

Oracle® Unified Session Manager
Maintenance Release Guide
Release SCZ735

May 2017

Notices

Copyright© 2017, 2004, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 S-CZ7.3.5 M1.....	7
Patch Equivalency.....	7
Content Map.....	8
Configurable Transaction Timeout for REGISTER Requests.....	8
SAR/UAR Suppression.....	9
Support of ATCF - 3GPP Rel 12.....	10
SIP Feature Capabilities.....	10
SRVCC Handover Support in Alerting Phase.....	12
ATCF INVITE ICSI Matching.....	12
Rx Interface Enhancement.....	13
AAR Message Optimization.....	13
Network Provided Location Information During Registration.....	15
Network Provided Location Information for Short Message Service.....	21
Subscription for Notification of Signaling Path Status.....	26
Emergency Call Handling Enhancement.....	27
IR.92 Multiple Emergency Numbers.....	27
2 S-CZ7.3.5 M2.....	29
Patch Equivalency.....	29
Content Map.....	30
Session Continued Support.....	30
Limiting SLB-Managed Registrations by Endpoint Count.....	31
Advanced Logging.....	32
Configuring Advanced Logging.....	32
sip-advanced-logging.....	33
sip-advanced-logging > condition.....	34
TCP Connection Tools.....	35
TCP and SCTP State Connection Counters.....	35
show sipd tcp connections.....	37
show sipd tcp.....	38
Updated Show Commands.....	40

About This Guide

This Oracle USM Maintenance Guide supports Release S-CZ7.3.5 and its documentation set. It provides an overview of features and functions in this maintenance release.

Supported Platforms

Release Version S-CZ7.3.5 includes both the Oracle Core Session Manager (CSM) and Unified Session Manager (USM) products. The Oracle USM is supported on the Acme Packet 4500, 4600, 6100, and 6300 series platforms. The Oracle CSM is supplied as virtual machine software or as a software-only delivery suitable for operation on server hardware. Refer to sales documentation for updates specifying hardware support.

Platform support for the Oracle SLRM is the same as for the Oracle CSM.

Refer to the S-CZ7.3.5 documentation set for more information about each platform.

Audience

This Maintenance Guide is for service provider technicians who need to know about new features, and other changes for this release. Please refer to the S-CZ7.3.5 Release Notes for updates on fixed issues, known issues, and caveats associated with this release.

Revision History

Date	Description
July, 2016	<ul style="list-style-type: none">Initial Release (M1)
December, 2016	<ul style="list-style-type: none">Removes multi-contact related restriction associated with SAR/UAR suppression
May, 2017	<ul style="list-style-type: none">Release with M2 content

S-CZ7.3.5 M1

This section provides descriptions, explanations, and configuration information for the contents of Maintenance Release S-CZ7.3.5M1. Maintenance Release content supercedes that distributed with the point release.

The following SPL engine versions are supported by this software:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.2.0
- C2.2.1
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3
- C3.1.4

Current patch baseline: S-CZ7.3.5 GA

Patch Equivalency

Patch equivalency indicates which patch content in neighbor releases is included in this release. This can assure you in upgrading that defect fixes in neighbor stream releases are included in this release.

Neighbor Release Patch Equivalency for S-CZ7.3.5M1:

- S-CZ7.3.0m1p4

Content Map

The following table identifies the new content in this S-CZ7.3.5 M1 Maintenance Release documentation.

Content Type	Description
Adaptation	Configurable Transaction Timeout for Register Method
Adaptation	SAR/UAR Suppression
Inherited Feature	Support of ATCF - 3GPP Rel 12 This support inherits 3 features: <ul style="list-style-type: none"> • SIP Feature Capabilities • SRVCC in Alerting Phase • ATCF INVITE ICSI Matching
Inherited Feature	Rx Interface Enhancement This support inherits 4 features: <ul style="list-style-type: none"> • Optimization of AAR Messages • NPLI during Registration • NPLI for SMS • Subscription for Notification of Signaling Path Status
Inherited Feature	Emergency Call Handling Enhancement This support inherits the IR.92 Multiple Emergency Numbers feature.

Configurable Transaction Timeout for REGISTER Requests

The I-CSCF function within Oracle's CSM, USM and SLRM allows the user to configure a device's I-CSCF functionality with a non-standard REGISTER expiry timer. On the Oracle CSM, USM, this is done on the **sip-registrar**. On the Oracle SLRM, this is done on the **1b-core-cfg**. Use of this setting allows the I-CSCF to select an alternative S-CSCF before the initial endpoint's request times out.

The default timeout for a REGISTER is 32 seconds. It may be desirable, however, to begin S-CSCF re-selection procedures sooner than 32 seconds if the first S-CSCF is not responsive. If the I-CSCF attempts to identify an alternative S-CSCF in less than 32 seconds, the endpoint does not have to issue a follow-up REGISTER.

Consider the example wherein the user configures the I-CSCF with a transaction timeout of 10 seconds. An endpoint attempts to register via P-CSCF and I-CSCF. The endpoint uses 32 seconds as its timeout for this transaction. The I-CSCF attempts to select an S-CSCF, using its timeout value of 10 seconds. If the S-CSCF fails to respond, the I-CSCF times out the request at 10 seconds and attempts to register via another S-CSCF. The second S-CSCF responds successfully and the I-CSCF initiates the reply to the endpoint's request within its 32 second timeout window.

For some deployments, the user must be careful not to set this too short. If the timer is too low, a Terminating Access Domain Selection (T-ADS) procedure on a Telecom Application Server (TAS) may never take place.


The user configures this transaction timeout on a per-registrar basis using the **icscfTransExpires** option. The syntax below shows the user configuring a CSM's or a USM's registrar with an expiry of 4 seconds.

```
ORACLE(sip-registrar)#options +icscfTransExpires=4
```


The syntax below shows the user configuring an SLRM's **lb-core-cfg** object with an expiry of 4 seconds.

```
ORACLE (lb-core-cfg) #options +icscfTransExpires=4
```

When this option is set, the system changes the client transaction expiry timer in the REGISTER it sends to the S-CSCF. Setting the option to 0 disables the function. The options value range is from 1 to 9999 seconds, although users are not expected to use any value higher than 31.

 **Note:** This option does not affect third party registrations or forwarding via local policy.

SAR/UAR Suppression

The Oracle USM provides the user with a means of reducing the amount of SAR/SAA and UAR/UAA traffic. The UAR suppression behavior is not compliant with TS 24.229, section 5.4.1.2.1, but may be preferred in some deployments. The user configures this behavior using **sip-registrar** options.

By default, the Oracle USM issues SAR messages for the following events:

- First time registration, with S-CSCF assigned
- New contact addition
- Contact updated (Replaced/Overwritten)
- Registration refresh after the expiry of the **location-update-interval** setting
- Registration cache expires for the last contact and the **force-unregistration** option is enabled in the **sip-config**
- Register message for an existing contact with:
 - A new call-id
 - A sequence number skipping a number
 - The UA capabilities changed
- Deregistration, after removal of last contact


The user can configure the system to reduce this SAR message traffic. The level of suppression is fixed by the system; the user either sets it on or off. With SAR suppression set, the Oracle USM only sends SARs when:

- The very first contact is added via registration
- The endpoint explicitly de-registers
- The last contact expires and the **force-unregistration** option is enabled.
- A registration refresh occurs upon the expiry of the **location-update-interval** value


The user configures SAR suppression with the following sip-registrar option:

```
ORACLE (sip-registrar) #options +sar-suppression-for-subseq-reg
```

This setting does not affect SAR handling for unregistered users, and has no impact on 3rd party registration.

 **Note:** This setting only refers to the **force-unregistration** option and the **location-update-interval** parameter for its functionality; it does not affect their behavior.


The user needs to be aware of a potential "split brain" scenarios with SAR suppression configured in a deployment that includes multiple contacts for a single AOR that are, for a variety of reasons, assigned to different Oracle USMs. If the HSS fails to issue RTRs for these users, the absence of the applicable SAR sequence can result in the contacts remaining registered via different Oracle USMs.

 **Note:** Per TS 29.228, section 8.1.1, *Cancellation of the old S-CSCF*, the HSS should send an RTR.

The user can also configure the system to reduce UAR message traffic. With the UAR suppression option set, the Oracle USM disables sending UARs upon receiving a registration refresh or deregistration and when both of the following conditions are true:

- The contact is in the cache
- The 'integrity-protected' parameter is not present in the authorization header

The resultant behavior prevents the system from issuing UARs, for example, in scenarios wherein the P-CSCF has not inserted the integrity protected parameter. This behavior can reduce the volume of UARs on the network.

 **Note:** The Oracle USM, when acting as a P-CSCF, internally sets the 'integrity-protected' parameter, based on the presence of the Authorization header and authorization type. This means that, in most Oracle USM deployment scenarios, enabling this option does not have any impact.

The user configures UAR suppression with the following sip-registrar option:

```
ORACLE (sip-registrar) #options +uar-suppression-for-no-integrity-protect
```

The system does not perform UAR suppression on registration requests that contain multiple contacts.

Support of ATCF - 3GPP Rel 12

This support inherits 4 features:

- SIP Feature Capabilities
- SRVCC in Alerting Phase
- ATCF INVITE ICSI Matching
- Subscription for Notification of Signaling Path Status

SIP Feature Capabilities

The ATCF can announce a feature capability in a message by transporting the information in the Feature-Caps header, which is supported by the Oracle USM.

The behavior of the two anchoring points, ATCF and ATGW, is defined by 3GPP in Release 12 of Technical Specification TS 24.237. Oracle Communications developed these functional entities based on the initial version of TS 24.237 Release 10, and has added the **sip-feature-caps** configuration element to align with Release 12. The element has three parameters:

- **state** — The value "enabled" triggers the feature and adds the Feature-Caps header to messages. The default value is "disabled".
- **atcf-management-uri** — identifies the feature capability indicator that will be used to transport the ATCF management URI. Possible values are "management" and "psi". The default value is "management". When the value is "management" and the value of state is "enabled", the Feature-Caps header "g.3gpp.atcf-mgmt-uri" is added and the value is the value of **atcf-psi-dn** in the **sip-config** configuration element. When the value is "psi" and the value of state is "enabled", the Feature-Caps header "g.3gpp.atcf-psi" is added and the value is the value of **atcf-psi-dn** in the **sip-config** configuration element.
- **atcf-alerting** — The value "enabled" adds the Feature-Caps header to messages and turns on the alerting feature. The default value is "disabled".

When **state** is set to "enabled", **atcf-management-uri** is empty, and **atcf-alerting** is set to "disabled", then the Feature-Caps header is added with:

- g.3gpp.atcf : value is configured STN-SR in **sip-config**
- g.3gpp.atcf-mgmt-uri: the value is **atcf-psi-dn** in **sip-config**
- g.3gpp.atcf-path: value is the ATCF URI for terminating requests
- g.3gpp.mid-call capability indicator

When **state** is set to "enabled", **atcf-management-uri** is set to "psi", and **atcf-alerting** is set to "disabled", then the Feature-Caps header is added with:

- g.3gpp.atcf : value is configured STN-SR in **sip-config**
- g.3gpp.atcf-psi: the value is **atcf-psi-dn** in **sip-config**
- g.3gpp.atcf-path: value is the ATCF URI for terminating requests
- g.3gpp.mid-call capability indicator

When **state** is set to “enabled”, **atcf-management-uri** is set to "management", and **atcf-alerting** is set to "disabled", then the Feature-Caps header is added with:

- g.3gpp.atcf : value is configured STN-SR in **sip-config**
- g.3gpp.atcf-mgmt-uri: the value is **atcf-psi-dn** in **sip-config**
- g.3gpp.atcf-path: value is the ATCF URI for terminating requests
- g.3gpp.mid-call capability indicator

When **state** is set to “enabled”, **atcf-management-uri** is set to "management", and **atcf-alerting** is set to "enabled", then the Feature-Caps header is added with:

- g.3gpp.atcf : value is configured STN-SR in **sip-config**
- g.3gpp.atcf-mgmt-uri: the value is **atcf-psi-dn** in **sip-config**
- g.3gpp.atcf-path: value is the ATCF URI for terminating requests
- g.3gpp.mid-call capability indicator
- g.3gpp.srvcc-alerting capability indicator

When **state** is set to “enabled”, **atcf-management-uri** is set to "psi", and **atcf-alerting** is set to "enabled", then the Feature-Caps header is added with:

- g.3gpp.atcf : value is configured STN-SR in **sip-config**
- g.3gpp.atcf-psi: the value is **atcf-psi-dn** in **sip-config**
- g.3gpp.atcf-path: value is the ATCF URI for terminating requests
- g.3gpp.mid-call capability indicator
- g.3gpp.srvcc-alerting capability indicator

If **sip-feature-caps** is disabled, the Oracle USM retains backward compatibility for environments not using SIP Feature Capability headers. Specifically, if the Oracle USM is using iFC-based third-party registration, it sends the third party register to the applicable AS with the original REGISTER and 200OK response embedded in the message. This embedded REGISTER would include a path header with the values the user has configured in the **sip-config**'s **atcf-stn-sr** and **atcf-psi-dn** parameters.

SIP Feature Capabilities Configuration

You can configure Oracle USMs to have the ATCF announce a feature capability in a message by transporting the information in the Feature-Caps header.

