MAE
V100R020C10

Trace Server LTE Standard Signaling Northbound File Interface Developer Guide

Issue	**01**
Date	**2020-05-31**


HUAWEI

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Preface

Purpose

This document provides information about the Trace Server northbound trace result file interface. It also provides guidance for interconnecting with the network management system (NMS).

NOTICE

When Trace Server collects NE data, such as, CHR, MR, and trace data, filters the data, and provides the data for the NMS, collection, storage, and transmission of personal data, such as MSISDNs, IMSIs, IMEIs, and cell IDs are involved. If the storage directory space or the storage duration reaches specified thresholds, data will be automatically deleted. The personal data in the content provided to NMS users is protected by the NMS. Sensitive data sources provided by NEs can be anonymized, and Trace Server provides the anonymization capability when data is moved out of the live network. To ensure personal data security, comply with applicable state laws or enterprise privacy policies and take sufficient measures.

Intended Audience

This document is intended for upgrade engineers. Upgrade engineers must:

- Be familiar with the current network topology and the version information of related NEs.
- Have device maintenance experience and be familiar with device operation and maintenance methods.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.

Symbol	Description
⚠ CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Contents

1 Overview of the Northbound Trace Result File Interface

About This Chapter

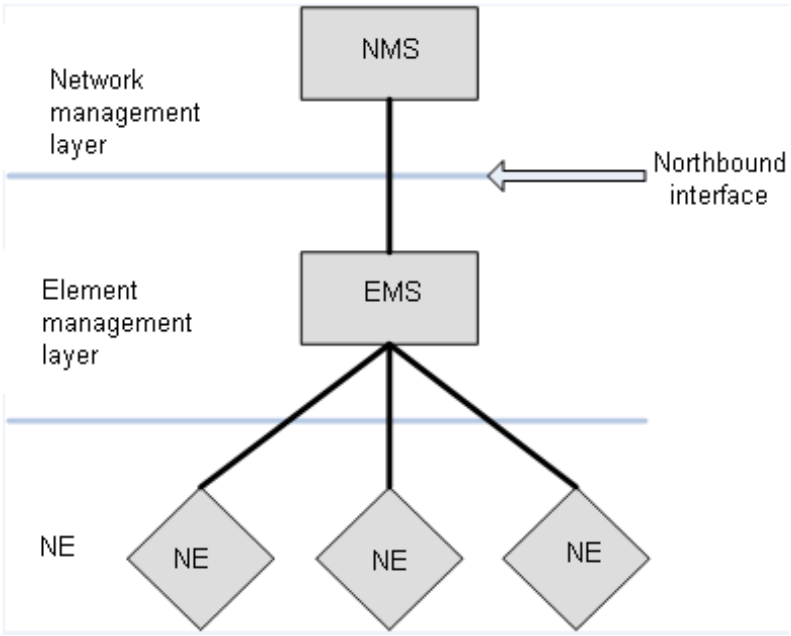
This chapter describes the definitions of the northbound interface and northbound trace result file interface provided by Trace Server.

1.1 Definition of the Northbound Interface

The northbound interface is the interface between the element management system (EMS) and the NMS.

The NMS obtains NE data, such as NE trace result data, from the EMS and issues commands over the northbound interface. Figure 1-1 shows the northbound interface.

Figure 1-1 Northbound interface



1.2 Definition of the Northbound Trace Result File Interface

The Trace Server northbound trace result file interface is a northbound interface, over which the NMS can obtain northbound trace result files stored on Trace Server.

Trace Server northbound trace result file supports the following protocols for transferring northbound trace result files:

- File Transfer Protocol (FTP): common FTP protocol
- Secure File Transfer Protocol (SFTP): SSH-based FTP transfer protocol

NOTE

SFTP is recommended because it is more secure than FTP.

1.3 Technical Specifications for the Northbound Trace Result File Interface

Table 1-1 describes the technical specifications for the Trace Server LTE northbound file interface.

Table 1-1 Technical specifications for the Trace Server LTE northbound file interface

Specification	Value
Maximum period (hour) during which	72

Specification	Value
northbound trace result files can be stored on the Trace Server server	
Maximum size (GB) of northbound trace result files that can be stored on the Trace Server server	180
Maximum size (GB) of northbound trace result files that can be stored on the shared space	256 **NOTE** • If the size of files saved on the shared space is less than 256 GB and the storage period does not expire, the northbound trace result files generated by Trace Server northbound trace result file are not deleted. • If the size of files saved on the shared space is greater than 256 GB and the storage period does not expire, other files generated by application systems and northbound trace result files generated are deleted in sequence before sizes of the files are less than their respective storage specifications or the size of files saved on the share space is less than 256 GB. • If the space usage of the **export/home** directory is higher than 80%, data is deleted from the shared space.
Maximum size (GB) of northbound trace result files that can be stored on a high-specification VM	720
Maximum size (GB) of northbound trace result files that can be stored on the shared space of a high-specification VM	1024 **NOTE** • If the size of files saved on the shared space of the high-specification VM is less than 1024 GB and the storage period does not expire, northbound trace result files are not deleted. • If the size of files saved on the shared space of the high-specification VM is greater than 1024 GB and the storage period does not expire, other files generated by application systems and northbound trace result files are deleted in sequence before sizes of the files are less than their respective storage specifications or the size of files saved on the share space of the high-specification VM is less than 1024 GB. • If the space usage of the **export/home** directory is higher than 80%, data is deleted from the shared space.

2 Overview of Northbound Trace Result Files

About This Chapter

This section describes the northbound trace result files for users to easily locate and obtain the files.

NOTE

To obtain result samples, contact Huawei technical support.

2.1 Types of Standard Signaling Northbound Result Files

Trace Server generates northbound result files based on NE data types.

The LTE standard signaling complies with the OSSii protocol and 3GPP specifications.

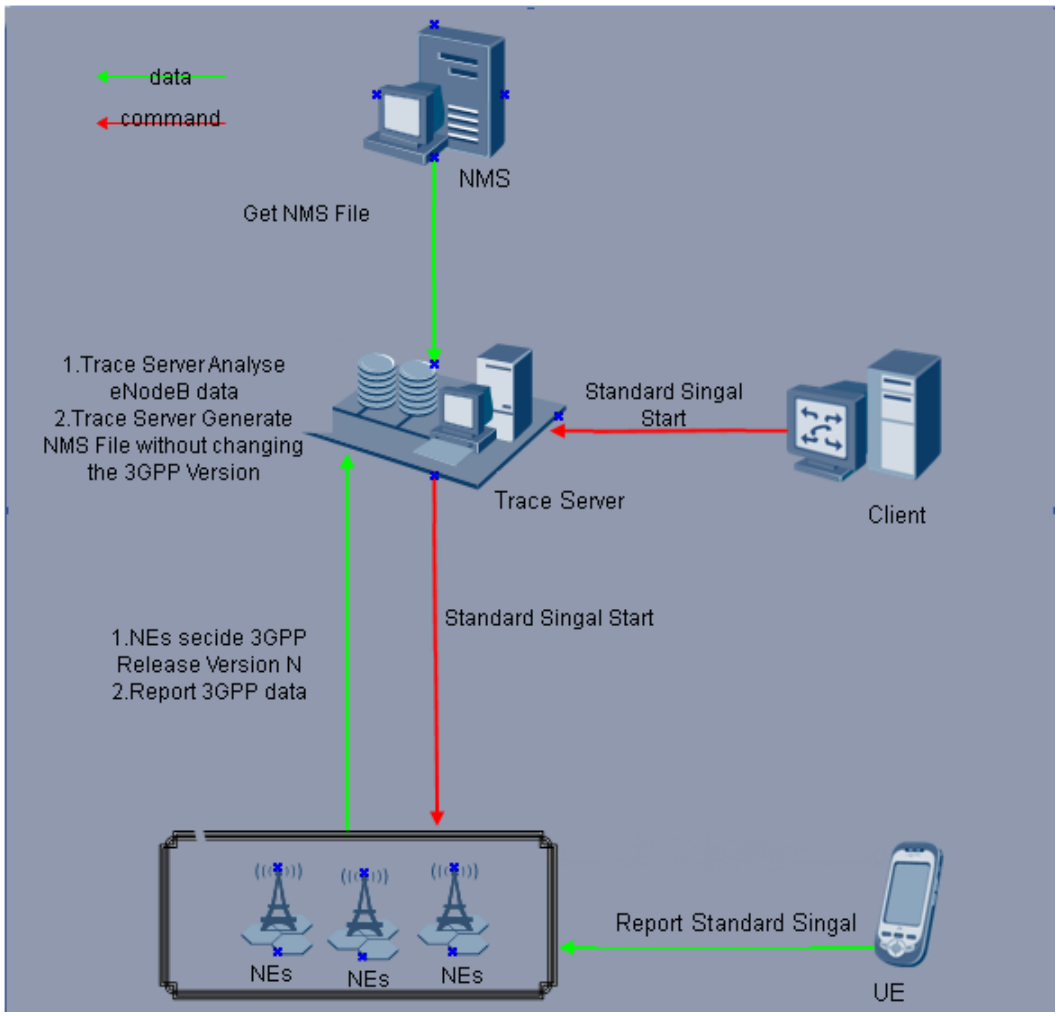
Table 2-1 Compliance relationship between LTE software release and 3GPP specifications

NE Software Release	3GPP Interface	3GPP Release
SRAN13.x	S1	3GPP TS 36.413 Release 13
	X2	3GPP TS 36.423 Release 13
	Uu	3GPP TS 36.331 Release 13
Pico 13.x	S1	3GPP TS 36.413 Release 13
	X2	3GPP TS 36.423 Release 13

NE Software Release	3GPP Interface	3GPP Release
	Uu	3GPP TS 36.331 Release 13
SRAN15.x	S1	3GPP TS 36.413 Release 15
	X2	3GPP TS 36.423 Release 15
	Uu	3GPP TS 36.331 Release 15
Pico 15.x	S1	3GPP TS 36.413 Release 15
	X2	3GPP TS 36.423 Release 15
	Uu	3GPP TS 36.331 Release 15
SRAN16.x	S1	3GPP TS 36.413 Release 16
	X2	3GPP TS 36.423 Release 16
	Uu	3GPP TS 36.331 Release 16
Pico 16.x	S1	3GPP TS 36.413 Release 16
	X2	3GPP TS 36.423 Release 16
	Uu	3GPP TS 36.331 Release 16

The 3GPP Release version is confirmed by an eNodeB. When reporting a message, the eNodeB identifies the UE 3GPP Release version and confirms the 3GPP Release version. Figure 2-1 shows the specific procedure.

Figure 2-1 Procedure for Trace Server to generate a standard signaling northbound file



The following scenarios indicate the 3GPP Release version used by the NMS and the 3GPP Release version defining messages reported by an eNodeB.

- The NMS uses 3GPP Release N, and the eNodeB reports messages defined in 3GPP Release N – X (X ≥ 1).

  The 3GPP Release version is compatible with earlier versions. If the NMS uses the ASN in 3GPP Release N to decode 3GPP Release N – X (X ≥ 1) data, the NMS can parse all messages and message fields reported by the eNodeB to obtain all required information. For example, if the eNodeB reports 10 messages with 100 fields, the NMS obtains all messages and fields.

- The NMS uses 3GPP Release N, and the eNodeB reports messages defined in 3GPP Release N.

  If the NMS uses the ASN in 3GPP Release N to decode 3GPP Release N data, indicating that the same 3GPP version is used, the NMS can parse all messages and message fields reported by the eNodeB to obtain all required information. For example, if the eNodeB reports 10 messages with 100 fields, the NMS obtains all messages and fields.

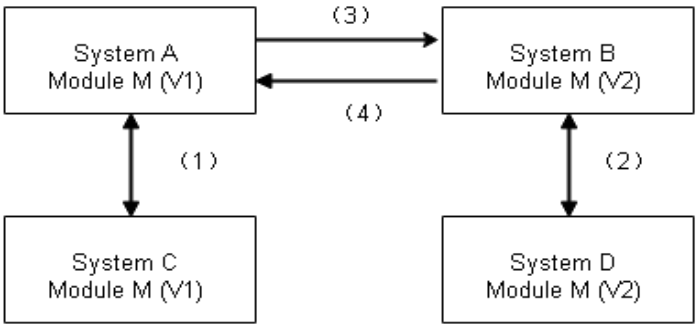
- The NMS uses 3GPP Release N, and the eNodeB reports messages defined in 3GPP Release N + X (X ≥ 1).

If the NMS uses the ASN.1 in 3GPP Release N to decode 3GPP Release N + X (X ≥ 1) data, indicating that the 3GPP version used by the NMS is earlier than that defining messages reported by the eNodeB, the NMS cannot obtain messages and fields reported by the eNodeB in either of the following cases.

- If the eNodeB reports a message added in 3GPP Release N + X, the NMS cannot parse this message. For example, if the eNodeB reports 10 messages containing one message added in 3GPP Release N + X and nine messages defined in 3GPP Release N, the NMS obtains only these 3GPP Release N-defined messages.
- If an eNodeB-reported message is defined in both 3GPP Release N + X and 3GPP Release N and a field of this message is added in 3GPP Release N + X, the NMS cannot obtain this field. For example, if the eNodeB reports a message with 100 fields, including 10 fields added in 3GPP Release N + X and 90 fields defined in 3GPP Release N, the NMS obtains only these 3GPP Release N-defined fields.

The preceding scenarios are described in ASN.1 design specifications. Figure 2-2 displays ASN.1 encoding and decoding rules for different versions and systems.

Figure 2-2 ASN.1 encoding and decoding rules for different systems



	If System	sends data to syste	Then
(1)	A C	C A	Everything goes well because both A and C have the same version (v1) of the ASN.1 specifivation
(2)	B D	D B	Everything goes well because both B and D have the same version (v2) of the ASN.1 specifivation
(3)	A	B	B does not receive all the data expected but should be able to recover
(4)	B	A	A receives too much data but should be able to ignore them

NOTE

Compared with the eNodeB-dedicated 3GPP Release version, the UE-dedicated 3GPP Release version is updated slowly. You are advised to configure the latest eNodeB-dedicated 3GPP Release version in the ASN.1 decoder of the NMS.

2.2 Save Path of Standard Signaling Northbound Result Files

After collecting and processing NE data, Trace Server saves standard signaling northbound result files in the **/export/home/omc/var/fileint/TSNBI/** directory on the server where NEs are located. Trace Server creates subdirectories in the directory.

