Oracle® Communications
EAGLE EIR User's Guide

Release 48.0

G48097-01

December 2025

ORACLE®

Oracle Communications EAGLE EIR User's Guide, Release 48.0

G48097-01

Contents

4   EIR Configuration

5   Maintenance

6   EIR Measurements

My Oracle Support (MOS)

[My Oracle Support (MOS)](#) is your initial point of contact for any of the following requirements:

- **Product Support**:
  The generic product related information and resolution of product related queries.

- **Critical Situations**
  A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

  – A total system failure that results in loss of all transaction processing capability

  – Significant reduction in system capacity or traffic handling capability

  – Loss of the system's ability to perform automatic system reconfiguration

  – Inability to restart a processor or the system

  – Corruption of system databases that requires service affecting corrective actions

  – Loss of access for maintenance or recovery operations

  – Loss of the system ability to provide any required critical or major trouble notification

  Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

- **Training Need**
  Oracle University offers training for service providers and enterprises.

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.

- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Acronyms and Terminology

The following table provides information about the acronyms and the terminology used in the document.

Table   Acronyms and Terminology

Acronym	Definition
EIR	Equipment Identity Register
EPAP	EAGLE Application Processor Provisioning
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity (IMSI)
MS	Mobile Stations
MSISDN	Mobile Station International ISDN Number
SIM	Subscriber Identity Module
NPP	Numbering Plan Processor
RTDB	Real Time Database

What's New in This Guide

This section introduces the documentation updates for Release 48.0 in Oracle Communications EAGLE EIR User's Guide.

Release 48.0 - G48097-01, December, 2025

- Updated the Port LED behavior under the section Hardware Requirements.

- Added a new section called Thermal Management Parameters.

1
Introduction

This chapter provides a brief description of the EIR feature of the Oracle Communications EAGLE. The chapter also includes the scope, audience, and organization of the manual; how to find related publications; and how to contact Oracle for assistance.

Overview

This manual describes the **Equipment Identity Register** (**EIR**) feature of Oracle Communications EAGLE. The EIR feature is used to reduce the number of **GSM** mobile handset thefts by providing a mechanism to assist network operators in preventing stolen or disallowed handsets from accessing the network. This control is accomplished by comparing the International Mobile Equipment Identity (**IMEI**) that is provided during handset registration to a set of three lists provided by the network operator:

- Black - Mobile Stations (**MS**) on the Blocklist will be denied access to the network
- White - MSs on the Allowlist will be allowed access to the network
- Gray - MSs on the Graylist will be allowed on the network, but may be tracked

EIR is an optional feature on EAGLE, and can be turned on but not off after the feature is enabled using a feature access key. EIR is mutually exclusive with **LNP** in the system, unless the Dual ExAP Configuration feature is enabled.

References

For EIR related configurations, refer to the following documents:

- *Application B Card Hardware and Installation Guide*
- *Hardware Reference Guide*
- *Commands User's Guide*
- *Administration Guide for EPAP*

2

Feature Description

This chapter provides a functional description of the EIR feature, including network perspectives, assumptions and limitations, a database overview, Service Module card provisioning and reloading, EIR user interface, and an audit overview.

Equipment Identity Register Overview

A handset theft problem exists in GSM networks in many countries. A person obtains a legitimate subscription to a network, and then obtains a legitimate IMSI, MSISDN, and SIM card. The person initially buys an inexpensive handset and then steals a better handset from another subscriber. After the handset is stolen, the thief replaces the SIM card with a legitimate SIM card. Because the SIM card and subscriber information contained on the SIM card (IMSI, MSISDN) are legitimate, the phone will operate and the network operator cannot determine that the subscriber is using a stolen handset. In addition to individual handset theft, organized groups stealing entire shipments of mobile handsets from warehouses and sell these handsets on the Black Market.

The Equipment Identity Register (EIR) is a network entity used in GSM networks that stores lists of IMEI numbers, which correspond to physical handsets (not subscribers). The IMEI is used to identify the actual handset, and is not dependent upon the International Mobile Subscriber Identity (IMSI), Mobile Station International ISDN Number (MSISDN), or the Subscriber Identity Module (SIM). The IMSI, MSISDN, and SIM are all subscriber-specific, and move with the subscriber when purchasing a new handset. The IMEI is handset-specific.

The EIR feature can be used to reduce the number of GSM mobile handset thefts by providing a mechanism that allows network operators to prevent stolen or disallowed handsets from accessing the network. This control is accomplished by comparing the International Mobile Equipment Identity (IMEI) that is provided during handset registration to the following set of three lists provided by the network operator:

- Black - Mobile Stations (MS) on the Blocklist are denied access to the network

- Gray - MSs on the Graylist are allowed on the network, but may be tracked

- White - MSs on the Allowlist are allowed access to the network

The EPAP Real Time Database (RTDB) stores the Allowlist, Graylist, and Blocklist of IMEI numbers. The RTDB is downloaded to Service Module cards in EAGLE. When a subscriber roams to a new MSC or VLR location, the handset attempts registration with the MSC or VLR. Before the MSC registers the subscriber with the VLR, it may send a query to the EAGLE for EIR status of the handset. EAGLE returns a response indicating whether the IMEI is allowed, disallowed, or not valid. If the IMEI is allowed, the MSC completes registration; otherwise, registration is rejected.

The RTDB may also contain associations between individual IMEIs and IMSIs. This can provide a further level of screening by directly associating a particular IMEI with a particular IMSI. This association is used in the following way:

- If an IMEI is found on a Blocklist, an additional check of the IMSI could then be made.

- If the IMSI from the handset matches the IMSI provisioned with the IMEI, this would override the Blocklist condition, and allow registration to continue. This could be used to

protect against mistaken Blocklist entries in the database, or to prevent unauthorized "handset sharing". This association could also be used in other ways.

The IMSI Range Logic Support feature includes an IMSI range check logic prior to an IMEI lookup in the database. This check prevents low ARPU users from using certain devices, in addition to the EIR stolen handset check.

The EIR feature is mutually exclusive with LNP, unless the Dual ExAP Configuration feature is enabled.

EIR Call Flows

When a handset roams into a new MSC/VLR area, it attempts a registration procedure with the VLR. In a network without the EIR function, this procedure results in the VLR sending a location update message to the HLR, providing the HLR with the current MSC location of the Mobile Station (MS)/handset. When the EIR function is deployed in a network, this registration procedure is interrupted in order to validate the IMEI of the MS/handset attempting to register before completing the registration procedure and updating the HLR.

In the network with EIR, the MSC/VLR sends a MAP_CHECK_IMEI message to the EAGLE requesting EIR processing before sending a location update to the HLR. This message contains, at a minimum, the IMEI of the MS attempting registration. It may also contain the IMSI of the subscriber whose SIM card is currently being used in the MS/handset. Upon receipt of this message, the EIR feature searches the White, Gray, and Block Lists for a match on the IMEI. The EIR feature then returns a response to the MSC. Depending upon the result of the search, the response contains either the Equipment Status of the MS/handset (whether the IMEI for the MS/handset is allowed or not, based on its status in the White, Gray, or Block Lists), or a User Error (invalid or unknown IMEI). The MSC then either continues the registration procedure (if the IMEI is allowed), or rejects it (if the IMEI is disallowed, invalid, or unknown).

If the IMSI is also included in the message, EIR attempts to match this IMSI to one provisioned with the IMEI before sending a response to the MSC. A match on IMSI in this case overrides any Block List condition found based on the IMEI match alone, and causes a response of MS allowed.

Figure 2-1 illustrates the steps of the following EAGLE EIR call flow process.

1. The MS/handset roams into a new serving MSC/VLR area, and begins the registration procedure with the Base Station (BS).

2. The BS begins the registration procedure with MSC/VLR.

3. Before allowing the MS/handset to register on the network, and before updating the HLR with the new MSC information, the MSC launches a MAP_CHECK_IMEI message to the EAGLE for EIR feature processing. This message is either MTP-routed directly to the point code of the EAGLE and the EIR local subsystem, or is GT-routed and the EAGLE performs global title translation on the message to its own point code and the EIR local subsystem.

4. EIR retrieves the IMEI and/or IMSI from the message and searches the EIR information in the RTDB for a match. See Table 2-1 and Table 2-2. This search may result in the IMEI being on one or more of the White, Gray, or Block Lists, or it may result in an invalid or unknown IMEI (no match). It may also result in an invalid IMSI-IMEI combination. Based on the results of the search, the EAGLE returns a MAP_CHECK_IMEI_ack containing either the Equipment Status (IMEI allowed or not allowed), or a User Error (invalid or unknown IMEI).

5. (Not shown). The MSC either rejects or completes the registration attempt, depending on the information returned from EIR.

Figure 2-1   EIR Call Flow
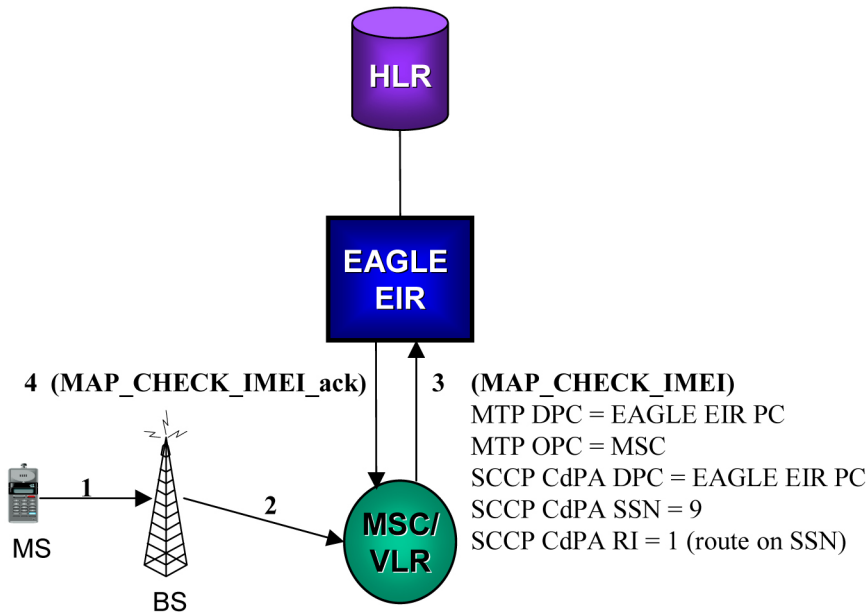
The RTDB EIR information contains lists of IMEIs, and an indication as to the list where they are located. There are two types of IMEIs: Individual IMEIs (Table 2-1) and ranges of IMEIs (Table 2-2). The Individual IMEIs are searched first. The IMEI entries in this list may also contain an association to an IMSI. If no individual IMEI match is found, IMEI ranges are searched.

EIR can support up to 32 million individual IMEIs. A total of up to 100,000 IMEI ranges are supported. The maximum EAGLE RTDB capacity for all EPAP service features, including EIR, G-Flex, and G-Port, is 120 million individual numbers. Entries for these other services (MSISDNs for G-Port or IMSIs for G-Flex), reduce the available capacity for IMEIs. Also, if IMSIs are entered for the `IMSI Check` of EIR, those entries also reduce the available IMEI capacity.

> ⓘ **Note**
>
> Database capacity can be expanded by using the EPAP Data Split feature and/or the EAGLE MNP Data Base Support for 240M DN feature.
>
> For extended database capability, refer to the 120M DN and 120M IMSIs via Split Database feature (Part Number: 893-0398-01) in *Database Administration - GTT User's Guide*.

Table 2-1   Example of Individual IMEIs

IMEI	IMSI (optional)	Allow List	Gray List	Block List
12345678901234	495867256894125	No	No	Yes
234567890123456		No	Yes	No
49876523576823		No	Yes	Yes
68495868392048	495867565874236	Yes	Yes	No

Table 2-1   (Cont.) Example of Individual IMEIs

IMEI	IMSI (optional)	Allow List	Gray List	Block List
29385572695759		Yes	Yes	Yes

As shown in Table 2-1, it is possible for a given IMEI to be on more than one list (on the Allow List, and also on the Gray and/or Block List). The logic illustrated by Table 2-2 is used to determine which answer to return in the CHECK_IMEI response, determined by which list or lists the IMEI is on. Table 2-2 also shows three possible EIR Response Types. The EIR Response Type is a system-wide EIR option that is configured by the user. The combination of the setting of the EIR Response Type, the list or lists in which the IMEI is located, and the optional IMSI check determines the response that is returned to the querying MSC.

Table 2-2   Logic for IMEIs in Multiple Lists

Presence in List			EIR Response Type		
White	Gray	Black	Type 1	Type 2	Type 3
X			in Allow List	in Allow List	in Allow List
X	X		in Gray List	in Gray List	in Gray List
X	X	X	in Block List	in Block List	in Block List
X		X	in Block List	in Block List	in Block List
	X		in Gray List	in Gray List	unknown
	X	X	in Block List	in Block List	unknown
		X	in Block List	in Block List	unknown
			in Allow List	unknown	unknown

Example Scenarios

Example 1

1. A CHECK_IMEI is received with IMEI = 49876523576823, no IMSI in message.

2. An individual IMEI match is found (Table 2-1, entry 3), indicating that the IMEI is on the Gray and Block Lists. The EIR Response Type is set to Type 3, and an IMSI is not present.

3. Table 2-2 indicates that the required response is *Unknown*.

4. EIR formulates a CHECK_IMEI error response with `Error = 7 unknownEquipment`.

Example 2
Example 2 is the same as Example 1, except that the setting of the EIR Response Type is re-provisioned by the operator to Type 2.

1. A CHECK_IMEI is received with IMEI = 49876523576823, no IMSI in message.

2. An individual IMEI match is found (Table 2-1, entry 3), indicating that the IMEI is on the Gray and Block Lists. The EIR Response Type is set to Type 2, and an IMSI is not present.

3. Table 2-2 indicates that the required response is Block Listed.

4. EIR formulates a CHECK_IMEI response with `Equipment Status = 1 blackListed`.

Example 3

1. A CHECK_IMEI is received with IMEI = 12345678901234, and IMSI = 495867256894125.

2. An individual IMEI match is found (Table 2-1, entry 1) indicating that the IMEI is on the Block List.

3. The EIR Response Type is set to Type 1.

4. Table 2-2 indicates that the normally required response would be Block Listed, however; because an IMSI is present in the message, and the IMEI is on the Block List, the IMSI is compared to the IMSI entry in the database for this IMEI.

5. In this case, the IMSI in the RTDB matches the IMSI in the query, thus the Block Listed condition is cancelled.

6. EIR formulates a CHECK_IMEI response with `Equipment Status = 0 whiteListed`.

Example 4

1. A CHECK_IMEI is received with IMEI = 12345678901234, and IMSI = 495867256894125.

2. An individual IMEI match is found (Table 2-1, entry 1), indicating that the IMEI is on the Block List.

3. The EIR Response Type is set to Type 1.

4. Table 2-2 indicates that the normally required response would be Block Listed, however; because an IMSI is present in the message, and the IMEI is on the Block List, the IMSI is compared to the IMSI entry in the RTDB for this IMEI.

5. In this case, the IMSI in the RTDB does not match the IMSI in the query, the Block Listed condition is maintained.

6. EIR formulates a CHECK_IMEI response with `Equipment Status = 1 blackListed`.

EIR List Determination

If the EIR Global Response configuration option is set (with the `eirgrsp` parameter of the `chg-gsmopts` command) to a value other than `off`, the IMEI is treated as being on the list indicated by the EIR Global Response option, regardless of the actual status of the IMEI. No list logic processing is performed on the IMEI.

If the EIR Global Response option is set to `off`, the individual IMEIs are searched first. If no match is found, the range IMEIs are searched next. If the IMEI is found only on the White List after either search, the list logic processing is complete, and the White List status of the IMEI is sent to the MSC.

Black List Processing

If the IMEI is found on the Black List after either search, list logic processing continues based on the EIR Response Type, set by the `eirrsptype` parameter of the `chg-gsmopts` command. If the EIR Response Type is type 3, and the IMEI is not also found on the White List, the status of the IMEI is unknown.

If the IMEI is also found on the White List, or if the EIR Response Type is either type 1 or 2, the value of the IMSI Check option, set with the `eirimsichk` parameter of the `chg-gsmopts` command, is checked. If the IMSI check option is `on`, and the IMSI is present in the message, the RTDB is searched for the IMSI. If there is a match for the IMSI, the status of the IMEI is determined to be "White with Override." If there is no match for the IMSI, the status of the IMEI is determined to be "Black with IMSI Match Failed." If the value of the IMSI Check option is `off`, the status of the IMEI is determined to be "on the Black List".

Gray List Processing

If the IMEI is found on the Gray List after either search, list logic processing continues based on the EIR Response Type, set by the `eirrsptype` parameter of the `chg-gsmopts` command. If the EIR Response Type is type 3, and the IMEI is not also found on the White List, the status of the IMEI is unknown.

