Oracle® Communications

EAGLE Stateful Applications User's Guide

Release 47.1
F88479-01
October 2023

Oracle Communications EAGLE Stateful Applications User's Guide, Release 47.1

F88479-01

Contents

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

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

Table Acronyms

Acronym	Description
EEDB	EAGLE External Database
GTT	Global Title Translation
IP	Intelligent Peripheral or Internet Protocol
SCP	Service Control Point
SLIC	Service and Link Interface Card
STP	Signal Transfer Point
UAM	Unsolicited Alarm Messages
UIM	Unsolicited Information Messages
VLR	Visitor Location Register

What's New in This Guide

This section introduces the documentation updates for Release 47.1 in Oracle Communications EAGLE Stateful Applications User's Guide.

Release 47.1 -F88479-01, October 2023

There are no updates in the document for this release.

1
Introduction

This chapter provides a brief description of the Stateful Applications 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.

1.1 Overview

This manual provides feature descriptions, along with commands, maintenance, measurements, and configuration details associated with the Stateful Applications feature of the Oracle Communications EAGLE. The Stateful Applications feature allows the Signal Transfer Point (STP) to validate the messages coming in for a subscriber roaming out by validating them against the Visitor Location Register (VLR) the subscriber was last seen by the Home Location Register (HLR). If the HLR provides a validity of the new VLR, the EAGLE will let the message into the network; if not, the message will be handled per configuration (either silent discard, fallback, or respond with error).

1.2 Scope and Audience

This manual is intended for anyone responsible for installing, maintaining, and using the Oracle Communications **EAGLE** Stateful Applications feature. Users of this manual must have a working knowledge of telecommunications and network installations.

1.3 References

For more information, refer to the following documents:

1. *Commands User's Guide*
2. *Database Administration - System Management User's Guide*
3. *Measurements Reference*
4. *Unsolicited Alarm and Information Messages Reference*

2
Feature Description

This chapter describes the Stateful Applications feature.

2.1 Introduction

SS7 Firewall - Stateful Applications allows the Signaling Transfer Point (STP) to validate the messages coming in for a subscriber roaming out by validating them against the Visitor Location Register (VLR) when the subscriber was last seen by the Home Location Register (HLR). Once the HLR provides a validity of the new VLR, the EAGLE lets the message into the network. If the message is not validated, it is handled per configuration (either silent discard, fallback, or respond with error).

The message forwarding from LIM to SFAPP cards will only work with IPSG+GTT SLIC cards. For all other LIM cards, messages will be forwarded to the SCCP cards, which will then forward the message to the SFAPP SLIC cards.

2.2 Supported MAP Operations

The following MAP Operations are supported by the Stateful Applications feature.

Table 2-1 Supported MAP Operations

MAP Operation	OpCode	Application Context (AC)	AC Code
sendParameters	9	infoRetrieval /v1	14
Registers	10	networkFunctionalSs	18
Erases	11	networkFunctionalSs	18
Activates	12	networkFunctionalSs	18
deactivates	13	networkFunctionalSs	18
interrogates	14	networkFunctionalSs	18
authenticationFailureReport	15	authenticationFailureReport /v3	39
registerPassword	17	networkFunctionalSs	18
processUnstructuredSS-Data	19	networkFunctionalSs /v1	18
mo-forwardSM	46	shortMsgMO-Relay	21
noteSubscriberPresent	48	mwdMngt/v1	24
beginSubscriberActivity	54	networkFunctionalSs /V 1	18
restoreData	57	networkLocUp/v2	1
processUnstructuredSS-Request	59	networkUnstructuredSs v2	19
readyForSM	66	mwdMngt /v2/v3	24
purgeMS	67	istAlerting /v2/v3	4

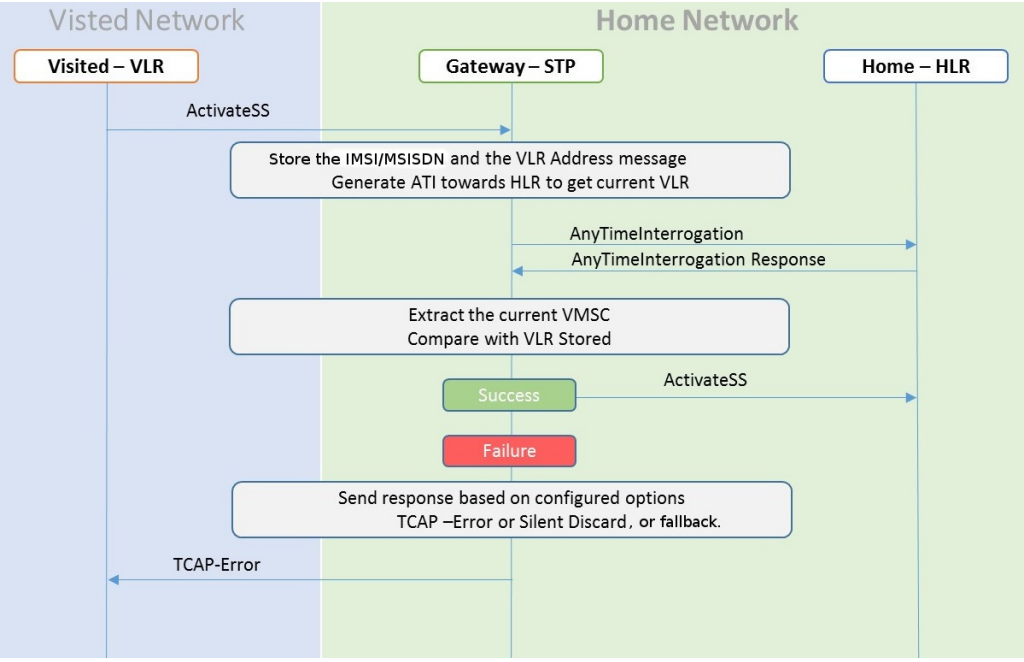
Table 2-1 (Cont.) Supported MAP Operations

MAP Operation	OpCode	Application Context (AC)	AC Code
purgeMS	67	msPurging /v3	27
ss-Invocation-Notification	72	ss-InvocationNotification	36
statusReport	74	reporting	7
istAlert	87	istAlerting /v3	4
NoteMM-Event	89	mm-EventReporting	42
updateLocation	2	networkLocUp	1
updateGprsLocation	23	gprsLocationUpdate/v3	32
sendAuthenticationInfo	56	infoRetrieval /v2/v3	14

2.3 VLR Validation

As seen in the following figure, VLR Validation uses the information stored in the HLR about the current VLR to validate the VLR from which the message is received.

Figure 2-1 Call Flow for VLR Validation



1. The incoming message will be decoded.
   a. An Error will be generated in case of decode failure.
2. The message information will be stored in the local database.
3. The Any Time Interrogation (ATI) request will be generated towards the HLR.

a. The ATI Request will be coded so that Acknowledgment is received on the same SLIC card, as the DB is local.

4. For a successful response from the HLR:
   a. The ATI Response will be decoded to get the current VLR address.
   b. The current VLR address will be compared with the CgPA stored in the local database for the subscriber.
   c. On a successful Match, the message will be routed as per the GTT result.
   d. In case of failure,
      i. Send the configured response.
      ii. Increment the measurement for failed messages.

The ATI sent to HLR must be formatted as follows:

1. MTP OPC=EAGLE SID, MTP DPC = HLR PC
2. SCCP CGPA (RI = SSN, PC = EAGLE SID, SSN = <SSFAPP SSN>, SCCP CDPA (received message CDPA)
3. TCAP BEGIN with valid MAP dialogue portion (as per MAP specification)
4. TCAP DTID = unique OTID generated for each ATI (The DTID will not be reused within 5 seconds)
5. ATI details: IMSI = IMSI/MSISDN received in received message, and other mandatory parameters

The EAGLE will validate the ATI_ACK received from the HLR. A valid ATI_ACK message is defined as:

1. It is a well formatted ANSI or ITU SCCP UDT, non-segmented XUDT message, with a valid TCAP END message, with valid dialogue portion, and single component in the component portion as return result with operation code = ATI_ACK
2. Value of DTID received in TCAP END matches with one of the ongoing transactions
3. Component type is a return result and contains ATI_ACK
4. VMSC digits are received in ATI_ACK

2.4 Velocity Check Using ATI

As seen in the following figure, Velocity Check using ATI uses the information stored in the HLR about the current VLR and the age of location parameter to identify if the new VLR is reachable from the current VLR stored in HLR.

This use case is dependent on the validity of the information stored in the VLR and the T3212 timer (periodic update location timer). This timer governs the rate at which the mobile subscriber autonomously updates their location. In case the time distance between two networks is less than the value of T3212 timer configured for the network, this use case test would provide false positives since the location age information would not have been properly updated in the VLR.

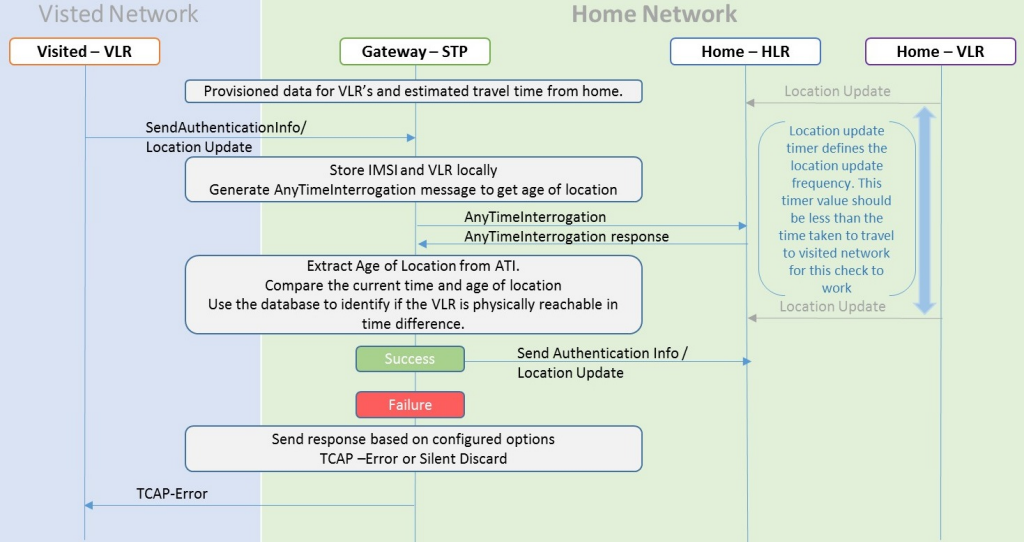
The assumption for successful execution of this use case are:

1. The First location update can be identified using the IMSI only in the address.
2. The Age of Location provided by HLR is accurate.