The rule for creating subdirectories is as follows:

LTE_CELL_TRC/*yyyymmdd*/*NE identifier*/ and **LTE_SIG/***yyyymmdd*/*NE identifier*/

NOTE

- *yyyymmdd* indicates the date when a standard signaling northbound result file is generated.
- NE identifiers include **NE FDN** and **NE Name**. **NE FDN** is a unique attribute of NEs, and the value range is 256 to 2945727. **NE Name** is user-defined and unique in the same EMS.
- You can query the IP address of the server where an NE is located on the MAE client. In the **Apps** area of the MAE home page, click **Access** to enter the MAE-Access home page. On the main menu, choose **Maintenance** > **Trace Server Maintenance** > **Query Subscription Information** to query the IP address. For details about operations on the **Query Subscription Information** page, click  on this page and view the help information.
- You can use MAE to modify configuration items. For details, see **Modifying Configuration Items** in 4.1 Negotiating Interconnection Parameters for the Standard Signaling Northbound File Interface.
- To prevent the NMS from collecting duplicate data, historical data remains unchanged after configuration items or NE names are changed.
- When the value of the configuration item is changed to **NE Name** and is used as the name of the directory for storing trace result files, **NE Name** cannot be **...**.
- The **dataList** subdirectory in the **/export/home/omc/var/fileint/TSNBI/LTE_CELL_TRC** or **/export/home/omc/var/fileint/TSNBI/LTE_SIG** directory stores the index files whose names start with **Datalist**. These index files are used to quickly send the standard signaling northbound result files, improving the file sending efficiency.

For example:

- When the NE identifier is **NE FDN**, if a result file is generated on November 11, 2019, the directory is automatically created for saving result files that are generated on November 11, 2019. For details, see Table 2-2.

Table 2-2 Directory for saving standard signaling result files

Event Name	Result File Name	Path
UE Period TA UE Period TA MDT	LTE_SIG	/export/home/omc/var/fileint/TSNBI/*LTE_SIG/20191111/NE FDN*/
S1 interface event X2 interface event Uu interface event	LTE_CELL_TRC	/export/home/omc/var/fileint/TSNBI/*LTE_CELL_TRC/20191111/NE FDN*/

- When the NE identifier is **NE Name**, if a result file is generated on November 11, 2019, the directory is automatically created for saving result files that are generated on November 11, 2019. For details, see Table 2-3.

Table 2-3 Directory for saving standard signaling result files

Event Name	Result File Name	Path
UE Period TA UE Period TA MDT	LTE_SIG	/export/home/omc/var/fileint/TSNBI/*LTE_SIG/20191111/NE Name/*
S1 interface event X2 interface event Uu interface event	LTE_CELL_TRC	/export/home/omc/var/fileint/TSNBI/*LTE_CELL_TRC/20191111/NE Name/*

2.3 Naming Conventions for Standard Signaling Northbound Result Files

Trace Server saves data reported by NEs as northbound result files.

The naming conventions are as follows:

- When the NE identifier is **NE FDN**,
  naming conventions for a result file are ***<NE FDN>_<StartTime>_<EndTime>_<SN>.<FilePostfix>*.gz**.
- When the NE identifier is **NE Name**,
  naming conventions for a result file are ***<NE Name>_<StartTime>_<EndTime>_<SN>.<FilePostfix>*.gz**.

Table 2-4 Naming convention parameters

Parameter	Description
NEFDN or neName	NE identifiers include **NE FDN** and **NE Name**. You can modify them on MAE. For details, see **Modifying Configuration Items** in 4.3 Commissioning the Interconnection of the Northbound Result File Interface.
StartTime	Start time in the name of an NE-reported file. The time format is *YYYYMMDDhhmmssDST*. *YYYY* indicates the year, *MM* indicates the month, *DD* indicates the day, *hh* indicates the hour, *mm* indicates the minute, *ss* indicates the second, and *DST* is optional, depending on whether the NE is in daylight saving time (DST) mode.
EndTime	End time in the name of an NE-reported file. The time format is *YYYYMMDDhhmmssDST*. *YYYY* indicates the year, *MM* indicates the month, *DD* indicates the day, *hh* indicates the hour, *mm* indicates the minute, *ss* indicates the second, and *DST* is optional, depending on whether the NE is in daylight saving time (DST) mode. **NOTE** If another NE uploads no files or no NEs upload files for a long time, the end time increases by one file generation period in the name of the

Parameter	Description
	last NE-reported file.
SN	Generated series number of the file. Value range: 0000 to 9999. The serial number ranges from 0000 to 9999 cyclically.
FilePostfix	File name extension. • The extension is **sig** for LTE_CELL_TRC result files. • The extension is **log** for LTE_SIG result files.

For example:

- When the NE identifier is **NE FDN**, the SN is 1234, the start time in an NE-reported file is 2019-11-11 17:30:30, and the end time in the NE-reported file is 2019-11-11 17:32:40, the name of the generated LTE_CELL_TRC result file is *NE FDN***_20191111173030_20191111173240_1234.sig.gz**, and the name of the generated LTE_SIG result file is *NE FDN***_20191111173030_20191111173240_1234.log.gz**.
- When the NE identifier is **NE Name**, the SN is 1234, the start time in an NE-reported file is 2019-11-11 17:30:30, and the end time in the NE-reported file is 2019-11-11 17:32:40, the name of the generated LTE_CELL_TRC result file is *NE Name***_20191111173030_20191111173240_1234.sig.gz**, and the name of the generated LTE_SIG result file is *NE Name***_20191111173030_20191111173240_1234.log.gz**.

2.4 Generation Period of Northbound Result Files

This section describes the generation period of northbound result files.

When the volume or generation period of northbound result files is greater than those specified in 4.1 Negotiating Interconnection Parameters for the Standard Signaling Northbound File Interface, northbound trace result files are generated. The default file size and generation period are 10 MB and 5 minutes, respectively.

NOTE

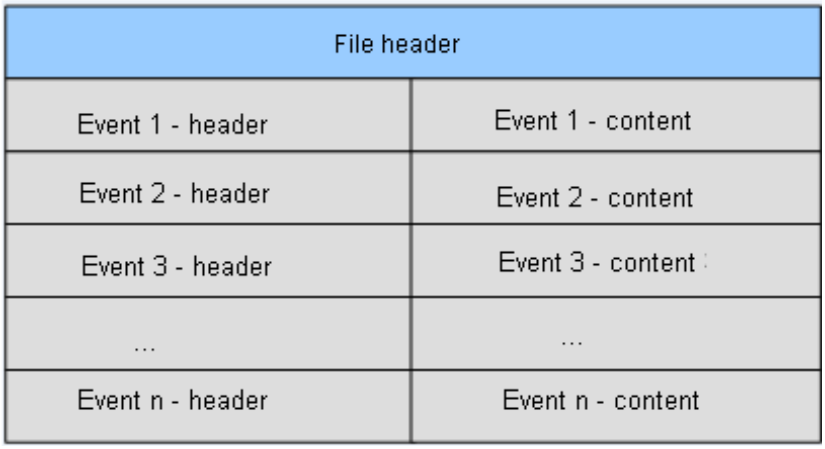
- If the NE does not report the new data file for at least 30 minutes or the Trace Server services stop, NE northbound result files are also generated.
- If the NE identifier has been modified, northbound result files are also generated.
- If the time sequence of files collected by Trace Server is incorrect, the out-of-order files are independently exported to generate northbound trace result files to ensure that contents of the northbound trace result files are properly arranged. In the name of a northbound result file, the start time is the time in the name of an out-of-order file, and the end time is the start time plus the file generation period.

2.5 Formats of Standard Signaling Northbound Result Files

This section describes the formats of northbound result files.

An LTE northbound trace result file consists of the header and body, as shown in Figure 2-3. File headers provide file information. File bodies consist of all events reported by NEs. Each event consists of the event header and event content.

Figure 2-3 Format of LTE northbound result files



Header Format of Standard Signaling Northbound Result Files

Table 2-5 Header format of LTE standard signaling files

Field	Data Type and Length	Description
Data Version	-	File format version information
>Main Version	UINT8	Main version
>Sub Version	UINT8	Sub-version
Spare	OCTET STRING (30)	Spare

NOTE

- > preceding a field indicates that this field is a subfield. For example, if seven fields **A**, **>B**, **>C**, **>>D**, **>>E**, **>F**, and **G** are available in a file in sequence, fields **B**, **C**, and **F** are the subfields of field **A** and fields **D** and **E** are the subfields of subfield **C**.
- In fields, invalid bytes are filled with **FF**, and invalid bits are filled with **0**.

Format of an LTE Standard Signaling Northbound Event Header

Table 2-6 Format of an LTE standard signaling event header

Field	Data Type and Length	Description	Introduced In
Event ID	UINT16	Event identifier	SRAN11.1 Pico 11.1

Field	Data Type and Length	Description	Introduced In
Event Length	UINT32	Event length, excluding lengths of **Event ID** and **Event Length**	SRAN11.1 Pico 11.1
eNodeB ID	UINT32	eNodeB identifier.	SRAN11.1 Pico 11.1
Cell ID	UINT8	Cell identifier Invalid value: all Fs. For example, the value of this field is invalid for base station events or cell events.	SRAN11.1 Pico 11.1
Call ID	UINT32	Call ID Invalid value: all Fs For example, the value of this field is invalid for base station events.	SRAN11.1 Pico 11.1
Date Time	-	Time when an event is triggered UTC time	SRAN11.1 Pico 11.1
>Year	UINT8	Difference between the current year and the year 2000	SRAN11.1 Pico 11.1
>Month	UINT8	Month Value range: 1 to 12	SRAN11.1 Pico 11.1
>Day	UINT8	Day Value range: 1 to 31	SRAN11.1 Pico 11.1
>Hour	UINT8	Hour Value range: 0 to 23	SRAN11.1 Pico 11.1
>Minute	UINT8	Minute Value range: 0 to 59	SRAN11.1 Pico 11.1
>Second	UINT8	Second Value range: 0 to 59	SRAN11.1 Pico 11.1
>Millisecond	UINT16	Millisecond Value range: 0 to 999 The value is **0** for events accurate to	SRAN11.1 Pico 11.1

Field	Data Type and Length	Description	Introduced In
		seconds.	
Extend Head Length	UINT8	Extension header length	-
Item Type	BIT STRING (4)	Event type. • **0000**: undefine • **0001**: FDD • **0010**: TDD • **0101**: NB-IoT • **1111**: Common	SRAN13.1
Reserved	BIT STRING (4)	reserved	-
C-RNTI	UINT16	C-RNTI Invalid value: all Fs. For example, the value of this field is invalid for base station events or cell events.	SRAN11.1 Pico 12.0

NOTICE

System Capacity Impact When independent MDT is enabled, reporting MDT data increases air interface resource consumption, and increases the CPU usage of boards by up to 5%.

Network Performance

- After independent MDT is enabled, intra-frequency or inter-frequency MDT measurement events may conflict with handover measurement events. As a result, the access success rate and the handover success rate decrease by not more than 0.5%.
- Inter-frequency measurement causes UEs to enter the GAP state, and some subframes will be temporarily unable to be adjusted, slightly decreasing the average cell throughput.

If NE-reported data contains the incorrect year, month, and day, the year, month, and day are 0-1-1 in the northbound analysis result. If NE-reported data contains the incorrect hour, minute, and second, the hour, minute, and second are 23-59-59 in the northbound analysis result. You are advised to prevent data analysis problems caused by data errors.

Formats of the LTE Standard Signaling Event Content

Table 2-7 Formats of the LTE standard signaling event content

Field	Data Type and Length	Description	Introduced In
Message Direction	UINT8	Message direction **0**: receive	SRAN11.1 Pico 11.1

Field	Data Type and Length	Description	Introduced In
		1: send Invalid value: **FFFFFFFF**	
Message Length	UINT32	Message length	SRAN11.1 Pico 11.1
Message Content	OCTET STRING (Message Length)	Message content If there is a Uu interface message, the first byte indicates the type of the logical channel where the message is sent. Value range: 1: DL DCCH 2: UL DCCH 3: DL CCCH 4: UL CCCH 18: MCCH 30: DL DCCH NB 31: UL DCCH NB 32: DL CCCH NB 33: UL CCCH NB	SRAN11.1 Pico 11.1

NOTE

For security purposes, the content of some events that involve user privacy is anonymized.

Table 2-8 Format of the UE Period TA (0x1211) event content

Field	Data Type and Length	Description	Introduced In
TA Value	UINT32	TA value Value range: 0 to 20512 Unit: Ts See 3GPP TS 36.133 Timing Advance (TADV): Type 2. If ucTaFlag is not 1 or ulTaValue is 7FFFFFFF, events are not reported.	SRAN11.1 Pico 11.1

NOTE

Date Time in the header of an event of this type is accurate to seconds.

Table 2-9 Format of the UE Period TA MDT (0x1212) event content

Field	Data Type and Length	Description	Introduced In
TA Value	UINT32	TA value Value range: 0 to 20512 Unit: Ts See 3GPP TS 36.133 Timing Advance (TADV): Type 2. If ucTaFlag is not 1 or ulTaValue is 7FFFFFFF, events are not reported.	SRAN11.1

NOTE

Date Time in the header of an event of this type is accurate to seconds.

3 Managing Northbound Users in RAN Sharing Scenarios

About This Chapter

This section describes how to manage northbound users in RAN sharing scenarios. In such scenarios, multiple operators can share one radio access network (RAN). Northbound files reported by one NE contain northbound data from different operators. Trace Server identifies different operators according to the PLMN in the northbound files and saves generated northbound result files in different directories. Operators create specified northbound users to obtain required northbound result files in FTP mode.

3.1 Creating Northbound Users

This section describes how to create specified northbound users using the northbound user configuration tool, helping operators obtain required northbound result files.

Prerequisites

You have obtained passwords of users sopuser and ossuser on the MAE server (Trace Server co-deployed with the MAE-Access) or on the Trace Server (Trace Server independently deployed).

Context

- User name can contain 32 characters, including digits 0 to 9, lowercase letters a to z, uppercase letters A to Z, special characters underscores (-), and special characters underscores (_).

Procedure

Step 1 Use PuTTY to log in to the MAE master server (Trace Server co-deployed with the MAE-Access) or Trace Server master server (Trace Server independently deployed) in SSH mode as user sopuser.

