Session Tracing

Session Tracing allows an operator to trace subscriber activity at various points in the network and at various levels of detail in an EPS network. This chapter provides information on how the MME implements subscriber Session Tracing functionality in the LTE service.

- Feature Description, on page 1
- How Session Tracing Works, on page 3
- Session Trace Configuration, on page 7
- Monitoring and Troubleshooting the Session Trace, on page 11

Feature Description

The Session Tracing feature provides a 3GPP standards-based subscriber session-level trace function for call debugging and testing new functions and access terminals in an LTE environment.

In general, the Session Trace capability records and forwards all control activity for the monitored subscriber on the monitored interfaces. This is typically all the signaling and authentication/subscriber services messages that flow when a UE connects to the access network.

The EPC network entities like MME, S-GW, P-GW support 3GPP standards based session-level trace capabilities to monitor all call control events on the respective monitored interfaces including S6a, S1-MME and S11 on MME, S5, S8, S11 at S-GW and S5 and S8 on P-GW. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a reference interface
- Signaling-based activation through signaling from subscriber access terminal

Important Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

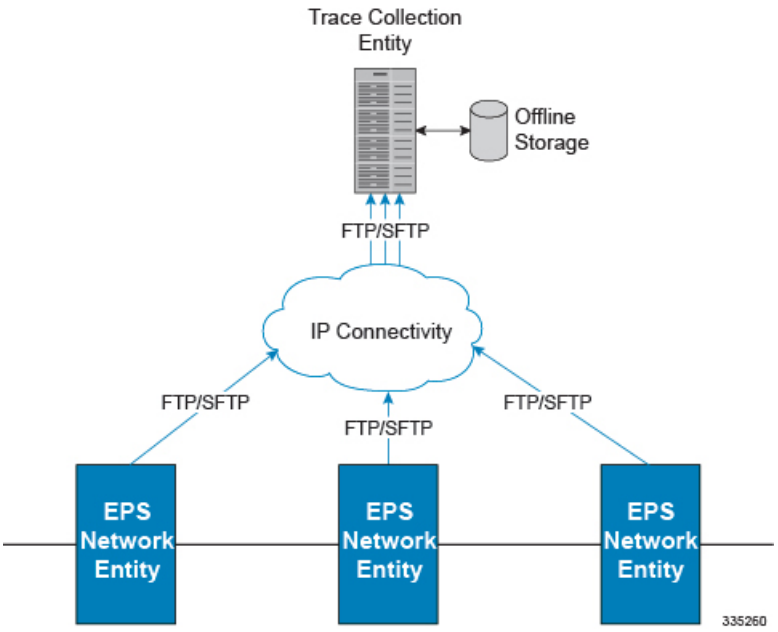
The session level trace function consists of trace activation followed by triggers. The time between the two events is where the EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the chassis. The trace depth defines the granularity of data

to be traced. Six levels are defined including maximum, minimum and medium with ability to configure additional levels based on vendor extensions.

Important Only maximum trace depth is supported.

The following figure shows a high-level overview of the session-trace functionality and deployment scenario:

Figure 1: Session Trace Function and Interfaces



All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a FTP or secure FTP (SFTP) connection.

Note: The IPv4 interfaces are used to provide connectivity to the TCE. trace activation is based on IMSI or IMEI.

Supported Functions

This section provides the list of supported functionality of this feature support:

- Support to trace the control flow through the access network.
  - Trace of specific subscriber identified by IMSI
  - Trace of UE identified by IMEI(SV)
- Ability to specify specific functional entities and interfaces where tracing should occur.
- Scalability and capacity
  - Support up to 32 simultaneous session traces per MME
  - Each MME is equipped with a storage buffer of size 40 MB to collect trace files locally
- Statistics and State Support

- Session Trace Details
- Management and Signaling-based activation models
- Trace Parameter Propagation
- Trace Scope (EPS Only)
  - MME: S10, S11, S13, S1-MME, S3, S6A
  - S-GW: S4, S5, S8, S11, Gxc
  - PDN-GW: S2a, S2b, S2c, S5, S6b, Gx, S8, SGi
- Trace Depth: Maximum, Minimum, Medium (with or without vendor extension)
- XML Encoding of Data as per 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09)
- Trace Collection Entity (TCE) Support
  - Active pushing of files to the TCE
  - Passive pulling of files by the TCE
- 1 TCE support per context
- Trace Session Recovery after Failure of Session Manager

Standards Compliance

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- 3GPP TS 32.421 V10.5.0: 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Telecommunication management Subscriber and equipment trace: Trace concepts and requirements (Release 10)
- 3GPP TS 32.422 V10.5.0: 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Telecommunication management Subscriber and equipment trace Trace control and configuration management (Release 10)
- 3GPP TS 32.423 V10.5.0: 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Telecommunication management Subscriber and equipment trace: Trace data definition and management (Release 10)

How Session Tracing Works

This section describes the various functionality involved in tracing subscriber sessions on EPC nodes.

