Table 50: GTP parameters in Call Trace

GTP CI	GTP ECI	GTP Radio Access Technology
GTP STN-SR Address	GTP Sv MME CP Address	GTP Sv MSC CP Address
GTP RNC ID	GTP Target CI	GTP SRVCC Cause
GTP PDP/PDN Type	GTP Uplink CP Address	GTP Uplink UP Address
GTP Downlink CP Address	GTP Downlink UP Address	GTP DL MBR
GTP DL GBR	GTP UL MBR	GTP UL GBR
GTP v2-C Interface	GTP v2-U Interface	GTP Mapped UE UT
GTP Serving PLMN UL Rate Limit	GTP Serving PLMN DL Rate Limit	GTP CIoT Optimizations Support
GTP Indication Flags	GTP Dual Connectivity NR	GTP MME Code
GTP Req Recovery Restart Counter	GTP Resp Recovery Restart Counter	GTP 2nd RAT Report
GTP 2nd RAT usage data DL	GTP 2nd RAT usage data UL	

Table 50: GTP parameters in Call Trace (Continued)

15.2.41 H.323

In Call Trace, the following parameters for H.323 are currently available:

H.323 Display	H.323 Calling Party Number	H.323 Called Party Number
H.323 Calling Type of Number	H.323 Called Type of Number	H.323 Cause Value
H.323 RAS Msg	H.323 Source Address Number	H.323 Source Address Text
H.323 Destination Address Number	H.323 Destination Address Text	H.323 Call Identifier GUID
H.3223 IP Address	H.323 Port Number	

Table 51: H.323 parameters in Call Trace

15.2.42 HTTP

In Call Trace, the following parameters for HTTP are currently available:

HTTP Method	HTTP Status Code	HTTP Request URI
HTTP Host	HTTP Uplink Bytes	HTTP Downlink bytes
HTTP Location	HTTP User Agent	HTTP Via

Table 52: HTTP parameters in Call Trace

15.2.43 HTTP - HTTP/2

In Call Trace, the following parameters for HTTP - HTTP/2 are currently available:

HTTP - HTTP/2 Stream Identifier	HTTP - HTTP/2 Header Lookup Status	HTTP - HTTP/2 Source Socket Address
HTTP - HTTP/Dest Socket Address		

Table 53: HTTP - HTTP/2 parameters in Call Trace

15.2.44 IMF

In Call Trace, the following parameters for IMF are currently available:

IMF Date	IMF From	IMF Sender
IMF To	IMF Cc	IMF Bcc

Table 54: IMF parameters in Call Trace

15.2.45 IP

In Call Trace, the following parameters for IP are currently available:

IP Source Address	IP Protocol	IP Tunnel Dest Address
IP Dest Address	IP Tunnel Source Address	IP Tunnel Protocol

Table 55: IP parameters in Call Trace

15.2.46 ISAKMP

In Call Trace, the following parameters for ISAKMP (Internet Security Association and Key Management Protocol)/IKE v2 (Internet Key Exchange Protocol Version 2) are currently available:

Initiator SPI	Responder SPI	Exchange Type

Table 56: ISAKMP parameters in Call Trace

15.2.47 ISDN

In Call Trace, the following parameters for ISDN are currently available:

ISDN Call Reference	ISDN CR Flag	ISDN Called Party Number
ISDN Calling Party Number	ISDN Called TypeOfNum	ISDN Calling TypeOfNum
ISDN Cause Value	ISDN Channel number	ISDN Information transfer capability
ISDN Conversation Duration	ISDN High Layer Characteristics	ISDN Transfer Mode
ISDN Userinfo Layer1 Protocol	ISDN Location	

Table 57: ISDN parameters in Call Trace

15.2.48 ISDN SS

In Call Trace, the following parameters for ISDN SS are currently available:

ISDN SS Called Number	ISDN SS Calling Number

Table 58: ISDN SS parameters in Call Trace

15.2.49 LCS-AP

In Call Trace, the following parameters for LCS-AP are currently available:

LCS-AP Correlation ID	LCS-AP MCC	LCS-AP eNB ID
LCS-AP Procedure Code	LCS-AP Cell Identity	LCS-AP Sector ID
LCS-AP MNC	LCS-AP LCS Cause	LCS-AP IMSI

Table 59: LCS-AP parameters in Call Trace

15.2.50 LDAP

In Call Trace, the following parameters for LDAP are currently available:

LDAP Msg	LDAP Msg ID	LDAP IMSI
LDAP MSISDN	LDAP SGSN Number	LDAP SGSN Address
LDAP VLR Number	LDAP MSC Number	LDAP Result Code.
LDAP IMPI	LDAP IMPU	LDAP Assoc Id
LDAP Policy id	LDAP Market Code id	LDAP TOA Status
LDAP TOA Level	LDAP AV Status	LDAP PC Status

Table 60: LDAP parameters in Call Trace

LDAP PC Week Schedule	LDAP DN dc	LDAP DN ou
LDAP DN cn	LDAP DN serv	LDAP DN mscId
LDAP Uplink Bytes	LDAP Downlink Bytes	LDAP Uplink Message Count
LDAP Downlink Message Count	LDAP DN Other Number	

Table 60: LDAP parameters in Call Trace (Continued)

15.2.51 LPPa

In Call Trace, the following parameters for LPPa are currently available:

LPPa Procedure Code	LPPa Cell Portion Id	LPPa E-UTRAN Cell Id
LPPa Type of Message	LPPa MCC	LPPa TAC
LPPa Transaction Id	LPPa MNC	LPPa Cause

Table 61: LPPa parameters in Call Trace

15.2.52 MEGACO

In Call Trace, the following parameters for MEGACO are currently available:

MEGACO Version	MEGACO Transaction Id	MEGACO Context Id
MEGACO Error Code	MEGACO Command	MEGACO Termination ID
MEGACO Second Termination ID	MEGACO Transport Layer Address	MEGACO BIR SUGR
MEGACO IMSI	MEGACO Called Number	MEGACO Calling Number
MEGACO Media Gateway Controller MId	MEGACO Media Gateway MId	MEGACO RTP Packet Loss %
MEGACO RTP Jitter	MEGACO RTP Delay	

Table 62: MEGACO parameters in Call Trace

15.2.53 MGCP

In Call Trace, the following parameters for MGCP are currently available:

MGCP Verb	MGCP Caller Id	MGCP Latency
MGCP Endpoint Name	MGCP Called Number	MGCP Media Gateway
MGCP Response Code	MGCP Packet Loss %	MGCP Media Gateway Controller
MGCP Call Id	MGCP Jitter	

Table 63: MGCP parameters in Call Trace

15.2.54 MM/SM

In Call Trace, the following parameters for MM/SM are currently available:

MM/SM Msg*	MM/SM APN	MM/SM Mobile IP Address
MM/SM IMSI	MM/SM TMSI	MM/SM NRI
MM/SM New TMSI	MM/SM New NRI	MM/SM M-TMSI
MM/SM IMEI	MM/SM IMEISV	MM/SM MCC
MM/SM MNC	MM/SM LAC	MM/SM RAC
MM/SM TAC	MM/SM CI	MM/SM MM Cause
MM/SM SM Cause	MM/SM Reject Cause	MM/SM CC Cause
MM/SM Service Type	MM/SM Other Rate Adaption	MM/SM Ciphering Algorithm
MM/SM Deciphered	MM/SM KSI	MM/SM QCI

Table 64: MM/SM parameters in Call Trace

MM/SM ESM Msg	MM/SM Traffic Handling Priority	MM/SM Location Update Type
MM/SM EPS Update Type	MM/SM Voice Domain Preference	MM/SM CSFB Indicator
MM/SM Integrity Algorithm	MM/SM GUTI Type	MM/SM P-TMSI Signature
MM/SM UE CP CIoT	MM/SM UE UP CIoT	MM/SM UE ER w/o PDN
MM/SM UE S1-U data	MM/SM UE HC-CP CIoT	MM/SM UE DCNR
MM/SM UE PNB-CIoT	MM/SM UE N1 mode	MM/SM NW CP CIoT
MM/SM NW UP CIoT	MM/SM NW ER w/o PDN	MM/SM NW S1-U data
MM/SM NW HC-CP CIoT	MM/SM NW Restrict DCNR	MM/SM Ext EMM cause EPS opt info
MM/SM Ext EMM cause NB-IoT allowed	MM/SM NW Control plane only indication	MM/SM T3412
MM/SM T3412 Extended	MM/SM P-CSCF IPv6	MM/SM Type of security context
MM/SM EPC Capability		

Table 64: MM/SM parameters in Call Trace (Continued)

15.2.55 MMS

In Call Trace, the following parameters for MMS are currently available:

MMS Msg Type	MMS Transaction Id	MMS From
MMS Msg ID	MMS Response Status	MMS To
MMS A Number	MMS B Number	MMS Recipient Count

Table 65: MMS parameters in Call Trace

15.2.56 MTP3/M3UA

In Call Trace, the following parameters for MTP3/M3UA are currently available:

MTP3/M3UA OPC	MTP3/M3UA OPC NI	MTP3/M3UA NI
MTP3/M3UA DPC	MTP3/M3UA DPC NI	

Table 66: MTP3/M3UA parameters in Call Trace

15.2.57 NBAP

In Call Trace, the following parameters for NBAP are currently available:

NBAP Procedure Code	NBAP Cell Id	NBAP DCH Port NodeB
NBAP UL Scrambling Code	NBAP Binding ID	NBAP DCH Port RNC
NBAP CRNC Communication Context Id	NBAP Radio Link Id	
NBAP NodeB Communication Context Id	NBAP Cause	

Table 67: NBAP parameters in Call Trace

15.2.58 NGAP

In Call Trace, the following parameters for NGAP are currently available:

NGAP Procedure Code	NGAP RAN UE ID	NGAP AMF UE ID
NGAP Source AMF UE ID	NGAP Cause	NGAP TAI MCC
NGAP TAI MNC	NGAP NR CGI MCC	NGAP NR CGI MNC

Table 68: NGAP parameters in Call Trace

NGAP NR Cell Identity	NGAP NR Last Cell Identity	NGAP RRC Establishment Cause
NGAP TAC	NGAP S-NSSAI SST	NGAP S-NSSAI SD
NGAP 5QI	NGAP UE AMBR UL	NGAP UE AMBR DL
NGAP 5G-TMSI	NGAP AMF Region	NGAP AMF Set
NGAP AMF Pointer	NGAP PDU Session ID	NGAP PDU Session Type
NGAP IMSI Enriched By	NGAP IMSI Enriched Reliability	NGAP NSSAI Allowed

Table 68: NGAP parameters in Call Trace (Continued)

15.2.59 PCAP

In Call Trace, the following parameters for PCAP are currently available:

PCAP Transaction Id	PCAP Request Type Event	PCAP Cell ID
PCAP Procedure Code	PCAP Positioning Method	PCAP Cause
PCAP Message Type	PCAP RNC ID	

Table 69: PCAP parameters in Call Trace

15.2.60 PFCP

In Call Trace, the following parameters for PFCP are currently available:

PFCP Message	PFCP Cause	PFCP UE IP Address
PFCP APN	PFCP URR ID	PFCP IMSI
PFCP S-NSSAI SST	PFCP S-NSSAI SD	

Table 70: PFCP parameters in Call Trace

15.2.61 PWS

In Call Trace, the following parameters for PWS are currently available:

PWS Message Identifier	PWS Geographical Scope	PWS Message Code
PWS Update Number		

Table 71: PWS parameters in Call Trace

15.2.62 RADIUS

In Call Trace, the following parameters for RADIUS are currently available:

RADIUS Packet Type	RADIUS Identifier	RADIUS Accounting Input Octets
RADIUS Accounting Output Octets	RADIUS Accounting Session ID	RADIUS Framed IP Address
RADIUS Calling User	RADIUS Called User	RADIUS IMSI
RADIUS Connect Info	RADIUS ERX Ingress Policy Name	RADIUS ERX Primary DNS
RADIUS ERX Secondary DNS	RADIUS ERX Virtual Router Name	RADIUS NAS Identifier
RADIUS NAS Port ID	RADIUS User name	RADIUS MCC
RADIUS MNC		

Table 72: RADIUS parameters in Call Trace

15.2.63 RAN

In Call Trace, the following parameters for RAN are currently available:

RAN Cell ID	RAN eNodeB ID	RAN Call ID
RAN MAC TA value	RAN C-RNTI	RAN Eutran Trace ID
RAN Huawei Msg Type ID	RAN Nokia Msg Type ID	RAN MAC Power Headroom
RAN MAC UL-SINR	RAN MAC Angle of Arrival	RAN MAC Radio Link Failure

Table 73: RAN parameters in Call Trace

15.2.64 RANAP

In Call Trace, the following parameters for RANAP are currently available:

RANAP Procedure Code	RANAP IMSI	RANAP LAI LAC
RANAP SAI LAC	RANAP SAC	RANAP RAC
RANAP Transport Layer Address	RANAP Cause	RANAP RAB Cause
RANAP Called Number	RANAP Calling Number	RANAP MCC
RANAP MNC	RANAP Binding ID	RANAP GTP uplink teid
RANAP GTP downlink teid	RANAP Domain Indicator	RANAP Reject Cause Value
RANAP Global RNC ID	RANAP HO Command	RANAP Relocation Type
RANAP Target Cell ID	RANAP RNC ID	RANAP Cell ID
RANAP CN ID	RANAP Last LAI LAC	RANAP Last SAI LAC
RANAP Last SAC		

Table 74: RANAP parameters in Call Trace

15.2.65 RNSAP

In Call Trace, the following parameters for RNSAP are currently available:

RNSAP UL Scrambling Code	RNSAP Binding ID	RNSAP Cell
RNSAP IMSI	RNSAP RNC	RNSAP IMEI
RNSAP LAC	RNSAP RAC	RNSAP SAC
RNSAP Procedure Code	RNSAP MCC	RNSAP MNC
RNSAP ARP		

Table 75: RNSAP parameters in Call Trace

15.2.66 RRC

In Call Trace, the following parameters for RRC are currently available:

RRC Largest Container Size	3G RRC Message Type	3G RRC TMSI
3G RRC P-TMSI	3G RRC NRI	3G RRC IMSI
3G RRC Establishment Cause	3G RRC UL Scrambling Code	3G RRC LAC
3G RRC Cell ID	3G RRC NBAP Cell ID	3G RRC SRCN-ITY
3G RRC S-RNTI	4G RRC M-TMSI	4G RRC MME Code
4G RRC EUTRA freq	4G RRC EN-DC freq	4G RRC NR-SA freq
4G RRC Feature Group Ind	4G RRC 4x4 MIMO	4G RRC locationInfo
4G RRC IMSI	4G RRC #MR Immediate	4G RRC #MR Logged
4G RRC MDT Mode	4G RRC MDT Type	4G RRC RSRP Max Logged
4G RRC RSRP Min Logged	4G RRC RSRP Avg Logged	4G RRC RSRQ Max Logged

Table 76: RRC parameters in Call Trace

4G RRC RSRQ Min Logged	4G RRC RSRQ Avg Logged	4G RRC RSRP Max Immediate
4G RRC RSRP Min Immediate	4G RRC RSRP Avg Immediate	4G RRC RSRQ Max Immediate
4G RRC RSRQ Min Immediate	4G RRC RSRQ Avg Immediate	5G RRC NR freq
5G RRC EUTRA freq		

Table 76: RRC parameters in Call Trace (Continued)

15.2.67 RTSP

In Call Trace, the following parameters for RTSP are currently available:

RTSP Method	RTSP Status code	RTSP Reason Phrase
RTSP Version	RTSP Session Id	RTSP Url
RTSP Authorization User	RTSP User Agent	RTSP Server
RTSP Media Type	RTSP Session Start Time	RTSP Session End Time
RTSP Session Duration		

Table 77: RTSP parameters in Call Trace

15.2.68 S1AP

In Call Trace, the following parameters for S1AP are currently available:

S1AP Procedure Code	S1AP eNB UE S1AP ID	S1AP MME UE S1AP ID
S1AP IMSI	S1AP LAC	S1AP TAC
S1AP RAC	S1AP TAI MCC	S1AP TAI MNC
S1AP ECGI MCC	S1AP ECGI MNC	S1AP Cell Identity
S1AP Last Cell Identity	S1AP MME Code	S1AP M-TMSI
S1AP NRI	S1AP Sector	S1AP Last Sector
S1AP eNB ID	S1AP Last eNB ID	RRC Establishment Cause
S1AP Cause	S1AP IMSI Enriched By	S1AP IMSI Enrichment Reliability
S1AP SRVCC HO Indication	S1AP SGW-U IP	S1AP eNB/gNB-U IP
S1AP EMI IP	S1AP Handover Type	S1AP NEA
S1AP NIA	S1AP 2nd RAT Req	S1AP 2nd RAT Report
S1AP NB IoT Paging eDRX Cycle	S1AP NB IoT Paging Time Window	S1AP NR Restriction
S1AP LTE-M indication	S1AP Source MME UE S1AP ID	

Table 78: S1AP parameters in Call Trace

15.2.69 SBc-AP

In Call Trace, the following parameters for SBc-AP are currently available:

SBc-AP Procedure Code	SBc-AP Cause

Table 79: SBc-AP parameters in Call Trace

15.2.70 SCCP

In Call Trace, the following parameters for SCCP are currently available:

SCCP GT Called	SCCP GT Called (E.164)	SCCP GT Calling
SCCP SSN Called	SCCP SSN Calling	SCCP PC Called
SCCP PC Calling	SCCP NOA Called	SCCP NOA Called (E.164)
SCCP NOA Calling	SCCP NP Called	SCCP NP Called (E.164)
SCCP NP Calling	SCCP TT Called	SCCP TT Called (E.164)
SCCP TT Calling	SCCP Dest Local Ref	SCCP Source Local Ref
SCCP Return Cause	SCCP Release Cause	SCCP Refusal Cause
SCCP Reset Cause	SCCP Error Cause	

Table 80: SCCP parameters in Call Trace

15.2.71 SDP

In Call Trace, the following parameters for SDP are currently available:

SDP Audio Dest A	SDP Audio Dest B	SDP Video Dest A
SDP Video Dest B	SDP Message Dest A	SDP Message Dest B
SDP Audio Codec Used	SDP Video Codec Used	SDP Image Format
SDP Transport Protocol	SDP Text Dest A	SDP Text Dest B
SDP Text Codec Used	SDP Real Time Text Type	

Table 81: SDP parameters in Call Trace

15.2.72 SGsAP

In Call Trace, the following parameters for SGsAP are currently available:

SGsAP Msg	SGsAP IMSI	SGsAP MME Name
SGsAP IMSI Detach EPS	SGsAP IMSI Detach NON EPS	SGsAP IMEI(SV)
SGsAP SGs Cause	SGsAP Reject Cause	SGsAP Service Indicator
SGsAP LAC	SGsAP TAC	SGsAP UE EMM Mode
SGsAP MCC	SGsAP MNC	SGsAP TMSI

Table 82: SGsAP parameters in Call Trace

15.2.73 SIGTRAN

In Call Trace, the following parameters for SIGTRAN are currently available:

IUA Interface Identifier	M2UA Interface Identifier

Table 83: SIGTRAN parameters in Call Trace

15.2.74 SIP

In Call Trace, the following parameters for SIP are currently available:

SIP Method	SIP From User	SIP From Host
SIP To User	SIP To Host	SIP Call ID
SIP Diversion User	SIP Termination Code	SIP Termination Phrase
SIP Authorization User	SIP Calling User	SIP Request URI User
SIP Called User	SIP P-Asserted-Identity	SIP P-Called-Party-ID

Table 84: SIP parameters in Call Trace

SIP P-Charging Vector ICID	SIP P-Charging Addresses CCF	SIP P-Charging Addresses ECF
SIP A P-Access-Network-Info	SIP B P-Access-Network-Info	SIP Last A P-Access-Network-Info
SIP Last B P-Access-Network-Info	SIP Remote Party	SIP User Agent
SIP Expires	SIP Reason Header	SIP Server Header
SIP Via IP	SIP Contact	SIP IMEI
SIP Last Dest IP	SIP Session Start Time	SIP Session End Time
SIP Session Duration	SIP Retransmission Count	SIP Country
SIP IMSI	SIP B IMPI	SIP Alert Info
SIP C-MSISDN	SIP Feature Tags	SIP Termination Code BYE
SIP Termination Phrase BYE	SIP Termination Code CANCEL	SIP Termination Phrase CANCEL
SIP Warning Header	SIP Signing Duration	SIP Verification Duration
SIP X-CallGuardian-ucat	SIP Identity Attest	SIP A Cellular Network Info
SIP B Cellular Network Info	SIP Last A Cellular Network Info	SIP Last B Cellular Network Info
SIP History-Info User	SIP P-Served-User	SIP Access Type
SIP MCC	SIP MNC	SIP CI
SIP ECI	SIP NCI	SIP LAC
SIP SAC	SIP TAC	SIP P-Charging-Vector orig-ioi
SIP P-Charging-Vector Related ICID	SIP UUID	SIP Last Source IP
SIP P-Associated-URI User	SIP P-Preferred-Identity User	SIP ALG
SIP EALG	SIP Offered ALG	SIP Offered EALG
SIP Emergency Call	SIP Routing Number	SIP Request URI
SIP P-Visited-Network-ID	SIP INVITE Type	SIP Priority
SIP Privacy		

Table 84: SIP parameters in Call Trace (Continued)

15.2.75 SMPP

In Call Trace, the following parameters for SMPP are currently available:

SMPP Source Address	SMPP Source NPI	SMPP Source Type of Number
SMPP Source Bearer Type	SMPP Source Network Type	SMPP Destination Address
SMPP Destination NPI	SMPP Destination Type of Number	SMPP Destination Bearer Type
SMPP Destination Network Type	SMPP Network Error Code	SMPP SMSC System ID
SMPP Message Type	SMPP Source IMSI	SMPP Destination IMSI
SMPP Bind TON	SMPP Bind NPI	SMPP Address Range
SMPP SM Length	SMPP Message ID	SMPP Data Coding
SMPP Command Status	SMPP Message State	SMPP Sequence Number

Table 85: SMPP parameters in Call Trace

15.2.76 SMS

In Call Trace, the following parameters for SMS are currently available:

SMS Dest Address	SMS Message Type	SMS TP Cause
SMS Orig Address	SMS CP Cause	SMS Text length
SMS Recipient Address	SMS RP Cause	SMS Protocol Identifier
SMS Data Coding Scheme		

Table 86: SMS parameters in Call Trace

15.2.77 SMTP

In Call Trace, the following parameters for SMTP are currently available:

SMTP From	SMTP To

Table 87: SMTP parameters in Call Trace

15.2.78 TCAP

In Call Trace, the following parameters for TCAP are currently available:

TCAP OTID/TID	TCAP DTID	TCAP Error Code
TCAP OP Code	TCAP Application Context Name	TCAP Return Error Problem

Table 88: TCAP parameters in Call Trace

15.2.79 TCAP/INAP

In Call Trace, the following parameters for TCAP are currently available:

TCAP/INAP Called Number	TCAP/INAP Calling Number	TCAP/INAP Correlation Id
TCAP/INAP Dest Route Address	TCAP/INAP Service Key	TCAP/INAP Called BCD Number
TCAP/INAP Event Type	TCAP/INAP Event Details	TCAP/INAP Redirecting Reason
TCAP/INAP IMSI	TCAP/INAP MSISDN	TCAP/INAP APN
TCAP/INAP CI	TCAP/INAP LAC	TCAP/INAP Additional Calling Number
TCAP/INAP Destination Reference ID	TCAP/INAP Origination Reference ID	TCAP/INAP Assisting SSPIP Routing Address
TCAP/INAP Called NOA	TCAP/INAP Calling NOA	TCAP/INAP MCC
TCAP/INAP MNC	TCAP/INAP Abort Cause	TCAP/INAP Abort Cause Type
TCAP/INAP Number of Connects	TCAP/INAP Message ID	TCAP/INAP Location Number
TCAP/INAP Event Type 0	TCAP/INAP Event Type 24	

Table 89: TCAP/INAP parameters in Call Trace

15.2.80 TCAP/IS-41

In Call Trace, the following parameters for IS-41 are currently available:

TCAP/IS-41 IMSI Number	TCAP/IS-41 Billing ID	TCAP/IS-41 Transaction Capability
TCAP/IS-41 Destination Address	TCAP/IS-41 MIN	TCAP/IS-41 SMS Original Originating Address

Table 90: TCAP/IS-41 parameters in Call Trace

TCAP/IS-41 SMS Original Destination Address	TCAP/IS-41 Mobile Directory Number	TCAP/IS-41 Routing Digits
TCAP/IS-41 ESN	TCAP/IS-41 TLDN	

Table 90: TCAP/IS-41 parameters in Call Trace (Continued)

15.2.81 TCAP/MAP

In Call Trace, the following parameters for MAP are currently available:

TCAP/MAP IMSI Number	TCAP/MAP TMSI Number	TCAP/MAP NRI
TCAP/MAP IMEI Number	TCAP/MAP HLR Number	TCAP/MAP VLR Number
TCAP/MAP MSC Number	TCAP/MAP MSISDN Number	TCAP/MAP Roaming Number
TCAP/MAP Handover Number	TCAP/MAP Target Cell Identity	TCAP/MAP Forwarding Reason
TCAP/MAP Target LAC	TCAP/MAP Service Centre Address	TCAP/MAP USSD String
TCAP/MAP USSD String length	TCAP/MAP Dialogue Abort Cause	TCAP/MAP Forwarded To Number
TCAP/MAP GSN Address	TCAP/MAP GSN Number	TCAP/MAP Supported Camel Phase (Oldest)
TCAP/MAP SM Delivery Failure Cause	TCAP/MAP Equipment Status	

Table 91: TCAP/MAP parameters in Call Trace

15.2.82 TUP France

In Call Trace, the following parameters for TUP France are currently available:

TUP Msg	TUP A Number
TUP CIC	TUP B Number

Table 92: TUP ITU parameters in Call Trace

15.2.83 USSD

In Call Trace, the following parameters for USSD are currently available:

USSD String	USSD String length

Table 93: USSD parameters in Call Trace

15.2.84 WAP

In Call Trace, the following parameters for WAP are currently available:

WAP URI	WAP Cause

Table 94: WAP parameters in Call Trace

15.2.85 X2AP

In Call Trace, the following parameters for X2AP are currently available:

X2AP UE X2AP ID

Table 95: X2AP parameters in Call Trace

15.2.86 XCAP

In Call Trace, the following parameters for XCAP are currently available:

XCAP A Number	XCAP IMSI

Table 96: X2AP parameters in Call Trace

15.3 Protocol Analyser

The protocol parameters listed are available for searching in Protocol Analyser.