Step 2 Run the following command to switch to the **root** user:

> **su - root**

```
Password: password for the root user
```

Step 3 Run the following commands to run the RAN sharing northbound user configuration tool:

\# **cd /opt/oss_sudobin_internal/oss/TSCollector/root/bin**

\# **bash setRANSharingUser.sh**

Step 4 When the following information is displayed, enter **B** or **b** and press **Enter**:

```
Please select an operation type.
A--Show the northbound user list.
B--Create a northbound user.
C--Reconfigure the password of northbound user.
D--Delete a northbound user or a single PLMN.
E--Set the RAN sharing switch.
F--Restart all Trace Server services.
Q--Exit
Please select:
```

Step 5 When the following information is displayed, enter the northbound user name and press **Enter**:

```
Please enter your user name.
```

Step 6 When the following information is displayed, enter the PLMN of the northbound user and press **Enter**:

```
Please enter your PLMN number.
```

Step 7 When the following information is displayed, choose **Yy** or **Nn** to determine whether northbound users need to access the public data and press **Enter**:

```
Are you sure you want to view common data? [Yy/Nn]:[default=Y]
```

Step 8 When the following information is displayed, enter the password of the northbound user and press **Enter**. You need to enter the new password twice.

```
Please enter password.
Please enter password again.
Changing password for Northbound user name
```

Step 9 If the following information is displayed, the RAN sharing northbound user has been created successfully. Otherwise, contact Huawei technical support.

```
User Northbound user name created successfully.
```

Step 10 Type **Q** or **q** and press **Enter** to exit the RAN sharing northbound user configuration tool.

Step 11 Add permissions for the new northbound user.

1. Use PuTTY to log in to the OSMU master node where Trace Server is installed as the **sopuser** user in SSH mode.

   NOTE

   If OSMU is deployed in cluster mode, perform the following operations only on OSMUM01.

2. Run the following command to switch to the **ossadm** user:

   > **su - ossadm**

   ```
   Password: password for the ossadm user
   ```

3. Run the following command to add permissions for the new northbound user:

   > **bash /opt/cloud/manager/tools/osconfigmgr/sshd_ipsadm.sh -type add_external_user -extuser** *northbound user name*

   NOTE

   Northbound user name is the user name entered in Step 5. Replace it as required.

----End

Follow-up Procedures

- If the PLMN needs to be separately added for created northbound users, repeat the operations from Step 1 to Step 6 and enter the PLMN to be added in Step 5. When the following information is displayed, the PLMN has been added successfully. Otherwise, contact Huawei technical support.

  ```
  The northbound user already exists.
  User Northbound user name created successfully.
  ```

- If access permissions of created northbound users on public data need to be changed, perform the operations from Step 1 to Step 6. Reconfigure the access permissions for northbound users in Step 6. When the following information is displayed, the permissions have been changed successfully. Otherwise, contact Huawei technical support.

  ```
  The northbound user already exists.
  User Northbound user name created successfully.
  ```

  NOTE

  After the access permissions of northbound users on public data are changed, you must log in to Trace Server again to make the change take effect.

3.2 Viewing Northbound Users

This section describes how to view created northbound users, their permissions, and PLMNs using the northbound user configuration tool.

Prerequisites

You have obtained passwords of users sopuser and ossuser on the MAE server (Trace Server co-deployed with the MAE-Access) or on the Trace Server (Trace Server independently deployed).

Procedure

Step 1 Use PuTTY to log in to the MAE master server (Trace Server co-deployed with the MAE-Access) or Trace Server master server (Trace Server independently deployed) in SSH mode as user sopuser.

Step 2 Run the following command to switch to the **root** user:

> **su - root**

```
Password: password for the root user
```

Step 3 Run the following commands to run the RAN sharing northbound user configuration tool:

cd /opt/oss_sudobin_internal/oss/TSCollector/root/bin

bash setRANSharingUser.sh

Step 4 When the following information is displayed, enter **A** or **a** and press **Enter** to view the created RAN sharing northbound users:

```
Please select an operation type.
A--Show the northbound user list.
B--Create a northbound user.
C--Reconfigure the password of northbound user.
D--Delete a northbound user or a single PLMN.
E--Set the RAN sharing switch.
F--Restart all Trace Server services.
Q--Exit
Please select:
```

Step 5 When information similar to the following is displayed, you can view created northbound users, their permissions to access public data, and PLMNs of all users:

```
-----------------------------------------------
Username    CommonData  PLMN
user1       Y           1111,22222,333333
user2       Y           44444
user3       N           555555
-----------------------------------------------
```

Step 6 Type **Q** or **q** and press **Enter** to exit the RAN sharing northbound user configuration tool.

----End

3.3 Modifying Northbound User Passwords

This section describes how to modify the password of a created northbound user using the northbound user configuration tool. To improve data security, properly keep the password of the northbound user and change it periodically.

Prerequisites

You have obtained passwords of users sopuser and ossuser on the MAE server (Trace Server co-deployed with the MAE-Access) or on the Trace Server (Trace Server independently deployed).

Procedure

Step 1 Use PuTTY to log in to the MAE master server (Trace Server co-deployed with the MAE-Access) or Trace Server master server (Trace Server independently deployed) in SSH mode as user sopuser.

Step 2 Run the following command to switch to the **root** user:

> **su - root**

```
Password: password for the root user
```

Step 3 Run the following commands to run the RAN sharing northbound user configuration tool:

cd /opt/oss_sudobin_internal/oss/TSCollector/root/bin

cd /opt/oss_sudobin_internal/oss/TSCollector/root/bin

Step 4 When the following information is displayed, enter **C** or **c** and press **Enter**:

```
Please select an operation type.
A--Show the northbound user list.
B--Create a northbound user.
C--Reconfigure the password of northbound user.
D--Delete a northbound user or a single PLMN.
E--Set the RAN sharing switch.
F--Restart all Trace Server services.
Q--Exit
Please select:
```

Step 5 When the following information is displayed, enter the northbound user name to be modified and press **Enter**:

```
Please enter the user name.
```

Step 6 When the following information is displayed, enter the new password of the northbound user and press **Enter**. You need to enter the new password twice.

```
Please enter password.
Please enter password again.
Changing password for Northbound user name
```

Step 7 If the following information is displayed, the password of the northbound user has been modified successfully. Otherwise, contact Huawei technical support.

```
Modify the password of Northbound user successfully.
```

Step 8 Type **Q** or **q** and press **Enter** to exit the RAN sharing northbound user configuration tool.

----End

3.4 Deleting Northbound Users

This section describes how to delete northbound users who are not used any more using the northbound user configuration tool.

Prerequisites

You have obtained passwords of users sopuser and ossuser on the MAE server (Trace Server co-deployed with the MAE-Access) or on the Trace Server (Trace Server independently deployed).

Procedure

Step 1 Use PuTTY to log in to the MAE master server (Trace Server co-deployed with the MAE-Access) or Trace Server master server (Trace Server independently deployed) in SSH mode as user sopuser.

Step 2 Run the following command to switch to the **root** user:

> **su - root**

```
Password: password for the root user
```

Step 3 Run the following commands to run the RAN sharing northbound user configuration tool:

cd /opt/oss_sudobin_internal/oss/TSCollector/root/bin

bash setRANSharingUser.sh

Step 4 When the following information is displayed, enter **D** or **d** and press **Enter**:

```
Please select an operation type.
A--Show the northbound user list.
B--Create a northbound user.
C--Reconfigure the password of northbound user.
D--Delete a northbound user or a single PLMN.
E--Set the RAN sharing switch.
F--Restart all Trace Server services.
Q--Exit
Please select:
```

Step 5 When the following information is displayed, enter **B** or **b** and press **Enter**:

```
Please select an operation type.
A--Delete a single PLMN under a user.
B--Delete a northbound user.
Q--Exit
Please select:
```

Step 6 When the following information is displayed, enter the northbound user name to be deleted, **user1** for example, and press **Enter**:

```
Please enter the user name to delete:
user1
```

Step 7 When the following information is displayed, enter **Y** or **y** and press **Enter**:

```
User user1 has the following PLMNs:
1111 22222 333333
Are you sure you want to delete all PLMNs under user user1? [Yy/Nn]
The operation will delete all NBI result files under the PLMN.
The operation will take a few minutes.
Please select:
```


Step 8 If the following information is displayed, the northbound user **user1** has been deleted successfully. Otherwise, contact Huawei technical support.

```
User user1 deleted successfully.
```

Step 9 Type **Q** or **q** and press **Enter** to exit the RAN sharing northbound user configuration tool.

----End

3.5 Deleting Northbound User PLMNs

This section describes how to delete northbound user PLMNs using the northbound user configuration tool.

Prerequisites

You have obtained passwords of users sopuser and ossuser on the MAE server (Trace Server co-deployed with the MAE-Access) or on the Trace Server (Trace Server independently deployed).

Procedure

Step 1 Use PuTTY to log in to the MAE master server (Trace Server co-deployed with the MAE-Access) or Trace Server master server (Trace Server independently deployed) in SSH mode as user sopuser.

Step 2 Run the following command to switch to the **root** user:

> **su - root**

```
Password: password for the root user
```

Step 3 Run the following commands to run the RAN sharing northbound user configuration tool:

cd /opt/oss_sudobin_internal/oss/TSCollector/root/bin

bash setRANSharingUser.sh

Step 4 When the following information is displayed, enter **D** or **d** and press **Enter**:

```
Please select an operation type.
A--Show the northbound user list.
B--Create a northbound user.
C--Reconfigure the password of northbound user.
D--Delete a northbound user or a single PLMN.
E--Set the RAN sharing switch.
F--Restart all Trace Server services.
Q--Exit
Please select:
```

Step 5 When the following information is displayed, enter **A** or **a** and press **Enter**:

```
Please select an operation type.
A--Delete a single PLMN under a user.
B--Delete a northbound user.
Q--Exit
Please select:
```


Step 6 When the following information is displayed, enter the northbound user name to be deleted that the PLMN belongs to, **user1** for example, and press **Enter**:

```
Please enter the user name to delete:
user1
```

Step 7 When the following information is displayed, enter the PLMN to be deleted, **1111** for example, and press **Enter**:

```
User user1 has the following PLMNs:
1111 22222 333333
Please enter the PLMN:
1111
```

Step 8 When the following information is displayed, enter **Y** or **y** and press **Enter**:

```
Are you sure you want to delete a single PLMN? [Yy/Nn]
The operation will delete all NBI result files under the PLMN.
The operation will take a few minutes.
Please select:
```

Step 9 If the following information is displayed, the value **1111** of the PLMN for northbound user **user1** has been deleted successfully. Otherwise, contact Huawei technical support.

```
Single PLMN under user user1 deleted successfully.
```

Step 10 Type **Q** or **q** and press **Enter** to exit the RAN sharing northbound user configuration tool.

----End

3.6 Configuring the Northbound RAN Sharing Function Switch

This section describes how to configure the RAN sharing function for Trace Server GSM/UMTS/LTE northbound file interfaces using the northbound user configuration tool. By default, the RAN sharing function is disabled.

Prerequisites

You have obtained passwords of users sopuser and ossuser on the MAE server (Trace Server co-deployed with the MAE-Access) or on the Trace Server (Trace Server independently deployed).

Context

After the RAN sharing function is enabled, northbound result files are saved in **/export/home/omc/var/fileint/TSNBI/shared/**. Trace Server creates subdirectories in this path.

- If PLMN values are not all Fs, the subdirectory naming conventions are ***PLMN value/Result File Name/yyyymmdd/NE identifier/***.
- If PLMN values are all Fs, the subdirectory naming conventions are **commonData/*Result File Name/yyyymmdd/NE identifier/***.

Procedure

Step 1 Use PuTTY to log in to the MAE master server (Trace Server co-deployed with the MAE-Access) or Trace Server master server (Trace Server independently deployed) in SSH mode as user sopuser.

Step 2 Run the following command to switch to the **root** user:

> **su - root**

```
Password: password for the root user
```

Step 3 Run the following commands to run the RAN sharing northbound user configuration tool:

cd /opt/oss_sudobin_internal/oss/TSCollector/root/bin

bash setRANSharingUser.sh

Step 4 When the following information is displayed, enter **E** or **e** and press **Enter**:

```
Please select an operation type.
A--Show the northbound user list.
B--Create a northbound user.
C--Reconfigure the password of northbound user.
D--Delete a northbound user or a single PLMN.
E--Set the RAN sharing switch.
F--Restart all Trace Server services.
Q--Exit
Please select:
```

Step 5 When the following information is displayed, enter **A** or **a** and press **Enter** (**enabling the GSM RAN sharing function is used as an example here**).

```
-----------RAN Sharing Switch Status-----------
A.GSM-------off
B.UMTS------off
C.LTE-------off
-----------------------------------------------
Please select an operation type.
A--Set the GSM switch status.
B--Set the UMTS switch status.
C--Set the LTE switch status.
Q--Exit
Please select:
```

Step 6 When the following information is displayed, enter **ON** or **on** and press **Enter** (**enabling the GSM RAN sharing function is used as an example here**).

```
Are you sure you want to set the status of the GSM switch? [ON/OFF]
```

Step 7 If the following information is displayed, the GSM RAN sharing function has been enabled successfully. Otherwise, contact Huawei technical support.

```
GSM switch set successfully.
-----------RAN Sharing Switch Status-----------
A.GSM-------on
B.UMTS------off
C.LTE-------off
-----------------------------------------------
Please select an operation type.
```



```
A--Set the GSM switch status.
B--Set the UMTS switch status.
C--Set the LTE switch status.
Q--Exit
Please select:
```

Step 8 Type **Q** and press **Enter**. Return to the RAN sharing northbound user configuration tool main interface.

Step 9 Type **F** and press **Enter** to restart the Trace Server services.

When information similar to the following is displayed, type **Y** and press **Enter** to restart the Trace Server services.

```
Are you sure to restart all Trace Server services, whether to continue (Y/N)
```

When the following information is displayed, the Trace Server services have been restarted successfully. Otherwise, contact Huawei technical support.

```
All Trace Server services restarted successfully.
```

Step 10 Type **Q** or **q** and press **Enter** to exit the RAN sharing northbound user configuration tool.

