Call and Session Trace in UMTS

Call and session trace of signaling procedures for multiple UMTS interfaces

Introduction

While UMTS brings overwhelming service capabilities it also brings complexity with several network layers and technologies interworking. Furthermore, there's a never decreasing drive for reducing cost while at the same time satisfying the customer expectation to quality. Likewise, a responsible manager will expect insight into network hotspots with relevant information about the causes. Fast and efficient monitoring and trouble shooting are essential to ensure proper network and service roll-out and hence customer satisfaction.

MasterClaw UMTS call and session trace is an application that even in such complex environments as UMTS can perform circuit and packet domain traces of mobile originating and terminating calls as well as SMS and PDP context activation and deactivation. This includes traces within the access or core networks and even traces across multiple interfaces. Hence covering the path from and to the UMTS terrestrial access network to and including the PSTN or ISP.

Typical issues can be related to user mobility, to DNS lookup, to handovers, to roaming partners, to access points, to RADIUS authentication and to SGSN, RNC, HLR, MSC or MGW configurations – the probable issues and potential root causes are nearly endless, and the exact cause and even the nature is usually difficult to locate. MasterClaw UMTS call and session trace application can be used to quickly find the reason why, e.g., a PDP context was rejected or why the user could not attach to the network.

MasterClaw UMTS call and session trace can be used to find problems related to a customer complaint or to identify causes related to roamers, mobile station types, handovers or network nodes. MasterClaw UMTS Call and Session Trace application is easy to use and can be used by first, second and third line support. First line support may use Call and Session Trace to find out whether a subscriber is really having a problem or not, or whether it is related to his subscription or to problems in the network. Second and third line support may use MasterClaw UMTS call and session trace to find the cause of the problem.

Benefits

- Simplifies root-cause analysis and troubleshooting UTRAN, circuit and packet core networks
- Provides real-time end-to-end network visibility across access, circuit and packet core networks
- Historical tracing capabilities allow troubleshooting during "normal business hours", and hence reduces the cost
- Multi-user – multi-skill support allows both customer facing staff and network engineers to use the application and share traces and results

Features

- Covers all standard UMTS signaling interfaces: e.g. IuPS, IuCS, Gn, Gi, Gr, Nc, Mc, plus vendor specific Iub and Iur variants.
- Supports inter technology signaling providing scenarios for troubleshooting issues related to handovers between GSM and UMTS networks.
- Real-time deciphering of Iub and Iur interface
- Seamless translation of TMSI to IMSI and IMEI, P-TMSI to IMSI and IMEI, and IMSI to MSISDN
- Fully integrated with Anritsu's GSM & GPRS solution

Application Note

This document provides a brief overview on the MasterClaw Call and Session Trace application with the focus on UMTS networks and interfaces. The term “call trace” is used throughput this document to also comprise session and transaction traces. The MasterClaw portfolio of products for UMTS also includes link & message statistics and protocol analysis and statistics packages like the service assurance package “Wireless Packet Key Performance Indicators” that can indicate problems in the core network regarding accessibility, setup time, QoS and throughput.

UMTS Interfaces

A UMTS network consists of a numerous interfaces. Some interfaces use specific bearers while other interfaces have optional bearer capabilities, i.e., ATM or Ethernet. Likewise, the nature of some of the interfaces is optional depending on the network release. MasterClaw UMTS supports release ’99 (See Figure 1), release 5 and 6 protocols including the SIP, SIP-T, BICC and MEGACO/H248 protocols. In addition, MasterClaw offers the combination of vendor specific Iu protocols, 2G interfaces and protocols like ISUP, MAP and CAP while also 2.5G interfaces like Ga, Gb, Gc, Ge, Gf, Gn, Gi, Gp, Gr and Gs for end to end call and session trace.