3. The quantum of information (Age of Location) will not be less than the time to get travel.

The ATI-based check can be completed in a reasonable amount of time for Location Update to succeed.

Figure 2-2 Call Flow for Velocity Check Using ATI



1. A local database on EAGLE will be configured to identify the network locations (using country codes for VLR addresses) and the shortest amount of time it may take to travel between them.
2. The incoming message will be decoded:
   a. An Error will be generated in case of decode failure.
   b. A Measurement will be pegged for the decode failure with OpCode and CgPA.
3. The message information will be stored in the local database.
4. The ATI request will be generated toward the HLR identified in the CdPA of the incoming message. The ATI request will be coded so that it is received on the same SLIC card, as DB is local.
5. In case the HLR sends a failure in the ATI response:
   a. A measurement will be pegged to identify HLR error corresponding message from CgPA (VLR).
6. For a success response, extract the Age of Location from the ATI Response message and the VMSC address in the HLR.
7. In case the VLR, from which the SAI/LU was received, matches the VLR in the ATI response, don't do anything.
8. In case the VLR addresses do not match:
   a. Calculate the time difference between the current time and the Age of Location.
   b. Verify the age of location is less than the travel time configured in the local Database.

c. In case of time value not within limits:
   i. A measurement will be pegged.
   ii. Response will be generated based on the configured option.

2.4.1 Velocity Check Flow Charts

The following flow charts provide an overview of the Velocity Check feature for Stateful Applications:

Figure 2-3 SFAPP Process Message

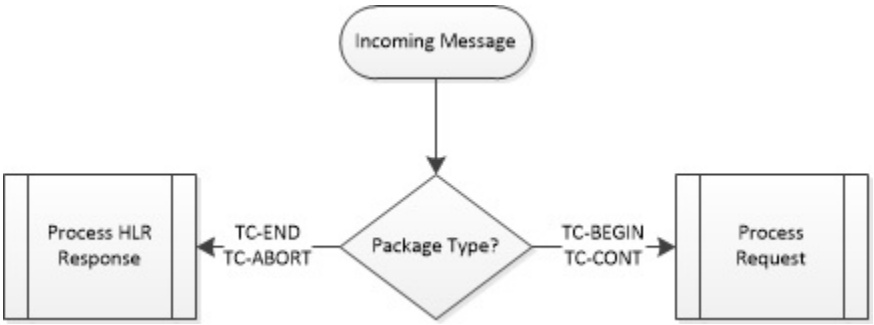


Figure 2-4 SFAPP Process Request

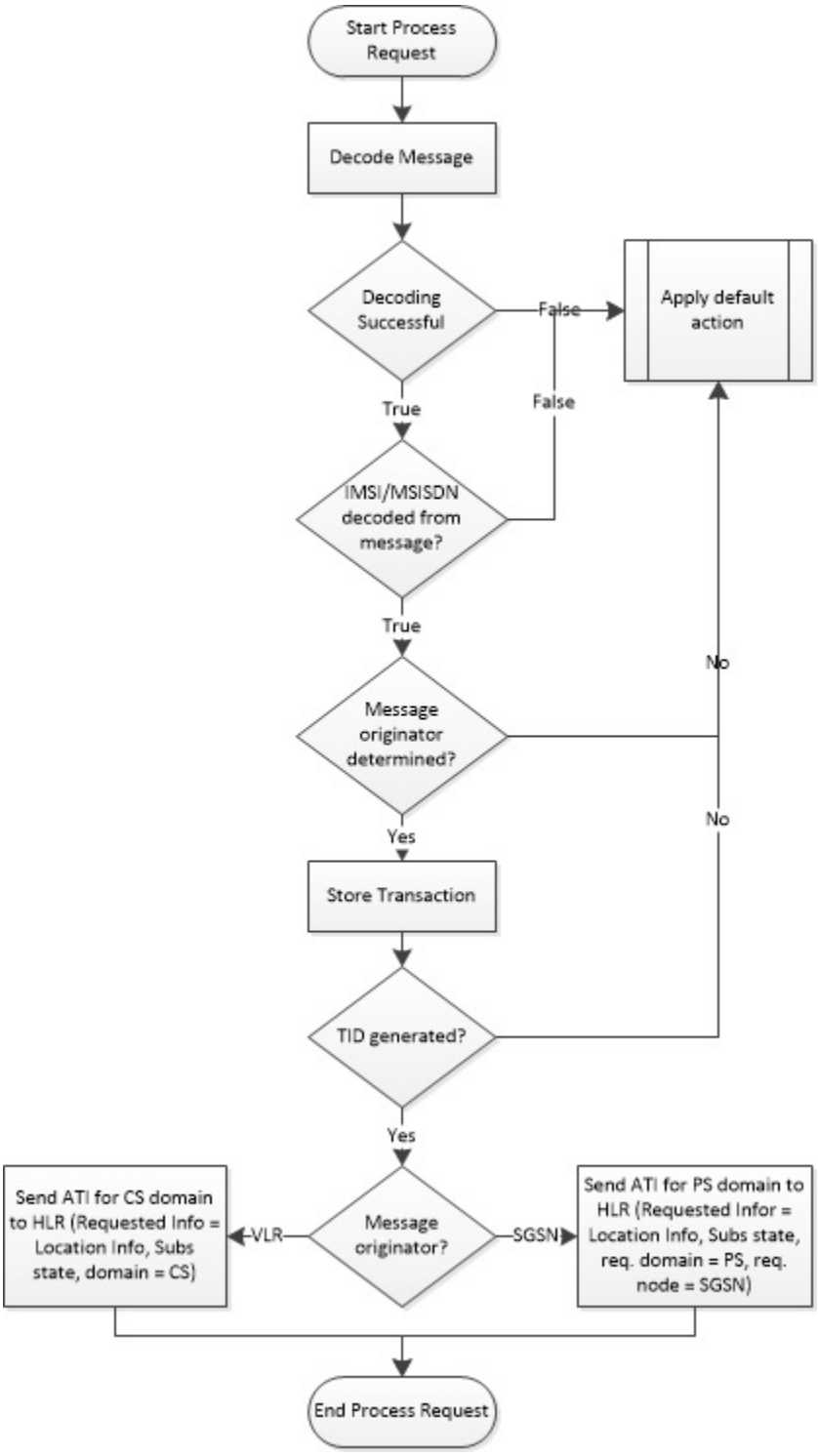


Figure 2-5 SFAPP Process HLR Response

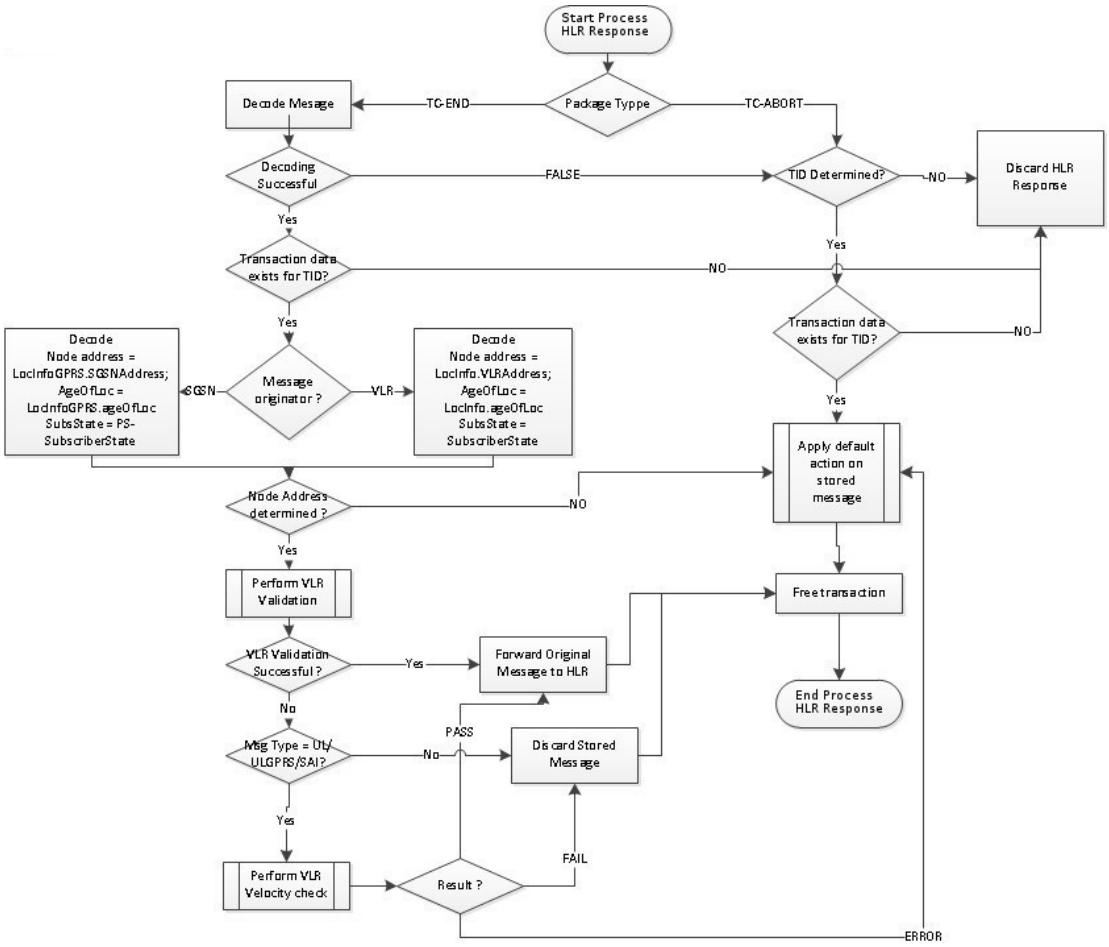
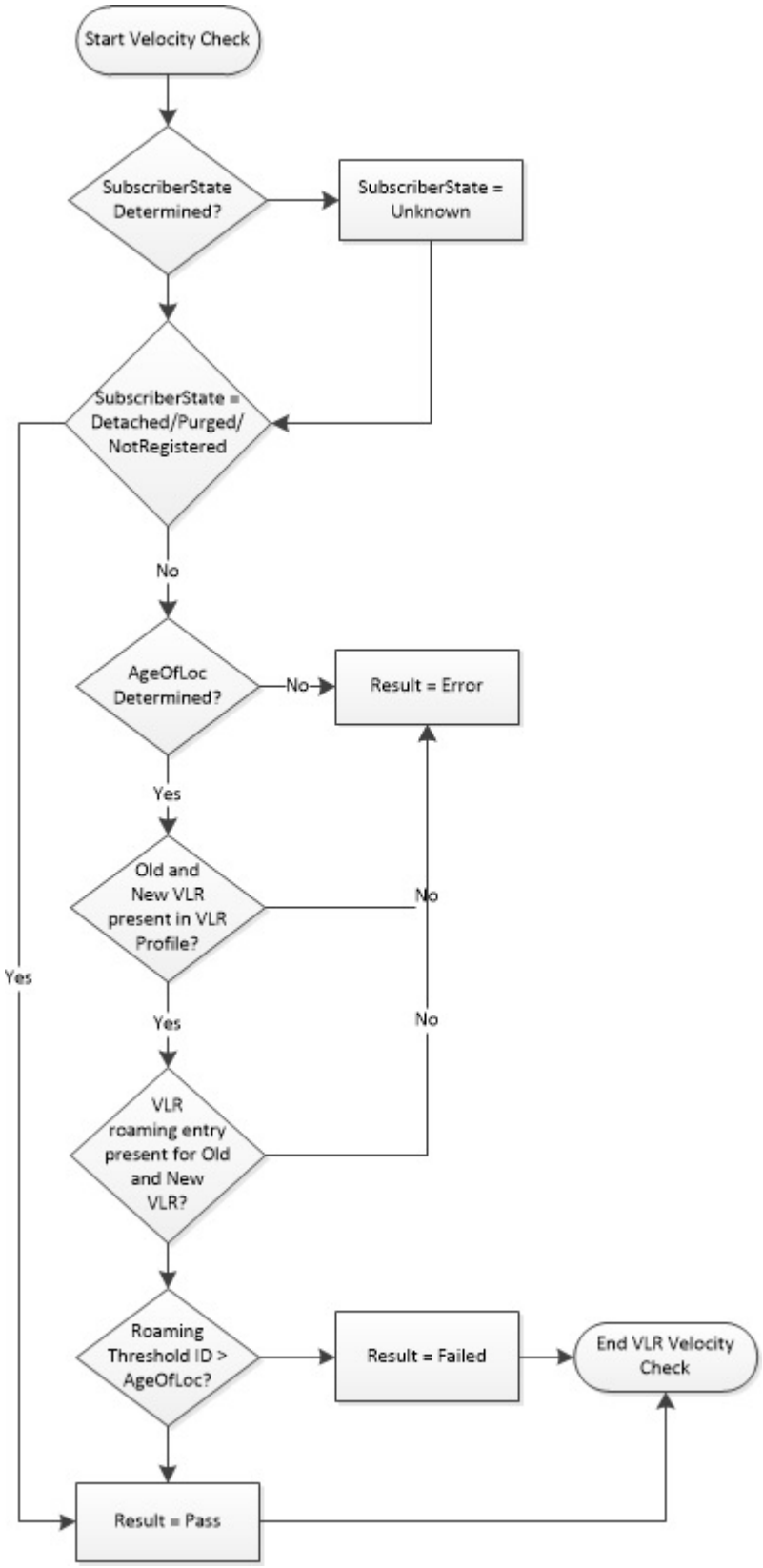


