eSE620X vESC V100R001C00 Operation and Maintenance

www.huawei.com

HUAWEI

Preface

- This course describes how to perform operation and maintenance (O&M) on the eSE620X vESC.

Objectives

- **After learning this course, you will be able to:**
  - Have an overview of O&M management.
  - Understand alarm, device, software, and log management.
  - Learn how to create tracing tasks.

Contents

- **eSE620X vESC O&M Management Overview**
- **eSE620X vESC Alarm Management**
- **eSE620X vESC Device Management**
- **eSE620X vESC Software Management**
- **eSE620X vESC Log Management**
- **eSE620X vESC Message Tracing Management**
- **eSE620X vESC Data Backup and Recovery**
- **eSE620X vESC Performance Management**

Definition and Functions of the LMT

The local maintenance terminal (LMT) is a logical concept. It refers to an O&M terminal with Huawei LMT software installed that connects to the O&M network for a network element (NE). You can operate and maintain NEs using the LMT.

The LMT is mainly used to locally locate and fix faults.

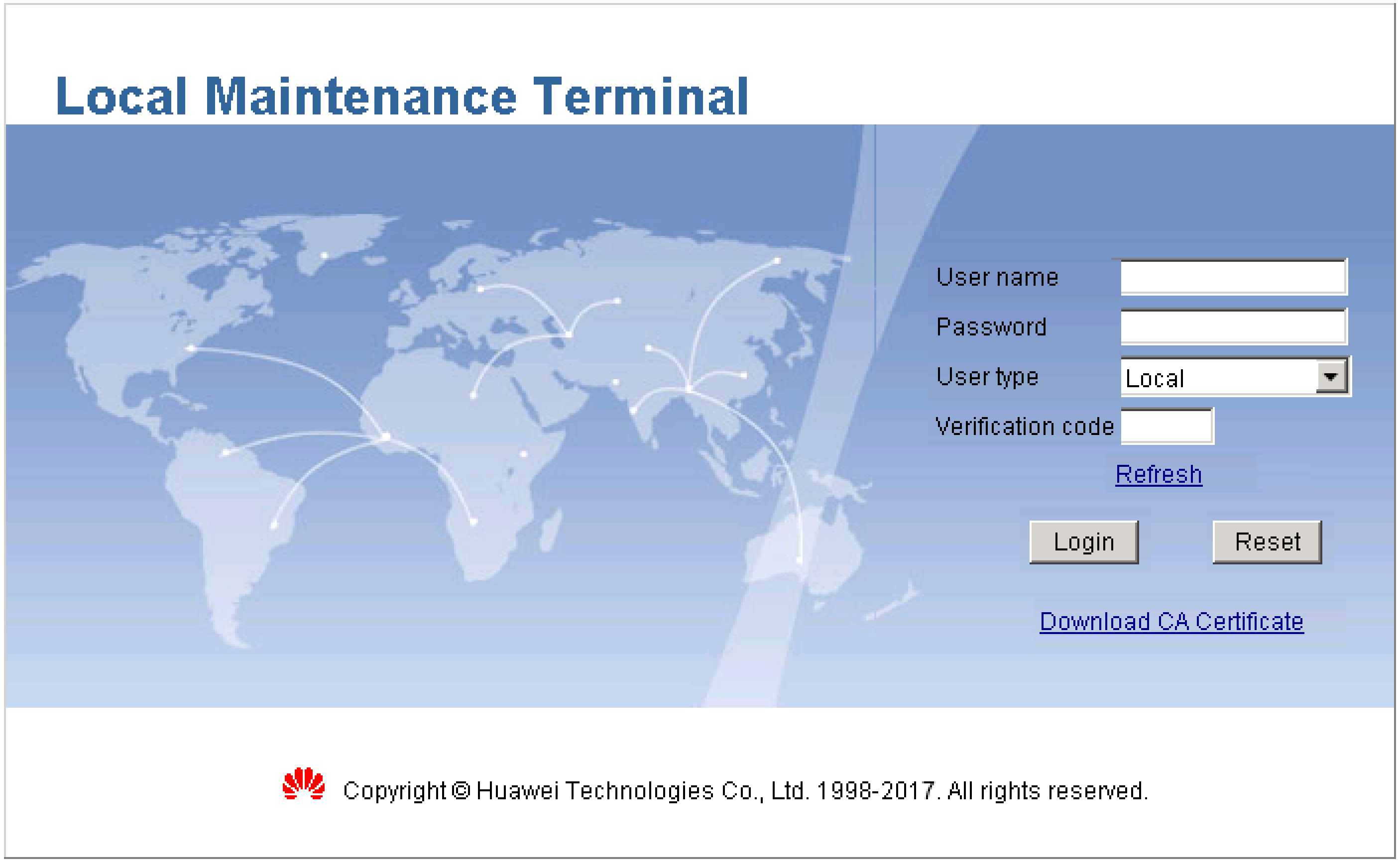
Use the LMT to operate and maintain the vESC in the following scenarios:

- Use the LMT to locally maintain the vESC.
- When alarms are generated on the eSE620X vESC, use the LMT to locate and fix the faults.

The LMT provides a Graphical User Interface (GUI), which helps users operate and maintain the vESC on the Web.

LMT Windows

- LMT login window



Local Maintenance Terminal

User name

Password

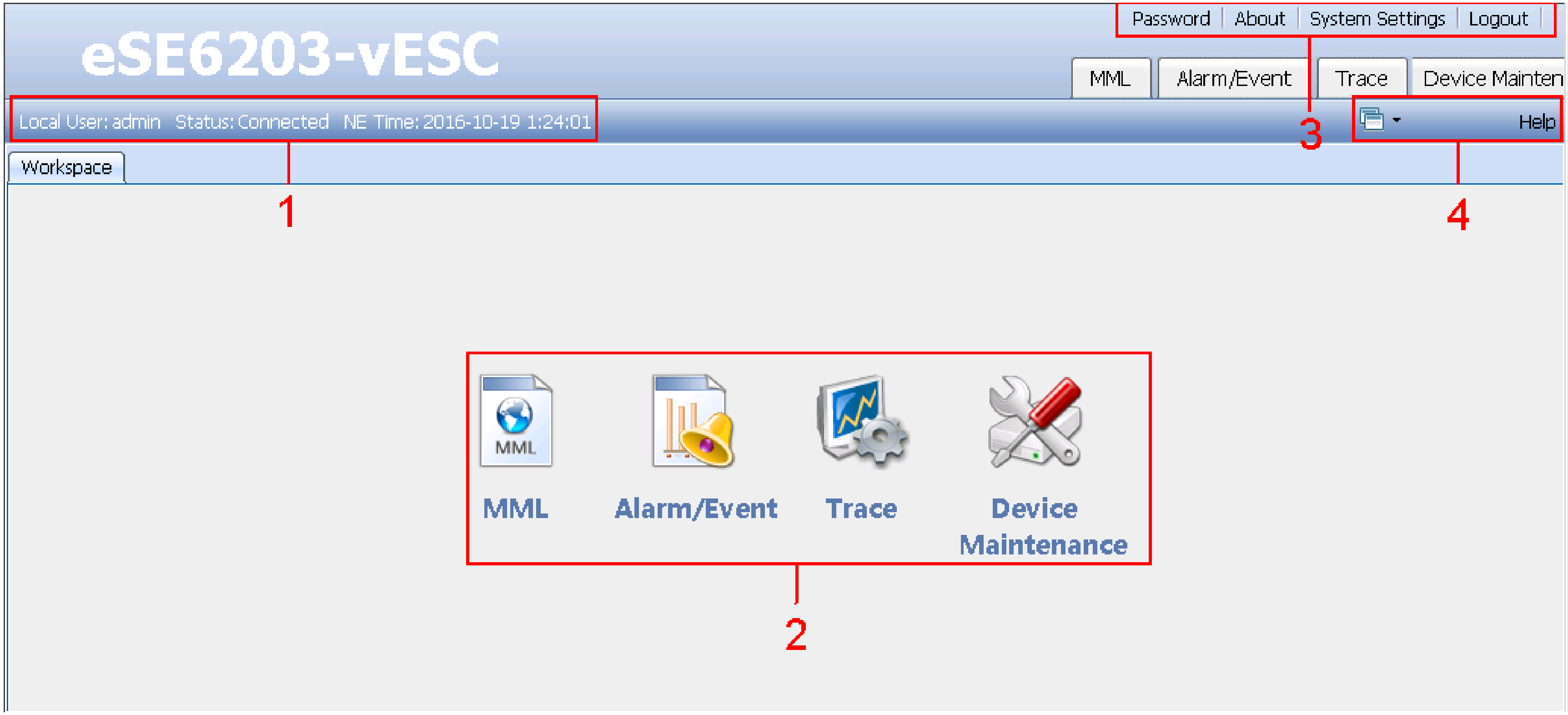
User type: Local

Verification code

Copyright © Huawei Technologies Co., Ltd. 1998-2017. All rights reserved.

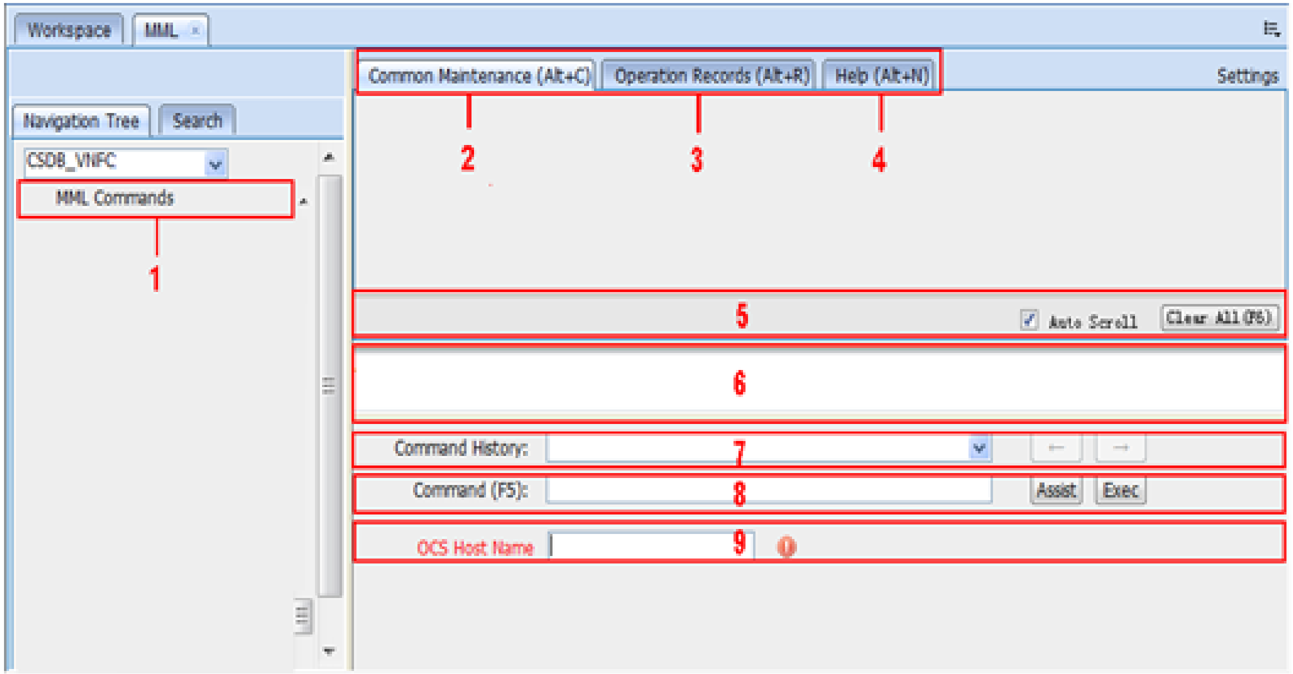
LMT Windows

LMT main window


eSE6203-vESC
Password | About | System Settings | Logout
MML
Alarm/Event
Trace
Device Mainten
Local User: admin Status: Connected NE Time: 2016-10-19 1:24:01
Help
Workspace
MML
Alarm/Event
Trace
Device Maintenance
1
2
3
4

Running MML Commands

- In the LMT main window, click the MML tab and enter the MML command window.



Introduction to MML Commands

- MML commands are used to operate and maintain the eSE620X vESC.
- The format of an MML command can be "Command Word: Parameter Name=Value;". For example, **SUB SYSLOG** is an MML command with only a command word.

Command Word	Meaning	Command Word	Meaning	Command Word	Meaning
ACT	Activate	ULD	Upload	BLK	Block
ADD	Add	DLD	Download	UBL	Unblock
RMV	Remove	RST	Reset	BKP	Back up
MOD	Modify	SET	Set		
DSP	Display (used to query dynamic information)	STP	Stop (Close)		
LST	List (used to query static information)	STR	Start (Open)		

Contents

- eSE620X vESC O&M Management Overview
- **eSE620X vESC Alarm Management**
- eSE620X vESC Device Management
- eSE620X vESC Software Management
- eSE620X vESC Log Management
- eSE620X vESC Message Tracing Management
- eSE620X vESC Data Backup and Recovery
- eSE620X vESC Performance Management

Alarm Overview

- The eSE620X vESC consists of the resource modules: vESC, MSP, and Node. The vESC realizes the logic functions of the core network, the MSP provides software platform functions, and the Node provides infrastructure functions.

Definitions

- An alarm is generated if the hardware (for example, a virtual machine (VM)) is faulty or a major function fails. An alarm has a higher severity than an event. Based on the status of the faults, alarms can be categorized into active and clear alarms.
- An event notifies users of important information when the vESC is operating correctly. Users do not need to handle an event.

Alarm Severities

Severity	Handling Suggestion
Critical	These alarms must be cleared immediately. Otherwise, the vESC may fail.
Major	These alarms must be cleared in a timely manner. Otherwise, some important functions cannot be implemented.
Minor	These alarms help maintenance personnel locate and clear potential faults before they become problems.
Warning	These alarms help maintenance personnel determine the operating status of the vESC.