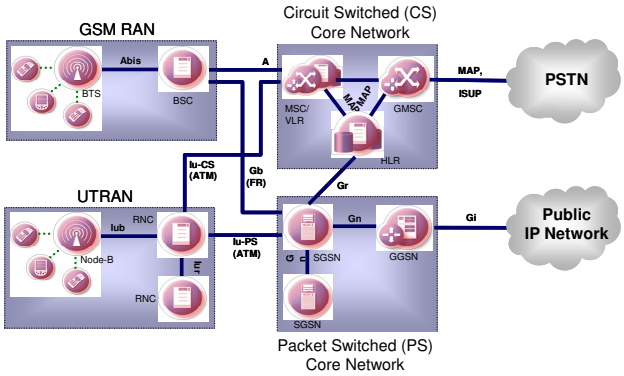

Figure 1: Release ’99 network with GSM, GPRS and UMTS side by side

The UMTS infrastructure may look different depending on whether UMTS is added to an existing 2.5G infrastructure with or without handover or comprises as a green field installation. In the greenfield scenario, the chosen network architecture is often release 4 or later as illustrated in Figure 2.

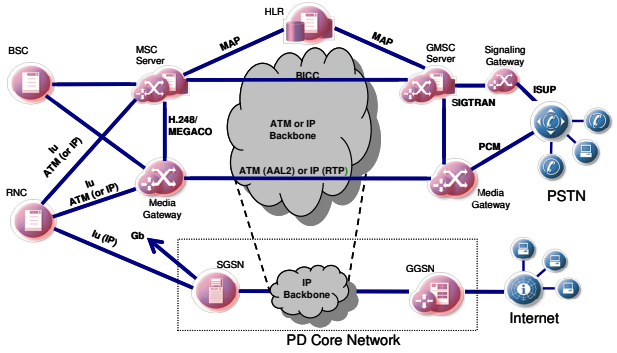

Figure 2: Release 4 network – the split architecture

The implementation of release 4 and 5 adds network layers by separating the control and switching functions while introducing new protocols such as SIGTRAN, H.248, BICC and SIP - all supported by MasterClaw UMTS.

Scenarios

MasterClaw supports dialogue call, transaction and session trace on all UMTS, GSM and GPRS interfaces for both circuit and packet domains. A dialogue or procedure call trace is a trace on one interface e.g. IuPS but on many physical and logical connections and multiple legs. A dialogue call trace may for instance be to find all IuPS Attach procedures having a certain reject cause or all “create PDP context” on the Gn interface to a certain APN and/or originated by a specific subscriber.

The traces possible depend upon which links are monitored and which bearers and services are deployed. An example of protocols and nodes involved in a trace in an end to end monitoring of the UMTS circuit domain is shown in Figure 3.

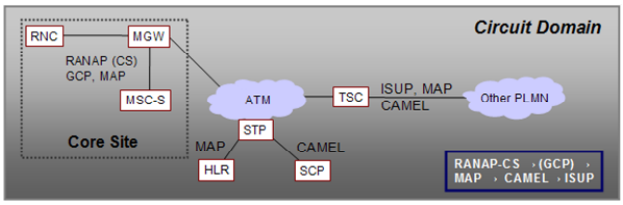

Figure 3: Example of protocols for Release 4 circuit domain trace

In addition to IuPS, IuCS and Gn, MasterClaw supports vendor specific Iub and Iur protocols. These protocols may also be part of an end-to-end call trace. For a list of protocols supported please contact Anritsu.
Likewise, packet domain traces are possible as shown in Figure 4. Figure 4 shows the control plane protocol mainly. Major user plane protocols are also supported and Anritsu is continuously adding support for more user plane protocols.

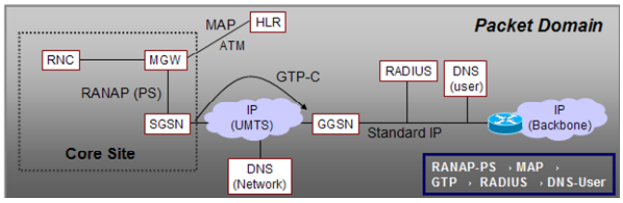

Figure 4: Example of protocols for Release 4 packet domain trace

To do a trace, a scenario has to be chosen; is it a mobile originating call or is it a mobile terminating SMS or is it a mobile to mobile call etc. A scenario may be predefined by Anritsu and/or customer defined or modified. Figure 5 shows some of the predefined UMTS scenarios.

