Release Change Reference, StarOS Release 21.18/Ultra Services Platform Release 6.12

First Published: 2020-03-06

Last Modified: 2022-03-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

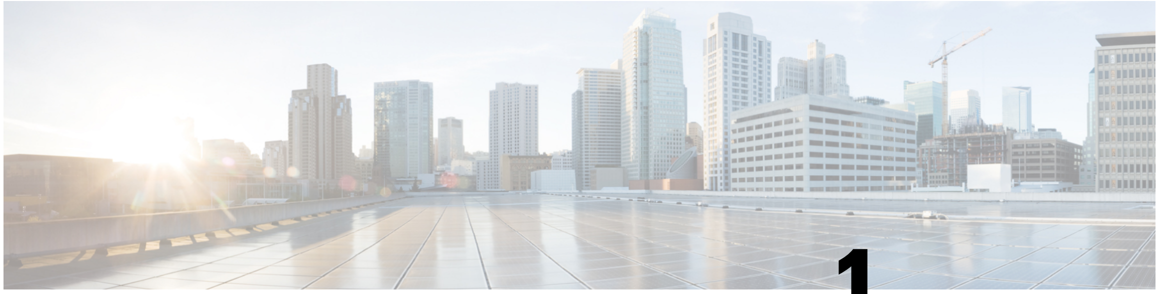
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.



CHAPTER 1

Release 21.18/N6.12 Features and Changes Quick Reference

Release 21.18/6.12 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Configuring UE Radio Capability IE Size, on page 9	MME	21.18
Deprecation of Manual Scaling, on page 11	UAS	6.0
Device ID in EDNS0 Records for DNS over UDP and TCP, on page 13	P-GW	21.18.23 21.18.21
Diameter Route Table Entries Display Limit and Filtration Enhancement , on page 25	• P-GW • SGW • SAEGW • GGSN	21.18.25
Enhancement to Data Record File Transfer in a Single SFTP Session, on page 27	All	21.18.15
Events Monitoring, on page 31	MME	21.18
GTPV1/V2 Echo Support for Peer MME and SGSN, on page 43	MME	21.18
Handling User Session During CCR-RAR Collision, on page 49	GGSN, HA, P-GW, PDSN	21.18.1

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
IPv4/IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW, on page 59	P-GW	21.18.25
MME Support for EN-DC SON Configuration Transfer IE on S1-AP, on page 61	MME	21.18
Routing Based on Realm name MME, on page 65	MME	21.18
RTLLI Management for 2G M2M Devices, on page 69	SGSN	21.18
TAI-based Routing for 20-bit and 28-bit eNB ID, on page 73	MME	21.18

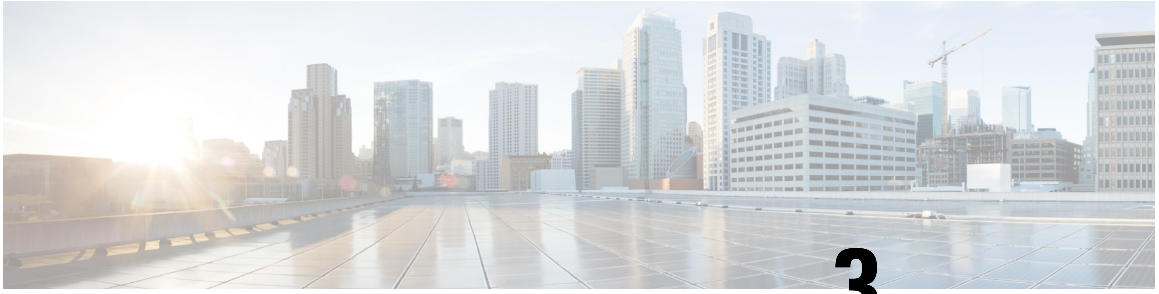
CHAPTER 2

Feature Defaults Quick Reference

Feature Defaults

The following table indicates what features are enabled or disabled by default.