----End

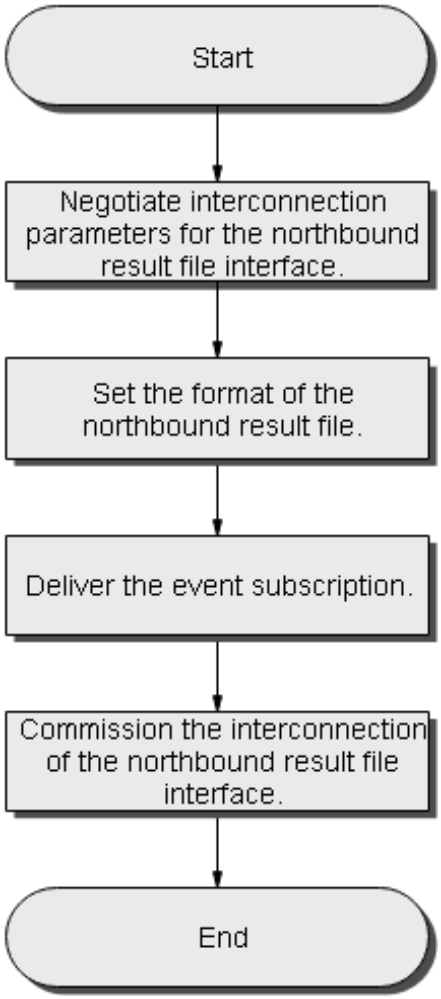
4 Process for Interconnecting the Standard Signaling Northbound Result File Interface

About This Chapter

This section describes the process for interconnecting the NMS with Trace Server using the northbound result file interface.

Figure 4-1 lists the process for interconnecting the standard signaling northbound result file interface.

Figure 4-1 Flow chart of process for interconnecting the standard signaling northbound result file interface



4.1 Negotiating Interconnection Parameters for the Standard Signaling Northbound File Interface

This section describes the preparations for interconnecting Trace Server with the NMS.

Checking Licenses

Perform the following operations to check whether MAE is licensed to use this NBI:

1. Log in to MAE.
2. In the **Apps** area of the MAE home page, click **Common** to enter the Common home page.
3. Choose **System** > **License Management** > **License Information** to enter the **License Information** page.
4. Click the **Resource Control Items** tab. If **Resource Name** contains the **WOFD-914301 Standard trace data BIN file interface - L** item, the standard signaling northbound file interface is available. If there is no license, the standard signaling northbound file interface is unavailable. If you need to use this function, contact Huawei technical support.

Negotiating Interconnection Parameters

Table 4-1 describes interconnection parameters to be negotiated.

Table 4-1 Negotiating interconnection parameters

FTP	Parameter	Parameter Description
(Recommended) If Trace Server serves as an FTP server, the NMS obtains files from Trace Server.	FTP user name	Value: ftpuser or the northbound user in RAN sharing scenery.
	Password	For details about how to obtain the password, contact the Trace Server administrator.
	FTP port	Value: **21** If you use FTP to transfer files, open the port on Trace Server.
	SFTP port	Value: **22** If you use SFTP to transfer files, open the port on Trace Server.
	Path for saving files	After collecting and processing NE-reported data, Trace Server saves northbound result files on the server managing NEs. • If RAN sharing is enabled, Trace Server saves northbound trace result files in the **/export/home/omc/var/fileint/TSNBI/shared/** directory and creates subdirectories. • If RAN sharing is disabled, Trace Server saves northbound trace result files in the **/export/home/omc/var/fileint/TSNBI/** directory and creates subdirectories.
If Trace Server serves as an FTP client, it automatically	FTP user name	Provided by the NMS.
	Password	Provided by the NMS.
	FTP port	Value: 21

FTP	Parameter	Parameter Description
uploads files to the NMS.		If you use FTP to transfer files, open the port on the NMS.
	SFTP port	Value: 22 If you use SFTP to transfer files, open the port on the NMS.
	Path for saving files	Provided by the NMS. Trace Server uploads northbound trace result files to this path on the NMS.

Modifying Configuration Items

Prerequisites

- You have logged in to MAE.
- You have loaded the northbound trace licenses on MAE.

Procedure

1. In the **Apps** area of the MAE home page, click **Access** to enter the MAE-Access home page.
2. In the **Apps** area of the MAE home page, click **Common** to enter the **Common** page.
3. In the navigation pane, choose **LTE Common Trace Server NBI**.
4. In the **Signaling Format** area box, select **OSSii**.
5. In the navigation pane, choose **OSSii**.
6. Set related parameters in the right area box by referring to Table 4-2 and Table 4-3.

Table 4-2 OSSii parameter settings

Area Box Name	Parameter Name	Description
OSSii Parameter Settings	Storage duration(hours)	Storage duration that northbound trace result files can be saved in the directory on the server Value range: 1 to 72 (hour) Default value: **72**
	NE identifier	You can change NE identifiers to set naming conventions for northbound result files. Value: **NE Name** or **NE FDN** Default value: **NE Name**
	Generated file size(MB)	Maximum size of the generated northbound trace

Area Box Name	Parameter Name	Description
		result file Values: **1**, **5**, **10**, **15**, and **30** (MB) Default value: **10**
	File generation period(mins)	Generation period of northbound trace result files Values: **1**, **5**, and **10** (minute) Default value: **5**
	MDT extended field display switch	This switch can be turned on or off to determine whether to report new parameters during the subscription to events with new parameters. Default value: **Off** If this switch is turned on, the settings of the following parameters change during subscription: • The version number in the file header is changed to 2.0. • Fields **Serving Cell SINR** and **>SINR** are added in the 0x1302 M1 Intra-Freq MDT event. • Fields **Serving Cell SINR** and **>SINR** are added in the 0x1303 M1 Inter-Freq MDT event. • Fields **UL CA Flag**, **Reserved**, and **CA Property** are added in the 0x1304 M2 MDT event. • Fields **UL Data Transmission Time of Last TTI per UE** and **DL Data Transmission Time of Last TTI per UE** are added in the 0x1307 M5 MDT event. **NOTICE** Before turning on this switch, ensure that the NMS has updated the data parsing tool. Otherwise, the NMS cannot parse events with new

Area Box Name	Parameter Name	Description
		parameters.
Subscription Time Offset Settings	Start subscription time(mins)	To prevent subscription issuing delays and ensure integrity of data reported over northbound interfaces, northbound interface data subscription allows you to issue subscription commands in advance. Values: **0**, **5**, **10**, and **15** (minute) Default value: **10**
	Stop subscription time(mins)	To prevent delays during southbound interface data reporting and northbound interface data processing and ensure integrity of data reported over northbound interfaces, northbound interface data subscription allows you to delay subscription cancellation. Values: **0**, **5**, **10**, and **15** (minute) Default value: **15**

Table 4-3 Compression parameter settings

Navigation Tree	Area Box Name	Parameter Name	Description
LTE Data Compression Switch **NOTE** This function applies only to LTE NEs whose version is eRAN13.0 or later and whose MPT type is not LMPT.	Compression Parameter Settings	Enable data compression	• **OFF**: After **OFF** is selected, data that Trace Server subscribes to is transmitted without being compressed. • **ON**: After **ON** is selected, data that Trace Server subscribes to is transmitted after being compressed. Default value: **OFF**

7. After settings are complete, click **Save**.

4.2 Issuing the Event Subscription

Before configuring the standard signaling northbound interface, you need to issue an event subscription task. After the event subscription is issued, NEs upload the standard signaling data to Trace Server and Trace Server processes the uploaded data and generates a northbound result file.

4.2.1 Subscribing to an LTE NE Trace Task

This section describes how to subscribe to an LTE NE trace task. You can subscribe to an NE trace task to obtain the northbound trace result files of Trace Server from a specified directory on the MAE server for northbound interconnection.

Prerequisites

- You have purchased the license for LTE cell trace.
- You have installed the mediations of LTE NEs. NEs are connected to MAE properly.
- You have obtained the Trace Server NBI management permission.
- You are authorized to use the **Trace Server NE Management** function.

Context

- After the NE version is upgraded, do not resubscribe to the messages that have been subscribed to on MAE.

Procedure

Step 1 In the **Apps** area of the MAE home page, click **Access** to enter the MAE-Access home page.

Step 2 Choose **Monitor** > **Trace Server NBI** > **LTE Common Trace Server NBI**. The **LTE Common Trace Server NBI** window is displayed.

Step 3 In the **NE** navigation tree, choose an NE type, an NE version, and NE information.

NE Name, **Subscribe Status**, **Start Time**, **End Time**, **Collection State**, **Collection Time**, and **Operation Result** are displayed on the right pane.

Step 4 In the right pane, select the NEs to which subscription is to be issued, and click **Subscribe**.

Step 5 Select **Auto**, **ALL**, or **Selected** as required.

NOTE

To use the function of automatically subscribing to new NEs, select **Auto**. After you select **Auto subscribe new NEs** and set related parameters as required, the system automatically issues the preset subscription to the new NEs. In this scenario, **Set area scope** is unavailable in the **Logged MDT Parameter Settings** page. For details about subscription parameters, see 4.2.3 Parameters for Subscribing to an LTE NE Trace Task (OSSii).

Step 6 In the **Message Settings** area, select the message contents that you want to subscribe to.

The **Message Settings** area displays the message contents supported by the NE, the message contents that you have subscribed to, and subscribe to a failed message.

NOTE

- If many message contents are available, enter the message keywords in the **Find message** text box and click **Previous** or **Next** to search for the required message contents.
- To subscribe to or unsubscribe from all message content, you can select **Select all** or **Clear all** for **Selection ploy** in the **Message Settings** area to quickly subscribe to or unsubscribe from all message content.
- To subscribe to message content, click **Export** or **Import** in the message list in the **Message Settings** area to export or import the configured message content.

Step 7 In the **Basic Settings** area, set the parameters related to the subscription.

NOTE

Collection time is used for controlling the time segment for reporting data. After this parameter is set to a time segment, Trace Server processes and reports data collected within the time segment. For example, if the subscription start time is 10:05 on December 22, 2019, the end time is 10:05 on December 23, 2019, and the collection time is 11:00-12:00, only the data from 11:00:00 on December 22 to 11:59:59 on December 22 is reported. If this parameter is not set (that is, the **Collection time** check box is deselected), data generated from the subscription start time to the end time is processed and reported.

Step 8 Click **Next**. In the displayed dialog box, set related subscription parameters in the **Periodic Messages Parameters Settings** and **MDT Parameter Settings** areas.

Step 9 Click **Apply**.

After the subscription is started, the NE subscription information is displayed on the GUI.

----End

4.2.2 GUIs for LTE Northbound Interface Trace (OSSii)

This section describes the function of each component in the **LTE Trace Server NBI** window.

Figure 4-2 shows the **LTE Trace Server NBI** window. Table 4-4 describes the window shown in Figure 4-2.

Figure 4-2 LTE Trace Server NBI-main window

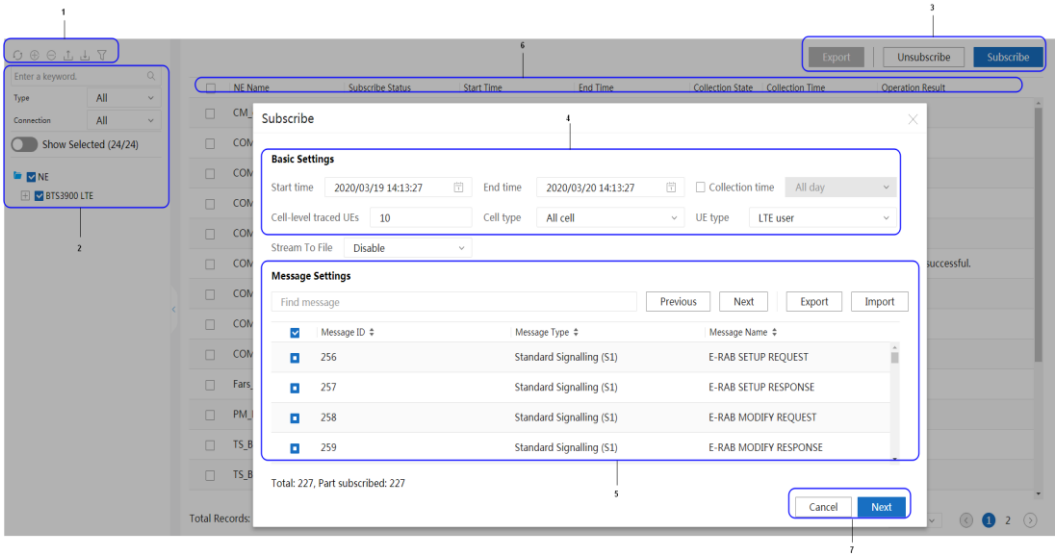


Table 4-4 LTE Trace Server NBI-main window

No.	Name	Description
1	Area for displaying function icons	You can click a function icon as required. The import and export icons allow you to import and export selected NEs. This function supports the import and export of only NEs of the same version. Therefore, you cannot select NEs of different versions at the same time.
2	NE navigation tree	By default, the NE navigation tree is displayed by **NE Type**.
3	Buttons	Allows you to export data, unsubscribe to NEs, or subscribing to NEs.
4	Parameter setting area	Allows you to set basic parameters for NE trace tasks. **NOTE** If a parameter setting area is unavailable, this parameter is inapplicable for the selected message.
5	Message setting area	Allows you to set messages provided by NEs. **NOTE** • If different licences of the northbound file interface are loaded, the displayed message list is different. • For the virtual cluster system, IP address here refers to OSS_Service plane IP address of the Trace Server master server. If NAT is configured, IP address here refers to default network port IP address or OSS_Service plane IP address after NAT. If you modify the IP address of the MAE master server or the Trace Server master server, you need to reconfigure the mapping between the TCE ID and TCE IP address.

No.	Name	Description
6	Detailed subscription information area	Displays detailed subscription information.
7	Buttons	Provides the **Next** and **Cancel** functions.

NOTE

If the attributes of Cell, eNodeB ID, PLMN, and TAC are modified, you need to re-issued subscription of the entire network.

4.2.3 Parameters for Subscribing to an LTE NE Trace Task (OSSii)

This section describes the parameters for subscribing to LTE NE trace tasks.

NOTICE

When you query multiple NEs. If the parameters of **Basic Settings** area are different, all parameters are displayed as default values. If the parameters of **Basic Settings** area are the same, all parameters are displayed as specific setting. When you click **Apply**, Trace Server will issue the parameters which are displayed to NEs.