If the IMEI is also found on the White List, or if the EIR Response Type is either type 1 or 2, the status of the IMEI is determined to be "on the Gray List".

EIR Protocol

The EAGLE supports the EIR capability point code type and a local subsystem that is entered into the MAP table. The EIR local subsystem has a mate subsystem, and a concerned point code group assigned to it. ANSI, ITU-I, and ITU-N point codes are supported in the MAP table. The EIR subsystem cannot be set to Load Shared mode (as end nodes do not perform load sharing), but is set to Dominant or Solitary mode.

Messages for Local Subsystems

The message arrives at the EIR subsystem as Rt-on-SSN or Rt-on-GT. If the message arrives as Rt-on-SSN, it must contain either the EAGLE true point code or the EIR capability point code in the DPC field of the message, and EAGLE EIR subsystem number in the Called Party Subsystem field of the message. If EIR query has the EAGLE capability point code for the DPC, then the EAGLE processes the message, but is not able to divert this message in the event of subsystem failure.

If a message arrives at the EIR subsystem as Rt-on-GT, it should also contain a service selector that translates to the EIR subsystem. These messages also contain one of EAGLE capability point codes in the DPC field. The EAGLE also processes the message if it has the EAGLE true point code for the DPC, but it is not able to divert these messages in the event of subsystem failure.

If the EIR local subsystem is offline and the mated subsystem is available, the Routing Indicator is used to determine whether to reroute:

- If the message arrived Rt-on-SSN, the message is not rerouted to the mate. In this case, EAGLE is acting as an end node, and end nodes do not reroute. If the return on error option is set, the EAGLE generates a UDTS, otherwise it discards the message.

- If the message arrived on Rt-on-GT, the message is rerouted to the mated subsystem. In this case, the EAGLE is acting as both STP and SCP, and STPs do reroute messages.

Multiple Local Subsystems

The EAGLE supports provisioning Capability Point Codes (CPCs) for two or more local subsystems, allowing local subsystems for two or more EPAP-related features to operate at the same time in the system. For example, local subsystems for the ATINP feature and the EIR feature can coexist in the system.

Though queries meant for any local system are still be processed if they are sent with DPC = STP CPC, it is strongly recommended not to use the STP CPC for such queries. Instead, the CPC for the appropriate subsystem should be used as the DPC of the message. For instance, for LNP queries use the LNP CPC, not the STP CPC; for EIR queries, use the EIR CPC, and so on.

MTP and SCCP Management to Support EIR

If the EIR local subsystem is offline, the EAGLE sends SSPs that cause the Rt-on-SSN message to be diverted to the mate subsystem. These do not cause the Rt-on-GT messages to be diverted. In order to make other nodes divert Rt-on-GT traffic to the mate, the EAGLE sends response method TFPs to the OPC of the message, when messages arrive Rt-on-GT for one of the EIR Capability Point Codes and the result of translation is the EAGLE EIR subsystem. This TFP should cause the OPC to divert traffic to the mate. If a message arrives Rt-on-GT for the EAGLE True Point Code, the EAGLE does not generate a TFP. Therefore, nodes that send Rt-on-GT traffic to the EAGLE should use an EIR Capability Point Code, not the EAGLE True Point Code.

If the EAGLE receives an RSP (Route Set Test Message - Prohibited) for an EIR Capability Point Code, and the EIR subsystem is offline, the EAGLE does not reply. If the EAGLE receives an RSR (Route Set Test Message - Restricted) for an EIR Capability Point Code, and the EIR subsystem is offline, the EAGLE replies with a TFP concerning the Capability Point Code. When the EIR subsystem is online, RSRT replies to both RSRs and RSPs for an EIR Capability Point Code with a TFA.

Check_IMEI Message Handling

When the CHECK_IMEI message is received by protocol, the, IMSI (if active) and SVN are parsed from the MSU. Because different vendors place the IMSI information in different locations within the message, the decoder searches for the IMSI in multiple locations.

Once the required data is parsed, a lookup is performed in the RTDB to determine the response type for the IMEI/IMSI combination.

The appropriate response message is sent to the originating MSC.

Encoding Errors

When a Response is generated, it is sent based on the CgPA information in the incoming message. However, some conditions may prevent the EAGLE from generating the response. Most of the errors involve GTT on the CgPA; if the incoming data is Rt-on-SSN, the number of potential errors is much smaller.

Whenever an encoding error is detected, the Response message is discarded.

Data Collection

See EIR Measurements for a description of the measurements collected for the EIR feature.

The `rept-stat-sccp` command output displays EIR subsystem status, EIR summary and card statistics, and CPU usage related to EIR. See rept-stat-sccp.

EIR List Log File

The EIR feature allows for detection and logging of subscribers using handsets that have been White Listed, Black Listed, or Grey Listed by a service provider. These messages are generated by the EAGLE and forwarded to the MPS platform for later retrieval. Messages may be forwarded from any of the provisioned Service Module cards. Messages are received and logged independently by both MPS servers.

The files are located in the/var/TKLC/epap/free filesystem and named as follows:
`eirlog_hostname.csv`

Where:

hostname = the hostname of the MPS server that recorded the log.

Each entry in the EIR log file contains information about the caller and handset, a timestamp documenting the time the server received the log entry, and a unique identifier used for comparison with the mate server. See EIR List Log Format for more information about the format of the file and the fields within the file.

The log file is available via Secure FTP using the appuser user.

The EIR log file contains the last 2 million entries received from the EAGLE. This file may be deleted through the EPAP GUI Manage Files & Backups screen.

EIR Log File Serviceability

The file system used by EIR Log Files is approximately 35 GB in size and is used for all of the following in addition to storing EIR log files:

- UI Configuration database backup

- Provisioning database backup

- Real-time database backup

- System log file captures

When the file system reaches 80% of it's total capacity a minor alarm is raised. A major alarm is raised at 90%. All of the files in this partition are managed from the Debug->Manage Logs & Backups screen on the GUI.

EIR Log entries are delivered to and stored on the MPS using a "best effort" approach. The following three major factors impact the successful delivery of a log entry:

- Service Module card connectivity: Service Module cards have a limited buffer for storage of EIR log entries. If the data cannot be delivered, it is discarded.

- UDP Broadcast: A Service Module card broadcasts a log entry to both MPS servers. Although experience shows this broadcast method on a private network to be highly reliable, it is not guaranteed.

- MPS server availability: If an MPS server is down or unreachable, log entries are not collected and stored. Hourly log entries may be later compared with those collected on the mate MPS server using the entry's unique identifier.

EIR List Log Format

The export IMEI Black List hits file consists of CSV entries separated by newlines. Each entry contains the following fields:

- Time/Date stamp: This field represents the time at which the MPS server received the entry from the Service Module card. The time is generated by the MPS using the configured system time. It is formatted as yyyyMMddhhmmss (year, month, day, hour, minute, second).

- Source Identifier: This field is an IP address that uniquely identifies the Service Module card that sent the log entry. This field can be used in combination with the Source Sequence Number to correlate log entries with those on the mate MPS server.

- Source Sequence Number: This field is an integer that uniquely identifies the entry per source Service Module card. This field can be used in combination with the Source Identifier to correlate log entries with those on the mate MPS server.

- IMSI: International Mobile Subscriber Identity for this entry

- IMEI: International Mobile Equipment Identity for this entry

- Response Code: These response codes are possible (2 and 4 are invalid values):

  – 0: Indicates that the IMEI is Black Listed.

  – 1: Indicates that the IMEI is Gray Listed.

  – 2: Indicates that the IMEI is White Listed.

  – 3: Indicates that the IMEI was Black Listed, but the IMSIs matched resulting in a White List Override.

  – 5: Indicates that the IMEI was Black Listed and the IMSIs did not match resulting in Black List Continues.

  – 6: Indicates that the IMEI was not Black/Gray/White Listed, resulting in White List.

- Point Code Type: Point code type of the message originator. Following point code types are possible:

  – Host: indicates the origin-host

  – ANSI: indicates ANSI point code

  – ITUI: indicates ITU International point code

  – ITUN: indicates a 14-bit ITU National point code

- Point Code or Hostname: Point code of the message originator (OPC) or hostname present in the origin-host of the diameter message.

For example, If an MPS server receives entry id 1234 on July 15, 2003, at exactly 4:36 PM from a Service Module card provisioned at address 192.168.120.1 indicating that Black Listed subscriber 9195551212 using handset 12345678901234 has been detected and the originator of the message is from the ANSI point code 3-3-1, the following log entry is created:

```
20030715163600,192.168.61.1,1234,9195551212,12345678901234,0,ANSI,3-3-1
```

Additional EIR Data Files

Additional Files

This feature makes significant use of the /var/TKLC/epap/free file system. The following files may be present:

Data Type	Size	Creation	Cleanup
UI Configuration database backup	< 1K each	On demand at upgrade	Manual
Provisioning database backup	Up to 12 GB each depending on the amount of customer data and the size of the transaction logs	On demand at upgrade	Manual
Real-time database backup	4 GB each	On demand at upgrade	Manual
System log file captures	5-20 MB or more depending on core files, and overall life of system.	On demand by customer service	Manual

Data Type	Size	Creation	Cleanup
EIR Export	Depends on the amount of customer data. Less than 100MB per million instances	Manual by customer	Manual
EIR Auto Export (new for EIR)	Depends on the amount of customer data. Less than 100MB per million instances	Scheduled by customer	Automatic after transferred to customer
PDBI Import	Determined by customer need	Manual (FSTP)	Manual
PDBI Auto Import (new for EIR)	Determined by customer need	Manual (FSTP)	Automatic after data imported
PDBI Auto Import results (new for EIR)	If no errors, very small. May be up to double the PDBI Auto Import file size worst case	Automatic	Automatic after transferred to customer
EIR blocklist logs (new for EIR)	Assuming no more than 360,000 updates per hour from the EAGLE, each file is no more than 25MB	Automatic	Automatic. There should be approximately 25 logs at most.

EIR S13/S13' Interface Support (Diameter EIR/DEIR)

Equipment Identity Register (EIR) is a database containing records of all mobile stations that are allowed or banned in a network. Generally, the banned mobile stations have been declared lost or stolen. Each mobile station is identified by its International Mobile Equipment Identity (IMEI). When a mobile station is detected by the network, the Mobility Management Entity (MME) or Serving GPRS Support Node (SGSN) requests the IMEI of the mobile station, which is sent to the EIR for authorization.

This feature supports the EIR using the Diameter protocol, or more precisely the S13 Diameter interface. It will be running on top of SCTP transport protocol. This feature adds the support for S13 interface to allow diameter requests to be received by an EAGLE card (S13 card). S13 card will forward this request to the EPAP/IMSI SCCP card. SCCP card will perform the EIR database lookup and send the response back to S13 card. S13 card will formulate a reply using response received from SCCP card and send back to the requester.

A new DEIRHC GPL supporting a S13/S13' diameter interface over SCTP will be added. This DEIRHC GPL will run on E5-SM8G-B hardware or SLIC hardware.

EIR S13/S13' Interface Support Limitations

- An E5-SM8G-B or SLIC card running DEIR64 GPL (S13 card) is required to support the EIR S13/S13' Interface Support feature.

- If the Signaling network interface on an SM8G card goes down, the S13 traffic corresponding to that interface is affected.

- An external load balancer is needed to support load-balancing of Diameter messages.

- For initial releases, relay and proxy modes are not included.

- The response is returned on the same Diameter connection on which the request was received. Routing a response over another connection will not be supported in the initial release.

- The EIR S13 Interface Support feature does not support FTRA for new commands.

- DEIRHC GPL can be loaded on E5 SM4G card using debug GPL or if the debug flag is set (in the OS) before the card is loaded.

- S13 feature will not support E5MS for new commands in Release 45.1 but it shall be supported in Release 46.0.

- DEIR GPL loaded on SM8G-B card will not be able to support 8000 TPS on a single association. One association will support approximately 1500 TPS.

S13 Architecture

S13 feature solution stands in between EAGLE EIR database and MME/SGSN acting as S13 EIR application gateway. It will enhance EAGLE's capability to support S13 interface on EAGLE and also provide EIR lookup using EAGLE's RTDB. This can be positioned as S13 solution for operators who are supporting/building LTE networks, and where EAGLE is already deployed to offer EIR solution.

S13 architecture will be:

- New DEIRHC GPL will be created for EAGLE S13 solution.

- DEIRHC GPL will run on E5-SM8G-B card or better.

- S13 card will communicate with OAMHC cards, EPAP/IMSI SCCP cards and MCP cards over IMT.

- S13 card will connect to diameter signaling network using port B.

- E5-SM8G-B card running SCCPHC and SIPHC GPL will continue to work as they work today.

With DEIR re-architecture, commands requiring MPS data or warm restart capability shall still be supported with only S13 feature activated. With the new architecture, SCCP cards can download data from EPAP even when only S13 Feature is activated. This is because DEIR card still requires MPS data from SCCP card for its full functionality.

S13 card supports maximum 8000 diameter transactions per second. In release 47.1, SCCP is also supporting DEIR traffic in addition to the existing traffic. Therefore, when SCCP is running on full capacity, it is recommended to have SCCP: DEIR configuration of 2:1 on the same shelf.

Figure 2-2   S13 Architecture
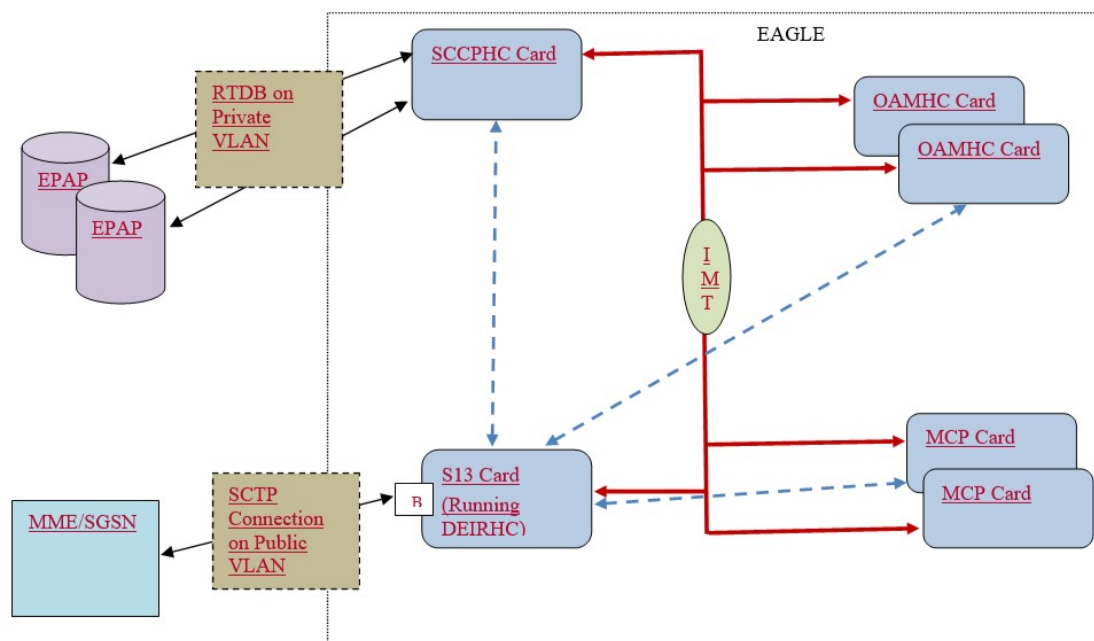
Communication with SCCP Card

S13 card will not support the EPAP connectivity. The EIR lookup will be done by EPAP/IMSI SCCP card. The S13 card will forward the diameter request of EIR lookup to SCCP card. SCCP card will do the lookup and send back the response to the S13 card.

DEIR card will also perform audit every three seconds to check the timer expiry of the message, which was sent to SCCP card. If this timer expires, DEIR card will send ECA back with equipment status set as UNKNOWN.

EIR S13 Connection States

S13 State

S13 Diameter connections maintain a state machine on the S13 Card. The states in #unique_32/unique_32_Connect_42_TABLE_3997F0DC907540918902D00126A496DC are maintained for each diameter connection.

State	Description
CLOSED	SCTP association is set to OPEN=NO and SCTP socket is closed.
INACTIVE	SCTP connection is not established. Initial state
OPEN	SCTP Connection is established. Ready to accept Capability Exchange Request
ACTIVE	Ready to process ECR messages
CLOSING	Transit state to process outstanding messages before moving to Inactive state
PENDING	Waiting for remote to send DWA

An event on the S13 diameter connection causes the transitions between these states. #unique_32/unique_32_Connect_42_TABLE_7C35EE15A7F343C8A7B7A78693045D47 depicts the events that cause a state transition and action taken on a particular event.