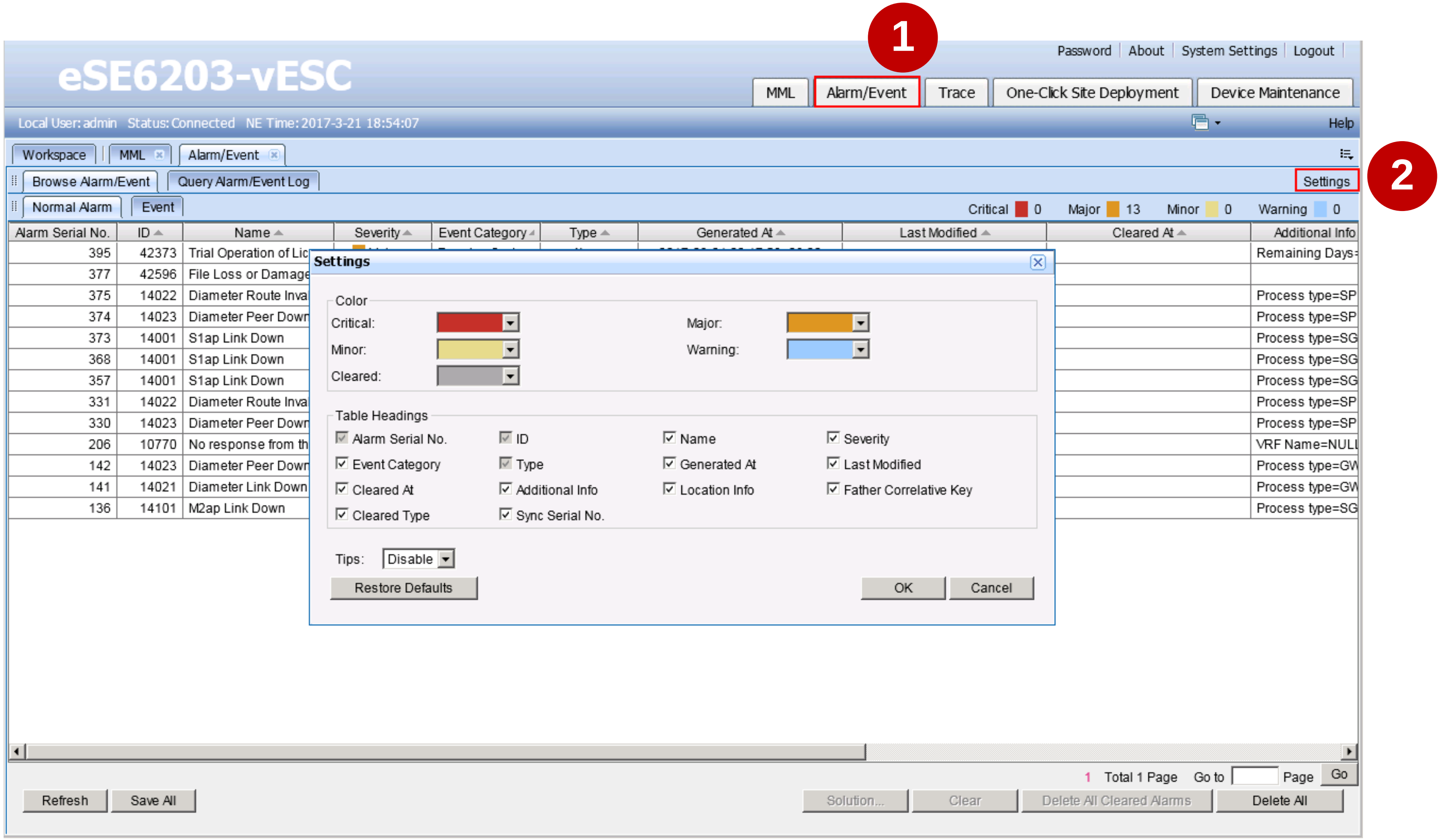
Alarm Types

- Network management alarm types
  - Power alarm
  - Environment alarm
  - Signaling alarm
  - Trunk alarm
  - Hardware alarm
  - Software alarm
  - Running alarm
  - Communication alarm

  - Quality of service (QoS) alarm
  - Integrity violation alarm
  - Operation violation alarm
  - Physical violation alarm
  - Security violation alarm
  - Time domain violation alarm
  - Processing error alarm
  - Network management system (NMS) alarm

Setting Alarm/Event Query Properties

- Setting alarm or event query properties specifies the settings in an alarm or event display dialog box. You can customize a color for each alarm or event severity, and set alarm or event display columns.



Local User: admin Status: Connected NE Time: 2017-3-21 18:54:07

Critical 🟥 0 Major 🟧 13 Minor 🟨 0 Warning 🟦 0

Alarm Serial No.	ID	Name	Severity	Event Category	Type	Generated At	Last Modified	Cleared At	Additional Info
395	42373	Trial Operation of Lic							Remaining Days=
377	42596	File Loss or Damage							
375	14022	Diameter Route Inva							Process type=SP
374	14023	Diameter Peer Down							Process type=SP
373	14001	S1ap Link Down							Process type=SG
368	14001	S1ap Link Down							Process type=SG
357	14001	S1ap Link Down							Process type=SG
331	14022	Diameter Route Inva							Process type=SP
330	14023	Diameter Peer Down							Process type=SP
206	10770	No response from th							VRF Name=NULL
142	14023	Diameter Peer Down							Process type=GW
141	14021	Diameter Link Down							Process type=GW
136	14101	M2ap Link Down							Process type=SG

1 Total 1 Page Go to Page

Settings

Color

Critical: 🟥 Major: 🟧

Minor: 🟨 Warning: 🟦

Cleared: ▨

Table Headings

☑ Alarm Serial No. ☑ ID ☑ Name ☑ Severity

☑ Event Category ☑ Type ☑ Generated At ☑ Last Modified

☑ Cleared At ☑ Additional Info ☑ Location Info ☑ Father Correlative Key

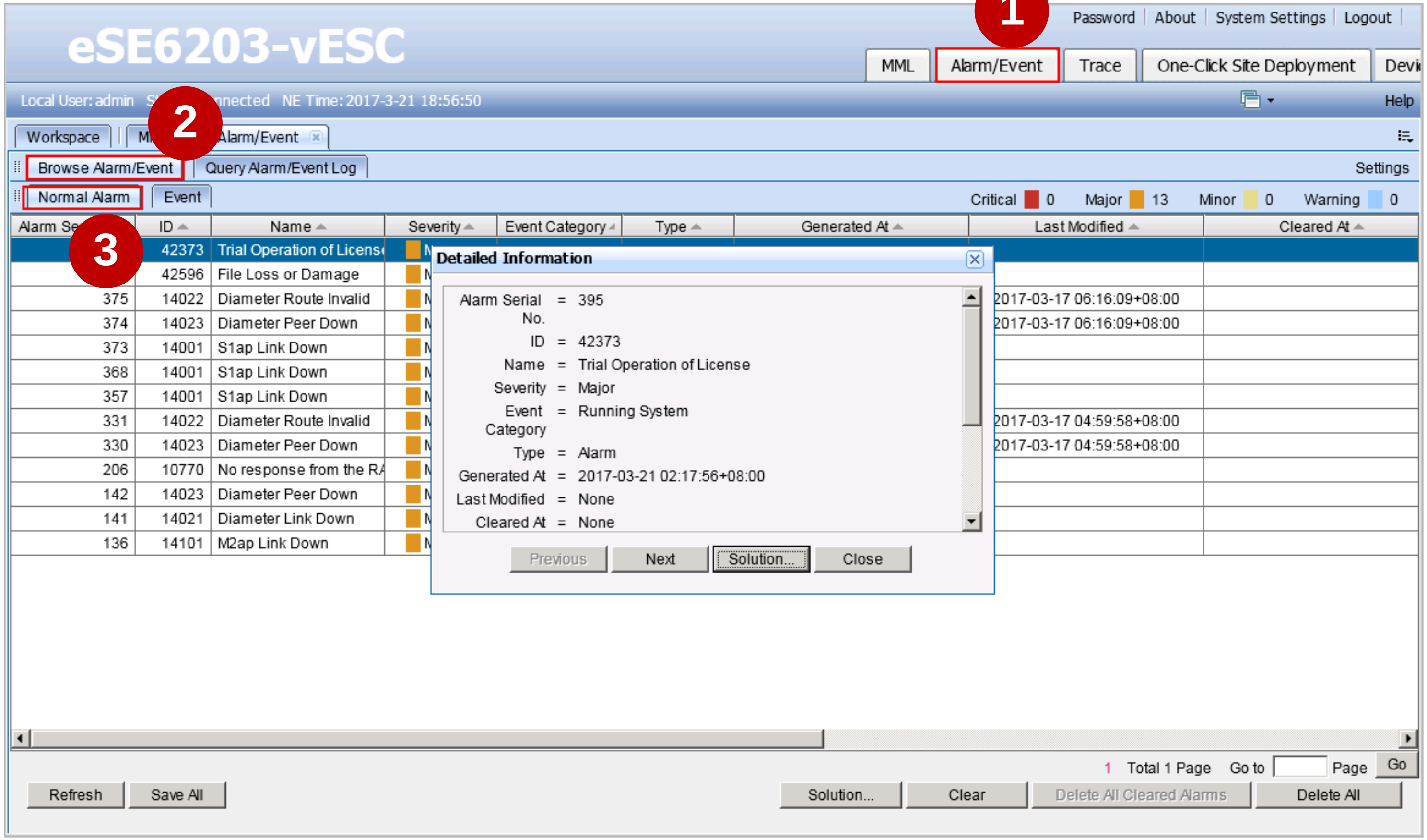
☑ Cleared Type ☑ Sync Serial No.

Tips: Disable

Restore Defaults OK Cancel

Browsing Active Alarms/Events

- Normal alarms and events reported to the LMT are displayed on the **Browse Alarm/Event** tab page in real time. You can view the detailed information about alarms and events to determine the real-time running status of the vESC.



Alarm Se	ID	Name	Severity	Event Category	Type	Generated At	Last Modified	Cleared At
	42373	Trial Operation of Licens	M					
	42596	File Loss or Damage	M					
375	14022	Diameter Route Invalid	M				2017-03-17 06:16:09+08:00	
374	14023	Diameter Peer Down	M				2017-03-17 06:16:09+08:00	
373	14001	S1ap Link Down	M					
368	14001	S1ap Link Down	M					
357	14001	S1ap Link Down	M					
331	14022	Diameter Route Invalid	M				2017-03-17 04:59:58+08:00	
330	14023	Diameter Peer Down	M				2017-03-17 04:59:58+08:00	
206	10770	No response from the RA	M					
142	14023	Diameter Peer Down	M					
141	14021	Diameter Link Down	M					
136	14101	M2ap Link Down	M					

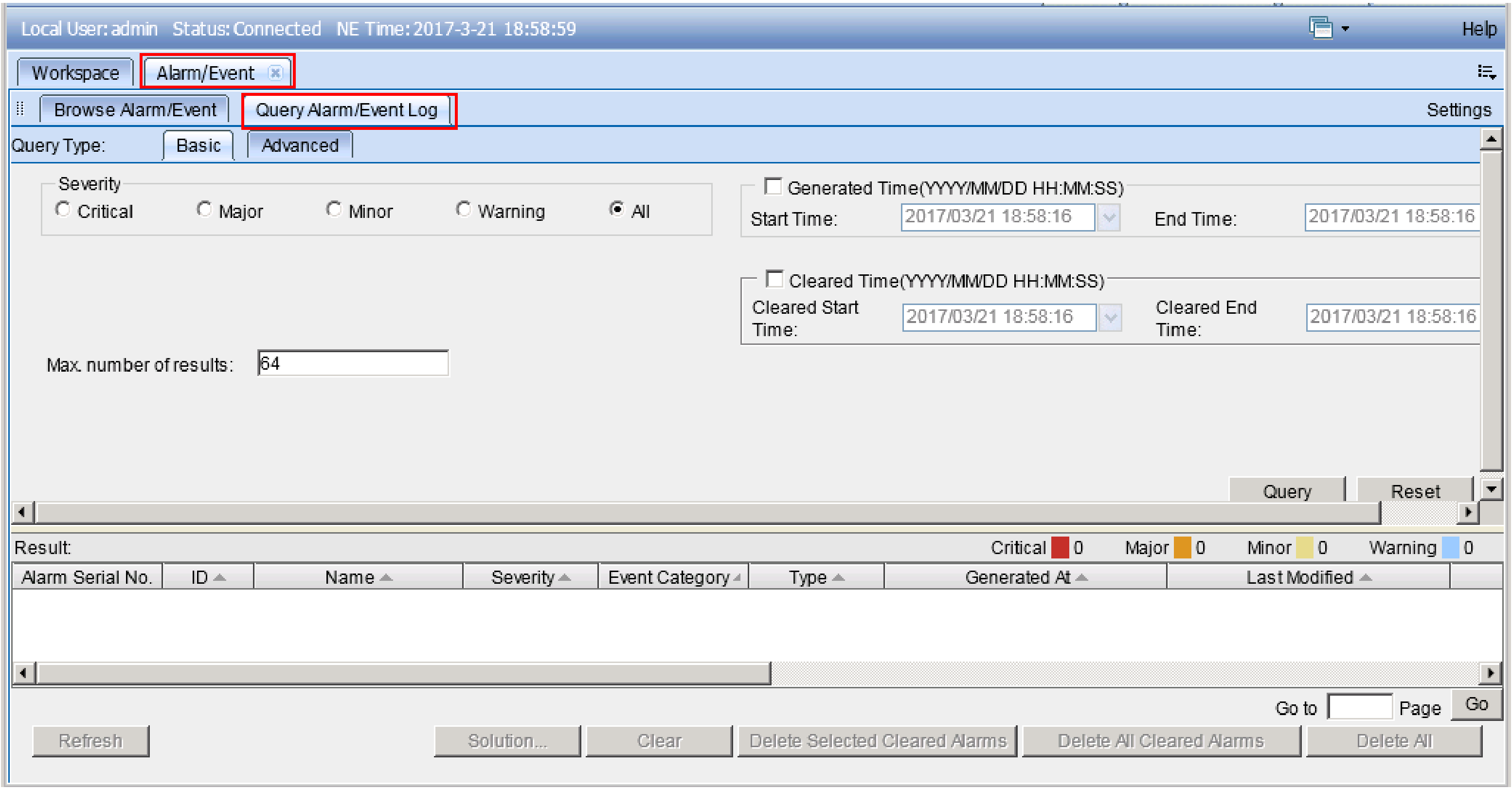
Detailed Information

Alarm Serial No.	=	395
ID	=	42373
Name	=	Trial Operation of License
Severity	=	Major
Event Category	=	Running System
Type	=	Alarm
Generated At	=	2017-03-21 02:17:56+08:00
Last Modified	=	None
Cleared At	=	None

Querying Alarm/Event Logs

- **GUI mode**

  You can query the historical alarms or events from the alarm or event logs to determine the previous running status of the equipment.