Table 4-5 Parameters for subscribing to an LTE NE trace task

Area		Parameter	Description
NE			By default, the NE navigation tree is displayed by network topology.
Basic Settings	Time parameter settings	Start time	Indicates the subscription start time.
		End time	Indicates the subscription end time.
		Collection time	Indicates the specific hour-level time segment for subscription. You can specify some hour-level time segments intersecting with the subscription start time and end time as the subscription time segments. Default value: **All day**
	Cell parameter settings	Cell-level traced UEs	Indicates the number of cell-level traced UEs and is used to group measurement report messages. Value range: 0 to 400 Default value: **10** **NOTE** • **0** indicates all UEs. Due to the limited capability of the LBBP, a maximum of 400 UEs are

Area		Parameter	Description
			supported. • The more the number of UEs to be traced concurrently, the greater the impact on system performance and subscriber services. • After periodic event subscription is issued, the base station randomly selects X online UEs (X is the preset number of cell-level traced UEs) and instructs each UE to periodically measure the throughput based on the period Y (Y is the preset measurement reporting period). When the period arrives, a periodic throughput measurement event is generated. Each UE reports the event for consecutive Z times (Z is the default consecutive reporting times, default value is 16) when the UE is online. The events reported are cached in NE memories. When the cache time reaches five minutes or the cache size reaches 1 MB, the NE reports the cached events to Trace Server. • After subscription to maximum-level standard signaling events is issued to a base station, the base station selects *X* UEs newly connected to the base station and reports events of the selected UEs to Trace Server. *X* indicates the predefined number of cell-level traced UEs. The base station saves the events in its memory. When the cache duration reaches 5 minutes or the cache size reaches 1 MB, the base station reports the cached events to Trace Server.
		Cell type	Indicates the cell type during cell tracing. This parameter is used to group messages of different events. Default value: **ALL cell** Values: **ALL cell**, **NB-IoT cell**, and **FDD-TDD cell**. • **ALL cell**: indicates configurations take effect for all cells on NEs. • **NB-IoT cell**: indicates configurations take effect for all NB-IoT cells on NEs. • **FDD-TDD cell**: indicates configurations take effect for all FDD-TDD cells on NEs. **NOTE** • Non-cell events and subscriber events are supported by default without being distinguished. • This parameter applies only to LTE NEs whose version is SRAN13.1 or later. • The pico NE only supports the **ALL cell** value.
		UE type	Indicates the type of the user to which the NE issues subscription. You can select different users as required. Value range: **LTE user**, **eMTC user**, and

Area		Parameter	Description
			LTE user and eMTC user Default value: **LTE user**
		Stream To File	Indicates that Trace Server converts stream data reported by NEs to a file. This option is deselected by default. **NOTE** When users subscribe to events for an NE that has been subscribed to, the last stream-to-file conversion setting is inherited.
	Periodic Messages Parameters Settings	Report interval	Select a period from the drop-down list. When the period is selected, the NE reports measurement events based on this period. **NOTE** If this parameter is set to different values for the same periodic measurement event on multiple upper-layer applications, Trace Server issues the minimum period to NEs. Values: **2048 ms**, **5120 ms**, **10240 ms**, and **1 Minute**. Default value: **10240 ms**.
		Report amount	Value range: **Eight Times**, **Sixteen Times**, **Thirty-two Times**, **Sixty-four Times**, and **Infinite Times**. Default value: **Sixteen Times**. **NOTE** If this parameter is set to different values for the same periodic measurement event on multiple upper-layer applications, Trace Server issues the maximum number of times to NEs.
	MDT Parameters Settings	UE selection	Value range: **Polling** and **Ability first**. Default value: **Polling**. **NOTE** If this parameter is set to different values for the same periodic measurement event on multiple upper-layer applications, Trace Server issues the polling policy to NEs.
		Proactively open UE GNSS	Value range: **YES** and **NO**. Default value: **NO**. **NOTE** Whether the GPS takes effect also depends on UE capability and behavior. If this parameter is set to different values for the same periodic measurement event on multiple upper-layer applications, Trace Server issues the most recent value to NEs.
		Subframe index	Indicates the subframe index of the M3 MDT event. Value range: **0** to **9**.

Area		Parameter	Description
			Default value: **2**.
		UEs	Indicates the number of cell-level traced UEs during MDT. When the number of cell-level traced UEs is 0, the value of this parameter ranges from 0 to 400. **NOTE** **0** indicates all UEs. The entered value of **Cell-level traced UEs** during MDT must be less than or equal to the number of cell-level traced UEs.
	Logged MDT Parameter	Logging interval	Value range: **5120 ms**, **10240 ms**, **20480 ms**, **30720 ms**, **40960 ms**, and **61440 ms**. Default value: **10240 ms**.
		Logging duration	Value range: **10 Minutes**, **20 Minutes**, **40 Minutes**, **60 Minutes**, **90 Minutes**, and **120 Minutes**. Default value: **10 Minutes**.
		Area Scope	• The **Set area scope** is cleared by default. If the measurement scope of Logged MDT events needs to be specified, select **Set area scope**. You can select **Cell** or **Tracking area**. A maximum of 32 cells or 8 tracking areas can be selected for each NE. – When **Cell** is selected: You can select the specified NE from the NE navigation tree, and the table in the right pane displays information about the cells under the NE; you can also configure the cells. – When **Tracking area** is selected: The system displays information about the tracking areas. You can configure the tracking areas. • If the measurement scope of Logged MDT events does not need to be specified, deselect **Set area scope**. If the measurement scope has been set by following **Cell** or **Tracking area**, select **Set area scope**, delete the original settings, and deselect **Set area scope**. **NOTE** When you only switch over to **Cell** or **Tracking area** without modifying other parameters, clicking **OK** will not modify parameters.
Message Settings		Find message	You can type the keywords and click **Previous** or **Next** to search for the required messages.

Area	Parameter	Description
	Message ID	Uniquely identifies a message.
	Message Name	Indicates the name of a message.
	Message Type	Indicates the type of a message. **NOTICE** The following operations have impact on system performance and user services. Be caution when performing these operations. • Select too many periodic MR events at a time. • Set the period for reporting periodic MR events too small. • Set the number of reporting periodic MR events too large.
	Export	Allows you to export message events configured on existing NEs and import them to message configurations on other NEs to configure message events quickly. You can also export a template that is not configured with message events, set required message events, and import the configured template to NE message configurations. TXT, HTML, CSV, PDF, XLS, and XLSX export files are available.
	Import	Allows you to import recently exported message event configurations or manually modified message event templates to NE message configurations to configure message events quickly. Message events to be imported are in the unavailable and selected state. If the message events are contained in the imported file, the message events are in the available state. Otherwise, status of the message events remains unchanged. CSV, XLS, and XLSX import files are available.
Detailed subscription information area	NE Name	Indicates the name of the NE whose data needs to be subscribed to.
	Subscribe Status	Indicates the existing subscription status. Values of the parameter are as follows: • **Subscribing**: indicates that the system is issuing subscription to a target NE. • **Subscribed**: indicates that the system issues subscription to a target NE successfully. • **Unsubscribed**: indicates that the system

Area	Parameter	Description
		has issued no subscription to a target NE or canceled subscription to a target NE. • **Unsubscribing**: indicates that the system is canceling subscription to a target NE.
	Start Time	Indicates the subscription start time.
	End Time	Indicates the subscription end time.
	Collection State	Indicates whether the system is collecting data from a selected NE. Values of the parameter are as follows: • **Running**: indicates that the system is collecting data from a target NE. • **Idle**: indicates that the system collects no data from a target NE.
	Collection Time	Indicates the specific hour-level time segment for subscription in a day.
	Operation Result	Summarizes successful and failed subscription information.

4.3 Commissioning the Interconnection of the Northbound Result File Interface

The NMS obtains northbound result files generated by Trace Server using FTP or SFTP. Based on the files, you can determine whether the standard signaling northbound file interface meets the requirements for interconnecting with the NMS.

Prerequisites

- The NMS and Trace Server are properly connected.
- You have obtained the IP address of Trace Server (the FTP server) and the FTP user name and password.
- You have obtained the names and directory of the northbound result files. For details, see 2 Overview of Northbound Trace Result Files.
- You have issued an event subscription task. For details, see 4.2.1 Subscribing to an LTE NE Trace Task.
- You have logged in to the NMS.

Context

The NMS obtains northbound result files from a specified directory on Trace Server using FTP or SFTP.

Procedure

Step 1 Run the following command to set the destination directory for storing northbound result files on the NMS, for example, **/opt/file**:

> **lcd** ***/opt/file***

Step 2 Log in to Trace Server in FTP or SFTP mode.

If You Need To...	Then...
Log in to Trace Server in FTP mode	Run the following command: **ftp** ***IP address of Trace Server***
Log in to Trace Server in SFTP mode	Run the following command: **sftp** ***user name@IP address of Trace Server***

NOTE

SFTP is recommended because it is more secure than FTP.

Step 3 Enter the password as prompted. The following uses the login in SFTP mode as an example.

Step 4 Run the following command to enter the directory for saving northbound trace result files on Trace Server:

> **cd /export/home/omc/var/fileint/***TSNBI/FileType/yyyymmdd/NE identifier/*

NOTE

FileType indicates the data type, such as LTE_CELL_TRC or LTE_SIG. *yyyymmdd* indicates the date. *NE identifier* includes **NE Name** and **NE FDN**.

Step 5 If the NMS obtains northbound result files in FTP mode, run the following command to set the transfer mode to binary. Otherwise, skip this step.

> **bin**

Step 6 Run the following command to download northbound result files:

> **get** *Northbound result file name*

Step 7 Run the **bye** command to exit the FTP or SFTP login mode.

Step 8 Check the obtained northbound result files.

1. Based on file names, check whether NE information, data types, and time are consistent with those in the event subscription task issued by a customer.
2. Parse the standard signaling northbound files. For details, see 2.5 Formats of Standard Signaling Northbound Result Files.

   If parsed data in files is consistent with signaling data that a customer subscribes to, the standard signaling northbound file interface meets the interconnection requirements. Otherwise, contact Huawei technical support engineer.

----End

4.4 Optional: Setting the Northbound Push FTP Server

Before commissioning the XFTP northbound file push function, you need to set an FTP server to receive data. After the FTP server is set successfully, Trace Server will scan the northbound files every 5 minutes and push the scanned files to the specified FTP server.

Prerequisites

- You have logged in to MAE.
- The mediation software of the NE has been installed on the MAE server.
- You have loaded the northbound trace licenses on MAE.
- You must have the permission of file server setting.

NOTE

- If you need to set the transmission mode between MAE co-deployed in the cluster system and the NMS to SFTP, see the "Configuring the SFTP for Actively Transferring Files over the Northbound Interface (Public and Private Keys)" or "Configuring the SFTP for Actively Transferring Files over the Northbound Interface (Password Authentication)" section for a specific MAE networking mode in the administrator guide.
- If you need to set the transmission mode between independently-deployed Trace Server and the NMS for the authentication to SFTP, see 5.3 Configuring the SFTP for Actively Transferring Files over the Northbound Interface (Public and Private Keys) or 5.4 Configuring the SFTP for Actively Transferring Files over the Northbound Interface (Password Authentication).

Procedure

Step 1 In the **Apps** area of the MAE home page, click **Access** to enter the MAE-Access home page.

Step 2 Choose **Software** > **FTP Auto Upload Management** > **Target Server Settings**. The **Target Server Setting** window is displayed.

Step 3 Set **Module Type** to **Trace Server NBI** and click **Add**. The **Target Server Settings** dialog box is displayed.

Step 4 In the **Target Server Settings** dialog box, set **Server IP**, **User Name**, **Password**, **Server Directory**, **Source Directory**, and **File Compression Type** parameters.

----End

5 Troubleshooting for the Standard Signaling Northbound Result File Interface

About This Chapter

The NMS is interconnected with Trace Server through the standard signaling northbound file interface. If problems occur when you obtain standard signaling data northbound of NEs on the network, you can resolve problems using the methods described in this section.

When Trace Server actively uploads files to the NMS over the northbound interface, Trace Server functions as an FTP client and the NMS functions as an FTP server. To ensure data security during file transmission, you can set the SFTP encryption mode.

When Trace Server actively uploads files to the NMS over the northbound interface, Trace Server functions as an FTP client and the NMS functions as an FTP server. To ensure data security during file transmission, you can set the SFTP encryption mode.

5.1 Troubleshooting and Information Collection

If faults occur when the NMS attempts to obtain standard signaling data northbound results of NEs through the standard signaling northbound result file interface, you can handle the faults by referring to common troubleshooting methods. If uncommon faults occur, collect information about the faults by following the instructions provided and contact Huawei technical support.

Common Troubleshooting

Table 5-1 lists methods for handling common faults that may occur when the NMS collects standard signaling data northbound of NEs.

Table 5-1 Common Troubleshooting

Common Fault	Troubleshooting Method
No standard signaling northbound result file is generated.	See 5.2 Handle the Problem That No Standard Signaling Northbound Result File Is Generated.

Information Collection

If uncommon faults occur when the NMS attempts to obtain the standard signaling data northbound of the NEs, you need to collect related information to locate the faults. For details about how to collect fault information, see Table 5-2.

Table 5-2 Information collection

Related Information	Description
Operation information	Record the operations performed before a fault occurs and the troubleshooting measures taken later.
Version information	Obtain version information about Trace Server and MAE-Access, NE mediations, and NEs.
IP information	Obtain IP addresses of Trace Server and MAE.
Log information	• If Trace Server is co-deployed in a cluster system, obtain logs from the **/export/home/osslog/MAE/TSCollector/log/iMAP.tscollector***XXXX***_agent.trace** and **/export/home/osslog/MAE/TSCollector/log/TS_CBB/***XX***/***XX***/CBB.log** directories on Trace Server nodes. **NOTE** • In **tscollector***XXXX*, the first two digits *XX* indicate the server number, and the last two digits *XX* indicate the number of the service on the server. • In **/export/home/osslog/MAE/TSCollector/log/TS_CBB/***XX***/***XX***, *XX* indicates the number of the service on the server. • If Trace Server is independently deployed in a cluster system, obtain logs from the **/export/home/osslog/TS/TSCollector/log/iMAP.tscollector***XXXX***_agent.trace** and **/export/home/osslog/TS/TSCollector/log/TS_CBB/***XX***/***XX***/CBB.log** directories

Related Information	Description
	on nodes. **NOTE** • In **tscollector***XXXX*, the first two digits *XX* indicate the server number, and the last two digits *XX* indicate the number of the service on the server. • In **/export/home/osslog/TS/TSCollector/log/TS_CBB/***XX*/*XX*/*XX*, *XX* indicates the number of the service on the server. • For the Trace Server system deployed in upgrade mode, the log path is **/export/home/osslog/*TS-X*/TSCollector/log**. Replace *X* in *TS-X* as required.

5.2 Handle the Problem That No Standard Signaling Northbound Result File Is Generated

Either of the following causes may lead to the problem that no standard signaling northbound result file is generated: NEs are disconnected, or the disk space of Trace Server is insufficient. This section describes how to handle this problem in either of the two situations

Problem Description

No standard signaling northbound result file is generated in the path, and the NMS cannot collect standard signaling northbound results of NEs.