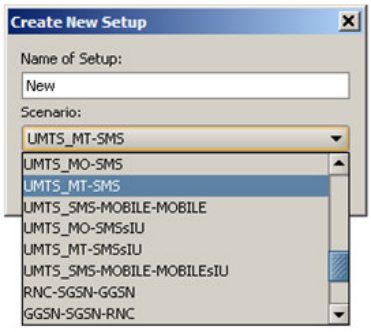

Figure 5: Subset of available scenarios for UMTS

The main reason for scenarios is to limit the data what is required and to speed up correlation. Scenarios may be predefined as a global trace like “give me all”, where you would attempt to correlate all interfaces in the entire network or as a specific trace always concerned with a specific path or even a specific area or dialogs. Scenarios are flexible in the sense that they may be changed by Anritsu or the customer using a correlation language defined in an ordinary text file.

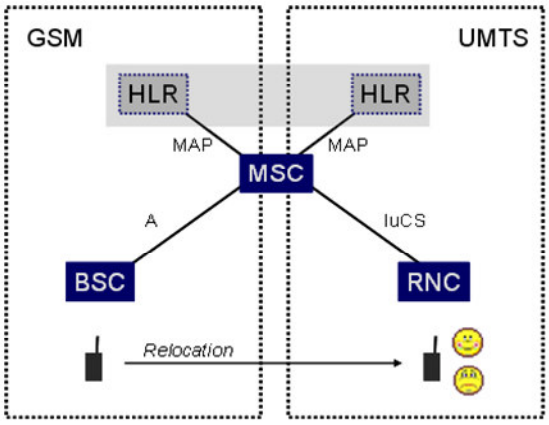

Figure 6: Inter-RAT Handover - GSM to UMTS

An example of a dialogue could be a Routing Area Update or as shown in Figure 7, a failed Attach procedure.

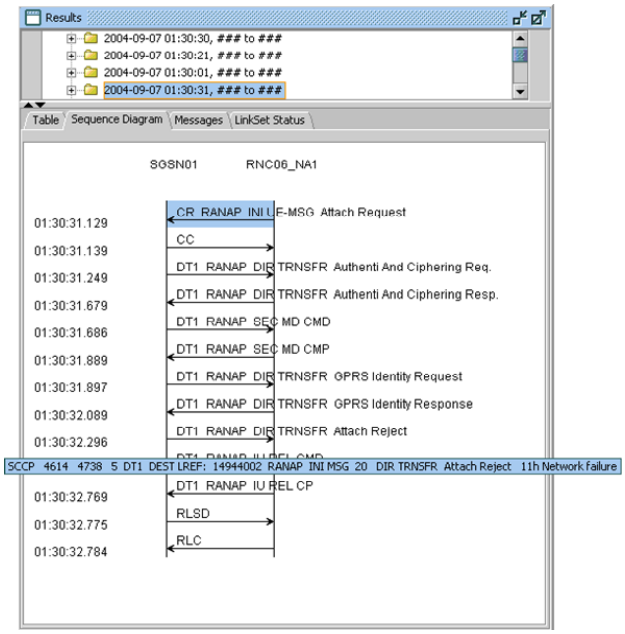

Figure 7: Simple IuPS dialogue trace with failed Attach procedure

MasterClaw call and session trace can also correlate individual dialogues together to form multi-interface session or call traces as shown in Figures 7, 8 and 9.

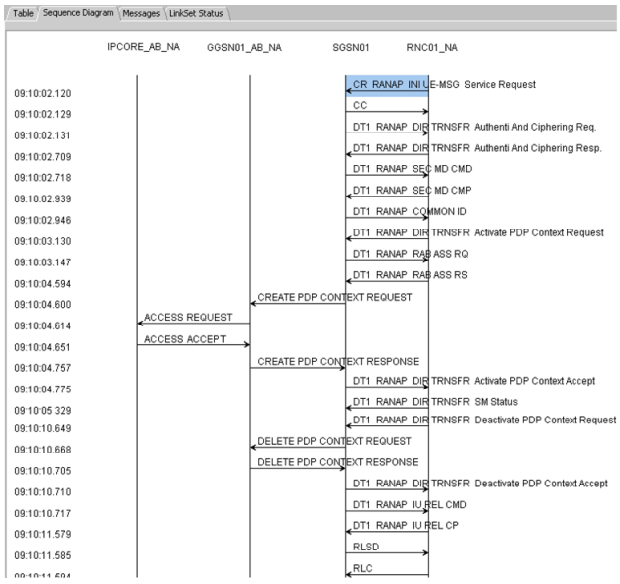

Figure 8: Example of multi interface scenario trace of PDP context activation

Figure 8 displays a packet domain trace including RANAP, GTP and RADIUS. The mobile Activate PDP context goes from the RNC to the SGSN on the IuPS interface, where after the SGSN checks the request against the subscription information previously updated from the HLR. Then the SGSN sends a Create PDP context request to the GGSN on the Gn interface, which in turn checks the subscriber authentication and account in the RADIUS server on the Gi interface.