15.3.1 General

In Protocol Analyser, the following General parameters are currently available:

Row Nr	Link Name	Link Identifier
Date	Time	Protocol
Decode Error	Traffic group	Transaction ID
Msg Size	Direction	Message flags
Routing Group	PRS ID	PRS IP
Message Source	Capture ID	HEP3 Correlation ID

Table 97: General parameters in Protocol Analyser

15.3.2 5GC

In Protocol Analyser, the following parameters for 5GC are currently available:

5GC Service	5GC Service Operation	5GC N2 Info
5GC Cause	5GC Title	5GC IMSI
5GC IMEI(SV)	5GC MSISDN	5GC RAT
5GC MCC	5GC MNC	5GC TAC
5GC NCI	5GC ECI	5GC AMF Region
5GC AMF Set	5GC AMF Pointer	5GC DNN
5GC S-NSSAI SST	5GC S-NSSAI SD	5GC PDU Session Type
5GC PDU Session ID	5GC 5QI	5GC EPS Interworking Indication
5GC UE IPv4 address	5GC HO State	5GC EIR Status
5GC NF Instance ID	5GC FQDN	5GC NF Type
5GC NF	5GC 3gpp-sbi-target-apiroot	5GC next-hop-authority
5GC Session AMBR DL (Mbps)	5GC Session AMBR UL (Mbps)	5GC Charging Characteristics
5GC Rating Group	5GC Used Total Volume	5GC Used Uplink Volume
5GC Used Downlink Volume	5GC Result Code	

Table 98: 5GC parameters in Protocol Analyser

15.3.3 5G NAS

In Protocol Analyser, the following parameters for 5G NAS are currently available:

5GMM Msg	5GMM Registration Type	5GMM Type of Security Context
5GMM KSI	5GMM IMEISV	5GMM IMSI
5GMM 5G-TMSI	5GMM Additional 5G-TMSI	5GMM TAC
5GMM Cause	5GMM PDU Session Status	5GMM Deciphered
5GMM Integrity Algorithm	5GMM Ciphering Algorithm	5GMM SUCI MCC
5GMM SUCI MNC	5GMM NSSAI Requested	5GMM NSSAI Allowed
5GMM NSSAI Rejected	5GSM Msg	5GSM Cause
5GSM DNN	5GSM S-NSSAI SST	5GSM S-NSSAI SD

Table 99: 5G NAS parameters in Protocol Analyser

5GSM SSC Mode	5GSM Session AMBR DL (Mbps)	5GS NAS MM Msg
5GS NAS MM Registration type	5GS NAS MM Type of Security Context	5GS NAS MM KSI
5GS NAS MM IMSI	5GS NAS SM SSC Mode	5GS NAS MM IMEISV
5GS NAS UE Policy Msg Type	5GS NAS UE Policy UPSC Indicated	5GS NAS UE Policy UPSC Added/Updated
5GS NAS UE Policy Removed		

Table 99: 5G NAS parameters in Protocol Analyser (Continued)

15.3.4 AggData

In Protocol Analyser, the following parameters for AggData are currently available:

AggData Protocol type	AggData User Data Bytes	AggData User Data Msgs
AggData Source IP	AggData Dest IP	AggData Tunneled Source IP
AggData Tunneled Source Port	AggData Tunneled Dest IP	AggData Tunneled Dest Port
AggData Tid/Teid	AggData HTTP Url	AggData HTTP Host
AggData HTTP Cause	AggData HTTP Referer	AggData HTTP User Agent
AggData HTTP Get Messages	AggData DNS Query Name	AggData DNS Response Code
AggData DNS IP address	AggData MMS Message Type	AggData MMS From
AggData MMS To	AggData MMS User Agent	AggData MMS Response Status
AggData MMS Message Size	AggData MMS Content Type	AggData RTSP Content Type
AggData RTSP Url	AggData RTSP User Agent	AggData RTSP Status
AggData FTP User Name	AggData FTP request First Error Reason	AggData FTP Files Uploaded
AggData FTP Files Downloaded	AggData IMAP User Name	AggData IMAP Mail Count
AggData IMAP First Failed Command	AggData SMTP User Name	AggData SMTP From Address
AggData SMTP To Address	AggData POP3 User Name	AggData POP3 Mail Count
AggData Tlli	AggData Bvci	AggData Dlci
AggData Stack	AggData Application	

Table 100: AggData parameters in Protocol Analyser

15.3.5 AggMSRP

In Protocol Analyser, the following parameters for AggMSRP are currently available:

AggMSRP Source IP	AggMSRP Destination IP	AggMSRP Source Port
AggMSRP Destination Port	AggMSRP Start Time	AggMSRP End Time
AggMSRP Packet Count	AggMSRP Byte Count	AggMSRP Transaction ID
AggMSRP To Path	AggMSRP From Path	AggMSRP Message ID
AggMSRP Byte Range	AggMSRP Content Type	AggMSRP Message Type
AggMSRP Response Code		

Table 101: AggMSRP parameters in Protocol Analyser

15.3.6 AggRTP - Codec Metrics

In Protocol Analyser, the following parameters for AggRTP - Codec Metrics are currently available:

AggRTP Vocoder Type

Table 102: AggRTP - Codec Metrics parameters in Protocol Analyser

15.3.7 AggRTP - Degradation Metrics

In Protocol Analyser, the following parameters for AggRTP - Degradation Metrics are currently available:

AggRTP Loss Degr.	AggRTP Discard Degr.	AggRTP CODEC Degr.
AggRTP Delay Degr.	AggRTP Signal Level Degr.	AggRTP Noise Level Degr.
AggRTP Echo Level Degr.	AggRTP Recency Degr.	

Table 103: AggRTP - Degradation Metrics parameters in Protocol Analyser

15.3.8 AggRTP - Delay Record

In Protocol Analyser, the following parameters for AggRTP - Delay Record are currently available:

AggRTP Avg. Round-trip Network Delay (ms)	AggRTP Avg. One-way Delay (ms)
AggRTP Max. Round-trip Network Delay (ms)	AggRTP Max. One-way Delay (ms)

Table 104: AggRTP - Delay Record parameters in Protocol Analyser

15.3.9 AggRTP - DTMF Record

In Protocol Analyser, the following parameters for AggRTP - DTMF Record are currently available:

AggRTP DTMF Packets Out Of Order	AggRTP DTMF Packets Lost	AggRTP DTMF Events Discarded
AggRTP DTMF Very Low Volume	AggRTP DTMF Very High Volume	AggRTP DTMF High Quality Sequence
AggRTP DTMF Digits		

Table 105: AggRTP - DTMF Record parameters in Protocol Analyser

15.3.10 AggRTP - End Point Descriptor

In Protocol Analyser, the following parameters for AggRTP - End Point Descriptor are currently available:

AggRTP UDP Source Address	AggRTP UDP Dest Address	AggRTP VLAN ID
AggRTP UDP Source Port	AggRTP UDP Dest Port	

Table 106: AggRTP - End Point Descriptor parameters in Protocol Analyser

15.3.11 AggRTP - Gap 500 Delay Record

In Protocol Analyser, the following parameters for AggRTP - Gap 500 Delay Record are currently available:

AggRTP Gap 500 Delay (ms)

Table 107: AggRTP - Gap 500 Delay Record parameters in Protocol Analyser

15.3.12 AggRTP - Jitter Records (RFC 3550)

In Protocol Analyser, the following parameters for AggRTP - Jitter Records are currently available:

AggRTP Max. PPDV (ms)	AggRTP Avg. PPDV (ms)

Table 108: AggRTP - Jitter Records parameters in Protocol Analyser

15.3.13 AggRTP - Packet Transport Record

In Protocol Analyser, the following parameters for AggRTP - Packet Transport Record are currently available:

AggRTP Packets Received	AggRTP Packets Discarded	AggRTP Avg. Packet Loss (%)
AggRTP Packets Lost	AggRTP Packets Duplicated	

Table 109: AggRTP - Packet Transport Record parameters in Protocol Analyser

15.3.14 AggRTP - Quality Records (G. 107)

In Protocol Analyser, the following parameters for AggRTP - Quality Records (G. 107) are currently available:

AggRTP R-LQ	AggRTP MOS-LQ	AggRTP R-G107
AggRTP R-CQ	AggRTP MOS-CQ	

Table 110: AggRTP - Quality Records(G. 107) parameters in Protocol Analyser

15.3.15 AggRTP - RTCP - Delay Record

In Protocol Analyser, the following parameters for AggRTP - Delay Record are currently available:

AggRTP RTCP Avg. Round-trip Network Delay (ms)	AggRTP RTCP Max. Round-trip Network Delay (ms)	AggRTP RTCP Avg. One-way Delay (ms)
AggRTP RTCP Max. One-way Delay (ms)		

Table 111: AggRTP - Delay Record parameters in Protocol Analyser

15.3.16 AggRTP - RTCP - End System Delay Record

In Protocol Analyser, the following parameters for AggRTP - End System Delay Record are currently available:

AggRTP RTCP Avg. Orig. End-System Delay (ms)	AggRTP RTCP Max. Orig. End-System Delay (ms)	AggRTP RTCP Avg. Term. End-System Delay (ms)
AggRTP RTCP Max. Term. End-System Delay (ms)		

Table 112: AggRTP - End System Delay Record parameters in Protocol Analyser

15.3.17 AggRTP - RTCP-RR Record

In Protocol Analyser, the following parameters for AggRTP - RTCP-RR Record are currently available:

AggRTP RTCP-RR Packets Lost	AggRTP RTCP-RR DLSR	AggRTP RTCP-RR Inter Arrival Jitter

Table 113: AggRTP - RTCP-RR Record parameters in Protocol Analyser

15.3.18 AggRTP - RTCP-SR Record

In Protocol Analyser, the following parameters for AggRTP - RTCP-SR Record are currently available:

AggRTP RTCP-SR # of RTP Packets	AggRTP RTCP-SR # of RR Reports	AggRTP RTCP-SR # of Octets

Table 114: AggRTP - RTCP-SR Record parameters in Protocol Analyser

15.3.19 AggRTP - RTCP SS/RR-based QoE Metrics

In Protocol Analyser, the following parameters for AggRTP - RTCP SS/RR-based QoE Metrics are currently available:

AggRTP RTCP-SR/RR MOS-LQ	AggRTP RTCP-SR/RR MOS-CQ

Table 115: AggRTP - RTCP SS/RR-based QoE Metrics parameters in Protocol Analyser

15.3.20 AggRTP - RTCP-XR Record

In Protocol Analyser, the following parameters for AggRTP - RTCP-XR Record are currently available:

AggRTP RTCP-XR Loss Rate (%)	AggRTP RTCP-XR Discard Rate (%)	AggRTP RTCP-XR Avg Burst Density (%)
AggRTP RTCP-XR Avg Gap Density (%)	AggRTP RTCP-XR Avg Burst Duration (ms)	AggRTP RTCP-XR Avg Gap Duration (ms)
AggRTP RTCP-XR RT Delay (ms)	AggRTP RTCP-XR End Sys. Delay (ms)	AggRTP RTCP-XR Signal lvl. (dBm)
AggRTP RTCP-XR Noise lvl (dBm)	AggRTP RTCP-XR Residual ERL (dB)	AggRTP RTCP-XR Gap Size (# of packets)
AggRTP RTCP-XR R-factor	AggRTP RTCP-XR Ext. R-factor	AggRTP RTCP-XR MOS-LQ
AggRTP RTCP-XR MOS-CQ	AggRTP RTCP-XR RX Config	

Table 116: AggRTP - RTCP-XR Record parameters in Protocol Analyser

15.3.21 AggRTP - Voice Jitter Records (G. 1020)

In Protocol Analyser, the following parameters for AggRTP - Voice Jitter Records (G. 1020) are currently available:

AggRTP Avg. MAPDV (ms)	AggRTP Max. MAPDV (ms)

Table 117: AggRTP - Voice Jitter Records (G. 1020) parameters in Protocol Analyser

15.3.22 AIN

In Protocol Analyser, the following parameters for AIN are currently available:

AIN Calling Number	AIN Called Number	AIN Routing Number

Table 118: AIN parameters in Protocol Analyser

15.3.23 ALCAP

In Protocol Analyser, the following parameters for ALCAP are currently available:

ALCAP Msg	ALCAP Dest SAI	ALCAP CID
ALCAP Cause	ALCAP SUGR	
ALCAP Orig SAI	ALCAP Aal2 Path Id	

Table 119: ALCAP parameters in Protocol Analyser

15.3.24 ATM

In Protocol Analyser, the following parameters for ATM are currently available:

ATM Path ID	ATM VCI	ATM CID
ATM VPI		

Table 120: ATM parameters in Protocol Analyser

15.3.25 BSSAP

In Protocol Analyser, the following parameters for BSSAP are currently available:

BSSAP Layer 3 Msg	BSSAP PDU	BSSAP SAPI
BSSAP BSSMAP Cause	BSSAP Assignment Failure Cause	BSSAP Handover Failure Cause
BSSAP Handover Required Reject Cause	BSSAP Handover Required Cause	BSSAP BSSMAP Transport Layer Address
BSSAP RR Cause	BSSAP LCS Cause	BSSAP RetErr Cause
BSSAP MCC	BSSAP MNC	BSSAP LAC
BSSAP CI	BSSAP DTAP PD	BSSAP CIC
BSSAP Called NPI	BSSAP Called TON	BSSAP Called Num
BSSAP Calling NPI	BSSAP Calling TON	BSSAP Calling Num
BSSAP Connected NPI	BSSAP Connected TON	BSSAP Connected Num
BSSAP Redir NPI	BSSAP Redir TON	BSSAP Redir Num
BSSAP DTAP CC Cause	BSSAP SS Cause type	BSSAP SS Cause
BSSAP SS Error	BSSAP SS Comp	BSSAP SS Oper
BSSAP SS Problem type	BSSAP SS Problem code	BSSAP MSISDN to IMSI
BSSAP Algorithm Identifier		

Table 121: BSSAP parameters in Protocol Analyser

15.3.26 BSSAP+

In Protocol Analyser, the following parameters for BSSAP+ are currently available:

BSSAP+ Msg	BSSAP+ IMSI	BSSAP+ SGSN Number
BSSAP+ IMSI Detach GPRS	BSSAP+ IMSI Detach Non GPRS	BSSAP+ Gs Cause
BSSAP+ Information Requested	BSSAP+ MS state	BSSAP+ Reject Cause
BSSAP+ Cell Global ID LAC	BSSAP+ Cell Global ID RAC	BSSAP+ LAI LAC
BSSAP+ TMSI	BSSAP+ NRI	

Table 122: BSSAP+ parameters in Protocol Analyser

15.3.27 Circuit - ISUP

In Protocol Analyser, the following parameters for ISUP are currently available:

ISUP Msg	ISUP CIC	ISUP A Nr
ISUP SAM Number	ISUP B Nr	ISUP Cause Value
ISUP Location Nr	ISUP Redirecting Nr	ISUP Original Called Nr
ISUP Generic Number	ISUP A NoA	ISUP B NoA
ISUP Grs/Gra Range	ISUP Charge Indicator	ISUP OPC CIC
ISUP DPC CIC	ISUP TMR	ISUP Route Identity

Table 123: ISUP parameters in Protocol Analyser

ISUP Redirection Reason	ISUP Call Identity	ISUP Network Exchange Identity
ISUP Cause Location	ISUP Correlation id	

Table 123: ISUP parameters in Protocol Analyser (Continued)

15.3.28 Circuit - IUP

In Protocol Analyser, the following parameters for IUP are currently available:

IUP CIC	IUP H0	IUP H1
IUP Called Nbr	IUP Calling Nbr	IUP Line ID
IUP Reason	IUP Line Id Type	IUP Line Id NAI
IUP Calling NAI	IUP Full Calling Line ID	IUP Full Calling NAI
IUP CNA Reason		

Table 124: IUP parameters in Protocol Analyser

15.3.29 Circuit - BICC

In Protocol Analyser, the following parameters for BICC are currently available:

BICC Msg	BICC CIC	BICC A Nr
BICC SAM Number	BICC B Nr	BICC Cause Value
BICC Location Nr	BICC Redirecting Nr	BICC Original Called Nr
BICC A NoA	BICC B NoA	BICC Grs/Gra Range
BICC Charge Ind	BICC Action Indicator	BICC TMR
BICC Transport Layer Address	BICC Backbone Network Id	

Table 125: BICC parameters in Protocol Analyser

15.3.30 Cisco Session Management

In Protocol Analyser, the following parameters for Cisco Session Management are currently available:

Cisco Session Management SM Message Type
Cisco Session Management Message Type

Table 126: Cisco Session Management parameters in Protocol Analyser

15.3.31 DHCP

In Protocol Analyser, the following parameters for DHCP are currently available:

DHCP Bootp Msg	DHCP Transaction ID	DHCP Client MAC
DHCP Hardware Address Type	DHCP Broadcast Flag	DHCP Client IP
DHCP Your IP	DHCP Relay agent IP	DHCP Next Server
DHCP Msg	DHCP Subnet Mask	DHCP Host Name
DHCP Domain Name	DHCP Lease Time	DHCP Server ID
DHCP Renewal Time	DHCP Rebinding Time	DHCP Vendor Class ID
DHCP Client ID	DHCP First Router Address	DHCP First DNS Address
DHCP Relay Agent Info Type	DHCP Relay Agent Circuit ID	DHCP Relay Agent Remote ID
DHCP Relay Agent Subscriber ID	DHCP First Classless Static Route	

Table 127: DHCP parameters in Protocol Analyser

15.3.32 DIAMETER

In Protocol Analyser, the following parameters for DIAMETER are currently available:

DIAMETER Command Type	DIAMETER Command Code	DIAMETER Application Id
DIAMETER Hop By Hop	DIAMETER End To End	DIAMETER Origin Host
DIAMETER Origin Realm	DIAMETER Destination Host	DIAMETER Destination Realm
DIAMETER Session Id	DIAMETER IMSI	DIAMETER MSISDN Number
DIAMETER CC Request Type	DIAMETER CC Request Number	DIAMETER Calling party address
DIAMETER Called party address	DIAMETER Public Identity	DIAMETER Reporting Reason
DIAMETER Multiple Services CC Result	DIAMETER Multiple Services CC Service Id	DIAMETER Multiple Services CC Rating group
DIAMETER Used Input Octets	DIAMETER Used Output Octets	DIAMETER Used Total Octets
DIAMETER Trigger Type	DIAMETER Framed IP	DIAMETER Called Station
DIAMETER SGSN IP	DIAMETER GGSN IP	DIAMETER Last Hop Dest IP
DIAMETER Charging Characteristics	DIAMETER Radio Access Type 2G/3G	DIAMETER ICID
DIAMETER User Name	DIAMETER Accounting Record Type	DIAMETER SIP Method
DIAMETER Cause Code	DIAMETER Result Code	DIAMETER Experimental result code
DIAMETER SGSN MCC	DIAMETER SGSN MNC	DIAMETER Charging rule name
DIAMETER Charging rule base name	DIAMETER Event trigger	DIAMETER Priority level
DIAMETER Preemption capability	DIAMETER Preemption vulnerability	DIAMETER Disconnect cause
DIAMETER MCC	DIAMETER MNC	DIAMETER LAC
DIAMETER SAC/CI	DIAMETER IMEI(SV)	DIAMETER Framed IPv6 prefix
DIAMETER QCI	DIAMETER Subscription Id	DIAMETER Subscription Type
DIAMETER Server Assignment Type	DIAMETER User Authorization Type	DIAMETER User Data Already Available
DIAMETER UE SRVCC Capability	DIAMETER ECI	DIAMETER Service selection
DIAMETER Data Reference	DIAMETER IPCAN Type	DIAMETER NIDD Used
DIAMETER NIDD Delivery	DIAMETER PDN Continuity	DIAMETER Operation Mode
DIAMETER 5GS Interworking	DIAMETER DRMP	DIAMETER NBIFOM
DIAMETER eDRX RAT	DIAMETER Additional APN	DIAMETER SCEF Realm
DIAMETER eDRX Cycle	DIAMETER Paging Window	DIAMETER UE Usage Type
DIAMETER ULR Flags	DIAMETER Access Restriction Data	DIAMETER Subscription Data Flags
DIAMETER Preferred Data Mode	DIAMETER V2X Permission	DIAMETER Core Network Restrictions
DIAMETER Ext Max Requested BW DL (kbps)	DIAMETER Ext Max Requested BW UL (kbps)	DIAMETER Ext APN AMBR DL (kbps)

Table 128: DIAMETER parameters in Protocol Analyser

DIAMETER Ext APN AMBR UL (kbps)	DIAMETER Ext GBR DL (kbps)	DIAMETER Ext GBR UL (kbps)
DIAMETER Service selection	DIAMETER 2nd RAT	DIAMETER Abort Cause
DIAMETER Termination cause	DIAMETER Ext BW NR	DIAMETER V2X Allowed
DIAMETER Visited NW Identifier	DIAMETER TAC	DIAMETER Equipment Status
DIAMETER RFSP		

Table 128: DIAMETER parameters in Protocol Analyser (Continued)

15.3.33 DNS

In Protocol Analyser, the following parameters for DNS are currently available:

DNS ID	DNS Message	DNS Opcode
DNS Query Name	DNS Qtype	DNS Qclass
DNS Response Code	DNS Answer Address	DNS Answer Count
DNS Answer Result	DNS Called Number	DNS Enum Service Address

Table 129: DNS parameters in Protocol Analyser

15.3.34 EMI

In Protocol Analyser, the following parameters for EMI are currently available:

EMI Operation Type	EMI O/R	EMI TRN
EMI Response Type	EMI Error Code	EMI Source Address
EMI Destination Address	EMI PID	EMI Message Type
EMI DCS		

Table 130: EMI parameters in Protocol Analyser

15.3.35 EMPP

In Protocol Analyser, the following parameters for EMPP are currently available:

EMPP Method	EMPP Response Status	EMPP CSeq
EMPP Message Type	EMPP A Number	EMPP B Number
EMPP Source IMSI	EMPP Destination IMSI	EMPP Charge IMSI
EMPP Charge MSISDN	EMPP Operation Result	

Table 131: EMPP parameters in Protocol Analyser

15.3.36 ESP (IP Encapsulating Security Payload)

In Protocol Analyser, the following parameters for ESP are currently available:

Security Parameters Index (SPI)	Sequence Number

Table 132: ESP parameters in Protocol Analyser

15.3.37 Ethernet

In Protocol Analyser, the following parameters for Ethernet are currently available:

VLAN Priority	VLAN CFI	VLAN ID
Ethernet Source Mac Address	Ethernet Dest Mac Address	

Table 133: Ethernet parameters in Protocol Analyser

15.3.38 GPRS Gb

In Protocol Analyser, the following parameters for GPRS Gb are currently available:

Frame Relay DLCI	NS PDU	NS BVCI
NS Cause	BSSGP PDU	BSSGP BVCI
BSSGP Cause	BSSGP Radio Cause	BSSGP IMSI
BSSGP MCC	BSSGP MNC	BSSGP LAC
BSSGP RAC	BSSGP CI	BSSGP TLLI
BSSGP TMSI	BSSGP NRI	LLC PD
LLC SAPI	LLC LFN	SNDCP More Segments
SNDCP Segment Number	SNDCP First Segment	SNDCP PDU type
SNDCP NPDU	SNDCP DCOMP	SNDCP PCOMP

Table 134: GPRS GB parameters in Protocol Analyser

15.3.39 GRE

In Protocol Analyser, the following parameters for GRE are currently available:

GRE Version	GRE Payload size	GRE Seq Number
GRE Protocol Type	GRE Call Id	GRE Ack Number

Table 135: GRE parameters in Protocol Analyser

15.3.40 GTP

In Protocol Analyser, the following parameters for GTP are currently available:

GTP Message	GTP Version	GTP IMSI
GTP MSISDN	GTP End User Address	GTP End User Address IPv6
GTP APN	GTP Cause	GTP Request Cause
GTP TEID	GTP TEID Data 1	GTP TEID Control Plane
GTP F-TEID	GTP Sequence Number	
GTP IMEI(SV)	GTP RADIO MCC	GTP RADIO MNC
GTP RADIO LAC	GTP CORE MCC	GTP CORE MNC
GTP CORE LAC	GTP TAC	GTP DTI
GTP NSAPI	GTP EBI	GTP RAN address for user traffic
GTP RAC	GTP SAC	GTP CI
GTP ECI	GTP Radio Access Technology	GTP STN-SR Address
GTP Sv MME CP Address	GTP Sv MSC CP Address	GTP RNC Id
GTP Target CI	GTP SRVCC Cause	GTP PDP/PDN Type
GTP DL MBR	GTP DL GBR	GTP UL MBR
GTP UL GBR	GTP Mapped UE UT	GTP Serving PLMN UL Rate Limit
GTP Serving PLMN DL Rate Limit	GTP CIoT Optimizations Support	GTP Indication Flags
GTP Dual Connectivity NR	GTP MME Code	GTP QCI
GTP Priority Level	GTP Recovery Restart Counter	GTP 2nd RAT Report
GTP 2nd RAT usage data DL	GTP 2nd RAT usage data UL	

Table 136: GTP parameters in Protocol Analyser

15.3.41 H.323

In Protocol Analyser, the following parameters for H.323 are currently available:

H.323 Message Type	H.323 Display	H.323 Calling Party Number
H.323 Called Party Number	H.323 Calling Type of Number	H.323 Called Type of Number
H.323 Cause Value	H.323 RAS Msg	H.323 Req Seq Number
H.323 Source Address Number	H.323 Source Address Text	H.323 Destination Address Number
H.323 Destination Address Text	H.323 Call Identifier GUID	H.323 H245 Message Type

Table 137: H.323 parameters in Protocol Analyser

15.3.42 HTTP

In Protocol Analyser, the following parameters for HTTP are currently available:

HTTP Method	HTTP Status Code	HTTP Reason Phrase
HTTP Request URI	HTTP Host	HTTP Content Length
HTTP Location	HTTP User Agent	HTTP Via

Table 138: HTTP parameters in Protocol Analyser

15.3.43 HTTP - HTTP/2

In Protocol Analyser, the following parameters for HTTP - HTTP/2 are currently available:

HTTP - HTTP/2 Stream Identifier	HTTP - HTTP/2 Header Lookup Status	HTTP - HTTP/2 Source Socket Address
HTTP - HTTP/2 Dest Socket Address	HTTP - HTTP/2 Frame Type	

Table 139: HTTP - HTTP/2 parameters in Protocol Analyser

15.3.44 ICMP

In Protocol Analyser, the following parameters for ICMP are currently available:

ICMP Msg Type	ICMP Identifier	ICMP Transport Src Port
ICMP Code	ICMP Seq Number	ICMP Transport Dest Port

Table 140: ICMP parameters in Protocol Analyser

15.3.45 IMF

In Protocol Analyser, the following parameters for IMF are currently available:

IMF Date	IMF From	IMF Sender
IMF To	IMF Cc	IMF Bcc
IMF Message ID		

Table 141: IMF parameters in Protocol Analyser

15.3.46 IP

In Protocol Analyser, the following parameters for IP are currently available:

IP Source Address	IP Dest Address	IP Protocol
IP Tunnel Source Address	IP Tunnel Dest Address	IP Tunnel Protocol

Table 142: IP parameters in Protocol Analyser

15.3.47 ISAMKMP

In Protocol Analyser, the following parameters for ISAKMP are currently available:

Initiator SPI	Responder SPI	Exchange Type
Message ID		

Table 143:

15.3.48 ISDN

In Protocol Analyser, the following parameters for ISDN are currently available:

LAPD N(S)	LAPD N(R)	LAPD SAPI
LAPD Msg	ISDN Protocol Discriminator	ISDN Call Reference
ISDN CR Flag	ISDN Message Type	ISDN Called Party Number
ISDN Calling Party Number	ISDN Display	ISDN Called TypeOfNum
ISDN Calling TypeOfNum	ISDN Cause Value	ISDN Channel number
ISDN Information transfer capability	ISDN High Layer Characteristics	ISDN Transfer Mode
ISDN Userinfo Layer1 Protocol	ISDN Location	

Table 144: ISDN parameters in Protocol Analyser

15.3.49 ISDN SS

In Protocol Analyser, the following parameters for ISDN SS are currently available:

ISDN SS Called Number	ISDN SS Calling Number

Table 145: ISDN SS parameters in Protocol Analyser

15.3.50 LCS-AP

In Protocol Analyser, the following parameters for LCS-AP are currently available:

LCS-AP Correlation ID	LCS-AP Procedure Code	LCS-AP Message Type Name
LCS-AP MNC	LCS-AP MCC	LCS-AP Cell Identity
LCS-AP LCS Cause	LCS-AP eNB ID	LCS-AP Sector ID
LCS-AP IMSI		

Table 146: LCS-AP parameters in Protocol Analyser

15.3.51 LDAP

In Protocol Analyser, the following parameters for LDAP are currently available:

LDAP Msg	LDAP Msg ID	LDAP IMSI
LDAP MSISDN	LDAP SGSN Number	LDAP SGSN Address
LDAP VLR Number	LDAP MSC Number	LDAP Result Code.
LDAP IMPI	LDAP IMPU	LDAP Assoc Id
LDAP Policy id	LDAP Market Code id	LDAP TOA Status
LDAP TOA Level	LDAP AV Status	LDAP PC Status
LDAP PC Week Schedule	LDAP DN dc	LDAP DN ou
LDAP DN cn	LDAP DN serv	LDAP DN mscId
LDAP DN Other Number		

