

Oracle® Communications Session Director
Maintenance Release Guide
Release S-D7.2.0

December 2014

Notices

Copyright ©2014, 2013, 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

About this guide.....	5
1 S-D7.2.0M1.....	7
Content Map for S-D7.2.0M1.....	7
CNAM Subtype Support for ENUM Queries.....	7
CNAM Unavailable Response.....	7
SIP Profile Inheritance.....	8
CNAM Subtype Support Configuration.....	8
2 S-D7.2.0M2.....	9
SIP REFER Method Call Transfer.....	9
Unsuccessful Transfer Scenarios.....	10
Call Flows.....	10
SIP REFER Method Configuration.....	12
REFER-Initiated Call Transfer.....	14
Supported Scenarios.....	14
REFER Source Routing.....	17
REFER Source Routing Configuration.....	17
180 & 100 NOTIFY in REFER Call Transfers.....	18
Sample Messages.....	20
180 and 100 NOTIFY Configuration.....	21
SIP REFER Re-Invite for Call Leg SDP Renegotiation.....	22
Scenario.....	22
Alterations to SIP REFER.....	22
Implementation Details.....	22
SIP REFER with Replaces.....	23
SIP REFER with Replaces Configuration.....	23
SIP REFER-to-BYE.....	24
CAC Utilization Statistics via SNMP.....	24
CAC utilization threshold trap on a session agent configuration.....	27
Configuring the CAC Utilization Thresholds - realm.....	27
High Capacity Entries in ifXTable SNMP Table.....	28
3 S-D7.2.0M3.....	29
Caveats and Known Issues.....	29



About this guide

The Maintenance Release Guide provides information about the contents of maintenance releases related to Net-Net OS S-D7.2.0. This information can be related to defect fixes, to adaptations made to the system software, and to adaptations ported to this release of the Net-Net OS from prior releases. When applicable, this guide contains explanations of defect fixes to the software and step-by-step instructions, if any, for how to enable these fixes on your system. This guide contains explanations of adaptations including conceptual information and configuration steps.

Purpose of this Document

Designed as a supplement to the main documentation set supporting release S-D7.2.0, this document informs you of changes made to the Net-Net OS software in the maintenance releases of S-D7.2.0. Consult this document for content specific to maintenance releases. For information about general Net-Net OS features, configuration, and maintenance, consult the Related Documentation listed in the section below and then refer to the applicable document.

Organization

The Maintenance Release Guide is organized chronologically by maintenance release number, started with the oldest available maintenance release and ending with the most recently available maintenance release.

This document contains a Maintenance Release Availability Matrix, showing when and if given maintenance releases have been issued and the date of issue. Each available maintenance release constitutes one chapter of this guide.

In certain cases, a maintenance release will not have been made generally available. These cases are noted in the Maintenance Release Availability Matrix. When Acme Packet has not made a maintenance release available, there will be no corresponding chapter for that release. Therefore, you might encounter breaks in the chronological number of maintenance release.

Maintenance Release Availability Matrix

The table below lists the availability for version S-D7.2.0 maintenance releases.

Maintenance release number	Availability Notes
S-D7.2.0M1	January 10, 2014
S-D7.2.0M2	April 16, 2014
S-D7.2.0M3	August 1, 2014

Related Documentation

The following table lists the members that comprise the documentation set for this release:

Document Name	Document Description
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration SBC.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.

About this guide

Document Name	Document Description
Maintenance and Troubleshooting Guide	Contains information about SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the SBC's accounting support, including details about RADIUS accounting.

Revision History

Date	Description
January 10, 2014	Initial Release
April 16, 2014	Corresponds with release of S-D7.2.0M2
August 1, 2014	Corresponds with release of S-D7.2.0M3
December 19, 2014	Adds max-untrusted-signaling caveat to M3 chapter.

S-D7.2.0M1

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-D7.2.0M1.

Current patch baselines: S-D7.1.0M6p5, S-D7.2.0p1, S-D7.2.3f3p8

Content Map for S-D7.2.0M1

This section provides a table listing all content in Release S-D7.2.0M1.

Content Type	Description
Forward Merge	S-D7.1.0M6 - This includes CNAM subtype support for ENUM queries feature.

CNAM Subtype Support for ENUM Queries

CNAM, calling name, data is a string up to 15 ASCII characters of information associated with a specific calling party name. The *Internet-draft, draft-ietf-enum-cnam-08.txt*, registers the Enumservice 'pstndata' and subtype 'cnam' using the URI scheme 'pstndata:' to specify the return of CNAM data in ENUM responses. The Oracle Communications Session Director recognizes CNAM data returned via this mechanism. CNAM data is then inserted into the display name of the From: header in the original Request. If a P-Asserted-ID header is present in the original request, the CNAM data is inserted there as well.

CNAM data is identified by an ENUM response with service-type: E2U+pstndata:cnam

CNAM support is configured in the sip profile configuration element, which can then be applied to either a session agent, realm, or SIP interface.

The Oracle Communications Session Director can preform CNAM queries on the signaling message's ingress or egress from the system by setting the cnam lookup direction parameter to either ingress or egress. If the CNAM lookup direction parameters are configured on both the ingress and egress sides of a call, the Oracle Communications Session Director will only preform the lookup on the ingress side of the call.

CNAM Unavailable Response

A CNAM response can include a Calling Name Privacy Indicator parameter ('unavailable=p') or Calling Name Status Indicator parameter ('unavailable=u') in responses. The Oracle Communications Session Director can insert a custom reason string into the SIP message's From and P-Asserted-ID header in the original requires.

Configuring the `cnam-unavailable-ptype` parameter inserts the specified text into the From and P-Asserted-ID headers when a CNAM response contains the `unavailable=p` parameter.

Configuring the `cnam-unavailable-utype` parameter inserts the specified text into the From and P-Asserted-ID headers when a CNAM response contains the `unavailable=u` parameter.

SIP Profile Inheritance

CNAM features, via the SIP Profile configuration element can be applied to session agents, realms, and SIP interfaces. The more generalized object inherits the more specific object's values. For example, if CNAM support via a SIP profile is configured on a session agent, the expected processing will override any SIP profile configuration on the downstream realm or SIP interface. Likewise, if CNAM support is unconfigured on the receiving session agent, but configured in the realm, CNAM configuration on the SIP interface will be ignored.

CNAM Subtype Support Configuration

To enable the Oracle Communications Session Director to preform CNAM subtype ENUM queries, you must configure a SIP profile with an `enum-config` object (that points to valid ENUM servers). The referenced `enum-config` configuration element lists the servers to contact for CNAM type queries (and other general ENUM server interaction parameters).

To configure CNAM subtype support:

1. In Superuser mode, type `configure terminal` and press Enter.

```
ACMEPACKET# configure terminal
```

2. Type `session-router` and press Enter to access the signaling-level configuration elements.

```
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)#
```

3. Type `sip-profile` and press Enter. The system prompt changes to let you know that you can begin configuring individual parameters.

```
ACMEPACKET(session-router)# sip-profile
ACMEPACKET(sip-profile)#
```

4. `name`—Enter a string that uniquely identifies this SIP profile configuration. You use this name in other areas of the Oracle Communications Session Director configuration to refer to this SIP profile in session agents, realms, or SIP interfaces.
5. `cnam-lookup-server`—Set this parameter to the name of an `ENUM-config` to that will query ENUM servers for CNAM data.
6. `cnam-lookup-dir`—Set this parameter to `ingress` or `egress` to identify where the Oracle Communications Session Director performs a CNAM lookup with respect to where the call traverses the system. The default value is `egress`.
7. `cnam-unavailable-ptype`—Set this parameter to a string, no more than 15 characters, to indicate that the `unavailable=p` parameter was returned in a CNAM response.
8. `cnam-unavailable-utype`—Set this parameter to a string, no more than 15 characters, to indicate that the `unavailable=u` parameter was returned in a CNAM response.
9. Save your work.

S-D7.2.0M2

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-D7.2.0M2.