Problem Analysis

Either of the following causes can result in the problem:

- NEs are disconnected.
- The disk space of Trace Server is insufficient.

Analysis of NE Disconnection

1. In the **Apps** area of the MAE home page, click **Access** to enter the MAE-Access home page.
2. Choose **Topology** > **Main Topology** from the main menu. On the **Main Topology** page, right-click a disconnected NE, and then choose **Reconnect NE** from the shortcut menu.
3. Check whether the network connection is normal.
4. Debug the NE mediation. To reinstall the NE mediation, see *Commissioning Guide* of the corresponding Trace Server networking mode.

Analysis of the Insufficient Disk Space of Trace Server

Clean up the disk space of Trace Server.

NOTICE

You must check whether files can be deleted when clearing the disk space. If files are deleted incorrectly, the system may run improperly.

Solution

Contact Huawei technical support.

5.3 Configuring the SFTP for Actively Transferring Files over the Northbound Interface (Public and Private Keys)

When Trace Server actively uploads files to the NMS over the northbound interface, Trace Server functions as an FTP client and the NMS functions as an FTP server. To ensure data security during file transmission, you can set the SFTP encryption mode.

Prerequisites

You have logged in to the NMS server as user *UserA*. *UserA* is the NMS server user. Replace it as required.

Context

- To set up an SFTP connection using public or private key authentication, save the public key file for the Trace Server server in the **authorized_keys** file of the related NMS server user. The system performs authentication using the private key for the Trace Server server and the public key for the Trace Server server stored on the NMS server. After the authentication is successful, the SFTP connection is set up successfully. Trace Server is not required to provide the NMS login password.
- The public and private key authentication files can be encrypted or not. For encrypted public and private key authentication files, set the password. If you forget the password, all public and private key authentication files must be generated again, and the new files will replace the existing files.
- When the XFTP service uploads files in FTP mode:
  - If the northbound server runs the Linux or Unix operating system, use the vsftpd software whose version is 2.0.5 or later.
  - If the northbound server runs the Windows operating system, use the ftpserver service delivered with the system.
- Unless otherwise specified, perform the following operations on each Trace Server node:

NOTE

- xftp-x-1 indicates the XFTP service name of the Trace Server server. Replace it as required.
- The service is deployed on the master and slave servers. The service name for the master server is xftp-1-1. The service name for the first slave server is xftp-2-1. The service name for the second slave server is xftp-3-1. This method applies to the service names for other servers.

Procedure

Step 1 Use PuTTY to log in to Trace Server as the **sopuser** user in SSH mode.

Step 2 Run the following command to switch to the **ossuser** user:

> **su - ossuser**

```
Password: password for the ossuser user
```

Step 3 Public and private key files are generated on the Trace Server master service server.

If You Need To...	Then...
Generate encrypted public and private key files	Only perform Step 3.1 to Step 3.4.
Generate non-encrypted public and private key files	Only perform Step 3.5 to Step 3.8.

1. Run the following command on Trace Server to check whether the **.ssh** directory exists in the home directory.

   ~> **cd /export/home/omc/.ssh/**

   - If **No such file or directory** is displayed, the **.ssh** directory is unavailable in the home directory. Perform Step 3.3 after running the following commands:

     ~> **mkdir -p /export/home/omc/.ssh/**

     ~> **cd /export/home/omc/.ssh/**

   - If no command output is displayed, the **.ssh** directory is available in the home directory. Perform Step 3.2.

2. Run the following command to check whether the **id_rsa_pwd.pub** file exists.

   ~> **ls id_rsa_pwd.pub**

   - If the system displays **id_rsa_pwd.pub: No such file or directory**, perform Step 3.3 to create a public key file.
   - If the system displays **id_rsa_pwd.pub**, perform Step 4.

3. Run the following command to create encrypted public and private key files.

   ~> **. /opt/oss/apps/OSSToolService/bin/ssh-keygen.sh**

   If the system displays the following message, enter **1** to create encrypted public and private key files.

   ```
   ------------------------------------------------------------------
   Please select an operation type:
   1--Generate PubKey File with Encrypt Key.
   2--Generate PubKey File without Encrypt Key.
   ------------------------------------------------------------------
   Please make a choice : 1
   ```

   If the system displays the following message, enter **/export/home/omc/.ssh/id_rsa_pwd**.

   ```
   Generating public/private rsa key pair.
   Enter file in which to save the key (/export/ossuser/.ssh/id_rsa):
   ```


If the following message is displayed, enter the password twice. When ~> is displayed, the encrypted public key file is generated.

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

NOTICE

- Keep the password for future use. If the password is lost, all public and private key files must be generated again, and the new files will replace the existing files.
- The password can contain 8 to 30 characters, including lowercase letters a to z, uppercase letters A to Z, digits 0 to 9, and special characters]@%-=_.}{. To improve password security, the password must meet the following requirements:
- The password contains at least one uppercase letter.
- The password contains at least one lowercase letter.
- The password contains at least one digit.
- The password contains at least one special character.

4. Run the following commands to modify permission of the public key file.

   ~> **cd /export/home/omc/.ssh/**

   ~> **chmod 600 id_rsa_pwd.pub**

5. Run the following command on the Trace Server master service server to check whether the **.ssh** directory exists in the home directory.

   ~> **cd ${HOME}/.ssh/**

   - If **No such file or directory** is displayed, the **.ssh** directory is unavailable in the home directory. Perform Step 3.7 after running the following command:

     ~> **mkdir -p ${HOME}/.ssh/**

   - If no command output is displayed, the **.ssh** directory is available in the home directory. Perform Step 3.6.

NOTE

The **${HOME}** parameter indicates the home directory of user **ossuser**.

6. Run the following command to check whether the **id_rsa** file exists.

   ~> **ls id_rsa**

   - If the system displays **id_rsa: No such file or directory**, perform Step 3.7 to create public and private key files.
   - If the system displays **id_rsa**, perform Step 4.

7. Run the following command to create non-encrypted public and private key files.

   ~> **. /opt/oss/apps/OSSToolService/bin/ssh-keygen.sh**

   If the system displays the following message, enter **2** to create non-encrypted public and private key files.

```
----------------------------------------------------------------
Please select an operation type:
1--Generate PubKey File with Encrypt Key.
2--Generate PubKey File without Encrypt Key.
```



```
----------------------------------------------------------------
Please make a choice : 2
```

If the system displays information similar to the following, the non-encrypted public key file has been created successfully:

```
Generating public/private rsa key pair.
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
```

8. Run the following commands to modify permission of the public key file.

   ~> **cd ${HOME}/.ssh/**

   ~> **chmod 600 id_rsa.pub**

Step 4 Enable public key authentication on the NMS.

1. Log in to the NMS server as user **UserA**. Run the **cd ${HOME}/.ssh/** command to check whether the **.ssh** directory exists in the home directory.
   - If **No such file or directory** is displayed, the **.ssh** directory is unavailable in the home directory. After running the **mkdir -p ${HOME}/.ssh/** command, perform Step 4.2.
   - If no command result is displayed, the **.ssh** directory is available in the home directory. Perform Step 4.2.

   NOTE

   The **${HOME}** parameter indicates the home directory of user **UserA**.

2. Run the **ls authorized_keys** command to check whether the **authorized_keys** file exists.
   - If the system displays **authorized_keys: No such file or directory**, run the **touch authorized_keys** command to create the **authorized_keys** file. Then, perform Step 4.3.
   - If the system displays **authorized_keys**, proceed to Step 4.3.
3. Copy the content of the **id_rsa.pub** or **id_rsa_pwd.pub** file on the Trace Server server to the **authorized_keys** file on the NMS server.

NOTICE

- For a non-encrypted public key file, copy the **id_rsa.pub** file's content.

  If the **id_rsa.pub** file does not exist, copy the **${HOME}/.ssh/authorized_keys** file's content on Trace Server.
- For an encrypted public key file, copy the **id_rsa_pwd.pub** file's content.

   a. Run the **cat id_rsa.pub** or **cat id_rsa_pwd.pub** command on the Trace Server server. The content of the **id_rsa.pub** or **id_rsa_pwd.pub** file is displayed.
   b. Run the vi command on the NMS server to write the content of the **id_rsa.pub** or **id_rsa_pwd.pub** file into the **authorized_keys** file.

NOTICE

- The content to be written into the **authorized_keys** file cannot contain any line feed. If any line feed exists, delete it.
- If the **authorized_keys** file contains any other data, perform a line feed operation. Then, write the content.

4. Run the vi command to modify the **/etc/ssh/sshd_config** file and configure SFTP parameters on the NMS server.

   su - root

   Password: *password for the root user*

   # **vi /etc/ssh/sshd_config**

   Table 5-3 lists the parameters to be configured.

Table 5-3 Parameters to be configured for the SFTP

Parameter	Value
RSAAuthentication	yes
PubkeyAuthentication	yes
AuthorizedKeysFile	.ssh/authorized_keys
PasswordAuthentication	yes/no. This parameter specifies whether the password authentication is used when the authentication of the public key and private key fails. You are advised to set this parameter to **yes**. • yes: password authentication is used. • no: password authentication is not used.

MaxStartups	Number of concurrent connections.
	The calculation method is as follows:
	1. Run the following command to query the number of the SFTP tasks deployed on Trace Server:
	• If the installed Trace Server software is a Chinese edition, run the following command:
	# **vi /export/home/ossshare/TS/XFTPService/etc/XFTPService/locale/zh_CN/TaskInfoCache.xml**
	NOTE
	TS is an example product alias. You can run the **ls /opt/cloud/ |grep TS** command to query the actual product alias.
	• If the installed Trace Server software is an English edition, run the following command:
	# **vi /export/home/ossshare/TS/XFTPService/etc/XFTPService/locale/en_US/TaskInfoCache.xml**
	`.....`
	`<ftpset>`
	`<dest>10.10.10.10</dest>`
	`<localpath.....`

Parameter	Value
	<localpath..... </ftpset> ..... The preceding command output is used as an example. **10.10.10.10** indicates the IP address of the northbound server, and each `localpath` value corresponds to a task. Record the number of tasks and enter **:q!** to exit the vi editor. 2. Run the following command to query the number of threads occupied by the SFTP tasks: # **cat /export/home/osshare/TS/XFTPService/etc/XFTPService/ModuleParam.xml |grep TaskThreadNum** <param name="TaskThreadNum">**10**</param> The preceding command output is used as an example. **10** indicates the number of threads occupied by the SFTP tasks. Record the number of threads. 3. The number of concurrent connections is obtained by multiplying the number of tasks by the number of occupied threads. **NOTE** If you change the number of SFTP tasks, you must change the number of concurrent connections at the same time.

5. Perform the following operations on the NMS server to check the SFTP service status.

If...	Then...
The NMS is running Euler OS	# **service sshd status** Checking for service sshd **running** • If the command result contains **running**, the SFTP service is running. Run the following command to restart the SFTP service: # **service sshd restart** • If the command result does not contain **running**, the SFTP service is disabled. In this case, contact Huawei technical support.
The NMS server is running any other OS	Contact Huawei technical support.

Step 5 If you use encrypted public and private key authentication files, perform this step. If you use non-encrypted public and private key authentication files, perform Step 6.

1. Run the following commands on Trace Server to query the password for encrypting the private key.

   ~> **. /opt/oss/oss_profile.sh**

~> **. /opt/oss/apps/XFTPService/tools/env_profile.sh > /dev/null 2>&1**

~> **/opt/oss/apps/XFTPService/bin/internal/XFTPPasswdEncrypt**

When the following information is displayed, enter the encryption password twice.

```
Please Enter Password :
Please Re-enter Password :
```

NOTICE

- The encryption password must be the same as that in Step 3.3.
- Keep the encryption password for future use. If the encryption password is lost, all public and private key files must be generated again, and the new files will replace the existing files.

The following information is displayed. **d67A29C93775A68AE21DDAF1052EBBD1** is the encryption password.

```
Success. Encrpt passwd :d67A29C93775A68AE21DDAF1052EBBD1
```

2. Run the **vi** command to change the values of **IsSupportEncrpt**, **PrivateExKeyFile**, and **EncrptKey** in the **ModuleParam.xml** file.

   This operation must be performed on each server where the *XFTPService* service is deployed.

   ~> **cd /export/home/osshare/TS/XFTPService/etc/XFTPService**

   ~> **vi ModuleParam.xml**

Table 5-4 Parameter description

Parameter	Description
IsSupportEncrpt	Change the value to **1**, indicating that the encryption password transfer mode is supported.
PrivateExKeyFile	Set this parameter to the absolute path where the public key file generated in Step 3.3 is saved, for example, **/export/home/omc/.ssh/id_rsa_pwd**.
EncrptKey	Enter the queried encryption password, for example, **d67A29C93775A68AE21DDAF1052EBBD1**.

3. Run the following command to check whether the **config** file exists:

   ~> **cd ${HOME}/.ssh/**

   - If **No such file or directory** is displayed, the **.ssh** directory is unavailable in the home directory. After running the following command. Perform the following steps.

     ~> **mkdir -p ${HOME}/.ssh/**

   - If no command output is displayed, the **.ssh** directory is available in the home directory. Perform the following steps.

   ~> **ls config**

NOTE

The **${HOME}** parameter indicates the home directory of user **ossuser**.

- If **config:No such file or directory** is displayed, the **config** file does not exist. Perform Step 5.4 after running the following command:

  ~> **touch ${HOME}/.ssh/config**

  ~> **chmod 600 ${HOME}/.ssh/config**
- If **config** is displayed, the **config** file exists. Proceed to Step 5.4.

4. Run the **vi** command to add the following contents to the **config** file:

   ~> **cd ${HOME}/.ssh**

   ~> **vi config**

```
IdentityFile /export/home/omc/.ssh/id rsa pwd
IdentityFile ~/.ssh/id_rsa
```

NOTE

If the **config** file contains the preceding information, you do not need to modify the **config** file.

Step 6 Run the Vi command on the Trace Server server to change the value of **DefaultFTPType** in the **ModuleParam.xml** file.

This operation must be performed on each server where the *XFTPService* service is deployed.

~> **cd /export/home/ossshare/TS/XFTPService/etc/XFTPService**

~> **vi ModuleParam.xml**

Search for the **DefaultFTPType** parameter and change the value to **1**.

NOTE

If **DefaultFTPType** is set to **1**, the SFTP encryption mode is used. If **DefaultFTPType** is set to **0**, the plaintext FTP mode is used.