Feature	Default
Attach Reject Random TLI statsto be printed per LAC Enhancement	Disabled - Configuration Required
Configuration of UE Radio Capability IE Size	Enabled - Configuration Required
Deprecation of Manual Scaling	Disabled - Configuration Required
Device ID in EDNS0 Records for DNS over UDP	Disabled – Configuration Required
Enhancement to Data Record File Transfer in a Single SFTP Session	Disabled - Configuration Required
Events Monitoring	Disabled - Configuration Required
GTPV1/V2 Echo Support for Peer MME and SGSN	Disabled - Configuration Required
Handling User Session During CCR-RAR Collision	Enabled-Always-On
IPv4/IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW	Enabled-Always on
MME Support for EN-DC SON Configuration Transfer IE on S1-AP	Disabled - Configuration Required
Routing based on Realm Name MME	Disabled - Configuration Required
TAI-based Routing for 20-bit and 28-bit eNB ID	Disabled - Configuration Required



CHAPTER 3

Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.18 software release.

Important For more information regarding bulk statistics identified in this section, see the latest version of the *BulkstatStatistics_document.xls* spreadsheet supplied with the release.

Bulk statistics changes for 21.18 include:

New Bulk Statistics

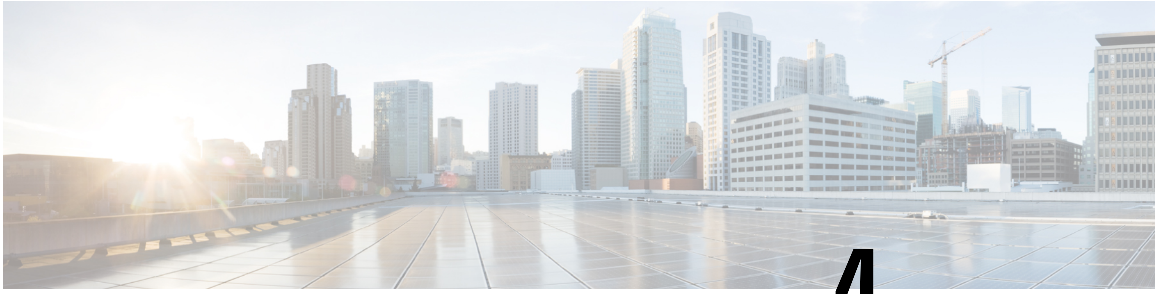
None in this release.

Modified Bulk Statistics

None in this release.

Deprecated Bulk Statistics

None in this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.18 and USP 6.12

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.18 and Ultra Services Platform (USP) 6.12 software releases.

SNMP MIB Object Changes for 21.18

This section provides information on SNMP MIB alarm changes in release 21.18.

Important For more information regarding SNMP MIB alarms in this section, see the *SNMP MIB Reference* for this release.

New SNMP MIB Object

This section identifies new SNMP MIB alarms available in release 21.18.

None in this release.

Modified SNMP MIB Object

None in this release.

Deprecated SNMP MIB Object

None in this release.

SNMP MIB Alarm Changes for 21.18

There are no new, modified, or deprecated SNMP MIB alarm changes in this release.

SNMP MIB Conformance Changes for 21.18

This section provides information on SNMP MIB alarm changes in release 21.18.

Important For more information regarding SNMP MIB alarms in this section, see the *SNMP MIB Reference* for this release.

New SNMP MIB Conformance

None in the release.

Modified SNMP MIB Conformance

None in the release.

Deprecated SNMP MIB Conformance

None in the release.

SNMP MIB Object Changes for 6.12

There are no new, modified, or deprecated SNMP MIB object changes in this release.

SNMP MIB Alarm Changes for 6.12

There are no new, modified, or deprecated SNMP MIB alarm changes in this release.

SNMP MIB Conformance Changes for 6.12

There are no new, modified, or deprecated SNMP MIB conformance changes in this release.

CHAPTER 5

Configuring UE Radio Capability IE Size

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• Command Line Interface Reference • MME Administration Guide

Revision History

Revision Details	Release
Configuration of UE Radio Capability IE Size	21.5.26
Configuration of UE Radio Capability IE Size Introduced to 21.18 release.	21.18
Configuration of UE Radio Capability IE Size Introduced to 21.17 release.	21.17.6
First introduced.	21.12.15

Feature Changes

Previous Behavior: When the UE sends its UE Radio Capability packet exceeding 6000 bytes to the MME, the MME is unable to respond to any subsequent Service Request. MME drops the message as the maximum S1AP packet size limit is 6144 bytes.