- Current patch baseline: S-D7.2.0M1P1

Content Map

This section lists all new content appearing in Release S-D7.2.0M1.

Content Type	Description
Adaptation	SIP REFER Support
Adaptation	Monitoring CAC and occupancy level
Adaptation	64-bits SNMP counters for IfInOctets and IfOutOctets

SIP REFER Method Call Transfer

In prior releases, the Oracle Communications Session Director supports the SIP REFER method by proxying it to the other UA in the dialog. A handling mode has been developed for the REFER method so that the Oracle Communications Session Director automatically converts a received REFER method into an INVITE method, thus allowing the Oracle Communications Session Director to transfer a call without having to proxy the REFER back to the other UA.

This function can be configured for a specified SIP interface, a realm, or a session agent. When all three elements have the SIP REFER method call transfer functionality configured, the session-agent configuration takes precedence over realm-config and sip-interface configurations. If session-agent is not configured, and realm-config and sip-interface are, realm-config takes precedence.

The Oracle Communications Session Director has a configuration parameter giving it the ability to provision the handling of REFER methods as call transfers. The parameter is called refer-call-transfer. When this feature is enabled, the Oracle Communications Session Director creates an INVITE message whenever it receives a REFER. The Oracle Communications Session Director sends this INVITE message to the address in the Refer-To header. Included in the INVITE message is all the unmodified information contained in the REFER message. The previously negotiated codec is also still used in the new INVITE message. NOTIFY and BYE messages are sent to the UA upon call transfer completion.

If a REFER method is received containing no Referred-By header, the Oracle Communications Session Director adds one, allowing the Oracle Communications Session Director to support all call agent screen applications.

In addition, the SIP REFER method call transfer feature supports the following:

- Both unattended and attended call transfers
- Both successful and unsuccessful call transfers
- Early media from the Referred-To party to the transferee
- REFER method transfer from different sources within the destination realm
- The REFER event package as defined in RFC 3515. This applies for situations where multiple REFER methods are used within a single dialog.
- Third party initiated REFER method signalling the transfer of a call by associating the REFER method to the dialogue via the REFER TargetDialog.
- The Referred-To party can be both in a different realm (and thus a different steering pool) from the referrer, and in the same realm
- The associated latching should not prohibit the Referred-To party from being latched to while the referee is still sending media.

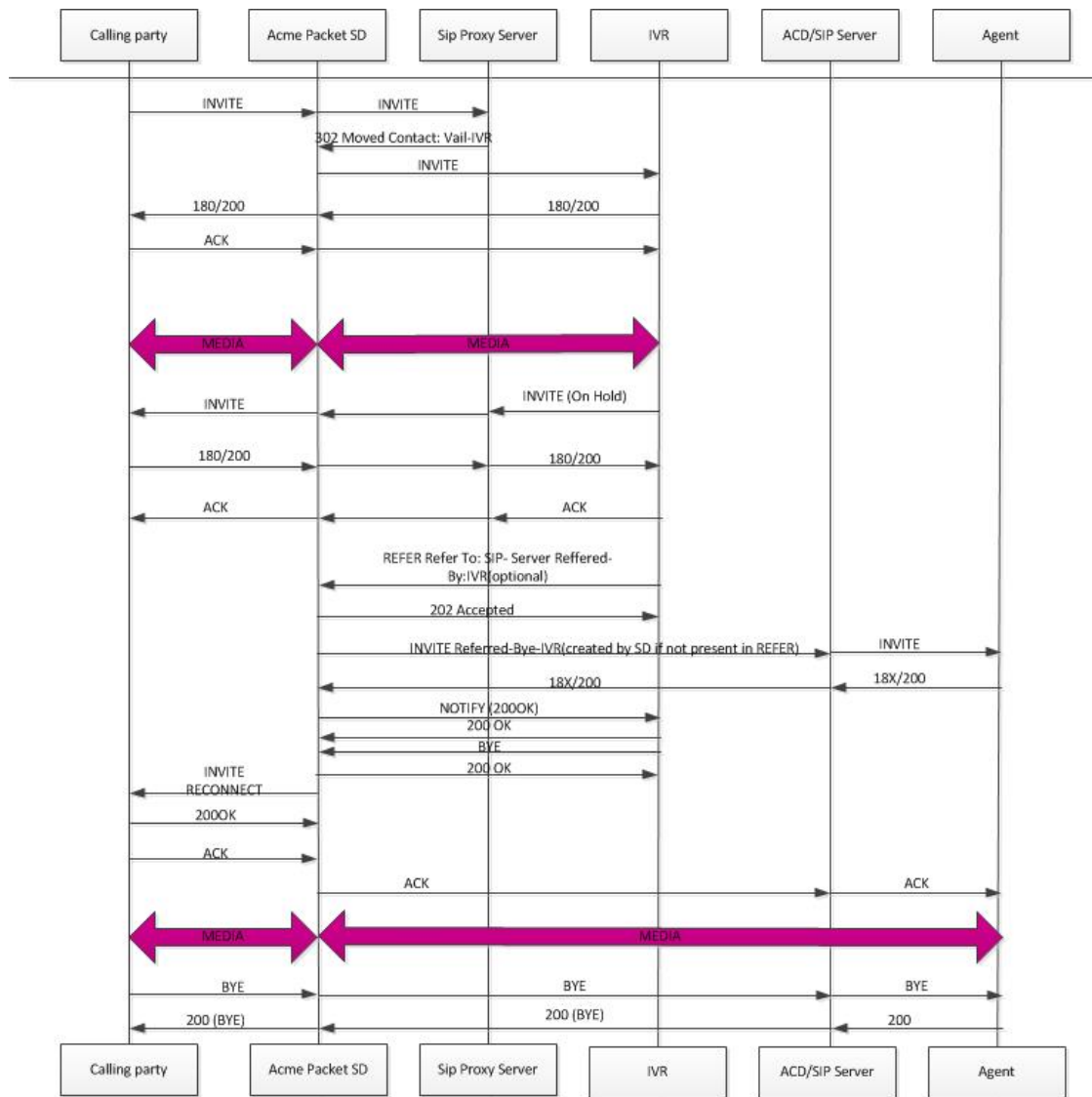
Unsuccessful Transfer Scenarios

The Oracle Communications Session Director does not successfully handle the following failed, unusual, and unexpected transfer scenarios:

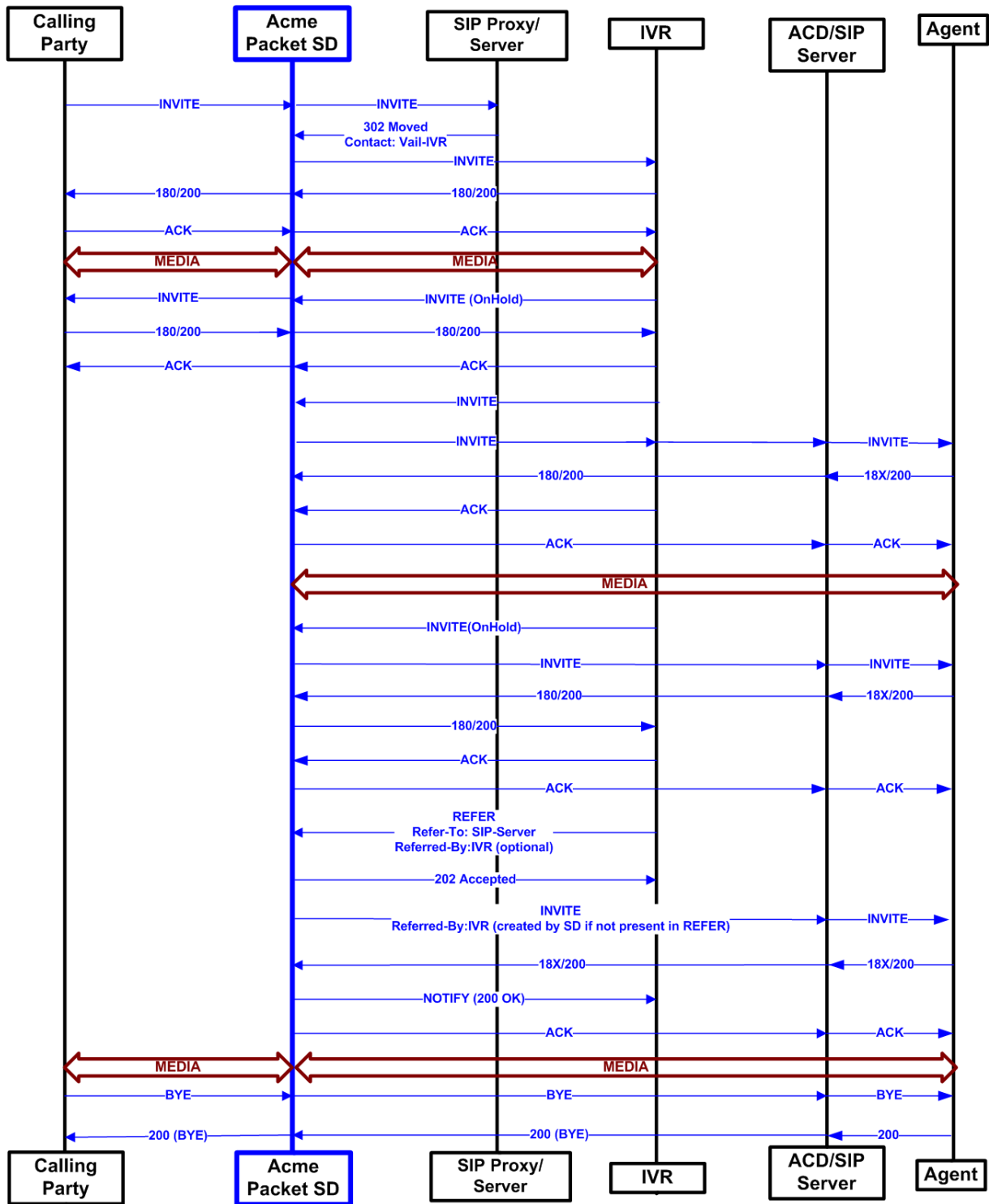
- The new INVITE to the Referred-To party gets challenged, the Oracle Communications Session Director does not answer the challenge. It is treated with the 401/407 response just as any other unsuccessful final response.
- The header of the REFER message contains a method other than INVITE or contains URI-parameters or embedded headers not supported by the Oracle Communications Session Director.
- The Oracle Communications Session Director shall allow the Referred-To URI that happens to resolve to the same next-hop as the original INVITE went to, to do so.
- The Oracle Communications Session Director ignores any MIME attachment(s) within a REFER method.
- The Oracle Communications Session Director recurses (when configured to do so) when the new INVITE sent to the Referred-To party receives a 3xx response.
- The transferee indicated support for 100rel, and the original two parties agreed on using it, yet the Referred-To party does not support it.
- The original parties negotiated SRTP keys.
- The original parties agreed on a codec using a dynamic payload type, and the Referred-To party happens to use a different dynamic payload number for that codec.

Call Flows

The following is an example call flow for an unattended call transfer:



The following is an example call flow of an attended call transfer:



SIP REFER Method Configuration

To enable SIP REFER method call transfer in the realm-config:

1. In Superuser mode, type configure terminal and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)#
```

2. Type media-manager and press Enter.

```
ACMEPACKET(configure)# media-manager
ACMEPACKET(media-manager)#
```

3. Type realm-config and press Enter.

```
ACMEPACKET(media-manager)# realm-config
ACMEPACKET(realm-config)#
```

4. refer-call-transfer—Set to enabled to enable the refer call transfer feature. The default for this parameter is disabled.

5. Save and activate your configuration.

To enable SIP REFER method call transfer in the sip-interface:

6. In Superuser mode, type configure terminal and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)#
```

7. Type session-router and press Enter.

```
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)#
```

8. Type sip-interface and press Enter.

```
ACMEPACKET(session-router)# sip-interface
ACMEPACKET(sip-config)#
```

9. refer-call-transfer—Set to enabled to enable the refer call transfer feature. The default for this parameter is disabled.

10. Save and activate your configuration.

To enable SIP REFER method call transfer in a realm:

11. In Superuser mode, type configure terminal and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)#
```

12. Type media-manager and press Enter.

```
ACMEPACKET(configure)# media-manager
ACMEPACKET(media-manager)#
```

13. Type realm-config and press Enter. The system prompt changes to let you know that you can begin configuring individual parameters.

```
ACMEPACKET(media-manager)# realm-config
ACMEPACKET(realm-config)#
```

14. refer-call-transfer—Set to enabled to enable the refer call transfer feature. The default for this parameter is disabled.

15. Save and activate your configuration.

To enable SIP REFER method call transfer in the session-agent:

16. In Superuser mode, type configure terminal and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)#
```

17. Type session-router and press Enter.

```
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)#
```

18. Type session-agent and press Enter.

```
ACMEPACKET(media-manager)# session-agent
ACMEPACKET(session-agent)#
```


19. refer-call-transfer—Set to enabled to enable the refer call transfer feature. The default for this parameter is disabled.

20. Save and activate your configuration.

REFER-Initiated Call Transfer

In prior releases, the Oracle Communications Session Director supported REFER-initiated call transfer either by proxying the REFER to the other User Agent in the dialog, or by terminating the received REFER and issuing a new INVITE to the referred party. These static alternate operational modes could be configured for specific SIP interfaces, realms, or session agents.

Release S-C6.2.0 enhances support with an additional operational mode that determines on a call-by-call basis whether to proxy the REFER to the next hop, or terminate the REFER and issue an INVITE in its stead.

 **Note:** With the release of Version S-C6.2.0, support for REFER-initiated call transfer is no longer available for SIP interfaces; support must be configured for realms and/or session agents.

Version S-C6.2.0 provides a new configuration parameter `dyn-refer-term`, and a revised `refer-call-transfer` parameter (both available in `realm-config` configuration mode) that specify call transfer modes.

With the `refer-call-transfer` parameter set to disabled (the default), all received REFERs are simply proxied to the peer User Agent.

With the `refer-call-transfer` parameter set to enabled, the Oracle Communications Session Director terminates all REFERs, generates a new INVITE, and sends the INVITE to the address in the `Refer-To` header.

With the `refer-call-transfer` parameter set to dynamic (a new value introduced with Version S-C6.2.0), the Oracle Communications Session Director determines REFER handling on a call-by-call basis as follows:

1. Check the `refer-call-transfer` value for the session agent from which the REFER was received, or for ingress realm (the realm that received the REFER).

If the value is disabled, proxy the REFER to the peer User Agent, to complete REFER processing.

If the value is enabled, terminate the REFER and issue a new INVITE to the referred party, to complete REFER processing.

If the value is dynamic, identify the next hop session agent or the egress realm.

2. Check the `dyn-refer-term` value for the next hop session agent, or for the egress realm.

If the `dyn-refer-term` value is disabled (the default), proxy the REFER to the next hop to complete REFER processing.

If the `dyn-refer-term` value is enabled, terminate the REFER and issue a new INVITE to the referred party to complete REFER processing

Supported Scenarios

In the basic scenario for REFER initiated call transfer, a call is established between two User Agents (Alice and Bob). User Agent Bob then sends a REFER request to transfer the call to a third User Agent Eva. With dynamic call-transfer enabled, the Oracle Communications Session Director prevents the REFER from being sent to Alice and generates the INVITE to Eva.

If the INVITE to Eva succeeds, the Oracle Communications Session Director sends a re-INVITE to Alice modifying the SIP session as described in Section 14 of RFC 3261, *SIP: Session Initiation Protocol*. At this point the Oracle Communications Session Director cancels the original dialog between the Net-Net SBC and Bob.

If the INVITE to Eva fails, call disposition depends on whether or not Bob issued a BYE after the REFER call transfer. If the Oracle Communications Session Director did receive a BYE from Bob (for instance, a blind transfer), it proxies the BYE to A. Otherwise, the Oracle Communications Session Director retains the original SIP session and media session, thus allowing Bob to re-establish the call with Alice by sending a re-INVITE. In this case, the Oracle Communications Session Director sets a timer (32 seconds), after which a BYE will be sent.