Local User: admin Status: Connected NE Time: 2017-3-21 18:58:59

Query Type: Basic

Severity: ○ Critical ○ Major ○ Minor ○ Warning ● All

□ Generated Time(YYYY/MM/DD HH:MM:SS)

Start Time: 2017/03/21 18:58:16 End Time: 2017/03/21 18:58:16

□ Cleared Time(YYYY/MM/DD HH:MM:SS)

Cleared Start Time: 2017/03/21 18:58:16 Cleared End Time: 2017/03/21 18:58:16

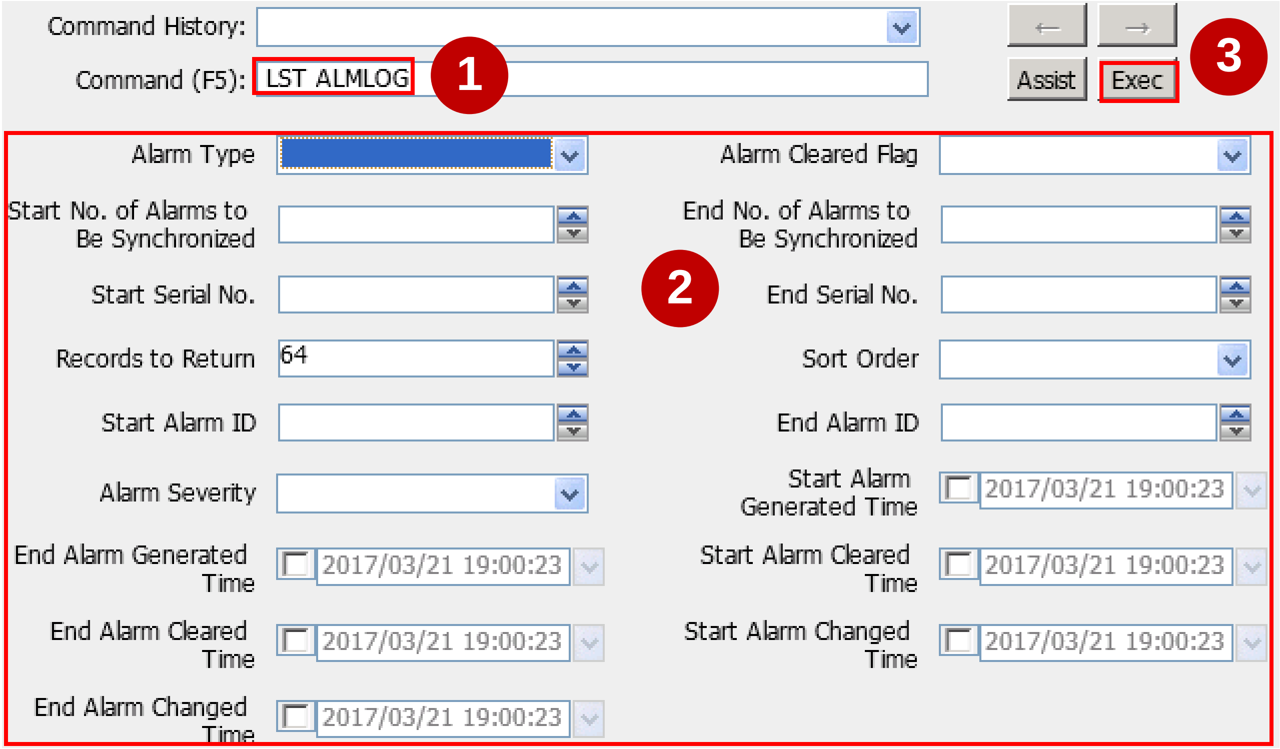
Max. number of results: 64

Result: Critical 🟥 0 Major 🟧 0 Minor 🟨 0 Warning 🟦 0

Alarm Serial No.	ID	Name	Severity	Event Category	Type	Generated At	Last Modified

Querying Alarm/Event Logs

- **Using MML commands**
- Run the **LST ALMLOG** command to query alarm or event logs.



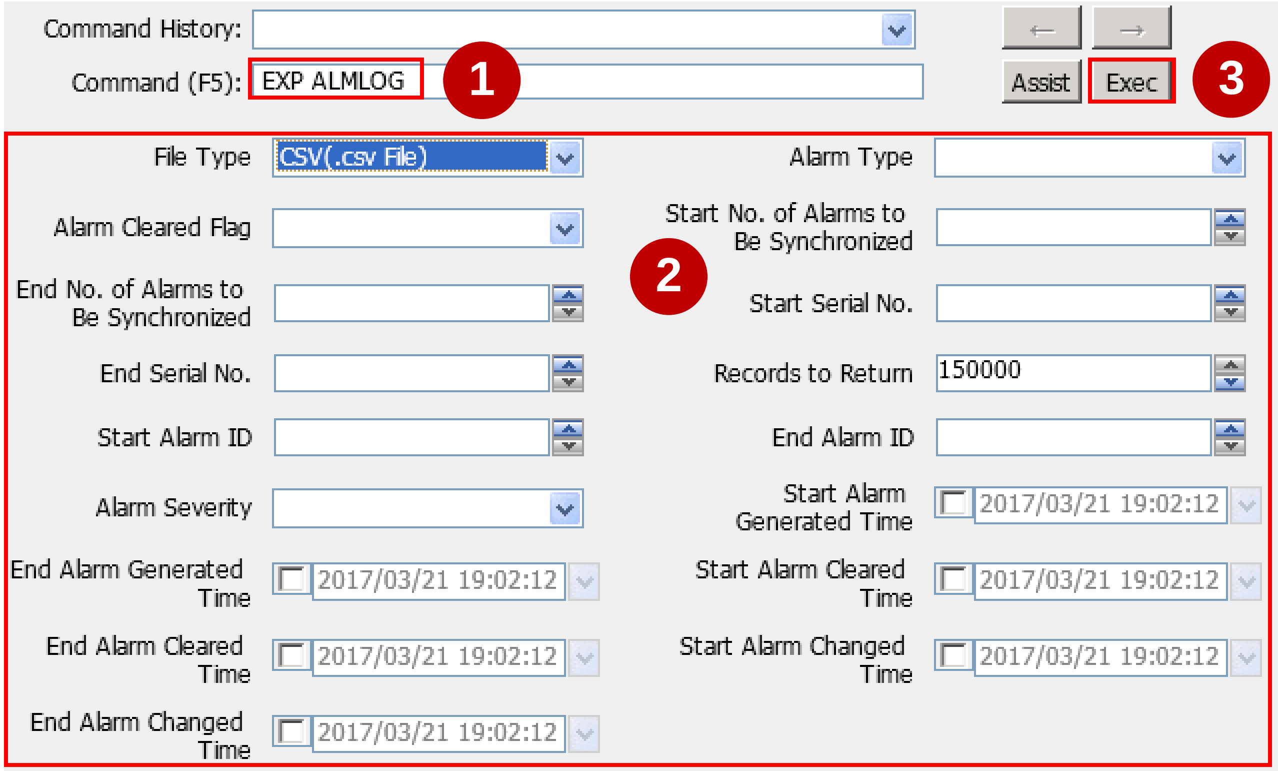
Command History:

Command (F5): LST ALMLOG

Alarm Type		Alarm Cleared Flag	
Start No. of Alarms to Be Synchronized		End No. of Alarms to Be Synchronized	
Start Serial No.		End Serial No.	
Records to Return	64	Sort Order	
Start Alarm ID		End Alarm ID	
Alarm Severity		Start Alarm Generated Time	□ 2017/03/21 19:00:23
End Alarm Generated Time	□ 2017/03/21 19:00:23	Start Alarm Cleared Time	□ 2017/03/21 19:00:23
End Alarm Cleared Time	□ 2017/03/21 19:00:23	Start Alarm Changed Time	□ 2017/03/21 19:00:23
End Alarm Changed Time	□ 2017/03/21 19:00:23		

Exporting Alarm Logs

- Run the **EXP ALMLOG** command to export alarm log records according to specified search criteria.
- The exported alarm logs are stored in ***/almexport/*** directory and the exported file name is **almlog_system time**.



Command History:

Command (F5): EXP ALMLOG

File Type: CSV(.csv File)

Alarm Type:

Alarm Cleared Flag:

Start No. of Alarms to Be Synchronized:

End No. of Alarms to Be Synchronized:

Start Serial No.:

End Serial No.:

Records to Return: 150000

Start Alarm ID:

End Alarm ID:

Alarm Severity:

Start Alarm Generated Time: □ 2017/03/21 19:02:12

End Alarm Generated Time: □ 2017/03/21 19:02:12

Start Alarm Cleared Time: □ 2017/03/21 19:02:12

End Alarm Cleared Time: □ 2017/03/21 19:02:12

Start Alarm Changed Time: □ 2017/03/21 19:02:12

End Alarm Changed Time: □ 2017/03/21 19:02:12

Common Alarm Handling Actions

- Common alarm handling actions are methods that are commonly locate and troubleshoot faults.

Common Fault Location Methods

Common Fault Location Methods	Methods Description
Comparison and Interchange	● Function description Comparison means to compare a faulty component with a functional component or compare a fault symptom with a normal symptom to find differences. This method is suitable for locating faults with specific fault ranges. Interchange means to interchange functional components (such as boards and fiber optic cables) with the components that are possibly faulty and to compare the changes in the running status before and after the interchange, to determine the scope or location of the fault. It applies to the scenario where the scope or location of the fault still cannot be determined after spare parts are changed. Interchange is generally applicable to cases in which the fault is caused by complicated factors. ● Application scenarios The hardware or software of an NE changes, or problems occur after new features are introduced. ● Use instructions Compare both the hardware and software of functional and possibly faulty components before replacement.

Common Fault Location Methods

Common Fault Location Methods	Methods Description
Segment-by-Segment Location	● Function description A problem may occur at any node in an end-to-end network. Therefore, this method helps locate the fault quickly. ● Application scenarios Transmission fails or resource-related problems occur. ● Use instructions Locate the problem segment by segment.

Common Fault Location Methods

Common Fault Location Methods	Methods Description
Layer-by-Layer Location	● Function description As specified by protocols, the upper layer can work properly only when its lower layers are working properly. When a fault occurs, all associated layers malfunction. In addition, the symptom of a fault may vary when different monitoring methods are used. Therefore, this method helps locating the layer where the fault is generated and facilitates the troubleshooting. ● Application scenarios Transmission fails or resource-related problems occur. ● Use instructions Locate the fault layer by layer.

Common Troubleshooting Methods

- After finding the root cause of a fault, you can rectify the fault and restore the system by performing proper operations based on fault details. The measures include checking and repairing lines, replacing boards, modifying configuration data, performing system switchover, and resetting VMs, hosts, or boards.

Common Methods of Collecting Fault Information

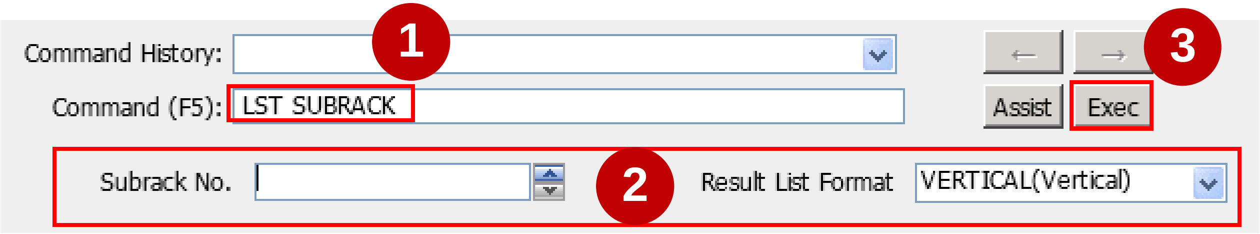
- When a fault cannot be rectified using the methods described in this troubleshooting guide, contact Huawei technical support personnel to rectify the fault and provide them with associated information.

Contents

- eSE620X vESC O&M Management Overview
- eSE620X vESC Alarm Management
- **eSE620X vESC Device Management**
- eSE620X vESC Software Management
- eSE620X vESC Log Management
- eSE620X vESC Message Tracing Management
- eSE620X vESC Data Backup and Recovery
- eSE620X vESC Performance Management

Listing Subrack Attributes

- Run the **LST SUBRACK** command to list attributes of a subrack. You can use the command to list the following attributes of a subrack: subrack number, subrack type, cabinet number and function description.



Command History:

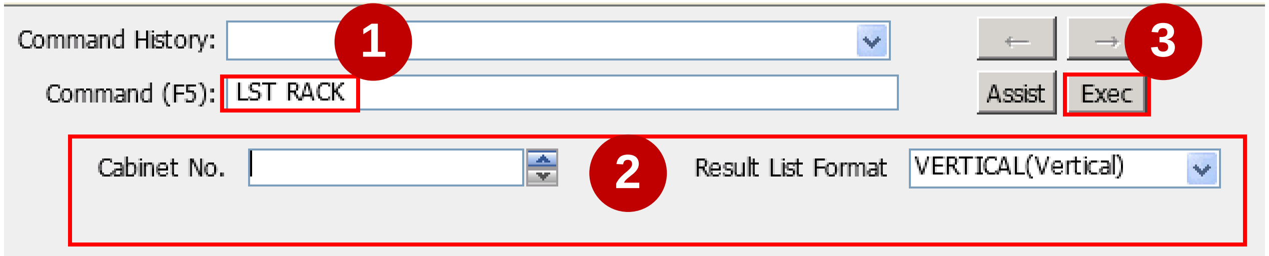
Command (F5): LST SUBRACK

Subrack No.

Result List Format: VERTICAL(Vertical)

Listing Rack Attributes

- Run the **LST RACK** command to list attributes of a cabinet. You can use the command to list the number and function description of a cabinet.



Command History:

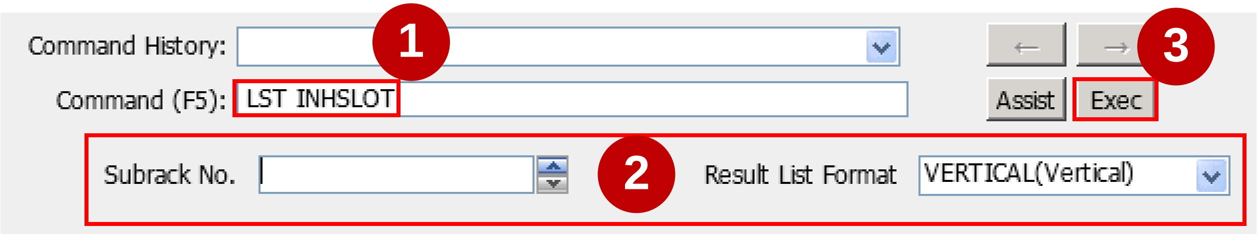
Command (F5): LST RACK

Cabinet No.

Result List Format VERTICAL(Vertical)

Listing Inhibited Slots

- Run the **LST INHSLOT** command to query the inhibited slots in a subrack.



Command History:

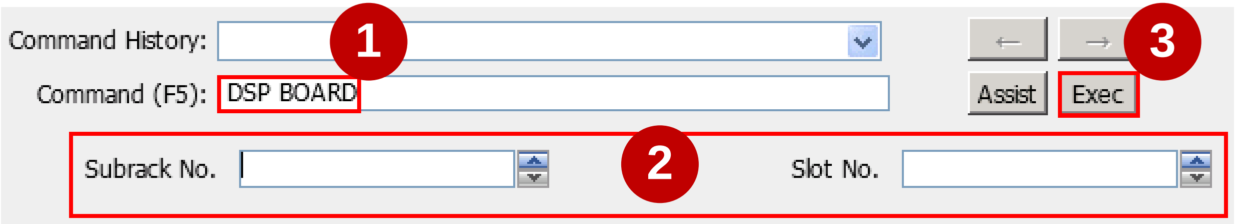
Command (F5): LST INHSLOT

Subrack No.

Result List Format: VERTICAL(Vertical)

Displaying Board Information

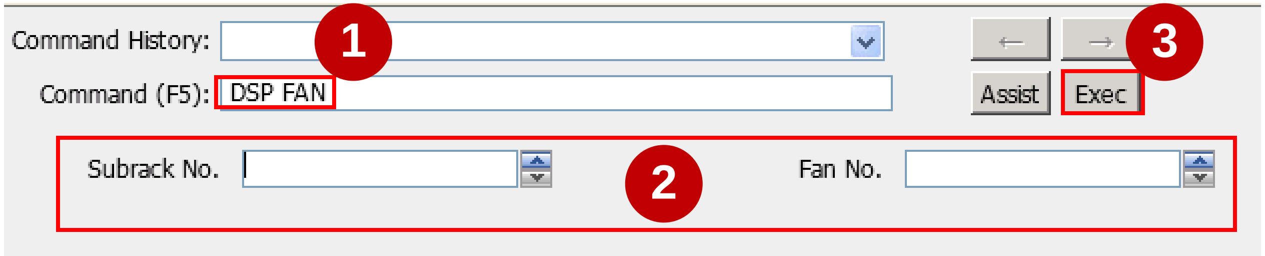
- Run the **DSP BOARD** command to query information about a board. You can use the command to query the following information about a board: subrack number, slot number, board class, board type, and availability.