New Behavior: MME checks the size of UE Radio Capability IE in UE Capability Information Indication message with the configured limit size from New CLI is introduced to limit the size of UE Radio Capability IE.

Command Changes

This section describes the CLI configuration required to configure UE Radio Capability IE size.

Configuring the UE Radio Capability IE

Use the following configuration to set the size of UE Radio Capability IE.

```
configure
  context context_name
    mme-service mme_service_name
    s1-mme ue-radio-cap
    s1-mme ue-radio-capsize
    no s1-mme ue-radio-cap
    end
```

NOTES:

- **ue-radio-cap**: Sets the size of UE Radio Capability IE default value 5632 bytes.
- **ue-radio-cap size**: Specifies the size of UE Radio Capability IE in bytes. **size** must be an integer in the range of 3072 to 9000 .
- **no s1-mme ue-radio-cap** Disables the UE radio capability size limit.

CHAPTER 6

Deprecation of Manual Scaling

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	UAS
Applicable Platform(s)	UGP
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Ultra M Solutions Guide* • *Ultra Services Platform Deployment Automation Guide*

Revision History

Revision Details	**Release**
The support for manual scale-in and scale-out functionality has been deprecated in this release.	6.0 through 6.14
First introduced	6.0

Feature Changes

Previous Behavior: In previous releases, the Service Function (SF) scaling (including the manual scale-in and scale-out) feature was supported.

New Behavior: In this release, the manual scale-out and scale-in functionalities have been deprecated. For more information, contact your Cisco account representative.

CHAPTER 7

Device ID in EDNS0 Records for DNS over UDP and TCP

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product (s) or Functional Area	P-GW
Applicable Platforms	• ASR 5500 • UAS • VPC-SI • VPC-DI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *Command Line Interface Reference*

Revision History

Table 2: Revision History

Revision Details	Release
The EDNS feature is enhanced to support both UDP and TCP protocols.	21.18.23
First Introduced	21.18.21

Feature Description

The Device ID in EDNS0 offers each enterprise with a customized domain blocking through Umbrella. To enable this functionality:

- The P-GW must reformat a subscriber DNS request into an EDNS0 request, and
- The P-GW must include an Umbrella "Device ID" in the EDNS0 packet so that the Umbrella DNS resolver can use the Device ID to apply the domain filter associated/configured with the Device ID in the EDNS0 packet.

Presently, the PCRF/PCF passes the content filtering policy ID to the P-GW in the Gx events (CCA-I/CCA-U/RAR). The gateway uses the content filtering policy ID to apply content filtering functionality to the subscriber:

As part of this feature, a new configurable EDNS0 content filtering range parameter to trigger the EDNS0 functionality is supported in P-GW to accept and use the full 64-bit Device ID from the PCRF/PCF. The new configurable parameter determines if the subscribers can have a content filtering service or an EDNS0 service.

Note The Device ID in EDNS0 records for DNS over UDP or TCP feature is based on the existing content-filtering license.

Also, P-GW allow subscribers to utilize both the content filter service and EDNS0 services. P-GW follows the following mechanism:

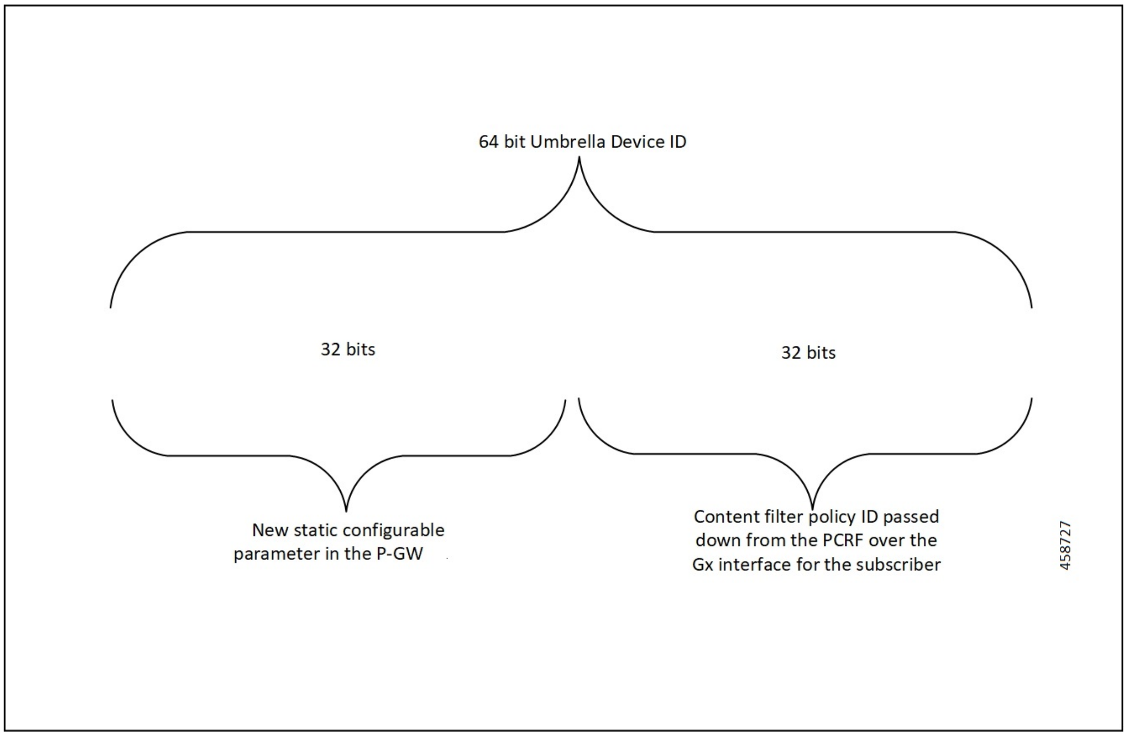
- In the EDNS0 packet, 64-bit Device ID is sent as OPT RR data.
- In the P-GW, the first (MSB) 32-bits of all Device IDs is configured as a fixed value.
- The content filter ID, which is the last (LSB) 32-bits of a subscriber's device ID is received from the PCRF over the Gx interface.
- The P-GW concatenates the two 32-bit values to build a subscriber's full 64-bit Device ID and displays in the subscriber's EDNS0 queries.

As part of this feature, using CLI command you can configure the first 32 bit of **static device-id** value addition.

How it Works

New CLIs are introduced to configure and trigger the EDNS0 functionality.

Figure 1:


64 bit Umbrella Device ID
32 bits
32 bits
New static configurable parameter in the P-GW
Content filter policy ID passed down from the PCRF over the Gx interface for the subscriber
458727

- To create a Device ID and send in EDNS0 query, the Content Filtering ID, which P-GW receives in Gx messages from PCRF is used. The EDNS0 packet includes the 64-bit device ID as OPT RR data.

Note The first 32 bits of all device IDs is a fixed value configured in the P-GW. The last 32 bits of a subscriber device ID is the content filter policy ID value received from the PCRF over Gx Interface.

- The CF-Policy-ID from the PCRF is received in any Gx event (CCA-I/CCA-U/RAR), when there is any change in the CF-Policy-ID, subscriber call line gets updated with the same ID. Later, based on this CF-Policy-ID, configured range gets evaluated at the time of the creation of the new flow.

Note To trigger EDNS0 encoding, it is mandatory that subscriber should get any Gx event, either of CCAI/CCAU/RAR from the PCRF and that event must contain CF policy ID AVP.

- Once CF-Policy-ID is received in Gx event for a subscriber, further on every Gx event range evaluation takes place, irrespective of the CF-Policy-ID presence in any Gx event. This allows to apply the range updates to the new flow.
- The trigger to create new flow is associated with the service-scheme configuration. Service-scheme configuration is associated with the subscriber, which is associated with the subscriber class.

  Note Range evaluation is done only during the flow creation. If flow1 is ongoing and if any change in the range configuration happens, it takes effect only during the new flow creation for that subscriber.