If a REFER method is received containing no `Referred-By` header, the Oracle Communications Session Director adds one, allowing the Oracle Communications Session Director to support all call agent screen applications.

In addition, the SIP REFER method call transfer feature supports the following:

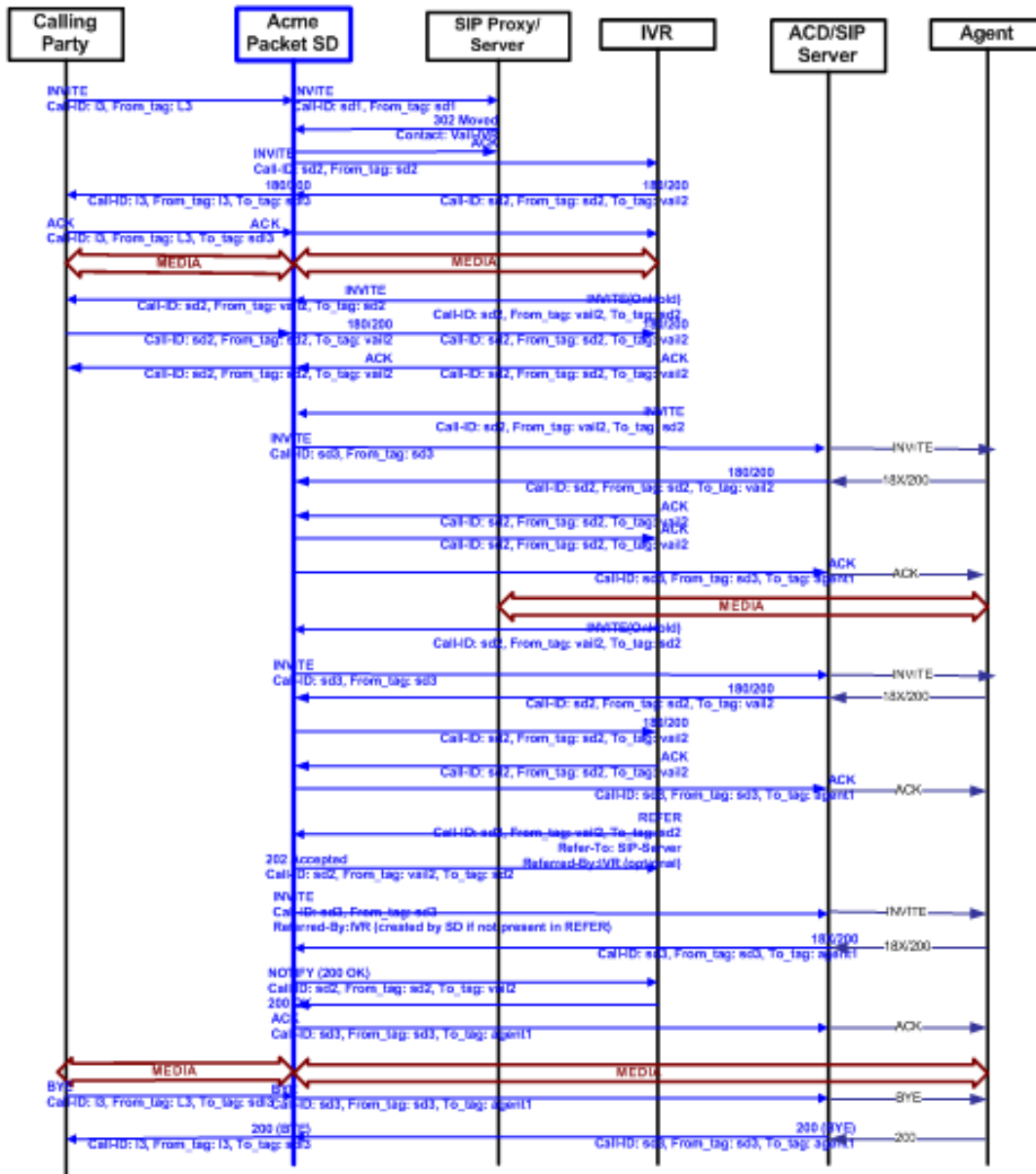
- Both unattended and attended call transfers
- Both successful and unsuccessful call transfers
- Early media from the Referred-To party to the transferee
- REFER method transfer from different sources within the destination realm
- The REFER event package as defined in RFC 3515. This applies for situations where multiple REFER methods are used within a single dialog.
- Third party initiated REFER method signalling the transfer of a call by associating the REFER method to the dialogue via the REFER TargetDialog.
- The Referred-To party can be both in a different realm (and thus a different steering pool) from the referrer, and in the same realm
- The associated latching should not prohibit the Referred-To party from being latched to while the referee is still sending media.

The Oracle Communications Session Director does not successfully handle the following anomalous transfer scenarios:

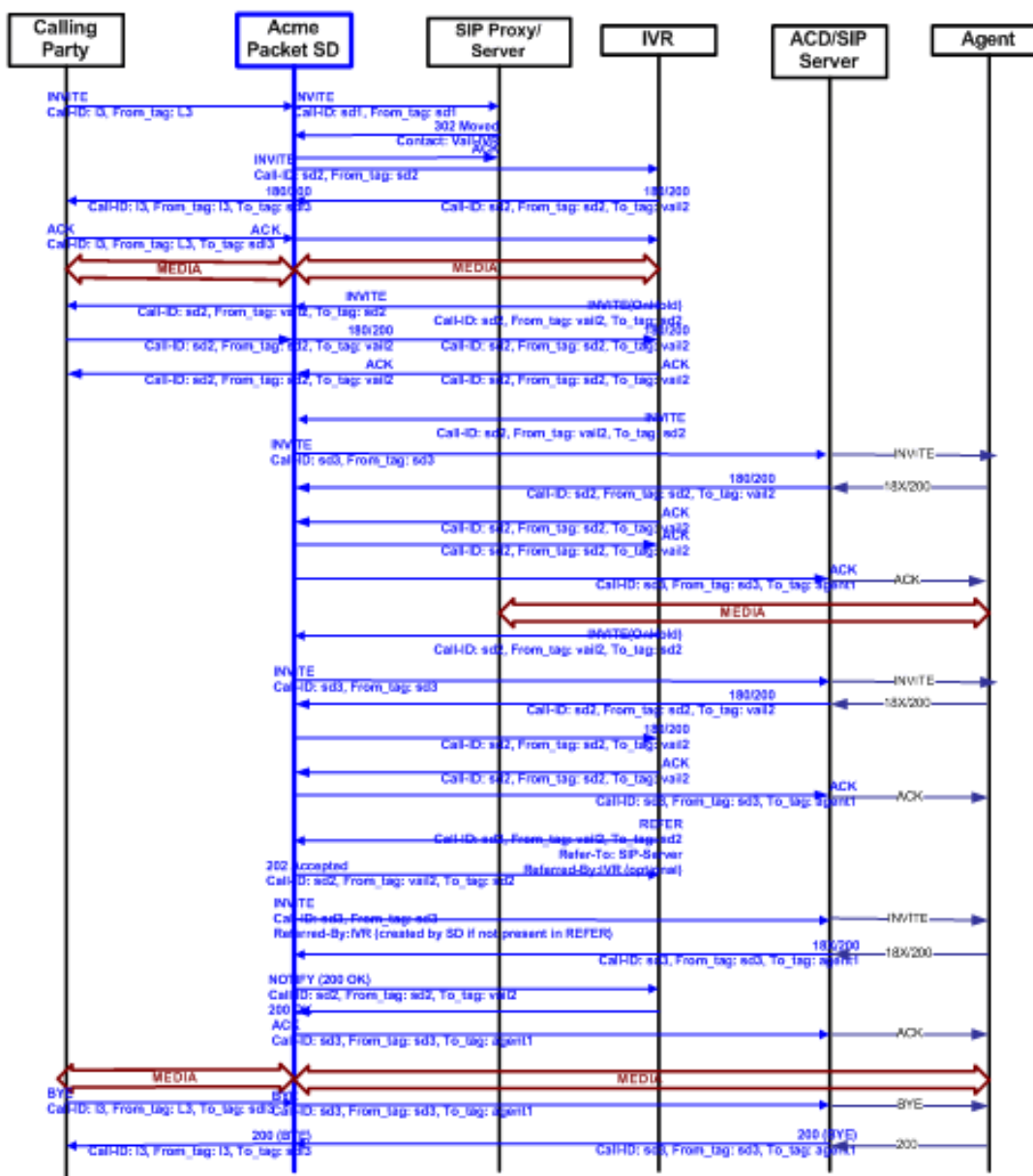
- The new INVITE to the Referred-To party gets challenged — the Oracle Communications Session Director does not answer the challenge. It is treated with the 401/407 response just as any other unsuccessful final response.
- The header of the REFER message contains a method other than INVITE or contains URI-parameters or embedded headers not supported by the Oracle Communications Session Director.
- The Oracle Communications Session Director shall allow the Referred-To URI that happens to resolve to the same next-hop as the original INVITE went to, to do so.
- The Oracle Communications Session Director ignores any MIME attachment(s) within a REFER method.
- The Oracle Communications Session Director recurses (when configured to do so) when the new INVITE sent to the Referred-To party receives a 3xx response.
- The transferee indicated support for 100rel, and the original two parties agreed on using it, yet the Referred-To party does not support it.
- The original parties negotiated SRTP keys.