To change the SFTP encryption mode to the plaintext FTP mode, change the value of **DefaultFTPType** to **0** and restart the XFTPService service.

Using the plaintext FTP mode has security risks. It is recommended that you use the SFTP mode.

```
<GeneralParams>
...
<param name="DefaultFTPType">1</param>
...
</GeneralParams>
```

Step 7 Run the following command to switch to the **ossadm** user:

~> **su - ossadm**

```
Password: password for the ossadm user
```

Step 8 Run the following commands on Trace Server to restart XFTPService to make the modification take effect.

This operation must be performed on each server where the *XFTPService* service is deployed.

~> **. /opt/cloud/manager/bin/engr_profile.sh**

~> **ipmc_adm -cmd restartapp -app XFTPService**

Step 9 Run the following command on Trace Server to view the XFTPService status.

This operation must be performed on each server where the *XFTPService* service is deployed.

~> **ipmc_adm -cmd statusapp -app XFTPService**

- If the xftp-x-0 service is in the **running** state in the command output, the service is running properly.
- If the xftp-x-0 service is in **not running** state in the command output, the service is not started. When this occurs, contact Huawei technical support.

----End

5.4 Configuring the SFTP for Actively Transferring Files over the Northbound Interface (Password Authentication)

When Trace Server actively uploads files to the NMS over the northbound interface, Trace Server functions as an FTP client and the NMS functions as an FTP server. To ensure data security during file transmission, you can set the SFTP encryption mode.

Prerequisites

You have logged in to the NMS server as user *UserA*. *UserA* is an NMS server user. Replace it as required.

Context

- When the password authentication is used, the password for logging in to the NMS server is required to set up an SFTP connection.
- Unless otherwise specified, perform the following operations on each Trace Server node:

NOTE

xftp-x-1 indicates the XFTP service name of the Trace Server server. Replace it as required.

The XFTP service is deployed on the master and slave servers. The service name for the master server is xftp-1-1. The service name for the first slave server is xftp-2-1. The service name for the second slave server is xftp-3-1. This method applies to the service names for other servers.

- When the XFTP service uploads files in FTP mode:
  - If the northbound server runs the Linux or Unix operating system, use the vsftpd software whose version is 2.0.5 or later.
  - If the northbound server runs the Windows operating system, use the ftpserver service delivered with the system.

Procedure

Step 1 Use PuTTY to log in to Trace Server as the **sopuser** user in SSH mode.

Step 2 Run the following command to switch to the **ossuser** user:

> **su - ossuser**

```
Password: password for the ossuser user
```

Step 3 Run the vi command to modify the **/etc/ssh/sshd_config** file and configure SFTP parameters on the NMS server.

~> **su - root**


```
Password: password for the root user
```

vi /etc/ssh/sshd_config

Table 5-5 lists the parameters to be configured.

Table 5-5 Parameters to be configured for the SFTP

Parameter	Value
PasswordAuthentication	yes/no. Set this parameter to **yes**. • yes: password authentication is used. • no: password authentication is not used.

MaxStartups	Number of concurrent connections.
	The calculation method is as follows
	1. Run the following command to query the number of the SFTP tasks deployed on Trace Server:
	• If the installed Trace Server software is a Chinese edition, run the following command:
	# **vi /export/home/ossshare/TS/XFTPService/etc/XFTPService/locale/zh_CN/TaskInfoCache.xml**
	NOTE
	TS is an example product alias. You can run the **ls /opt/cloud/ |grep TS** command to query the actual product alias.
	• If the installed Trace Server software is an English edition, run the following command:
	# **vi /export/home/ossshare/TS/XFTPService/etc/XFTPService/locale/en_US/TaskInfoCache.xml**
	`...... <ftpset> <dest>10.10.10.10</dest> <localpath...... <localpath...... </ftpset> ......`
	The preceding command output is used as an example. **10.10.10.10** indicates the IP address of the northbound server, and each `localpath` value corresponds to a task. Record the number of tasks and enter **:q!** to exit the vi editor.
	2. Run the following command to query the number of threads occupied by the SFTP tasks:
	# **cat /export/home/ossshare/TS/XFTPService/etc/XFTPService/ModuleParam.xml |grep TaskThreadNum**
	`<param name="TaskThreadNum">10</param>`
	The preceding command output is used as an example. **10** indicates the number of threads occupied by the SFTP tasks. Record the number of threads.

Parameter	Value
	3. The number of concurrent connections is obtained by multiplying the number of tasks by the number of occupied threads. **NOTE** If you change the number of SFTP tasks, you must change the number of concurrent connections at the same time.

Step 4 Perform the following operations on the NMS server to check the SFTP service status.

If...	Then...
The NMS is running Euler OS	# **service sshd status** `Checking for service sshd running` • If the command result contains **running**, the SFTP service is running. Run the following command to restart the SFTP service: # **service sshd restart** • If the command result does not contain **running**, the SFTP service is disabled. In this case, contact Huawei technical support.
The NMS server is running any other OS	Contact Huawei technical support.

Step 5 Perform the following operations on Trace Server to change the value of the **DefaultFTPType** field in the **ModuleParam.xml** file.

This operation must be performed on each server where the *XFTPService* service is deployed.

~> **cd /export/home/ossshare/TS/XFTPService/etc/XFTPService**

~> **vi ModuleParam.xml**

Search for the **DefaultFTPType** parameter and change the value to **1**.

NOTE

If **DefaultFTPType** is set to **1**, the SFTP encryption mode is used. If **DefaultFTPType** is set to **0**, the plaintext FTP mode is used.

To change the SFTP encryption mode to the plaintext FTP mode, change the value of **DefaultFTPType** to **0** and restart the XFTPService service.

```
<GeneralParams>
...
<param name="DefaultFTPType">1</param>
...
</GeneralParams>
```

Press **Esc** and run the **:wq** command to save the file and exit the vi editor.

Step 6 Run the following command to switch to the **ossadm** user:

~> **su - ossadm**

```
Password: password for the ossadm user
```

Step 7 Run the following commands on Trace Server to restart XFTPService to make the modification take effect.

This operation must be performed on each server where the *XFTPService* service is deployed.

~> **. /opt/cloud/manager/bin/engr_profile.sh**

~> **ipmc_adm -cmd restartapp -app XFTPService**

Step 8 Run the following command on Trace Server to view the XFTPService status.

This operation must be performed on each server where the *XFTPService* service is deployed.

~> **ipmc_adm -cmd statusapp -app XFTPService**

- If the xftp-x-0 service is in the **running** state in the command output, the service is running properly.
- If the xftp-x-0 service is in **not running** state in the command output, the service is not started. When this occurs, contact Huawei technical support.

----End

5.5 Setting the DST

DST is optional, depending on whether the NE is in daylight saving time (DST) mode. The DST identifier is disabled by default.

Prerequisites

- You have obtained the IP addresses of the Trace Server master service board (independently-deployed) and the MAE master server (co-deployed in the cluster system).
- You have obtained the password for the **sopuser** user.
- The trust relationship between Trace Server and MAE has been configured.

Context

NOTE

The following command output is for reference only.

Procedure

Step 1 Use PuTTY to log in to the MAE master server (Trace Server co-deployed with the MAE-Access) or Trace Server master server (Trace Server independently deployed) in SSH mode as user sopuser.

Step 2 Run the following command to switch to the **ossuser** user:

> **su - ossuser**

```
Password: password for the ossuser user
```


Step 3 Run the following commands to run the Trace Server maintenance and measurement tool:

~> **. /opt/oss/oss_profile.sh**

~> **executeScriptProxy.sh single tsNorthTools.sh**

Step 4 When information similar to the following is displayed, select **Set Trace Server Param** and press **Enter** to access the setting Trace Server parameter function.

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+                                                              +
+                                                              +
+                  Welcome to use Trace Server Toolkit                 +
+                                                              +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Please select query condition
A--Set Trace Server Param
Q--Quit
Please make a choice:
```

NOTE

You can select **Set Trace Server Param** by typing **A**.

Step 5 When information similar to the following is displayed, select **Set the DST identifier** and press **Enter** to run the setting DST identifier function.

```
A--Set the switch of the CDR
B--Set the NE label type
C--Set the WLAN Result Format
D--Set the DST identifier
Q--Quit
```

NOTE

You can select **Set the DST identifier** by typing **D**.

Step 6 When information similar to the following is displayed, select **disabled:false** or **enabled:true** and press **Enter** to change the DST identifier.

```
The value of DST in the current configuration file is false.

Please enter a DST number to be set:
A--disabled:false
B--enabled:true
Q--Quit
```

NOTE

You can select **disabled:false** or **enabled:true** by typing **A** or **B**.

Step 7 When information similar to the following is displayed, type **Y** and press **Enter** to restart the Trace Server services.

```
Are you sure to restart all Trace Server services, whether to continue (Y/N)
```

When the following information is displayed, the Trace Server services have been restarted successfully. Otherwise, contact Huawei technical support.

```
All Trace Server services restarted successfully.
```

When the following information is displayed, the modification is successful. Otherwise, contact Huawei technical support.