The S13 Diameter connection is CLOSED initially when OPEN is set to NO for the associated SCTP connection. When OPEN is changed to YES using the `chg-assoc` command, the Diameter connection is set to INACTIVE state, and attempts to change the SCTP connection status to UP by exchanging SCTP related messages (INIT/INIT-ACK). When the SCTP connection is established, the Diameter connection moves to the OPEN state and waits for a CER message from the peer. If an Invalid CER or any message other than CER is received in the OPEN state, the message is discarded and the SCTP connection is closed by sending an abort to the peer. If a Valid CER is received in the OPEN state, a CEA response is formatted per the connection configuration and is sent to the peer. The Diameter connection moves to the ACTIVE state and is able to receive and process ECR messages. If the SCTP connection is locally closed (by changing OPEN=NO), the corresponding Diameter connection sends a DPR to the peer and waits for an Acknowledgement (DPA) from the peer, and the Td timer is started. The SCTP connection continues to process the outstanding messages on the Diameter connection until the DPA message is received or the Td timer expires. In both cases, the Diameter connection and SCTP connection are closed. If the diameter connection is in the INACTIVE state or the OPEN state, manually closing the local connection moves the state back to CLOSED.

Current State	Event	Action	New State
Any State	Transport Connection disconnected	Stop Any running timer	INACTIVE
INACTIVE	Receive Any message	Discard Message	INACTIVE
INACTIVE	Transport Connection established	None	OPEN
INACTIVE	Manually Close Local Connection	None	CLOSED
OPEN	Invalid CER	Send CEA with Error Cause Disconnect Transport	INACTIVE
OPEN	Any Message other than CER	Silently Discard Message Disconnect Transport	INACTIVE
OPEN	Valid CER	Send CEA with SUCCESS Start Tw timer	ACTIVE
OPEN	Manually Close Local Connection	None	CLOSED
ACTIVE	ECR message	Send ECA Restart Tw timer	ACTIVE
ACTIVE	DWR message	Send DWA Restart Tw timer	ACTIVE
ACTIVE	Any message other than ECR / DWR / DWA / DPR	Discard Message and send error response	ACTIVE
ACTIVE	CER message	Silently discard message	ACTIVE
ACTIVE	Invalid DPR message	Send DPA with Error Cause	ACTIVE
ACTIVE	Valid DPR message	Send DPA Stop all timers Disconnect Transport	INACTIVE

Current State	Event	Action	New State
ACTIVE	Tw timer Expiry #1	Send DWR Restart Tw timer	ACTIVE
ACTIVE	Tw timer Expiry #2	Send DWR Restart Tw timer	PENDING
ACTIVE	Manually Close Local Connection	Send DPR Stop Tw timer Start Td timer	CLOSING
CLOSING	ECR message	Send ECA message	CLOSING
CLOSING	DPA message	Disconnect Transport	INACTIVE
CLOSING	DPR message	Disconnect Transport	INACTIVE
CLOSING	None	Wait for Td Disconnect Transport	CLOSED
PENDING	DWA Message	Restart Tw Timer	ACTIVE
PENDING	ECR Message	Send ECA Restart Tw Timer	ACTIVE
PENDING	Tw timer Expiry #3	Send DPR Stop Tw timer Start Td timer	CLOSING
PENDING	DPR Message	Send DPA Stop all timers Disconnect Transport	INACTIVE
PENDING	Manually Close Local Connection	Send DPR Stop Tw timer Start Td timer	CLOSING

S13 Supported Messages

S13 Messages supported by EAGLE

Diameter messages are classified as requests or responses. The Diameter request and response messages in #unique_33/ unique_33_Connect_42_TABLE_A483FD8274C24B61BE5C7575E13B50D5 are processed by the EAGLE. The S13 card processes only these messages and sends a 3001 response for all unsupported Diameter request messages.

Message Name	Short Name	Command Code	EAGLE Behavior	Description
Capability Exchange Request	CER	257	Receive	Exchanged between peers to discover the identity and capabilities of the peer.
Capability Exchange Answer	CEA	257	Send	
Disconnect-Peer-Request	DPR	282	Recv/Send - Both	These messages are exchanged between peers when they agree to disconnect the transport layer connection.
Disconnect-Peer-Answer	DPA	282	Recv/Send - Both	
Device-Watchdog-Request	DWR	280	Recv/Send - Both	These messages check the status of connection between two peers

Message Name	Short Name	Command Code	EAGLE Behavior	Description
Device-Watchdog-Answer	DWA	280	Recv/Send - Both	when no traffic has been exchanged between them.
ME-Identity-Check-Request	ECR	324	Receive	These messages are exchanged on S13/S13' interface between MME/ SGSN and EIR database to track the lost/stolen handset.
ME-Identity-Check-Answer	ECA	324	Send	

S13 Supported AVPs

AVPs Supported by S13

The Diameter Attribute Value Pairs (AVPs) supported on the S13 card are shown in #unique_34/unique_34_Connect_42_TABLE_BBB36FAF69364B29BF814682550A7307.

AVP Name	AVP Code	Description
AUTH-APPLICATION-ID	258	This AVP contains the list of application IDs supported. The value of the Auth-Application-Id AVP in ECR/ECA must match the Application Id present in the Diameter message header.
AUTH_SESSION_STATE	277	This AVP is present in the ECR message and specifies whether the state for a particular session is to be maintained. These values are supported: • STATE_MAINTAINED 0 • NO_STATE_MAINTAINED 1
DESTINATION_REALM	283	This AVP contains the Realm to which the message is to be routed. This is a mandatory AVP in an ECR message. The value is checked against the local Realm value configured in the IPHOST table.
DISCONNECT_CAUSE	273	This AVP is included in a DPR request message to inform the peer of the reason for its intention to shut down the transport connection. It is of type Enum and supports these values: • Rebooting - 0 • Busy - 1 • Do_not_want_to_talk_to_you - 2 Disconnect cause to be specified in outgoing DPR message is configured in DEIROPTS table.

AVP Name	AVP Code	Description
EQUIPMENT_STATUS	1445	This mandatory AVP in the ECA message contains the status of equipment after performing EIR database lookup (Blocklist, Allowlist, Greylist, or Unknown).
ERROR-MESSAGE	281	The Error message AVP contains the human readable text of error result code to be sent to the peer.
FAILED_AVP	279	This is a grouped AVP and provides the debugging information when a request is rejected or not fully processes due to erroneous information in a specified AVP.
HOST_IP_ADDRESS	257	This AVP contains IP addresses of the originator of the Diameter message. **Note**: Only one instance of this AVP is supported. All other instances are discarded.
IMEI	1402	This AVP contains the IMEI of the specific equipment.
ORIGIN_HOST	264	The Origin Host AVP contains the hostname of the originator of the Diameter message. The value is checked against the remote host value configured in the IPHOST table.
ORIGIN_REALM	296	This AVP contains the Realm of the originator of the Diameter message. The value is checked against the remote Realm value configured in the IPHOST table.
PRODUCT_NAME	269	This AVP contains the vendor assigned name of the product. Product Name to be specified in outgoing message is configured in DEIROPTS table. **Note**: This is a mandatory AVP in CER.
PROXY-INFO	284	If any Proxy-Info AVP is present in the request, it is added to the answer message in the same order as it is present in the request.
ROUTE-RECORD	282	If this AVP is present in the request, it is added to the answer message in the same order as it is present in the request.
RESULT_CODE	268	This AVP indicates whether a particular request was completed successfully or an error occurred.

AVP Name	AVP Code	Description
SESSION-ID	263	If this AVP is present in the request message, copy the same session ID in the response message.
TERMINAL_INFORMATION	1401	The mandatory grouped AVP of the ECR message contains IMEI and software version. The IMEI AVP value is used for EIR database lookup.
USER_NAME	1	This AVP contains the IMSI of the specific equipment. The IMSI value along with IMEI is used for database lookup.
VENDOR_ID	266	This AVP contains the predefined IANA value assigned to the Diameter Software vendor. For CEA message outgoing from EAGLE, this parameter is set to 0.
VENDOR_SPECIFIC_APPLICATION_ID	260	This grouped AVP in the CEA message contains these AVPs: • vendor-id avp - Vendor Id to be specified in outgoing message is 10415. • auth-application-id - auth-application-id to be specified in outgoing message is configured in DEIROPTS table as APPLID.

EIR S13/S13' Interface Support - ECA Message Encoding

After the Equipment status is determined, the ECA message with the following details is send to the originator of the request.

• Common information

• Session-ID, Route-record or Proxy-Info AVP: If the Session-ID, Route-record or Proxy-Info AVP is present in the ECR message, they are appended in the same order as presented in the request message. A maximum of ten Route-record and Proxy-Info AVPs can be copied from the request message.
In case of multiple AVPs, derating will be applied basis of message size. The following table lists the de-rating factor and the supported TPS per association.

Table 2-3   Multiple AVPs supported TPS (de-rating)

Message size (in bytes)	Traffic supported
Message size <= 232	250
Message size > 232	0.7 *250 – ((RoundUp (message size - 232 / 32) -1) * 25)

Example of the TPS supported by the association if the message size is 264:

= [0.7*250 – (((RoundUp (264 - 232)/32) -1) *25)]

= 175 – ((RoundUp (32/32) -1) * 25)

= 175 – (0*25)

= 175

Thus, when the message size is 264, the supported TPS for that association will be 175.

- Result-Code and Equipment-Status AVPs: Result-Code and Equipment-Status AVPs are populated as shown in Table 2-4.

Table 2-4   Mapping of EIR database Response and ECR Result

EIR Response	ME-Check-Identity Response	
	Result Code	Equipment-Staus
in Whitelist	DIAMETER_SUCCESS	WHITELISTED (0)
in Blacklist	DIAMETER_SUCCESS	BLACKLISTED (1)
in Graylist	DIAMETER_SUCCESS	GREYLISTED (2)
Unknown*	DIAMETER_ERROR_EQUIPME NT_UNKNOWN	NA

EIR S13/S13' Interface Support - ECR Message Processing

The following diagram describes the overall flow of ECR Message processing by S13 card. After successful decoding, S13 card will send the ECR request to EPAP/IMSI SCCP card to determine the status of equipment.

Figure 2-3   ECR Message Processing
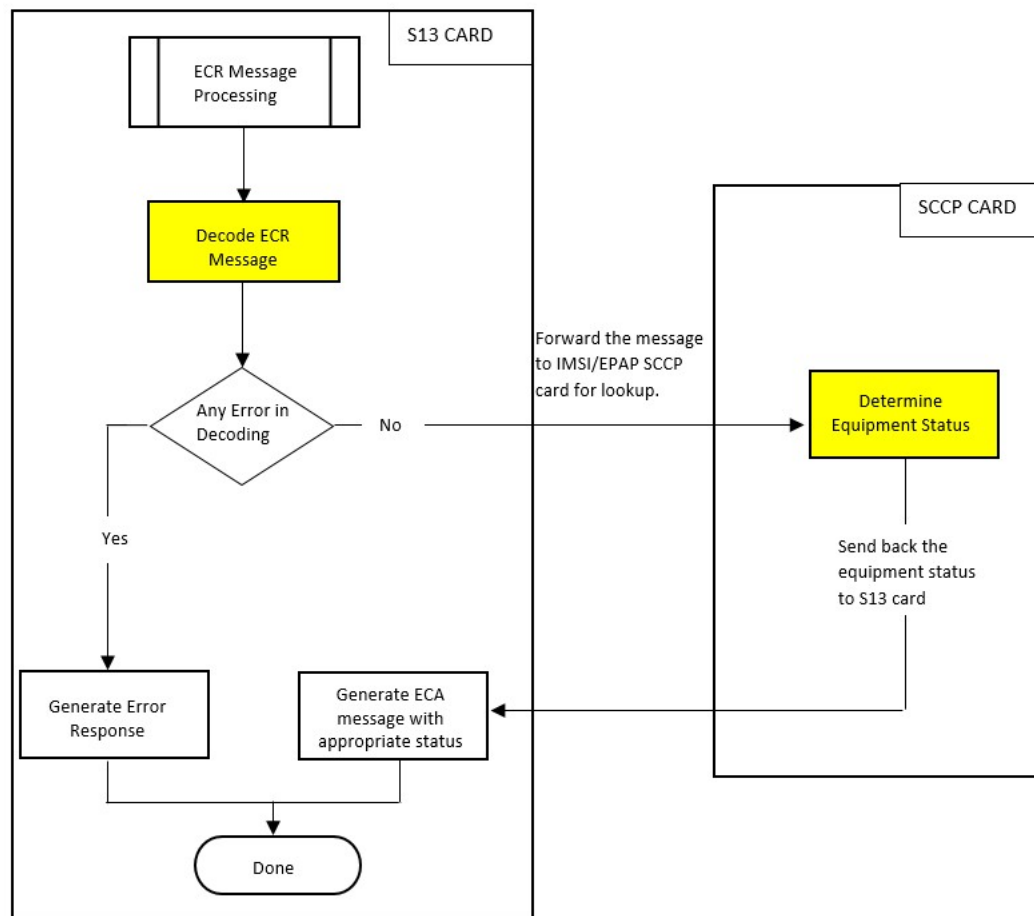
EIR S13/S13' Interface Support Result Codes

Supported Result Codes

Result Code Value	Readable Value	Error-Message AVP Values	
		Text String	
2001	DIAMETER_SUCCESS	diameter success	
3001	DIAMETER_COMMAND_UNSUPPORTED	diameter Command not supported	
3004	DIAMETER_TOO_BUSY	diameter is busy	
3007	DIAMETER_APPLICATION_UNSUPPORTED	diameter application not supported. **Note**: Only EIR Application ID is supported.	
3008	DIAMETER_INVALID_HDR_BITS	invalid bits in diameter header	
3010	DIAMETER_UNKNOWN_PEER	unknown peer	
5001	DIAMETER_AVP_UNSUPPORTED	diameter avp not supported	
2001	DIAMETER_SUCCESS	diameter success	

Result Code Value	Readable Value	Error-Message AVP Values
		Text String
3001	DIAMETER_COMMAND_UN SUPPORTED	diameter Command not supported
3004	DIAMETER_TOO_BUSY	diameter is busy
3007	DIAMETER_APPLICATION_ UNSUPPORTED	diameter application not supported. **Note**: Only EIR Application ID is supported.
5004	DIAMETER_INVALID_AVP_V ALUE	invalid avp value **Note**: Received invalid IMEI or IMSI value .
5005	DIAMETER_MISSING_AVP	missing avp
5006	DIAMETER_RESOURCES_E XCEEDED	Diameter Resource Exceeded
5009	DIAMETER_AVP_OCCURS_ TOO_MANY_TIMES	diameter avp occurs too many times
5010	DIAMETER_NO_COMMON_ APPLICATION	no common application
5011	DIAMETER_UNSUPPORTE D_VERSION	diameter version not supported
5014	DIAMETER_INVALID_AVP_L ENGTH	invalid avp length
5015	DIAMETER_INVALID_MESS AGE_LENGTH	invalid message length
5422	DIAMETER_ERROR_EQUIP MENT_UNKNOWN	unknown equipment

DEIR on SLIC Network Redundancy Enhancement

The DEIR on SLIC Network Redundancy Enhancement introduces network communication redundancy.

The existing functionality has been enhanced by introducing network communication redundancy. Currently, the Diameter EIR (DEIR) application architecture uses a single signaling network.

Overview

With the DEIR on SLIC Network Redundancy Enhancement, two network interfaces will be supported for Diameter 2 interfaces for signaling and two signaling networks at the same time.Interfaces B/C will be used for signaling network. The DEIR card will not support EPAP connectivity.

Signaling Network Redundancy

SLIC Card with DEIR application will be connected to signaling network using interface B and C to support redundancy.

If one interface/switch goes down then traffic switches to another port/switch, as SLIC card running DEIR application supports Multi-homing. Please refer section 10.3 for Multi-homing. Figure 2-4 depicts signaling network redundancy.