Call Flows

The following is an example call flow for an unattended call transfer:



The following is an example call flow of an attended call transfer:



REFER Source Routing

If, after the conclusion of static or dynamic REFER handling, the REFER is terminated and a new INVITE issued, users now can specify a policy lookup behavior based upon either the source realm of the calling party (the INVITE originator), or the source realm of the referring party (the REFER originator).

Behavior is controlled by a new refer-src-routing parameter in the sip-config configuration element.

disabled, the default value, specifies that the Oracle Communications Session Director performs a policy lookup based on the source realm of the calling party.

enabled specifies that the Oracle Communications Session Director performs a policy lookup based on the source realm of the referring party.

REFER Source Routing Configuration

To enable realm-based REFER method call transfer:

1. In Superuser mode, type configure terminal and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure) #
```

2. Type `media-manager` and press Enter.

```
ACMEPACKET(configure) # media-manager
ACMEPACKET(media-manager) #
```

3. Type `realm-config` and press Enter.

```
ACMEPACKET(media-manager) # realm-config
ACMEPACKET(realm-config) #
```

4. `refer-call-transfer` — Retain the default (disabled) to proxy all REFERs to the next hop. Use `enabled` to terminate all REFERs and issue a new INVITE. Use `dynamic` to specify REFER handling on a call-by-call basis, as determined by the value of the `dyn-refer-term` parameter.

5. `dyn-refer-term` (meaningful only when `refer-call-transfer` is set to `dynamic`) — Retain the default (disabled) to terminate the REFER and issue a new INVITE. Use `enabled` to proxy the REFER to the next hop.

6. Save and activate your configuration.

To enable session-agent-based REFER method call transfer:

7. In Superuser mode, type `configure terminal` and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure) #
```

8. Type `session-router` and press Enter.

```
ACMEPACKET(configure) # session-router
ACMEPACKET(session-router) #
```

9. Type `session-agent` and press Enter.

```
ACMEPACKET(media-manager) # session-agent
ACMEPACKET(session-agent) #
```

10. `refer-call-transfer` — Retain the default (disabled) to proxy all REFERs to the next hop. Use `enabled` to terminate all REFERs and issue a new INVITE. Use `dynamic` to specify REFER handling on a call-by-call basis, as determined by the value of the `dyn-refer-term` parameter.

11. Save and activate your configuration.

To specify policy lookup for a newly generated INVITE:

12. In Superuser mode, type `configure terminal` and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure) #
```

13. Type `session-router` and press Enter.

```
ACMEPACKET(configure) # session-router
ACMEPACKET(session-router) #
```

14. Type `sip-config` and press Enter.