Figure 2-6 Perform VLR Velocity Check



2.5 Graylisted VLR Validation Using IMEI

Graylisted VLR Validation Using IMEI challenges the VLR after the Update Location procedure is completed by asking for the IMEI information in the provide subscriber information message.

This use case addresses these MAP 3.2 messages:

- Update Location/GPRS Update Location - VLR or the SGSN initiates the MAP send authentication information procedure to retrieve authenticated information from the HLR.
- Provide Subscriber Info - This message is sent by EAGLE to the VLR or SGSN to retrieve the subscriber state, location information and, in this case, IMEI.
- Provide Subscriber Info ACK - This message is sent from VLR or SGSN to the EAGLE as an acknowledgement to the PSI.
- AnyTime Interrogation – This message is sent as part of use cases 1 and 2.
- Purge MS - If a roaming subscriber is suspected as a malicious or fake user, EAGLE generates this message to HLR. Upon receiving this message, HLR marks the subscriber unreachable.

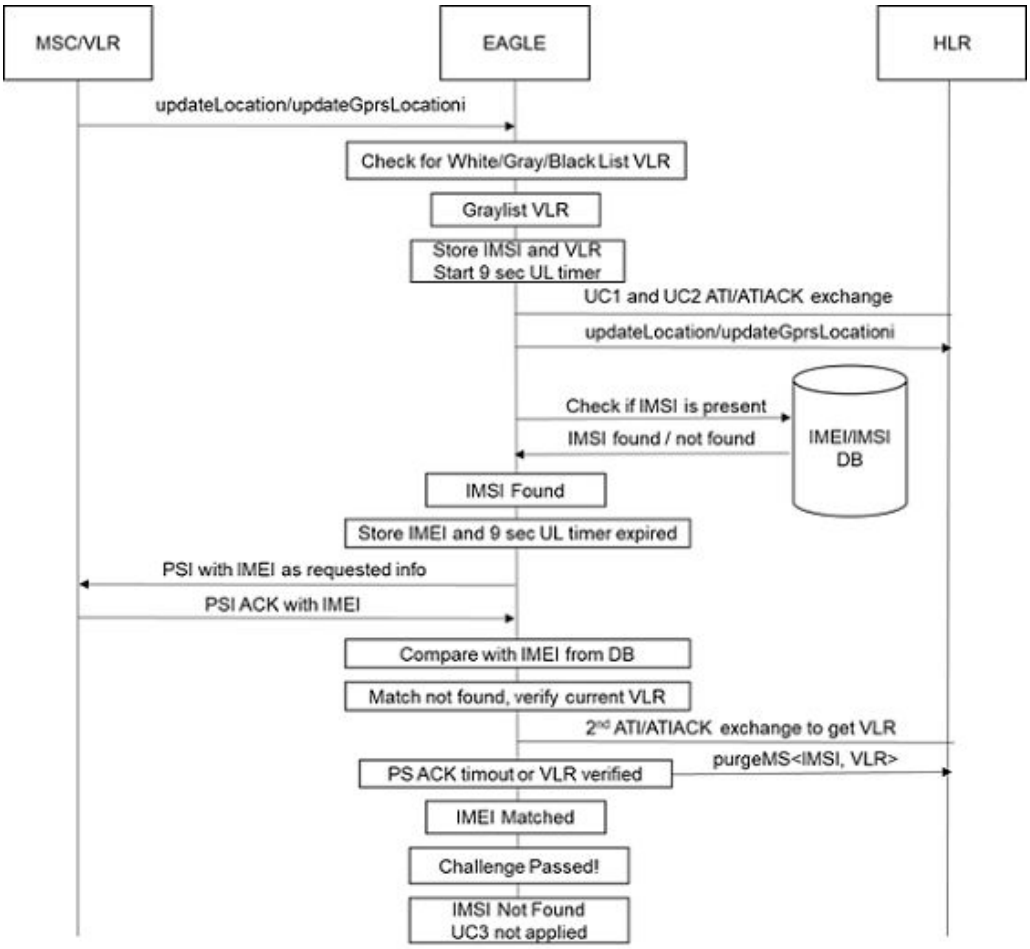
2.5.1 Graylisted VLR Validation Flow Chart

This use case challenges the visited VLR after the procedure for location update has been completed by asking for the subscriber's IMEI information in a PSI message. After that, one of these actions is taken:

1. The IMEI information can then be compared against an external database to validate the IMEI and consequently the VLR by either allowing the original procedure to complete or fail it by initiating in a Purge MS operation, or
2. The IMEI information can be added to/updated in the external database if the VLR is trusted and the IMEI is validated.

Figure 2-7 shows the call flow.

Figure 2-7 Graylisted VLR Challenge



1. Incoming UL message on the LIM card, either from the VLR or SGSN, is forwarded to the SCCP card by GT routing using GTT action for SFAPP. The SCCP card uses GTT based on SFAPP action to forward the message to the SFAPP card.
2. UL message is decoded on the SFAPP card. An error is generated in case of decoding failure. Details of the decoding failure errors are described in Decoding Errors Generated EAGLE.
3. The VLR address is checked to see if it is white/gray/blacklisted in the VLR database on the card. If graylisted, IMSI and the VLR address information is stored in a local data structure for further challenging the visited VLR with IMEI information for the mobile subscriber.
4. After extracting the IMSI and VLR address, the UL message is forwarded to the CdPA(HLR).
5. UL timer of 9 seconds timeout value is started to wait for update location procedure to complete on the mobile subscriber by the visited VLR to HLR. At the expiry of the UL timer, IMEI challenge begins.
6. The IMEI information for the subscriber is retrieved from the EEDB, if present. If not found, use case 3 is terminated and no further action is taken.

7. If found, the IMEI is stored and a PSI message is encoded by EAGLE with the IMSI and VLR from the original UL message and sent to the visited VLR. The SCCP portion of the PSI message is encoded to route on SSN SFAPP. CgPA from the original UL message is copied as the CdPA. CGPA is created from the `psirescgmodid` parameter of `ent-gtmod` command. TCAP layer of the PSI message is filled with the PSI opcode and IMSI tag/length/value, and requested information in the component portion is updated with IMEI tag/length fields. Transaction ID for an outgoing PSI message is encoded as described in Routing of PSI Response Back to Originating SFAPP Card.
8. Encoded PSI message is routed on SSN SFAPP to the SCCP card and is further GTT routed on to the visited VLR by the LIM card. A transaction timer of 4 seconds timeout (with a unique `transaction_id`) is started to track the PSI message sent. If the timer expires, the challenge is considered to have failed and a purgeMS is generated as described in 13.
9. When a PSI ACK arrives at EAGLE, upon arrival of the MSU at the SCCP card, if the `mate_id` in the TCAP transaction ID matches with the stored `STP_ID` of EAGLE, PSI ACK is sent to the SFAPP card. The details of the implementation of this functionality on the SCCP card is discussed in Routing of PSI Response Back to Originating SFAPP Card.
10. FAILACTID is enforced on the SFAPP card for the IMEI challenge just like in the case of velocity check challenge. If the IMEI decoded from the PSI_ACK does not match the IMEI retrieved from the EEDB and the VLR is graylisted, the provisioned FAILACTID is enforced.
    a. If the FAILACTID is FALLBACK, then the PSI_ACK is not decoded (for example, no further data is decoded from the PSI_ACK) and the IMSI is not marked with an ms_purged_flag in HLR.
    b. If the FAILACTID is DISCARD, then it is used to send a purgeMS message to the HLR for a given IMSI.
11. If the FAILACTID is not provisioned by the customer, every PSI_ACK message is decoded at the SFAPP card by matching TID (transaction_index) in the TCAP information with the appropriate PSI_ACK_TID and looking for PSI map_opcode to look for the IMEI tag in the ACK message. If the IMEI tag is present and the value matches with what was retrieved from the EEDB, the IMEI challenge is considered as passed. An absent IMEI tag in the PSI_ACK is considered a failure.
12. An IMEI challenge failure results in generating another ATI to the HLR (as in use case 2) to verify the subscriber's current VLR. Upon receiving the ATI ACK or a timeout, a purgeMS is sent by EAGLE to the HLR. The encoding of the purgeMS message is as follows:
    a. HLR address (CdPA - used at SCCP layer) is obtained by the saved copy of the UL message in the local data structure.
    b. CgPA is the EAGLE self PC.
    c. The SCCP portion of the PSI message is encoded to route on SSN SFAPP.