DSP BOARD

Displaying Fan Information

- Run the **DSP FAN** command to query information of a fan. You can use the command to query the following information of a fan: subrack number, fan number, speed adjustment mode, and fan speed.



Command History:

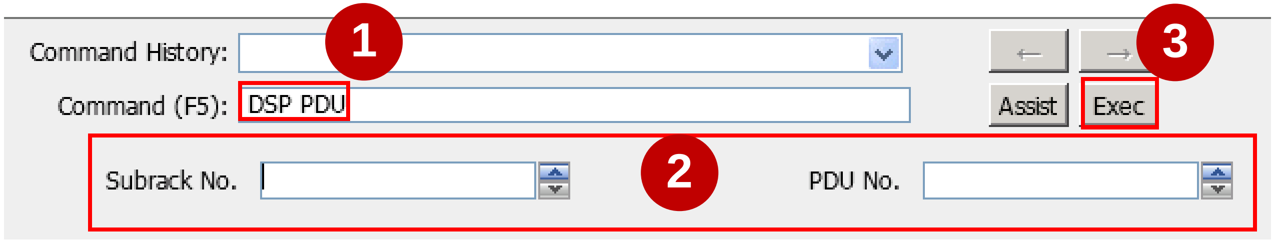
Command (F5): DSP FAN

Subrack No.

Fan No.

Displaying PDU Information

- Run the **DSP PDU** command to query information about a power distribution unit (PDU). You can use the command to query the following information of a PDU: subrack number, PDU number, PDU type, and input voltage.



Command History:

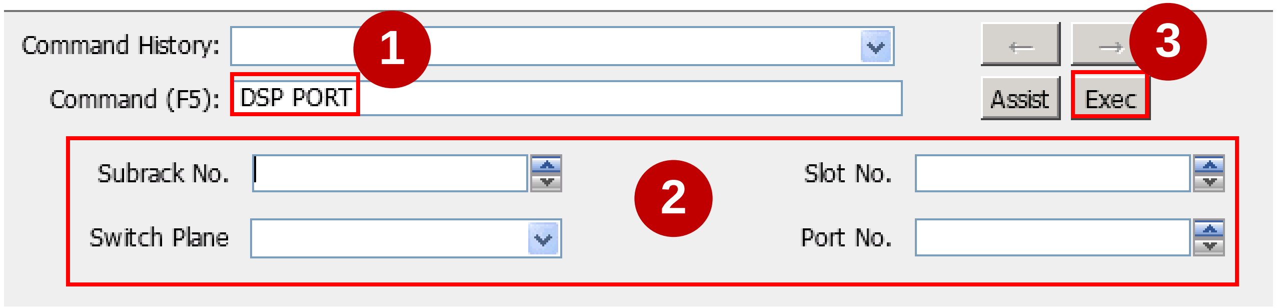
Command (F5): DSP PDU

Subrack No.

PDU No.

Displaying Port Information

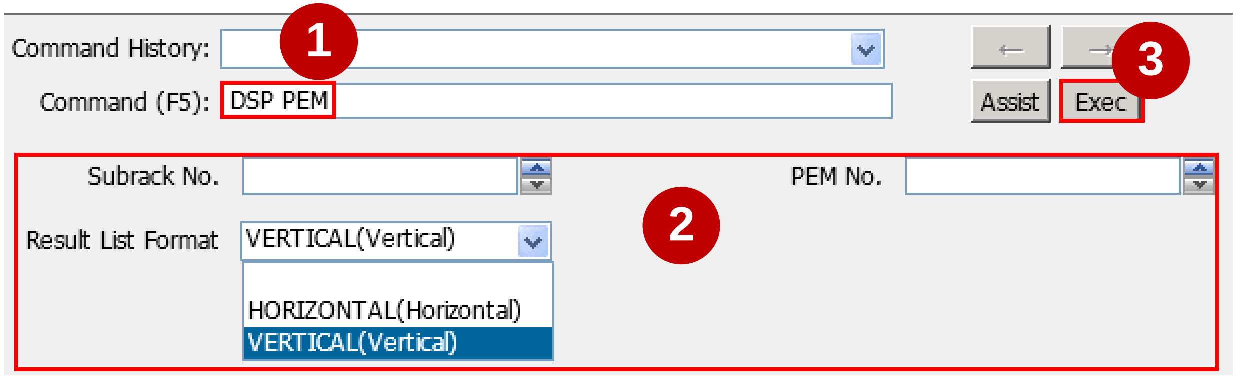
- Run the **DSP PORT** command to query information about a port. You can use this command to query the following information about a port: subrack number, slot number, switch plane, port No., board type, working mode, activation status, flow control switch, link status, allowed VLAN of the port, PVID and port isolation group ID.



Command History:	
Command (F5):	DSP PORT
Subrack No.	
Switch Plane	
Slot No.	
Port No.	

Displaying PEM Information

- Run the **DSP PEM** command to query information of the power entry module (PEM). You can use this command to query the following information: subrack No., PEM No., PEM power supply type, and PEM rated power (W).



Command History:

Command (F5): DSP PEM

Subrack No.

PEM No.

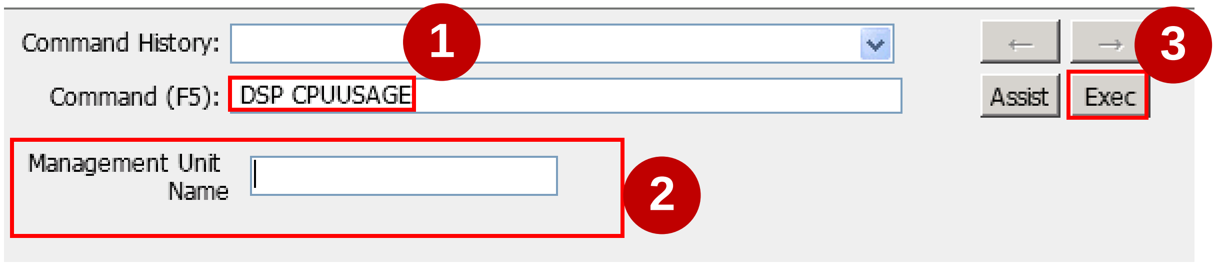
Result List Format VERTICAL(Vertical)

HORIZONTAL(Horizontal)

VERTICAL(Vertical)

Displaying CPU Usage

- Run the **DSP CPUUSAGE** command to query the CPU usage of application processes on a VM.



Command History:

Command (F5): DSP CPUUSAGE

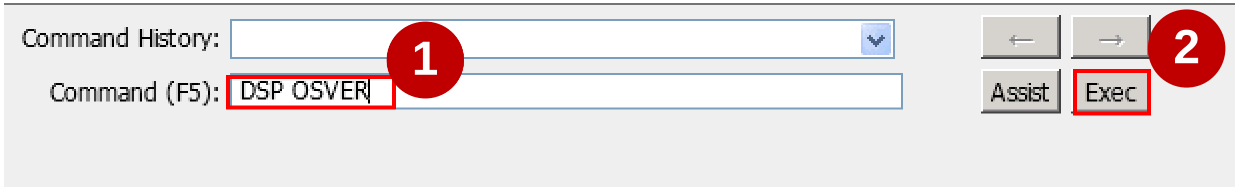
Management Unit Name

Contents

- eSE620X vESC O&M Management Overview
- eSE620X vESC Alarm Management
- eSE620X vESC Device Management
- **eSE620X vESC Software Management**
- eSE620X vESC Log Management
- eSE620X vESC Message Tracing Management
- eSE620X vESC Data Backup and Recovery
- eSE620X vESC Performance Management

Querying OS Version

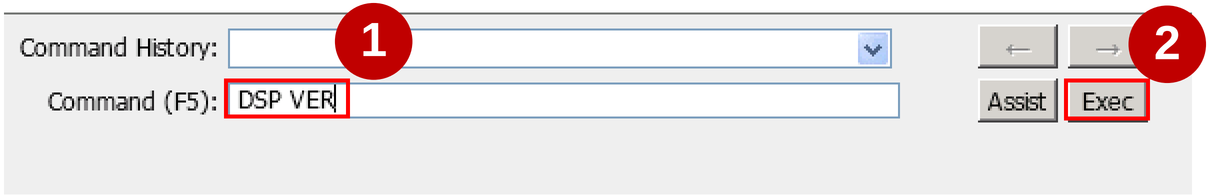
- Run the **DSP OSVER** command to query the version of an operating system (OS). If a VM is migrated, the version that the VM can be rolled back to is displayed as "NULL".



Command (F5): DSP OSVER

Querying Software Version

- Run the **DSP VER** command to query the software version. If a VM is migrated, the version that the VM can be rolled back to is displayed as "NULL".

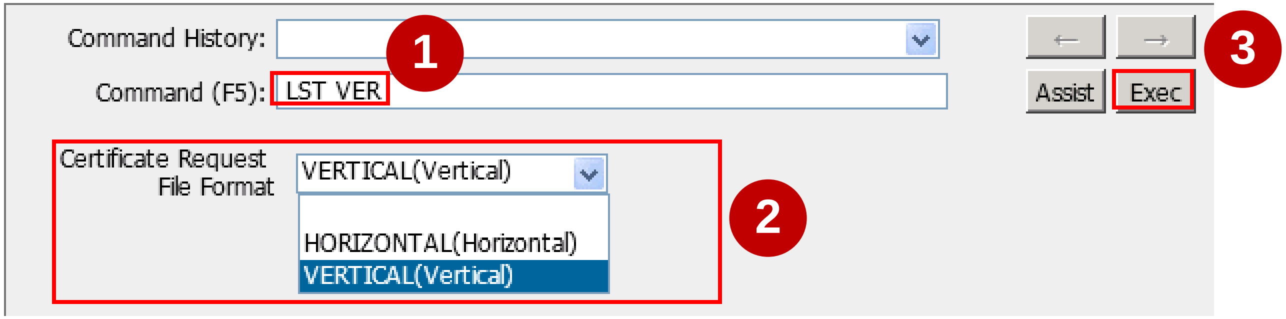


Command History:

Command (F5): DSP VER

Listing NE Version

- Run the **LST VER** command to list the version status of an NE.



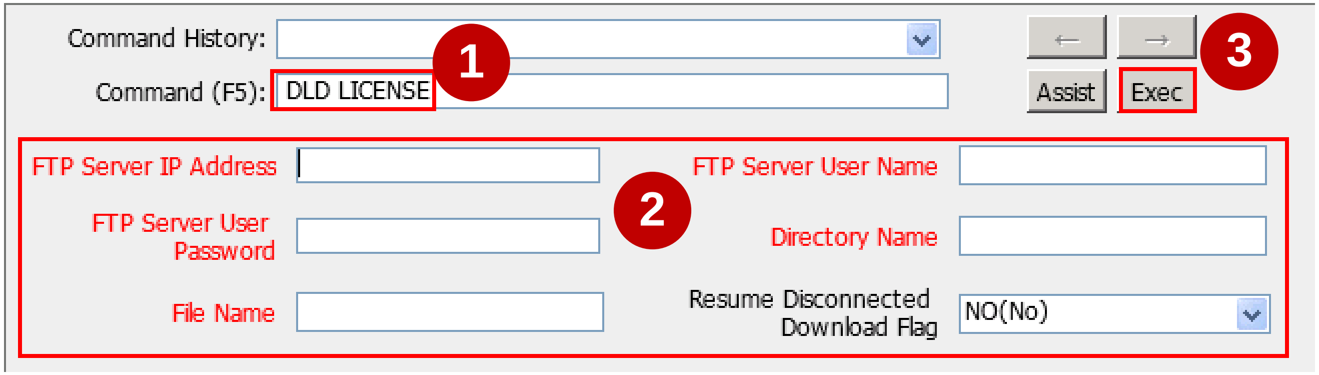
Command History:

Command (F5): LST VER

Certificate Request File Format: VERTICAL(Vertical)

Downloading a License File

- Run the **DLD LICENSE** command to download a license file from a File Transfer Protocol (FTP) server to an NE.



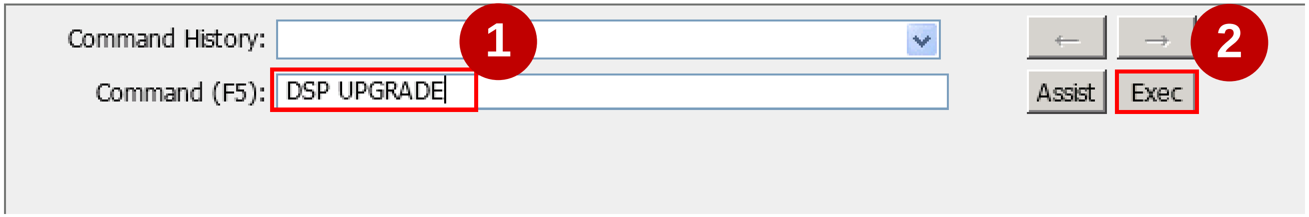
Command History:

Command (F5): DLD LICENSE

FTP Server IP Address		FTP Server User Name	
FTP Server User Password		Directory Name	
File Name		Resume Disconnected Download Flag	NO(No)

Displaying Upgrade Status

- Run the **DSP UPGRADE** command to query the information about the latest upgrade or rollback.



Command History:

Command (F5): DSP UPGRADE

Contents

- eSE620X vESC O&M Management Overview
- eSE620X vESC Alarm Management
- eSE620X vESC Device Management
- eSE620X vESC Software Management
- **eSE620X vESC Log Management**
- eSE620X vESC Message Tracing Management
- eSE620X vESC Data Backup and Recovery
- eSE620X vESC Performance Management

Common Methods of Collecting Fault Information

- When a fault cannot be rectified using the methods described in this troubleshooting guide, contact Huawei technical support personnel to rectify the fault and provide them with associated information.

Common Methods of Collecting Fault Information

Information to Be Collected		Collection Method
Version information of the faulty NE		Run the **LST NE** command to query the NE software version.
NE data		Run the **BKP DB** command and set **File Name** to specify the file for storing the data. The data is backed up in a specified directory. The default save path is **/backupdb**.
Collected log information	Performance measurement result file	Run the **COL LOG** command with **Log Type** set to **PFM_RESULT**(Performance Result) to obtain the performance measurement result file. The save path is **/COLLOGINFO/PFM_RESULT**. The normal measurement period is either 30 or 60 minutes. You can set it on the U2000. The short measurement period is either 5 or 15 minutes. You can set it on the U2000. The long measurement period is 24 hours by default.

Common Methods of Collecting Fault Information

Information to Be Collected		Collection Method
Collected log information	Subsystem result file	Run the **COL LOG** command with **Log Type** set to **RAW_PFM_RESULT**(Subsystem Result File). Obtain the subsystem result file from the queried save path. The default save path is **/COLLOGINFO/RAW_PFM_RESULT**.
	Measurement task file	Run the **COL LOG** command with **Log Type** set to **MEAS_TASK_FILE**(Measurement Task File). Obtain the measurement task file from the queried save path. The default save path is **/COLLOGINFO/MEAS_TASK_FILE**.
	Historical alarms	Run the **COL LOG** command with **Log Type** set to **ALARM**(Alarm File). Obtain the historical alarm file from the queried save path. The default save path is **/COLLOGINFO/ALARM**.