```
ACMEPACKET(configure) # sip-config
ACMEPACKET(sip-config) #
```

15. `refer-src-routing` — Retain the default (disabled) to perform a policy lookup based upon the source realm of the calling party (the issuer of the original INVITE). Use `enabled` to perform a policy lookup based upon the source realm of the referring party (the issuer of the REFER).

16. Save and activate your configuration.

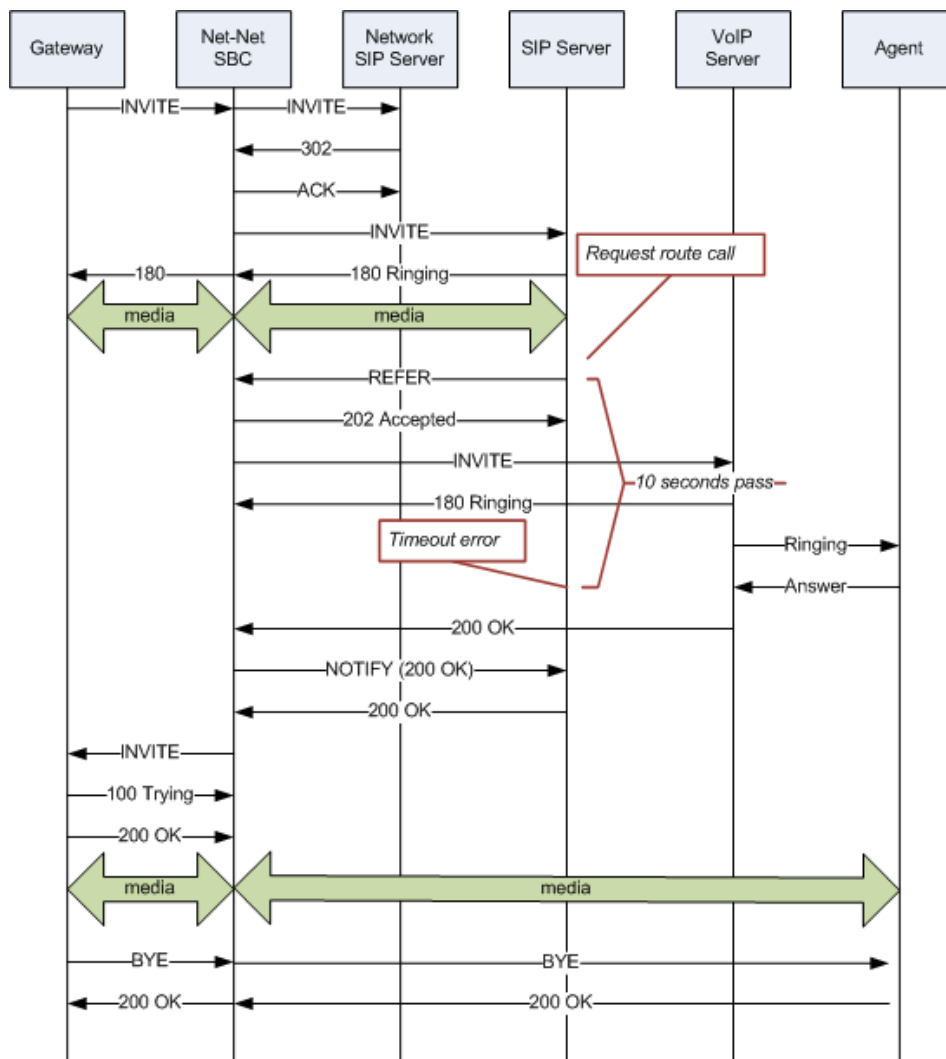
180 & 100 NOTIFY in REFER Call Transfers

When you configure your Oracle Communications Session Director to support REFER call transfers, you can enable it to send a NOTIFY message after it has sent either a 202 Accepted or sent a 180 Ringing message. If your network

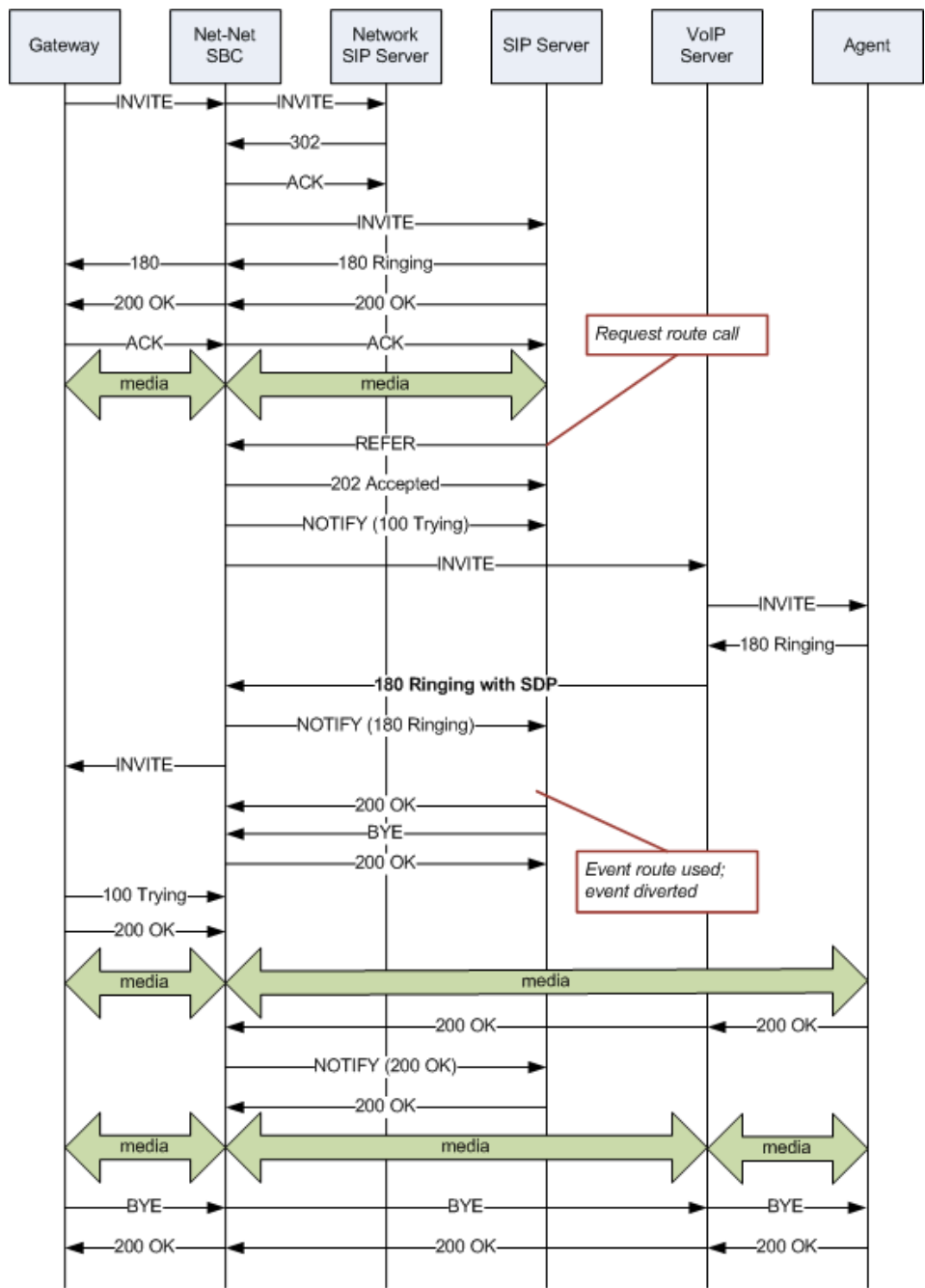
contains elements that comply with RFC 5589, and so expect the NOTIFY message after the 202 Accepted and each provisional 180 Ringing, you want to set the refer-notify-provisional to either initial or all, according to your needs.

Without this parameter changed from its default (none), the Oracle Communications Session Director does not return send the NOTIFY until it receives the 200 OK response from the agent being called. If the time between the REFER and the NOTIFY exceeds time limits, this sequencing can cause the Oracle Communications Session Director's NOTIFY to go undetected by devices compliant with RFC 5589. Failures during the routing process can result.

You can see how a sample call flow works without setting the refer-notify-provisional parameter.



When you compare the call flow above to the one depicting the scenario when the Oracle Communications Session Director has the refer-notify-provisional changed from its default, you can see that the Oracle Communications Session Director now response with a NOTIFY in response to the 202 Accepted and it sends another after the 180 Ringing. This causes the event to be diverted successfully.



Sample Messages

In compliance with RFC 5589, the NOTIFY message with 100 Trying as the message body looks like the sample below. Note that the expires value in the subscription state header is populated with a value that equals 2* TIMER C, where the default value of TIMER C is 180000 milliseconds.

```
NOTIFY sips:4889445d8kjt3@atlanta.example.com;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 73 NOTIFY
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
```

```
Supported: replaces, tdialog
Event: refer
Subscription-State: active;expires=360
Content-Type: message/sipfrag
Content-Length: ...
SIP/2.0 100 Trying
```

Also in compliance with RFC 25589, the NOTIFY message with 180 Ringing as the message body looks like the sample below. Again, the expires value in the subscription state header is populated with a value that equals 2* TIMER C, where the default value of TIMER C is 180000 milliseconds.

```
NOTIFY sips:4889445d8kjdk3@atlanta.example.com;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkpw@biloxi.example.com;gr=3413kj2ha>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 73 NOTIFY
Contact: <sips:3ld812adkpw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, tdialog
Event: refer
Subscription-State: active;expires=360
Content-Type: message/sipfrag
Content-Length: ...
SIP/2.0 180 Ringing
```

Also in compliance with RFC 25589, the NOTIFY message with 200 OK as the message body looks like the sample below.

```
NOTIFY sips:4889445d8kjdk3@atlanta.example.com;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkpw@biloxi.example.com;gr=3413kj2ha>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 74 NOTIFY
Contact: <sips:3ld812adkpw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, tdialog
Event: refer
Subscription-State: terminated;reason=noresource
Content-Type: message/sipfrag
Content-Length: ...
SIP/2.0 200 OK
```

180 and 100 NOTIFY Configuration

You can apply the refer-notify-provisional setting to realms or to session agents. This section shows you how to apply the setting for a realm; the same steps and definitions apply to session agents.

If you do not want to insert NOTIFY messages into the exchanges that support REFER call transfers, you can leave the refer-notify-provisional set to none. This means that the Oracle Communications Session Director will send only the final result NOTIFY message. Otherwise, you want to choose one of the two settings described in the instructions below.

To enable 100 and 180 NOTIFY messages in REFER call transfers:

1. In Superuser mode, type configure terminal and press Enter.

```
ACMEPACKET# configure terminal
```

2. Type media-manager and press Enter to access the media-related configurations.

```
ACMEPACKET(configure)# media-manager
```

3. Type `realm-config` and press Enter. The system prompt changes to let you know that you can begin configuring individual parameters.