    > **Note:**
    >
    > If the timer for the ATI ACK expires, no UIM displays indicating the expiration.

13. If the challenge has failed, the SFAPP categorizes the VLR as an intruder and generates a purgeMS message to the HLR for the subscriber from the original UL. The purgeMS

incorporates the IMSI tag/length/value. The important piece in the TCAP layer component portion is msPurgingContext 5 bytes value which is as follows: 0x02-operation tag 0x01-length, 0x43-purge MAP opcode 0xa3-sequence tag, 0x00-length. There is no requested information built into the purgeMS message at the TCAP layer. EAGLE does not expect and process response from HLR for purgeMS. Hence, the transaction ID at the TCAP has 4 bytes OTID as 'ff ff ff ff' to indicate an INVALID TID.

14. HLR marks the mobile subscriber as MS_purged_flag so that any request for routing information for a mobile-terminated call or mobile-terminated short message is treated as if the MS were not reachable.

2.5.2 Decoding Errors Generated EAGLE

The following decoding errors can result from the call flow:

- Unsupported Opcode is generated when invalid value is provided in the opcode filed by the VLR/SGSN
- Invalid message type error is generated on an invalid component type. An invalid component type isn't equal to TCAP_ITU_RETURN_RESULT_LAST
- Transaction ID is not found in the transaction_db error
- Unsupported message type error for the case of invalid SCCP MSU type
- TCAP decoding failure errors
- PSI ACK not received
- Purge MS error
- PSI encoding error

2.5.3 PSI Encoding and Decoding of the PSI_ACK Extended

- As a special identification aid, a special TCAP/MAP invoke_id is embedded in the PSI message as a special fixed value. This invoke_id is not user configurable.
- When the PSI_ACK returns to the SCCP card, if the map_opcode is not present, the combination of the special invoke_id/TCAP_END and return_result_last is used to validate that the PSI_ACK received has been generated by the Eagle and the PSI_ACK can be decoded for IMEI validation.

2.5.4 Routing of PSI Response Back to Originating SFAPP Card

Transaction ID Encoding and Decoding

The SFAPP card encodes the Originating Transaction ID in the PSI message in this format to identify the STP Node that generated the message:

Transaction ID changes to incorporate the Mate ID:

```
struct {
t_u8 card_loc;
t_u8 ref_count:4;
t_u8 mate_id:4;
```

```
t_u16 trans_index;
}field
```

The Mate ID is the index of the location of the STP's self ID provisioned in the STP mate table. The mate table is populated with the STP's mate point codes as well as its own. If the mate tables of each STP that forms a pair/quad contains the same point codes, the order of the tables for each node is guaranteed to be the same.

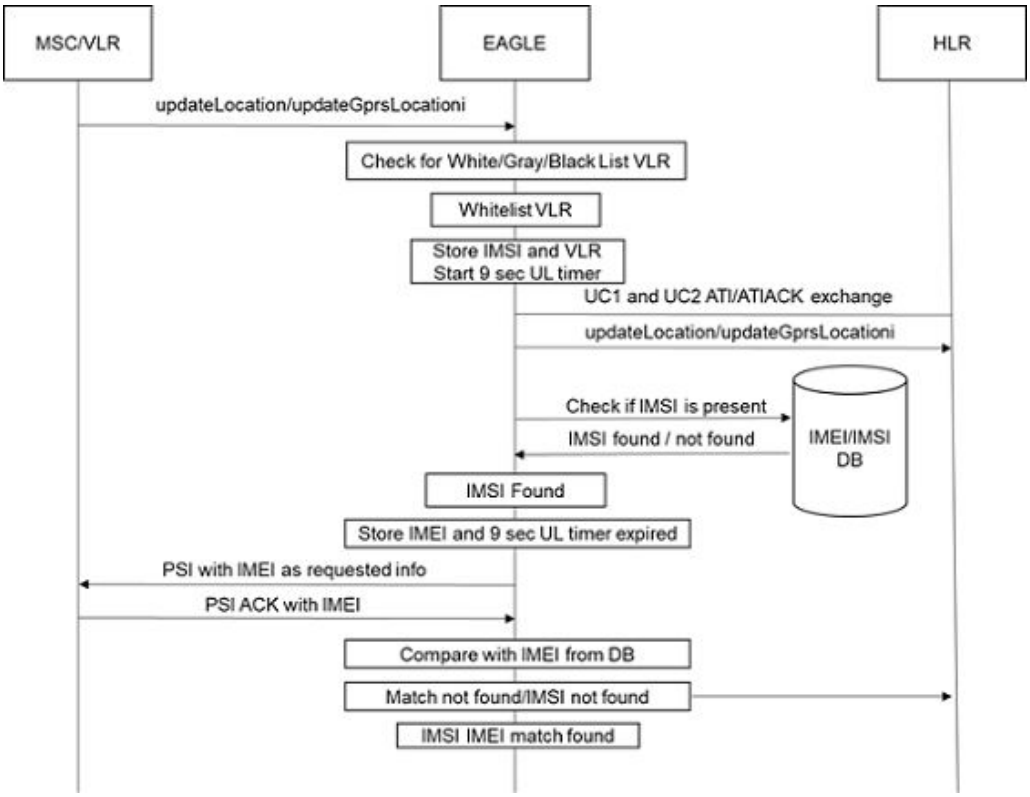
PSI Response Handling on SCCP Card

1. When the PSI Response is received on the LIM card, it does the normal processing and sends that message to the SCCP card.
2. When the message is received on the SCCP card, it applies the GT rules on that message.
3. After applying GT rules, it filters the message with these rules. If all the rules match, then it goes to step 4, otherwise it does the normal GT processing:
   a. SFAPP GTT action is provisioned for the matching translation or forwarding the message to SFAPP SS.
   b. Dlg Type is END or ABORT
   c. Comp type is Return result last/Abort/Return error
   d. OpCode is PSI response
   e. Invoke ID is some high value 0x7F
4. Decode the Mate ID from the destination Transaction ID and match the Mate ID in the message with the Mate ID stored in the table (to verify the response for EAGLE-generated request).
   a. If Mate ID matches with the ID stored in the table and the entry is the node's self ID, then forward that to the SFAPP card.
   b. Or forward that to the correct mate node that generated the request
5. If Mate ID does not match with the stored value, do the normal processing.

2.5.5 IMEI Learning Using the EAGLE External Database (EEDB)

As indicated in Figure 2-8, an IPSM card that is configured with a TCP connection will maintain a connection to an external database containing IMSI/IMEI data indexed by IMSI. To support IMEI validation when a VLR is graylisted, the SFAPP card will generate an addition or an update containing the subscriber data that is then routed to the EEDB via the IPSM card if the VLR has been determined to be whitelisted (learning).

Figure 2-8 Whitelisted VLR DB Learn - Whitelisted VLR DB Learning



When the UL message has been intercepted by EAGLE, if the VLR is determined to be whitelisted, a query to the EEDB is launched. If the IMSI is not found, when the IMEI is extracted from the PSI_ACK, it is added to the EEDB. If it was found and the data matched to that returned in the PSI_ACK, the record in the EEDB is updated with aging data.

2.6 Intelligent VLR Whitelist

Intelligent VLR Whitelist uses a whitelist that is created as part of learning from the validation attempts defined in VLR Validation and Graylisted VLR Validation Using IMEI.

To implement a whitelist-based, learning-based validation, VLR is implemented where the VLR addresses are validated from tables configured/stored on disk in the STP. The tables are differentiated into 2 classes - Static and Dynamic VLR tables. There are two static VLR tables – a static VLR profile table (same as VLR profile table in use case 2) and a static VLR roaming table (same as VLR roaming table in use case 2). Also, there are two dynamic VLR tables – a dynamic VLR profile table and a dynamic VLR roaming table. The VLR validation process is the same in concept, for example, they block messages until velocity check is applied. But, with the introduction of new tables, EAGLE can now support dynamic VLR learning and populate dynamic VLR tables autonomously from the network traffic. However, the VLR DB UI commands work the same as in use case 2.

Both static and dynamic VLR tables are disk-resident tables on the OAM. The dimensions of static VLR profile and dynamic VLR profile tables are exactly the same.

Similarly, the dimensions of static VLR roaming and dynamic VLR roaming tables are exactly the same. The main difference between the two classes of tables lies in the process of their population and maintenance. Static VLR tables are only updated by UI commands whereas dynamic VLR tables are populated by the information learned by EAGLE through network traffic over time. Information flow for static VLR tables is in the form of provisioning (RADB) packets - originating at OAM and terminating at SFAPP cards - which are generated per UI command where information flow for dynamic VLR tables is dictated by sync cycles - originating from secondary SFAPP cards and terminating at OAMs - which are triggered by timers. Network traffic is only received on secondary SFAPP cards, while the primary SFAPP card is always in flow-control and does not process any traffic.

Learning is controlled by these modes using a mode parameter in the new SFAPPOPTS command:

- Learn Mode - This mode allows all unknown VLRs that are learned to be added to the dynamic VLR database, but does not update existing data in any manner.
- Test Mode - This mode validates the unknown VLRs and moves to whitelist/blacklist per thresholds configured. However, no further action is taken (no messages are rejected).
- Active Mode - This mode validates VLRs based on the learned white lists in the system. In case the VLR is not available in the list, the message is rejected.

The term new VLR means the CgPA GT address of the incoming network message is not found either in the Static VLR table nor in the Dynamic VLR table on the SFAPP card where the network message was originally received. These network messages can be messages such as ActivateSS, UpdateLocation, UpdateLocationGPRS, and SendAuthenticationInfo.