Common Methods of Collecting Fault Information

Information to Be Collected		Collection Method
Collected log information	Operation logs	Run the **COL LOG** command with **Log Type** set to **OPT_LOG**(Operation Log). Obtain the operation log file from the queried save path. The default save path is **/COLLOGINFO/OPT_LOG**.
	System running logs	Run the **COL LOG** command and set **Log Type** to **RUN_LOG**(Run Log), **PROCESS_LOG**(Process Log), **OS_LOG**(Operating System Log), and **DEBUG_LOG**(Debug Log). Obtain the system running logs from the queried save path. The default save paths are **/COLLOGINFO/RUN_LOG, /COLLOGINFO/PROCESS_LOG, /COLLOGINFO/OS_LOG, and /COLLOGINFO/DEBUG_LOG**, respectively.
	Data configuration file	Run the **COL LOG** command with **Log Type** set to **CFG_MML**(Data Configuration File). Obtain the data configuration file from the queried save path. The default save path is **/COLLOGINFO/CFG_MML**.

Common Methods of Collecting Fault Information

Information to Be Collected		**Collection Method**
Collected log information	Basic information	Run the **COL LOG** command with **Log Type** set to **BASIC_INFO**(Basic Information). Obtain the basic information from the queried save path. The default save path is **/COLLOGINFO/BASIC_INFO**.
	UVP log file	Run the **COL LOG** command with **Log Type** set to **UVP_LOG**(UVP Log). To avoid collecting unnecessary logs, UVP logs can be collected host by host. When running the **COL LOG** command, specify the name of the host whose UVP logs are to be collected. Obtain the FS log file from the queried save path. The default save path is **/COLLOGINFO/UVP_LOG**.
	VM template files	Run the **COL LOG** command with **Log Type** set to **TEMPLATE_FILE**(VM Template File) to obtain the APP template information, including the project template file, APP template file, and flavor file. Obtain these template files from the queried save path. The default save path is **/COLLOGINFO/TEMPLATE_FILE**.

Common Methods of Collecting Fault Information

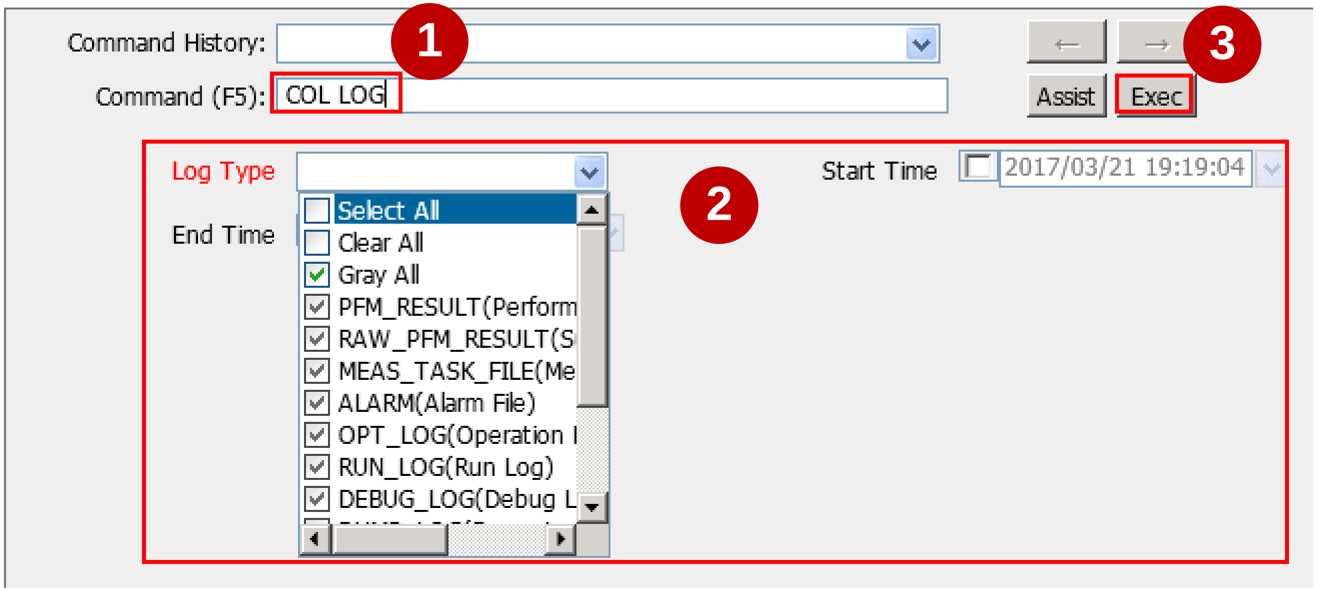
Information to Be Collected		Collection Method
Collected log information	VNF information	Run the **COL LOG** command with Log Type set to VNF_INFO(VNF Information) to obtain the VNF information, including project/APP template, flavor information, project/APP status, resource usage, and topology information. Obtain the VNF information from the queried save path. The default save path is /COLLOGINFO/VNF_INFO.
	Hardware log file	Run the **COL LOG** command with Log Type set to HW_LOG and HW_HC_INFO to obtain hardware logs and hardware health check logs. To avoid collecting unnecessary logs, hardware logs can be collected host by host. When running the **COL LOG** command, specify the name of the subrack whose logs are to be collected. Obtain the hardware log file from the queried save path. The default save paths are /COLLOGINFO/HW_LOG and /COLLOGINFO/HW_HC_LOG, respectively.

Common Methods of Collecting Fault Information

Information to Be Collected		Collection Method
Collected log information	OS dump log file	Run the **COL LOG** command with **Log Type** set to **DUMP_LOG**(Dump Log). Obtain the dump log file from the queried save path. The default save path is **/COLLOGINFO/DUMP_LOG**.
	OS health check log file	Run the **COL LOG** command with **Log Type** set to **OS_HC_LOG**(OS Health Check Log). Obtain the OS health check log file from the queried save path. The default save path is **/COLLOGINFO/OS_LOG/OS_HC_LOG**.

Collecting Logs

- Run the **COL LOG** command to collect logs of non-faulty nodes. The logs can be used for troubleshooting.



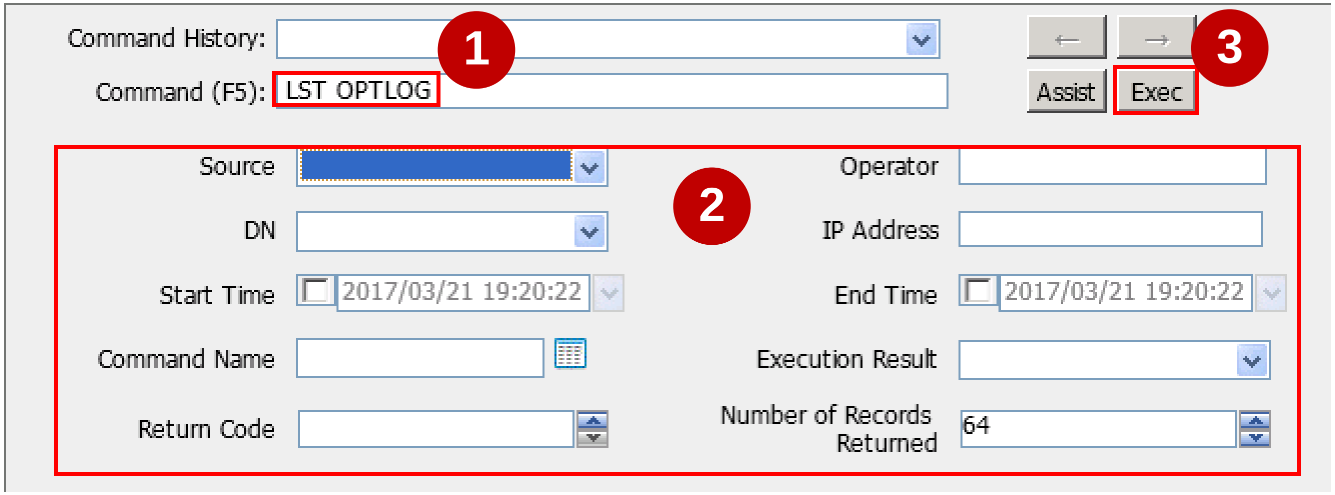
Command (F5): COL LOG

Start Time ☐ 2017/03/21 19:19:04

☐ Select All
☐ Clear All
☑ Gray All
☑ PFM_RESULT(Perform
☑ RAW_PFM_RESULT(S
☑ MEAS_TASK_FILE(Me
☑ ALARM(Alarm File)
☑ OPT_LOG(Operation I
☑ RUN_LOG(Run Log)
☑ DEBUG_LOG(Debug L

Listing Operation Logs

- Run the **LST OPTLOG** command to list the records in operation logs. The operation logs are listed in reverse order based on the recorded time.



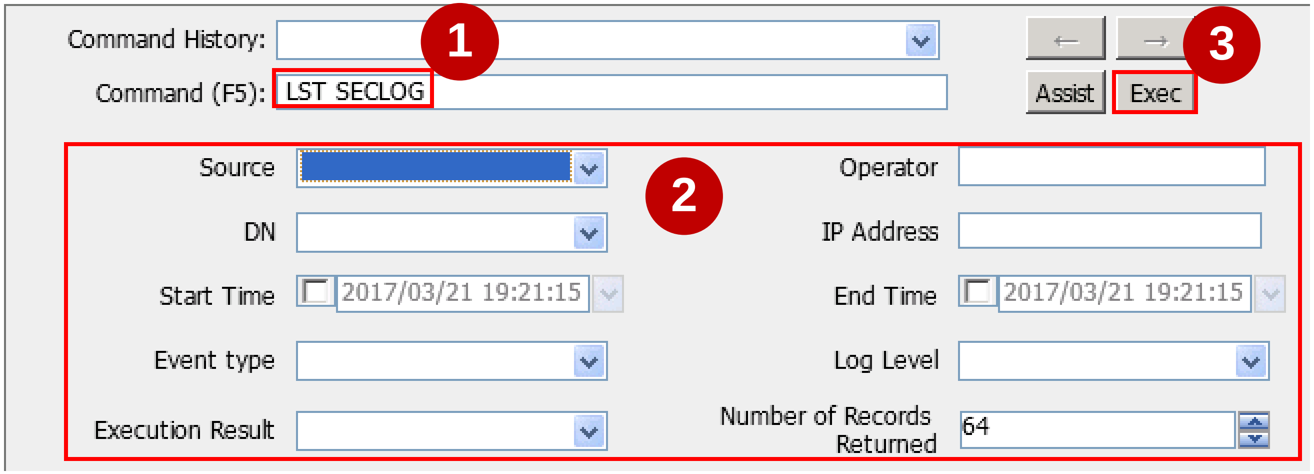
Command History:

Command (F5): LST OPTLOG

Source		Operator	
DN		IP Address	
Start Time	□ 2017/03/21 19:20:22	End Time	□ 2017/03/21 19:20:22
Command Name		Execution Result	
Return Code		Number of Records Returned	64

Listing Security Logs

- Run the **LST SECLOG** command to list the records in security logs. The security logs are listed in reverse order based on the recorded time.



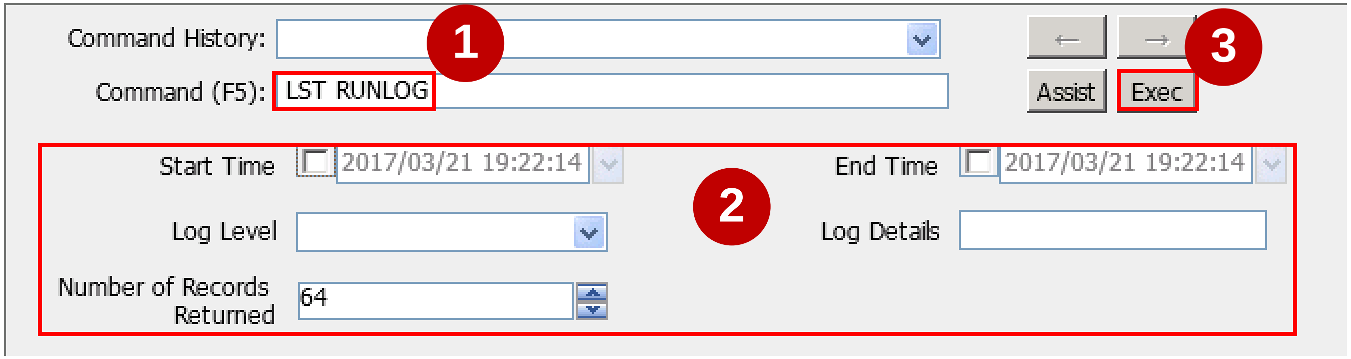
Command History:

Command (F5): LST SECLOG

Source		Operator	
DN		IP Address	
Start Time	□ 2017/03/21 19:21:15	End Time	□ 2017/03/21 19:21:15
Event type		Log Level	
Execution Result		Number of Records Returned	64

Listing Run Logs

- Run the **LST RUNLOG** command to list run logs. The logs will be listed in reverse chronological order.



Command History:

Command (F5): LST RUNLOG

Start Time □ 2017/03/21 19:22:14

End Time □ 2017/03/21 19:22:14

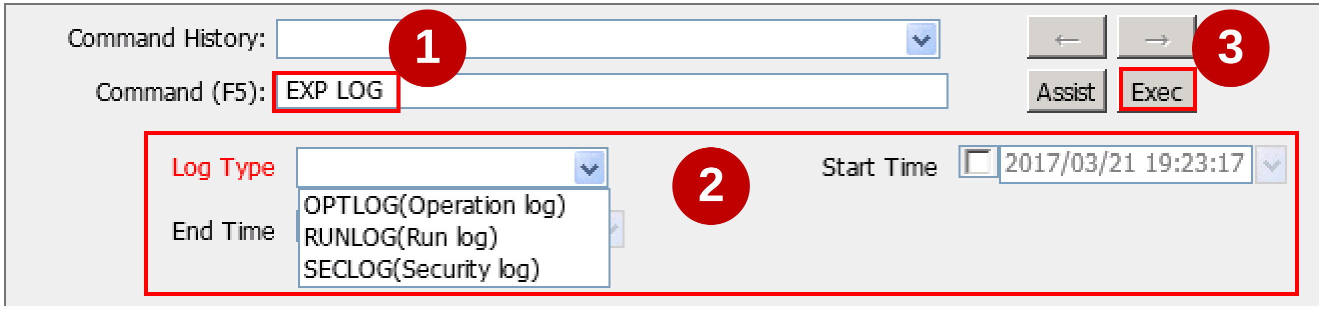
Log Level

Log Details

Number of Records Returned 64

Exporting Logs

- Run the **EXP LOG** command to export the records in operation logs, run logs, and security logs to a file. During command execution, the system reports the execution progress to the client.


Command History:

Command (F5): EXP LOG

Log Type

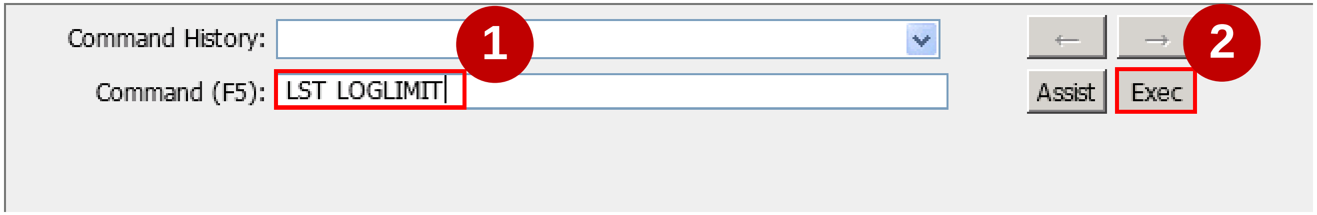
OPTLOG(Operation log)
RUNLOG(Run log)
SECLOG(Security log)

End Time

Start Time □ 2017/03/21 19:23:17

Listing Log Storage Limits

- Run the **LST LOGLIMIT** command to list the maximum storage capacity for operation logs, security logs, and run logs.