Circuit domain traces may be a mobile to mobile call within the same network, a mobile to PSTN call, PSTN to mobile call or mobile originating or mobile terminating SMS. Use of IN services like CAMEL may further increase the number of scenarios.

An example of a circuit domain trace is shown in Figure 9, covering a PSTN to mobile call including ISUP, MAP and RANAP. In the example the ISUP call enters the gateway server via an STP node, causing a query to the HLR which provides a temporary roaming number to the MSC covering the subscriber. The MSC is called using ISUP and the roaming number and the mobile is paged using RANAP towards the RNC. If the Node-B's were monitored this could also have been displayed in the sequence diagram.

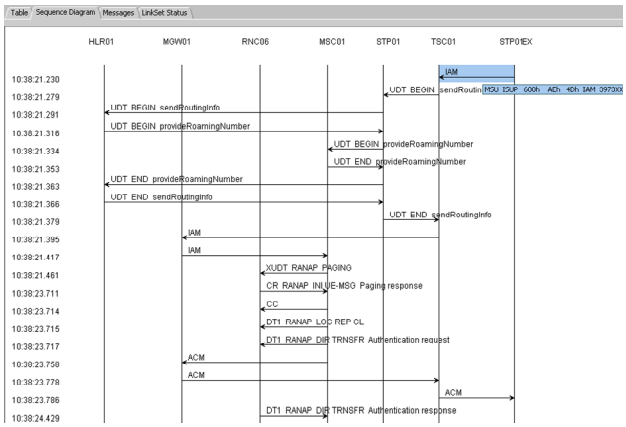

Figure 9: Sample of multi interface scenario trace of PSTN to mobile call

Figure 10 shows a trace where RANAP, MAP, BICC and CAMEL are correlated together. Besides from the sequence diagram the messages may be individually decoded by clicking on the arrows or all messages may at the same time be decoded using the Messages tap.

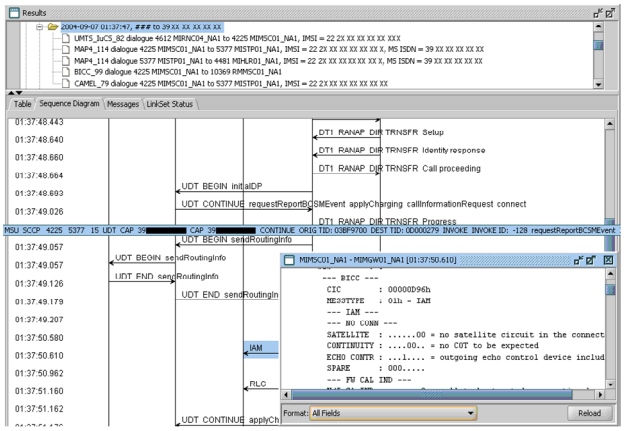

Figure 10: Sample of multi interface scenario of RANAP, MAP, CAP and BICC

Instead of sequence diagrams parameters may also be displayed in a table view, which is customizable by the MasterClaw call and session trace user. The sequence diagram shows the direction and order of flow whereas the table views show the end result, parameter by parameter. An example of some of the parameters available for the RANAP protocol is shown in Figure 11. The user may choose to add or remove fields from the table or to change the order. The number of fields available is in the order of 25 to 100 fields depending on the actual protocol.

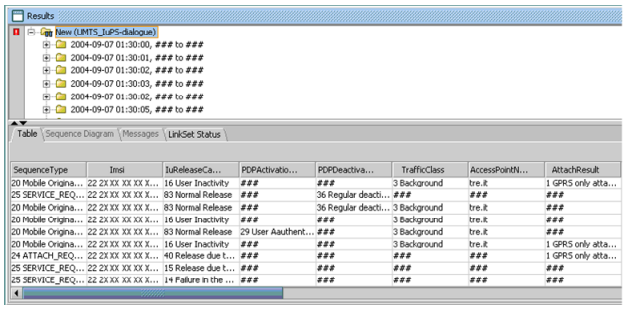

Figure 11: Example of table view for simple RANAP dialogue

Usage of Call and Session Trace

Call and session trace can be used by different departments with different levels of network and protocol knowledge. For a first line customer care center a simple push button system can be used and for more advanced users a more detailed set-up is possible.