1. Access the **session-router** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# sip-feature-caps
ORACLE(sip-feature-caps)#
```

2. **state** — identifies whether to enable the feature and add the Feature-Caps header to messages. Possible values are "enabled" and "disabled". The default value is "disabled".
3. **atcf-alerting** — identifies whether to turn on the alerting feature and add the alerting Feature-Caps header to messages. Possible values are "enabled" and "disabled". The default value is "disabled".
4. **atcf-management-uri** — identifies the feature capability indicator that will be used to transport the ATCF management URI. Possible values are "management" and "psi". The default value is "management". When the value is "management" and the value of **state** is "enabled", the Feature-Caps header “g.3gpp.atcf-mgmt-uri” is added and the value is the value of **atcf-psi-dn** in the **sip-config** configuration element. When the value is "psi" and the value of **state** is "enabled", the Feature-Caps header “g.3gpp.atcf-psi” is added and the value is the value of **atcf-psi-dn** in the **sip-config** configuration element.

5. Type **done** to save your configuration.

SRVCC Handover Support in Alerting Phase

The Oracle USM supports handovers between Packet-Switched (PS) and Circuit-Switched(CS) networks for calls in an alerting phase; that is, a 180 ringing response for the initial INVITE has been sent or received and the SIP final response has not been sent or received.

The behavior of the two anchoring points, ATCF and ATGW, is defined by 3GPP in Release 12 of Technical Specification TS 24.237. Oracle Communications developed these functional entities based on the initial version of TS 24.237 Release 10, and has added the **sip-feature-caps** configuration element to align with Release 12.

To ensure that calls in an alerting phase are transferred between PS and CS networks, set the **sip-feature-caps** value as follows:

- Set **state** to "enabled"
- Set **atcf-management-uri** to "management" or "psi"
- Set **atcf-alerting** to "enabled"

For information on the results of these settings, refer to the *SIP Feature Capabilities* section.

ATCF INVITE ICSI Matching

The Oracle USM can check, on reception of an INVITE on an ingress sip-interface that has a configured ATCF and before applying any of the already implemented logic, whether the incoming INVITE includes the ICSI (Instantaneous Channel-State Information) of the requested service. The ATCF will be involved in the call flow when the configured ICSI value matches the ICSI value in the original INVITE; otherwise the handoff call will be rejected with code 480 (Temporarily Unavailable).

The system looks for the ICSI string in the following headers:

- P-Preferred-Service
- P-Asserted-Service
- Feature-Caps (within the "g.3gpp.icsi-ref" feature-capability indicator)
- Accept-Contact (within the tag-value within the g.3gpp.icsi-ref media feature tag)

An example of the ICSI string in the P-Preferred-Service or P-Asserted-Service header is "urn:urn-7:3gpp-service.ims.icsi.mmstel". Examples of the ICSI string in the Feature-Caps or Accept-Contact headers are "+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmstel" and "g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmstel". The ATCF will be involved in the call flow only when the ICSI matches. Configure the **atcf-icsi-match** parameter with the ICSI string you want to match. If **atcf-icsi-match** is blank, the check is not done and the behavior remains the same as before.

ATCF INVITE ICSI Matching Configuration

You can configure the Oracle USM to check, on reception of an INVITE on an ingress sip-interface that has a configured ATCF and before applying any of the already implemented logic, whether the incoming INVITE includes the ICSI (Instantaneous Channel-State Information) of the requested service and, if so, to involve the ATCF in the call flow.

1. Access the **sip-interface** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# sip-interface
ORACLE(sip-interface)#
```

2. Select the **sip-interface** object to edit.

```
ORACLE(sip-interface)# select
<RealmID>:
1: realm01 172.172.30.31:5060
```

```
selection: 1
ORACLE(sip-interface) #
```

3. **atcf-icsi-match** — enter the ICSI string you want to match.
4. Type **done** to save your configuration.

Rx Interface Enhancement

This support inherits 3 features:

- Optimization of AAR Messages
- NPLI during Registration
- NPLI for SMS

AAR Message Optimization

Currently, upon receiving an INVITE with a Proxy-Authorization header, the P-CSCF sends an Authorization-Authentication Request (AAR) message when the values of the **optimize-aar** and the **reserve-incomplete** parameters in the **ext-policy-server** configuration element are set to **enabled**. If the INVITE does not contain a Proxy-Authorization header then an AAR message is not sent. However, for mobile VoLTE, because IMS AKA is used for security there is no need to authenticate requests, so all INVITE messages are sent without Proxy-Authorization headers. This enhancement allows the P-CSCF to generate an AAR message when the INVITE is identified as coming from an IMS AKA user.

When the Oracle USM acts as a P-CSCF, the Diameter Rx interface updates bandwidth and addressing changes during a session. Many transactions between the P-CSCF and a PCRF server trigger a new SDP offer resulting in the transmission of an P-CSCF-initiated AA-Request (AAR) sent to the PCRF for the purpose of updating bearer parameters. However, not all transactions need to be reported to the PCRF, for example transactions that do not carry any bandwidth or addressing changes. In such instances, the issuance of an AAR is unnecessary and wasteful.

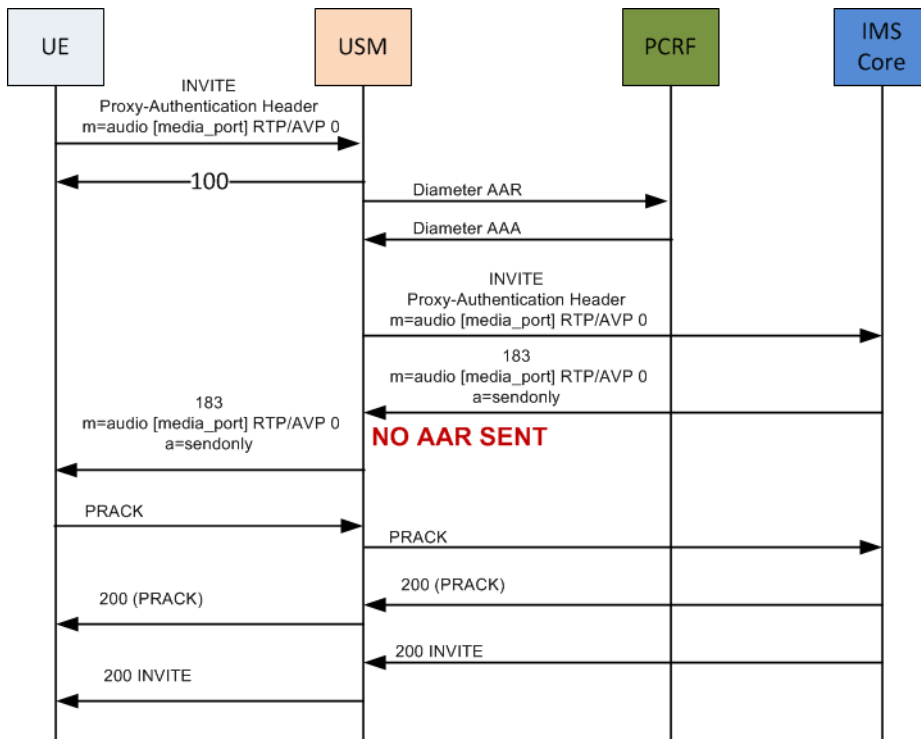
AAR message optimization (the suppression of unnecessary AARs) is activated by setting the **optimize-aar** parameter in the **ext-policy-server** configuration element to **enabled**.

If optimization is enabled, AARs are suppressed when:

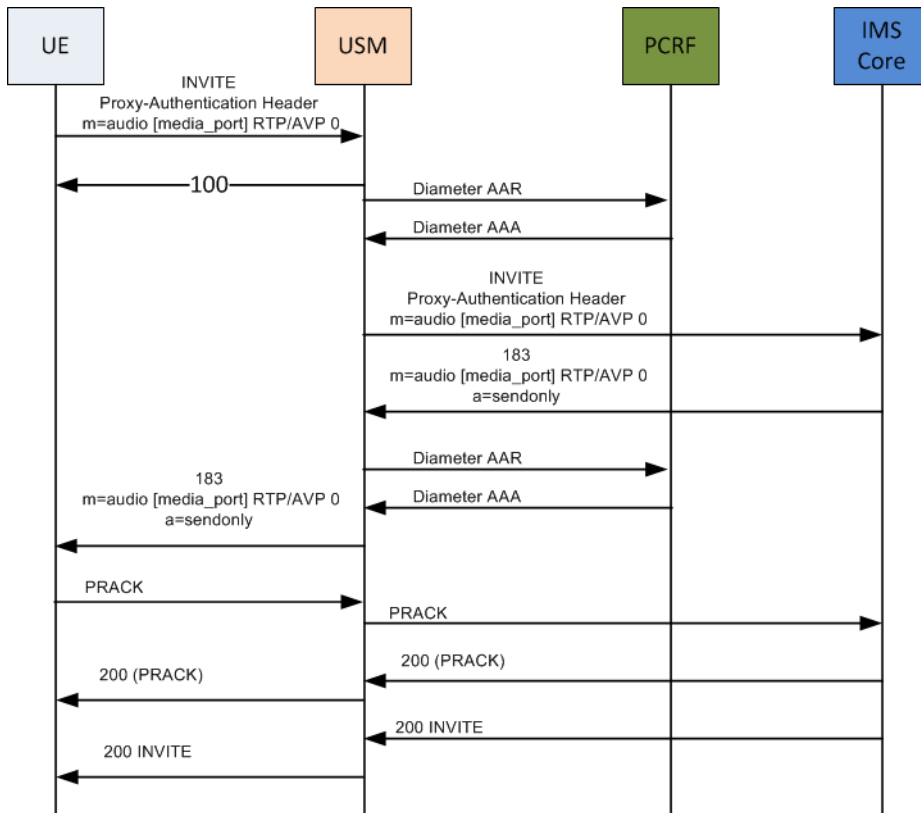
- the originating INVITE does not contain a proxy-authorization header, except for INVITE messages coming from IMS AKA users
- the codec & bandwidth provided in the m-line of an SDP response, and media IP address and port have not changed since the last SDP message
- In the MTC scenario, AAR is suppressed on reception of the originating non-IMS-AKA INVITE with no NPLI configured

AAR Optimization for Supplementary Services

In some call flows, a reINVITE or UPDATE request or response is sent to the P-CSCF and neither the bandwidth nor codec has changed. Such reINVITES or UPDATES may include SDP offers/answers with new a=sendonly, a=recvonly, or a=inactive. These SDP parameters are directly related to the provision of Supplementary Services such as Call Hold. By default the Oracle USM does not send an AAR to the PCRF for these changes.



The Oracle USM can be configured to allow the generation of an AAR in these cases by adding the **optimized-aar=supplementary-service** option to the **ext-policy-server** configuration element. (You may also configure the option as **optimized-aar= supplementary** resulting in identical behavior.) The following call flow reflects this optimized behavior.



AAR Message Configuration

To optimize the use of AAR messages:

1. Access the **ext-policy-server** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# media-manager
ORACLE(media-manager)# ext-policy-server
ORACLE(ext-policy-server)#
```

2. Select the **ext-policy-server** object to edit.

```
ORACLE(ext-policy-server)# select
<name>:1: name=extpoll

selection: 1
ORACLE(ext-policy-server)#
```

3. **optimize-aar**—Set this parameter to **enabled** to optimize the use of AAR messages.
4. **reserve-incomplete**—Set this parameter to **enabled** in conjunction with **optimize-aar** set to enabled for the system to not send an AAR to the PCRF if the Proxy-authorization header is absent from the INVITE.
5. Type **done** to save your configuration.

AAR Optimization with supplementary-service Configuration

This configuration sets the Oracle USM to send AAR messages to the PCRF when in a reINVITE or UPDATES the SDP offer/answer contains changes to the a=sendrecv, a=recvonly, a=sendonly, a=inactive lines lines.

1. Access the **ext-policy-server** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# media-manager
ORACLE(media-manager)# ext-policy-server
ORACLE(ext-policy-server)#
```


2. Select the **ext-policy-server** object to edit.

```
ORACLE(ext-policy-server)# select
<name>:1: name=extpoll

selection: 1
ORACLE(ext-policy-server)#
```

3. **options**—Set the options parameter by typing **options**, a space, **+optimized-aar=supplementary-service** to generate an AAR when a reINVITE or UPDATE contains SDP that changes an a=sendonly | recvonly | inactive parameter.

```
ORACLE(ext-policy-server)# options +optimized-aar=supplementary-service
```

 **Note:** You may also configure the option as **optimized-aar=supplementary** resulting in identical behavior.

If this option is not configured and **optimize-aar** is enabled, changes to these SDP parameters will not generate an AAR.

4. Type **done** to save your configuration.

Network Provided Location Information During Registration

For most cases, location information is relevant at the time of the session request. However, Network Provided Location Information (NPLI) upon REGISTER is required for some Authorization-Authentication Requests (AAR) and Authorization-Authentication Answers (AAA).

The access awareness feature in the Serving Call Session Control Function (S-CSCF) uses the P-Access-Network-Info header in the initial REGISTER request for selecting the registration and authentication

profile. This in turn depends on the access class of the IP Connectivity Access Network (IP-CAN) being used by the user equipment. For that reason, the Oracle USM Proxy Call Session Control Function (P-CSCF) requires that the Authorization-Authentication Answer (AAA) from the Policy Charging and Rules Function (PCRF) to contain the Radio Access Technology (RAT-type) Attribute Value Pair (AVP). It uses this information to populate the P-Access-Network-Info (PANI) header in the forwarded REGISTER request according to that value. The **npli-upon-register** parameter must be set to **enabled** for this behavior.

Example Call Flows

When user equipment(UE) registers to the third-party registrar based on the service profile, the Oracle USM buffers the incoming REGISTER and sends an AAR to the PCRF. The AAA from the PCRF contains a 3GPP-User-Location Info AVP: IP-CAN-Type and RAT-Type AVP. The Oracle USM uses those AVPs to populate a PANI header in the REGISTER that is forwarded to the registrar. The Oracle USM uses those AVPs to populate a PANI header in the REGISTER that is forwarded to the registrar.