- To create the flow associated with service scheme, association of the trigger condition and the trigger action is used. Then external-content-filtering trigger condition gets evaluated for the same flow, and associated trigger actions (edns-encoding/ip-readdressing) is taken on that flow. If no CF-Policy-ID is received in Gx event, then previous value is used.

  Note When Security-profile has device-id configured instead of cf-policy-id-static-prefix, eDNS encoding is done with prefix all 00 for MSB 32 bits and PCRF received value as LSB 32 bits.

- The P-GW concatenates the two 32-bit values to build a subscriber full 64-bit Device ID for populating in the subscriber EDNS0 queries. New CLI helps to configure the first 32 bit of static device-id value.

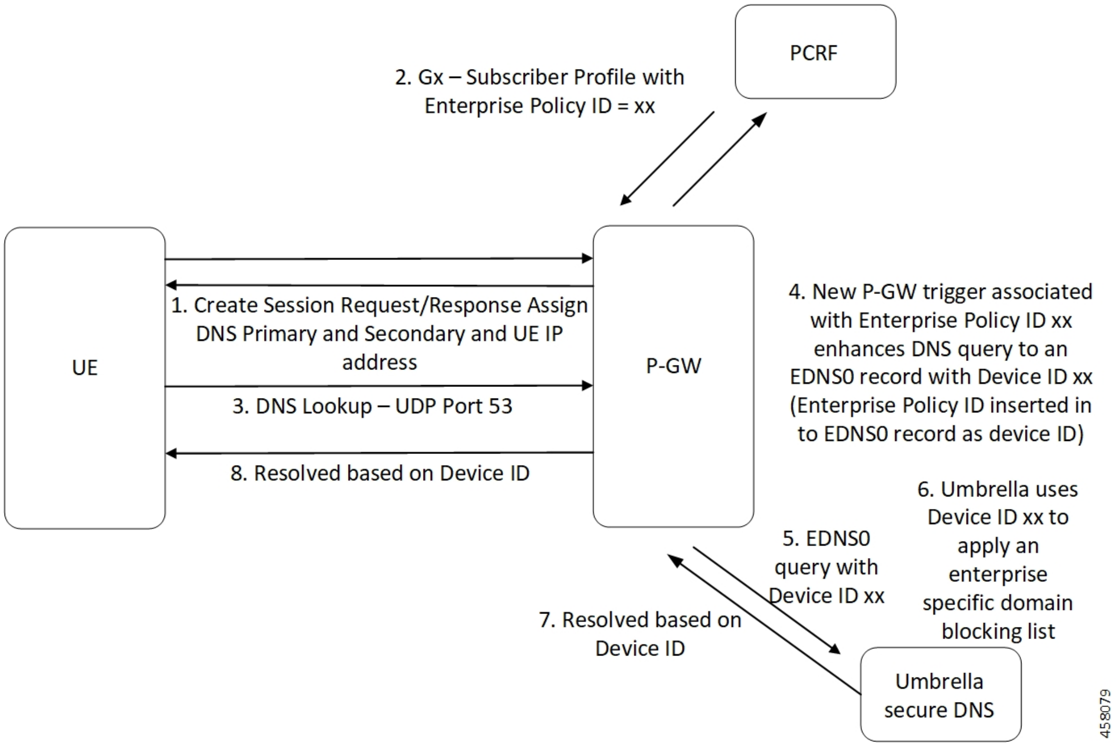
The Device ID number in the EDNS0 record allows the Umbrella DNS system to apply a custom set of domain filters for the EDNS0 queries.

Note DNS analyzer configuration is mandatory for this feature.

Process Flow

The following process flow describes about the Content Filtering enhancement to insert Device ID in EDNS0 records:

Figure 2:


PCRF
2. Gx – Subscriber Profile with Enterprise Policy ID = xx
UE
P-GW
1. Create Session Request/Response Assign DNS Primary and Secondary and UE IP address
3. DNS Lookup – UDP Port 53
8. Resolved based on Device ID
4. New P-GW trigger associated with Enterprise Policy ID xx enhances DNS query to an EDNS0 record with Device ID xx (Enterprise Policy ID inserted in to EDNS0 record as device ID)
6. Umbrella uses Device ID xx to apply an enterprise specific domain blocking list
5. EDNS0 query with Device ID xx
7. Resolved based on Device ID
Umbrella secure DNS
458079

EDNS over TCP

The EDNS over TCP feature supports an enterprise/group offer that allows each enterprise to have customized domain blocking through Umbrella. As part of this feature, unlike UDP, the need for extra messages and extra processing of the TCP sequence (seq) and acknowledgment (ack) numbers is required.