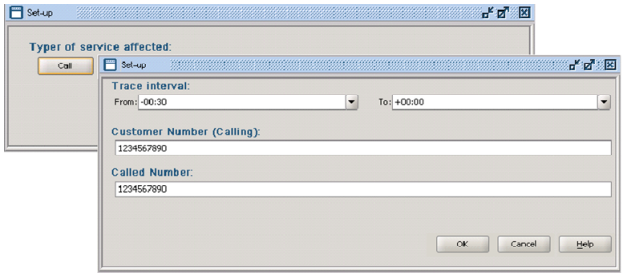

Figure 12: Example of customer care usage for tracing an ordinary ISUP call

After choosing the scenario one or more filter settings may be applied. The filtering options available differ from scenario to scenario.
When a scenario is selected the trace can be started. In most cases however further filtering or another time interval will be needed.

Filtering is used to limit the number of calls or sessions in the result. Filtering on IMSI for instance can be used to trace the activities of a specific subscriber or a series of subscribers, like all subscribers from a specific operator or country. Other filters like RANAP procedure type, APN and MSISDN are commonly used filters to get information on specific procedures, services or network nodes. The filters can also be used to make statistics on e.g. how many PDP contexts failed to access a specific APN from 12:00 to 13:00 o'clock.

Depending on the type of protocol, between 25 to 100 different parameters are available. Each of the parameters represents an information element.

An example of a filter applied to the Ericsson GCP General Cause field is shown in Figure 13.

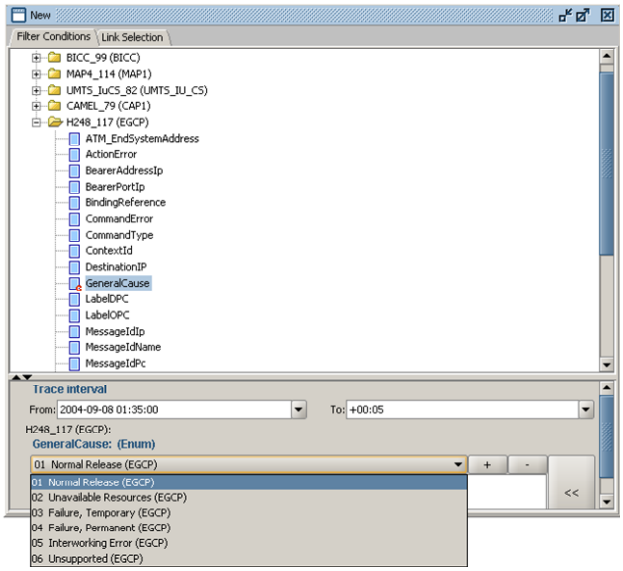

Figure 13: Example of filters available for EGCP

After entering the filter options the trace is started by activating the start button. The result appears in the result window as they are found.

Results are presented in traces in the result window and each trace and procedure may be examined even while the search is ongoing.

A trace may also be setup to end in the future, and may in this way be used as trigger to find specific traces like a test call.

The result of a trace may be saved for later usage. For example a customer complaint may be handled by the customer support department and the trace of the subscriber can then be passed on to the next support level that then do not need to make another trace but can immediately see the results and the filters used.

How Does it Work

MasterClaw call and session trace is based on distributed processing power and hence provide results very fast. In a troubleshooting situation you want to have quick response to your ad-hoc request, you simply do not want to wait for an application to decode through all the messages you want to search on parameters already decoded. The advantage of this becomes apparent when one wants to search for the subscriber activities of a specific subscriber e.g. in the last 24 hours or the last week.

All probes correlate the procedures and generate parameterized records that are stored locally on the probe hard disk. No back hauling of traffic or centralized probe or storage sever is needed. The Call and Session Trace application sends a request to some or all probes with the search parameters e.g. “APN=’internet AND IMSI=123*”. The response to these request are sent to the Call and Session Trace server that may do further correlation if needed. Multiple call traces can be performed simultaneously, hence not limiting this to a single user at a time.