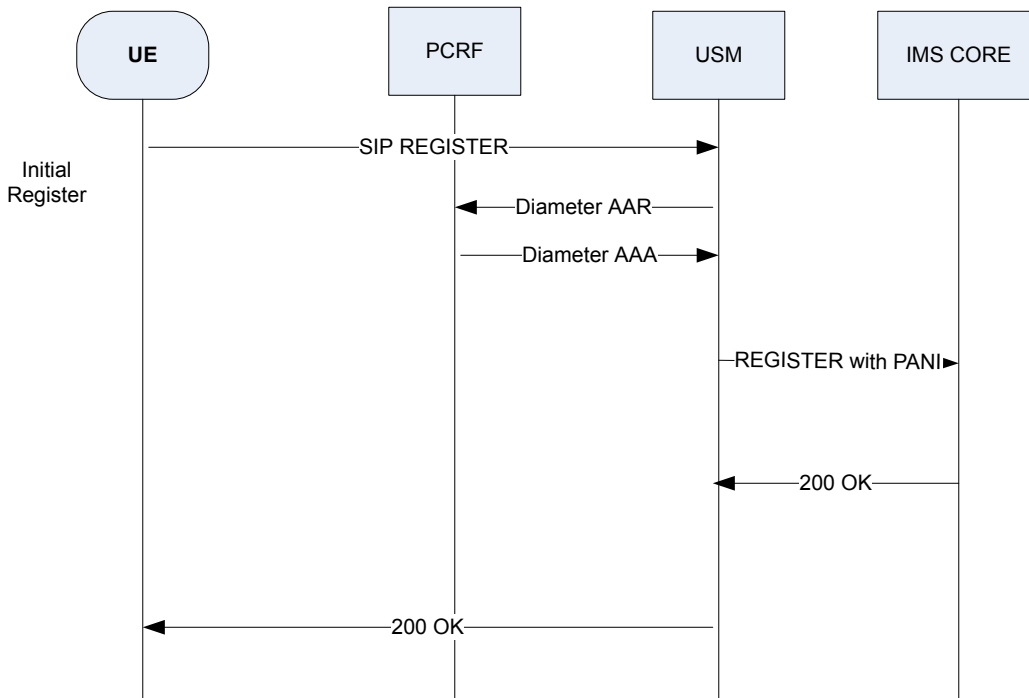


Figure 1: Initial Registration Flow

If a registration refresh is received before the half time of the registration expiration interval then the registration cache is not updated and the Oracle USM sends a 200 OK to the UE. No AAR is sent to the PCRF.

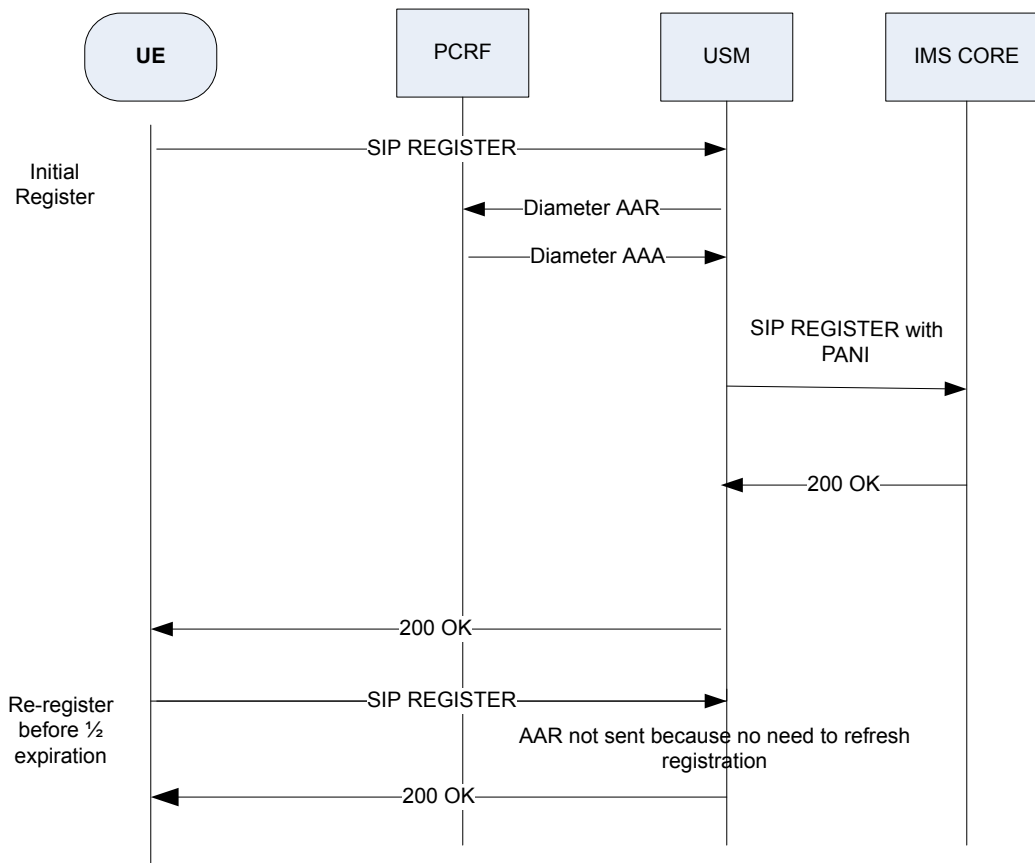


Figure 2: Re-Register before Half Time of Expiration

If a registration refresh is received after the half time of the registration expiration interval or if any registration information is changed then the Oracle USM will send an AAR to the PCRF. The AAA response from the PCRF contains a 3GPP-User-Location Info AVP: IP-CAN-Type and RAT-Type AVP. The Oracle USM will use the AVPs to populate a PANI header in the REGISTER that is forwarded to the third-party registrar.

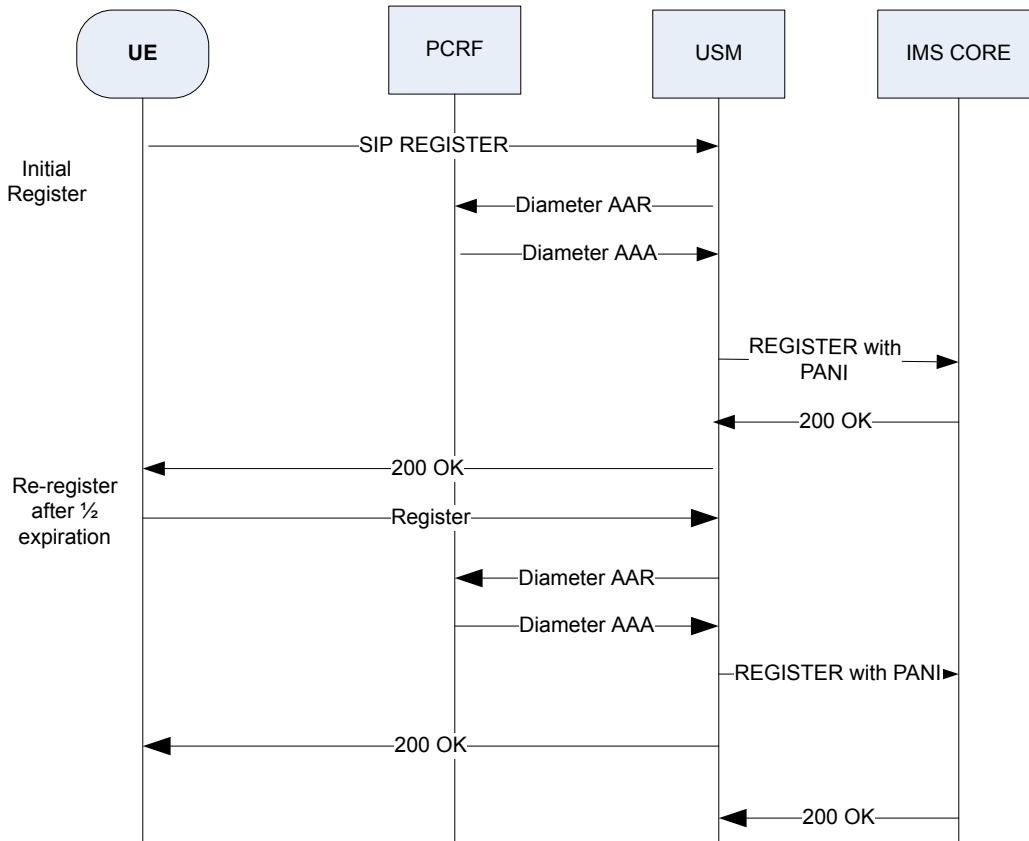


Figure 3: Re-Register after Half Time of Expiration

De-Register

When an endpoint removes all of its contacts from registration by sending a REGISTER with **expires=0**, the Oracle USM will buffer the incoming REGISTER and send an AAR to the PCRF. The AAA response from the PCRF contains a 3GPP-User-Location Info AVP: both IP-CAN-Type and RAT-Type AVP. The Oracle USM will use the AVPs to populate a PANI header in the REGISTER that is forwarded to the Registrar. The Oracle USM sends a STR message to the PCRF to terminate the session.

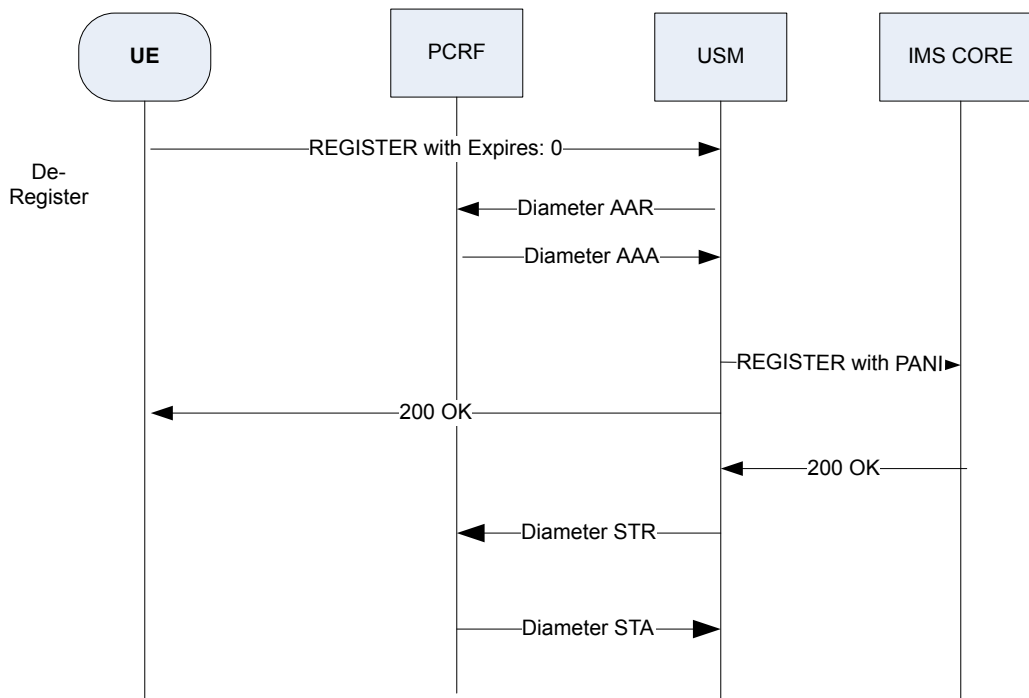


Figure 4: De-Registration

If the AAA is not received before the timeout, the AAA returns with an error, or the AAA is missing the required location information, then the Oracle USM will search the NPLI cache for cached location information to construct the PANI header to forward to the Registrar. If there is no cached location information, then the default-location-string configuration parameter will be used to create the PANI header. The default-location-string is obtained from the configuration in either the Realm or the SIP interface, with the Realm taking precedence; in both cases the value will be taken from the Access Realm. If the default-location-string is not set, then the REGISTER will be forwarded to the core without a PANI header.

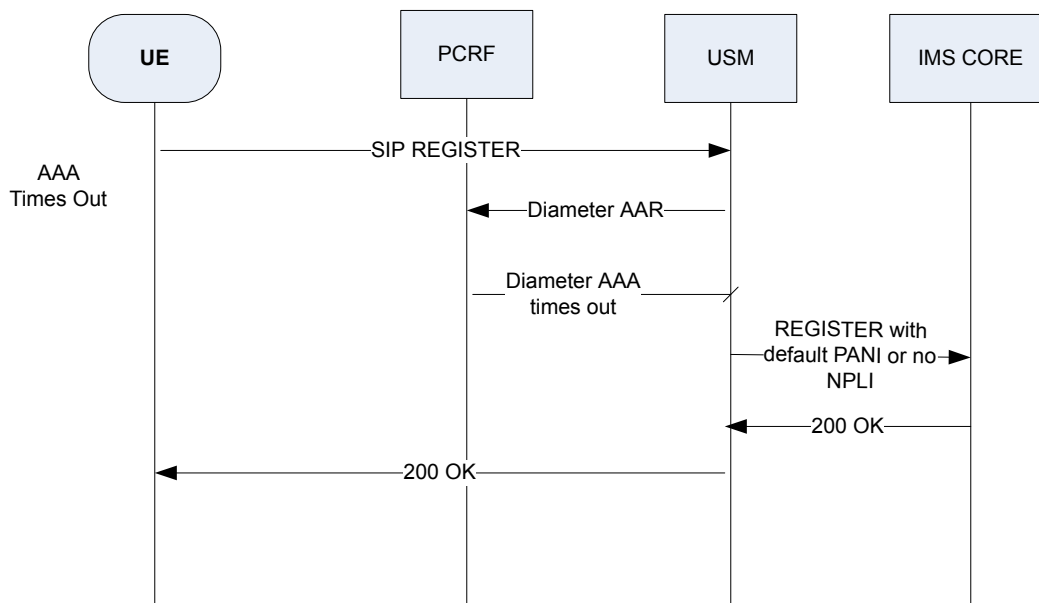


Figure 5: AAA Timeout/Error or AAA does not have Location Information

Register with IMS-AKA Enabled

If the IP Multimedia Subsystem Authentication and Key Agreement (IMS-AKA) is enabled then when a UE registers for the first time, the Oracle USM will reply with a 401 Authentication Required response. The UE and the PCRF will use the information in the 401 response to create a secure channel. The UE will then send a protected REGISTER that will trigger the Oracle USM to send an AAR to the PCRF. The AAA response from the PCRF contains a 3GPP-User-Location Information AVP: both IP-CAN-Type and RAT-Type AVP. The Oracle USM will use those AVPs to populate a PANI header in the REGISTER that is forwarded to the third-party registrar.