Figure 2-4   SLIC Card Signaling Network Redundancy
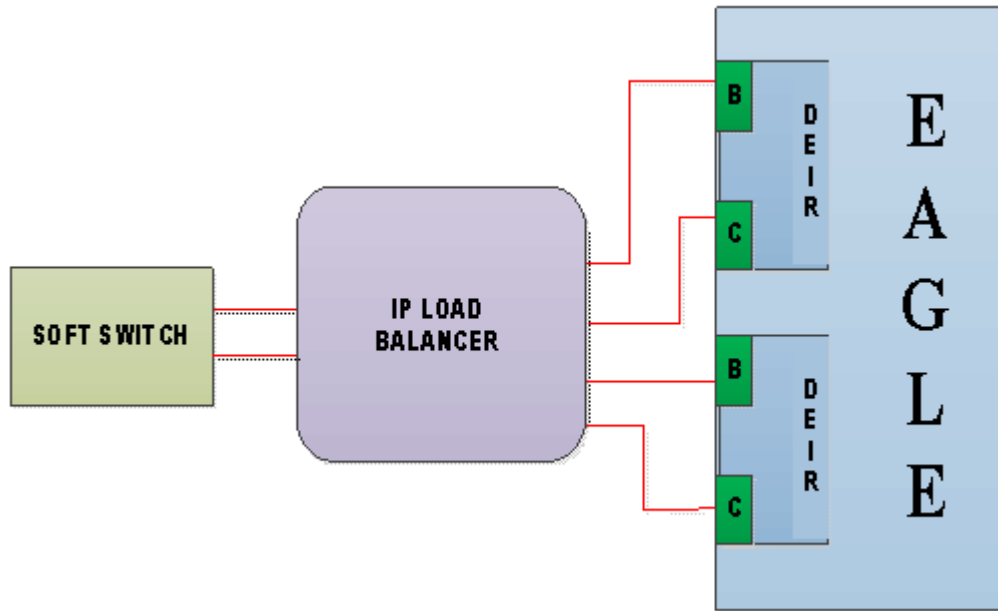
If one interface/switch goes down, traffic switches to another port/switch, as the SLIC card running the DEIR application supports multi-homing (see Multi-Homing Support).

Multi-Homing Support

SCTP multi-homing provides a level of fault tolerance against network failures by using alternate paths through the IP network between two endpoints, as shown in Figure 2-5.

By enabling the redundant port in this feature, the SCTP protocol now provides SCTP multi-homing endpoint support; that is, when an SCTP association is formed, it lists both the IP addresses for the respective interfaces (B and C). As a multi-homed association endpoint, SCTP data is allowed to flow on either of the Ethernet interfaces and thus provides more robust network connectivity.

Figure 2-5   Multi-Homed SCTP Association
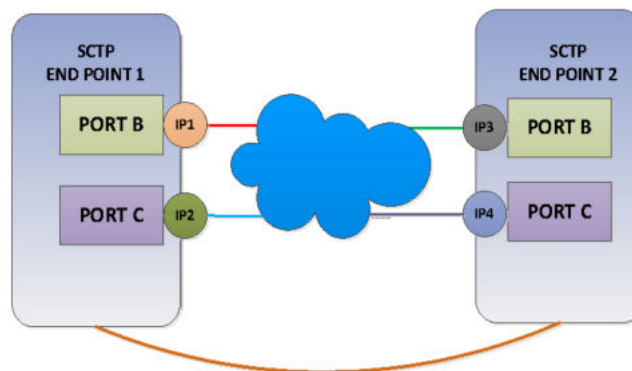
DEIR supports SCTP IETF multi-homed server associations using both interfaces B and C on a SLIC card. The presence of an assigned local host (`lhost`) and an alternate local host

(`alhost`) indicates that an association is multi-homed and capable of utilizing both Ethernet interfaces for association operations.

The `lhost` parameter of the `ent-assoc` and `chg-assoc` commands is used to represent the IP address that corresponds to either the B or C port of the SCTP association end point. Multi-homed endpoints are SCTP associations configured with both the `lhost` and `alhost` parameters. In this case, the `lhost` represents an IP address corresponding to one interface (B or C) while the `alhost` represents an IP address corresponding to the other interface of the same end point.

Hardware Requirements

EPAP-related features that perform an RTDB lookup require Service Module cards (E5-SM8G-B or SLIC cards) running the SCCPHC application (for MAP-based EIR) or E5-SM8G-B/SLIC cards running the DEIR64 application (for Diameter-based EIR). The EAGLE can be equipped with up to 32 (31+1) Service Module cards.

Features that do not perform an RTDB lookup require Service Module cards only for GTT processing that might be performed for the feature. These features can coexist in systems with EPAP, but do not require an EPAP connection.

Front Panel LED Operation

On SM8G-B card, the Ethernet Interface B is used for the Signaling Network. Table 2-5 captures the LED operations for the Ethernet Interfaces on E5-SM8G-B cards.

Table 2-5   E5-SM8G-B Faceplate IP Interface/Logical Link Status LED Operation for Port B

IP Interface Status	Signaling Connection		
	Link/Connection Status	PORT B LED	ACT B LED
IP port not configured	N/A	Off	Off
Card inhibited			
Cable removed and/or not synched	N/A	Red	Red
Sync	Not configured	Green	Red
Sync and/or `act-ip-lnk`	All are OOS-MT-DISABLED or OOS-MT	Green	Red
	At least one connection is down (OOS-MT-DISABLED or OOS-MT)	Green	Red
	All configured connections are Active	Green	Green
`dact-ip-lnk`	N/A	Green	Red

On SLIC card, the Ethernet Interface 2 and 3 (mapped to port B and C respectively) are used for the Signaling Network. Table 21 and Table 22 Table 20 captures LED operations for the Ethernet Interfaces on SLIC cards

Table 2-6   SLIC Front Faceplate IP Interface/Logical Link Status LED Operation for Port B & C (represented by LED 3 & 2 respectively)

| IP Interface Status | Signaling Connection | | |
	Link/Connection Status	PORT LED	LINK LED
IP port not configured Card inhibited	N/A	Off	Off
Cable removed and/or not synched	N/A	Red	Red
Sync	Not configured	Green	Red
Sync and/or `act-ip-lnk`	All are OOS-MT-DISABLED or OOS-MT	Green	Red
	At least one connection is down (OOS-MT-DISABLED or OOS-MT)	Green	Red
	All configured connections are Active	Green	Green
`dact-ip-lnk`	N/A	Green	Red

Figure 2-6   SLIC Faceplate Status LEDs
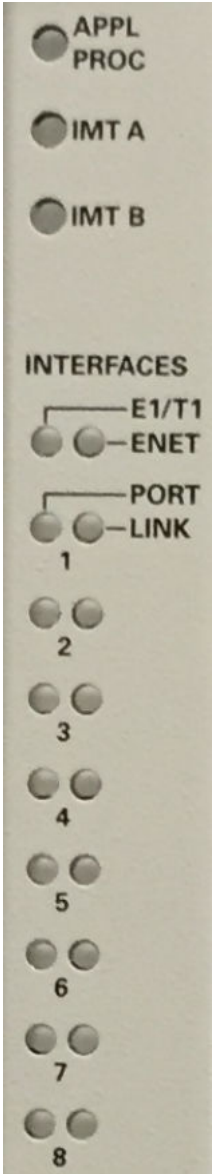
Table 2-7 describe LED operations for the Ethernet Interfaces on SLIC cards.

Table 2-7   SLIC Faceplate IP Interface/Logical Link Status LED Operation for Port B and C (Represented by LEDs 3 and 2 Respectively)

IP Interface Status	Link/Connection Status	Signaling Connection	
		PORT LED	LINK LED
IP port not configured	N/A	Off	Off
Card inhibited			
Cable removed and/or not synched	N/A	Red	Red
Sync	Not configured	Green	Red

Table 2-7 (Cont.) SLIC Faceplate IP Interface/Logical Link Status LED Operation for Port B and C (Represented by LEDs 3 and 2 Respectively)

IP Interface Status	Signaling Connection		
	Link/Connection Status	PORT LED	LINK LED
Sync and/or act-ip-lnk	All are OOS-MT-DISABLED or OOS-MT	Green	Red
	At least one connection is down (OOS-MT-DISABLED or OOS-MT)	Green	Red
	All configured connections are Active	Green	Green
dact-ip-lnk	N/A	Green	Red

On SLIC card front plate, E1/T1 LED should be off and ENET LED should be green.

The PORT LED will be GREEN when IP setting is 100/full. If IP setting is 1000/FULL, PORTLED will be AMBER.

> ⓘ **Note**
>
> `dact-ip-lnk` command causes the detachment of IP stack from the GEI driver for the specified port, but does not stop the GEI driver.

MPS/EPAP Platform

Oracle provides the Multi-Purpose Server (MPS) platform as a subsystem of the Oracle Communications EAGLE. The MPS provides support for EPAP-related features that perform Real Time Database (RTDB) lookups.

The MPS is composed of hardware and software components that interact to create a secure and reliable platform. For details about the MPS hardware, refer to *Application B Card Hardware and Installation Guide*. The MPS provides the means of connecting the customer provisioning application with the EAGLE and accepts the customer number portability data, while accommodating numbers of varying lengths.

The Oracle Communications EAGLE Application Processor (EPAP) is software that runs on the MPS hardware platform. EPAP collects and organizes customer provisioning data, and forwards the data to the EAGLE Service Module cards. For detailed information about EPAP, refer to *Administration Guide* for EPAP.

In this manual, Service Module card refers to an E5-SM4G, E5-SM8G-B, or SLIC card unless a specific card is required. For more information about the supported cards, refer to *Hardware Reference*.

3

EAGLE EIR Commands

This chapter contains brief descriptions of the EAGLE commands that can be used for configuration of the EIR feature.

EAGLE Commands for EIR

This chapter describes the EAGLE commands that are used for the configuration of the EIR feature.

Refer to *Commands User's Guide* for complete command descriptions including parameter names, valid parameter values, examples, and dependencies.

Table 3-1   Commands used for EIR

Type	Commands
System Serial Number	ent/rtrv-serial-num
Card	ent/dlt/rtrv/alw/inh/init/rept-stat-card
Feature Control	chg/rtrv-feat, enable/chg/rtrv-ctrl-feat
EAGLE STP Self Identification	chg/rtrv-sid
Mated Application (MAP)	chg/dlt/ent/rtrv-map
Subsystem Application	chg/dlt/ent/rtrv-ss-appl
Service Selector	chg/dlt/ent/rtrv-srvsel
EIR GSM Options	chg/rtrv-gsmopts
Local Subsystem Activation	alw/inh-map-ss
SCTP Associations in Table IPAPSOCK	chg/dlt/ent/rept-stat/rtrv-assoc
IP Host Table	dlt/ent/rtrv-ip-host
Alarm Thresholds	chg/rtrv-th-alm

EAGLE EIR GSM Options Commands

The GSM Options (gsmopts) commands are used to change and report on the values of one or more of the system-level processing options maintained in the GSMOPTS table. All values are assigned initially to system defaults at STP installation time, and they can be updated later using the `chg-gsmopts` command.

The options described in Table 3-2 apply to EIR.

Table 3-2   GSMOPTS Options for EIR

Parameter	Range	Description
EIRIMSICHK	OFF or ON	EIR IMSI Check status
EIRRSPTYPE	TYPE1, TYPE2, TYPE3	EIR Response Type
EIRGRSP	OFF, WHITELST, GRAYLST, BLKLST, UNKNOWN	EIR Global Response status

The EIRIMSICHK (EIR IMSI Check status) parameter is used to indicate whether or not the IMSI will be used when determining if an IMEI is to be Black Listed. If this parameter is `on` and an IMEI is found on the Black List, then the corresponding IMSI is retrieved. If the IMSI found in the message matches the IMSI retrieved, then the IMEI is considered to be on the White List. If the IMSIs do not match or the IMSI is not found, then the IMEI will remain Black Listed.

The EIRRSPTYPE parameter is used to determine the EIR Response Type. The Response Type is used to determine how the lists are searched, as shown in Table 3-3.

Table 3-3   Individual IMEI List Determination

Black List	Gray List	White List	IMSI Check	IMSI Match	Result Type	LOG Entry	LOG Entry Result	MSU Result Equipment Status
Y	N	N	Y	Y	1	N	White with IMSI Override	0
Y	N	N	Y	Y	2	N	White with IMSI Override	0
Y	N	N	Y	Y	3	N	Unknown	Return Error=7
Y	N	N	Y	N	1	Y	Black with IMSI Failed	1
Y	N	N	Y	N	2	Y	Black with IMSI Failed	1
Y	N	N	Y	N	3	N	Unknown	Return Error=7
Y	N	Y	N	DC	1	Y	Black	1
Y	N	Y	N	DC	2	Y	Black	1
Y	N	Y	N	DC	3	Y	Black	1
Y	N	Y	Y	Y	1	N	White with IMSI Override	0
Y	N	Y	Y	Y	2	N	White with IMSI Override	0
Y	N	Y	Y	Y	3	N	White with IMSI Override	0
Y	Y	N	N	DC	1	Y	Black	1
Y	Y	N	N	DC	2	Y	Black	1
Y	Y	N	N	DC	3	N	Unknown	Return Error=7
Y	Y	N	Y	Y	1	Y	White with IMSI Override	0
Y	Y	N	Y	Y	2	Y	White with IMSI Override	0
Y	Y	N	Y	Y	3	Y	White with IMSI Override	0
N	Y	N	Y	DC	1	Y	Gray	2
N	Y	N	Y	DC	2	Y	Gray	2
N	Y	N	Y	DC	3		Unknown	Return Error=7
N	Y	Y	DC	DC	1	Y	Gray	2
N	Y	Y	DC	DC	2	Y	Gray	2
N	Y	Y	DC	DC	3	Y	Gray	2
N	N	Y	DC	DC	1	N	White	0

Table 3-3   (Cont.) Individual IMEI List Determination

Black List	Gray List	White List	IMSI Check	IMSI Match	Result Type	LOG Entry	LOG Entry Result	MSU Result Equipment Status
N	N	Y	DC	DC	2	N	White	0
N	N	Y	DC	DC	3	N	White	0
N	N	N	DC	DC	1	N	White	0
N	N	N	DC	DC	2	N	Unknown	Return Error=7
N	N	N	DC	DC	3	N	Unknown	Return Error=7
Y	Y	Y	N	DC	1	Y	Black	1
Y	Y	Y	N	DC	2	Y	Black	1
Y	Y	Y	N	DC	3	Y	Black	1
Y	Y	Y	Y	Y	1	N	White with IMSI Override	0
Y	Y	Y	Y	Y	2	N	White with IMSI Override	0
Y	Y	Y	Y	Y	3	N	White with IMSI Override	0
Y	Y	Y	Y	N	1	N	Black with IMSI Failed	1
Y	Y	Y	Y	N	2	N	Black with IMSI Failed	1
Y	Y	Y	Y	N	3	N	Black with IMSI Failed	1

For EIR Response Types 1 or 2, the IMEI searches are handled in the following manner:

- If the IMEI is found in the Black List table, the search stops without searching the White and Gray List tables. The IMEI is considered Black Listed regardless of IMEI's presence on the White or Gray List tables.

- If the IMEI is found in the Gray List table, but not found in the Black List table, the search stops without searching the White List table. The IMEI is considered Gray Listed regardless of the IMEI's presence on the White List table.

For EIR Response Type 3, the IMEI searches are handled in the following manner:

- The White List table is searched first. If the IMEI is not found in the White List table, the IMEI is treated as unknown - no other table searches need to be performed.

- If the IMEI is found in the White List table, the Black List table is searched next. If the IMEI is in the White and Black List tables, the IMEI is considered Black Listed - no need to search the Gray List table.

- If the IMEI is found in White List table, but not in the Black List table, the Gray List table is searched. If the IMEI is in the White and Gray list tables, the IMEI is considered Gray Listed. If the IMEI is in the White List table, but not in the Gray List table, the IMEI is considered White Listed.

The EIRGRSP parameter is used to turn on the EIR Global Response Type. The Global Response Type is used to override the response that is normally sent back to the MSC. The default is set to OFF. When set to OFF, the normal list logic is applied to the IMEI. If the Global

Response Type is set to something other than `OFF`, then there is no list logic processing and the corresponding response is sent to the MSC.

EAGLE EIR Service Selector Commands

The EIR service selector (srvsel) commands are used to enter, delete, change, and display the service selectors required to change a service entry for a DSM service entry.

- The EIR service is `eir`.

- EIR supports ANSI, ITU-I, and ITU-N Global Title Indicators.

  The Global Title Indicator (GTI) value can be either 2 or 4. The Numbering Plan and Nature of Address Indicator cannot be specified when the GTI is 2, and must be specified when the GTI is 4.

- EIR does not support the Service Nature of Address or the Service Numbering Plan.

- The Subsystem Number (SSN) must be defined in the MAP table, and supports the asterisk (*) value.

EAGLE Feature Control Commands

The `chg/rtrv-feat` commands are used to turn on and display the on/off status of features, such as the GTT feature, that are controlled with feature bits. After a feature that is controlled with a feature bit is turned on, the feature cannot be turned off.

The `enable/chg/rtrv-ctrl-feat` commands are used to enable, turn on, and display the status of controlled features that are controlled by feature access keys. The feature access key is based on the feature part number and the serial number of the system that uses the feature, making the feature access key site-specific. When a feature is enabled by entering the `enable-ctrl-feat` command with the feature part number and feature access key, the feature is recognized by the system. Other actions might be required to make the feature fully operational, such as turning the feature on, installing hardware, and provisioning information in database tables.