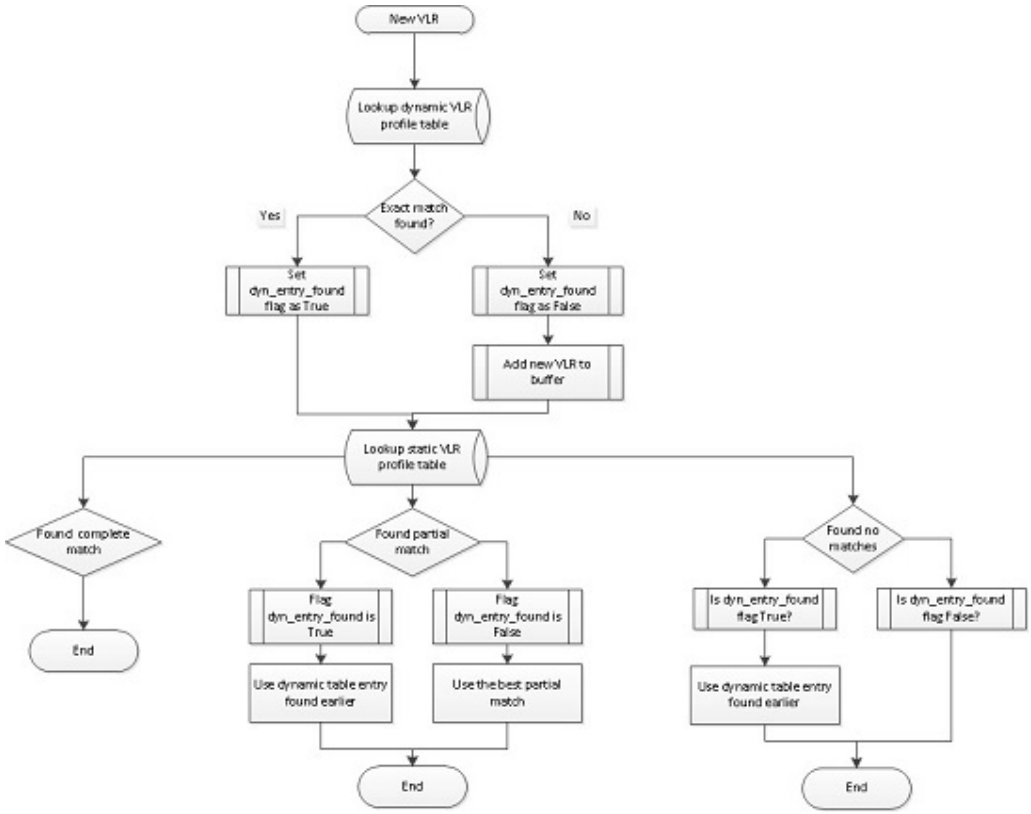
These updates flow from the SFAPP cards configured in EAGLE to the OAMs. SFAPP cards are divided into primary SFAPP card that does not process traffic, and secondary SFAPP cards that do traffic handling. The secondary cards copy the updates to the primary card, which collates them and updates the OAM cards and the secondary cards. In this fashion, all secondary cards are synced even if an update is received by only one secondary card.

> **Note:**
>
> There is no flow-control or recovery mechanism to get the dynamic update buffers lost in transit. For example, if a dynamic update is lost in transit between a secondary SFAPP card and the primary card, the update is relearned when the next message from that VLR is received.

2.6.1 Dynamic VLR Whitelisting Flow

Figure 2-9 shows the VLR challenge flow including learning.

Figure 2-9 Dynamic VLR learning (VLR Whitelisting)



Secondary SFAPP Cards

When a new VLR in the incoming network message is received on a secondary SFAPP card, the VLR is first searched in the dynamic VLR profile table. If exact match is found, a control flag - for example, dynamic_entry_found - is set and a subsequent static VLR profile table search is applied. If an exact match is NOT found, the new VLR is added to a buffer, but the static VLR profile table search is still applied. In static table search, there can be three cases:

- **Complete match found:** If complete match is found, nothing needs to be done.
- **Partial match found:** If partial match is found, use the best matching partial static VLR profile entry.
- **No matches found:** If no matches are found for new VLR in static VLR profile table, check the value of dynamic_entry_found flag.

If the flag is set, use matching dynamic VLR profile entry for VLR validation. Otherwise, nothing needs to be done. A secondary SFAPP card keeps populating said buffer with such new VLRs either until the end of 500ms tick or when buffer has 48 VLRs in it, whichever occurs first. When either of these two conditions are met, secondary SFAPP cards send their buffer to the primary SFAPP card.

> **Note:**
>
> A secondary SFAPP card only makes one buffer worth up to 48 VLRs in one 500ms cycle. But since there could be n number of secondaries in EAGLE, the primary SFAPP card receives n number of new VLR buffers in one 500ms cycle.

Primary SFAPP Cards

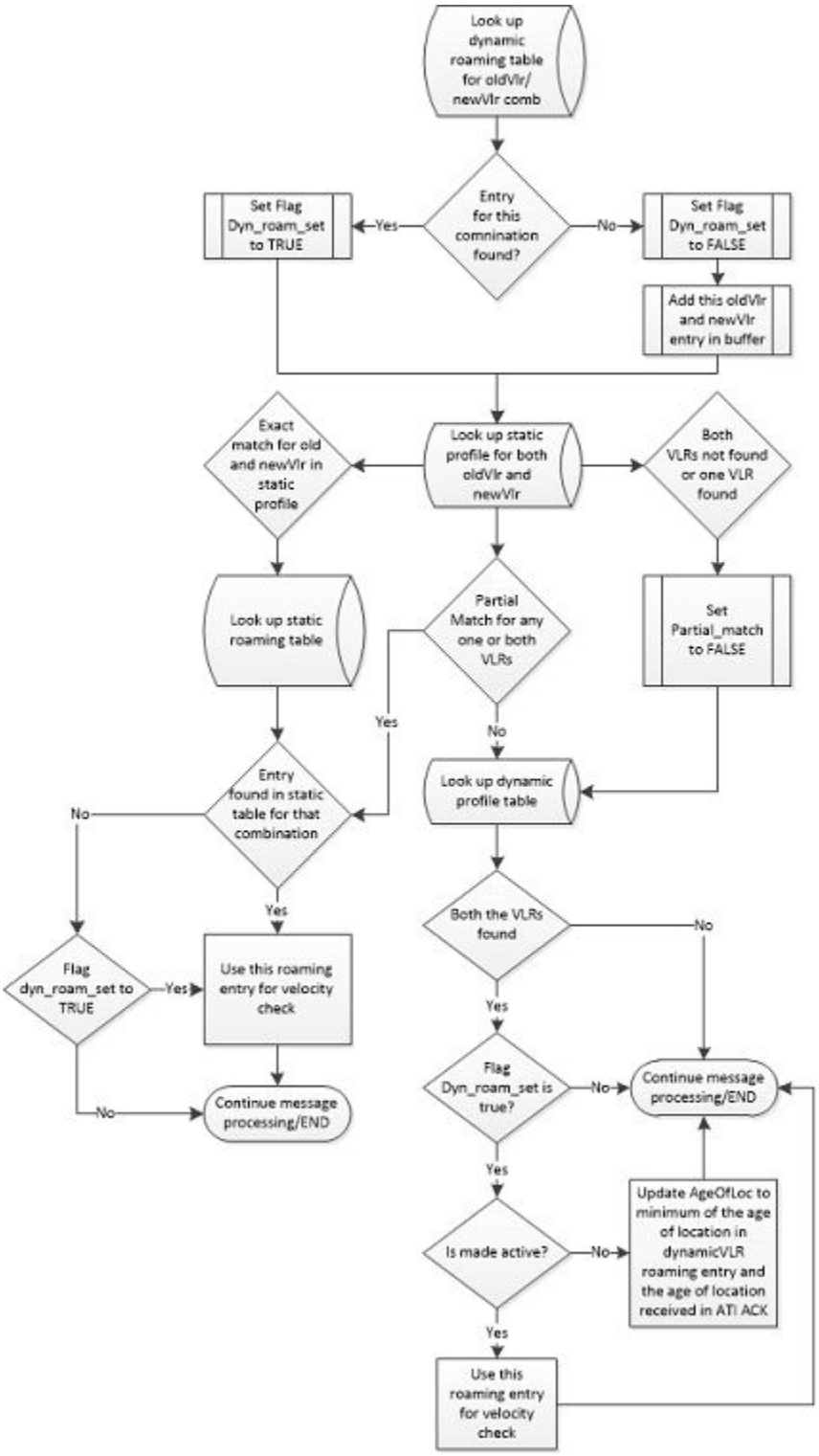
The primary SFAPP card, at the end of each 500ms cycle, picks each buffer it received in that time and intelligently inserts the new VLRs in to its dynamic VLR profile table. Since, the traffic from the same VLR could be going to different SFAPP cards on different occasions, we except to get collisions in the incoming buffers from the secondary SFAPP cards. To remove this collision and insert only unique VLR entries, the primary SFAPP card picks each VLR from each buffer and searches its dynamic table for that VLR. If the entry is found, that VLR is discarded and the card moves on to the next new VLR. Meanwhile, a timer of three seconds is active on the primary SFAPP card. As soon as one 3-second cycle ends, the primary SFAPP card pauses new inserts into its dynamic VLR profile table and starts to make buffers worth of 30 dynamic VLR profile table entries each. These dynamic VLR profile table entries are the delta between the dynamic VLR profile table on the primary and the dynamic VLR profile table on the secondary SFAPP card. The primary then sends these buffers out to the secondary SFAPP cards so they can insert these new dynamic VLR updates in their dynamic VLR profile table.

> **Note:**
>
> The primary SFAPP card has a second timer of 1-hour duration which is responsible for triggering dynamic VLR table synchronization between SFAPP(P) and OAM card.

2.6.2 VLR Velocity Check Flow

Figure 2-10 shows the VLR velocity check flow.

Figure 2-10 VLR Velocity Check



Secondary SFAPP Cards

The dynamic VLR roaming table is used on these occasions:

- When both new VLR and old VLR are found in the dynamic VLR profile table.
  In this case, we look up the dynamic VLR roaming table with the dynamic VLR profile table indices of new VLR and old VLR to get threshold and subscriber state. If the threshold value is less than or equal to the age of location found in the ATI ACK, then VLR validation is considered successful.
- When one VLR is found in the dynamic VLR profile table and the other VLR is found in the static VLR profile table.
  In this case, the VLR entry found in the static VLR profile table is duplicated into the dynamic VLR profile table on that SFAPP card. This is done so as to obtain both new and old VLR indices from the same profile table.