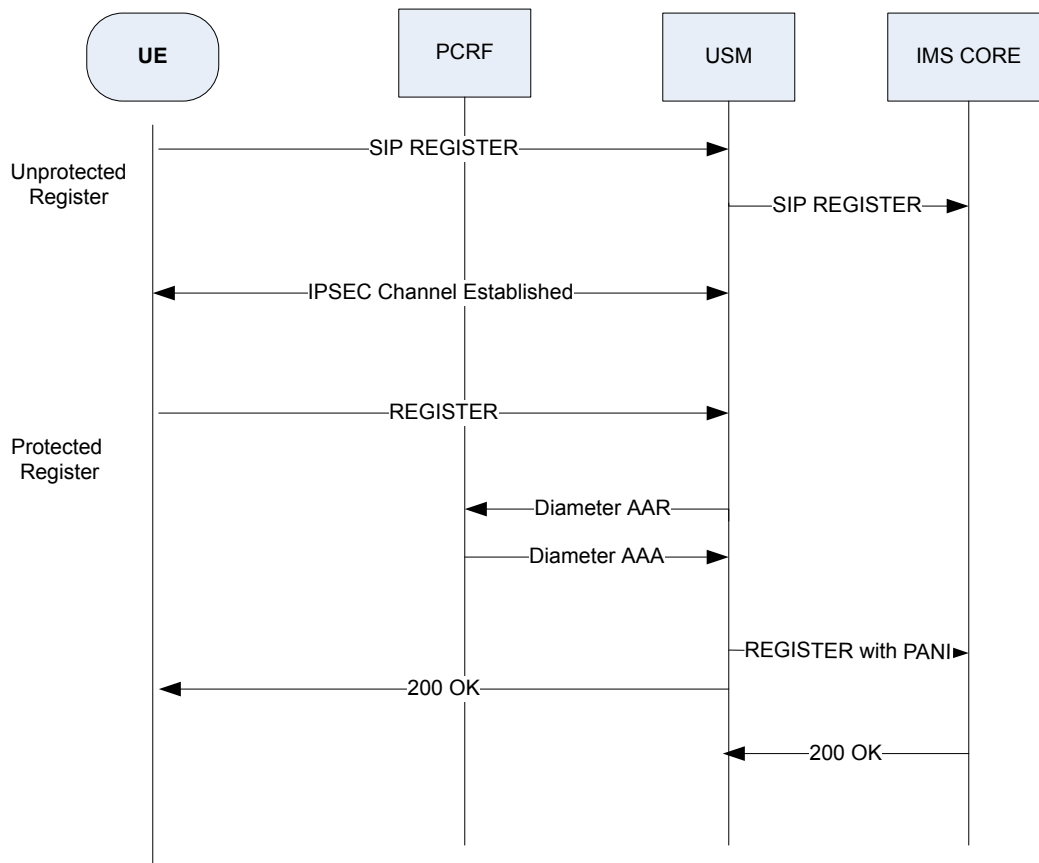


Figure 6: Register with IMS-AKA Enabled

Network Provided Location Information upon Register Configuration

Enable the `npli-upon-register` parameter to allow the capture of Network Provided Location Information during the registration process.

1. Access the `sip-config` configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# sip-config
ORACLE(sip-config)#
```

2. Select the `sip-config` object to edit.

```
ORACLE(sip-config)# select
ORACLE(sip-config)#
```

3. `npli-upon-register`— Enable to allow capture of Network Provided Location Information (NPLI) during the registration process

- `enabled` | `disabled`

4. Type **done** to save your configuration.

Network Provided Location Information for Short Message Service

For most cases, location information is relevant at the time of the session request. Network Provided Location Information (NPLI) for SIP is delivered by DIAMETER in Authentication-Authorization Answers (AAA) and Re-authentication-Authorization Requests (RAR). In certain countries, it is a regulatory requirement to provide location information also for the Short Message Service (SMS), which in LTE networks is implemented using the SIP MESSAGE method to carry the text.

The access awareness feature in the Serving Call Session Control Function (S-CSCF) uses the P-Access-Network-Information (PANI) header in the initial MESSAGE request for selecting the registration and authentication profile RAT-type and User Location Information. This in turn depends on the access class of the IP Connectivity Access Network (IP-CAN) being used by the user equipment (UE). For that reason, the Oracle USM Proxy Call Session Control Function (P-CSCF) requires that the Authorization-Authentication Answer(AAA) from the Policy Charging and Rules Function (PCRF) to contain IP-Can, the Radio Access Technology (RAT-type) and user location information attribute value pairs (AVPs). All three values are used to populate the PANI header in the forwarded MESSAGE request according to that value.

The Oracle USM P-CSCF will map User Location Information AVP and RAT type AVP into the PANI header for all subsequent SIP messages towards the core and acknowledge the RAA to the PCRF. The *np* parameter will be added to the PANI header to indicate a PANI header field is provided by a network element. This content can differ from a PANI header field without this parameter, which is provided by the UE. In the case the received message by the P-CSCF already contains information provided by the UE, that information will be preserved if **include-ue-loc-info** is enabled.

If the location information is not received from PCRF before the holding time expires, the Oracle USM will use the default location string if it is present as **default-location-string** in either the SIP Interface or Realm configuration.

Registration caching has to be enabled, e.g. **registration-caching=enabled**, for this feature to work. NPLI will be cached on a per-contact basis.

The **msghold-for-loc-info** object must be set to a non-zero value for this behavior. The location information will be held for no longer than the value set in **cache-loc-info-expire** unless the **keep-cached-loc-info-after-timeout** option is set

If this feature is disabled (i.e. **msg-hold-for-loc-info** = 0), SMS messages will not be held for NPLI and PANI headers will not be present in the SMS MESSAGES. There is no need to set **cache-loc-info-expire** in this case.

NPLI for Short Message Service Examples

The following scenarios illustrate the Oracle USM behavior when the Network Provided Location Information(NPLI) is not present in cache or the cached entry has expired. There are two types of scenarios: mobile originated(MO) and mobile terminated(MT). Descriptions precede each diagram.

MO message with NPLI information provided in the Authorization-Authentication Request and Answer(AAR/AAA) message and later updated with the Reauthorization-Reauthentication Request and Answer(RAR/RAA) message. Both AAA and RAR arrive within the holding period. The NPLI value is present in the P-Access Network Information (PANI) header.

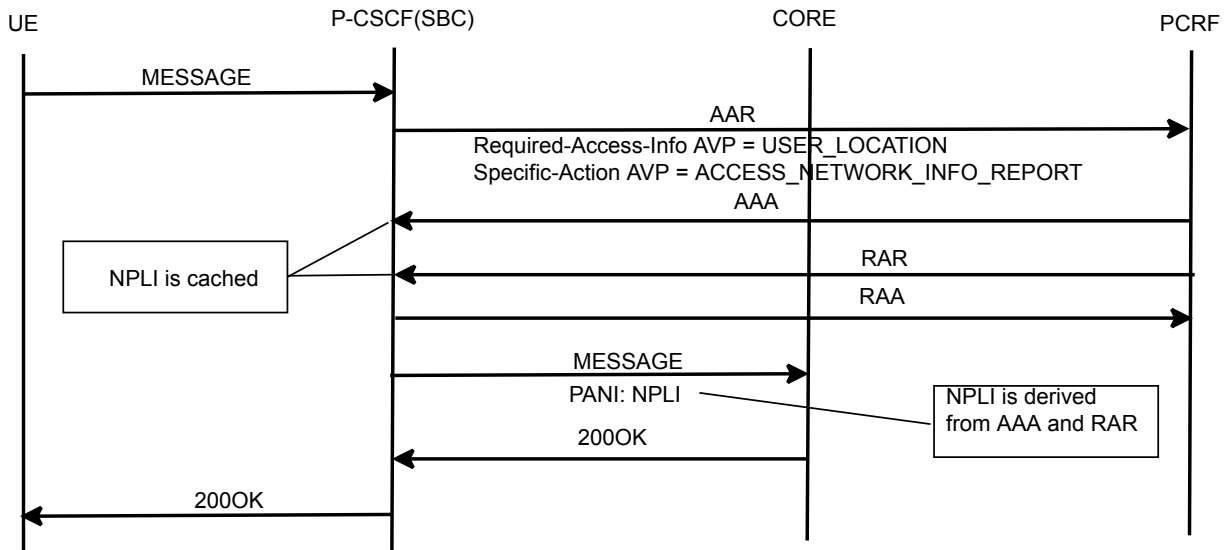


Figure 7: MO Message with AAR/AAA and RAR/RAR and within Holding Period

The below example shows a MO MESSAGE with NPLI information provided in the AAA, but the RAR arrives after the holding period expires. The NPLI value is present in the PANI header

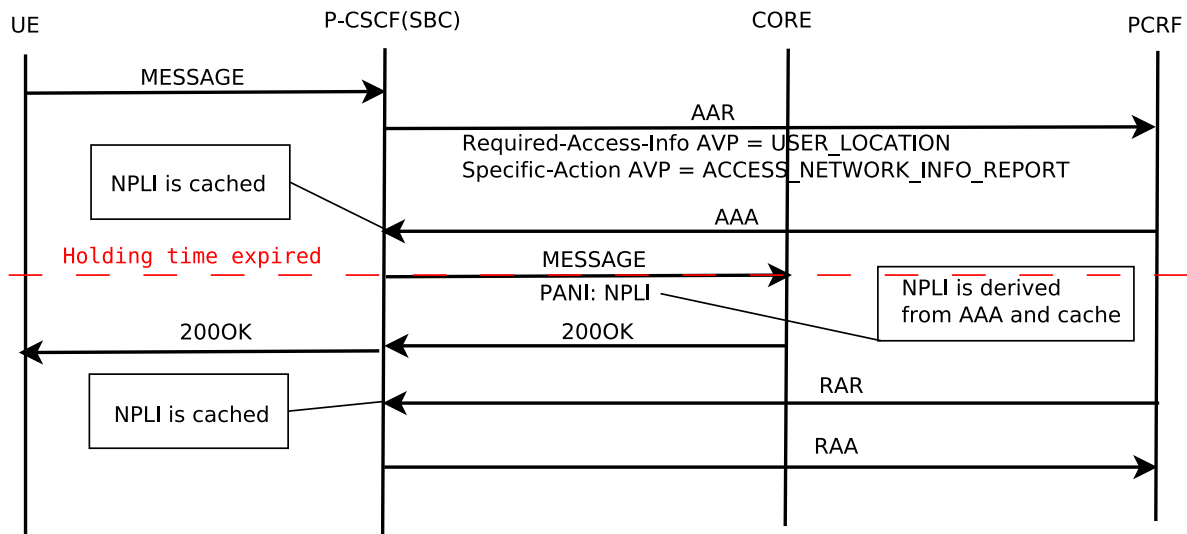


Figure 8: MO Message with AAR/AAA but RAR arrives after Holding Period

MO MESSAGE with no NPLI or cached NPLI. Both AAA and RAR arrive after the holding period expires.

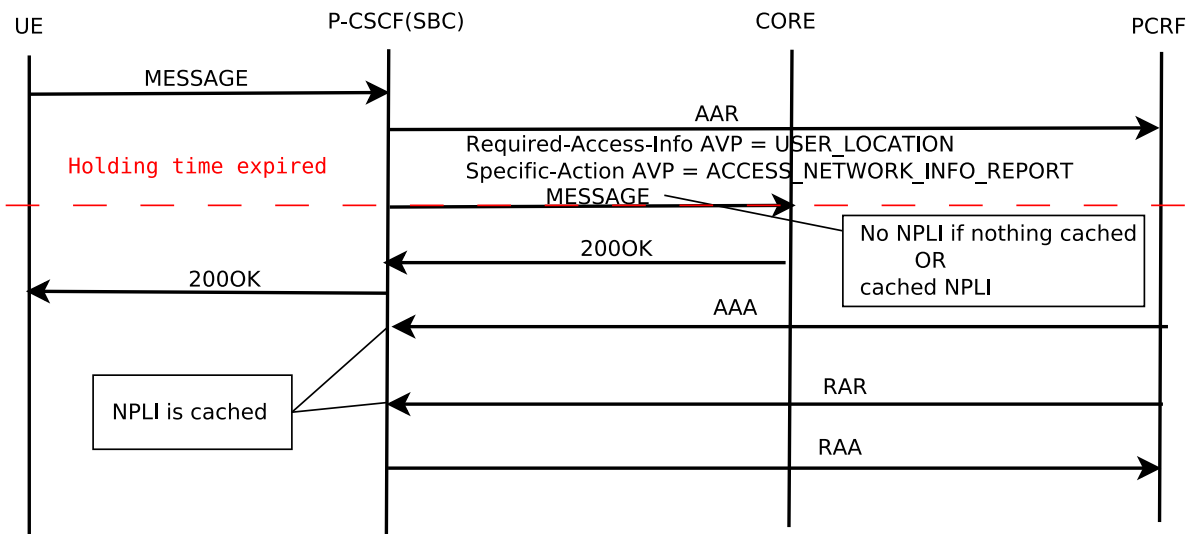


Figure 9: MO Message with no/cached NPLI; both AAR and RAR arrive after Holding Period

MT MESSAGE with NPLI provided in AAA and later updated with RAR. Both AAA and RAR arrive within the holding period. The NPLI value is present in the PANI header in 200OK response.

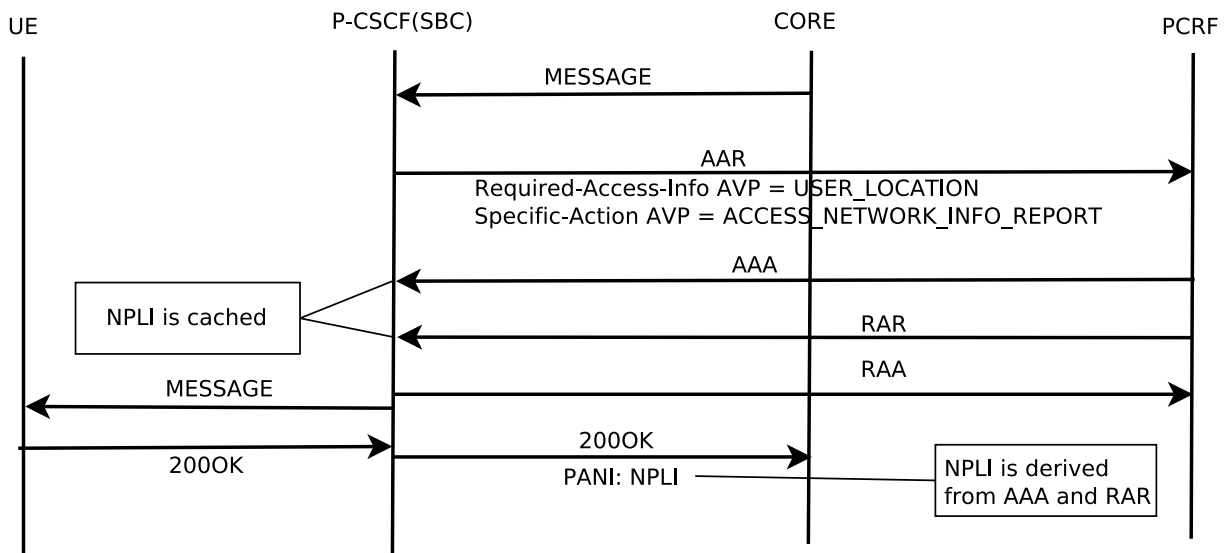


Figure 10: MT Message with NPLI in both AAR/AAA and RAR/RAA within the Holding Period

MT MESSAGE with NPLI provided in AAA, RAR arrives after the holding period expires. The NPLI value is present in the PANI header in 200OK response.

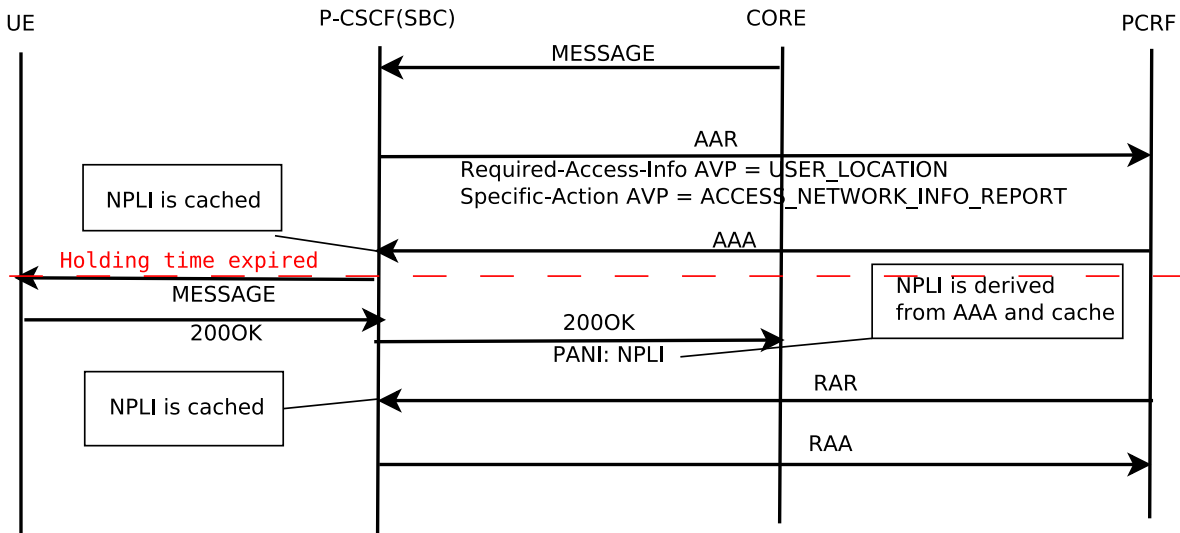


Figure 11: MT Message with NPLI provided in AAR/AAA, RAR arrives after Holding Period

MT MESSAGE with neither NPLI nor cached NPLI. Both AAA and RAR arrive after the holding period expires.

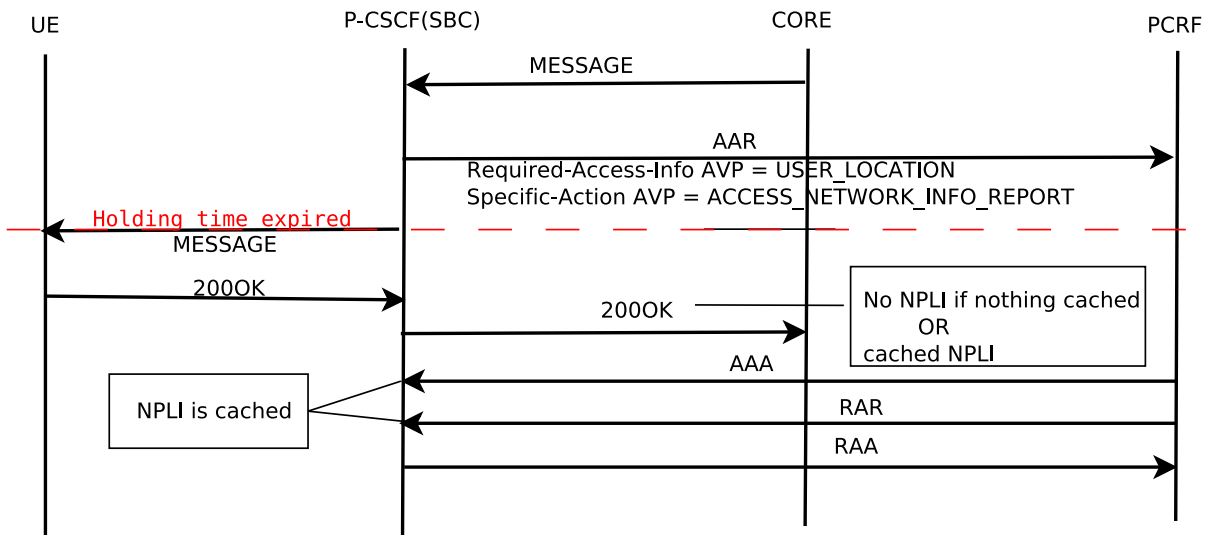


Figure 12: MT Message with no NPLI; both AAA and RAR arrive after the Holding Period

Network Provided Location Information present in Cache Examples

The following scenarios describe the Oracle USM behavior when the Network Provided Location Information (NPLI) is present in the cache.

MO MESSAGE cached NPLI value present in PANI header as the cached NPLI is current. Note that there is no AAR/AAA/RAR/RAA exchange.

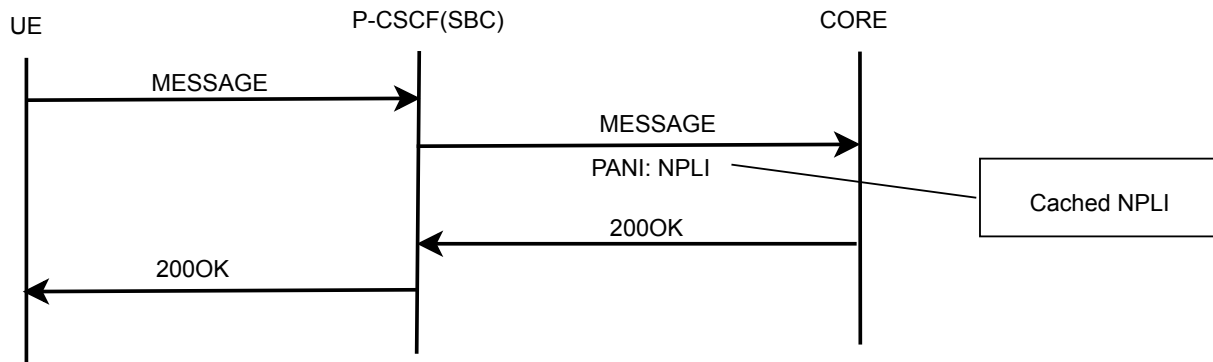


Figure 13: MO Message with cached NPLI in PANI Header

Mobile terminated(MT) MESSAGE cached NPLI included in PANI header as the cached NPLI is current. Note that there is no AAR/AAA/RAR/RAA exchange

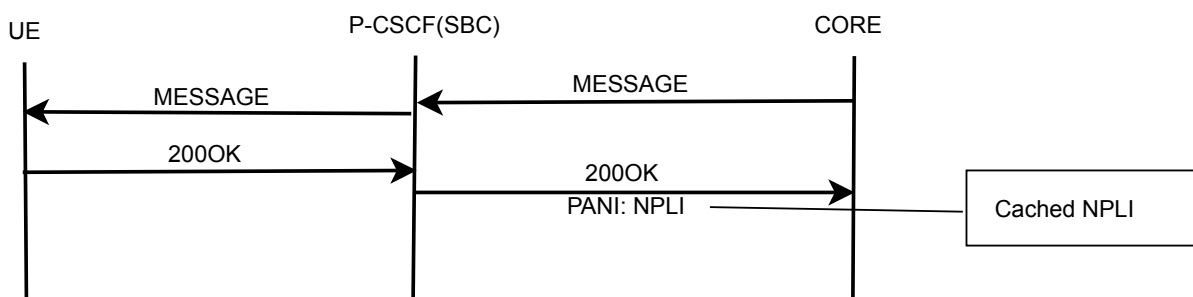


Figure 14: MT Message with cached NPLI in PANI header

NPLI for Short Message Configuration

Set to create a new or update the existing P-Access-Network Information (PANI) header based on the Network Provided Location Information (NPLI): values IP Connectivity Access Network (IP-CAN) , RAT-Type and user-location-information for SMS.

1. Access the **sip-config** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# sip-config
ORACLE(sip-config)#
```