Some features can be enabled with a temporary part number and feature access key for a limited trial of the feature. When the trial period expires, the feature must be enabled with a permanent part number and feature access key to continue use of the feature.

EIR S13/S13' Interface Support Commands

The commands in support the EIR S13/S13' Interface Support feature.

Table 3-4   Commands for EIR S13/S13' Interface Support feature

Command	Description
`chg-deiropts`	configures S13-specific options
`rtrv-deiropts`	displays S13-specific options
`ent-dconn`	configures Diameter connection and flow control by entering Diameter connection values associated to a particular association in table IPAPSOCK
`chg-dconn`	changes Diameter connection and flow control configuration values
`dlt-dconn`	deletes Diameter connection
`rtrv-dconn`	displays Diameter connection status and flow control data

Table 3-4   (Cont.) Commands for EIR S13/S13' Interface Support feature

Command	Description
`rept-stat-deir`	displays S13 card statistics
`rept-stat-sccp`	displays the status of the Service Module cards and the services executing on those cards
`rept-stat-mfc`	displays the status of the Message Flow Control (MFC) service

Table DEIROPTS

The `chg-deiropts` and `rtrv-deiropts` commands configure and display the EIR S13/S13' Interface Support options of the virtual table DEIROPTS, which is part of table EGLEOPTS. The table DEIROPTS options are shown in Table 3-5.

Table 3-5   Table DEIROPTS options

Name	Values	Description
DEIRIMSICHK	OFF	IMSI Check
	ON	The IMSI Check specifies whether IMSI is used when determining if an IMEI is to be blocklisted. If this option is set to ON and an IMEI is found on the Blocklist, then the corresponding IMSI will be retrieved. If the IMSI found in the message matches the IMSI retrieved, then the IMEI is considered to be on the Allowlist. If the IMSIs do not match or the IMSI is not found, then the IMEI will remain blocklisted.
		Default value is OFF.
DEIRRSPTYPE	TYPE1	S13 Response Type
	TYPE2	The S13 Response Type is used to determine how the lists are to be searched.
	TYPE3	Default value is TYPE1.
DEIRGRSP	OFF	S13 Global Response Type
	WHITELST	The S13 Global Response Type is used to override the response that is sent to the MME or SGSN. When S13 Global Response Type is set to OFF, the normal list logic is applied to the IMEI. If the S13 Global Response Type is set to any value except OFF, then list logic processing is not performed and the corresponding response is sent to the MME or SGSN.
	GRAYLST	
	BLKLST	
	UNKNOWN	
		Default value is OFF.
CONGERR	3004	Congestion Error
	5006	This is the value in the result code Attribute Value Pair (AVP) of the response sent at the time of congestion. If the incoming messages on the card running the DEIR64 GPL exceed the card or connection capacity and the card is not able to process the messages, the messages are discarded and the card responds with the configured value in the result code.
		• 3004 - DIAMETER_TOO_BUSY [default value]
		• 5006 - DIAMETER RESOURCES EXCEEDED

Table 3-5   (Cont.) Table DEIROPTS options

Name	Values	Description
VENDID	*unsigned32*	S13 local Vendor ID
		All outgoing messages that require Vendor ID in VENDOR_SPECIFIC_APPLICATION_ID use this configured value. Because only the value 10415 is supported, the CEA message contains 10415 as the Vendor Id in the response.
		Default value is 0.
PRODUCT	*alphanumeric string*	Product Name
		The configured value contains the vendor-assigned name for the product. All outgoing messages that require the Product Name AVP use this configured value.
		Default value is NONE.
APPLID	*unsigned32*	Authentication Application ID
		The configured Application ID should match the Auth-Application-Id (AVP Code 258) value in the Vendor-Specific-Application-ID AVP. Currently, only 16777252 APPLID is supported by EAGLE and this parameter cannot be changed.
		Default value is 16777252.
DPRCAUSE	REBOOTING (0) BUSY (1) DO_NOT_WANT_TO_TALK (2)	Disconnect Cause
		The Disconnect Cause in all DPR messages generated by EAGLE use this value.
		Default value is DO_NOT_WANT_TO_TALK (2).

Table DCONN

The `ent-dconn`, `chg-dconn`, `dlt-dconn`, and `rtrv-dconn` commands configure and display the EIR S13/S13' Interface Support options of the table DCONN, which supports the provisioning information associated with the Diameter connection. The table DCONN options are shown in .

Table 3-6   Table DCONN options

Name	Values	Description
DCNAME	*alphanumeric string*	Diameter Connection Name
		The Diameter Connection Name identifies the Diameter connection linked to an association. This option is mandatory.
ANAME	*alphanumeric string*	Association Name
		This name identifies the association configured in the association table with the Diameter adapter. This option is mandatory.
RSVDTPS	*integer from 100 to 8000, inclusive*	Reserved TPS
		This is the guaranteed TPS for a connection. Total RSVDTPS on a card cannot exceed 8000.
		Default value is 250.

Table 3-6   (Cont.) Table DCONN options

Name	Values	Description
MAXTPS	*integer from 100 to 8000, inclusive*	Max TPS
		The unused S13 card capacity is allocated among the connections that have exceeded their RSVDTPS values up to the limit of MAXTPS value provisioned for the particular connection.
		Default value is 8000.
TW	6sec - 30sec	Diameter Watchdog Timer
		Default value is 6sec.
TD	1sec - 10sec	Diameter Peer Disconnect Timer
		Default value is 3sec.

REPT-STAT-DEIR Command

The `rept-stat-deir` command displays the overall status of the Diameter EIR S13/S13' service on the EAGLE. This command is similar to the `rept-stat-sccp` and `rept-stat-sip` commands. The Diameter connection status is displayed in the *Status* field when the `rept-stat-deir` command is entered with the `dcname` parameter. The possible values for Diameter *Status* parameter are:

- UP - The Diameter connection status is up and active. This status supports the following Diameter connection states: Active, Closing, Pending.

- DOWN - The Diameter connection status is down or closed. This status supports the following Diameter connection states: Inactive, Open, Closed.

The `rept-stat-deir` command can be entered with or without parameters. If the `rept-stat-deir` command is entered without parameters, the displayed consists of a *per diameter card* status, TPS on each S13 card, total S13 statistics, and alarms associated with the Diameter EIR S13/S13' service in the `DEIR ALARM STATUS` field. The following parameters can be entered with the `rept-stat-deir` command:

- `loc` - Diameter card location for which card status, overall card TPS, and per-connection card statistics are reported

- `peakreset` - Reset peak values for a card or a specified Diameter connection

- `mode` - Overall S13 TPS and per diameter connection statistics in the EAGLE displayed; allowed value: perf

- `dcname` - Diameter connection name, which is the unique logical name assigned to each diameter connection; output display: status, TPS, and statistics of the specified Diameter connection

The `rept-stat-deir` command displays the pegs shown in Table 3-7.

Table 3-7   REPT-STAT-DEIR Pegs

Pegs	Condition
SUCCESS	Messages which fall in these categories: • Success response • IMEI Lookup failure and DEIRRSPTYPE=TYPE1

Table 3-7   (Cont.) REPT-STAT-DEIR Pegs

Pegs	Condition
ERROR	Messages which fall in these categories: • Decoding error • Unsupported messages
WARNING	Messages which fall in these categories: • IMEI Lookup failure and DEIRRSPTYPE=TYPE2 or TYPE3 • Unknown equipment is sent in response
OVERFLOW	Number of message discarded due to congestion
TOTAL MSGS	Total number of messages received: Success + Error + Warning messages

PASS Commands supported by S13 card

The S13 card supports the following PASS commands:

- **ARP** - displays and modifies the Internet to Ethernet address translation tables used by the address resolution protocol

- **ASSOCRTT** - displays round-trip statistics for a given association

- **CPUM** - displays CPU utilization

- **MSUCOUNT** - displays MSU count for particular association and routes, including S13/S13' protocol

- **NETSTAT** - displays network statistics from the IP stack

- **NSLOOKUP** - returns the IP address for a specified hostname, or returns a hostname for a specified IP address

- **PING** - tests for the presence of hosts on the network

- **SCTP -** displays MSU count and current state of specific association

- **SYSSTAT** - display system buffer, CPU configuration, and database-related information

- **TRACEROUTE** - returns/traces the complete path a message has taken to reach the destination

4

EIR Configuration

This chapter identifies prerequisites and procedures for configuration of the EIR feature in the EAGLE.

Introduction

This chapter describes prerequisites and procedures for configuration of the EIR feature on the EAGLE.

The Equipment Identity Register (EIR) feature is configured on the EAGLE and on the **EPAP** (in association with either the **G-Flex** or **G-Port** feature). This chapter covers the EAGLE configuration only. Refer to *Administration Guide* for EPAP and EPAP Entity Provisioning in this manual for information about EPAP configuration.

EIR Configuration Procedure lists the steps for enabling and turning on the feature, and for the provisioning required for the feature. Each step contains a link or reference to information and procedures to use to complete the step. Feature provisioning can be performed only after the EIR feature is turned on. Refer to *Commands User's Guide* for complete descriptions of the commands used in these procedures.

> ⓘ **Note**
>
> The EIR feature is optional and you must be entitled to use it in your system. If you are not sure whether you are entitled to use a specific feature, contact your Sales Representative or Account Representative.

EPAP Entity Provisioning

Oracle recommends that EPAP entity (**SP** or **RN**) administration not be performed until after the Point Code and/or Subsystem Number has been entered into the EAGLE MAP table.

- EPAP-administered entity data can become out-of-sync with the EAGLE MAP table when the creation of Point Codes and/or Subsystem Numbers in the MAP table is performed after EPAP database administration.

- If this mismatch is discovered in real-time operations, a UIM is sent to the EAGLE maintenance terminal. (Example UIMs: `SCCP did not route – DPC not in MAP tbl`, `SCCP did not route – SS not in MAP tbl`.)

System Prerequisites

Before any feature that is described in this manual can be enabled, the prerequisites listed in Table 4-1 are required in the system.

Table 4-1   System Prerequisites

Prerequisite	Verification and Provisioning
The system serial number must be correct and locked. For new installations, the system is shipped with an unlocked serial number. The serial number can be changed if necessary and must be locked after the system is on-site.	**Note**: The serial number cannot be changed after it is entered and locked in the system. Locate the serial number for the system on a label affixed to the control shelf (1100). Enter the `rtrv-serial-num` command to display the serial number and its locked status.
For systems that are being upgraded, the serial number is usually already verified and locked.	Verify that the displayed serial number is correct for the system. If no serial number is displayed, enter the `ent-serial-num` command (without the lock parameter) to provision the serial number that appears on the control shelf label. Enter the `rtrv-serial-num` command and verify that the serial number was entered correctly. Enter the `ent-serial-num` command with the `lock=yes` parameter to lock the serial number in the system.
A sufficient number of Service Module cards must be equipped.	Enter the `rept-stat-card:appl=vsccp` command to list the Service Module cards in the system. If more cards or cards of a different type are needed, refer to the procedures in *Database Administration - GTT User's Guide* to add or remove Service Module cards.
The GTT feature must be on in the system. Some features require an additional GTT-related feature such as EGTT. See the specific feature prerequisites in this section.	Enter the `rtrv-feat` command to display the GTT feature status. If the GTT feature is on, the gtt=on entry appears in the output. If the `gtt=off` entry appears in the output, use the procedures in *Database Administration - GTT User's Guide* to turn on and provision the GTT feature and any other GTT-related features and functions that will be used in the system.

EIR Feature Prerequisites

Before the EIR feature can be enabled, the following prerequisites are required in the system:

Table 4-2   EIR Feature Prerequisite

Prerequisite	Verification and Provisioning
The ANSIGFLEX system option cannot be set to Yes.	Enter the `rtrv-stpopts` command. Verify that the ANSIGFLEX entry does not appear in the command output or that the ANSI GFLEX entry shows a value of No.

Table 4-2   (Cont.) EIR Feature Prerequisite

Prerequisite	Verification and Provisioning
The LNP feature cannot be on in the system.	Enter the `rtrv-ctrl-feat` command. If the LNP feature is on, shown with a quantity greater than zero for the `LNP ported TNs` entry in the command output, the feature described in this manual cannot be enabled.

EIR Configuration Procedure

The EAGLE configuration of the Equipment Identity Register (EIR) feature consists of the following steps. The steps contain links and references to detailed procedures and information needed to complete each step.

1. Verify, and provision if needed, the system prerequisites. See System Prerequisites.

2. Verify, and provision if needed, the feature prerequisites. See EIR Feature Prerequisites.

3. Enable the EIR feature, set system STP options, and turn on the EIR feature. See Enabling and Turning On the EIR Feature.

4. Change the self identification of the EAGLE node to include true point codes and EIR capability point codes. Refer to the procedures in *Database Administration - SS7 User's Guide*.

5. Refer to the procedures in *Database Administration - GTT User's Guide* to provision the following items:

   • Translation types and mappings

   • Mated Application (MAP) table entries for the EIR feature that contain the EAGLE ANSI, ITU-I, and ITU-N true point codes, the EIR capability point codes, and the EIR subsystem number. Only solitary and dominant loadsharing are supported.

   The EIR subsystem can have a mate subsystem and a concerned point code group assigned to it in the MAP table.

   If multiple point code types for EIR are provisioned in the MAP table, then the point code type for the Subsystem Out-of-Service Request message (SOR) is determined using the following order:

   a. ANSI

   b. ITU-N

   c. ITU-N Spare

   d. ITU-I

   e. ITU-I Spare

6. Provision the state and subsystem number for the EIR local subsystem application. See Adding the EIR Subsystem Application.

7. Provision the service selector mechanism to route MSUs to the EIR subsystem. See Provisioning the EIR Service Selectors.
The EIR service is `eir`.

The Translation Type and Subsystem Number are the values assigned for the EIR local subsystem when the MAP table entries were defined. See Step 5 in this procedure. The asterisk value (*) for the Subsystem Number is supported for the EIR subsystem.

EIR supports ANSI, ITU-I, and ITU-N Global Title Indicators.

- The `gtii`/`gtin`/`gtin24` value can be either 2 or 4.

- If the `gtii`/`gtin`/`gtin24` value is 2, the `np`, `nai`, `npv`, or `naiv` parameters cannot be specified with the `ent-srvsel` command.

- If the `gtii`/`gtin`/`gtin24` value is 4, either the `np` and `nai` or the `npv` and `naiv` parameters must be specified with the `ent-srvsel` command.

EIR does not support the Service Nature of Address or the Service Numbering Plan.

8. Provision GSM options, including the EIR Global Response status, EIR Response Type, and EIR IMSI Check status options. See Changing the EIR Options.

9. Activate the EIR local subsystem. See Activating the EIR Local Subsystem.

10. Configure the Measurements Platform feature or the E5-OAM Integrated Measurements feature if measurements are to be collected for EIR.

   Refer to the procedures in *Database Administration - System Management User's Guide* for configuring the Measurements Platform feature, the E5-OAM Integrated Measurements feature, and the EAGLE OA&M IP Security feature in the EAGLE. OAM-based measurements reports are not available for EIR.

Enabling and Turning On the EIR Feature

This procedure is used to enable and turn on the **EIR** feature in the EAGLE.

- The EIR feature must be enabled using the EIR feature part number 893012301 and a feature access key.

> ⓘ **Note**
>
> Controlled features are optional and you must be entitled to use them in your system. If you are not sure whether you are entitled to use a specific feature, contact your Sales Representative or Account Representative.

> ⓘ **Note**
>
> Controlled features must be purchased before you can receive a feature access key to use to enable the feature. If you are not sure if you have purchased a feature and received the feature access key, contact your Sales Representative or Account Representative.

The feature access key is based on the EIR feature part number and the serial number of the system, making the feature access key site-specific.

When the EIR feature is enabled, it is permanently enabled. The EIR feature cannot be temporarily enabled.

- After the EIR feature has been enabled, the EIR feature must be turned on using the `chg-ctrl-feat` command with the EIR feature part number and the status=on parameter.

1. Enable the EIR feature. Enter the `enable-ctrl-feat` command with the EIR feature part number 893012301 and the FAK.

2. Turn on the EIR feature on. Enter the `chg-ctrl-feat` command with the EIR feature part number 893012301 and the `status=on` parameter.

3. Verify the changes. Enter the `rtrv-ctrl-feat` command with part number 893012301.

```
rlghncxa03w 10-06-30 21:16:37 GMT  EAGLE5 42.0.0
The following features have been permanently enabled:
Feature Name              Partnum    Status  Quantity
HC-MIM SLK Capacity       893012707  on          64
EIR                       893012301  on      ------
```

4. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

   These messages should appear; the active **Maintenance and Administration Subsystem** Processor (**MASP**) appears first:

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

Provisioning the EIR Local Subsystem

The following procedures in this section are used to add or remove a local subsystem application:

- Adding the EIR Subsystem Application
- Removing the EIR Subsystem Application

See the procedures in Changing the State of a Subsystem Application to take the subsystem application online or offline.