```
ACMEPACKET(media-manager) # realm-config
ACMEPACKET(realm-config) #
```

4. `refer-notify-provisional`—Choose from one of the following settings, where the Oracle Communications Session Director:
 - `initial`—Sends an immediate 100 Trying NOTIFY, and the final result NOTIFY
 - `all`—Sends an immediate 100 Trying NOTIFY, plus a notify for each non-100 provisional messages the Oracle Communications Session Director receives; and the final result NOTIFY

```
ACMEPACKET(realm-config) # refer-notify-provisional all
```

5. Save your work.

SIP REFER Re-Invite for Call Leg SDP Renegotiation

Enhancing the original implementation of SIP REFER termination introduced in Release S-C6.0.0, this change to Oracle Communications Session Director behavior allows for SDP renegotiation between both parties of a transferred call.

Scenario

In a call transfer initiated by SIP REFER, a call is established between two user agents, UA-A and UA-B. UA-B then sends a REFER request to transfer the call to UA-C. The challenge is that UA-A and UA-B had already been communicating using mutually agreed-on codec, while UA-C might not be using an entirely different codec.

To solve this problem, the Oracle Communications Session Director causes a new SIP session and new media session to be created between UA-A and UA-C. The Oracle Communications Session Director removes any resources allocated for use between UA-A and UA-B, and then severs its connection with UA-B. The session between UA-A and UA-C continues.

Alterations to SIP REFER

The original implementation of the SIP REFER feature made available in Oracle Communications Session Director Release S-C6.0.0 resulted in instances where SDP parameters were not being communicate properly. Issues arose when the Oracle Communications Session Director maintained the original dialog with the user agent that did not support REFER and failed to communicate and SDP changes to that endpoint.

The alterations to SIP REFER made available in Oracle Communications Session Director Release S-C(X)6.1.0M2 solve those issues. Now, the Oracle Communications Session Director sends re-INVITE with the negotiated SDP to the user agent for which the Oracle Communications Session Director performs the call transfer.

Implementation Details

This section describes the details of how the Oracle Communications Session Director behaves in SIP REFER scenarios with the changes made in Oracle Communications Session Director Release S-C(X)6.1.0M2. The Oracle Communications Session Director makes the new call between Party A and Party C appear as though A were participating to allow the Oracle Communications Session Director's natural media setup occur in the same way as if the REFER had actually been sent to A and A had sent a new INVITE.

When the Oracle Communications Session Director receives a REFER request and determines it needs to handle it locally, it creates a new INVITE made to look like one from Party A. And the Oracle Communications Session Director actually processes this INVITE as though it were from Party A. As a result, new SIP and new media sessions are created with new media ports for Parties A and C. When the INVITE to Party C receives a final response, the Oracle Communications Session Director sends the result to Party B using a SIP NOTIFY request.

If the new INVITE succeeds, the old context and flows disappear and the new context and flows for the A-to-C connection remain in place. Because of the new media ports, the Oracle Communications Session Director sends a re-INVITE to Party A, directing media to the new port and forwarded to Party C. Next, the original dialog with Party B needs to be terminated; if the Oracle Communications Session Director has not received Party B's BYE, it will wait five second and then send Party B a BYE.

If the INVITE to Party C fails, the new SIP and media sessions are deleted as are the new context and flows. The Oracle Communications Session Director treats Party A differently depending on whether or not a BYE was received from Party B. If a BYE was received from Party B, then the Oracle Communications Session Director sends a BYE to Party A. If not, the original SIP and media sessions as well as the context and media flows remain in tact. This way, Party B can re-establish the call with Party A using a re-INVITE. In the case, the Oracle Communications Session Director waits 32 second before sending a BYE.

If the Oracle Communications Session Director receives a BYE while processing the INVITE to Party C, it sends a CANCEL message to Party C in an attempt to cancel the call. The BYE passes to Party B, and associated sessions, contexts, and flows terminate normally. Still, the Oracle Communications Session Director waits for the final response to the INVITE to Party C. If the Oracle Communications Session Director receives a successful response, it sends an ACK and then a BYE to terminate the abandoned call. If the Oracle Communications Session Director receives an unsuccessful final response, it uses its normal response error handling processes. In either of these last two cases, all sessions, context, and flow are deleted.

Please note that the Oracle Communications Session Director does not remove the a=sendonly attribute from the SDP it sends to Party A during the A-to-B call, and extra media ports are not allocated for the original media session.

SIP REFER with Replaces

To support enterprise and call center applications, the Oracle Communications Session Director provides the ability for one party participating in a three-way call to request direct connectivity between the other two parties and to leave the call silently when that connectivity is established. SIP supports this function using the Replaces header in a REFER message, also known as REFER with Replaces.

The most common application of REFER with Replaces handling occurs in a high-level sequence like this:

1. The customer calls a customer service line and reaches—via the Oracle Communications Session Director—an IVR/ACD (Interactive Voice Response system/Automatic Call Distribution system). In some architectures, these are two separate elements.
2. Based on the customer's selection from the menu of options, the IVR/ACD contacts an agent via the Oracle Communications Session Director.
3. Since the ultimate goal is for the IVR/ACD to drop out of the path, it sends a REFER with Replaces to the Oracle Communications Session Director. This message indicates the Oracle Communications Session Director should replace the IVR/ACD endpoint in the call leg with the agent's endpoint.
4. The Oracle Communications Session Director processes the REFER with Replaces, issuing ReINVITEs to the customer with the agent's parameters.
5. The IVR/ACD drops out of the media path once the bridged call between the customer and the agent is established.

Note that direct media connectivity between endpoints must be possible in order for the REFER with Replaces to be carried out properly. For example, if both endpoints (such as the customer and agent from the example above) are behind the same firewall, direct media connectivity should be possible. However, if one endpoint is behind a firewall and the other is not, then direct media connectivity may not be possible.

For licensing capacity purposes, note that a bridged session counts as a single call.

SIP REFER with Replaces Configuration

You enable SIP REFER with Replaces handling either in the realm configuration or in the session agent configuration. This section show you how to configure the feature for session agent, though the steps are the same for adding this feature to a realm.

To enable sending ReINVITES to a referred agent on an existing session/dialog:

1. In Superuser mode, type configure terminal and press Enter.

```
ACMEPACKET# configure terminal
```

2. Type session-router and press Enter.

```
ACMEPACKET(configure)# session-router  
ACMEPACKET(session-router)#
```

3. Type session-agent and press Enter.

```
ACMEPACKET(session-router)# session-agent  
ACMEPACKET(session-agent)#
```

If you are adding support for this feature to a pre-existing configuration, then you must select (using the ACLI select command) the configuration that you want to edit.

4. options—Set the options parameter by typing options, a Space, and then the option name refer-reinvite. Then press Enter.

```
ACMEPACKET(session-agent)# options +refer-reinvite
```

If you type the option without the plus sign, you will overwrite any previously configured options. In order to append the new options to this configuration's options list, you must prepend the new option with a plus sign as shown in the previous example.

SIP REFER-to-BYE

The Oracle Communications Session Director's SIP REFER-to-BYE capability addresses situations when other network elements do not support the REFER method but do offer blind transfer in a SIP BYE request. The target number is encoded in a Reason header of the BYE request. In such cases, the Oracle Communications Session Director terminates the REFER and passes the Refer-To number in a Reason header of the BYE.

You configure both SIP interfaces and SIP session agents with the refer-to-bye option to use this function:

- SIP interface—You add this ability to SIP interfaces facing the SIP elements that need to receive a BYE instead of a REFER. This setting only applies when the next hop is not a session agent.
- SIP session agent—The SIP session agent takes precedence over the SIP interface. You add this ability to SIP session agents that need to receive a BYE instead of a REFER. If the next hop SIP element—the remote target in the dialog—is a session agent, in other words, you need to configure the option for it. Note that when you use this option for SIP session agents, the SIP interface or realm on which the REFER is received takes precedence over the REFER-to-BYE capability.

When a REFER request arrives and the REFER-to-BYE capability applies, the Oracle Communications Session Director responds to it with a 202 Accepted and sends a NOTIFY to terminate the implicit refer subscription. This NOTIFY contains a message/sipfrag body with SIP/2.0 200 OK. Upon receiving the response to this NOTIFY, the Oracle Communications Session Director sends a BYE with an added Reason header (encoded with the Refer-To number) to the other end.

The network element that does not accept REFERs takes the BYE with the Reason header and issues a new initial INVITE that initiates transfer, which the Oracle Communications Session Director sees as starting a new and independent session.

CAC Utilization Statistics via SNMP

The Oracle Communications Session Director allows you to retrieve information on current session utilization and burst rate as a percentage of their configured maximums on per session-agent and/or realm basis. The Oracle Communications Session Director uses the configured max-session and max-burst-rate settings in conjunction with a percentage formula to calculate this value. The system also uses an ACLI configuration setting to establish the threshold at which trap and trap clear messages are sent from the SNMP agent to the configured manager(s).

The user must load the MIB version associated with this software version on all pertinent SNMP managers to query these CAC utilization (occupancy) values and interpret the traps. In addition, the user must configure the threshold at which the system generates the CAC utilization trap. Note that the corresponding clear trap uses the same threshold setting, sending the clear trap when utilization falls below 90% of the threshold.

SNMP Get for CAC Utilization

Using a MIB browser, the user can query the current percentage utilization values for both max-session and max-burst-rate for any session-agent or realm. The calculations for these utilization levels are:

- Session utilization level = (current session count * 100) / max-sessions
- Burst rate utilization level = (current burst rate * 100) / max-burst-rate

The MIB objects associated with these statistics are parallel for session agent and realm and include a table to contain the objects, an object associating the objects containing the values with the applicable table, and objects containing the values themselves. These objects are listed below.

The MIB objects containing CAC utilization data for Session Agents are listed below.

The object establishing the statistics table for session agent CAC utilization follows:

```
--apSip Session Agent Connection Admission Control Stats Table
apSipSaCacStatsTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF ApSipSaCacStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "SIP Session Agent Connection Admission Control Stats Table."
    ::= { apSipMIBTabularObjects 5 }
```

The object establishing the session agent CAC utilization statistics objects follows:

```
apSipSaCacStatsEntry OBJECT-TYPE
    SYNTAX          ApSipSaCacStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "Connection Admission Control Statistics."
    AUGMENTS { apSipSessionAgentStatsEntry }
    ::= { apSipSaCacStatsTable 1 }
```

The session agent CAC utilization statistics values include:

```
ApSipSaCacStatsEntry ::= SEQUENCE {
    apSipSaCacSessionUtilLevel      Gauge32,
    apSipSaCacBurstRateUtilLevel    Gauge32
}
```

The above objects, specifying the CAC utilization value for sessions and burst rate utilization for session agents include:

```
apSipSaCacSessionUtilLevel OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "percentage"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "Current session utilization level."
    ::= { apSipSaCacStatsEntry 1 }

apSipSaCacBurstRateUtilLevel OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "percentage"
    MAX-ACCESS      read-only
    STATUS          current
```

```
DESCRIPTION
    "Current burst rate utilization level."
 ::= { apSigSaCacStatsEntry 2 }
```

The MIB objects containing CAC utilization data for Realms are listed below.

The object establishing the statistics table for realm CAC utilization follows:

```
--apSig Realm Connection Admission Control Stats Table
apSigRealmCacStatsTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF ApSigRealmCacStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "Realm Connection Admission Control Stats Table."
 ::= { apSigMIBTabularObjects 6 }
```

The object establishing the realm CAC utilization statistics objects follows:

```
apSigRealmCacStatsEntry OBJECT-TYPE
    SYNTAX          ApSigRealmCacStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "Connection Admission Control Statistics."
    AUGMENTS { apSigRealmStatsEntry }
 ::= { apSigRealmCacStatsTable 1 }
```

The session agent CAC utilization statistics values include:

```
ApSigRealmCacStatsEntry ::= SEQUENCE {
    apSigRealmCacSessionUtilLevel      Gauge32,
    apSigRealmCacBurstRateUtilLevel    Gauge32
}
```

The above objects, specifying the CAC utilization value for sessions and burst rate utilization for realms include:

```
apSigRealmCacSessionUtilLevel          OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "percentage"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "Current session utilization level."
 ::= { apSigRealmCacStatsEntry 1 }

apSigRealmCacBurstRateUtilLevel        OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "percentage"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "Current burst rate utilization level."
 ::= { apSigRealmCacStatsEntry 2 }
```

CAC Utilization Traps

The Oracle Communications Session Director can issue a trap when either the value of max-session or CAC burst rate exceeds a configured value. The system only sends one trap when the threshold is exceeded. When the value falls back under 90% of this threshold, the Oracle Communications Session Director sends a clear trap.

You configure the value that triggers these traps as a percentage of the max-session and max-burst-rate settings configured for the applicable session agent and/or realm. The system uses the same setting to specify when to send both the sessions and burst rate traps. The name of this parameter is the **cac-trap-threshold**.

For realms, you configure a **session-constraint** element with the **cac-trap-threshold** setting and apply that session constraint to the realm. For a session agent however, you configure the **cac-trap-threshold** directly within the session agent's configuration.

The syntax for the command is the same within session constraint and session agent configurations.

cac-trap-threshold[0-99]

You must express the value as a number less than 100. There is no default setting; the system does not generate a trap if you have not configured this setting.

The `apSipCACUtilAlertTrap` identifies the threshold exceeded on a per-element and per-value (session count or burst rate) for each trap, including:

- `apSipSaCacSessionUtilLevel`
- `apSipSaCacBurstRateUtilLevel`
- `apSipRealmCacSessionUtilLevel`
- `apSipRealmCacBurstRateUtilLevel`

CAC utilization threshold trap on a session agent configuration

The CAC utilization threshold causes the system to generate a trap when session count or CAC max-burst-rate exceeds the configured percentage value of these values maximums. This setting is available within a session agent's configuration.

To configure the CAC trap threshold on a session agent, follow the procedure below.

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

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)# session-agent
ACMEPACKET(session-agent)
```

2. Select the **session-agent** object to edit.

```
ACMEPACKET(session-agent)# select
<hostname>:
1: 192.168.100.101:1813

selection: 1
ACMEPACKET(session-agent)#
```

3. **cac-trap-threshold**—Set the threshold when reached, expressed as a percentage of **max-sessions**, when the CAC trap is sent.
4. Type **done** to save your configuration.

Configuring the CAC Utilization Thresholds - realm

To configure the CAC trap threshold on a realm or sip interface, create a session constraint object and apply it to your realm, as shown below.

1. Use the following sequence to navigate to session constraint elements.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)# session-constraints
ACMEPACKET(session-constraints)#
```

2. Select or create the desired session constraint element.

```
ACMEPACKET(session-constraints)#name trap-at-90-percent
```

3. Configure the desired value for `cac-trap-threshold` expressed as a percentage value, such as 90%, as follows.

```
ACMEPACKET(session-constraints)#cac-trap-threshold 90
```

4. Navigate to the realm-config to which you want to apply the session constraint.

```
ACMEPACKET(realm-config)#session-constraint trap-at-90-percent
```

5. Execute the done and exit commands.
6. Save and activate your configuration.

High Capacity Entries in ifXTable SNMP Table

The AP9200 supports 64-bit counters for interface statistics in the ifXTable object.

The ifXTable supports the following MIB objects which can capture 64-bit values. These standard MIB objects are defined in RFC 2863, The Interfaces Group MIB.

- ifHCInOctets
- ifHCInUcastPkts
- ifHCInMulticastPkts
- ifHCInBroadcastPkts
- ifHCOctets
- ifHCOUcastPkts
- ifHCOMulticastPkts
- ifHCOBroadcastPkts
- ifHighSpeed

Definitions of these MIBs may be found in the rfc2863-if.mib file located in the MIB package accompanying this documentation. This MIB package is clearly labeled to be for S-D7.2.0M2.

S-D7.2.0M3

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-D7.2.0M3.

- Current patch baseline: S-D7.2.0M2

Content Map

This section lists all new content appearing in Release S-D7.2.0M3.

Content Type	Description
Firmware update	

Caveats and Known Issues

- Untrusted bandwidth metering on systems with NPU3 cards has been reimplemented in S-D7.2.0M3p1. Note that the default value of `media-manager > max-untrusted-signaling` is 100. If left to this default, all trusted signaling traffic is denied. Thus it is advisable to set this parameter to a usable value for your network. One best current practice is setting `max-untrusted-signaling` to 30, for an enforced 70/30 split of trusted/untrusted traffic.

Oracle recommends that you change the `max-untrusted-signaling` value as required before the performing the software upgrade.