2. Select the **sip-config** object to edit.

```
ORACLE(sip-config)# select
ORACLE(sip-config)#
```

3. **msg-hold-for-loc-info**— maximum number of seconds that the Oracle USM will hold MESSAGES for location information.

- 1-30— seconds
- 0— disabled; default

4. **cache-loc-info-expire**— number of seconds after which the Oracle USM will drop network location information.

- 1-4294967295— seconds
- 32— default

5. **keep-cached-loc-info-after-timeout**— If this option is enabled, the location information will be left in the cache and used in subsequent MESSAGES after the **cache-loc-info-expire** time expires.

options +keep-cached-loc-info-after-timeout

6. Type **done** to save your configuration.

Subscription for Notification of Signaling Path Status

The Oracle USM can explicitly open a flow for the signaling and through a subscription to this flow, provide status change notifications.

The Oracle USM supports provisioning of signaling flows to send a Authentication-Authorization Request (AAR) message to the Policy and Charging Rule Function (PCRF) when an endpoint registers, reregisters and deregisters. Service Providers want status information of the signaling flows to be able to react to state changes. By enabling the **specific-action-sig-flow-subscription** parameter, the Oracle USM subscribes for signaling flow status change notifications. The Policy and Charging Rule Function (PCRF) informs the Proxy Call Session Control Function (P-CSCF) when signaling flow state changes have taken place so that the P-CSCF can then take action, e.g. de-registering the User Equipment in the Serving Call Session Control Function (S-CSCF).

The Oracle USMP-CSCF supports the Specific Action attribute value pair (AVP) in conjunction with the AAR being sent to provision a signaling flow. The request to subscribe to this flow status change notifications will enable the handling of either `INDICATION_OF_LOSS_OF_BEARER` and/or `INDICATION_OF_RELEASE_OF_BEARER`, the two values of the specific action AVP.

Once enabled, the Oracle USM P-CSCF accepts the Re-Authentication Request (RAR) from the PCRF and its notification. The Oracle USM P-CSCF replies with a Re-Authentication Authorization acknowledging the RAR as per usual.

When the notification in the RAR is `INDICATION_OF_RELEASE_OF_BEARER`, the P-CSCF cancels the registration of that UE. The Oracle USM deletes the contact on `INDICATION_OF_RELEASE_OF_BEARER` only if this action is specified in the **specific-action-sig-flow-subscription** parameter settings. Further action is not taken when the RAR notification is "INDICATION_OF_LOSS_OF_BEARER" as the bearer can be re-established. This notification service is not available for VoLTE.

Subscription for Notification of Signaling Path Status Configuration

To enable **specific-action-sig-flow-subscription** to receive notifications regarding signal state change information.

1. Access the **ext-policy-server** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# media-manager
ORACLE(media-manager)# ext-policy-server
ORACLE(ext-policy-server)#
```

2. Select the **ext-policy-server** object to edit.

```
ORACLE(ext-policy-server)# select
<name>:1: name=extpoll

selection: 1
ORACLE(ext-policy-server)#
```

3. **specific-action-sig-flow-subscription**—Signaling path status changes information available for notification

- **loss of bearer**— Within a Re-authorization Request (RAR), this value shall be used when the server reports a loss of a bearer (e.g. in the case of General Packet Radio Service - Packet Data Protocol (GPRS PDP) context bandwidth modification to 0 kbit) to the Application Function (AF). The Service Data Flows (SDFs) that are deactivated as a consequence of this loss of bearer shall be provided within the Flows Attribute Value Pair (AVP). In the Authentication-Authorization Request (AAR), this value indicates that the AF requests the server to provide a notification at the loss of a bearer.
- **release of bearer**— Within a RAR, this value shall be used when the server reports the release of a bearer (e.g. PDP context removal for GPRS) to the AF. The SDFs that are deactivated as a consequence of this release of bearer shall be provided within the Flows AVP. In the AAR, this value

indicates that the AF requests the server to provide a notification at the removal of a bearer.tate where the bearer connection has been released.

4. Type **done** to save your configuration.

Emergency Call Handling Enhancement

This support inherits the IR.92 Multiple Emergency Numbers feature.

IR.92 Multiple Emergency Numbers

The Oracle USM expands compliance with the IR.92 standard by including an alternative service and message for emergency traffic.

The Oracle USM can be configured with multiple emergency services based on the dialed number match. Custom messages can be configured through the **sip-380-reason** parameter.

When an emergency call is received at the Oracle USM Proxy Call Session Control Function, the system checks any Network Management Control (NMC) rules that are enabled for the ingress realm. If the call matches a rule's **destination-identifier** parameter and fails with a 380 response, then that rule's **sip-380-reason** will be used in the response. Conversely, if the matching rule's **sip-380-reason** is empty or no matching NMC rule is found, then the value of the **sip-interface**'s **send-380-response** will be used as the reason. If the **send-380-response** is also empty, the default reason "priority calls not allowed" will be used. This logic also applies if the call fails and no matching network management control rule is found. The Oracle USM will use the value of the **sip-interface**'s **send-380-response** as the reason or the default message if the value is empty. The valid values for **send-380-response** are any string. It is not required.

This functionality is configured through the **sip-380-reason** parameter in the **net-management-ctrl** object.

IR.92 Multiple Emergency Numbers Configuration

To configure multiple emergency numbers and custom messages.

1. Access the **net-management-control** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# net-management-control
ORACLE(net-management-control)
```

2. Select the **net-management-control** object to edit.

```
ORACLE(net-management-control)# select
<name>:
1: NMC01 (type=priority)
2: NMC02 (type=priority)

selection: 1
ORACLE(net-management-control)#
```

3. **sip-380-reason** — Enter a reason phrase enclosed in quotes.
4. Type **done** to save your configuration.