> ⓘ **Note**
>
> The EAGLE supports the operation of two or more local subsystems for **EPAP-related features** in the system at one time. For example, the local subsystems for INP and EIR can coexist in the system.

Adding the EIR Subsystem Application

This procedure is used to define the EIR subsystem application. The subsystem application can be taken online when it is defined or later in the configuration process (see Changing the State of a Subsystem Application).

Before the EIR local subsystem can be added to the database, the following prerequisites must exist in the system:

Table 4-3   EIR Local Subsystem Prerequisites

Prerequisite	Verification
The EIR feature must be enabled and turned on.	Enter the `rtrv-ctrl-feat` command. If the EIR entry with Status of on does not appear in the output, see the Enabling and Turning On the EIR Feature procedure.
The application specified by the `appl` parameter (`eir`) cannot already be in the database.	Enter the `rtrv-ss-appl` command. If the EIR entry appears in the output , this procedure cannot be performed.
EAGLE true point codes and EIR capability point codes must be defined, and entered in the Mated Application (MAP) table with a subsystem number to be used for the EIR subsystem application.	Only one subsystem number for the application can be defined, and must be used for all point code types assigned to the local subsystem. Enter the `rtrv-sid` command, and verify that the true and capability point codes (`PCI` and `PCN` fields) needed for the feature are correct. If changes are required, refer to the procedures in *Database Administration - SS7 User's Guide*. Enter the rtrv-map command, and verify that the MAP table entries include EAGLE true point code and the SSN for the EIR local subsystem. If changes are required, refer to the procedures in *Database Administration - GTT User's Guide* for provisioning solitary and dominant mated applications.

The example in this procedure reserves the subsystem number 100 for the EIR application and sets the EIR application status to `online`.

1. Add the EIR application and subsystem number, using the `ent-ss-appl` command.

   If the `stat=online` parameter is not specified, the status defaults to `offline`.

2. Verify the changes; enter the `rtrv-ss-appl` command.

   ```
   tekelecstp 10-07-25 08:02:22 EST  EAGLE5 42.0.0
   APPL   SSN  STAT
   EIR    100  online

   SS-APPL TABLE IS 25% FULL (1 OF 4)
   ;
   ```

3. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

   The following messages should appear; the active Maintenance and Administration Subsystem Processor (**MASP**) appears first:

   ```
   BACKUP (FIXED): MASP A - Backup starts on active MASP.
   BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
   BACKUP (FIXED): MASP A - Backup starts on standby MASP.
   BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
   ```

Removing the EIR Subsystem Application

This procedure is used to remove a subsystem application from the database. The subsystem application to be removed must be in the database and the subsystem must be out of service.

1. Display the subsystem number for the EIR local subsystem application in the database; enter the `rtrv-ss-appl` command.

2. Display the operating status of the EIR subsystem; enter the `rept-stat-sccp` command.

   If the subsystem is out of service, shown by an entry containing OOS-MT-DSBLD for the subsystem in the `rept-stat-sccp` output, go to 5.

3. Place the EIR subsystem application out of service. Enter the `inh-map-ss` command and specify the EIR subsystem number displayed in 1.

   ```
   inh-map-ss:ssn=100
   ```


   ```
   rlghncxa03w 10-06-28 14:42:38 GMT  EAGLE5 42.0.0
   Inhibit map subsystem command sent to all SCCP cards.
   Command Completed.
   ```

4. Verify that the EIR subsystem is out of service by entering the `rept-stat-sccp` command.

   If the local subsystem is not out of service, return to 3 and enter the `inh-map-ss` command with the `force=yes` parameter specified.

5. Remove the local subsystem application from the database, by entering the `dlt-ss-appl` command.

   When this command has successfully completed, the following message appears:


   ```
   rlghncxa03w 09-04-05 17:34:20 EST  EAGLE 41.0.0
   DLT-SS-APPL: MASP A - CAUTION: DELETED APPL SSN MAY BE REFERENCED BY GTT
   ENTRY
   DLT-SS-APPL: MASP A - COMPLTD
   ;
   ```

6. Verify the changes; enter the `rtrv-ss-appl` command.

7. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

   The following messages should appear, the active **Maintenance and Administration Subsystem** Processor (**MASP**) appears first:


   ```
   BACKUP (FIXED): MASP A - Backup starts on active MASP.
   BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
   BACKUP (FIXED): MASP A - Backup starts on standby MASP.
   BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
   ```

Changing the State of a Subsystem Application

The procedures in this section are used to set the state of an existing subsystem application to either online or offline.

The online or offline status of the subsystem application is shown in the `STAT` field of the `rtrv-ss-appl` command output.

The `rept-stat-sccp` command displays the operating state (in or out of service) of the subsystem.

If the subsystem application is to be taken online, the subsystem application must be offline.

When the subsystem is taken online (regardless of how the subsystem was taken offline), the EAGLE sends SNR/SSA. A UAM is generated, indicating that the subsystem is ALLOWED.

If the subsystem application is to be taken offline, the subsystem application must be online. The subsystem must be taken out of service (OOS-MT-DSBLD) with the `inh-map-ss` command before it can be taken offline.

A subsystem application can be taken offline using coordinated state change, or forced offline without using coordinated state change.

When the `inh-map-ss` command is entered for the subsystem, a coordinated shutdown is attempted. If the coordinated shutdown fails, a UIM is generated, indicating that the shutdown failed. If the `force` parameter is specified, the subsystem is forced to shut down; a coordinated shutdown is not performed.

For coordinated state change, SCMG sends an **SOR** message to the mated subsystem and will start a T_{coord} timer (30 seconds). If SCMG receives an SOG message from the mated subsystem before the T_{coord} timer expires, SCMG will broadcast SSPs to the concerned point code group, send SBR/SSP, and take the subsystem offline. A UAM is generated, indicating that the subsystem is PROHIBITED. If the SOG is not received before T_{coord} expires, then the inhibit request is denied and a UIM is generated.

When the subsystem is taken offline without coordinated state change, the EAGLE sends SBR/SSPs. A UAM is generated, indicating that the subsystem is PROHIBITED.

When the EAGLE receives an **SOR** message from its mated subsystem, it will reply with an **SOG** message if both of the following conditions are met. If either of these conditions is not met, the EAGLE will not reply to the SOR message.

- The local subsystem is available

- The total load on the DSM subsystem is less than 45% of its capacity

Taking the Subsystem Application Online

Use the procedure in this section to take the subsystem application online.

1. Verify the state of the subsystem application - online or offline, by entering the rtrv-ss-appl command.

```
    tekelecstp 08-07-25 08:02:22 EST   EAGLE5 42.0.0
    APPL   SSN  STAT
    EIR    11   offline
```

```
            SS-APPL TABLE IS 25% FULL (1 OF 4)
        ;
```

If the EIR subsystem is online, this procedure does not need to be performed.

2. Display the operating status of the subsystem by entering the `rept-stat-sccp` command.

3. Take the subsystem application online. Enter the `chg-ss-appl` command with the `nstat=online` parameter.

   ```
   chg-ss-appl:appl=eir:nstat=online
   ```

4. Verify the changes by entering the `rtrv-ss-appl` command.

   ```
       tekelecstp 08-07-25 08:02:22 EST  EAGLE5 42.0.0
       APPL    SSN  STAT
       EIR     11   online

       SS-APPL TABLE IS 25% FULL (1 OF 4)
   ;
   ```

5. Back up the new changes using the `chg-db:action=backup:dest=fixed` command.

   The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

   ```
   BACKUP (FIXED): MASP A - Backup starts on active MASP.
   BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
   BACKUP (FIXED): MASP A - Backup starts on standby MASP.
   BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
   ```

Taking the Subsystem Application Offline

Use the procedure in this section to take a subsystem application offline.

1. Verify the online or offline state of the subsystem application, by entering the rtrv-ss-appl command.

   ```
       tekelecstp 08-07-25 08:02:22 EST  EAGLE 42.0.0
       APPL    SSN  STAT
       EIR     11   online

       SS-APPL TABLE IS 25% FULL (1 OF 4)
   ;
   ```

If the EIR subsystem application is offline, this procedure does not need to be performed.

2. Verify the operating status of the subsystem by entering the `rept-stat-sccp` command.

3. Place the subsystem out of service. Specify the subsystem number displayed in the output in [Taking the Subsystem Application Online](#).

   ```
   inh-map-ss:ssn=11

       rlghncxa03w 08-06-28 14:42:38 GMT EAGLE 42.0.0
       Inhibit map subsystem command sent to all SCCP cards.
   ```

```
     Command Completed.
;
```

4. Verify that the subsystem is out of service, by entering the `rept-stat-sccp` command.

5. Take the subsystem offline. Enter the `chg-ss-appl` command with the `nstat=offline` parameter.

   `chg-ss-appl:appl=eir:nstat=offline`

6. Verify the changes by entering the `rtrv-ss-appl` command.

```
     tekelecstp 08-07-25 08:02:22 EST  EAGLE 42.1.0
     APPL   SSN  STAT
     EIR    11   offline

     SS-APPL TABLE IS 25% FULL (1 OF 4)
;
```

7. Back up the new changes using the `chg-db:action=backup:dest=fixed` command.

   The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Provisioning the EIR Service Selectors

The procedures in this section describe how to add, change, and remove a service selector. The information is indicated that is specific to EIR.

Adding an EIR Service Selector

This procedure is used to add a service selector for the EIR feature.

The EIR feature must be enabled and turned on before an EIR service selector can be added.

1. Verify that the EIR feature is enabled and turned on, by entering the `rtrv-ctrl-feat` command.

   If the EIR feature is enabled and turned on, the status of the EIR feature is `on`

```
rlghncxa03w 10-06-30 21:15:37 GMT  EAGLE5 42.0.0
The following features have been permanently enabled:
Feature Name              Partnum    Status  Quantity
HC-MIM SLK Capacity       893012707  on            64
EIR                       893012301  on          ----
;
```

   • If the EIR feature is enabled and turned on, continue with 2.

   • If the EIR feature is not enabled or turned on, go to the Enabling and Turning On the EIR Feature procedure to enable and turn on the EIR feature. Then continue with 2.

2. Display the EIR service selectors in the database, using the `rtrv-srvsel:serv=eir` command.

```
rlghncxa03w 10-06-28 14:42:38 GMT  EAGLE5 42.0.0

GTII  TT   NP        NAI   SSN  SNP    SNAI   SERV
4     1    e214      intl  3    ----   -----  eir
4     2    e214      intl  *    ----   -----  eir

SRV SELECTOR table is (4 of 20992)   1 % full
;
```

3. Add the EIR service selector using the `ent-srvsel` command.

   For example, enter a command like these:

   `ent-srvsel:serv=eir:tt=35:ssn=100:gtin=4:np=e214:nai=natl`

   `ent-srvsel:serv=eir:tt=57:ssn=75:gtin=2`

4. Verify the changes; enter the `rtrv-srvsel` command with the parameters and values used in 3.

   `rtrv-srvsel:serv=eir:tt=35:ssn=100:gtin=4:np=e214:nai=intl`

```
rlghncxa03w 10-06-28 14:42:38 GMT  EAGLE5 42.0.0

GTIN  TT   NP        NAI   SSN  SNP    SNAI   SERV
4     35   e214      natl  100  ----   -----  eir

SRV SELECTOR table is (6 of 20992)   1 % full
;
```

   `rtrv-srvsel:serv=eir:tt=57:ssn=75:gtin=2`

```
rlghncxa03w 10-06-28 14:42:38 GMT  EAGLE5 42.0.0

GTIN  TT   NP        NAI   SSN  SNP    SNAI   SERV
2     57   ---       ----  75   ----   -----  eir

SRV SELECTOR table is (6 of 20992)   1 % full
;
```

5. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

   The following messages should appear, the active **Maintenance and Administration Subsystem** Processor (**MASP**) appears first:

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Removing a Service Selector

This procedure is used to remove a service selector from the database.

1. Display the service selectors in the database, using the `rtrv-srvsel` command.

   The serv, gtii, gtin, gtin24, tt, ssn, np, nai, npv, and naiv parameter values can be used to limit the amount of information displayed with the `rtrv-srvsel` command.

2. Remove the service selector from the database, using the `dlt-srvsel` command.

   To remove a service selector, the `gtii`/`gtin`/`gtin24`, `tt`, and `ssn` parameter values must be entered as shown in the `rtrv-srvsel` output.

   For example, enter a command like these:

   `dlt-srvsel:serv=eir:tt=35:ssn=100:gtin=4:np=e214:nai=natl`

   `dlt-srvsel:serv=eir:tt=57:ssn=75:gtin=2`

3. Verify the changes; enter the `rtrv-srvsel` command with the parameters and values used in [2](#).

4. Back up the changes, using the `chg-db:action=backup:dest=fixed` command.

   The following messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first:

   ```
   BACKUP (FIXED): MASP A - Backup starts on active MASP.
   BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
   BACKUP (FIXED): MASP A - Backup starts on standby MASP.
   BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
   ```

Changing an Existing Non-EIR Service Selector to an EIR Service Selector

This procedure is used to change a non-EIR service selector to an EIR service selector for the EIR feature.

The only parameters that can be changed using this procedure are:

`:nserv` – New DSM service type, `EIR`

`:nsnp` – An EIR service selector cannot contain an SNP value; if the service selector being changed contains an SNP value, this value must be changed to `none` with this parameter. `:nsnai` – An EIR service selector cannot contain an SNAI value; if the service selector being changed contains an SNAI value, this value must be changed to `none` with this parameter.

The `chg-srvsel` command requires that the `gtii`/`gtin`/`gtin24`, `tt`, `np`, `nai`, `npv`, `naiv`, `ssn`, and `serv` parameters be specified with the values shown in the `rtrv-srvsel` output for the service selector being changed. If you want to change any of these parameter values for an EIR service selector, use the Removing a Service Selector procedure to remove the existing service selector. Then use the Adding an EIR Service Selector procedure to add the new EIR service selector with the new parameter information.

1. Display the service selectors in the database using the `rtrv-srvsel` command.

   ```
   rlghncxa03w 03-06-28 14:42:38 GMT  EAGLE5 42.0.0
   ```

```
GTII   TT   NP      NAI    SSN  SNP    SNAI    SERV
4      1    e214    intl   3    ---    ---     eir
4      1    e214    intl   4    e164   intl    gport
4      1    e214    intl   5    e164   intl    smsmr
4      2    e214    intl   *    ---    ---     eir

GTIN   TT   NP      NAI    SSN  SNP    SNAI    SERV
2      75   ---     ---    57   ---    ---     eir
4      4    e214    natl   34   e164   intl    gflex
4      9    e214    natl   250  e164   intl    gflex
4      35   e214    natl   100  ---    ---     eir

SRV SELECTOR table is (8 of 20992)   1 % full
;
```

- If the `rtrv-srvsel` output in 1 does not show any EIR service selectors, continue with 2.

- If the `rtrv-srvsel` output in 1 shows at least one EIR service selector, go to 3.

2. Verify that the EIR feature is enabled and turned on; enter the `rtrv-ctrl-feat` command.

   - If the EIR feature is not enabled (does not appear in the command output) or is not turned on, go to the Enabling and Turning On the EIR Feature procedure to enable and turn on the EIR feature. Then continue with 3.

   - If the EIR feature is enabled and turned on, continue with 3.

3. Change the service selector, using the `chg-srvsel` command.

   For example, enter a command like the following one:
   ```
   chg-
   srvsel:gtin=4:tt=4:np=e214:nai=natl:ssn=34:nsnp=none :nsnai=none:ns
   erv=eir
   ```

   If the `snp` or `snai` parameter values are shown as dashes in the `rtrv-srvsel` output, these parameters cannot be specified with the `chg-srvsel` command. If the `gtii`/`gtin`/ `gtin24` parameter value is 2, the `np`, `nai`, `npv`, and `naiv` parameters cannot be specified with the `chg-srvsel` command.

   If the `gtii`/`gtin`/`gtin24` parameter value is 4, either the `np` and `nai`, or the `npv` and `naiv` parameters must be specified with the `chg-srvsel` command. The `np` and `nai` parameters can be specified in place of the `npv` and `naiv` parameters, and the `npv` and `naiv` parameters can be specified in place of the `np` and `naiv` parameters so long as parameter values be specified correspond to the values shown in the `rtrv-srvsel` output.

   The `gtii`/`gtin`/`gtin24`, `tt`, `ssn`, `np`, `nai`, `npv`, or `naiv` parameters cannot be changed in this procedure. To change these parameters, use the Removing a Service Selector procedure to remove the service selector. Then use the Adding an EIR Service Selector procedure to re-enter the service selector as an EIR service selector.