The TCP massager acts between the UE and EDNS Server and UE will massage the seq/ack number changes. Through this process, the UE and EDNS server is unaware of the TCP packets that are manipulated at the P-GW.

Delay Charging and Post Processing

For TCP DNS flows, if delay charging is enabled, you need to enable post processing feature in ACS.

This enables post processing of packets even if rule matching for packets is disabled. When delay charging is enabled, initial TCP handshake packets, such as the SYN and SYN/ACK, does not get processed and IP readdressing is not applied. To apply IP readdressing correctly, apply post processing rule feature, which enables the processing of initial handshake packets, and thus packets are readdressed correctly.

EDNS0 Packet Format

The enterprise policy ID (CF_POLICY_ID) from PCRF helps to create the Device ID. The PCRF sends the device ID to the P-GW. Adding the Device ID to the DNS packet helps in creating the EDNS0 packet. The format of EDNS0 packets is specified by RFC2671. The following are few specifics:

- Following is the structure for the fixed part of an OPT RR:

```
Field Name   Field Type     Description
------------------------------------------------------
NAME         domain name    empty (root domain)
TYPE           u_int16_t          OPT
CLASS          u_int16_t          sender's UDP payload size
TTL            u_int32_t          extended RCODE and flags
RDLEN          u_int16_t          describes RDATA
RDATA          octet stream       {attribute, value} pairs
```

- Following is the variable part of an OPT RR encoded in its RDATA:

```
      +0  (MSB)                           +1  (LSB)
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
0: |                       OPTION-CODE                             |
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
2: |                       OPTION-LENGTH                           |
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
4: |                                                               |
   /                       OPTION-DATA                             /
   /                                                               /
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

  - OPTION-CODE: Assigned by IANA
  - OPTION-LENGTH: Size (in octets) of OPTION-DATA
  - OPTION-DATA- Varies per OPTION-CODE

Example: If received policy-id from PCF/PCRF is “1234” and static prefix configured on P-GW is “5678”.

64-bits Device-ID will be “0000162e000004d2”.

- 0000162e -- 5678 (Decimal)
- 000004d2 -- 1234 (Decimal)

RDATA 69 42 00 0f 4f 70 65 6e 44 4e 53 00 00 16 2e 00 00 04 d2

- 6942 -- option-code
- 000f -- option-length
- 4f70656e444e53 -- OpenDNS (String)
- 0000162e -- 5678 (MSB)
- 000004d2 -- 1234 (LSB)

EDNS with IP Readdressing

The new CLI is configured within trigger action to readdress the DNS traffic to the Umbrella DNS. This CLI uses the existing readdress server list configuration from the ACS service. Readdressing of packets based on the destination IP address of the packets enables redirecting gateway traffic to configured server/port in the readdressed server list.

Behavior and Restrictions

Following are the behavior and restrictions applicable for this feature:

- Trigger Condition is evaluated at flow creation time. Any change in trigger condition in between the flow doesn't affect the existing flow but affects the new flows.
- Any change to trigger action is applicable on the same flow.
- Cases where the 'security-profile' CLI is not associated with the 'EDNS format' CLI in Trigger Action, the device-id in the outgoing EDNS packet is sent with only 32-bit CF Policy ID.
- DNS queries with type other than A, AAAA, CNAME, NS, PTR, SRV, TXT, NULL are not to be EDNS converted.
- CF Policy ID change over Gx in between inflow are not applicable for the current flows. The current flows continue to insert the CF Policy ID present at the time of flow creation.

Limitations

Following are the limitations for this feature:

- When malformed DNS packet is received by analyzer and marked invalid, packets gets EDNS encoded and readdressed as a normal DNS packet.
- When PCRF sends cf-policy-id 0 and external-content-filtering config as true in trigger condition, trigger condition does not match and encoding/readdressing does not apply.
- When there is configuration change in content-filtering range for any subscriber, it disables EDNS feature and enables the content filtering feature. EDNS disables for the next flow. To enable content filtering feature, it is mandatory to trigger the Gx event with cf policy ID from PCRF.
- If packet received with additional RR value as FFFF, the EDNS encoding is not done and marked as EDNS failure. In this case even if EDNS encoding fails readdressing happens.
- The feature does not support the interoperability with next hop and vlan ID.
- The CLI available in trigger action supports only server list configuration, It does not support single server IP or port configuration like charging action.
- Due to several limitations in the DNS Analyzer it does not support TCP Segmentation and it does not recognize multiple queries in the same data packet. These limitations affects the processing of statistics in both DNS Queries and Responses.
- EDNS encoding is implemented at the layer 4 TCP level with the following limitations:
  - If this CLI setting is not set, each segment is processed as an EDNS failed encoded packet.
  - The mechanism relies on the DNS Payload length not being corrupted/incorrect.
  - The mechanism rejects segments lower than 14 bytes in size.

Configuring EDNS0

Use the following configuration to configure Content Filtering Range, Trigger Action, Trigger Condition, edns static prefix, edns fields and edns tags under the active changing service.