```
Set the DST successfully.
```

Step 8 Type **Q** and press **Enter** to return to the Trace Server maintenance and measurement tool home page.

Step 9 Type **Q** and press **Enter** to exit the Trace Server maintenance and measurement tool.

----End

6 Appendix

About This Chapter

6.1 Supported NE Types and Versions

Table 6-1 lists NE types and versions supported by the standard signaling northbound file interface.

Table 6-1 Related NE types and versions

NE Type	NE Version
BTS3900	BTS3900 V100R016C10 BTS3900 V100R016C00 BTS3900 V100R015C10 BTS3900 V100R015C00 BTS3900 V100R013C10 BTS3900 V100R013C00
BTS5900	BTS5900 V100R016C10 BTS5900 V100R016C00 BTS5900 V100R015C10 BTS5900 V100R015C00 BTS5900 V100R013C10 BTS5900 V100R013C00
PICO BTS5900	PICO BTS5900 V100R016C00 PICO BTS5900 V100R015C10 PICO BTS5900 V100R015C00 PICO BTS5900 V100R013C10

NE Type	NE Version
PICO BTS3900	PICO BTS3900 V100R016C00 PICO BTS3900 V100R015C10 PICO BTS3900 V100R015C00 PICO BTS3900 V100R013C10 PICO BTS3900 V100R013C00
MICRO BTS3900	MICRO BTS3900 V100R016C10 MICRO BTS3900 V100R016C00 MICRO BTS3900 V100R015C10 MICRO BTS3900 V100R015C00 MICRO BTS3900 V100R013C10 MICRO BTS3900 V100R013C00
eNodeB	DBS5900 LTE V100R016C10 BTS5900L LTE V100R016C10 BTS5900AL LTE V100R016C10 BTS5900A LTE V100R016C10 BTS5900 LTE V100R016C10 DBS5900 LampSite LTE V100R016C10 DBS3900 LTE V100R016C10 BTS3900L LTE V100R016C10 BTS3900AL LTE V100R016C10 BTS3900A LTE V100R016C10 BTS3900 LTE V100R016C10 BTS3901A LTE V100R016C10 BTS3901E TDLTE V100R016C10 BTS3202B V100R016C10 BTS3202E V100R016C10 BTS3203E LTE V100R016C10 BTS3205E V100R016C10 DBS5900 LTE V100R016C00 BTS5900L LTE V100R016C00 BTS5900AL LTE V100R016C00 BTS5900A LTE V100R016C00 BTS5900 LTE V100R016C00 DBS5900 LampSite LTE V100R016C00 DBS3900 LTE V100R016C00 BTS3900L LTE V100R016C00 BTS3900AL LTE V100R016C00 BTS3900A LTE V100R016C00 BTS3900 LTE V100R016C00

NE Type	NE Version
	BTS3901A LTE V100R016C00 BTS3901E TDLTE V100R016C00 BTS3202B V100R016C00 BTS3202E V100R016C00 BTS3203E LTE V100R016C00 BTS3205E V100R016C00 DBS5900 LTE V100R015C10 BTS5900L LTE V100R015C10 BTS5900AL LTE V100R015C10 BTS5900A LTE V100R015C10 BTS5900 LTE V100R015C10 DBS5900 LampSite LTE V100R015C10 DBS3900 LTE V100R015C10 BTS3900L LTE V100R015C10 BTS3900AL LTE V100R015C10 BTS3900A LTE V100R015C10 BTS3900 LTE V100R015C10 BTS3901A LTE V100R015C10 BTS3901E TDLTE V100R015C10 BTS3202B V100R015C10 BTS3202E V100R015C10 BTS3203E LTE V100R015C10 BTS3205E V100R015C10 DBS5900 LTE V100R015C00 BTS5900L LTE V100R015C00 BTS5900AL LTE V100R015C00 BTS5900A LTE V100R015C00 BTS5900 LTE V100R015C00 DBS5900 LampSite LTE V100R015C00 DBS3900 LTE V100R015C00 BTS3900L LTE V100R015C00 BTS3900AL LTE V100R015C00 BTS3900A LTE V100R015C00 BTS3900 LTE V100R015C00 BTS3901A LTE V100R015C00 BTS3901E TDLTE V100R015C00 BTS3202B V100R015C00 BTS3202E V100R015C00 BTS3203E LTE V100R015C00 BTS3205E V100R015C00

NE Type	NE Version
	DBS5900 LTE V100R013C10 BTS5900L LTE V100R013C10 BTS5900AL LTE V100R013C10 BTS5900A LTE V100R013C10 BTS5900 LTE V100R013C10 DBS5900 LampSite LTE V100R013C10 DBS3900 LTE V100R013C10 BTS3900L LTE V100R013C10 BTS3900AL LTE V100R013C10 BTS3900A LTE V100R013C10 BTS3900 LTE V100R013C10 BTS3901A LTE V100R013C10 BTS3901E TDLTE V100R013C10 BTS3202B V100R013C10 BTS3202E V100R013C10 BTS3203E LTE V100R013C10 BTS3205E V100R013C10 DBS5900 LTE V100R013C00 BTS5900L LTE V100R013C00 BTS5900AL LTE V100R013C00 BTS5900A LTE V100R013C00 BTS5900 LTE V100R013C00 DBS5900 LampSite LTE V100R013C00 DBS3900 LTE V100R013C00 BTS3900L LTE V100R013C00 BTS3900AL LTE V100R013C00 BTS3900A LTE V100R013C00 BTS3900 LTE V100R013C00 BTS3901A LTE V100R013C00 BTS3901E TDLTE V100R013C00 BTS3202B V100R013C00 BTS3202E V100R013C00 BTS3203E LTE V100R013C00 BTS3205E V100R013C00

6.2 LTE Event List

Table 6-2 Event list of LTE standard signaling

Event ID	Event Name	Interface	Introduced In	Supported
0x0100	E-RAB SETUP REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0101	E-RAB SETUP RESPONSE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0102	E-RAB MODIFY REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0103	E-RAB MODIFY RESPONSE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0104	E-RAB RELEASE COMMAND	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0105	E-RAB RELEASE RESPONSE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0106	E-RAB RELEASE INDICATION	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0107	INITIAL CONTEXT SETUP REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0108	INITIAL CONTEXT SETUP RESPONSE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0109	INITIAL CONTEXT SETUP FAILURE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x010a	UE CONTEXT RELEASE REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x010b	UE CONTEXT RELEASE COMMAND	S1	SRAN11.1 Pico 11.1	NB-IoT
0x010c	UE CONTEXT RELEASE COMPLETE	S1	SRAN11.1 Pico 11.1	NB-IoT

Event ID	Event Name	Interface	Introduced In	Supported
0x010d	UE CONTEXT MODIFICATION REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x010e	UE CONTEXT MODIFICATION RESPONSE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x010f	UE CONTEXT MODIFICATION FAILURE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0110	HANDOVER REQUIRED	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0111	HANDOVER COMMAND	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0112	HANDOVER PREPARATION FAILURE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0113	HANDOVER REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0114	HANDOVER REQUEST ACKNOWLEDGE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0115	HANDOVER FAILURE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0116	HANDOVER NOTIFY	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0117	PATH SWITCH REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0118	PATH SWITCH REQUEST ACKNOWLEDGE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0119	PATH SWITCH REQUEST FAILURE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x011a	HANDOVER CANCEL	S1	SRAN11.1 Pico 11.1	NB-IoT

Event ID	Event Name	Interface	Introduced In	Supported
0x011b	HANDOVER CANCEL ACKNOWLEDGE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x011c	eNB STATUS TRANSFER	S1	SRAN11.1 Pico 11.1	NB-IoT
0x011d	MME STATUS TRANSFER	S1	SRAN11.1 Pico 11.1	NB-IoT
0x011e	PAGING	S1	SRAN11.1 Pico 11.1	NB-IoT
0x011f	INITIAL UE MESSAGE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0120	DOWNLINK NAS TRANSPORT	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0121	UPLINK NAS TRANSPORT	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0122	NAS NON DELIVERY INDICATION	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0123	RESET	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0124	RESET ACKNOWLEDGE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0125	ERROR INDICATION	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0126	S1 SETUP REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0127	S1 SETUP RESPONSE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0128	S1 SETUP FAILURE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0129	ENB CONFIGURATION UPDATE	S1	SRAN11.1 Pico 11.1	NB-IoT

Event ID	Event Name	Interface	Introduced In	Supported
0x012a	ENB CONFIGURATION UPDATE ACKNOWLEDGE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x012b	ENB CONFIGURATION UPDATE FAILURE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x012c	MME CONFIGURATION UPDATE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x012d	MME CONFIGURATION UPDATE ACKNOWLEDGE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x012e	MME CONFIGURATION UPDATE FAILURE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x012f	DOWNLINK S1 CDMA2000 TUNNELING	S1	SRAN11.1	NB-IoT
0x0130	UPLINK S1 CDMA2000 TUNNELING	S1	SRAN11.1	NB-IoT
0x0131	UE CAPABILITY INFO INDICATION	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0132	TRACE START	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0133	TRACE FAILURE INDICATION	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0134	DEACTIVATE TRACE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0135	LOCATION REPORTING CONTROL	S1	SRAN11.1 Pico 11.1	NB-IoT

Event ID	Event Name	Interface	Introduced In	Supported
0x0136	LOCATION REPORT FAILURE INDICATION	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0137	LOCATION REPORT	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0138	OVERLOAD START	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0139	OVERLOAD STOP	S1	SRAN11.1 Pico 11.1	NB-IoT
0x013a	WRITE-REPLACE WARNING REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x013b	WRITE-REPLACE WARNING RESPONSE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x013c	eNB DIRECT INFORMATION TRANSFER	S1	SRAN11.1 Pico 11.1	NB-IoT
0x013d	MME DIRECT INFORMATION TRANSFER	S1	SRAN11.1 Pico 11.1	NB-IoT
0x013e	CELL TRAFFIC TRACE	S1	SRAN11.1	NB-IoT
0x013f	eNB CONFIGURATION TRANSFER	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0140	MME CONFIGURATION TRANSFER	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0141	KILL REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0142	KILL RESPONSE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0143	DOWNLINK UE ASSOCIATED LPPA TRANSPORT	S1	SRAN11.1 Pico 11.1	NB-IoT

Event ID	Event Name	Interface	Introduced In	Supported
0x0144	UPLINK UE ASSOCIATED LPPA TRANSPORT	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0145	DOWNLINK NON UE ASSOCIATED LPPA TRANSPORT	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0146	UPLINK NON UE ASSOCIATED LPPA TRANSPORT	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0147	UE RADIO CAPABILITY MATCH REQUEST	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0148	UE RADIO CAPABILITY MATCH RESPONSE	S1	SRAN11.1 Pico 11.1	NB-IoT
0x0151	UE CONTEXT MODIFICATION CONFIRM	S1	SRAN12.1	NB-IoT
0x0152	CONNECTION ESTABLISHMENT INDICATION	S1	SRAN12.1	NB-IoT
0x0153	UE CONTEXT SUSPEND REQUEST	S1	SRAN12.1	NB-IoT
0x0154	UE CONTEXT SUSPEND RESPONSE	S1	SRAN12.1	NB-IoT
0x0155	UE CONTEXT RESUME REQUEST	S1	SRAN12.1	NB-IoT
0x0156	UE CONTEXT RESUME RESPONSE	S1	SRAN12.1	NB-IoT
0x0157	UE CONTEXT RESUME	S1	SRAN12.1	NB-IoT

Event ID	Event Name	Interface	Introduced In	Supported
	FAILURE			
0x0158	Secondary RAT Data Usage Report	S1	SRAN15.0	NB-IoT
0x0159	E-RAB Modification Indication	S1	SRAN15.0	NB-IoT
0x015a	E-RAB Modification Confirm	S1	SRAN15.0	NB-IoT
0x0200	HANDOVER REQUEST	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0201	HANDOVER REQUEST ACKNOWLEDGE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0202	HANDOVER PREPARATION FAILURE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0203	SN STATUS TRANSFER	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0204	UE CONTEXT RELEASE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0205	HANDOVER CANCEL	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0206	LOAD INFORMATION	X2	SRAN11.1	NB-IoT
0x0207	ERROR INDICATION	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0208	X2 SETUP REQUEST	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0209	X2 SETUP RESPONSE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x020a	X2 SETUP FAILURE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x020b	RESET REQUEST	X2	SRAN11.1 Pico 11.1	NB-IoT

Event ID	Event Name	Interface	Introduced In	Supported
0x020c	RESET RESPONSE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x020d	ENB CONFIGURATION UPDATE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x020e	ENB CONFIGURATION UPDATE ACKNOWLEDGE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x020f	ENB CONFIGURATION UPDATE FAILURE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0210	RESOURCE STATUS REQUEST	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0211	RESOURCE STATUS RESPONSE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0212	RESOURCE STATUS FAILURE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0213	RESOURCE STATUS UPDATE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0214	MOBILITY CHANGE REQUEST	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0215	MOBILITY CHANGE ACKNOWLEDGE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0216	MOBILITY CHANGE FAILURE	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0217	RLF INDICATION	X2	SRAN11.1 Pico 11.1	NB-IoT
0x0218	HANDOVER REPORT	X2	SRAN11.1 Pico 11.1	NB-IoT

Event ID	Event Name	Interface	Introduced In	Supported
0x0219	CELL ACTIVATION REQUEST	X2	SRAN11.1	NB-IoT
0x021a	CELL ACTIVATION RESPONSE	X2	SRAN11.1	NB-IoT
0x021b	CELL ACTIVATION FAILURE	X2	SRAN11.1	NB-IoT
0x0221	RETRIEVE UE CONTEXT REQUEST	X2	SRAN12.1	NB-IoT
0x0222	RETRIEVE UE CONTEXT RESPONSE	X2	SRAN12.1	NB-IoT
0x0223	RETRIEVE UE CONTEXT FAILURE	X2	SRAN12.1	NB-IoT
0x0224	EN-DC X2 Setup Request	X2	SRAN15.0	NB-IoT
0x0225	EN-DC X2 Setup Response	X2	SRAN15.0	NB-IoT
0x0226	EN-DC X2 Setup Failure	X2	SRAN15.0	NB-IoT
0x0227	SgNB Addition Request	X2	SRAN15.0	NB-IoT
0x0228	SgNB Addition Request Acknowledge	X2	SRAN15.0	NB-IoT
0x0229	SgNB Addition Request Reject	X2	SRAN15.0	NB-IoT
0x022a	SgNB Reconfiguration Complete	X2	SRAN15.0	NB-IoT
0x022b	SgNB Modification Request	X2	SRAN15.0	NB-IoT
0x022c	SgNB Modification Request	X2	SRAN15.0	NB-IoT

Event ID	Event Name	Interface	Introduced In	Supported
	Acknowledge			
0x022d	SgNB Modification Request Reject	X2	SRAN15.0	NB-IoT
0x022e	SgNB Modification Required	X2	SRAN15.0	NB-IoT
0x022f	SgNB Modification Confirm	X2	SRAN15.0	NB-IoT
0x0230	SgNB Modification Refuse	X2	SRAN15.0	NB-IoT
0x0231	SgNB Change Required	X2	SRAN15.0	NB-IoT
0x0232	SgNB Change Confirm	X2	SRAN15.0	NB-IoT
0x0233	SgNB Change Refuse	X2	SRAN15.0	NB-IoT
0x0234	SgNB Release Request	X2	SRAN15.0	NB-IoT
0x0235	SgNB Release Request Acknowledge	X2	SRAN15.0	NB-IoT
0x0236	SgNB Release Request Reject	X2	SRAN15.0	NB-IoT
0x0237	SgNB Release Required	X2	SRAN15.0	NB-IoT
0x0238	SgNB Release Confirm	X2	SRAN15.0	NB-IoT
0x0239	RRC Transfer	X2	SRAN15.0	NB-IoT
0x0300	CSFBParametersRequestCDMA2000	Uu	SRAN11.1	NB-IoT
0x0301	CSFBParametersResponseCDMA2000	Uu	SRAN11.1	NB-IoT
0x0302	CounterCheck	Uu	SRAN11.1	NB-

Event ID	Event Name	Interface	Introduced In	Supported
			Pico 11.1	IoT
0x0303	CounterCheckResponse	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0304	DLInformationTransfer	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0305	HandoverFromEUTRAPreparationRequest (CDMA2000)	Uu	SRAN11.1	NB-IoT
0x0306	MasterInformationBlock	Uu	SRAN11.1	NB-IoT
0x0307	MeasurementReport	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0308	MobilityFromEUTRACommand	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x030a	RRCConnectionReconfiguration	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x030b	RRCConnectionReconfigurationComplete	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x030c	RRCConnectionReestablishment	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x030d	RRCConnectionReestablishmentComplete	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x030e	RRCConnectionReestablishmentReject	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x030f	RRCConnectionReestablishmentRequest	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0310	RRCConnectionReject	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0311	RRCConnectionRelease	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0312	RRCConnectionR	Uu	SRAN11.1	NB-

Event ID	Event Name	Interface	Introduced In	Supported
	equest		Pico 11.1	IoT
0x0313	RRCConnectionSetup	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0314	RRCConnectionSetupComplete	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0315	SecurityModeCommand	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0316	SecurityModeComplete	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0317	SecurityModeFailure	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x031a	UECapabilityEnquiry	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x031b	UECapabilityInformation	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x031c	ULHandoverPreparationTransfer (CDMA2000)	Uu	SRAN11.1	NB-IoT
0x031d	ULInformationTransfer	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0324	UEInformationRequest	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0325	UEInformationResponse	Uu	SRAN11.1 Pico 11.1	NB-IoT
0x0327	LoggedMeasurementsConfiguration	Uu	SRAN11.1	NB-IoT
0x032c	MBSFNAreaConfiguration	Uu	SRAN11.1	NB-IoT
0x0351	RRCConnectionReconfiguration-NB	Uu	SRAN12.1	NB-IoT
0x0352	RRCConnectionReconfigurationComplete-NB	Uu	SRAN12.1	NB-IoT
0x0353	RRCConnectionReestablishment-NB	Uu	SRAN12.1	NB-IoT

Event ID	Event Name	Interface	Introduced In	Supported
0x0354	RRCConnectionReestablishmentComplete-NB	Uu	SRAN12.1	NB-IoT
0x0355	RRCConnectionReestablishmentRequest-NB	Uu	SRAN12.1	NB-IoT
0x0356	RRCConnectionReject-NB	Uu	SRAN12.1	NB-IoT
0x0357	RRCConnectionRelease-NB	Uu	SRAN12.1	NB-IoT
0x0358	RRCConnectionRequest-NB	Uu	SRAN12.1	NB-IoT
0x0359	RRCConnectionSetup-NB	Uu	SRAN12.1	NB-IoT
0x035A	RRCConnectionSetupComplete-NB	Uu	SRAN12.1	NB-IoT
0x035B	RRCConnectionResume-NB	Uu	SRAN12.1	NB-IoT
0x035C	RRCConnectionResumeComplete-NB	Uu	SRAN12.1	NB-IoT
0x035D	RRCConnectionResumeRequest-NB	Uu	SRAN12.1	NB-IoT
0x035E	UECapabilityEnquiry-NB	Uu	SRAN12.1	NB-IoT
0x035F	UECapabilityInformation-NB	Uu	SRAN12.1	NB-IoT
0x0360	ULInformationTransfer-NB	Uu	SRAN12.1	NB-IoT
0x0361	DLInformationTransfer-NB	Uu	SRAN12.1	NB-IoT
0x0362	SCGFailureInformationNR	Uu	SRAN15.0	NB-IoT
0x0363	ULInformationTransferMRDC	Uu	SRAN15.0	NB-IoT
0x1211	UE Period TA	-	SRAN11.1 Pico 11.1	-

Event ID	Event Name	Interface	Introduced In	Supported
0x1212	UE Period TA MDT	-	SRAN11.1	-