  For example, say new VLR is found in the dynamic profile table, but the old VLR is found in the static profile table. We replicate the old VLR entry from the static profile table into the dynamic profile table and get the indices of both the new VLR entry and the newly-created old VLR entry from the dynamic profile table. With these indices, the search is performed in the dynamic VLR roaming table to get the threshold, subscriber state, and last activity time.

> **Note:**
>
> If the same combination of old VLR and new VLR is observed again in another VLR validation and the value of age of location is the same as that in the dynamic VLR roaming entry, age of location value in roaming entry is not updated.

> **Note:**
>
> If the same combination of old VLR and new VLR is observed again in another VLR validation and the value of age of location is different than that in the dynamic VLR roaming entry, age of location value in roaming entry is updated to a minimum of the age of location in dynamic VLR roaming entry and the age of location received in ATI ACK. Here, we take the minimum of both age of locations since we assume the ATI ACK is always coming from the True VLR since ATI and ATI ACK are internal messages for the SS7 network.
> For example, say combination of old VLR=123 and new VLR=456 is searched into the dynamic VLR roaming table. A matching entry is found in the table and the age of location entered as 10 hours. But, the value of age of location in the ATI ACK is 8 hours. Then, we update the age of location of the existing dynamic VLR roaming entry to 8 hours using the following formula.

Primary SFAPP Cards

The syncing of the dynamic VLR roaming table is the same as that of dynamic VLR profile table.

2.6.3 Primary Card Selection

With this feature, SFAPP cards are now split into two groups: Primary - having only one member, and Secondary - all other SFAPP cards. To select the primary, the general rule is one having the lowest IMT address is designated as the primary SFAPP card, but if any SFAPP card having higher IMT address becomes active before others and primary cards

selection procedure completes on it before other SFAPP cards becomes active, then that SFAPP card continues to be a primary SFAPP card and all the other cards are designated as secondary SFAPP cards. The primary SFAPP card has numerous responsibilities for dynamic VLR information management and therefore, does not process any traffic - its primary duties are to collate the updates from the secondaries and act as a sync between the secondaries and OAMs. The secondary SFAPP cards, however, are the ones that process traffic to inform primary SFAPP card of the new VLRs they have learned individually over time.

In EAGLE, there can be more than one SFAPP card. When all SFAPP cards are initialized, they download registered tables through ADL. When all registered tables have been downloaded, the ADL task, on a given SFAPP card, sends a DETERMINE_ROLE signal to SFAPP manager on itself. The SFAPP manager task encompasses the primary SFAPP selection mechanism on a SFAPP card and works as follows:

1. On receiving the DETERMINE_ROLE signal from ADL, the SFAPP manager initializes the SFAPP Role Change Manager. When this is initialized, it starts a 250ms timer on the SFAPP card. This timer is responsible for triggering the role determination algorithm on the SFAPP card.
2. When the 250ms timer expires, the SFAPP card checks if it has received a broadcast message from any other SFAPP card in the system indicating the other card has become primary. If no such broadcast message has been received, the SFAPP card checks if it has been 1 second without an incoming broadcast message and if it has not been 1 second, the 250ms timer is restarted. If it has been 1 second without a broadcast message, the SFAPP card sets its state as primary and sends out a broadcast message to all other SFAPP cards in the system indicating so. The primary SFAPP card also puts itself in flow-control since primary SFAPP card does not process any traffic.
3. When this broadcast message is received on some other SFAPP card in the system, it checks if its IMT address is less than the IMT address of the card from where the broadcast message is coming. If the check returns FALSE, this SFAPP card sets its state as secondary and starts to process network traffic.

> **Note:**
>
> 1. If two SFAPP cards in the system become primary at the same time and broadcast their respective messages, each card receives the broadcast message from the other card and compares the IMT addresses, for example, IMT address of itself and the IMT address of the card from which broadcast message was received - and the card which has the lower IMT address becomes the primary SFAPP card while the other becomes a secondary SFAPP card.
> 2. When a primary SFAPP card is re-initialized, the SFAPP card having the lowest IMT address becomes the primary SFAPP card and puts itself in flow-control.

2.6.4 Dynamic Entry Aging

Dynamic entries have an aging process applied to remove dynamic VLR entries, which do not get referenced. An agetime parameter is added to the new SFAPPOPTS

command to define an age limit that a dynamic VLR entry must be referenced (updated) within to avoid being aged out/removed.

The aging process is performed per the time interval set in the agetime (in hours) parameter in SFAPPOPTS table. The primary SFAPP card performs the ageing mechanism on dynamic VLR profile and roaming tables by deleting the entries, which were not referenced for the duration set in agetime. Once the ageing mechanism completes on primary SFAPP card, it then syncs the complete tables with secondary SFAPP cards and OAM using the table copy mechanism.

The ageing mechanism is overloaded with the one-hour primary SFAPP to OAM sync. When ageing and one-hour sync intersect, then only the ageing mechanism is performed since it also covers the one-hour sync mechanism.

2.6.5 OAM Processing

There are two processes on the OAM where dynamic updates and the use of dynamic VLR tables are used.

Dynamic VLR Table Sync with Primary SFAPP Card

The primary SFAPP card has a 1-hour timer, on expiry of which it begins the dynamic VLR profile table sync between itself and the active OAM. The beginning of the hourly sync process is indicated using a UIM. At 1-hour timer expiry, the primary SFAPP card sends a signal to the active OAM to indicate the start of the dynamic VLR table sync cycle. On receiving this signal, OAM checks if there are any pending updates that need to be done on dynamic VLR table before sync begins. If there are no updates, the OAM sends back an ACK informing the primary SFAPP card that it is ready for syncing. If there are pending updates, those updates are processed before sending out the ACK. On receiving the ACK from OAM, the primary SFAPP card initiates table copy mechanism and sends three dynamic VLR tables (dbmm, profile, and roaming) to the OAM. The OAM then refreshes its RAM and binary trees. Once the RAM copy of dynamic VLR profile table on the active OAM is updated, the active OAM then sends the updated dynamic VLR profile table to the standby OAM. The standby OAM writes the table in the RAM first and then to its disk.

During this process, access to the dynamic tables must be controlled and no other access can be allowed. Therefore, the following commands are inhibited:

- Chg-db
- Copy-meas
- Copy-disk
- Format-disk
- Act-upgrade
- Rept-stat-db
- FTRA
  - RTRV-VLR-PROF
  - RTRV-VLR-ROAMING
  - ENT-VLR-PROF
  - CHG-VLR-PROF
  - CHG-TH-ALM

  - REPT-STAT-MFC
  - ENT-MATE-STP
  - DLT-MATE-STP
  - RTRV-MATE-STP
  - CHG-SFAPPOPTS
  - RTRV-SFAPPOPTS
- Rtrv-vlr-prof/rtrv-vlr-roaming - these commands are inhibited for dynamic tables only, that is, access to the static tables is allowed.

The sync process start is signaled by issuing UIM 1316, and sync completion by UIM 1317.

Dynamic VLR Table Sync with Secondary SFAPP Card

When all SFAPP cards are initialized, they download all the required static tables from the OAM. But the OAM sends the dynamic VLR tables only to the primary SFAPP card. It is the responsibility of the primary SFAPP card to send the dynamic VLR tables to the secondary SFAPP cards. When the secondary SFAPP cards have downloaded the entire dynamic VLR table from the primary SFAPP card, they transition into IS-NR state and start processing traffic for autonomous learning. This mechanism helps to minimize the possibility of single/multiple SFAPP cards going out of sync with other SFAPP cards as well as the OAM.

2.7 Hardware Requirements

- SS7 Firewall - Stateful Applications is only compatible with SLIC hardware.
- SS7 Firewall - Stateful Applications is only supported on the 64-bit flash GPL.
- An SFAPP card is able to run 4000 cat 3.1 or 3.2 validations per second.
- A maximum limit of six (6) SFAPP cards (n+1 configuration) per EAGLE is enforced on the OAM.

Stateful Applications on EAGLE is able to perform 20k TPS per node.

The EAGLE provides a mechanism to store the message information. It is possible to store the following information in the local DB:

- The IMSI or MSISDN from the incoming message
- CgPA
- CdPA
- The incoming message

3
Commands

This chapter contains brief descriptions of the EAGLE commands used for the configuration and control of the Stateful Applications feature.

3.1 Introduction

This chapter contains the EAGLE commands used to support the Stateful Applications feature. Refer to *Commands User's Guide* for complete command descriptions, including parameter names, valid parameter values, examples, and dependencies.

3.2 EAGLE Command Added to Support Stateful Applications

The new command to support configuration of the Stateful Applications feature is described as follows:

Mate STP Table Commands

The mate STP commands are used to administer the mate STP table. Since responses to messages generated by the features cannot be guaranteed to be routed back to the original node that generated them, this table is used to determine whether or not a response is received by the node that originated or must be 'hopped' to the proper mate node that originated it.

The following restrictions exist:

1. The entry must already exist in either the destination or SID tables.
2. All entries must be in the same network domain.

`chg-mate-stp`
This command is used to modify a self point code of a mate node forming the gateway.
Command Examples:

- `chg-mate-stp:pc=10-20-30`
- `chg-mate-stp:pcn24=99-99-99`
- `chg-mate-stp:pcn=s-12345`
- `chg-mate-stp:pcn16=121-5-10`

`dlt-mate-stp`
This command is used to remove the self point codes of the nodes forming the gateway.
Command Examples:

- `dlt-mate-stp:pc=10-20-30`
- `dlt-mate-stp:pcn24=99-99-99`
- `dlt-mate-stp:pcn=s-12345`

- `dlt-mate-stp:pcn16=121-5-10`

`ent-mate-stp`
This command is used to provision the self point codes of the nodes forming the gateway.
Command Examples:

- `ent-mate-stp:pc=10-20-30`
- `ent-mate-stp:pcn24=99-99-99`
- `ent-mate-stp:pcn=s-12345`
- `ent-mate-stp:pcn16=121-5-10`

`rtrv-mate-stp`
This command is used to display the table.
Command Example:

```
rtrv-mate-stp

tekelecstp 18-05-29 11:19:05 MST  EAGLE 46.6.2.0.0-73.19.0
    rtrv-mate-stp
    Command entered at terminal #2.
   tekelecstp 18-05-29 11:19:05 MST  EAGLE 46.6.2.0.0-73.19.0

      STP POINT CODE(PCI)
      -------------------
           1-001-1
           3-003-1
    Mate Stp table is (2 of 16) 13% full.
```

SFAPPOPTS Commands

The SFAPPOPTS commands are implemented to administer the SFAPPOPTS table. This table contains the following:

- Nnode-wide options to enable/disable the VLR IMEI challenge (UC #3)
- Dynamic whitelisting learning mode (UC #4), success/fail thresholds for which counts of challenges of dynamically learned VLRs must exceed in order to transition a dynamically learned VLR from graylist to either white or blacklist
- A velocity check threshold to define the number of velocity check attempts needed for a dynamic roaming entry to be marked as Learned
- An agetime to define a value for aging out VLR entries

Restrictions for these commands include the following:

1. The learn mode should not be switched to either OFF or LEARN during the sync from the primary SFAPP card to OAM.
2. At least one active SFAPP card must be present in the EAGLE in order to modify the table.