Operation

The session trace functionality is separated into two steps - activation and trigger.

Before tracing can begin, it must be activated. Activation is done either via management request or when a UE initiates a signaled connection. After activation, tracing actually begins when it is triggered (defined by a set of trigger events).

Trace Session

A trace session is the time between trace activation and trace de-activation. It defines the state of a trace session, including all user profile configuration, monitoring points, and start/stop triggers. It is uniquely identified by a Trace Reference.

The Trace Reference id is composed of the MCC (3 digits) + the MNC (3 digits) + the trace Id (3 byte octet string).

Important On a session manager failure, the control activity that has been traced, but not written to file, will be lost. However, the trace sessions will continue to persist and future signals will be captured as expected.

Trace Recording Session

A trace recording session is a time period in which activity is actually being recorded and traceable data is being forwarded to the TCE. A trace recording session is initiated when a start trigger event occurs and continues until the stop trigger event occurs and is uniquely identified by a Trace Recording Session Reference.

Network Element (NE)

Network elements are the functional component to facilitate subscriber session trace in mobile network.

The term network element refers to a functional component that has standard interfaces in and out of it. It is typically shown as a stand-alone AGW. Examples of NEs are the MME, S-GW, and P-GW.

Currently, subscriber session trace is not supported for co-located network elements in the EPC network.

Activation

Activation of a trace is similar whether it be via the management interface or via a signaling interface. In both cases, a trace session state block is allocated which stores all configuration and state information for the trace session. In addition, a (S)FTP connection to the TCE is established if one does not already exist (if this is the first trace session established, odds are there will not be a (S)FTP connection already established to the TCE).

If the session to be traced is already active, tracing may begin immediately. Otherwise, tracing activity concludes until the start trigger occurs (typically when the subscriber or UE under trace initiates a connection). A failure to activate a trace (due to max exceeded or some other failure reason) results in a notification being sent to the TCE indicating the failure. If the (S)FTP connection is not established with the TCE, the TCE connectivity needs to checked. Nevertheless, the MME continues to send the trace files to the TCE, and tries to establish an (S)FTP connection. The MME provides a storage buffer of size 40 MB to collect the trace files locally.

Management Activation

The Operator can activate a trace session by directly logging in to the NE and enabling the session trace (for command information, see *Enabling Subscriber Session Trace on EPC Network Element* section below). The NE establishes the trace session and waits for a triggering event to start actively tracing. Depending upon the configuration of the trace session, the trace activation may be propagated to other NEs.

Signaling Activation

With a signaling based activation, the trace session is indicated to the NE across a signaling interface via a trace invocation message. This message can either be piggybacked with an existing bearer setup message (in order to trace all control messages) or by sending a separate trace invocation message (if the user is already active).

Start Trigger

A trace recording session starts upon reception of one of the configured start triggers. Once the start trigger is received, the NE generates a Trace Recording Session Reference (unique to the NE) and begins to collect and forward trace information on the session to the TCE.

List of trigger events are listed in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

Deactivation

Deactivation of a Trace Session is similar whether it was management or signaling activated. In either case, a deactivation request is received by the NE that contains a valid trace reference results in the de-allocation of the trace session state block and a flushing of any pending trace data. In addition, if this is the last trace session to a particular TCE, the (S)FTP connection to the TCE is released after the last trace file is successfully transferred to the TCE.

Stop Trigger

A trace recording session ends upon the reception of one of the configured stop triggers. Once the stop trigger is received, the NE will terminate the active recording session and attempt to send any pending trace data to the TCE. The list of triggering events can be found in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

Data Collection and Reporting

Subscriber session trace functionality supports data collection and reporting system to provide historical usage and event analysis.

All data collected by the NE is formatted into standard XML file format and forwarded to the TCE via (S)FTP. The specific format of the data is defined in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09)

Trace Depth

The Trace Depth defines what data is to be traced. There are six depths defined: Maximum, Minimum, and Medium all having with and without vendor extension flavors. The maximum level of detail results in the entire control message getting traced and forwarded to the TCE. The medium and minimum define varying subsets of the control messages (specific decoded IEs) to be traced and forwarded. The contents and definition of the medium and minimum trace can be found in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09).

Important Only Maximum Trace Depth is supported.

Trace Scope

The Trace Scope defines what NEs and what interfaces have the tracing capabilities enabled on them. This is actually a specific list of NE types and interfaces provided in the trace session configuration by the operator (either directly via a management interface or indirectly via a signaling interface).