S-CZ7.3.5 M2

This section provides descriptions, explanations, and configuration information for the contents of Maintenance Release S-CZ7.3.5M2. Maintenance Release content supercedes that distributed with the point release.

The following SPL engine versions are supported by this software:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.2.0
- C2.2.1
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3
- C3.1.4
- C3.1.5
- C3.1.6

Current patch baseline: S-CZ7.3.5M1

Patch Equivalency

Patch equivalency indicates which patch content in neighbor releases is included in this release. This can assure you in upgrading that defect fixes in neighbor stream releases are included in this release.

Neighbor Release Patch Equivalency for S-CZ7.3.5M2:

- S-CZ7.3.0m1p4

Content Map

The following table identifies the new content in this S-CZ7.3.5 M2 Maintenance Release documentation.

Content Type	Description
Adaptation	IMS Restoration Procedure Support
Adaptation	Session Continued Support
Adaptation	Limiting SLB-Managed Registrations by Endpoint Count
Inherited Feature	Advanced Logging
Inherited Feature	TCP Connection Tools

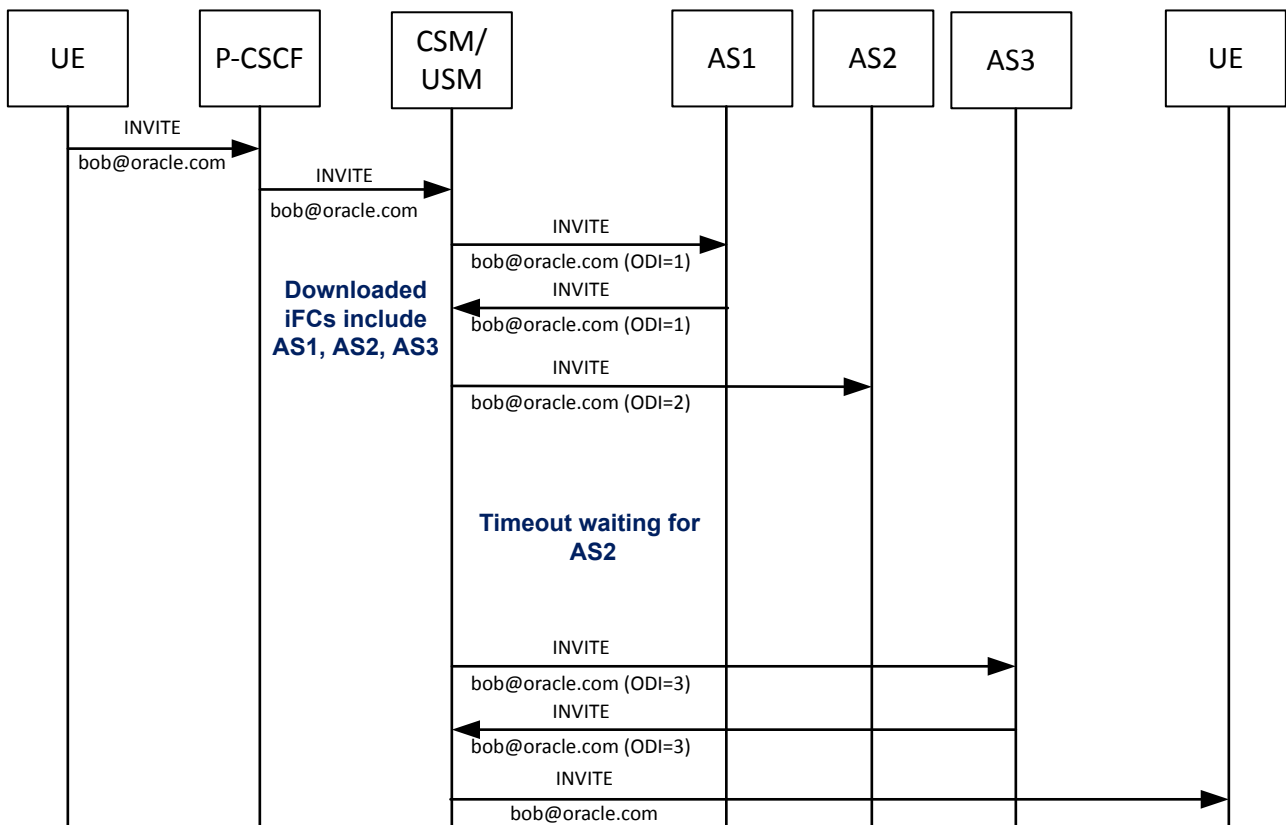
Session Continued Support

The Oracle Communications Core Session Manager (OCCSM) complies with 3GPP TS 29.228 with respect to third party registration and iFC DEFAULT_HANDLING. This support allows calls to proceed or terminate, based on AS availability, via iFC profile configuration option and the instructions in the iFC for each AS. If desired, the user can configure the system to bypass iFC default handling and always performing SESSION_TERMINATED when an AS fails to respond or responds with an error.

The Oracle USM responds according the 3GPP TS 29.228 when it finds iFC DEFAULT_HANDLING set to SESSION_TERMINATED, SESSION_CONTINUED, or absent in iFCs, as follows:

- The system performs SESSION_CONTINUED if iFC DEFAULT_HANDLING is not set or is set to SESSION_CONTINUED, proceeding with the call if the AS times out or responds with a 480 or 500 error.
- The system terminates a call if an AS iFC with DEFAULT_HANDLING set to SESSION_TERMINATED times out or responds with a 480 or 500 error.

The diagram below presents a call scenario wherein AS2 does not respond to the INVITE. In this case, the AS iFC had DEFAULT HANDLING set to SESSION_CONTINUED or did not include a default handling setting. The call succeeds, with AS1 and AS3 services available to it.



The user can disable session continued support using the `ifc-profile-config`'s `disable-session-continued` option. With this option set, the system always performs `SESSION_TERMINATED` procedures in response to unresponsive AS servers, regardless of `DEFAULT_HANDLING` settings in the iFC.


```
ORACLE (ifc-profile-config) #options +disable-session-continued
```

The system replicates this real-time configuration across HA pairs.

The user must also set the `sip-interface`'s `initial-invite-trans-expire` timer, which defaults to zero, to specify the amount of time it waits for an AS to respond.

```
ORACLE (sip-interface) #initial-invite-trans-expire
```

The user should set this value to be less than the `sip-interface`'s `trans-expire` timer to ensure that the system has a chance to connect with the remaining ASs before the transaction expires.

 **Note:** The Oracle USM does not currently support the `SESSION_TERMINATED` component of this feature for third party deregistration.

Limiting SLB-Managed Registrations by Endpoint Count

By default, the Oracle Communications Subscriber Aware Load Balancer (SLB) manages registration load distributed to a Oracle USM (USM) using the `sip-config`'s `registration-cache-limit`. Because a Oracle USM's contact count is not the same as the endpoint count tracked on the SLB, an SLB may attempt to over-subscribe a Oracle USM, resulting in rejected registrations. The user can configure a `sip-config` option, called `max-lb-endpoints-set`, to specify the endpoint count that the SLB must honor, and reduce the possibility of over-subscription.

By default, the Oracle USM provides the SLB with its registration cache limit when it registers itself with the SLB. The SLB then uses this number to manage the number of registrations it sends to that Oracle USM. Alternatively, the user can configure the Oracle USM to provide the SLB with the preferred value.

The user configures this maximum endpoint value using the **max-lb-endpoints-set** option. The syntax below shows the user configuring this option to a maximum of 30,000 endpoints.

```
ORACLE (sip-config) #options +max-lb-endpoints-set=30000
```

This option is real-time configurable and is supported within HA deployments.

Advanced Logging

Advanced Logging allows targeted logging by overriding log levels, so that only a specific SIP request and its related messages are logged. The system matches criteria that you configure to determine which requests to log. The system also logs all messages related to the request, such as any responses, in-dialog messages, media, timers, and so on. Advanced Logging supports multiple matching criteria for incoming requests and rate limiting. Advanced log files are smaller than debug files because the system logs only the specified number of matches in the specified period of time. Since the files are smaller, Advanced Logging uses fewer system resources than debug logging. To make searching easier, the system labels each log.

You can deploy advanced logging via configuration. Define `sip-advanced-logging` under `session-router`. This method reconfigures the system and the configuration persists after a system reboot.

The system provides the following options for configuring the scope of advanced logging.

- Request-only. Logs only the matched message.
- Transaction. Logs only the request and the response.
- Session. Logs the matched message and anything else related to the session.
- Session and Media. Logs the matched message, anything related to the session, and media.

The system provides the following options for configuring the advanced logging criteria.

- Received Session-Agent. By IP address or hostname
- Request Type. Such as INVITE vs. SUBSCRIBE
- Received Realm Name.
- Request URI. User and host. Limited to 2 condition entries, when using both types.
- To header. User and host. Limited to 2 condition entries, when using both types.
- From header. User and host. Limited to 2 condition entries, when using both types.
- Call-id. Matches the Call-id header.
- Rate Limiting. By specified number of matched requests over a specified period of time.
- Scope of Logging. Options include Request Only, Transaction, All Relating to Session, All Relating to Session and Media.

 **Note:** This function logs messages from the Oracle USM's `Atcpd`, `Ebmd`, `Lrtd`, `Radd`, and `Sipd` processes.

Configuring Advanced Logging

From Configure mode, define `sip-advanced-logging` and `advanced-log-condition`. The criteria that you configure remaps the message logging and modifies the system configuration. You must save and activate the changes to the configuration.

When configuring multiple `sip-advanced-logging` configurations, note the following:

- The system evaluates each configuration individually in an **OR** relationship.
- The system evaluates all conditions and they must all match in an **AND** relationship.

1. Access the **ifc-profile** configuration element.

```
ORACLE# configure terminal
ORACLE (configure) # session-router
ORACLE (session-router) # sip-advanced-logging
ORACLE (sip-advanced-logging) #
```


2. Configure the following parameters.

- Name. Name to display on the log message for this set of criteria.
- State. Activates or deactivates this advanced logging object.
- Level. Type one: zero, none, emergency, critical, major, minor, warning, notice, info, trace, debug, or detail.
- Scope. Type one: request-only, transaction, session, or session-and-media.
- Matches-per-window. Type a number between 1 and 999999999 for how many matches to log per window of time.
- Window-size. Type a number between 1 and 999999999 seconds for the length of time the logging window is open.
- Type conditions.

The system displays the adv-log-condition subelement.

3. Select the **sip-advanced-logging > conditions** object to edit, or create a new one.

```
ORACLE(sip-advanced-logging)# adv-log-condition
ORACLE(adv-log-condition)# select
<name>:
1: name=condition1
ORACLE(adv-log-condition)#
```

4. From the adv-log-condition prompt, configure the following:

- Match-type. Type one or more of the following sip objects with either the "and" or the "or" operator between objects: request-type, recv-agent, recv-realm, request-uri-user, request-uri-host, to-header-user, to-header-host, from-header-user, from-header-host, or call-id.
- Match-value. Type the incoming message text string that you want to match.

For example, to match "To-header-user" to the value 1234@<companyname>.com, type "to-header-user" for Match type and type " 1234" for Match value.

 **Note:** The match-value parameter does not support regex expressions.

5. Type **done** (twice) to retain your sub-element and element configuration.

6. Exit, save, and activate.

sip-advanced-logging

The sip-advanced-logging configuration element allows you to configure advanced logging objects on the Oracle USM.

Parameters

name	Name to display on the log message for this set of criteria.
level	Log level for this advanced logging set of criteria. This corresponds to the system's available log levels. <ul style="list-style-type: none"> • Default: DEBUG • Values: ZERO NONE EMERGENCY CRITICAL MAJOR MINOR WARNING NOTICE INFO TRACE DEBUG DETAIL
scope	The range of SIP messages and, if configured, media for which this advanced logging criteria creates log messages. <ul style="list-style-type: none"> • Default: session-and-media • Values: request-only transaction session session-and-media

matches-per-window	The number of matches, within the window size, for which the system generates log messages. <ul style="list-style-type: none">• Default: 1• Values: An integer between 1 and 999999999
window-size	The amount of time, in seconds, to sample for matches within the traffic. <ul style="list-style-type: none">• Default: 1• Values: An integer between 1 and 999999999
condition	Type this parameter to enter the adv-logging-conditions subelement. Specify the match criteria for which the system creates log messages. Each logging criteria set supports multiple match conditions.


Path: **sip-advanced-logging** is an element of the session-router path. The full path from the topmost CLI prompt is: configure terminal > session-router > sip-advanced-logging.

Release

First appearance: E-C7.1.0

RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

sip-advanced-logging > condition

The sip-advanced-logging's condition subelement allows you to configure multiple sets of matching criteria for the associated sip-advanced-logging element on the Oracle USM.