Table 147: LDAP parameters in Protocol Analyser

15.3.52 LPPa

In Protocol Analyser, the following parameters for LPPa are currently available:

LPPa Procedure Code	LPPa Cell Portion ID	LPPa E-UTRAN Cell ID
LPPa Type of Message	LPPa MCC	LPPa TAC
LPPa Transaction ID	LPPa MNC	LPPa Cause
LPPa Msg		

Table 148: LPPa parameters in Protocol Analyser

15.3.53 MEGACO

In Protocol Analyser, the following parameters for MEGACO are currently available:

MEGACO Version	MEGACO Transaction	MEGACO Transaction Id
MEGACO Context Id	MEGACO Error Code	MEGACO Command
MEGACO Termination ID	MEGACO Transport Layer Address	MEGACO BIR SUGR
MEGACO Trace Id	MEGACO IMSI	MEGACO Observed Event
MEGACO Calling Number	MEGACO Mld	MEGACO Audio Dest Local
MEGACO Audio Dest Remote	MEGACO Stream Mode	MEGACO Signal Name

Table 149: MEGACO parameters in Protocol Analyser

15.3.54 MGCP

In Protocol Analyser, the following parameters for MGCP are currently available:

MGCP Verb	MGCP Response String	MGCP Observed Events
MGCP Transaction ID	MGCP Local Connection Options	MGCP Signal Requests
MGCP Endpoint Name	MGCP Connection Parameters	MGCP Caller ID
MGCP Response Code	MGCP Call Id	

Table 150: MGCP parameters in Protocol Analyser

15.3.55 MM/SM

In Protocol Analyser, the following parameters for MM/SM are currently available:

MM/SM Msg	MM/SM Security header type	MM/SM APN
MM/SM Mobile IP Address	MM/SM IMSI	MM/SM TMSI
MM/SM NRI	MM/SM M-TMSI	MM/SM IMEI
MM/SM IMEISV	MM/SM MCC	MM/SM MNC
MM/SM LAC	MM/SM RAC	MM/SM TAC
MM/SM CI	MM/SM MM Cause	MM/SM SM Cause
MM/SM Reject Cause	MM/SM CC Cause	MM/SM Protocol Discriminator
MM/SM CP Msg	MM/SM CP Cause	MM/SM RP Msg
MM/SM RP Cause	MM/SM Service Type	MM/SM Other Rate Adaption
MM/SM Ciphering Algorithm	MM/SM NSAPI	MM/SM MME Group Id
MM/SM MME Code	MM/SM Deciphered	MM/SM KSI
MM/SM QCI	MM/SM ESM Msg	MM/SM EPS PTI
MM/SM EBI	MM/SM Traffic Handling Priority	MM/SM Location Update Type

Table 151: MM/SM parameters in Protocol Analyser

MM/SM EPS Update Type	MM/SM Voice Domain Preference	MM/SM CSFB Indicator
MM/SM Integrity Algorithm	MM/SM GUTI Type	MM/SM P-TMSI Signature
MM/SM UE CP CIoT	MM/SM UE UP CIoT	MM/SM UE ER w/o PDN
MM/SM UE S1-U data	MM/SM UE HC-CP CIoT	MM/SM UE DCNR
MM/SM UE PNB-CIoT	MM/SM UE N1 mode	MM/SM NW CP CIoT
MM/SM NW UP CIoT	MM/SM NW ER w/o PDN	MM/SM NW S1-U data
MM/SM NW HC-CP CIoT	MM/SM NW Restrict DCNR	MM/SM Ext EMM cause EPS opt info
MM/SM Ext EMM cause NB-IoT allowed	MM/SM NW Control plane only indication	MM/SM T3412
MM/SM T3412 Extended	P-CSCF IPv6	MM/SM Type of security context
MM/SM EPC Capability		

Table 151: MM/SM parameters in Protocol Analyser (Continued)

15.3.56 MMS

In Protocol Analyser, the following parameters for MMS are currently available:

MMS Msg Type	MMS Transaction Id	MMS From
MMS Msg ID	MMS Response Status	MMS To
MMS A Number	MMS B Number	MMS Recipient Count

Table 152: MMS parameters in Protocol Analyser

15.3.57 MSRP

In Protocol Analyser, the following parameters for MSRP are currently available:

MSRP Transaction ID	MSRP To Dest	MSRP From Dest
MSRP Method	MSRP Status Code	MSRP Status Comment
MSRP Message ID	MSRP Byte Range	MSRP Content Type

Table 153: MSRP parameters in Protocol Analyser

15.3.58 MTP2

In Protocol Analyser, the following parameters for MTP2 are currently available:

MTP2 Msg	MTP2 Link Status

Table 154: MTP2 parameters in Protocol Analyser

15.3.59 MTP3/M3UA

In Protocol Analyser, the following parameters for MTP3/M3UA are currently available:

MTP3/M3UA SI	MTP3/M3UA OPC	MTP3/M3UA DPC
MTP3/M3UA OPC NI	MTP3/M3UA DPC NI	MTP3/M3UA NI
MTP3/M3UA SLS	MTP3/M3UA Msg	

Table 155: MTP3/M3UA parameters in Protocol Analyser

15.3.60 Multimedia

In Protocol Analyser, the following parameters for Multimedia are currently available:

Multimedia Control Msg

Table 156: Multimedia parameters in Protocol Analyser

15.3.61 NBAP

In Protocol Analyser, the following parameters for NBAP are currently available:

NBAP Msg	NBAP Message Name	NBAP Procedure Code
NBAP Transaction ID	NBAP UL Scrambling Code	NBAP DL Channel Code Number
NBAP CRNC Communication Context Id	NBAP NodeB Communication Context Id	NBAP Cell Id
NBAP Binding ID	NBAP Radio Link Id	NBAP Cause
NBAP DCH Port		

Table 157: NBAP parameters in Protocol Analyser

15.3.62 NGAP

In Protocol Analyser, the following parameters for NGAP are currently available:

NGAP Msg	NGAP Procedure Code	NGAP RAN UE ID
NGAP NSSAI Allowed	NGAP Cause	NGAP TAI MCC
NGAP TAI MNC	NGAP NR CGI MCC	NGAP NR CGI MNC
NGAP NR Cell Identity	NGAP TAC	NGAP S-NSSAI SST
NGAP S-NSSAI SD	NGAP 5QI	NGAP UE AMBR UL
NGAP UE AMBR DL	NGAP 5G-TMSI	NGAP AMF Region
NGAP AMF Set	NGAP AMF Pointer	NGAP PDU Session ID
NGAP PDU Session Type	NGAP AMF UE ID	NGAP Source AMF UE ID

Table 158: NGAP parameters in Protocol Analyser

15.3.63 PCAP

In Protocol Analyser, the following parameters for PCAP are currently available:

PCAP Transaction Id	PCAP Message Type Name	PCAP RNC ID
PCAP Procedure Code	PCAP Request Type Event	PCAP Cell ID
PCAP Message Type	PCAP Positioning Method	PCAP Cause

Table 159: PCAP parameters in Protocol Analyser

15.3.64 PFCP

In Protocol Analyser, the following parameters for PFCP are currently available:

PFCP Message	PFCP Sequence Number	PFCP SEID
PFCP F-SEID	PFCP Cause	PFCP UE IP Address
PFCP APN	PFCP URR ID	PFCP S-NSSAI SST
PFCP S-NSSAI SD		

Table 160: PFCP parameters in Protocol Analyser

15.3.65 PWS

In Protocol Analyser, the following parameters for PWS are currently available:

PWS Message Identifier	PWS Geographical Scope	PWS Message Code
PWS Update Number		

Table 161: PWS parameters in Protocol Analyser

15.3.66 QSAAL

In Protocol Analyser, the following parameters for QSAAL are currently available:

QSAAL SSCOP Msg	QSAAL N(MR)	QSAAL N(S)
QSAAL N(PS)	QSAAL N(R)	QSAAL N(SQ)

Table 162: QSAAL parameters in Protocol Analyser

15.3.67 RADIUS

In Protocol Analyser, the following parameters for RADIUS are currently available:

RADIUS Packet Type	RADIUS Identifier	RADIUS Length
RADIUS Accounting Session ID	RADIUS Accounting Status	RADIUS Framed IP Address
RADIUS Calling User	RADIUS Called User	RADIUS IMSI
RADIUS Accounting Input Octets	RADIUS Accounting Output Octets	

Table 163: RADIUS parameters in Protocol Analyser

15.3.68 RAN

In Protocol Analyser, the following parameters for RAN are currently available:

RAN Cell ID	RAN eNodeB ID	RAN Call ID
RAN MAC TA value	RAN C-RNTI	RAN Eutran Trace ID
RAN Huawei Msg Type ID	RAN Nokia Msg Type ID	RAN MAC Power Headroom
RAN MAC UL-SINR	RAN MAC Angle of Arrival	RAN MAC Radio Link Failure

Table 164: RAN parameters in Protocol Analyser

15.3.69 RANAP

In Protocol Analyser, the following parameters for RANAP are currently available:

RANAP Msg	RANAP Message Name	RANAP Procedure Code
RANAP PNAS IMSI	RANAP LAI LAC	RANAP SAI LAC
RANAP SAC	RANAP RAC	RANAP Transport Layer Address
RANAP Cause	RANAP Called Number	RANAP Calling Number
RANAP MCC	RANAP MNC	RANAP Binding ID
RANAP GTP TEI	RANAP Domain Indicator	RANAP TMSI
RANAP NRI	RANAP Reject Cause Value	RANAP Global RNC ID
RANAP Relocation Type	RANAP RNC ID	RANAP Cell ID
RANAP Target Cell ID	RANAP CN ID	

Table 165: RANAP parameters in Protocol Analyser

15.3.70 RNSAP

In Protocol Analyser, the following parameters for RNSAP are currently available:

RNSAP Msg	RNSAP Message Name	RNSAP UL Scrambling Code
RNSAP Binding ID	RNSAP Cell	RNSAP IMSI
RNSAP Logical Channel	RNSAP RNC	RNSAP IMEI
RNSAP LAC	RNSAP RAC	RNSAP SAC
RNSAP Procedure Code	RNSAP MCC	RNSAP MNC
RNSAP ARP	RNSAP RL	

Table 166: RNSAP parameters in Protocol Analyser

15.3.71 RRC

In Protocol Analyser, the following parameters for RRC are currently available:

RRC Largest Container Size	3G RRC Message Type	3G RRC TMSI
3G RRC P-TMSI	3G RRC NRI	3G RRC IMSI
3G RRC Establishment Cause	3G RRC UL Scrambling Code	3G RRC DL Channel Code
3G RRC Event Result	3G RRC Primary Scrambling Code	3G RRC U-RNTI
3G RRC LAC	3G RRC Cell ID	3G RRC SRCN-ITY
3G RRC S-RNTI	4G RRC Message Type	4G RRC M-TMSI
4G RRC MME Code	4G RRC EUTRA freq	4G RRC EN-DC freq
4G RRC NR-SA freq	4G RRC Feature Group Ind	4G RRC 4x4 MIMO
4G RRC locationInfo	4G RRC Establishment Cause	4G RRC New C-RNTI
4G RRC Release Clause	4G RRC MDT Mode	4G RRC MDT Type
4G RRC #MR Immediate	4G RRC #MR Logged	4G RRC RSRP Max Logged
4G RRC RSRP Min Logged	4G RRC RSRP Avg Logged	4G RRC RSRQ Max Logged
4G RRC RSRQ Min Logged	4G RRC RSRQ Avg Logged	4G RRC RSRQ Immediate
4G RRC RSRP Immediate	4G RRC Reestablishment Cause	5G RRC EUTRA freq
5G RRC NR freq		

Table 167: RRC parameters in Protocol Analyser

15.3.72 RTCP

In Protocol Analyser, the following parameters for RTCP are currently available:

RTCP Packet Type

Table 168: RTCP parameters in Protocol Analyser

15.3.73 RTP

In Protocol Analyser, the following parameters for RTP are currently available:

RTP Payload Type	RTP Seq	RTP Timestamp
RTP SSRC		

Table 169: RTP parameters in Protocol Analyser

15.3.74 RTSP

In Protocol Analyser, the following parameters for RTSP are currently available:

RTSP Method	RTSP Session Id	RTSP User Agent
RTSP Status Code	RTSP Url	RTSP Server
RTSP Reason Phrase	RTSP CSEQ Value	RTSP Media Type
RTSP Version	RTSP Authorization User	

Table 170: RTSP parameters in Protocol Analyser

15.3.75 RUDP

In Protocol Analyser, the following parameters for RUDP are currently available:

RUDP Segment Type

Table 171: RUDP parameters in Protocol Analyser

15.3.76 S1AP

In Protocol Analyser, the following parameters for S1AP are currently available:

S1AP Msg	S1AP Procedure Code	S1AP eNB UE S1AP ID
S1AP LTE-M indication	S1AP IMSI	S1AP LAC
S1AP TAC	S1AP RAC	S1AP TAI MCC
S1AP TAI MNC	S1AP ECGI MCC	S1AP ECGI MNC
S1AP Cell Identity	S1AP MME Code	S1AP M-TMSI
S1AP NRI	S1AP Sector	S1AP eNB ID
S1AP Cause	S1AP SRVCC HO Indication	S1AP SGW-U IP
S1AP eNB/gNB-U IP	S1AP EMI IP	S1AP Handover Type
S1AP NEA	S1AP NIA	S1AP 2nd RAT Req
S1AP 2nd RAT Report	S1AP NB IoT Paging eDRX Cycle	S1AP NB IoT Paging Time Window
S1AP NR Restriction	S1AP MME UE S1AP ID	S1AP Source MME UE S1AP ID

Table 172: S1AP parameters in Protocol Analyser

15.3.77 SBc-AP

In Protocol Analyser, the following parameters for SBc-AP are currently available:

SBc-AP Msg	SBc-AP Procedure Code	SBc-AP Cause

Table 173: SBc-AP parameters in Protocol Analyser

15.3.78 SCCP

In Protocol Analyser, the following parameters for SCCP are currently available:

SCCP Msg	SCCP Class	SCCP GT Called
SCCP GT Calling	SCCP SSN Called	SCCP SSN Calling
SCCP PC Called	SCCP PC Calling	SCCP NOA Called
SCCP NOA Calling	SCCP NP Called	SCCP NP Calling
SCCP TT Called	SCCP TT Calling	SCCP Dest Local Ref
SCCP Source Local Ref	SCCP Return Cause	SCCP Release Cause
SCCP Refusal Cause	SCCP Reset Cause	SCCP Error Cause

Table 174: SCCP parameters in Protocol Analyser

SCCP Called Party Routing Information	SCCP Calling Party Routing Information	SCMG Message Type
SCMG Affected Point Code		

Table 174: SCCP parameters in Protocol Analyser (Continued)

15.3.79 SDP

In Protocol Analyser, the following parameters for SDP are currently available:

SDP Media Address	SDP Origin Username	SDP Media Format
SDP Media Port		

Table 175: SDP parameters in Protocol Analyser

15.3.80 SGsAP

In Protocol Analyser, the following parameters for SGsAP are currently available:

SGsAP Msg	SGsAP IMSI	SGsAP MME Name
SGsAP IMSI Detach EPS	SGsAP IMSI Detach NON EPS	SGsAP IMEI(SV)
SGsAP SGs Cause	SGsAP Reject Cause	SGsAP Service Indicator
SGsAP LAC	SGsAP TAC	SGsAP UE EMM Mode
SGsAP MCC	SGsAP MNC	SGsAP TMSI

Table 176: SGsAP parameters in Protocol Analyser

15.3.81 SIGTRAN

In Protocol Analyser, the following parameters for SIGTRAN are currently available:

SCTP Source Port	SCTP Dest Port	SCTP Chunk Type
SCTP Initiate Tag	SCTP Verification Tag	M3UA Message Type
M3UA Message Class	M3UA Affected Point Codes	IUA Message Type
IUA Message Class	IUA Interface Identifier	M2PA Message Type
M2PA Message Class	M2UA Message Type	M2UA Message Class
M2UA Interface Identifier		

Table 177: SIGTRAN parameters in Protocol Analyser

15.3.82 SIP

In Protocol Analyser, the following parameters for SIP are currently available:

SIP Method	SIP Status Code	SIP Reason Phrase
SIP Media Type	SIP From User	SIP From Host
SIP To User	SIP To Host	SIP Call Id
SIP Diversion User	SIP CSeq Number	SIP CSeq Method
SIP Authorization User	SIP Request URI User	SIP P-Asserted-Identity
SIP P-Called-Party-ID	SIP P-Charging Vector ICID	SIP P-Charging Addresses CCF
SIP P-Charging Addresses ECF	SIP P-Access-Network-Info	SIP Remote Party
SIP User Agent	SIP Expires	SIP Reason Header
SIP Server Header	SIP Via IP	SIP Contact
SIP Country	SIP Alert Info	SIP C-MSISDN

Table 178: SIP parameters in Protocol Analyser

SIP Feature Tags	SIP Warning Header	SIP Cellular Network Info
SIP History-Info User	SIP P-Served-User	SIP Access Type
SIP MCC	SIP MNC	SIP CI
SIP ECI	SIP NCI	SIP LAC
SIP SAC	SIP TAC	SIP P-Charging-Vector orig-ioi
SIP P-Charging-Vector Related ICID	SIP IMEI	SIP IMSI
SIP UUID	SIP P-Associated-URI User	SIP P-Preferred-Identity User
SIP SPI-C	SIP SPI-S	SIP ALG
SIP EALG	SIP Offered ALG	SIP Offered EALG
SIP Request URI	SIP Routing Number	SIP Identity Attest
SIP X-CallGuardian-ucat	SIP P-Visited-Network-ID	SIP Priority
SIP Privacy		

Table 178: SIP parameters in Protocol Analyser (Continued)

15.3.83 SMPP

In Protocol Analyser, the following parameters for SMPP are currently available:

SMPP Message Type	SMPP Command Status	SMPP Message State
SMPP Source Address	SMPP Source NPI	SMPP Source Type of Number
SMPP Source Bearer Type	SMPP Source Network Type	SMPP Destination Address
SMPP Destination NPI	SMPP Destination Type of Number	SMPP Destination Bearer Type
SMPP Destination Network Type	SMPP Network Error Code	SMPP SMSC System ID
SMPP Sequence Number	SMPP Source IMSI	SMPP Destination IMSI
SMPP Bind TON	SMPP Bind NPI	SMPP Address Range
SMPP SM Length	SMPP Message ID	SMPP Data Coding

Table 179: SMPP parameters in Protocol Analyser

15.3.84 SMS

In Protocol Analyser, the following parameters for SMS are currently available:

SMS Dest Address	SMS Orig Address	SMS Recipient Address
SMS Orig NPI	SMS Orig TON	SMS Orig Addr
SMS Dest NPI	SMS Dest TON	SMS Dest Addr
SMS Message type	SMS CP Msg	SMS CP Cause
SMS RP Msg	SMS RP Cause	SMS TP Cause
SMS text length	SMS Protocol Identifier	SMS Data Coding Scheme

Table 180: SMS parameters in Protocol Analyser

15.3.85 SMTP

In Protocol Analyser, the following parameters for SMTP are currently available:

SMTP From	SMTP To	SMTP Command
SMTP Reply Code		

Table 181: SMTP parameters in Protocol Analyser

15.3.86 TAXUP

In Protocol Analyser, the following parameters for TAXUP are currently available:

TAXUP Logical Channel	TAXUP P(s)	TAXUP Charging Header Code
TAXUP Type	TAXUP P(r)	

Table 182: TAXUP parameters in Protocol Analyser

15.3.87 TCAP

In Protocol Analyser, the following parameters for TCAP are currently available:

TCAP Msg	TCAP OTID/TID	TCAP DTID
TCAP Error Code	TCAP Invoke ID	TCAP OP Code
TCAP Application Context Name	TCAP Return Error Problem	

Table 183: TCAP parameters in Protocol Analyser

15.3.88 TCAP/INAP

In Protocol Analyser, the following parameters for TCAP/INAP are currently available:

TCAP/INAP Called Number	TCAP/INAP Calling Number	TCAP/INAP Correlation Id
TCAP/INAP Dest Route Address	TCAP/INAP Service Key	TCAP/INAP Called BCD Number
TCAP/INAP Event Type	TCAP/INAP Event Details	TCAP/INAP Redirecting Reason
TCAP/INAP IMSI	TCAP/INAP MSISDN	TCAP/INAP APN
TCAP/INAP Additional Calling Number	TCAP/INAP Assisting SSPIP Routing Address	TCAP/INAP Called NOA
TCAP/INAP Calling NOA	TCAP/INAP Abort Cause	TCAP/INAP Abort Cause Type
TCAP/INAP Message ID	TCAP/INAP Location Number	TCAP/INAP Event Type 0
TCAP/INAP Event Type 24		

Table 184: TCAP/INAP parameters in Protocol Analyser

15.3.89 TCAP/IS-41

In Protocol Analyser, the following parameters for IS-41 are currently available:

TCAP/IS-41 IMSI Number	TCAP/IS-41 Action code	TCAP/IS-41 Alert Result
TCAP/IS-41 Billing Id	TCAP/IS-41 Calling Party Number Digits 1	TCAP/IS-41 Calling Party Number Digits 2
TCAP/IS-41 Calling Party Number String 1	TCAP/IS-41 Calling Party Number String 2	TCAP/IS-41 Cancellation Type
TCAP/IS-41 Transaction Capability	TCAP/IS-41 Destination Address	TCAP/IS-41 MIN
TCAP/IS-41 SMS Original Originating Address	TCAP/IS-41 SMS Original Destination Address	TCAP/IS-41 Mobile Directory Number
TCAP/IS-41 Routing Digits	TCAP/IS-41 ESN	TCAP/IS-41 Target Cell Id
TCAP/IS-41 Serving Cell Id		

Table 185: IS-41 parameters in Protocol Analyser

15.3.90 TCAP/MAP

In Protocol Analyser, the following parameters for MAP are currently available:

TCAP/MAP IMSI Number	TCAP/MAP TMSI Number	TCAP/MAP NRI
TCAP/MAP IMEI Number	TCAP/MAP HLR Number	TCAP/MAP VLR Number
TCAP/MAP MSC Number	TCAP/MAP MSISDN Number	TCAP/MAP Roaming Number
TCAP/MAP Handover Number	TCAP/MAP Target Cell Identity	TCAP/MAP Forwarding Reason
TCAP/MAP Target LAC	TCAP/MAP Service Centre Address	TCAP/MAP USSD String
TCAP/MAP USSD String length	TCAP/MAP Dialogue Abort Cause	TCAP/MAP Forwarded To Number
TCAP/MAP GSN Address	TCAP/MAP GSN Number	TCAP/MAP Supported Camel Phase (Oldest)
TCAP/MAP SM Delivery Failure Cause	TCAP/MAP Equipment Status	

Table 186: MAP parameters in Protocol Analyser

15.3.91 TCP

In Protocol Analyser, the following parameters for TCP are currently available:

TCP Source Port	TCP Seq Number	TCP Control Bits
TCP Dest Port	TCP Ack Number	

Table 187: TCP parameters in Protocol Analyser

15.3.92 TUP FRANCE

In Protocol Analyser, the following parameters for TUP France are currently available:

TUP Msg	TUP A Number
TUP CIC	TUP B Number

Table 188: TUP France parameters in Protocol Analyser

15.3.93 UDP

In Protocol Analyser, the following parameters for UDP are currently available:

UDP Source Port	UDP Dest Port

Table 189: UDP parameters in Protocol Analyser

15.3.94 USSD

In Protocol Analyser, the following parameters for USSD are currently available:

USSD String	USSD String length

Table 190: USSD parameters in Protocol Analyser

15.3.95 WAP

In Protocol Analyser, the following parameters for WAP are currently available:

WSP URI	WSP Cause	WSP PDU Type
WTP Retransmission Indicator	WTP TID	WTP GTR TTR

Table 191: WAP parameters in Protocol Analyser

WTP Packet Seq Number	WTP PDU	WTP Concatenated PDU
WTP Transaction Class		

Table 191: WAP parameters in Protocol Analyser (Continued)

15.3.96 X2AP

In Protocol Analyser, the following parameters for X2AP are currently available:

X2AP Message Type	X2AP Message Name	X2AP UE X2AP ID

Table 192: X2AP parameters in Protocol Analyser

15.3.97 XCAP

In Protocol Analyser, the following parameters for XCAP are currently available:

XCAP A Number	XCAP IMSI

Table 193: XCAP parameters in Protocol Analyser

16 SOS columns

The division in this chapter is based on top level protocols, and the parameters correspond to the information you get in CSE/MSE.

These parameters can be used for server-side filtering in historical searches. The parameters marked as index are faster when performing historical searches.

The following tables show the parameters with CSE/MSE support for each protocol, including which that are indexed.

16.1 SOS columns - CSE

16.1.1 AIN

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Operation Code	
Error Code	
Calling Number	
Called Number	
Routing Number	
Source IP	
Destination IP	

Table 194: SOS columns for AIN

16.1.2 ALCAP

Parameter name	Key
Originating Point Code	
Destination Point Code	
Cause Value	
Originating Signalling Association Identifier	
Destination Signalling Association Identifier	
Served User Generated Reference	

Table 195: SOS columns for ALCAP

16.1.3 ALL

Parameter name	Key
Timestamp	

Table 196: SOS columns for all protocols

Parameter name	Key
Duration (only for ended calls)	
Transaction ID	

Table 196: SOS columns for all protocols (Continued)

16.1.4 BICC

Parameter name	Key
Calling Party Number	index
Called Party Number	index
Call Instance Code	
Originating Point Code	
Destination Point Code	
Network Indicator	
Cause Value	
Address Complete Timestamp	
Answer Timestamp	
Release Timestamp	
Calling Nature Of Address Indicator	
Called Nature Of Address Indicator	
Redirecting Number	
Backbone Network Connection Identifier	
SDP Identifier A	
SDP Identifier B	
Source IP	
Destination IP	

Table 197: SOS columns for BICC

16.1.5 BSSAP

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
International Mobile Subscriber Identity	index
Called Number	index
Calling Number	index
International Mobile Equipment Identity	index
International Mobile Equipment Identity and Software Version number	index
SMS Destination Address	
SMS Recipient Address	
SMS Originating Address	
Answer Time	
Release Time	
Cell Identity	index

Table 198: SOS columns for BSSAP

Parameter name	Key
MM SM Message	
MM SM Location Area Code	
Incoming Handover Command Data	
Outgoing Handover Command Data	
MM Cause	index
CC Cause	
Reject Cause	
Location Area Code	
SMS Message Type	
Layer 3 Message	
LCS Cause	index
Source IP Address	
Destination IP Address	
MM/SM LAC	
RAC	
SAC	
MCC	
MNC	
Mobile IP Address	
Access Point Name	
SDP Audio Destination A	
SDP Audio Destination B	
DTAP CC Cause	
Algorithm Identifier	

Table 198: SOS columns for BSSAP (Continued)

16.1.6 BSSAP+ (GSM09_18)

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
International Mobile Subscriber Identity	index
IMSI detach from GPRS service type	
IMSI detach from non-GPRS service type	
GS Cause	index
Message Type	
Routing Area Code	
Location Area Code	
Source IP	
Destination IP	

Table 199: SOS columns for BSSAP+

16.1.7 DHCP

Parameter name	Key
Transaction ID	index
Client (your) IP address	index
Client hardware address	index
Subnet Mask	
Router Address	
Domain Name System Address	
Host Name	
Domain Name	
Lease Time	
Server Identifier	
Renewal Time	
Rebinding Time	
Vendor Class Identifier	
Client Identifier	
Relay Agent Info Type	
Relay Agent Circuit Identifier	
Relay Agent Remote Identifier	
Relay Agent Subscriber Identity	
Source IP	
Destination IP	

Table 200: SOS columns for DHCP

16.1.8 DIAMETER (RFC3588)

Parameter name	Key
Reloaded	
Link Id	
Source IP Address	
Destination IP Address	
Framed IP Address AVP	
Command Code	
International Mobile Subscriber Identity	index
MS International PSTN/ISDN Number	index
Calling Party Number	index
Called Party Number	index
IMS Charging Identifier	
Cause Code	index
Max Response Time	
Result Code	
Username	
Public Identity	
Session ID	
MCC	
MNC	