`chg-sfappopts`
This command is used to modify a parameter of the SFAPPOPTS table.
Command Examples:

- `chg-sfappopts:vlrimeichallenge=yes`
- `chg-sfappopts:mode=off`
- `chg-sfappopts:mode=learn`
- `chg-sfappopts:mode=test`
- `chg-sfappopts:mode=active`
- `chg-sfappopts:succth=3`
- `chg-sfappopts:failth=5`

Note:

- **VLRIMEICHALLENGE** - Enables/Disables the VLR IMEI challenge for CAT3.2 messages
- **MODE**- Provides option to turn off dynamic learning, test the learning algorithm, and move the system in operation using various modes
  - *OFF*- Turn off the dynamic whitelist learning. Delete all the dynamic VLR profile and dynamic VLR roaming entries.
  - *LEARN* - Only learn about new VLRs, no challenges are performed (newly learned VLRs are considered as Whitelisted). Delete dynamic entries without parent in static when switch from ACTIVE or TEST mode
  - *ACTIVE* - Challenges are performed. Status of dynamically learned VLRs are changed to Whitelisted or Blacklisted if they meet criteria
  - *TEST* - Challenges are performed. However, learned VLRs remain Grey listed
- **SUCCTH** If system-wide success threshold is 0 i.e., None, then do not transition any VLR to whitelist
- **VELTH** - In case VELTH is set to None, all dynamic VLR roaming entries will always be in LEARNING phase and will never be used for VLR validation
- **AGETIME** - In case agetime is set to None, ageing will not perform

`rtrv-sfappopts`
This command is used to display the table.
Command Example:

```
rtrv-sfappopts

rtrv-sfappopts
     tekelecstp 18-09-13 01:26:30 EST  EAGLE 46.7.0.0.0-75.10.0
     rtrv-sfappopts
    Command entered at terminal #17.
;
Command Accepted - Processing
    tekelecstp 18-09-13 01:26:30 EST  EAGLE 46.7.0.0.0-75.10.0
    SFAPP OPTIONS TABLE
    ------------------
```

```
VLRIMEICHALLENGE = no
MODE             = active
SUCCTH           = none
FAILTH           = none
VELTH            = none
AGETIME          = none
```

Status Command

rept-stat-sfapp
This command is used to display the overall status of the SFAPP Card service in the EAGLE.
Command Examples:

- `rept-stat-sfapp`
- `rept-stat-sfapp:peakreset=yes:loc=1101`
- `rept-stat-sfapp:loc=1101`

Visitor Location Register Commands

These commands are used to change, delete, enter, and display Visitor Location Register Profiles and Roaming entries:

chg-vlr-prof
Use this command to change a Visitor Location Register (VLR) Profile for a mobile subscriber. A VLR-Profile entry helps in getting information required to locate the user while roaming and is subsequently used in VLR-ROAM table.
Command Examples:

- `chg-vlr-prof:vlr=4234:filter=blacklist`
- `chg-vlr-prof:vlr=4234:ageofloc=no:lastact=yes`

dlt-vlr-prof
Use this command to delete a Visitor Location Register (VLR) Profile for a mobile subscriber for existing entries.
Command Examples:

- `dlt-vlr-prof:vlr=4234`

ent-vlr-prof
Use this command to enter a Visitor Location Register (VLR) Profile for a mobile subscriber. A VLR-Profile entry helps in getting information required to locate the user while roaming and is subsequently used in VLR-ROAM table.
Command Examples:

- `ent-vlr-prof:vlr=12345`
- `ent-vlr-prof:vlr=4234:filter=blacklist`
- `ent-vlr-prof:vlr=4234:filter=blacklist`

rtrv-vlr-prof
Use this command to display entries from the Visitor Location Register (VLR) Profile table.
Command Examples:

- `rtrv-vlr-prof`
- `rtrv-vlr-prof:num=2`
- `rtrv-vlr-prof:filter=blacklist`

`chg-vlr-roaming`
Use this command to change a Visitor Location Register (VLR) roaming entry for a mobile subscriber. A VLR-Roaming entry uses existing entries for both new as well as old entries from vlr-prof table.
Command Examples:

- `chg-vlr-roaming:oldvlr=1234:newvlr=56545:time=20`

`dlt-vlr-roaming`
Use this command to delete a Visitor Location Register (VLR) Roaming entry for a mobile subscriber for existing entries.
Command Examples:

- `dlt-vlr-roaming:newvlr=12345:oldvlr=56780`

`ent-vlr-roaming`
Use this command to enter a Visitor Location Register (VLR) roaming entry for a mobile subscriber. A VLR-Roaming entry uses existing entries for both new as well as old entries from vlr-prof table.
Command Examples:

- `ent-vlr-roaming:newvlr=12345:oldvlr=56780:time=10`

`rtrv-vlr-roaming`
Use this command to display entries from the Visitor Location Register (VLR) Profile table.
Command Examples:

- `rtrv-vlr-roaming`
- `rtrv-vlr-roaming:num=2`
- `rtrv-vlr-roaming: newvlr=12345:oldvlr=56780`

3.3 EAGLE Commands Modified to Support Stateful Applications

These commands are modified as described below to support the Stateful Applications feature:

Table 3-1 EAGLE Commands Modified to Support SFAPP

Modifications	Affected Commands

Generate measurements reports and FTPed SFAPP measurements data	`chg-measopts`
	`rept-meas`
	`rtrv-measopts`
	`rtrv-mtc-measopts`

Table 3-1 (Cont.) EAGLE Commands Modified to Support SFAPP

Modifications	Affected Commands

Support SFAPP GPL	`act-gpl`
	`chg-gpl`
	`init-card`
	`rept-stat-card`
	`rept-stat-gpl`
	`rtrv-gpl`

Support `appl=sfapp` for SFAPP cards	`dlt-ss-appl`
	`ent-card`
	`ent-ss-appl`
	`init-card`
	`rept-stat-card`

Support display of alarms	`chg-th-alm`
	`rept-stat-alm`
	`rtrv-alm`
	`rtrv-th-alm`

Support SFAPP cards	`dlt-card`
	`ent-card`
	`rtrv-card`

Support Global Title Translation (GTT) Action	`chg-gttact`
	`ent-gttact`
	`rtrv-gttact`

Support status display of databases on SFAPP cards	`rept-stat-db`

Support for VLR Profile and Roaming	`chg-vlr-prof`
	`ent-vlr-prof`
	`rtrv-vlr-prof`
	`rtrv-vlr-roaming`

4
Feature Configuration

This chapter provides the procedure for configuring the EAGLE Stateful Applications feature.

4.1 Introduction

This chapter contains example commands for configuring the Stateful Applications feature of the Oracle Communications EAGLE.

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

4.2 Stateful Applications Configuration

Example commands for configuring the SFAPP feature are as follows:

1. Configure the SFAPP card.

   ```
   ent-card:loc=xxx:type=slic:appl=sfapp
   ```

2. Configure the SFAPP local subsystem.

   ```
   ent-ss-appl:appl=SFAPP:ssn=12:stat=online
   ```

3. Configure SFAPP GTT actions.

   ```
   ent-gttact:actid=disc:act=disc
   ```

   ```
   ent-
   gttact:actid=uc3:act=sfapp:on=uimreqd:failactid=disc:defactid=fal
   lback:scfaddr=1111111111
   ```

   ```
   ent-
   gttact:actid=sfaptparm:act=sfapp:hlraddr=tcapparm:scfaddr=1911111
   111:defactid=disc:failactid=disc:tt=29
   ```

   ```
   chg-
   gttact:actid=uc3:ATIRESCGMODID=sfappati:PSIRESCGMODID=sfapppsi
   ```
   (step 5 needs to be executed first before this command)

4. Configure GTMOD for CgPA portion for ATI and PSI messages (to be assigned to ATIRESCGMODID and PSIRESCGMODID of the SFAPP GTTACTION)

   ```
   ent-
   gtmod:GTMODID=sfapppsi:NTT=23:NGTI=4:NNP=1:NNAI=4:PRECD=pfx:CGPAS
   SN=10:NPDS=22222222223
   ```

   ```
   ent-
   gtmod:GTMODID=sfappati:NTT=23:NGTI=4:NNP=1:NNAI=4:PRECD=pfx:CGPAS
   SN=10:NPDS=22222222221
   ```

5. Configure GTT for translating the incoming UL message to the SFAPP GTT action.

   GTT action set table: `ent-gttaset:actsn=sfappuc3:actid1=uc3`

   GTT SET table: `ent-gttset:gttsn=sfapp:netdom=itu:settype=cdgta`

GTT SEL table: `ent-gttsel:gtii=4:cdgttsn=sfapp:tt=20:np=e164:nai=intl` and `ent-gttsel:gtii=4:cdgttsn=sfapp:tt=23:np=e164:nai=intl`

6. Configure GTT for translating the ATI/PSI message to the SFAPP GTT Action or SFAPP subsystem (based on the HANDLRESP parameter configured under SFAPP GTT action).