Parameters

match-type	A string identifying the type of information within the SIP message on which the system attempts to find a matching value. <ul style="list-style-type: none">• Default: rcv-agent• Values: request-type rcv-agent rcv-realm request-uri-user request-uri-host to-header-user to-header-host from-header-user from-header-host
match-value	A string the system uses as the matching string within the SIP message. <ul style="list-style-type: none">• If the match-type is "request-type", valid values include:<ul style="list-style-type: none">• REGISTER INVITE ACK BYE CANCEL PRACK OPTION INFO SUBSCRIBE NOTIFY REFER UPDATE MESSAGE PUBLISH• For all other match-types, enter the string the system must find in the message.

Path: **adv-log-condition** is a subelement of the sip-advanced-logging element. The full path from the topmost CLI prompt is: configure terminal > session-router > sip-advanced-logging > condition.

Release

First appearance: E-C7.1.0

RTC Status

Supported



Note: This is a multiple instance configuration subelement.

TCP Connection Tools

Transmission Control Protocol (TCP) connection tools can assist you in gauging performance, identifying potential memory leaks, and debugging connections for performance tracking and improvement.

The **show ip tcp** command shows the following socket connections by state:

- inbound
- outbound
- listen
- IMS-AKA (Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.)

The **show sipd tcp** and **show sipd tcp connections** commands display counters to track usage. Use the **reset sipd** command to reset the counters.

TCP and SCTP State Connection Counters

The Oracle USM (Oracle USM) can provide systemwide counts of Transmission Control Protocol (TCP) and Stream Control Transmission Protocol (SCTP) states by way of the **show ip tcp** and **show ip sctp** commands from the ACLI.

The **show ip tcp** command includes the following section of counters that correspond to counts of TCP states per active connections, including counts differentiated by inbound, outbound, listen and IMS-AKA connections.



Note: Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.

Connections By State:

```

0      CLOSED
0      LISTEN
0      SYN_SENT
0      SYN_RCVD
0      ESTABLISHED
0      CLOSE_WAIT
0      FIN_WAIT_1
0      CLOSING
0      LAST_ACK
0      FIN_WAIT_2
0      TIME_WAIT

```

Inbound Socket Connection By State:

```

0      CLOSED
0      LISTEN
0      SYN_SENT
0      SYN_RCVD
50     ESTABLISHED
0      CLOSE_WAIT
0      FIN_WAIT_1
0      CLOSING
0      LAST_ACK
0      FIN_WAIT_2
0      TIME_WAIT

```

Outbound Socket Connection By State:

```

0      CLOSED
0      LISTEN

```

```
0 SYN_SENT
0 SYN_RCVD
1 ESTABLISHED
0 CLOSE_WAIT
0 FIN_WAIT_1
0 CLOSING
0 LAST_ACK
0 FIN_WAIT_2
0 TIME_WAIT
```

Listen Socket Connection By State:

```
0 CLOSED
2 LISTEN
0 SYN_SENT
0 SYN_RCVD
0 ESTABLISHED
0 CLOSE_WAIT
0 FIN_WAIT_1
0 CLOSING
0 LAST_ACK
0 FIN_WAIT_2
0 TIME_WAIT
```

IMSAKA Inbound Socket Connection By State:

```
0 CLOSED
0 LISTEN
0 SYN_SENT
0 SYN_RCVD
0 ESTABLISHED
0 CLOSE_WAIT
0 FIN_WAIT_1
0 CLOSING
0 LAST_ACK
0 FIN_WAIT_2
0 TIME_WAIT
```

IMSAKA Outbound Socket Connection By State:

```
0 CLOSED
0 LISTEN
0 SYN_SENT
0 SYN_RCVD
0 ESTABLISHED
0 CLOSE_WAIT
0 FIN_WAIT_1
0 CLOSING
0 LAST_ACK
0 FIN_WAIT_2
0 TIME_WAIT
```

IMSAKA Listen Socket Connection By State:

```
0 CLOSED
0 LISTEN
0 SYN_SENT
0 SYN_RCVD
0 ESTABLISHED
0 CLOSE_WAIT
0 FIN_WAIT_1
0 CLOSING
0 LAST_ACK
0 FIN_WAIT_2
```

```
0    TIME_WAIT
```

```
Number of Connections Counted = 0
Maximum Connection Count = 0
Maximum Number of Connections Supported = 220000
```

The **show ip sctp** command includes the following section of counters that correspond to counts of SCTP states per active connections.

```
Connections By State:
```

```
0    CLOSED
0    BOUND
0    LISTEN
0    COOKIE_WAIT
0    COOKIE_ECHOED
0    ESTABLISHED
0    SHUTDOWN_SENT
0    SHUTDOWN_RECEIVED
0    SHUTDOWN_ACK_SENT
0    SHUTDOWN_PENDING
```

```
Number of Connections Counted = 0
Maximum Connection Count = 0
Maximum Number of Connections Supported = 10000
```

The output of the state counters indicates the number of connections currently in each state. The statistics from the counters do not accumulate like many of the other statistics in the **show ip** command tree. Most states are ephemeral, and you may see many "0" counters for states other than LISTEN and ESTABLISHED.

show sipd tcp connections

The **show sipd tcp connections** command displays Transmission Control Protocol (TCP) connection information details on remote and local address/port and connection states for analysis. Oracle recommends that you use the command only during non-peak times or maintenance windows.

The **show sipd tcp connections** command displays all SIP/TCP connections including each connection's direction, type, state, local and remote addresses, SIP interface and IMS-AKA details. Arguments include:

- sip-interface—Optional parameter that limits output to sockets in the specified sip-interface
- start start—Integer indicating which connection to start displaying. This can be a negative number. When the number selected for the start variable is greater than the number of TCP connections, the system displays nothing.
- start-count start—Integer as per above plus the count integer, specifying how many TCP connections to display from the start.
- all—Display all of the sipd tcp connections. Exercise caution due to the possibility of consuming all CPU time; preferably use during a maintenance window

 **Note:** Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.

For example:

```
ORACLE# show sipd tcp connections
```

```
sipd tcp connections
```

Dir	Type	State	Local Address	Remote Address	sip-
	interface-id	isImsaka			
	LISTEN	TCP_LISTENING	172.16.101.149:5060		
net172					
in	FORKED	TCP_CONNECTED	172.16.101.149:5060	172.16.23.100:51678	
net172					

```

in FORKED TCP_CONNECTED 172.16.101.149:5060 172.16.23.100:51679
net172
[...]
in FORKED TCP_CONNECTED 172.16.101.149:5060 172.16.23.100:51727
net172
in FORKED TCP_CONNECTED 172.16.101.149:5060 172.16.23.100:51728
net172
in FORKED TCP_CONNECTED 172.16.101.149:5060 172.16.23.100:51729
net172
LISTEN TCP_LISTENING 192.168.101.149:5060
net192
out CONNECT TCP_CONNECTED 192.168.101.149:8192 192.168.23.100:5060
net192

Connections Displayed: 53
Total Connections: 53

```

show sipd tcp

The **show sipd tcp** command displays TCP connection state information for the following:

- inbound
- outbound
- listen
- total
- IMS-AKA (Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.)

For example:

```

ORACLE# show sipd tcp
11:11:54-110
SIP TCP Sockets
Active High Total Total PerMax High
All States 53 53 108 108 108 53
TCP_INITIAL 0 0 0 0 0 0
TCP_STARTING 0 0 0 0 0 0
TCP_AVAILABLE 0 1 51 51 51 1
TCP_BOUND 0 1 3 3 3 1
TCP_CONNECTED 51 51 51 51 51 51
TCP_CONNECTING 0 1 1 1 1 1
TCP_LISTENING 2 2 2 2 2 2
TCP_DISCONNECT 0 0 0 0 0 0
TCP_CLOSED 0 0 0 0 0 0

-----
SIP Inbound TCP Sockets
Active High Total Total PerMax High
All States 50 50 100 100 100 50
TCP_INITIAL 0 0 0 0 0 0
TCP_STARTING 0 0 0 0 0 0
TCP_AVAILABLE 0 1 50 50 50 1
TCP_BOUND 0 0 0 0 0 0
TCP_CONNECTED 50 50 50 50 50 50
TCP_CONNECTING 0 0 0 0 0 0
TCP_LISTENING 0 0 0 0 0 0
TCP_DISCONNECT 0 0 0 0 0 0
TCP_CLOSED 0 0 0 0 0 0

```

```

-----
SIP Outbound TCP Sockets      -- Period --  ----- Lifetime -----
                                Active   High   Total      Total  PerMax   High
All States                    1       1       4         4      4        1
TCP_INITIAL                   0       0       0         0      0        0
TCP_STARTING                   0       0       0         0      0        0
TCP_AVAILABLE                 0       1       1         1      1        1
TCP_BOUNDED                    0       1       1         1      1        1
TCP_CONNECTED                  1       1       1         1      1        1
TCP_CONNECTING                 0       1       1         1      1        1
TCP_LISTENING                  0       0       0         0      0        0
TCP_DISCONNECT                 0       0       0         0      0        0
TCP_CLOSED                     0       0       0         0      0        0
-----

```

```

-----
SIP Listen TCP Sockets       -- Period --  ----- Lifetime -----
                                Active   High   Total      Total  PerMax   High
All States                    2       2       4         4      4        2
TCP_INITIAL                   0       0       0         0      0        0
TCP_STARTING                   0       0       0         0      0        0
TCP_AVAILABLE                 0       0       0         0      0        0
TCP_BOUNDED                    0       1       2         2      2        1
TCP_CONNECTED                  0       0       0         0      0        0
TCP_CONNECTING                 0       0       0         0      0        0
TCP_LISTENING                  2       2       2         2      2        2
TCP_DISCONNECT                 0       0       0         0      0        0
TCP_CLOSED                     0       0       0         0      0        0
-----

```

IMS-AKA portion of show sipd tcp command:

```

ORACLE# show sipd tcp
15:28:51-197
[...]
```

```

-----
SIP IMSAKA In TCP Sockets    -- Period --  ----- Lifetime -----
                                Active   High   Total      Total  PerMax   High
All States                    0       0       0         0      0        0
TCP_INITIAL                   0       0       0         0      0        0
TCP_STARTING                   0       0       0         0      0        0
TCP_AVAILABLE                 0       0       0         0      0        0
TCP_BOUNDED                    0       0       0         0      0        0
TCP_CONNECTED                  0       0       0         0      0        0
TCP_CONNECTING                 0       0       0         0      0        0
TCP_LISTENING                  0       0       0         0      0        0
TCP_DISCONNECT                 0       0       0         0      0        0
TCP_CLOSED                     0       0       0         0      0        0
-----

```

```

-----
SIP IMSAKA Out TCP Sockets   -- Period --  ----- Lifetime -----
                                Active   High   Total      Total  PerMax   High
All States                    0       0       0         0      0        0
TCP_INITIAL                   0       0       0         0      0        0
TCP_STARTING                   0       0       0         0      0        0
TCP_AVAILABLE                 0       0       0         0      0        0
TCP_BOUNDED                    0       0       0         0      0        0
TCP_CONNECTED                  0       0       0         0      0        0
TCP_CONNECTING                 0       0       0         0      0        0
TCP_LISTENING                  0       0       0         0      0        0
TCP_DISCONNECT                 0       0       0         0      0        0
-----

```

```

TCP_CLOSED                0          0          0          0          0          0
-----
SIP IMSAKA Listen TCP Sockets -- Period -- ----- Lifetime -----
                        Active    High    Total    Total    PerMax    High
All States              1          1          0          2          2          1
TCP_INITIAL             0          0          0          0          0          0
TCP_STARTING            0          0          0          0          0          0
TCP_AVAILABLE           0          0          0          0          0          0
TCP_BOUNDED              0          0          0          1          1          1
TCP_CONNECTED           0          0          0          0          0          0
TCP_CONNECTING          0          0          0          0          0          0
TCP_LISTENING           1          1          0          1          1          1
TCP_DISCONNECT          0          0          0          0          0          0
TCP_CLOSED              0          0          0          0          0          0
-----

```

Updated Show Commands

show ip

Syntax

```
show ip <arguments>
```

Displays IP statistics for the Oracle USM.

Arguments

The following is a list of valid show ip arguments:

- **statistics** —Display detailed IP statistics
- **connections** —Display all TCP and UDP connections
- **sctp**—Display all SCTP statistics, including a list of current connections per SCTP state and systemwide counts.
- **tcp** —Display all TCP statistics, including a list of current connections per TCP state and differentiated by inbound, outbound, listen and IMS-AKA connections as well as systemwide counts. (Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.)
- **udp** —Display all UDP statistics


Executing the **show ip** command with no arguments returns the equivalent of the **show ip statistics** command.

show sipd

Syntax

```
show sipd <arguments>
```

The show sipd command displays SIP statistics on your Oracle USM.

 **Note:** (Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.)

Arguments

status—Display information about SIP transactions. These statistics are given for the Period and Lifetime monitoring spans. This display also provides statistics related to SIP media events. The following statistics are displayed when using the show sipd status command.

- Dialogs—Number of end-to-end SIP signaling connections
- CallID Map—Total number of successful session header Call ID mappings
- Sessions—Number of sessions established by an INVITE
- Subscriptions—Number of sessions established by SUBSCRIPTION
- Rejections—Number of rejected INVITEs
- ReINVITEs—Number of ReINVITEs
- Media Sessions—Number of successful media sessions
- Media Pending—Number of media sessions waiting to be established
- Client Trans—Number of client transactions
- Server Trans—Number of server transactions that have taken place on the Oracle USM
- Resp Contexts—Number of current response contexts
- Saved Contexts—Total number of saved contexts
- Sockets—Number of active SIP sockets
- Req Dropped—Number of requests dropped
- DNS Trans—Number of DNS transactions
- DNS Sockets—Number of DNS Sockets
- DNS Results—Number of dns results
- Session Rate—The rate, per second, of SIP invites allowed to or from the Oracle USM during the sliding window period. The rate is computed every 10 seconds
- Load Rate—Average Central Processing Unit (CPU) utilization of the Oracle USM during the current window. The average is computed every 10 seconds. When you configure the load-limit in the SIPConfig record, the system computes the average every 5 seconds

errors —Display statistics for SIP media event errors. These statistics are errors encountered by the SIP application in processing SIP media sessions, dialogs, and session descriptions (SDP). Errors are only displayed for the lifetime monitoring span.