Command History:

Command (F5): LST LOGLIMIT

Contents

- eSE620X vESC O&M Management Overview
- eSE620X vESC Alarm Management
- eSE620X vESC Device Management
- eSE620X vESC Software Management
- eSE620X vESC Log Management
- **eSE620X vESC Message Tracing Management**
- eSE620X vESC Data Backup and Recovery
- eSE620X vESC Performance Management

Message Tracing Tasks

- Message tracing tasks trace interfaces, signaling links, and UEs. It applies to routine equipment maintenance and fault location.
- The tracing task can be performed on the LMT only when the LMT is successfully connected to the NE.
- The message tracing time displayed on the LMT is the NE time, rather than the LMT time.

Internal Process of Message Tracing

1. Creating a tracing task on the LMT.

- After you create a tracing task on the LMT, the LMT sends a binary command to the NE to create the task.
- The NE forwards the command to a specified tracing management module.
- After receiving the command, the tracing management module records the tracing parameters contained in the command in the filter table and sends messages to the service processing module.
- The service processing module updates the local filter table based on the messages from the tracing management module.

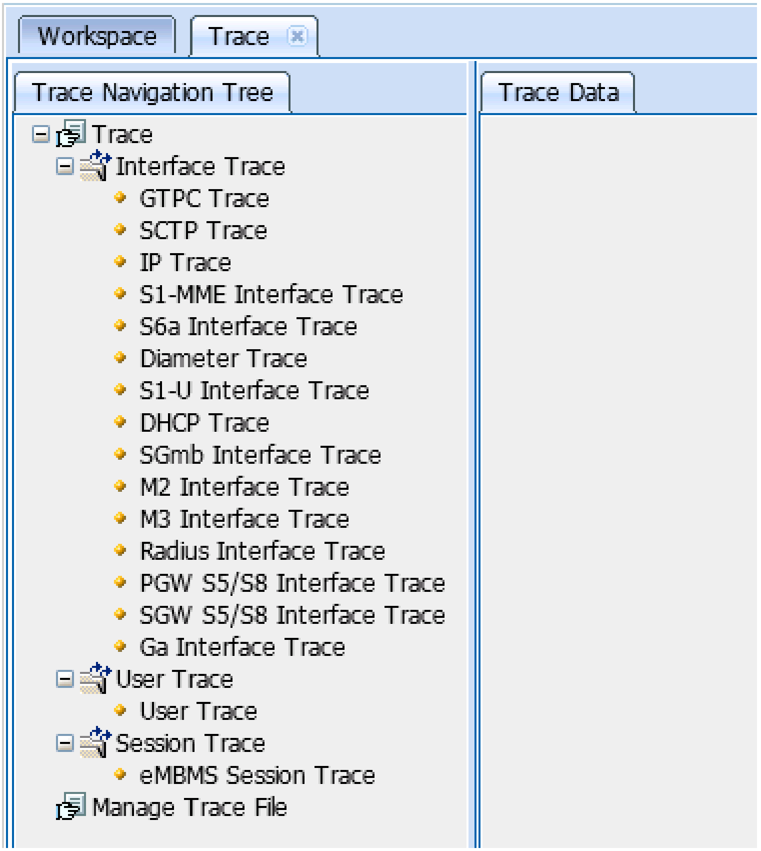
Internal Process of Message Tracing

2. Reporting results to the LMT

- After receiving messages from the tracing management module, the service processing module matches the messages against the parameters in the local filter table. Then, it reports the messages meeting the filter criteria to the LMT based on the task IDs contained in the messages.
- The LMT analyzes the messages and displays tracing results.

Managing Message Tracing

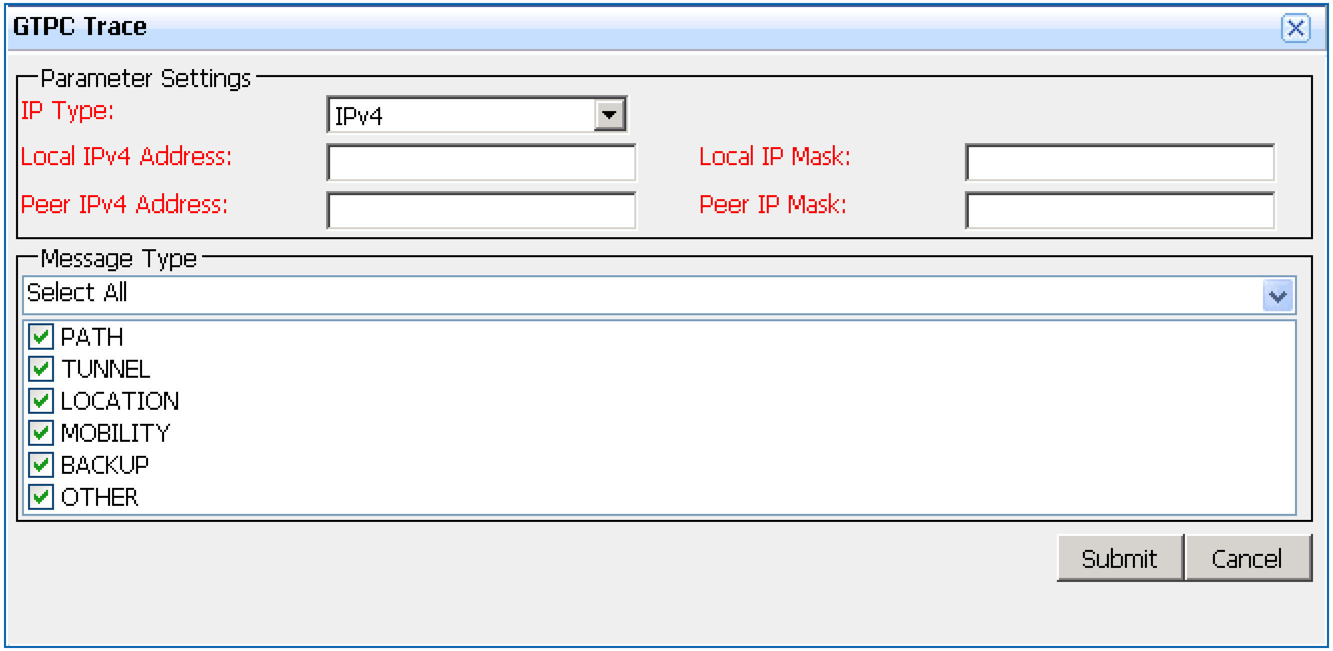
- You can verify data and identify faults through message tracing. After a message tracing task is created, the traced messages can be browsed and saved. Each tracing file can contain a maximum of 5000 traced messages.



- Trace
  - Interface Trace
    - GTPC Trace
    - SCTP Trace
    - IP Trace
    - S1-MME Interface Trace
    - S6a Interface Trace
    - Diameter Trace
    - S1-U Interface Trace
    - DHCP Trace
    - SGmb Interface Trace
    - M2 Interface Trace
    - M3 Interface Trace
    - Radius Interface Trace
    - PGW S5/S8 Interface Trace
    - SGW S5/S8 Interface Trace
    - Ga Interface Trace
  - User Trace
    - User Trace
  - Session Trace
    - eMBMS Session Trace
  - Manage Trace File

Creating GTPC Trace

- Click **Trace** in the workspace.
- Double-click **GTPC Trace**. The **GTPC Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



GTPC Trace

Parameter Settings

IP Type: IPv4

Local IPv4 Address:

Local IP Mask:

Peer IPv4 Address:

Peer IP Mask:

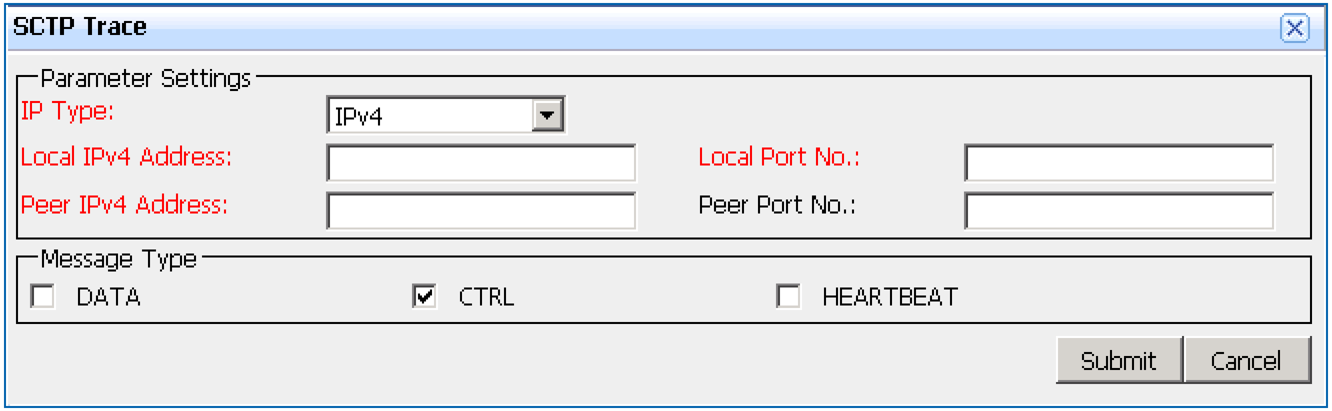
Message Type

Select All

☑ PATH
☑ TUNNEL
☑ LOCATION
☑ MOBILITY
☑ BACKUP
☑ OTHER

Creating SCTP Trace

- Click **Trace** in the workspace.
- Double-click **SCTP Trace**. The **SCTP Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



SCTP Trace

Parameter Settings

IP Type: IPv4

Local IPv4 Address:

Local Port No.:

Peer IPv4 Address:

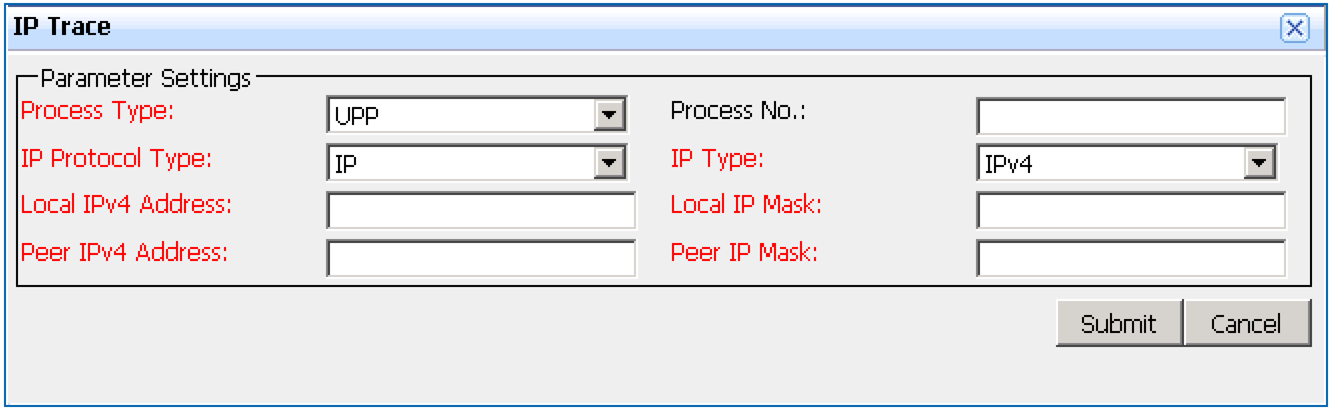
Peer Port No.:

Message Type

□ DATA ☑ CTRL □ HEARTBEAT

Creating IP Trace

- Click **Trace** in the workspace.
- Double-click **IP Trace**. The **IP Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



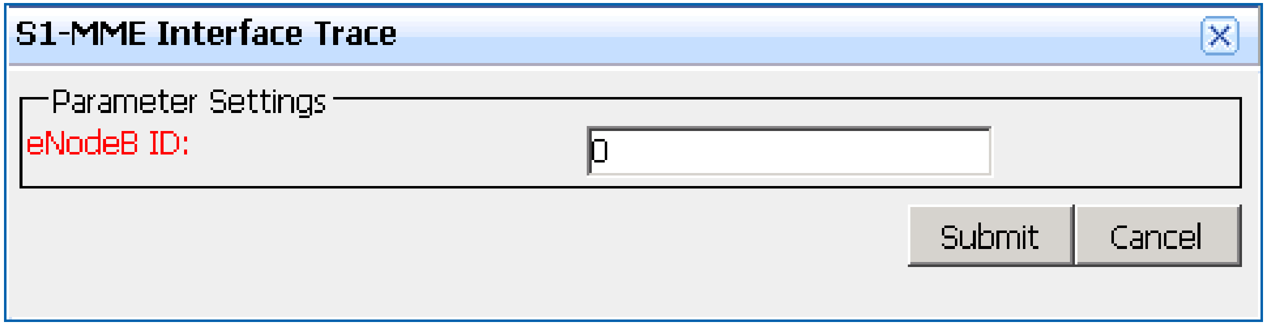
IP Trace

Parameter Settings

Process Type:	UPP	Process No.:	
IP Protocol Type:	IP	IP Type:	IPv4
Local IPv4 Address:		Local IP Mask:	
Peer IPv4 Address:		Peer IP Mask:	

Creating S1-MME Interface Trace

- Click **Trace** in the workspace.
- Double-click **S1-MME Interface Trace**. The **S1-MME Interface Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



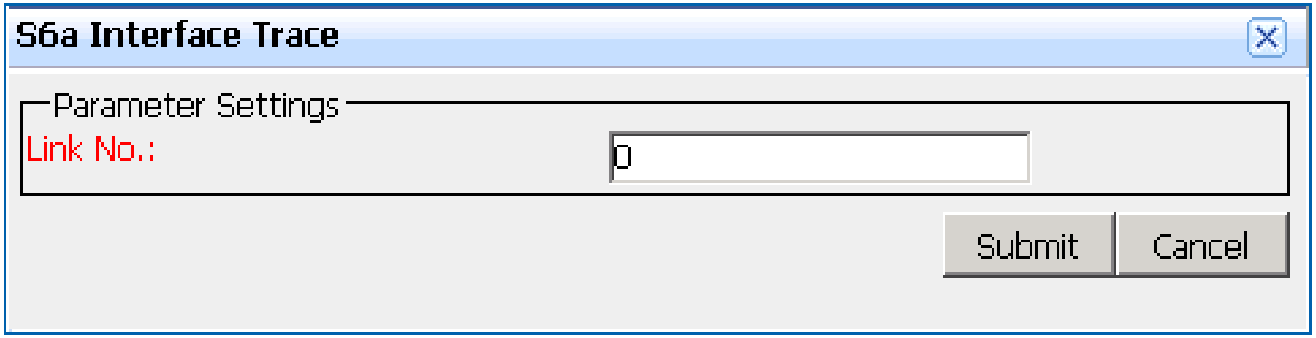
S1-MME Interface Trace

Parameter Settings

eNodeB ID: 0

Creating S6a Interface Trace

- Click **Trace** in the workspace.
- Double-click **S6a Interface Trace**. The **S6a Interface Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