This makes MasterClaw call and Session trace very scalable and very fast. Adding more probes is not an issue because the scaling is horizontal. The records contain references to all the messages it is based on, meaning that all messages and information elements can be viewed if required. The Call and Session Trace and probe interaction is illustrated in Figure 14.

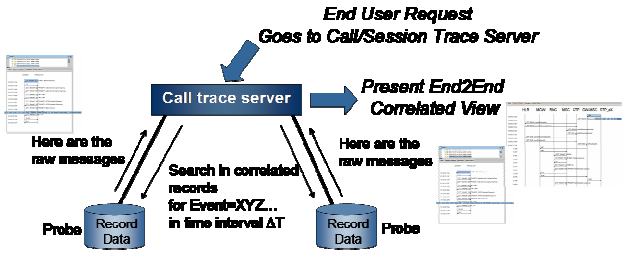

Figure 14: Probe and Call and Session Trace server interaction

Depending on the chosen scenario the Call and Session Trace server may issue a request for data from multiple interfaces, e.g. an IuPS and Gn scenario will search in both IuPS records and in Gn records and will correlate them together in the Call and Session Trace server.

The probes them selves are usually located around core nodes such as the SGSNs, around a media gateway or around STPs. An example of such deployment is shown below in Figure 15.

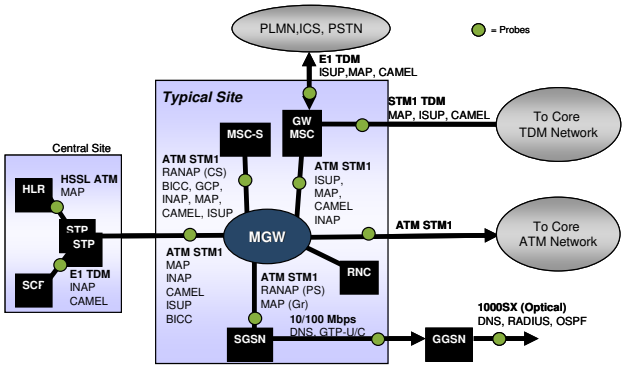

Figure 15: Probe location within a theoretical UMTS Release 4 network

Security Options

An optional security package provides restrictions on which features can be used and what information can be seen depending on the user’s access rights. For example phone numbers, SMS text and other information can be masked in a way that ensures the confidentiality of the subscriber.

MasterClaw Call and Session Trace may be launched from the MasterClaw Portal. When the user logs in to the MasterClaw WEB Portal this is with a single sign-on that

reflects all applications, which can be launched from the Portal. When launching MasterClaw Call and Session Trace the user activities are logged in a protected log only accessible by the administrator. From this log it is possible to see which user used which trace criteria and when.

Summary

MasterClaw call and session trace is a full network wide application that is both easy to use and very quickly deliver the results.

MasterClaw Call and Session Trace is easy to use because it hides the complexity for the end user, e.g. the dialog correlation is done in advance and relevant parameters are available for filtering. The client may run on both Windows and Linux platforms. MasterClaw Call and Session Trace application provides options to ensure the confidentiality of the subscribers if needed and additionally log the activity of the Call and Session Trace users.

A call/session trace may be launched on the behalf of another application and the results may be stored in a file for processing by the other application.

Combined with MasterClaw link and message statistics, Protocol Analysis and Alarm Manager, MasterClaw Call and session trace is a very powerful application that can be used for fast troubleshooting in UMTS, GSM, PSTN, VoIP, GPRS and Edge networks.

ISO 9001:2000 certified. ©2006 Anritsu. All Rights Reserved.
Specifications subject to change without notice. E&EO. 0606

Anritsu A/S
Kirkebjerg Allé 90
DK-2605 Brøndby, Denmark
Tel: +45 72 11 22 00
Fax: +45 72 11 22 10
E-mail: nordic.support@anritsu.com
Web: www.anritsu.com

Headquarter:
Japan +81-46-223-11111
Sales Offices:
Hong Kong +852-2301-4980
UK +44 (0) 1582-433 200
USA +1-972-644-1777
USA toll free +1-800-ANRITSU (267-4878)