Table 201: SOS columns for DIAMETER

Parameter name	Key
ECI	
LAC	
SAC/CI	
Framed IPv6 prefix	
IMEI	
IMSI	
Service selection	
Origin Realm	
Destination Realm	
Origin Host	
Destination Host	
Radio Access Type 2G/3G	
Access Restriction Data	
Core Network Restrictions	
2nd RAT	
Experimental result code	
Abort Cause	
Termination cause	
Equipment Status	

Table 201: SOS columns for DIAMETER (Continued)

16.1.9 DNIS (RFC1035)

Parameter name	Key
Source IP Address	
Destination IP Address	
International Mobile Subscriber Identity	index
MS International PSTN/ISDN Number	index
Called Number	

Table 202: SOS columns for DNIS

16.1.10 DNS

Parameter name	Key
ID	

Table 203: SOS columns for DNS

16.1.11 EMI

Parameter name	Key
Source IP	index
Destination IP	index
Operation Type	
Response Type	
Error Code	
Source Address	index
Destination Address	index

Table 204: SOS columns for EMI

Parameter name	Key
PID	
Message Type	
DCS	

Table 204: SOS columns for EMI (Continued)

16.1.12 GPRSGB

Parameter name	Key
International Mobile Subscriber Identity	index
Access Point Name	
MM Cause	index
SM Cause	index
MM SM Message	
MM SM Location Area Code	
Location Area Code	
Routing Area Code	
Cell Identity	index
Mobile IP Address	index
International Mobile Equipment Identity	index
International Mobile Equipment Identity and Software Version number	index
BSSGP Virtual Connection Identifier	index
Reject Cause	
SMS Message Type	
MM/SM LAC	
MCC	
MNC	
Source IP	
Destination IP	
SMS Destination	
SMS Recipient	
SMS Orig Address	

Table 205: SOS columns for GPRSGB

16.1.13 GTP

Parameter name	Key
Reloaded Call	
Link Id	
GTP Message	
Access Point Name	
MS International PSTN/ISDN Number	index
International Mobile Subscriber Identity	index
International Mobile Equipment Identity and Software Version number	index
End User Address	index
End User Address IPv6	

Table 206: SOS columns for GTP

Parameter name	Key
Cause	index
Source Address	
Destination Address	
Tunneled Source IP	
Tunneled Dest IP	
Radio Access Technology	
Routing Area Code	
Tracking Area Code	
Service Area Code	
Cell Identity	
E-UTRAN Cell Identity (ECI)	
STN SR Address	
MME CP Address	
MSC CP Address	
RNC ID	
Target Cell Identity	
SRVCC Cause	

Table 206: SOS columns for GTP (Continued)

16.1.14 H225

Parameter name	Key
Calling Party number	index
Called Party number	index
Display	
Source Address Number	
Source Address Text	
Destination Address Number	
Destination Address Text	
Cause Value	

Table 207: SOS columns for H225

16.1.15 HTTP

Parameter name	Key
Source IP Address	
Destination IP Address	
Requested Uniform Resource Identifier	
IMSI	index
A Number	index
MMS A Number	
MMS B Number	index
Method	
Status Code	
Location	
User Agent	

Table 208: SOS columns for HTTP

16.1.16 HTTP2

Parameter name	Key
SMS Message Type	
Source Address	
Destination Address	
Stream ID	
Method	
Request URI	
Status Code	
IMSI	index
SSC Mode	
DNN	
Session Management Message	
S-NSSAI	
MCC	
MNC	
IMEI	
MSISDN	index
RAT	
AMF Region	
AMF Set	
AMF Pointer	
Location	
Source Port	
Destination Port	
Service	
S-NSSAI SST	
S-NSSAI SD	
5QI	
NCI	
TAC	
PDU Session Type	
PDU Session ID	
Cause	
Service Operation	
UE IPv4 address	
Orig Address MS	
Dest Address MS	
Recipient Address	
Source NF Type	
Target NF Type	
Request Cause	
HO State	
EPS Interworking Indication	
ECI	
SM Cause	

Table 209: SOS columns for HTTP2

Parameter name	Key
APN	
Title	
Source FQDN	
Target FQDN	
Destination FQDN	
Source NF	
Destination NF	
3gpp-sbi-target-apiroot	
5GC next-hop-authority	
5GC N2 Info	

Table 209: SOS columns for HTTP2 (Continued)

16.1.17 INAP (TCAP/INAP Ericsson CS1+ B)

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Called Global Title E164	
Operation Code	index
Error Code	
Destination Routing Address	index
Calling Number	index
Correlation ID Number	
Called Number	index
Called BCD Number	index
SSP IP Routing Address	
Additional Calling Number	
International Mobile Subscriber Identity	
Cell Identity	
Location Area Code	
Origination Reference	
Destination Reference	
Source IP	
Destination IP	
Calling NBR NOA	
Called NBR NOA	
Service Key	
Abort Cause Value	
Abort Cause Type	
Number Of Connects	
Message ID	

Table 210: SOS columns for INAP

Parameter name	Key
Return Error Problem	
Location Number	
Event Type 0	
Event Type 24	

Table 210: SOS columns for INAP (Continued)

16.1.18 IS-41 (TCAP/IS-41)

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Operation Code	
Error Code	
Temporary Local Directory Number	
International Mobile Subscriber Identity	index

Table 211: SOS columns for IS-41

16.1.19 ISAKMP (RFC7296IKEv2bis)

Parameter name	Key
Source Address	
Destination Address	
Initiator SPI	index
Responder SPI	index
Exchange Type	

Table 212: SOS columns for ISAKMP

16.1.20 ISDN

Parameter name	Key
Calling Party Number	index
Called Party Number	index
Cause Value	
IUA Interface Identifier	
IUA Source IP Address	
IUA Destination IP Address	
Transfer Capability	

Table 213: SOS columns for ISDN

16.1.21 ISDN_SS_SCCP (ISDN SS)

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Operation Code	index
Calling Number	index
Called Number	index
Error Code	
Source IP	
Destination IP	

Table 214: SOS columns for ISDN_SS_SCCP

16.1.22 ISUP (ISUP93ver2ET97)

Parameter name	Key
A Number	index
B Number	index
Circuit Identification Code	
Originating Point Code	
Destination Point Code	
Release Originating Point Code	
TX MED RQ	
Network Indicator	
Cause Value	
Cause Location	
Address Complete Time	
Answer Time	
Release Time	
A Nature Of Address Indicator	
B Nature Of Address Indicator	
Redirecting Number	
Original Called Number	index
Generic Number	
Correlation ID	
Source IP	
Destination IP	index
IMSI	

Table 215: SOS columns for ISUP

16.1.23 IUP

Parameter name	Key
A Number	index
B Number	index
Line Identity Type	
Circuit Identification Code	
Originating Point Code	
Destination Point Code	
Network Indicator	
Cause Value	
Connection Not Admitted Reason	
ANS Time	
Answer Time	
Release Time	
A Nature of Address Indicator	
Full Calling Line	
Full Calling Nature of Address Indicator	
Source IP	
Destination IP	

Table 216: SOS columns for IUP

16.1.24 LCS-AP

Parameter Name	Key
Correlation ID	
Procedure Code	
CI	
MNC	
MCC	
LCS Cause	
IMSI	index
eNB ID	
Sector ID	
Source Address	
Dest Address	

Table 217: SOS columns for LCS-AP

16.1.25 LDAP

Parameter Name	Key
International Mobile Subscriber Identity	index
MS International PSTN/ISDN Number	index
Result Code	index
Source IP	
Destination IP	
DN Other Number	index

Table 218: SOS columns for LDAP

16.1.26 LPPa

Parameter Name	Key
Type of Message	
Cause	

Table 219: SOS columns for LPPa

16.1.27 MAP (TCAP/MAP)

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Called Global Title E164	
Operation Code	index
Error Code	
International Mobile Subscriber Identity	index
MS International PSTN/ISDN Number	index
Roaming Number	
MSC Number	
GMSC Address	
SMS Destination Address	
SMS Recipient Address	
SMS Originating Address	
Incoming Handover Command Data	
Outgoing Handover Command Data	
Handover Number	
Cell Identity	
Location Area Code	
International Mobile Equipment Identity	
SMS Message Type	
Layer 3 Message	
Source IP	
Destination IP	
DTAP CC Cause	
Equipment Status	

Table 220: SOS columns for MAP

16.1.28 MEGACO (Megaco Binary/Text)

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	

Table 221: SOS columns for MEGACO

Parameter name	Key
Transaction ID	
Context ID	
Error Code	
Command	
Termination ID	
Second Termination ID	
International Mobile Subscriber Identity	index
Source IP Address	
Destination IP Address	
Called Number	
Calling Number	
GW MID	
GW Controller MID	
BIR SUGR	
Process Sequence Number	
SDP Identifier A	
SDP Identifier B	

Table 221: SOS columns for MEGACO (Continued)

16.1.29 MGCP

Parameter name	Key
Verb	
Transaction ID	
Endpoint Name	index
Response Code	
Caller ID	
Called Number	
SDP Identifier A	
SDP Identifier B	
Source Address	
Destination Address	

Table 222: SOS columns for MGCP

16.1.30 NBAP

Parameter name	Key
Procedure Code	
Binding ID	
Uplink Scrambling	

Table 223: SOS columns for NBAP

16.1.31 NGAP

Parameter name	Key
Procedure code	
Cause	

Table 224: SOS columns for NGAP

Parameter name	Key
Source Address	
Dest Address	
TAI MCC	
TAI MNC	
NR CGI MCC	
NR CGI MNC	
Cell Identity	
Last Cell Identity	
5GMM Registration Type	
5GMM Msg	
5GSM SSC Mode	
TAC	
5QI	
S-NSSAI SST	
5G-TMSI	
AMF Region	
AMF Set	
AMF Pointer	
5GMM 5G-TMSI	
5GMM Old 5G-TMSI	
5GMM Additional 5G-TMSI	
5GSM DNN	
5GSM Cause	
5GMM Cause	
5GSM Msg	
5GMM IMSI	index
RAN UE ID	index
AMF UE ID	index
Last AMF UE ID	index
IMSI Enriched By	
IMSI Enrichment Reliability	
PDU Session ID	
PDU Session Type	
Orig Address MS	
Dest Address MS	
Recipient Address	
5GMM Deciphered	
IMEI	
Largest Container Size	
Message Type	
5GMM SUCI MCC	
5GMM SUCI MNC	
Msg	
S-NSSAI SD	
5GSM S-NSSAI SD	

Table 224: SOS columns for NGAP (Continued)

Parameter name	Key
UE Policy Msg Type	
5GMM NSSAI Requested	
5GMM NSSAI Allowed	
5GMM NSSAI Rejected	
NSSAI Allowed	

Table 224: SOS columns for NGAP (Continued)

16.1.32 PCAP

Parameter name	Key
Procedure Code	
RNC ID	
Transaction ID	
Message Type	
Positioning Method	
Request Type	
Cell ID	index
Cause	
Source IP	
Destination IP	

Table 225: SOS columns for PCAP

16.1.33 PFCP

Parameter name	Key
Source Address	
Dest Address	
Message	
Cause	
UE IP Address	
APN/DNN	
S-NSSAI SST	
S-NSSAI SD	
URR ID	
IMSI	index
IMEI	

Table 226: SOS columns for PFCP

16.1.34 RADIUS (RFC2865Radius)

Parameter name	Key
Source Address	
Dest Address	
Identifier	
Framed IP Address	
IMSI	index
MSISDN	index

Table 227: SOS columns for RADIUS

Parameter name	Key
Calling User	index
Called User	index
MCC	
MNC	
Accounting Session ID	index

Table 227: SOS columns for RADIUS (Continued)

16.1.35 RANAP

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Cause	
Access Point Name	
International Mobile Subscriber Identity	index
Called Number	index
Calling Number	index
Binding ID	
International Mobile Equipment Identity	index
International Mobile Equipment Identity and Software Version number	index
SMS Destination Address	
SMS Recipient Address	
SMS Originating Address	
Mobile IP Address	index
MM SM Message	
MM SM Location Area Code	
Service Area Code	
Location Area Code	
Routing Area Code	
MM Cause	index
SM Cause	index
CC Cause	
Reject Cause	
Global RNC	
Handover Command Data	
SMS Message Type	
MM/SM LAC	
CI	
MCC	
MNC	
Source IP	
Destination IP	

Table 228: SOS columns for RANAP

Parameter name	Key
SDP Audio Destination A	
SDP Audio Destination B	
Last SAC	
Last LAI LAC	
Last SAI LAC	

Table 228: SOS columns for RANAP (Continued)

16.1.36 RNSAP

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Procedure Code	
International Mobile Subscriber Identity	index
International Mobile Equipment Identity	
RNC ID	index
Routing Area Code	
Location Area Code	
Service Area Code	
Binding ID	
UL Scrambling	
MCC	
MNC	
Source IP	
Destination IP	

Table 229: SOS columns for RNSAP

16.1.37 RRC

Parameter name	Key
Channel ID	
Establishment Cause	
Uplink Scrambling Code	
International Mobile Subscriber Identity	
Location Area Code	
MM SM Location Area Code	

Table 230: SOS columns for RRC

16.1.38 RTSP

Parameter name	Key
Method	
Session ID	index
Media Address	index

Table 231: SOS columns for RTSP

Parameter name	Key
Media Port	index
Tunnel Start Time	
Tunnel Process Sequence Number	

Table 231: SOS columns for RTSP (Continued)

16.1.39 S1AP

Parameter name	Key
IMSI	index
M-TMSI	
LAC	
RAC	
TAC	
MCC	
MNC	
MME Code	
CI	
Last Cell Identity	
APN	
Mobile IP Address	
Msg	
MM Cause	
SM Cause	
Source Address	
Dest Address	
Dest Address MS	
Recipient Address	
Orig Address MS	
Procedure Code	
Cause	
ECGI MCC	
ECGI MNC	
LAC	
Message Type	
Cause	
IMEISV	
M-TMSI	
UE CP CIoT	
UE UP CIoT	
UE DCNR	
UE N1 mode	
NW CP CIoT	
NW UP CIoT	
NW Restrict DCNR	
2nd RAT Req	
2nd RAT Report	