Network Element Details

Trace functionality for each of the specific network elements supported by this functionality are described in this section.

This section includes the trace monitoring points applicable to them as well as the interfaces over which they can send and/or receive trace configuration.

MME

The MME supports tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S1a	eNodeB	N	Y
S3	SGSN	Y	Y
S6a	HSS	Y	N
S10	MME	Y	Y
S11	S-GW	N	Y
S13	EIR	N	N

S-GW

The S-GW supports tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S1-U	eNodeB	Y	N
S4	SGSN	N	N
S5	P-GW (Intra-PLMN)	Y	N
S8	P-GW (Inter-PLMN)	N	N
S11	MME	Y	N
S12	RNC	Y	N
Gxc	Policy Server	Y	N

P-GW

The P-GW supports tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S2abc	Various NEs	N	N
S5	S-GW (Intra-PLMN)	Y	N
S6b	AAA Server/Proxy	Y	N
S8	S-GW (Inter-PLMN)	N	N
Gx	Policy Server	Y	N
SGi	IMS	Y	N

Session Trace Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system to enable the Subscriber Session Trace collection and monitoring function on network elements s in LTE/EPC networks.

Important This section provides the minimum instruction set to enable the Subscriber Session Trace functionality to collect session traces on network elements on EPC networks. Commands that configure additional function for this feature are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in the *System Administration Guide* and specific product Administration Guide.

To configure the system to support subscriber session trace collection and trace file transport on a system:

Step 1 Enable the subscriber session trace functionality with NE interface and TCE address at the Exec Mode level on an EPC network element by applying the example configurations presented in the *Enabling Subscriber Session Trace on EPC Network Element* section.

Step 2 Configure the network and trace file transportation parameters by applying the example configurations presented in the *Trace File Collection Configuration* section.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Step 4 Verify the configuration of Subscriber Session Trace related parameters by applying the commands provided in the *Verifying Your Configuration* section of this chapter.

Enabling Subscriber Session Trace on EPC Network Element

This section provides the configuration example to enable the subscriber session trace on a system. Enter a command similar to the following in the Exec mode:

session trace subscriber network-element mme template-name *template_name* **{ imei** *imei_id* **| imsi** *imsi_id* **} trace-ref** *trace_ref_id* **collection-entity** *ip_address*

Notes:

- *template_name* specifies the name of the session trace template. This template must be configured by using the **template-session-trace** command in the Global Configuration mode.
- **imsi** *imsi_id* specifies the International Mobile Subscriber Identification Number for the subscriber.
- **imei** *imei_id* specifies the International Mobile Equipment Identification Number for the subscriber.
- **trace-ref** *trace_ref_id* is the configured Trace Id to be used for the present trace collection instance. It is composed of MCC (3 digit)+MNC (3 digit)+Trace Id (3 byte octet string).
- **collection-entity** *ip_address* specifies the IP address of the Trace Collection Entity (TCE) to which the trace file generated will be sent. The IP address must be in IPv4 format.

Configuring a Session Trace Template for the MME

Operators have the option of creating a template for a management trace in configuration mode for the MME. Session traces executed in the Exec mode will use this template. Once created, the template can be associated with different subscribers to trace the interfaces configured in the template.

Important To activate subscriber session traces for specific IMSI/IMEI, the operator must use the Exec mode **session trace subscriber** command specifying a pre-configured template and the IMSI/IMEI, trace reference and TCE address.

To configure a template-session-trace, use the following configuration:

```
configure
   template-session-trace network-element mme template-name template_name
      interface { all | s10 | s11 | s13 s1mme | s3 | s6a
      target-ne { all | enb | pgw | sgwall | sgw } [ target-interface [
all | s1mme | uu | x2 ] } }     end
      end
```

Notes:

- Available **interface** options for MME include:
  - **all:** Sets the trace to be performed on all interfaces from the MME.
  - **s10:** Sets the trace to be performed on the S10 interface between the MME and another MME.
  - **s11:** Sets the trace to be performed on the S11 interface between the MME and the S-GW.
  - **s13:** Sets the trace to be performed on the S13 interface between the MME and the EIR.
  - **s1mme:** Sets the trace to be performed on the S1-MME interface between the MME and the eNodeB.
  - **s3:** Sets the trace to be performed on the S3 interface between the MME and an SGSN.
  - **s6a:** Sets the trace to be performed on the S6a interface between the MME and the HSS.