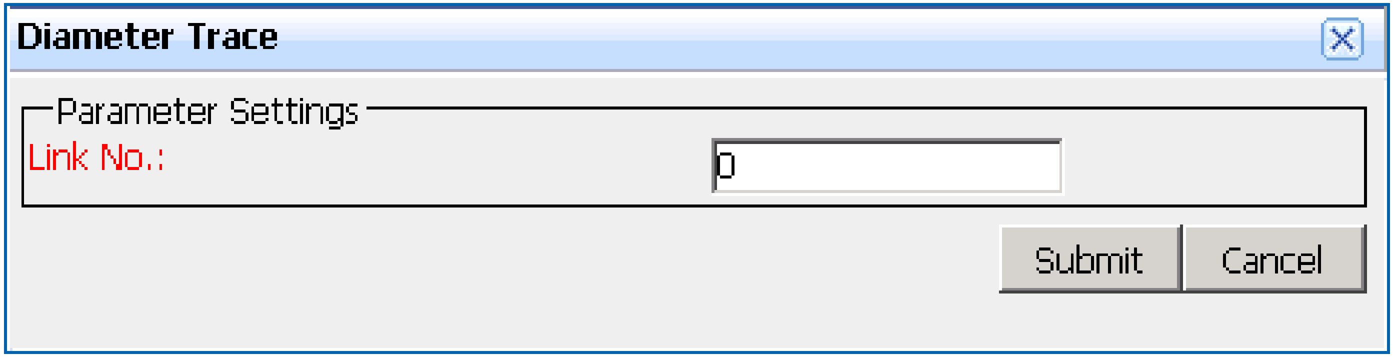
S6a Interface Trace

Parameter Settings

Link No.: 0

Creating Diameter Trace

- Click **Trace** in the workspace.
- Double-click **Diameter Trace**. The **Diameter Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



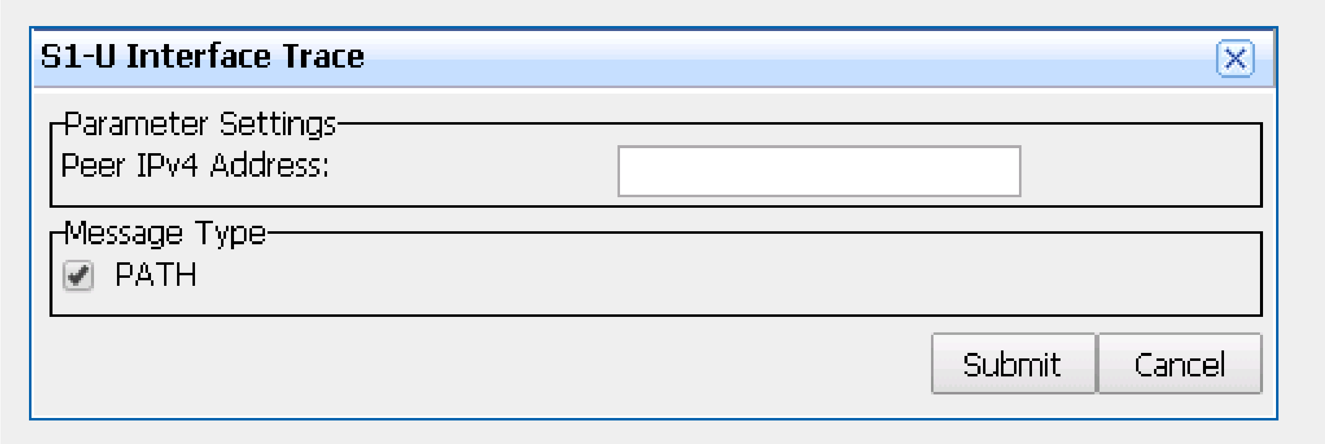
Diameter Trace

Parameter Settings

Link No.: 0

Creating S1-U Interface Trace

- Click **Trace** in the workspace.
- Double-click **S1-U Interface Trace**. The **S1-U Interface Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



S1-U Interface Trace

Parameter Settings

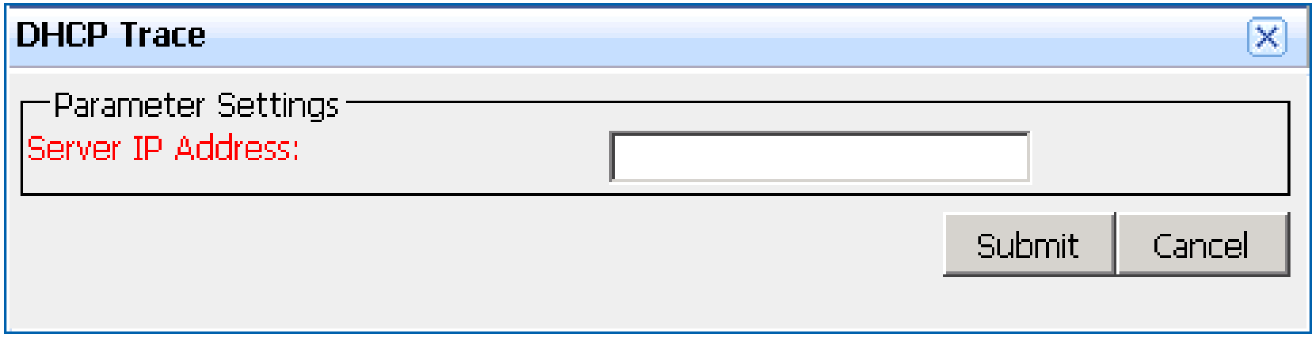
Peer IPv4 Address:

Message Type

☑ PATH

Creating DHCP Trace

- Click **Trace** in the workspace.
- Double-click **DHCP Trace**. The **DHCP Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



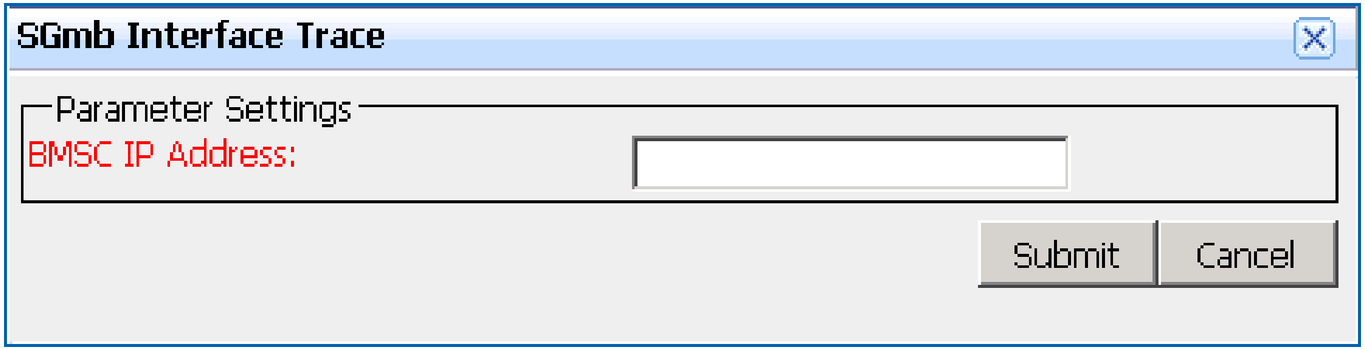
DHCP Trace

Parameter Settings

Server IP Address:

Creating SGmb Interface Trace

- Click **Trace** in the workspace.
- Double-click **SGmb Interface Trace**. The **SGmb Interface Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



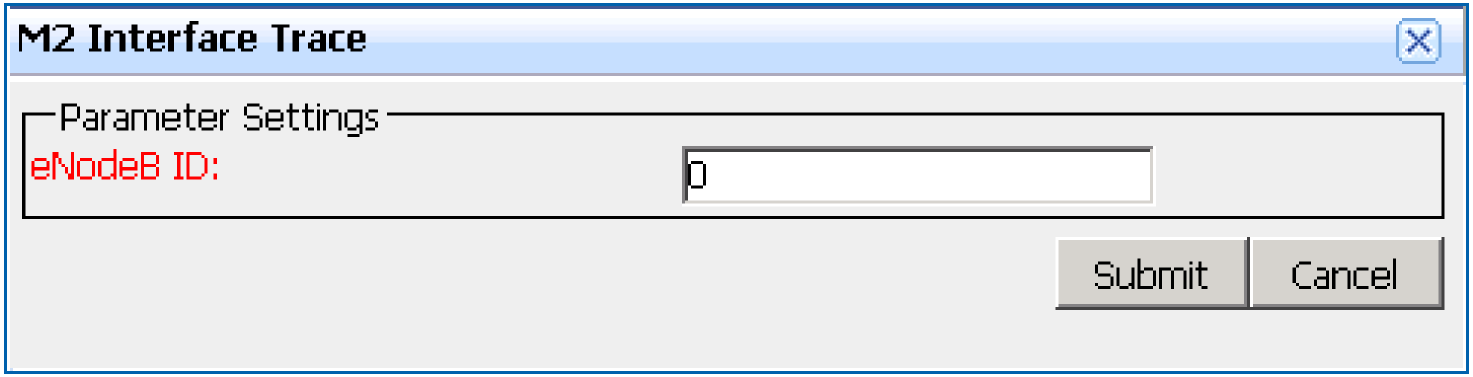
SGmb Interface Trace

Parameter Settings

BMSC IP Address:

Creating M2 Interface Trace

- Click **Trace** in the workspace.
- Double-click **M2 Interface Trace**. The **M2 Interface Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



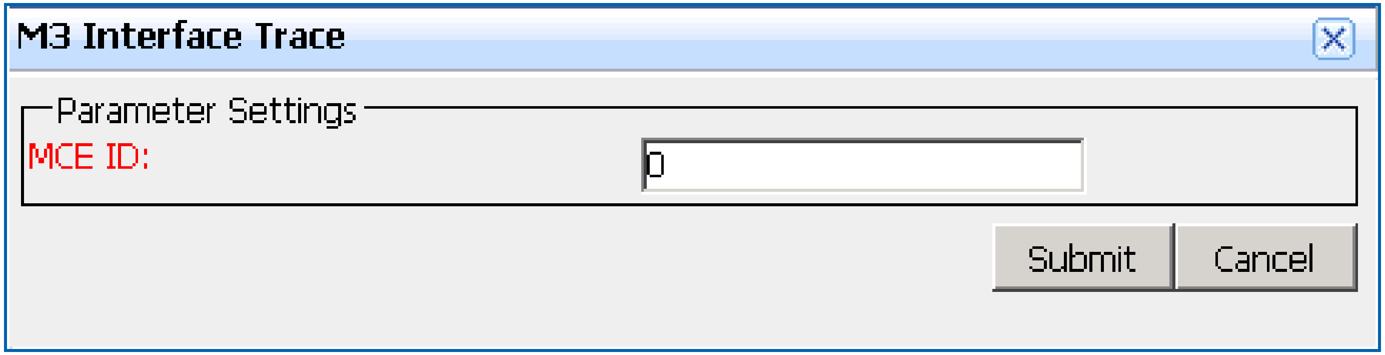
M2 Interface Trace

Parameter Settings

eNodeB ID: 0

Creating M3 Interface Trace

- Click **Trace** in the workspace.
- Double-click **M3 Interface Trace**. The **M3 Interface Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



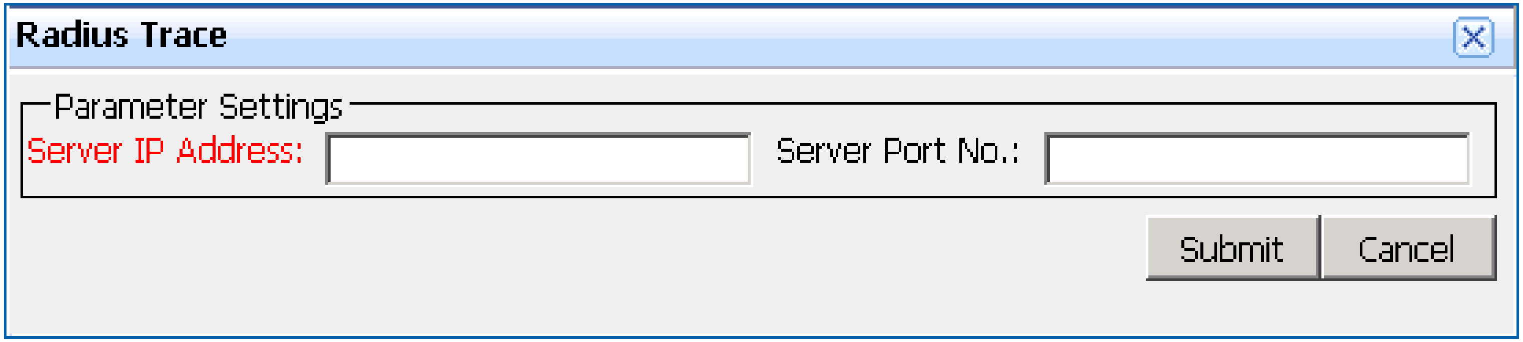
M3 Interface Trace

Parameter Settings

MCE ID: 0

Creating Radius Trace

- Click **Trace** in the workspace.
- Double-click **Radius Trace**. The **Radius Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



Radius Trace

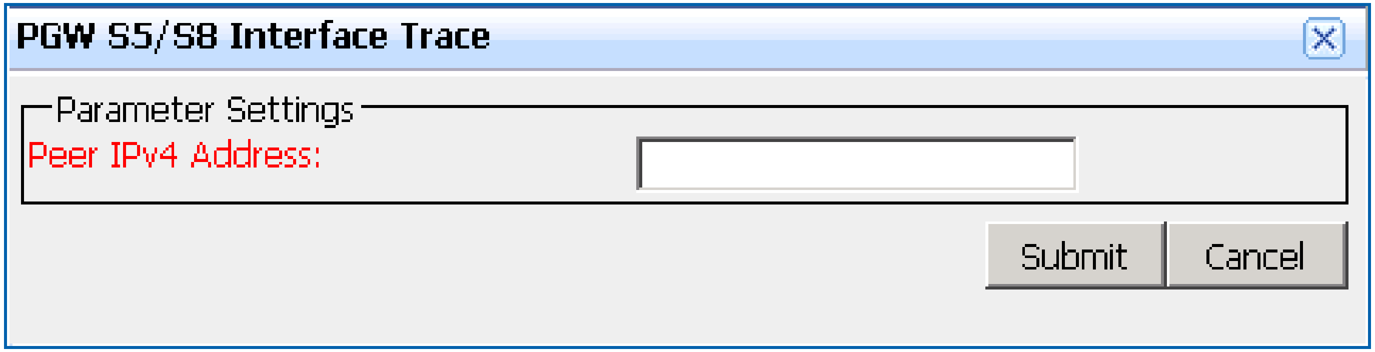
Parameter Settings

Server IP Address:

Server Port No.:

Creating PGW S5/S8 Interface Trace

- Click **Trace** in the workspace.
- Double-click **PGW S5/S8 Interface Trace**. The **PGW S5/S8 Interface Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