Table 232: SOS columns for S1AP

Parameter name	Key
NR Restriction	
eNB Id	
Handover Type	
IMSI Enriched By	
IMSI Enrichment Reliability	
NW Control plane only indication	
TAC	
EMI IP	
P-CSCF IPv6	
Feature Group Ind	
LTE-M indication	
Largest Container Size	
Message Type	
MME UE S1AP ID	index
Last MME UE S1AP ID	index

Table 232: SOS columns for S1AP (Continued)

16.1.40 SBc-AP

Parameter name	Key
Procedure Code	

Table 233: SOS columns for SBc-AP

16.1.41 SGsAP

Parameter name	Key
SGsAP Message Type	
IMSI	index
SGsAP MME Name	
IMSI detach from EPS service type	
IMSI detach from non-EPS service type	
SGsAP Cause	index
SGsAP Reject Cause	
SGsAP UE EMM Mode	
SMS Message Type	
IMEI SV	
LAC	
SMS Destination	
SMS Recipient	
SMS Origin Address	
Source IP	
Destination IP	
MCC	
MNC	

Table 234: SOS columns for SGsAP

16.1.42 SIP

Parameter name	Key
Method	
From User	index
To User	index
Call ID	index
Diversion User	index
Termination Code	
Authorization	index
Calling User	
Called User	
Reason Header	
Source Address	
Destination Address	
SDP Audio Dest A	
SDP Audio Dest B	
P Charging Vector ICID	
Tunnel Start Time	
Tunnel Process Sequence Number	
Contact	
IMSI	
P Associated URI User	
TERMINATION_CODE_BYE	
TERMINATION_CODE_CANCEL	
SMS Message Type	
IMEI	
SMS Destination	
SMS Recipient	
SMS Orig Address	
SDP Message Destination A	
SDP Message Destination B	
SDP Media Transport	
ALG	
EALG	
Offered ALG	
Offered EALG	
Emergency Call	
Reason	
P-Charging-Vector Related ICID	
Feature Tags	
Warning	
Last Source Address	
Last Dest Address	
Request URI	
Routing Number	
Session Duration	

Table 235: SOS columns for SIP

Parameter name	Key
History Info User	
P-Served-User	
MCC	
MNC	
CI	
ECI	
NCI	
LAC	
SAC	
TAC	
P-Visited-Network-ID	
Orig Trunk	
Term Trunk	
INVITE Type	
Priority	

Table 235: SOS columns for SIP (Continued)

16.1.43 SIP_PSTN (SIP+PSTN)

Parameter name	Key
Method	
From User	
To User	
Call ID	
Diversion User	
Termination Code	
Authorization	
Calling User	
Called User	
Source Address	
Destination Address	
SDP Audio Dest A	
SDP Audio Dest B	
P-Charging Vector ICID	
Tunnel Start Time	
Tunnel Process Sequence Number	
Contact	
IMSI	
P Associated URI User	
Transfer Capability	
Transfer Mode	
Layer 1 Protocol	
High Layer Characteristics	
Location	

Table 236: SOS columns for SIP_PSTN

16.1.44 SIP_T

Parameter name	Key
Method	
From User	
To User	
Call ID	
Diversion User	
Termination Code	
Authorization	
Calling User	
Called User	
Source Address	
Destination Address	
SDP Audio Dest A	
SDP Audio Dest B	
P-Charging Vector ICID	
A Number	
B Number	
Cause Value	
A Nature of Address	
B Nature of Address	
Redirecting Number	
Original Called Number	

Table 237: SOS columns for SIP_T

16.1.45 SMPP

Parameter name	Key
SRC IP Address	
Destination IP Address	
SRC Address	index
Destination Address	index
Network Error	
SMSC ID	index
Source IMSI	
Destination IMSI	
Message Type	
Command Status	
Message State	

Table 238: SOS columns for SMPP

16.1.46 SMTP

Parameter name	Key
From	
To	
Source Address	

Table 239: SOS columns for SMtP

Parameter name	Key
Dest Address	
A Number	
B Number	
Msg ID	

Table 239: SOS columns for SMtP (Continued)

16.1.47 WSP

Parameter name	Key
Source Address	
Destination Address	
International Mobile Subscriber Identity	index
MS International PSTN/ISDN Number	index

Table 240: SOS columns for WSP

16.2 SOS columns - MSE

16.2.1 All

Parameter name	Key
Timestamp	
Transaction ID	
Link ID	
Decode Error	

Table 241: SOS columns for all protocols

16.2.2 Unknown

Parameter name	Key
Link ID	
Decode Error	
Protocol	

Table 242: SOS columns for unknown protocols

16.2.3 AggData

Parameter name	Key
Type	
Source Address	
Destination Address	
TLLI	
BVCI	

Table 243: SOS columns for AggData

16.2.4 BSSAP

Parameter name	Key
Chunk Type	
Originating Point Code	

Table 244: SOS columns for BSSAP

Parameter name	Key
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Called Global Title E164	
Source Local Reference	
Destination Local Reference	
International Mobile Subscriber Identity	index
Called Number	index
Calling Number	index
International Mobile Equipment Identity	index
International Mobile Equipment Identity and Software Version number	index
SMS Destination Address	
SMS Recipient Address	
SMS Originating Address	
Cell Identity	index
MM SM Message	
MM Cause	index
CC Cause	
Reject Cause	
Local Area Code	

Table 244: SOS columns for BSSAP (Continued)

16.2.5 DIAMETER (RFC3588Diameter)

Parameter name	Key
Source Address	
Destination Address	
Framed IP Address	
International Mobile Subscriber Identity	index
MS International PSTN/ISDN Number	index
Calling Party Number	index
Called Party Number	index
Cause Code	index
IMS Charging Identifier	
Result Code	
Latency	

Table 245: SOS columns for DIAMETER

16.2.6 GPRSGB

Parameter name	Key
TLLI	index
International Mobile Subscriber Identity	index

Table 246: SOS columns for GPRSGB

Parameter name	Key
Access Point Name	
MM Cause	index
SM Cause	index
MM SM Message	
Location Area Code	
Routing Area Code	
Cell Identity	index
Mobile IP Address	index
International Mobile Equipment Identity	index
International Mobile Equipment Identity and Software Version number	index
BSSGP Virtual Connection Identifier	index
Reject Cause	

Table 246: SOS columns for GPRSGB (Continued)

16.2.7 GTP

Parameter name	Key
GTP Message	
Version	
Access Point Name	
MS International PSTN/ISDN Number	index
International Mobile Subscriber Identity	index
End User Address	index
End User Address IPv6 Address	
Cause Value	index
Source Address	
Destination Address	
Tunnel Process Sequence Number	
International Mobile Equipment Identity and Software Version number	index
E-UTRAN Cell Identity (ECI)	
Radio Access Technology Type	
Routing Area Code	
Service Area Code	
Cell Identity	
NSAPI	
TEID	
TEID CP	
TEID Data	
Sequence Number	
STN SR Address	
MME CP Address	
MSC CP Address	
RNC ID	

Table 247: SOS columns for GTP

Parameter name	Key
Target ID	
SRVCC Cause	

Table 247: SOS columns for GTP (Continued)

16.2.8 ISAKMP (RFC7296IKEv2bis)

Parameter name	Key
Source Address	
Destination Address	
Initiator SPI	index
Responder SPI	index
Message ID	
Exchange Type	

Table 248: SOS columns for ISAKMP

16.2.9 ISUP (ISUP93ver2ET97)

Parameter name	Key
Chunk Type	
A Number	index
B Number	index
Circuit Identification Code	
Originating Point Code	
Destination Point Code	
Release Originating Point Code	
TX MED RQ	
Network Indicator	
Cause Value	
Cause Location	
A Nature Of Address Indicator	
B Nature Of Address Indicator	
Redirecting Number	
Original Called Number	index
Generic Number	
Correlation ID	

Table 249: SOS columns for ISUP

16.2.10 RANAP

Parameter name	Key
Chunk Type	
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	

Table 250: SOS columns for RANAP

Parameter name	Key
Called Global Title	
Called Global Title E164	
Source Local Reference	
Destination Local Reference	
Cause	
Access Point Name	
International Mobile Subscriber Identity	index
Called Number	index
Calling Number	index
Binding ID	
International Mobile Equipment Identity	index
International Mobile Equipment Identity and Software Version number	index
SMS Destination Address	
SMS Recipient Address	
SMS Originating Address	
Mobile IP Address	index
MM SM Message	
Service Area Code	
Location Area Code	
Routing Area Code	
MM Cause	index
SM Cause	index
CC Cause	
Reject Cause	
Global RNC	
Handover Command Data	

Table 250: SOS columns for RANAP (Continued)

16.2.11 RNSAP

Parameter name	Key
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Called Global Title E164	
Source Local Ref	
Destination Local Ref	
Procedure Code	
International Mobile Subscriber Identity	index
International Mobile Equipment Identity	
RNC ID	index

Table 251: SOS columns for RNSAP

Parameter name	Key
Routing Area Code	
Location Area Code	
Service Area Code	
Binding ID	
UL Scrambling	

Table 251: SOS columns for RNSAP (Continued)

16.2.12 SCCP

Parameter name	Key
Chunk Type	
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Called Global Title E164	
Source Local Reference	
Destination Local Reference	

Table 252: SOS columns for SCCP

16.2.13 SMPP (SMPP v.3.4)

Parameter name	Key
Message Type	index
Command Status	
Message State	
Source Address	index
Destination Address	index
Network Error	
SMSC ID	index

Table 253: SOS columns for SMPP

16.2.14 TCAP

Parameter name	Key
Chunk Type	
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Called Global Title E164	

Table 254: SOS columns for TCAP

Parameter name	Key
Source Local Reference	
Destination Local Reference	

Table 254: SOS columns for TCAP (Continued)

16.2.15 INAP (TCAP/INAP Ericsson CS1+ B)

Parameter name	Key
Chunk Type	
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Called Global Title E164	
Source Local Reference	
Destination Local Reference	
OTID	
DTID	
Operation Code	index
Error Code	
Destination Route Address	index
Calling Number	index
Correlation ID Number	
Called Number	index
Called BCD Number	index
SSPIP Routing Address	
Additional Calling Number	
International Mobile Subscriber Identity	

Table 255: SOS columns for TCAP/INAP

16.2.16 MAP (TCAP/MAP)

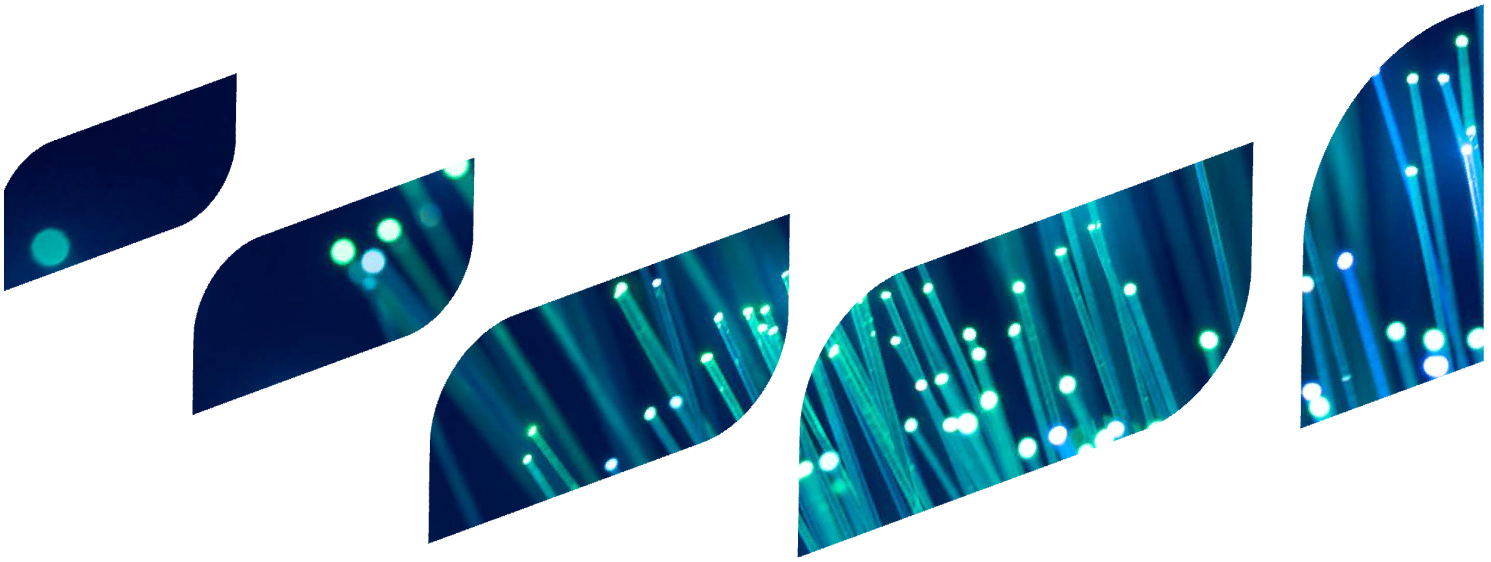
Parameter name	Key
Chunk Type	
Originating Point Code	
Destination Point Code	
Network Indicator	
Calling Subsystem Number	
Called Subsystem Number	
Calling Global Title	
Called Global Title	
Called Global Title E164	
Source Local Reference	
Destination Local Reference	
OTID	

Table 256: SOS columns for TCAP/MAP

Parameter name	Key
DTID	
Operation Code	index
Error Code	
International Mobile Subscriber Identity	index
MS International PSTN/ISDN Number	index
Roaming Number	
MSC Number	
GMSC Address	
SMS Destination Address	
SMS Recipient Address	
SMS Originating Address	
International Mobile Equipment Identity	

Table 256: SOS columns for TCAP/MAP (Continued)

Polystar | ELISA INDUSTRIQ



Polystar | ELISA INDUSTRIQ

Hammarby Allé 29
120 32 Stockholm
Sweden

Phone: +46 8 50 600 600

Follow us on social media