4. Verify the changes; enter the `rtrv-srvsel` command with the parameters and values that were used in 3.

5. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first:

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Changing the EIR Options

This procedure is used to change the EIR Global Response status, EIR Response Type, and EIR **IMSI** Check status option values with the `chg-gsmopts` command. The `chg-gsmopts` command uses these parameters to detect circular routing in the system. See EAGLE EIR GSM Options Commands.

1. Verify that the EIR feature is enabled and turned on; enter the `rtrv-ctrl-feat` command.

```
    rlghncxa03w 09-06-29 16:40:40 EST  EAGLE5 41.1.0
    The following features have been permanently enabled:
    Feature Name               Partnum    Status  Quantity
    HC-MIM SLK Capacity        893012707  on            64
    EIR                        893012301  on          ----
;
```

    •   If the EIR feature is not enabled (the EIR entry does not appear in the output) or is not turned on, go to the Enabling and Turning On the EIR Feature procedure to enable and turn on the EIR feature. Then continue with 2.

    •   If the EIR feature is enabled and turned on, continue with 2.

2. Display the status of the EIR options; enter the `rtrv-gsmopts` command.

3. Change the EIR options by entering the `chg-gsmopts` command with at least one of the EIR option parameters.

4. Verify the changes; enter the `rtrv-gsmopts` command.

5. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

    These messages should appear; the active **Maintenance and Administration Subsystem** Processor (**MASP**) appears first:

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

Configuring EIR S13/S13' Interface Support (Diameter EIR/DEIR)

This procedure configures the EIR S13/S13' Interface Support feature. 6 through 9 configure the DEIR connection.

1. Enable the EIR S13/S13' Interface Support feature with the `enable-ctrl-feat` command.

   `enable-ctrl-feat:partnum=893042401:fak=<FeatureAccessKey>`

2. Turn on the EIR S13/S13' Interface Support feature with the `chg-ctrl-feat` command.

   `chg-ctrl-feat:partnum=893042401:status=on`

3. Provision the S13 card (DEIR64).

   `ent-card:loc=1101:type=dsm:appl=deir64`

4. Configure the Default Router.

   `chg-ip-card:loc=1101:defrouter=10.248.13.1`

5. Configure Port A and B of the S13 card.

   `chg-ip-lnk:port=b:submask=255.255.255.0:mcast=no:ipaddr=10.248.13.11:loc=1101:duplex=full:speed=100`

6. Enter the HOST information.

   `ent-ip-host:host=hss:ipaddr=10.248.13.11:type=local:realm=abcdefg.com`

   `ent-ip-host:host=lmno:ipaddr=10.248.13.9:type=remote:realm=lmnopq.com`

   `ent-ip-host:host=lmno3:ipaddr=10.248.13.3:type=remote:realm=lmnopq.com`

7. Enter the SCTP Association.

   `ent-assoc:aname=assoc1:lhost=hss:lport=5555:rhost=lmno:rport=5556`

   `ent-assoc:aname=assoc2:lhost=hss:lport=5557:rhost=lmno3:rport=5558`

8. Enter the Diameter Connection.

   `ent-dconn:  dcname=dcon1:aname=assoc1`

   `ent-dconn:  dcname=dcon2:aname=assoc2`

9. Open the Diameter Connection.

   `chg-assoc:aname=assoc1:open=yes`

   `chg-assoc:aname=assoc2:open=yes`

Configuring DEIR on SLIC

This procedure configures the EIR S13/S13' Interface Support (DEIR) feature on the SLIC card to provide network redundancy. Step 5 through step 8 configure the DEIR connection.

1. Enable the DEIR feature with the `enable-ctrl-feat` command.

   `enable-ctrl-feat:partnum=893042401`

2. Turn on the DEIR feature with the `chg-ctrl-feat` command.

   `chg-ctrl-feat:partnum=893042401:status=on`

3. Provision the SLIC S13 card (DEIR64).

   `ent-card:loc=1101:type=dsm:appl=deir64`

4. Configure ports A, B, C, and D of the SLIC S13 card.

```
chg-ip-
lnk:port=b:submask=255.255.255.0:mcast=no:ipaddr=10.248.13.11:loc=1
101:duplex=full:speed=100
```

```
chg-ip-
lnk:port=c:submask=255.255.255.0:mcast=no:ipaddr=10.248.14.12:loc=1
101:duplex=full:speed=100
```

```
chg-ip-
lnk:port=d:submask=255.255.255.0:mcast=yes:ipaddr=192.168.121.20:lo
c=1101:duplex=full:speed=100
```

5. Enter the HOST information.

```
ent-ip-
host:host=hss:ipaddr=10.248.13.11:type=local:realm=abcdefg.com
```

```
ent-ip-
host:host=hss2:ipaddr=10.248.14.12:type=local:realm=abcdefg.com
```

```
ent-ip-
host:host=lmno:ipaddr=10.248.13.9:type=remote:realm=lmnopq.com
```

```
ent-ip-
host:host=lmno3:ipaddr=10.248.13.3:type=remote:realm=lmnopq.com
```

```
ent-ip-
host:host=lmno4:ipaddr=10.248.14.5:type=remote:realm=lmnopq.com
```

```
ent-ip-
host:host=lmno5:ipaddr=10.248.14.7:type=remote:realm=lmnopq.com
```

6. Enter the SCTP Association.

```
ent-
assoc:aname=assoc1:lhost=hss:alhost=hss2:lport=5555:rhost=lmno:rpor
t=5556
```

```
ent-
assoc:aname=assoc2:lhost=hss:alhost=hss2:lport=5557:rhost=lmno3:rpo
rt=5558
```

7. Enter the Diameter Connection.

```
ent-dconn: dcname=dcon1:aname=assoc1
```

```
ent-dconn: dcname=dcon2:aname=assoc2
```

8. Open the Diameter Connection.

```
chg-assoc:aname=assoc1:open=yes:rhost=lmno4:rhosttype=alternate
```

```
chg-assoc:aname=assoc2:open=yes:rhost=lmno5:rhosttype=alternate
```

Activating the EIR Local Subsystem

The procedure in this section explains how to activate the EIR local subsystem.

When all feature configuration is complete, the EIR subsystem application must taken online and the local subsystem must be activated to allow it to begin operation.

When the local subsystem operating state is Inhibited, the `chg-ss-appl` command can be used to change the online or offline database state of the subsystem. The `rtrv-ss-appl` command displays the online or offline provisioned value.

When the first Service Module card is loaded, the local subsystem operating state tells whether the subsystem should be considered allowed (online) or inhibited (offline). This is a database state. If the command is accepted, then the change is made to the tables and can be read after an `init-sys` command is entered to initialize the system.

When the Service Module cards are in-service and the subsystem application is online, the `alw/inh-map-ss` commands can be used to change the dynamic operating state of the local subsystem to allowed or inhibited. The `inh-map-ss` command does not necessarily force a state change, because it can fail if the mate does not send an SOG. The `force=yes` parameter must be specified to bypass the SOR/SOG exchange and inhibit immediately. (There is no `rtrv-map-ss` command.)

The procedures in Changing the State of a Subsystem Application explain how to take a local subsystem online and offline.

Table 4-4   Subsystem Allow/Inhibit

Command\ Subsystem State	Offline	Online
`alw-map-ss`	Command is rejected because the subsystem must be online to be in the Allowed state.	Attempts to make the local subsystem active
`inh-map-ss`	Command accepted, but no action because offline implies inhibited.	Attempts to inhibit the local subsystem. Use of the `force=yes` parameter bypasses the SOR/SOG exchange and inhibits immediately
`chg-ss-appl:appl=eir :nstat=online`	Changes local subsystem status to online.	No change to local subsystem status in the database
`chg-ss-appl:appl=eir :nstat=offline`	Command is rejected because the subsystem must be inhibited to go offline.	Changes local subsystem database status to `offline`.

1. Display the online/offline status of the EIR subsystem application, by entering the `rtrv-ss-appl` command.

```
    tekelecstp 08-07-25 08:02:22 EST  EAGLE5 39.2.0
    APPL    SSN   STAT
    EIR     11    offline

    SS-APPL TABLE IS 25% FULL (1 OF 4)
;
```

2. Change the EIR subsystem status to online.

   `chg-ss-appl:appl=eir:nstat=online`

3. Enter the command to allow the EIR subsystem to begin operation.

```
alw-map-ss:ssn=<EIR ssn>

        integrat40 08-05-24 10:37:22 EST  EAGLE5 39.2.0
        Allow map subsystem command sent to all SCCP cards.
        Command Completed.
    ;
```

4. Display and verify the operating status of the EIR subsystem, by entering the rept-stat-sccp command.

5
Maintenance

This chapter describes commands and reports that can be used for EIR maintenance, including status reporting and problem identification.

EIR Alarms

EIR UAMs

#unique_68/unique_68_Connect_42_V5554906 lists the UAMs that specifically support the EIR feature. All EIR-related UAMs are generated to the Maintenance Output Group.

Refer to *Unsolicited Alarm and Information Messages Reference* for complete descriptions and corrective procedures for all UAMs.

Refer to *Alarms and Maintenance Guide* for EPAP for the descriptions and corrective procedures for MPS-related alarms.

UAM ID	Severity	Message Text
0455	Critical	EIR Subsystem is not available
0456	Critical	EIR Subsystem is disabled
0457	Minor	EIR Subsystem normal, card(s) abnormal
0458	None	EIR Subsystem is available
0459	None	EIR Subsystem is removed
0483	Critical	DEIR System is not available
0484	Major	DEIR System normal, card(s) abnormal
0485	Normal	DEIR System is available
0486	Minor	DEIR Threshold -Level1 exceeded
0487	Major	DEIR Threshold -Level2 exceeded
0488	Normal	DEIR Threshold Condition Cleared
0489	Critical	DEIR capacity exceeded
0490	Normal	DEIR normal
0491	Major	Connection TPS exceed
0492	Normal	Connection TPS normal
0493	Major	Diameter Connection Down
0494	Normal	Diameter Connection UP
0495	Normal	Diameter Connection Closed
0496	Normal	DEIR System is removed

EIR UIMs

EIR UIMs

lists the UIMs that specifically support the EIR feature. Refer to *Unsolicited Alarm and Information Messages Reference* for complete descriptions of all UIM text, formats, and recovery procedures.

UIM	Text	Description	Recovery
1030	Inh EIR SS request already outstanding	An `inh-map-ss` command is already entered and queued.	None
1031	Failure Inhibiting EIR **SS**	The `inh-map-ss` command was unsuccessful in taking the EIR subsystem off-line.	Enter the `inh-map-ss` command with the `force` parameter.
1102	Invalid Length for Map IMEI Parameter	The EIR subsystem received a Check-**IMEI** message in which the Map IMEI parameter had an invalid length.	None
1103	**LSS**:No Map IMEI Parameter present	The EIR subsystem received a Check-IMEI message in which the Map IMEI parameter is not present	None
1306	GSMOPTS: EIR Global Response is ON	The EIR Global Response Type is on. The EIR Global Response Type is set by the `chg-gsmopts` command and the `eirgrsp` parameter.	For information about `eirgrsp`, refer to the `chg-gsmopts` command in *Commands User's Guide*
1307	GSMOPTS: EIR Global Response is OFF	The EIR Global Response Type is off. The EIR Global Response Type is set by the `chg-gsmopts` command and the `eirgrsp` parameter.	For information about `eirgrsp`, refer to the `chg-gsmopts` command in *Commands User's Guide*.
1133	Diameter msg decode failed	Diameter message parsing FAILS. Examples: • ECR Message does not have IMEI AVP or value in IMEI AVP. • CER Message does not have mandatory AVP present. • DPR message received does not have disconnect cause AVP present. Output Group: LINK	
1134	Diameter msg encode failed	Diameter message Encoding FAILS. Output Group: LINK	
1135	Invalid Diameter Msg received	Diameter message was received which is not supported in the EAGLE or an error exists in Diameter message header. Output Group: LINK	
1136	Invalid Diameter Msg length	Total Diameter message length specified in diameter header does not match with the actual diameter message length. Output Group: LINK	
1137	Diameter AVP Decode Fail	AVP decoding failed. Output Group: LINK	

UIM	Text	Description	Recovery
1138	Connection Refused	• Origin host and Origin Realm AVPs in CER message does not match with the host and realm values provisioned in the IPAPSOCK table. • Source IP Address of the CER message does not match with the IP Address present in the Host-IP-Address AVP. Error Cause: • Origin Host Mismatch • Origin Realm Mismatch • IP Address Mismatch • No common application Output Group: LINK	
1139	DEIR Global Response is ON	DEIR Global Response is set to Allowlist/Graylist/Blocklist/Unknown from OFF in DEIROPTS table. Output Group: APSS	
1140	DEIR Global Response is OFF	DEIR Global Response is set to OFF from Allowlist/Graylist/Blocklist/Unknown in DEIROPTS table. Output Group: APSS	

UIM Format for EIR S13/S13' Support Feature

The UIMs added for the EIR S13/S13' Interface Support feature are displayed in the format shown in . The maximum length of origin host/ origin realm/AVP code and error to be displayed in the UIM is 32 bytes.

UIM format for EIR S13/S13' Support Feature

Literal	RPT_DEIR_MSG (I-85)

UIM format for EIR S13/S13' Support Feature

Format

```
            1         2         3         4         5
6         7         8
123456789012345678901234567890123456789012345678901
2345678901234567890
    xxxx.xxxx    CARD cccc,ppp INFO    'text'
                 DCNAME= xxxxxxxxxxxxxx
                 Command Code = xxxx
                 Error Cause=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx


            1         2         3         4         5
6         7         8
123456789012345678901234567890123456789012345678901
2345678901234567890
    xxxx.xxxx    CARD cccc,ppp INFO    'text'
                 DCNAME= xxxxxxxxxxxxxx
                 Command Code = xxxx
                 Origin Realm=
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
                 Error Cause=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx



            1         2         3         4         5
6         7         8
123456789012345678901234567890123456789012345678901
2345678901234567890
    xxxx.xxxx    CARD cccc,ppp INFO    'text'
                 DCNAME= xxxxxxxxxxxxxx
                 Command Code = xxxx
                 Origin Host=
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
                 Error Cause=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

UIM format for EIR S13/S13' Support Feature

Output Examples

```
                        1           2           3           4           5
        6           7           8
        123456789012345678901234567890123456789012345678901234567890
        2345678901234567890
            0014.1133    CARD 1103,B   INFO     Diameter msg decode
        failed
                        DCNAME= Con1
                        Command Code = 324
                        Error Cause= Unsupported appl id

                        Report Date:10-10-12  Time:16:20:19


                        1           2           3           4           5
        6           7           8
        123456789012345678901234567890123456789012345678901234567890
        2345678901234567890
            0014.1138    CARD 1103,B   INFO      Connection Refused
                        DCNAME= Con3
                        Command Code = 324 (R)
                        IP Address=10.248.4.5
                        Error Cause= IP Addr Mismatch