- SDP Offer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Offer in the Offer/Answer model (RFC 3264)
- SDP Answer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Answer in the Offer/Answer model (RFC 3264)
- Drop Media Errors—Number of errors encountered in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction; or b) a BYE transaction received from one of the participants in a dialog or session; or c) a BYE initiated by the system due to a timeout notification from MBCD
- Transaction Errors—Number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session
- Missing Dialog—Number of requests received by the SIP application for which a matching dialog count not be found
- Application Errors—Number of miscellaneous errors in the SIP application that are otherwise uncategorized
- Media Exp Events—Flow timer expiration notifications received from MBCD
- Early Media Exps—Flow timer expiration notifications received for media sessions that have not been completely set up due to an incomplete or pending INVITE transaction
- Exp Media Drops—Number of flow timer expiration notifications from the MBCD that resulted in the termination of the dialog/session by the SIP application
- Multiple OK Drops—Number of dialogs terminated upon reception of a 200 OK response from multiple UASs for a given INVITE transaction that was forked by a downstream proxy
- Multiple OK Terms—Number of dialogs terminated upon reception of a 200 OK response that conflicts with an existing established dialog on the Oracle USM
- Media Failure Drops—Number of dialogs terminated due to a failure in establishing the media session

- Non-ACK 2xx Drops—Number of sessions terminated because an ACK was not received for a 2xx response
- Invalid Requests—Number of invalid requests; an unsupported header for example
- Invalid Responses—Number of invalid responses; no Via header for example
- Invalid Messages—Number of messages dropped due to parse failure
- CAC Session Drop—Number of call admission control session setup failures due to user session count exceeded
- Expired Sessions—Number of sessions terminated due to the session timer expiring
- CAC BW Drop—Number of call admission control session setup failures due to insufficient bandwidth

Lifetime displays show information for recent, total, and period maximum error statistics:

- Recent—Number of errors occurring in the number of seconds listed after the time stamp
- Total—Number of errors occurring since last reboot
- PerMax—Identifies the highest individual Period Total over the lifetime of the monitoring

policy—Display SIP local policy / routing statistics for lifetime duration

- Local Policy Lookups—Number of Local policy lookups
- Local Policy Hits—Number of successful local policy lookups
- Local Policy Misses—Number of local policy lookup failures
- Local Policy Drops—Number of local policy lookups where the next hop session agent group is H323
- Agent Group Hits—Number of successful local policy lookups for session agent groups
- Agent Group Misses—Number of successful local policy lookups where no session agent was available for session agent group
- No Routes Found—Number of successful local policy lookups but temporarily unable to route; session agent out of service for instance
- Missing Dialog—Number of local policy lookups where the dialog is not found for a request addressed to the Oracle USM with a To tag or for a NOTIFY-SUBSCRIBE sip request
- Inb SA Constraints—Number of successful local policy lookups where inbound session agent exceeded constraints
- Outb SA Constraints—Number of successful outbound local policy lookups where session agent exceeded constraints
- Inb Reg SA Constraints—Number of successful inbound local policy lookups where registrar exceeded constraints
- Out Reg SA Constraints—Number of successful outbound local policy lookups where registrar exceeded constraints
- Requests Challenged—Number of requests challenged
- Challenge Found—Number of challenges found
- Challenge Not Found—Number of challenges not found
- Challenge Dropped—Number of challenges dropped

server—Display statistics for SIP server events when the Oracle USM acts as a SIP server in its B2BUA role. Period and Lifetime monitoring spans for SIP server transactions are provided.

- All States—Number of all server transactions
- Initial—Number of times the “initial” state was entered after a request was received
- Queued—Number of times the “queued” state is entered because resources are temporarily unavailable
- Trying—Number of times the “trying” state was entered due to the receipt of a request
- Proceeding—Number of times a server transaction has been constructed for a request
- Cancelled—Number of INVITE transactions that received a CANCEL
- Established—Number of times the server sent a 2xx response to an INVITE
- Completed—Number of times the server received a 300 to 699 status code and entered the “completed” state
- Confirmed—Number of times that an ACK was received while the server was in “completed” state and transitioned to “confirmed” state

- Terminated—Number of times that the server received a 2xx response or never received an ACK in the “completed” state, and transitioned to the “terminated” state

client —Display statistics for SIP client events when the Oracle USM is acting as a SIP client in its B2BUA role. Period and Lifetime monitoring spans are displayed.

- All States—Number of all client transactions
- Initial—State when initial server transaction is created before a request is sent
- Trying—Number of times the “trying” state was entered due to the sending of a request
- Calling—Number of times that the “calling” state was entered due to the receipt of an INVITE request
- Proceeding—Number of times that the “proceeding” state was entered due to the receipt of a provisional response while in the “calling” state
- Early Media—Number of times that the “proceeding” state was entered due to the receipt of a provisional response that contained SDP while in the “calling” state
- Completed—Number of times that the “completed” state was entered due to the receipt of a status code in the range of 300-699 when either in the “calling” or “proceeding” state
- SetMedia—Number of transactions in which the Oracle USM is setting up NAT and steering ports
- Established—Number of situations when client receives a 2xx response to an INVITE, but cannot forward it because it NAT and steering port information is missing
- Terminated—Number of times the “terminated” state was entered after a 2xx message

acls—Display ACL information for Period and Lifetime monitoring spans

- Total entries—Total ACL Entries, including both trusted and blocked
- Trusted—Number of trusted ACL entries
- Blocked—Number of blocked ACL entries
- Blocked NATs—Number of blocked entries that are behind NATs

Lifetime monitoring span is displayed for SIP ACL Operations.

- ACL Requests—Number of ACL requests
- Bad Messages —Number of bad messages
- Promotions—Number of ACL entry promotions
- Demotions—Number of ACL entry demotions
- Trust->Untrust—Number of ACL entries demoted from trusted to untrusted
- Untrust->Deny—Number of acl entries demoted from untrusted to deny

sessions—Display the number of sessions and dialogs in various states for the Period and Lifetime monitoring spans, in addition to the current Active count:

- Sessions—Identical to the identically named statistic on the show sipd status command
- Initial—Displays sessions for which an INVITE of SUBSCRIBE is being forwarded
- Early—Displays sessions for which the first provisional response (1xx other than 100) is received
- Established—Displays sessions for which a success (2xx) response is received
- Terminated—Displays sessions for which the session is ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or “Early” session. The session will remain in the “Terminated” state until all the resources for the session are freed.
- Dialogs—Identical to the identically named statistic on the show sipd status command
- Early—Displays dialogs that were created by a provisional response
- Confirmed—Displays dialogs that were created by a success response. An “Early” dialog will transition to “Confirmed” when a success response is received
- Terminated—Displays dialogs that were ended by receiving/sending a BYE for an “Established” session or receiving/sending error response “Early” dialog. The dialog will remain in the “Terminated” state until all the resources for the session are freed.

sessions all—Display all SIP sessions currently on the system

sessions by-agent <agent name>—Display SIP sessions for the session agent specified; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-ip <endpoint IP address>—Display SIP sessions for the specified IP address for an endpoint; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-user <calling or called number>—Display SIP sessions for the specified user; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-callid <call ID>—Display SIP sessions for the specified call ID; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

redundancy—Display sipd redundancy statistics. Executing the show sipd redundancy command is the equivalent to the show redundancy sipd command.

agents [hostname][method][-t]—Display statistics related to defined SIP session agents. Entering this command without any arguments list all SIP session agents. By adding the IP address or hostname of a session agent as well as a specified method at the end of the command, you can display statistics for that specific session agent and method. For a specific session agent, identified by IP address, the show sipd agents command lists:

- session agent state
 - D—disabled
 - I—in-service
 - O—out-of-service
 - S—transitioning from out-of-service to in-service
- inbound and outbound statistics
- average and maximum latency for each session agent
- maximum burst rate for each session agent as total number of session invitations sent to or received from the session agent within the amount of time configured in the burst-rate-window field

Inbound Statistics:

- Active—Number of active sessions sent to each session agent listed
- Rate—Average rate of session invitations (per second) sent to each session agent listed
- ConEx—Number of times the constraints have been exceeded

Outbound Statistics:

- Active—Number of active sessions sent from each session agent
- Rate—Average rate of session invitations (per second) sent from each session agent listed
- ConEx—Number of times the constraints have been exceeded

Latency:

- Avg—Average latency for packets traveling to and from each session agent
- Max—Maximum latency for packets traveling to and from each session agent listed

-t—Append to the end of the command to specify the current time period for the max-burst value.

interface [interface-id][method]—Display SIP interface statistics. By adding the optional interface-id and method arguments you can narrow the display to view just the interface and method you want to view.

ip-cac <IP address>—Display CAC parameters for an IP address

publish—Display statistics related to incoming SIP PUBLISH messages

agent <agent>—Display activity for the session agent that you specify

- Inbound Sessions:

Rate Exceeded—Number of times session or burst rate was exceeded for inbound sessions

- Num Exceeded—Number of times time constraints were exceeded for inbound sessions

Outbound Sessions:

- Rate Exceeded—Number of times session or burst rate was exceeded for outbound sessions
- Num Exceeded—Number of times time constraints were exceeded for inbound sessions
- Burst—Number of times burst rate was exceeded for this session agent
- Out of Service—Number of times this session agent went out of service
- Trans Timeout—Number of transactions timed out for this session agent
- Requests Sent—Number of requests sent by way of this session agent
- Requests Complete—Number of requests that have been completed for this session agent
- Messages Received—Number of messages received by this session agent

realm—Display realm statistics related to SIP processing

routers—Display status of Oracle USM connections for session router functionality

directors—Display the status of Oracle USM connections for session director functionality

<message>—Add one of the following arguments to the end of a show sipd command to display information about that type of SIP message:

- INVITE—Display the number of SIP transactions including an INVITE method
- REGISTER—Display the number of SIP transactions including a REGISTER method
- OPTIONS—Display the number of SIP transactions including an OPTIONS method
- CANCEL—Display the number of SIP transactions including a CANCEL method
- BYE—Display the number of SIP transactions including a BYE method
- ACK—Display the number of SIP transactions including an ACK method
- INFO—Display the number of SIP transactions including an INFO method
- PRACK—Display the number of SIP transactions including a PRACK method
- SUBSCRIBE—Display the number of SIP transactions including a SUBSCRIBE method
- NOTIFY—Display the number of SIP transactions including a NOTIFY method
- REFER—Display the number of SIP transactions including a REFER method
- UPDATE—Display the number of SIP transactions including an UPDATE method
- other—Display the number of SIP transactions including non-compliant methods and protocols used by specific customers

The following lists information displayed for each individual SIP message statistic. Some or all of the following messages and events may appear in the output from a show sipd command.

- INVITE Requests—Number of times method has been received or sent
- Retransmissions—Information regarding sipd message command requests received by the Oracle USM
- 100 Trying—Number of times some unspecified action is being taken on behalf of a call (e.g., a database is being consulted), but user has not been located
- 180 Ringing—Number of times called UA identified a location where user has registered recently and is trying to alert the user
- 200 OK—Number of times request has succeeded
- 408 Request Timeout—Number of times server could not produce a response before timeout
- 481 Does Not Exist—Number of times UAS received a request not matching existing dialog or transaction
- 486 Busy Here—Number of times callee's end system was contacted successfully but callee not willing to take additional calls
- 487 Terminated—Number of times request was cancelled by a BYE or CANCEL request
- 4xx Client Error—Number of times the 4xx class of status code appeared for cases where the client seems to have erred
- 503 Service Unavail—Number of times server was unable to handle the request due to a temporary overloading or maintenance of the server

- 5xx Server Error—Number of times the 5xx class of status code appeared
- Response Retransmissions—Number of response retransmissions sent and received
- Transaction Timeouts— Number of times a transaction timed out. The timer related to this transaction is Timer B, as defined in RFC 3261
- Locally Throttled—Number of locally throttled invites. Does not apply to a server.

show sipd <message> output is divided in two sections: Server and Client, with information for recent, total, and period maximum time frames. This command also displays information about the average and maximum latency. For each type of SIP message, only those transactions for which there are statistics are shown. If there is no data available for a certain SIP message, the system displays the fact that there is none and specifies the message about which you inquired.

groups—Display cumulative information for all session agent groups on the Oracle USM. This information is compiled by totaling the session agent statistics for all of the session agents that make up a particular session agent group. While the show sipd groups command accesses the sub-commands described in this section, the main show sipd groups command (when executed with no arguments) displays a list of all session agent groups.

groups -v—Display statistics for the session agents that make up the session agent groups that are being reported. The -v (meaning “verbose”) executed with this command must be included to provide verbose detail.

groups <specific group name>— Display statistics for the specified session agent group

endpoint-ip <phone number> —Displays registration information for a designation endpoint entered in the <phone number> argument; also show IMS-AKA data

all—Display all the show sipd statistics listed above

sip-endpoint-ip—See show sipd endpoint-ip

sa-nsep-burst—Display NSEP burst rate for all SIP session agents

subscriptions-by-user—Display data for SIP per user subscribe dialog limit

rate—Displays the transaction rate of SIP messages

codecs—Displays codec usage per realm, including counts for codecs that require a license such as SILK and opus.

pooled-transcoding—Pooled transcoding information for the client and server User Agents on the P-CSCF

srvcc—Displays EATF Session information

tcp—Displays TCP connection state information for the following

- inbound
- outbound
- listen
- IMS-AKA
- total

tcp connections—Dump TCP connections for analysis. Options include:

- sip-interface—Optional parameter that limits output to sockets in the specified sip-interface
- start start—Integer indicating which connection to start display. This can be a negative number. If the number selected for the start variable is greater than the number of TCP connections, nothing will be displayed
- start-count start—Integer as per above plus the count integer, specifying how many TCP connections to display from the start.
- all—Dump all of the sipd tcp connections. Exercise caution due to the possibility of consuming all CPU time; preferably use during a maintenance window

Example

```
ORACLE# show sipd errors
```