   HLR: `ent-gta:gttsn=sfapp:gta=2222222210:egta=2222222260:xlat=dpc:ri=gt:pci=3-003-3:ACTSN=sfappuc3:mrnset=none`

   VLR: `ent-gta:gttsn=sfapp:gta=95604:egta=95604:xlat=dpc:ri=gt:pci=2-002-2:mrnset=none`

7. Configure Mate-stp table with TPC and mate STP PCs.

   ```
   ent-mate-stp:pci=4-185-3 (Eagle 11 TPC)
   ```

   ```
   ent-mate-stp:pci=xxxx (for mate)
   ```

8. Configure SFLOG card for connecting EEDB.

   ```
   ent-card:loc=1103:type=ipsm:appl=ips:sflog
   ```

   ```
   chg-ip-lnk:loc=1103:port=a:ipaddr=10.75.52.61:SUBMASK=255.255.255.0:MACTYPE=DIX:auto=yes:mcast=no
   ```

   ```
   chg-ip-card:loc=1103:SRCHORDR=SRVR:DEFROUTER=10.75.52.1
   ```

9. Configure IP connection (ENT-IP-CONN) for connecting EEDB.

   ```
   ent-ip-host:host=eedb:ipaddr=10.75.50.106:type=remote
   ```

   ```
   ent-ip-host:host=sflog:ipaddr=10.75.52.61:type=local
   ```

   ```
   ent-ip-conn:cname=conn1:prot=tcp:lhost=sflog:lport=2100:rport=17529:rhost=eedb
   ```

   ```
   chg-ip-conn:cname=conn1:open=yes
   ```

10. Configure VLR profile entries (ENT-VLR-PROF) are configured with filter graylist.

    ```
    ent-vlr-prof:vlr=95604:filter=graylist:ageofloc=no:IMEIRTRV=yes
    ```

    ```
    ent-vlr-prof:vlr=ab123:filter=graylist:ageofloc=no:IMEIRTRV=yes
    ```

11. Configure VLR roaming table (ENT-VLR-ROAMING).

    `ent-vlr-roaming:oldvlr=ab123:newvlr=95604:time=10` (This entry goes in the static table)

12. Turn on the global UC3 option.

    ```
    SFAPPOPTS:VLRIMEICHALLENGE=YES
    ```

    ```
    chg-sfappopts:VLRIMEICHALLENGE=yes
    ```

13. Use AGEOFLOC and IMEIRTRV parameter under VLR profile entry (RTRV-VLR-PROF) selectively turn OFF or ON UC2 and UC3 for the VLR.

    ```
    chg-vlr-prof:vlr=95604:ageofloc=no:IMEIRTRV=yes
    ```

14. Use DEFACTID and FAILACTID and under the SFAPP GTT action to selectively configure the Default and Failure actions for the SFAPP GTT action.

```
chg-gttact:actid=uc3:on=HANDLRESP
```

5 Measurements

This chapter describes the measurements information available from the EAGLE Stateful Applications feature.

5.1 Stateful Applications Measurements

Refer to *Measurements Reference* for information about measurement systems and reporting.

Refer to *Commands User's Guide* for descriptions of commands used to generate, schedule, and transfer measurements reports.

Refer to *Database Administration - System Management User's Guide* for provisioning information and procedures for these measurement systems:

- Measurements Platform
- E5-OAM Integrated Measurements

Supported report types include SYSTOT-SFAPP and MTCDSDAPP. For Stateful Applications, the EAGLE allows the capturing of the following measurement reports:

- Successful validations
- Failed validations

The EAGLE will keep the message and its information for at maximum 5 seconds. The message will be dropped and a measurement pegged in case a response is not received within the 5 second time frame.

There are 32 SFAPP GTT actions. Each SFAPP GTT action will have the following four (4) measurement pegs:

1. PASSED - Number of messages that were successfully routed after the validation passed.
2. FAILED - Number of messages for which validation was performed and the validation did not pass.
3. ERROR1 - All errors due to which validation could not be performed on the messages that the EAGLE did not generate (ActivateSS, UpdateLocation, for example).
4. ERROR2 - All errors due to which validation could not be performed on the messages that the EAGLE generated or their response (ATI, ATI_ACK, for example).

6
Maintenance

This chapter describes the maintenance information available from the Stateful Applications feature. The information includes status, alarms (UAMs), and information messages (UIMs).

6.1 Alarms

Refer to *Unsolicited Alarm and Information Messages Reference* for descriptions and corrective procedures for alarms related to EAGLE features and functions.

This section lists new Unsolicited Alarm Messages (UAMs) used to support the EAGLE Stateful Applications feature.

Table 6-1 Unsolicited Alarm Messages

UAM	Message Text	Description	Severity	Output Group
0543	VLR Dynamic Learning is suspended	If only one SFAPP card is present in the system.	Critical	SFAPP
0544	VLR Dynamic Learning Started	If more than one SFAPP card is present in the system and Dynamic learning is turned ON.	Normal	SFAPP
0634	SFAPP is available	All SFAPP cards are IS-NR	Normal	SFAPP
0635	SFAPP is not available	All SFAPP cards are isolated	Critical	SFAPP
0636	SFAPP is removed	Last SFAPP card is deleted from the system	Normal	SFAPP
0637	SFAPP Threshold Level1 Exceeded	SFAPP Threshold Level1 Exceeded	Minor	CARD
0638	SFAPP Threshold Level2 Exceeded	SFAPP Threshold Level2 Exceeded	Major	CARD
0639	SFAPP Threshold Level Critical	SFAPP traffic is above the system supported traffic limit	Critical	CARD
0640	SFAPP Threshold Condition Cleared	SFAPP Threshold Condition Cleared	Normal	CARD
0641	SFAPP Capacity normal, card(s) abnormal	SFAPP Capacity normal, card(s) abnormal	Minor	SFAPP
0642	System SFAPP TPS normal	Isolated SFAPP card comes in service	Normal	SFAPP
0643	System SFAPP Threshold Exceeded	System SFAPP Threshold Exceeded	Major	SFAPP
0644	System SFAPP Capacity Exceeded	System SFAPP capacity Exceeded	Critical	SFAPP
0645	LIM/SCCP card(s) denied SFAPP service	One or more LIM/SCCP cards has been denied SFAPP service	Major	SFAPP

Table 6-1 (Cont.) Unsolicited Alarm Messages

UAM	Message Text	Description	Severity	Output Group
0646	SFAPP Dynamic Learning Alarm cleared	Occurs when alarm 0543 (VLR Dynamic Learning is suspended) is raised and changed the value of the `mode` parameter of the SFAPPOPTS table to OFF	Normal	SFAPP
0647	EEDB Connectivity Down	The EEDB connectivity is down	Major	SYS_MAINT
0648	EEDB Connectivity Up	The EEDB connectivity is restored	Normal	SYS_MAINT

6.2 UIMs

This section lists new Unsolicited Information Messages (UIMs) used to support the EAGLE Stateful Applications feature. Refer to *Unsolicited Alarm and Information Messages Reference* for complete descriptions of all UIM text and formats.

Table 6-2 Unsolicited Information Messages

UIM	Text	Description	Output Group
1241	SCCP/SFAPP Card logging capacity exceeded	An SFAPP card logging capacity has been exceeded	SFAPP
1312	Dynamic VLR profile table full	The Dynamic VLR Profile Table is full	SFAPP
1313	Dynamic VLR roaming table full	The Dynamic VLR Roaming Table is full	SFAPP
1314	IPS TCP connection established	An IPS TCP connection has been established	LINK
1315	IPS TCP connection terminated	An IPS TCP connection has been terminated	LINK
1316	SFAPP(P) to OAM Sync started	An SFAPP(P) to OAM sync has started	SFAPP
1317	SFAPP(P) to OAM Sync Completed	An SFAPP(P) to OAM sync has completed	SFAPP
1327	Mate PC not found in table	The Mate PC is not found in the table	SYSM
1328	Incorrect network domain	Incorrect network domain used	SYSM
1477	SFAPP Validation Response Timeout Error	An SFAPP validation response timeout error has occurred	SFAPP
1478	SFAPP Validation Encoding Error	And SFAPP validation encoding error has occurred	SFAPP
1479	SFAPP Validation Matching State not fnd	An SFAPP validation matching state was not found	SFAPP
1480	SFAPP Validation Error	An SFAPP validation error has occurred	SFAPP
1481	SFAPP Validation Velocity Chk Failed	An SFAPP validation velocity check has failed	SFAPP

Table 6-2 (Cont.) Unsolicited Information Messages

UIM	Text	Description	Output Group
1482	SFAPP Validation Failed	An SFAPP validation failure has occured	SFAPP
1483	SFAPP VLR Status Changed	The SFAPP VLR Status has changed	SFAPP
1484	SFAPP New VLR Created	A new SFAPP VLR has been created	SFAPP
1485	SFAPP New Roaming Entry Created	A new SFAPP Roaming entry has been created	SFAPP
1486	SFAPP New Primary Card Chosen	A new primary SFAPP card has been chosen	SFAPP
1487	SFAPP Dyn VLR ROAM Entry Deleted	An SFAPP Dynamic VLR Roaming entry has been deleted	SFAPP
1488	SFAPP Velocity Threshold Crossed	The SFAPP Velocity Threshold has been crossed	SFAPP
1489	SFAPP Dyn VLR Prof Entry deleted	An SFAPP Dynamic VLR Profile entry has been deleted	SFAPP
1495	TCP IPS Message Failure	A TCP IPS Message has failed	SFAPP
1496	EAGLE EEDB Message Failure	An EAGLE EEDB Message has failed	SFAPP

6.3 Thermal Management Parameters

The SFAPP card supports thermal monitoring to protect the temperature-sensitive hardware components. The processor on the SFAPP card can overheat as a result of high ambient temperature or airflow blockage. If the junction temperature increases above operating limits, the CPU halts and the SFAPP 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 (Temperature Level 1), a major alarm is raised against the SFAPP card. If the temperature continues to increase and exceeds a second thermal threshold (Temperature Level 2), a critical alarm is raised against the SFAPP card and traffic processing is stopped. When the second thermal threshold is exceeded, the application is notified from the operating system. The state of card will transition to the IN-ANR Restricted state. The following table shows the thermal events, actions, and alarms.

After the temperature decreases below the Temperature Level 2 threshold, the raised critical alarm is cleared and the corresponding major alarm is raised. When the temperature returns to its nominal range (below Temperature Level 1), a clearing alarm will be raised for the SFAPP card and the SFAPP card resumes traffic processing. These thermal thresholds (Temperature Level 1 and Temperature Level 2) are user-configurable using the `chg-thm-alm` command.

Table 6-3 Thermal Management Parameters

Board Temperature	Actions / Clearing Condition	UAM
Temperature Level 1 Exceeded on SFAPP card; Major	Major alarm UAM 0078 raised on SFAPP card	0078 Card temperature exceeds nominal lvl:T1
Temperature Level 2 Exceeded on SFAPP card; Critical	Critical alarm UAM 0077 raised on SFAPP card; State of SFAPP card transitions to IS-ANR/Restricted	0077 Card temperature is at critical lvl:T2
Temperature abated (cooling below Temp Level 2 but at level 1)	Major alarm UAM 0078 raised on SFAPP card; State of SFAPP card transitions to IS-NR/Active	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