                        Report Date:03-22-13  Time:16:20:19
```

Maintenance Commands

The following commands can be used for maintenance when an EPAP-related feature is on.

Refer to *Commands User's Guide* for complete descriptions of the commands, including parameters, valid parameter values, rules for using the commands, and output examples.

Table 5-1   Maintenance Commands

Command	Description
rept-stat-sys	Reports the status of system entities, including cards. The output includes the number of Service Module cards that are in service (IS-NR) and how many are in another state (IS-ANR, OOS-MT, OOS-MT-DSBLD).
rept-stat-sccp	Reports operating status of services and subsystems, CPU usage, and Service Module card status. When the `loc` parameter is specified, the command displays detailed card traffic statistics, including cards that are denied SCCP service. See the section in this manual that describes the use of the `rept-stat-sccp` command.
rept-stat-mps	Displays the overall status of the EPAP application running on the MPS (multi-purpose server). Command output for the various reports of this command include overall MPS alarm status and card status, and status for a specific Service Module card when a feature is on.
rept-stat-trbl	Includes a summary of any trouble notifications (**UAM**s) for local subsystems, cards, and linksets. The severity of each alarm is indicated in the output report.

Table 5-1   (Cont.) Maintenance Commands

Command	Description
rept-stat-alm	Displays the alarm counts and totals for local subsystems and Service Module card/EPAP IP links.
rept-stat-db	Displays the status information for the EAGLE databases. This includes the level information for each Service Module card, and for the active and standby EPAP RTDB. The command reports database exception status such as corrupted, incoherent, or inconsistent, as well as providing the birth dates and levels. It shows the status of each PDB and RTDB when an EPAP-related feature is enabled.
rtrv-tbl capacity	Retrieves table use capacity summary information. For each table listed, the number of table entry elements in use and the total allowed number of table elements is presented, along with a percent (%) full value. Information is shown for some tables only if the feature that uses the table is enabled.
inh-card/alw-card	The `inh-card` command is used to change the operating state of the card from In-Service Normal (IS-NR) to Out-of-Service Maintenance-Disabled (OOS-MT-DSBLD). A craftsperson then can test the card or physically remove it from the shelf. The `alw-card` command is used to change the card from OOS-MT-DSBLD (Out-of-Service Maintenance-Disabled) to IS-NR (In-Service Normal) if card loading is successful.
inh-alm/unhb-alm	Used to allow and inhibit reporting of alarms for a given device, including the Service Module card ports. The commands allow both Port A and Port B to be specified. Inhibited alarms will not generate UAMs or cause alarm indicators to be turned on. All `rept-stat-xxx` commands continue to display the alarms with an indication that the device has its alarms inhibited.
rtrv-data-rtdb	Retrieves Entity data, DN data, IMEI data, IMSI data, TN data, NPANXX data, and LRN data from the RTDB on an active Service Module card. If the `loc` parameter is specified and the target card is an active Service Module card, the RTDB data is retrieved from that card. If the `loc` parameter is not specified, the RTDB data is retrieved on the active Service Module card that has the lowest IMT address. The RTDB status on the active Service Module card can be coherent or incoherent.

rept-stat-sccp

The `rept-stat-sccp` command provides statistics for Service Module cards and for the services that execute on the cards. The statistics can be displayed for all Service Module cards, or for a specified card.

Refer to *Commands User's Guide* for a description of the `rept-stat-sccp` command, including parameter names, valid parameter values, examples, and dependencies for the command.

EIR Feature Statistics

The `rept-stat-sccp` command counts and displays the following statistics when the EIR feature is enabled and turned on (WARNINGS and FORWARD TO GTT are not reported for EIR):

• TOTAL = the total number of messages that contain a CheckIMEI MAP Operation.

• SUCCESS = the number of messages that passed CheckIMEI processing

- ERRORS = the number of messages that were not counted in SUCCESS.

EAGLE Debug Commands

Commands User's Guide contains descriptions of debug commands that can be used in assessing and modifying system status and operation. Most of the debug commands are used only under the direction of Oracle support personnel.

Refer to *Commands User's Guide* for a complete description of the debug commands, including the `ent-trace` command.

The `ent-trace` command can be used for EIR to provide a trap-and-trace function for MSUs on the Service Module cards.

- Trap Message will be performed on a Query message with:
  - A decode error, and Trace-On-Error set
  - IMEI match
  - IMSI match
  - SSP
  - GT
- Because the Response message will not contain the IMEI or IMSI information, it will be trapped if the Query message was trapped.

> ⚠ **Caution**
>
> This command can cause OAM to reset if too many MSUs are trapped.

A trace must be set on all Service Module cards; specify the `card=sccp-all` parameter. Use a repetition parameter (`rep`) to control the number of MSUs that are trapped.

The 14-digit IMEI is a trapping field. MSUs are trapped only when the SDS count (REP) is positive. If a Query and Response are both trapped, that is 2 SDS counts.

MSUs that satisfy any trigger criteria are trapped on the Service Module card, forwarded to OAM, and displayed.

Status Reporting and Problem Identification

EAGLE commands can be used to obtain status and statistics for the EAGLE system, the EPAP systems, system devices including Service Module cards, EPAP-related features, local subsystems, and SCCP services.

Refer to *Commands User's Guide* for complete descriptions of the commands, including parameters and valid values, rules for using the commands correctly, and output examples.

Refer to *Unsolicited Alarm and Information Messages Reference* for descriptions and recovery procedures for UAMs and UIMs.

Refer to *Administration Guide* for EPAP for descriptions of EPAP functions and operation.

Refer to *Alarms and Maintenance Guide* for descriptions and recovery procedures for EPAP alarms.

Refer to the appropriate feature User's Guide for information about the functions and operation of EPAP-related features.

Table 5-2   Status Reporting for EPAP-Related Features

Reports, Status, and Statistics	Command
EAGLE	
Maintenance Status Report - indicates whether Maintenance, Routing, and SCCP Baselines have been established.	`rept-stat-sys`
Alarms and operating state for system devices, including Service Module ("SCCP") cards.	`rept-stat-sys`
Unsolicited Alarm Messages (UAMs) and Unsolicited Information Messages (UIMs)	`rept-stat-alm` `rept-stat-trbl`
EPAP/MPS (from the EAGLE)	
EPAP code version and operating state for each EPAP.	`rept-stat-mps`
MPS hexadecimal alarm strings for the active and standby EPAPs.	`rept-stat-mps`
Operating state and alarm status of equipped Service Module cards and their DSM ports and IP connections.	`rept-stat-mps` `rept-stat-mps:loc=<Service Module card location>`
Amount of memory used by the RTDB on the specified card, as a percent of available Service Module card memory.	`rept-stat-mps:loc=<Service Module card location>`
EPAP Provisioning Database (PDB), EPAP Real Time Database (RTDB), and Service Module card RTDB status information - Coherent, birthdate (date and time of creation), and exception (condition when a problem was detected).	`rept-stat-db` `rept-stat-db:db=mps`
Service Module Cards, EPAP-Related Features, Services, Local Subsystems	
Status of the Service Module cards, and the services executing on the cards for EPAP-related features that are turned on. Includes Service Report, Subsystem Report, and Alarm Status; Total Service Statistics.	`rept-stat-sccp`
Operating state and alarm status of equipped Service Module cards and their DSM ports and IP connections; EPAP-related feature status per card.	`rept-stat-mps:loc=<Service Module card location>`
Alarms and operating state for Service Module ("SCCP") cards.	`rept-stat-sys` `rept-stat-mps`
Any cards that are denied SCCP service.	`rept-stat-sccp`
Detailed view of the status of SCCP services provided by the specified Service Module card. Includes Card Alarm Status, Card Service Statistics	`rept-stat-sccp:loc=<Service Module card location>`
General SCCP traffic performance for Service Module cards. Message rates for TVG performance.	`rept-stat-sccp:mode=perf`
Statistics for EPAP-related feature local subsystems - Subsystem Report	`rept-stat-sccp`

Table 5-2   (Cont.) Status Reporting for EPAP-Related Features

Reports, Status, and Statistics	Command
Statistics for EPAP-related features	`rept-stat-sccp`

EPAP Status and Alarm Reporting

Because EPAP has no direct means of accepting user input or displaying output messages on EAGLE terminals, EPAP maintenance, measurements, and status information are routed through a Service Module card. EPAP sends two types of messages to the Service Module card: EPAP Maintenance Blocks and DSM Status Requests and DSM Status Messages. Each message type is discussed in the following sections.

EPAP Maintenance Blocks

The EPAP forwards all status and error messages to the Service Module cards in maintenance blocks. Maintenance blocks are asynchronously sent whenever the EPAP has something to report. The status information that is displayed when a `rept-stat-mps` command is issued includes information that came from the maintenance blocks.

The active EPAP generates and sends maintenance blocks to the primary Service Module card. One maintenance block is sent as soon as the IP link is established between the active EPAP and the primary Service Module card. Additional maintenance blocks are sent whenever the EPAP needs to report any change in status or error conditions. The information returned in maintenance blocks is included in the output of the `rept-stat-mps` and `rept-stat-sccp` commands.

The EPAP sends maintenance blocks that contain at least the following information:

- Status of EPAP A - actual states are active, standby, and down (inoperative). Maintenance blocks include a field for this information so that it can be available for the output of the `rept-stat-mps` command.

- Status of EPAP B - actual states are active, standby, and down (inoperative). Maintenance blocks include a field for this information so that it can be available for the output of the `rept-stat-mps` command.

- Identification of Active EPAP - a field to identify the active EPAP.

- Congestion Indicator - an indicator showing provisioning link congestion. The link between the EPAPs and the external source of provisioning data can become congested in high-provisioning traffic situations. When this occurs and subsequently as the congestion clears, the EPAP sends maintenance blocks to the Service Module card.

- Alarm Conditions - an error code field. If the EPAP needs to report an alarm condition, it puts an appropriate UAM identifier in this field.

- Current MPS Database Size - a field indicating the current RTDB size. The Service Module card uses this information to calculate the percentage of memory used by the RTDB.

DSM Status Requests and DSM Status Messages

When the EPAP needs to know the status of a Service Module card, the EPAP sends a DSM Status Request to all Service Module cards, and each Service Module card returns its status to the EPAP.

Service Module cards send a DSM Status Message to the EPAP when any the following events occur in the Service Module card:

- The Service Module card is booted.

- The Service Module card receives a DSM Status Request message from the EPAP.

- The Service Module card determines that it needs to download the entire RTDB; for example, the Service Module card determines that the RTDB needs to be downloaded because it is totally corrupted, or a user requests that the RTDB be reloaded. The Service Module card sends a Full Download Request message to the EPAP

- The Service Module card starts receiving RTDB downloads or updates. When a Service Module card starts downloading the RTDB or accepting updates, the Service Module card sends a DSM Status Message informing the EPAP of the first record received. This helps the EPAP keep track of downloads in progress.

The DSM Status Message provides the following information to the EPAP:

- **DSM Memory Size**. When the Service Module card is initialized, it determines the amount of memory present. The EPAP uses the value to determine if the Service Module card has enough memory to hold the RTDB.

- **Load Mode Status**. This indicator indicates whether or not a sufficient number of the IS-NR (In-Service Normal) LIMs have access to SCCP services.

Thermal Management Parameters

The DEIR card supports thermal monitoring to protect the temperature-sensitive hardware components. The processor on this card can overheat as a result of high ambient temperature or airflow blockage. If the junction temperature goes above operating limits i.e. 95%, the CPU halts and the card shuts itself down to prevent permanent, catastrophic damage. In the event of thermal shutdown, all processor activity ceases.

To minimize data loss due to overheating, a graceful shutdown is implemented to detect and alert the user to the increasing thermal conditions. When the CPU temperature rises above nominal range and exceeds a thermal threshold (thermal level 1), a major alarm is raised against the card. If the temperature continues to increase and exceeds a second thermal threshold (thermal level 2), a critical alarm is raised against the card and it stops processing of traffic. When this second thermal event occurs, the application is notified from the OS. The state of card will transition to 'IN-ANR Restricted' state.

Once the temperature recedes under the Temperature Level 2 threshold, the raised critical alarm will be cleared and the corresponding major alarm will be raised. When the temperature returns to its nominal range (below Temperature Level 1) a clearing alarm will be raised for the card and the card starts traffic processing. These thermal thresholds (Temperature Level 1 and Temperature Level 2) are user configurable. For more information on setting thermal thresholds see the CHG-TH-ALM command

Table 5-3   Thermal Management Parameters

Board Temperature	Actions / Clearing Condition	UAM
Temp Level 1 Exceeded on DEIR card; major	Major alarm UAM 0078 raised on DEIR card State of DEIR card shall transition from IS-NR to IS-ANR / Restricted	0078 ("Card temperature exceeds nominal lvl:T1")
Temp Level 2 Exceeded on DEIR card; critical	Critical alarm UAM 0077 raised on DEIR card; State of DEIR card shall transition to IS-ANR / Restricted	0077 ("Card temperature is at critical lvl:T2")

Table 5-3   (Cont.) Thermal Management Parameters

Board Temperature	Actions / Clearing Condition	UAM
Temperature abated (cooling below Temp Level 2 but at level 1)	Major alarm UAM 0078 raised on DEIR card; State of DEIR card shall transition to IS-ANR / Restricted	0078 ("Card temperature exceeds nominal lvl:T1")
Temperature abated (cooling below Temp Level 1)	Major alarm UAM 0078 cleared.	0079 ("Card temperature again at nominal level")

6
EIR Measurements

This chapter describes measurements that can be collected and generated for the EIR feature.

EIR Measurements

The EAGLE Measurements system supports the collection and retrieval of measurements related to the EIR feature. The EIR measurements can be collected and reported with either of the following collection methods:

- The Measurements Platform feature enabled and the Measurements Platform collection option on
- The E5-OAM Integrated Measurements feature enabled and on and the E5-OAM Integrated Measurements collection option on

15 Minute Measurements collection can be used with Measurements Platform or E5-OAM Integrated Measurements.

OAM-based measurements collection is not available for EIR.

The EAGLE Measurements system supports the collection and retrieval of measurements related to the EIR feature. The EIR measurement registers are supported only with the Measurements Platform feature enabled and the Measurements Platform collection option on.

Refer to *Measurements Reference* for descriptions of collection methods, measurements, and measurements reports.

Refer to *Commands User's Guide* for descriptions of the commands used to enable and turn on features, turn on measurements collection options, and schedule and generate measurements reports.

Refer to the procedures in *Database Administration - System Management User's Guide* to configure the Measurements Platform feature or E5-OAM Integrated Measurements feature and the EAGLE OA&M IP Security feature for use with EIR.

The EIR feature must be enabled to provision scheduling of the EIR measurements reports. The EIR feature must be turned on for full measurements collection functions to operate for the feature.

Table 6-1 describes eight measurement registers that are used specifically for the EIR feature. The registers are reported in two Per System reports for the EIR entity type: Hourly Maintenance Measurements (MTCHEIR) and Daily Maintenance Measurements (MTCDEIR). The data for these registers originates on the Service Module cards.

For IMEIs present in multiple lists, the appropriate measurement peg is determined by the logic in Table 2-2 and the outcome of the IMSI Check.

Table 6-1   Pegs for Per System EIR Measurements

Event Name	Description	Type	Unit
IMEIRCV	Total number of MAP_CHECK_IMEI messages received.	System	Peg count

Table 6-1 (Cont.) Pegs for Per System EIR Measurements

Event Name	Description	Type	Unit
WHITEIMEI	Total number of searches that resulted in a match with a "Allow Listed" IMEI.	System	Peg count
GRAYIMEI	Total number of searches that resulted in a match with a "Gray Listed" IMEI.	System	Peg count
BLACKIMEI	Total number of searches that resulted in a match with a "Block Listed" IMEI.	System	Peg count
BLKALIMEI	Total number of searches that resulted in a match with a "Block Listed" IMEI, but were allowed due to IMSI Check match.	System	Peg count
BLKNALIMEI	Total number of searches that resulted in a match with a "Block Listed" IMEI, and the IMSI in the database did not match the IMSI in the message.	System	Peg count
UNKNIMEI	Total number of searches that resulted in a match with an "unknown" IMEI.	System	Peg count
NOMTCHIMEI	Total number of searches that resulted in no match in the database.	System	Peg count

Measurement Registers for EIR S13/S13' Support Feature

Eight new measurement registers are added for the EIR S13/S13' Interface Support feature and are supported on a per Diameter connection basis. These new measurement registers listed in Table 6-2 are supported only with the Measurements Platform feature enabled and the Measurements Platform option on. The data for these registers originate from the S13 cards running DEIR64 GPL. The existing SCTPASSOC and SCTPCARD measurement registers are also supported by the DEIR64 GPL.

Table 6-2 EIR S13/S13' Interface Support Measurement Registers

Register	Description
ECRRCV	Total number of ME-Identity-Check requests (ECR) received by the EIR
WHITEIMEI	Total number of searches that resulted in a match with a *whitelisted* IMEI
GRAYIMEI	Total number of searches that resulted in a match with a *graylisted* IMEI
BLACKIMEI	Total number of searches that resulted in a match with a *blacklisted* IMEI
BLKALIMEI	Total number of searches that resulted in a match with a *blacklisted* IMEI, but were allowed due to IMSI Check match
BLKNALIMEI	Total number of searches that resulted in a match with a *blacklisted* IMEI, and the IMSI in the database did not match the IMSI in the message
UNKNIMEI	Total number of searches that resulted in a match with an Unknown IMEI
NOMTCHIMEI	Total number of searches that resulted in no match in the database

Measurement Reports for EIR S13/S13' Support Feature

The new measurement registers are reported in new DEIR SYS and DEIR DCONN measurement reports: Hourly Maintenance Measurements on S13 System (MTCHDEIR) and Daily Maintenance Measurements on S13 System (MTCDDEIR). The MTCHDEIR and MTCDDEIR reports are transferred to an FTP server.

Table 6-3   DEIR Measurement Reports

Report	Reporting modes	Period	Retention	Display	Reports supported on GPLs
DEIR SYS System Wide report Hourly (60 minute) and Daily (24 hour)	On-demand, Scheduled (MTCHDEIR / MTCDDEIR)	Hourly Daily	24 hours for Hourly data 7 days for Daily data	FTP	MCP / MCPHC / OAMHC
DEIR DCONN report Hourly (60 minute) and Daily (24 hour)	On-demand, Scheduled (MTCHDEIR / MTCDDEIR)	Hourly Daily	24 hours for Hourly data 7 days for Daily data	FTP	MCP / MCPHC / OAMHC