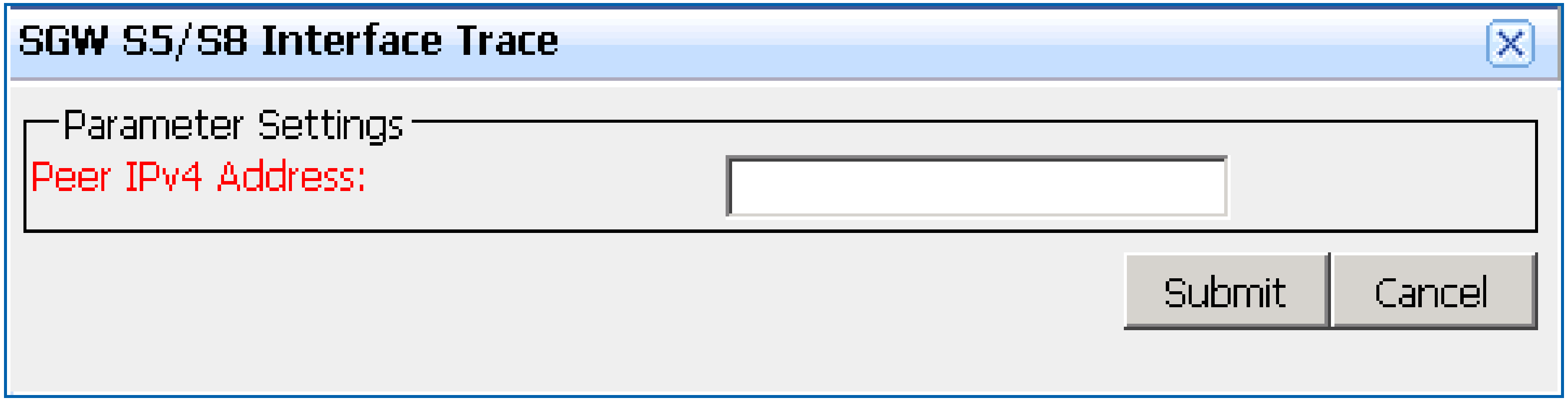
PGW S5/S8 Interface Trace

Parameter Settings

Peer IPv4 Address:

Creating SGW S5/S8 Interface Trace

- Click **Trace** in the workspace.
- Double-click **SGW S5/S8 Interface Trace**. The **SGW S5/S8 Interface Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



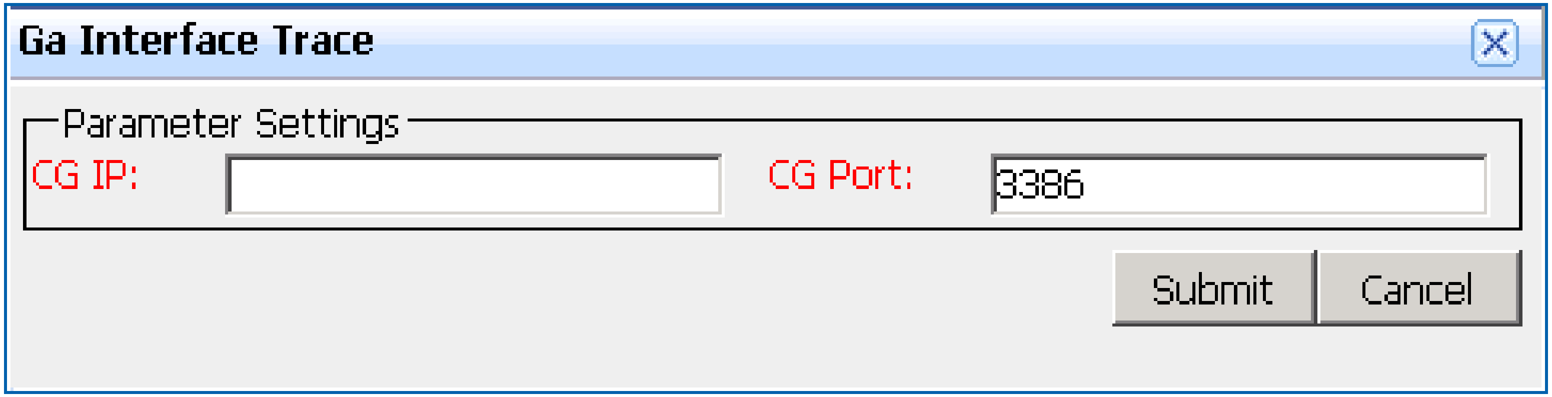
SGW S5/S8 Interface Trace

Parameter Settings

Peer IPv4 Address:

Creating Ga Interface Trace

- Click **Trace** in the workspace.
- Double-click **Ga Interface Trace**. The **Ga Interface Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.

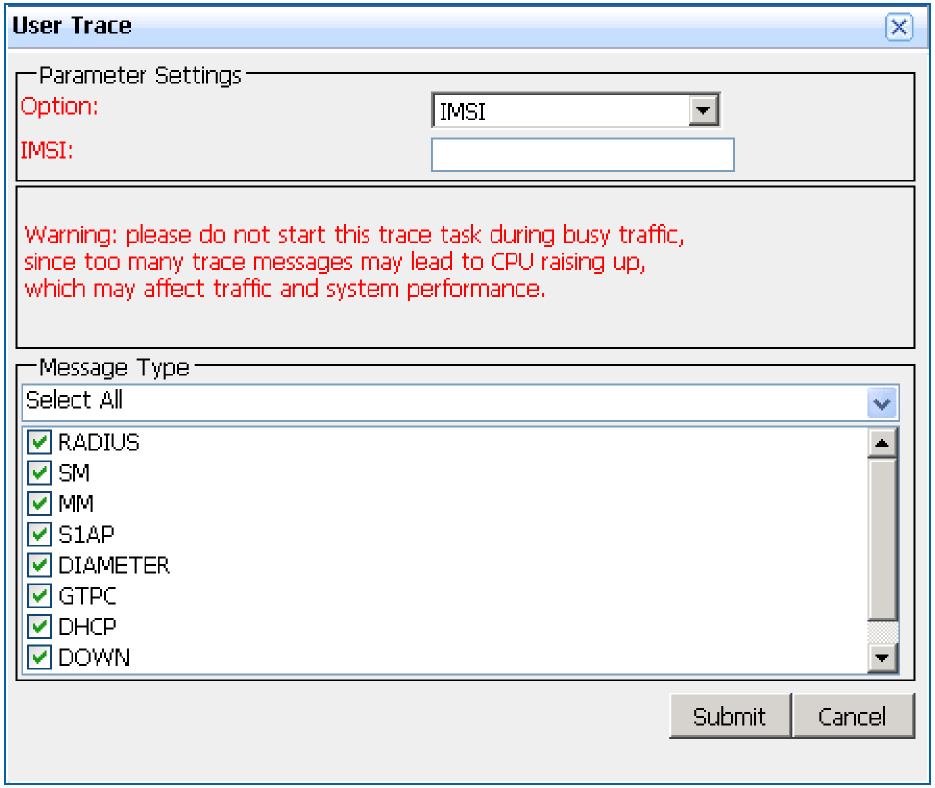


CG IP:

CG Port: 3386

Creating User Trace

- Click **Trace** in the workspace.
- Double-click **User Trace**. The **User Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



User Trace

Parameter Settings

Option: IMSI

IMSI:

Warning: please do not start this trace task during busy traffic, since too many trace messages may lead to CPU raising up, which may affect traffic and system performance.

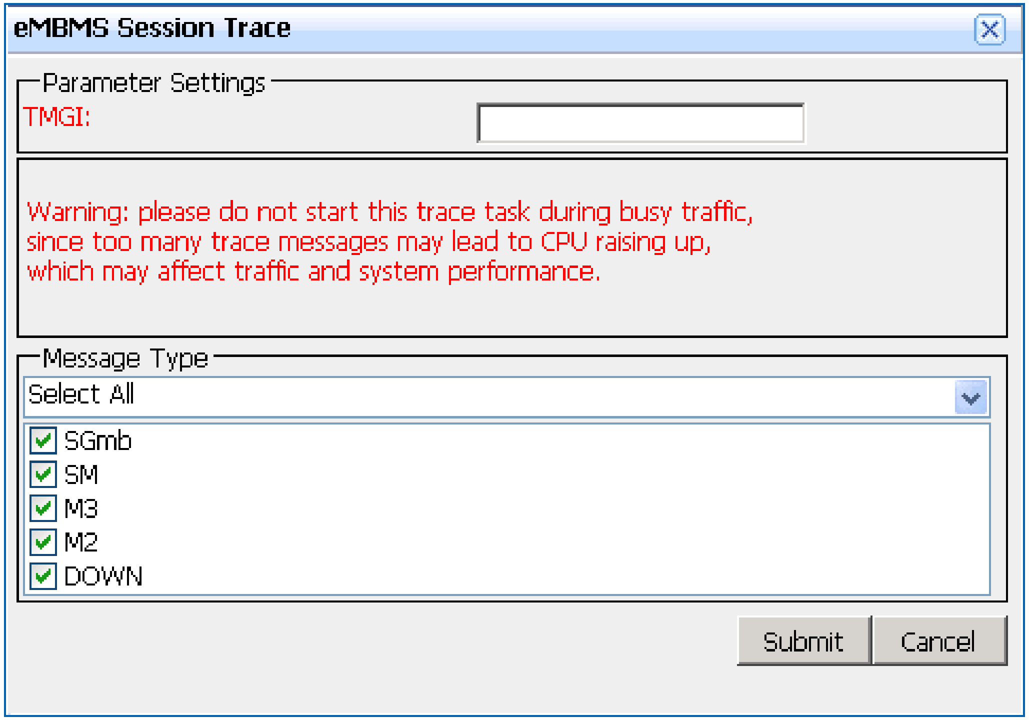
Message Type

Select All

☑ RADIUS
☑ SM
☑ MM
☑ S1AP
☑ DIAMETER
☑ GTPC
☑ DHCP
☑ DOWN

Creating eMBMS Session Trace

- Click **Trace** in the workspace.
- Double-click **eMBMS Session Trace**. The **eMBMS Session Trace** dialog box is displayed. Set trace-related parameters, and click **Submit**.



eMBMS Session Trace

Parameter Settings

TMGI:

Warning: please do not start this trace task during busy traffic, since too many trace messages may lead to CPU raising up, which may affect traffic and system performance.

Message Type

Select All

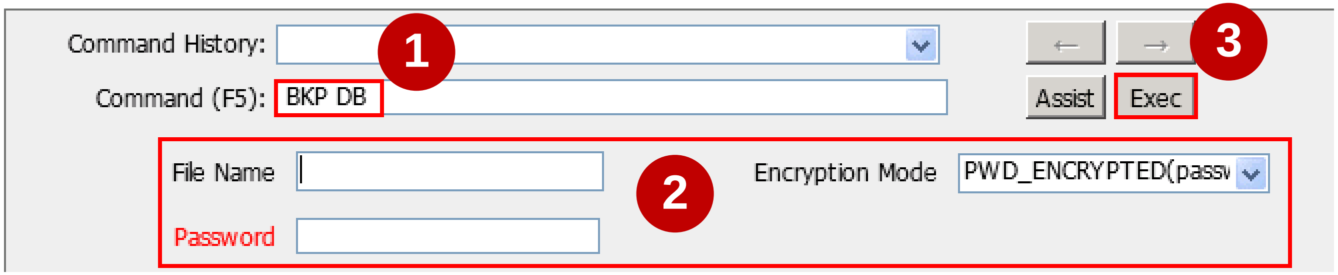
☑ SGmb
☑ SM
☑ M3
☑ M2
☑ DOWN

Contents

- eSE620X vESC O&M Management Overview
- eSE620X vESC Alarm Management
- eSE620X vESC Device Management
- eSE620X vESC Software Management
- eSE620X vESC Log Management
- eSE620X vESC Message Tracing Management
- **eSE620X vESC Data Backup and Recovery**
- eSE620X vESC Performance Management

Backing Up Data

- Before key configuration data adjustment, capacity expansion, and upgrade, back up the configuration data so that the data can be restored even when an operation fails.
- Run the **BKP DB** command of the Node with **File Name** specified to back up data to this file.
- After the backup is completed, download the backup data to the local PC from the path contained in the command output.



Command History:

Command (F5): BKP DB

File Name

Password

Encryption Mode: PWD_ENCRYPTED(passw

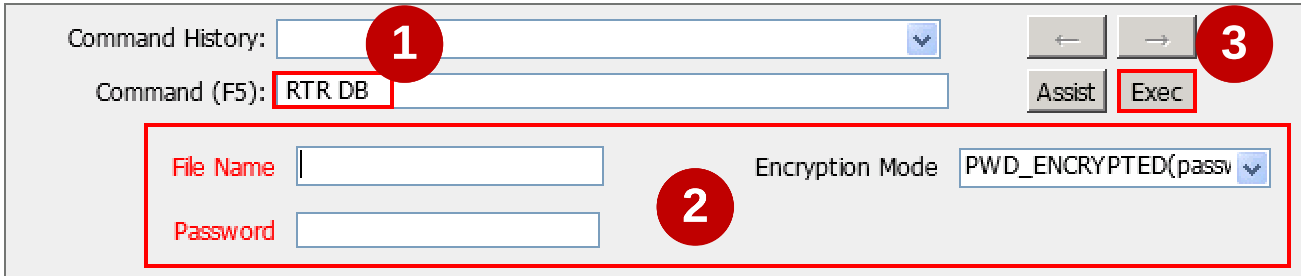
Restoring Data

- **Background**

- The eSE6201 Basic/eSE6203 Basic has been reinstalled.
- Data files to be restored exist on the eSE6201 Basic/eSE6203 Basic. If the files do not exist, upload the backup files to the **backupdb** directory of the eSE6201 Basic/eSE6203 Basic.
- The image file used during data backup exists on the eSE6201 Basic/eSE6203 Basic. If the image file does not exist, run the **DLD DEPLOYFILE** command of the Node to download the file.

Restoring Data

- Run the **RTR DB** command of the Node with File Name specified and restore data in the specified file.
- After data restoration is completed on the eSE6201 Basic/eSE6203 Basic, run the **RTR DB** command of the Node on each VNF to restore data.
- If **ALM-41388 Virtual Resource Data Inconsistency Alarm** is reported after the data restoration is completed, handle the alarm according to the instructions provided in the alarm help. If VNF data loss occurs due to data restoration, run the **RTR DB** command on the corresponding VNFs to restore VNF data.


Command History:

Command (F5): RTR DB

File Name

Password

Encryption Mode PWD_ENCRYPTED(passw

Contents

- eSE620X vESC O&M Management Overview
- eSE620X vESC Alarm Management
- eSE620X vESC Device Management
- eSE620X vESC Software Management
- eSE620X vESC Log Management
- eSE620X vESC Message Tracing Management
- eSE620X vESC Data Backup and Recovery
- **eSE620X vESC Performance Management**

Definition of Performance Management

- Performance management is a process in which a carrier evaluates the network performance of telecommunication devices and the effectiveness of NEs, and monitors and optimizes network performance. In performance management, a carrier performs the following:
  - Monitoring network running and service quality.
  - Removing faults.
  - Removing faults.
  - Planning network capacity and allocating network resources effectively.
  - Optimizing network performance indicators.

Applications of Performance Management

The major applications of performance management are routine maintenance, performance monitoring, and network optimization.

- Routine maintenance
  - Enables you to detect the network abnormalities in time using threshold alarms to prevent faults from exacerbating.
  - Enables you to locate faults with certain measurement items of an NE.
- Performance monitoring

  Enables the vESC to detect the bottleneck of the network load, improve the QoS, and explore the potential of the equipment.
- Network optimization

  Provides you with a data foundation for the network planning and network upgrade.

Thank You

www.huawei.com