- **target-ne** initiates tracing towards peer network elements and available options include:
  - **all:** Initiates the trace towards all NEs.
  - **enb:** Initiates the trace towards the eNodeBs.
  - **pgw:** Initiates the trace towards the P-GWs.
  - **sgw:** Initiates the trace towards the S-GWs.
- Available **target-interface** specifies the interface for the selected Network Element for tracing and options for **enb** are as follows:
  - **all:** Identify all interfaces between the MME and eNodeB.
  - **s1mme:** Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
  - **uu:** Specifies that the interface where the trace will be performed is the UU interface between the MME and the eNodeB.
  - **x2:** Specifies that the interface where the trace will be performed is the X2 interface between the MME and the eNodeB.
- Available **target-interface** options for **pgw** are as follows:
  - **all**
  - **gx:** Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **s2a:** Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.
  - **s2b:** Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
  - **s2c:** Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.
  - **s5:** Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s6b:** Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
  - **s8:** Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
  - **sgi:** Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.
- Available **target-interface** options for **sgw** are as follows:
  - **all**
  - **gxc:** Specifies that the interface where the trace will be performed is the Gx interface between the PGW and the PCRF.
  - **s11:** Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
  - **s4:** Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and the SGSN.
  - **s5:** Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s8:** Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.

Trace File Collection Configuration

This section provides the configuration example to configure the trace fil e collection parameters and protocols to be used to store trace files on TCE through FTP/S-FTP:

```
configure
  session trace subscriber network-element { all | ggsn | mme | pgw | sgw
 } [ collection-timer dur ] [ tce-mode { none | push transport { ftp |
sftp } path string username name { encrypted password enc_pw ] | password
password } } ]
  end
```

Notes:

- *string* is the location/path on the trace collection entity (TCE) where trace files will be stored on TCE. For more information, refer to the session trace command in the *Command Line Interface Reference*.

Verifying Your Configuration

This section explains how to display and review the configurations after saving them in a .cfg file as described in the *System Administration Guide* and also to retrieve errors and warnings within an active configuration for a service.

Important All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the Subscriber Session Trace configuration.

Step 1 Verify that your subscriber session support is configured properly by entering the following command in Exec Mode:

show session trace statistics

The output of this command displays the statistics of the session trace instance.

```
Num current trace sessions: 5
Total trace sessions activated:  15
Total Number of trace session activation failures:  2
Total Number of trace recording sessions triggered:  15
Total Number of messages traced:  123
Number of current TCE connections:  2
Total number of TCE connections: 3
Total number of files uploaded to all TCEs:  34
```

Step 2 View the session trace references active for various network elements in an EPC network by entering the following command in Exec Mode:

show session trace trace-summary

The output of this command displays the summary of trace references for all network elements:

```
MME
    Trace Reference:  310012012345
    Trace Reference:  310012012346
SGW
    Trace Reference:  310012012345
    Trace Reference:  310012012346
```

```
PGW
    Trace Reference:  310012012347
```

Monitoring and Troubleshooting the Session Trace

The following section describes commands available to monitor Session Trace functionality on the MME.

Session Trace Show Command(s) and/or Outputs

show session trace statistics

On running the above mentioned show command, statistics similar to the following are displayed:

- Number of current trace sessions
- Number of total trace sessions
- Total sessions activated
- Number of activation failures
- Number of sessions triggered
- Total messages traced
- Number of current TCE connections
- Total number of TCE connections
- Total number of files uploaded to all TCEs

show session trace subscriber network-element trace-ref

This command shows detailed information about a specific trace, based on the trace-ref value of the session and network element type. It includes activation time, IMSI, start time, number of trace messages, and total number of files created. It also lists the interfaces that this session trace is configured to track.

The following command displays the summary of a Session Trace for a particular Reference Id

show session trace subscriber network-element mme trace-ref 310012012345

```
Trace Reference:    310012012345
      Activation time:  Fri Jul 10 16:19:10 2009
      IMSI:  0000012345
      Actively Tracing:  yes
      Trace Recording Session Reference:  1
      Recording start time:  Fri Jul 10 16:19:10 2009
      Total number of trace recording sessions triggered:  1
      Total number of messages traced:  32
      Total number of files created:  5
      Traced Interfaces:
            S1mme
            S6a
            S11
      Trace Triggers:
            service-request
            initial-attach
            ue-disconnect
            bearer-activation
```

```
      handover
Target Network Elements:
      SGW
      Target Interfaces
           S8b
           S11
```

show session trace tce-summary

This command provides the IP address and index information for all configured TCEs. The following fields are displayed on executing the above command:

```
TCE IP Address:
      Index 1
TCE IP Address:
      Index 5
```

show session trace tce-address

This command provides detailed information about a specific TCE, including IP address, start time, and total number of files uploaded.

The following example displays the summary of a Session Trace for a particular Refernence Id

`show session trace tce-address 10.172.1.5 tce-index 5`

```
TCE IP Address:    10.172.1.5
      Start time:  Fri Jul 10 16:19:10 2009
      Total number of files uploaded:  12
```