```
configure
   active-charging-service service_name
   [default] content-filtering range range
      trigger-condition trigger_condition_name
         app-proto = dns
         external-content-filtering
                end
```

NOTES:

- **app-proto = dns** : Avoids the IP readdressing of the non-DNS traffic. If this CLI is enabled with multiline-or cli, then all DNS traffic will be EDNS encoded.
- **external-content-filtering** : Enables EDNS0 feature.When this flag is true along with the range criteria, EDNS0 feature is enabled. By default, this flag is disabled.
- **content-filtering range**: Enter start number and end number for the **cf-policy-id**. *range_values* can be integers. For example, 1-4294967295.
- If range parameter is set to 1-1000, any subscriber with a content filtering policy ID greater than or equal to 1 and lower than or equal to 1000 should use the standard content filtering functionality. And any subscriber profile with a content filter policy ID outside the range of 1-1000 can trigger the new EDNS0 functionality.
- **default** : By default, the content-filtering range is 1 to 4294967295. Any value in CF-Policy-ID AVP is considered for CF. It will not be shown by default and will be shown in verbose config. To restore default functionality, use the cli **default content-filtering range**

If the content filter policy ID for any Subscriber profile is outside the range of 1 to 1000, use the following CF policy id range CLI commands to enable the new EDNS0 functionality.

```
configure
   active-charging-service service_name
   content-filtering
         category
         range
           content-filitering range range_start_number to range_end_number
           content-filtering range 1 to 1000
           [ default ] content-filtering
           [ no ] content-filtering
        end
```

NOTES:

- **range**: Specifies policy-id range for content filtering feature.
- **content-filitering range** : Enter the starting number and ending number for the cf-policy-id range. *range_start_number* to *range_end_number* can be integers. For example, 1-4294967295.
- **no content-filitering range**: When chassi comes up, the **no content-filitering range** CLI is displayed in verbose.
- **default content-filitering range**If you configure a default content filtering range, then range configured should be between 1 to 4294967295. In this scenario CF-Policy-ID value that comes up in Gx event is considered for Content Filtering. You can view this range in both verbose and non- verbose mode.

- If you change either the minimum or maximum value, any value outside this range is for EDNS. To restore default functionality, the **default content-filtering range** CLI.

The following configuration leads the trigger action to define the EDNS format to be inserted in the EDNS packet. The following CLI also associates the security profile with the EDNS format as part of the trigger action:

```
configure
   active-charging-service service_name
      trigger-action trigger_action_name
         edns-format format_name [ security-profile ] profile_name
         flow action readdress server-list  server_list_name  [ hierarchy ] [
round-robin ][ discard-on-failure ]
            end
```

NOTES:

- **trigger-action** *trigger_action_name*: To use EDNS with IP readdressing configure the flow action CLIs in the trigger action.
- **edns-format** *format_name*: Use the EDNS format when EDNS is applied.
- **security-profile** *profile_name*: Defines the security profile configuration in the EDNS to add mapping with the Device-id.
- **flow action readdress server-list** *server_list_name* **[hierarchy] [round-robin][discard-on-failure]**: Use IP readdressing to readdress the packets to the configured server Ips. This CLI in trigger action supports only server list configuration. It does not support single server IP or port configuration like charging action.

In the ACS You can configure the trigger condition and trigger action under service-scheme:

```
configure
   active-charging-service service_name
       service-scheme service-scheme_name
           trigger flow-create
            priority  number trigger-condition value trigger-action value
            end
```

NOTES: For readdressing, port configuration in server list is not mandatory. In case only readdressed server IP is configured under server-list, destination port from incoming packet is used for readdressing.

Use the following configuration to insert the CF policy ID in the EDNS:

```
configure
   active-charging-service service_name
      edns
         security-profile  security_profile cf-policy-id-static-prefix
static_prefix_value
         fields fields_name
            [ default ] tag  number cf-policy-id  payload-length ( tcp | udp
 )
            end
```

NOTES:

- **security-profile**: Security profile is used to configure the 32 MS bit static value.

- **cf-policy-id-static-prefix** *static_prefix_value*: Enter the integer value.

  The 32 bit static ID is used as MSB bytes in 64 bit device ID. If security-profile static prefix does not have any **cf-policy-id-prefix** defined, then device-id is encoded with only 32 bit **cf-policy-id**.

- **payload-length (tcp | udp)**: Specifies the RR UDP or TCP Payload-length value. You can enter the value ranging from 512 to 4096.
- **tcp** : Specifies the RR UDP-Payload-Length value for TCP.
- **udp** : Specifies RR UDP-Payload-Length value for UDP.

  Note If the optional **udp** or **tcp** CLI **payload-length** field is not configured, a default value of 1280 is added into the EDNS **Additional RR CLASS/UDP Payload size** field.

- **default tag** *number* **cf-policy-id** : Resets the UDP or TCP payload-length field to an unconfigured default value of 1280.

  Note If you enter a **default tag** *number* on a tag number that is not configured, the following error message is displayed:

```
Failure: Cannot reset the payload-length value as no such tag value
configured with cf-policy-id in edns field.
```

Sample Configuration

Following is the sample configuration for configuring the EDNS packets:

```
config
  active-charging service ACS
    content-filtering range 1 to 1000
    edns
      security-profile SP1 cf-policy-id-static-prefix 999999
      fields CFPiD
        tag 1 cf-policy-id
        #exit
      format FP1
        fields CFPiD encode
        #exit
      #exit
   readdress-server-list SL
     server 40.40.40.3
     server 4001::3
   #exit
   ruledef dns_route
     udp either-port = 53
     rule-application routing
   #exit
   rulebase RB1
      route priority 100 ruledef dns_route analyzer dns
   #exit
   trigger-action TA1
      edns format FP1 security-profile SP1
      flow action readdress server-list SL
   #exit
   trigger-condition TC1
      app-proto = dns
      external-content-filtering
   #exit
   service-scheme SS1
      trigger flow-create
      priority 1 trigger-condition TC1 trigger-action TA1
    #exit
   subs-class SC1
      rulebase = RB1
   #exit
   subscriber-base SB1
      priority 1 subs-class SC1 bind service-scheme SS1
   #exit
#exit
```

Viewing Configured and Unconfigured Payload-length Values

show config | grep tag

Use the following sample configuration to view configured tag number cf-policy-id payload-length values:

```
[local]qvpc-si# show config | grep tag
        tag 1 cf-policy-id payload-length udp 1300
```

show config verbose | grep tag

Use the following sample configuration to view the configured and unconfigure tag number cf-policy-id payload-length values.

```
[local]qvpc-si# show config verbose | grep tag
         tag 1 cf-policy-id payload-length udp 1300 tcp 1280
```

show configuration active-charging service name acs v | grep range

Use the sample configuration to view the EDNS statistics:

```
[local]qvpc-si(config-acs)#  no content-filtering range
        [local]qvpc-si# show configuration active-charging service name
         acs v | grep range no content-filtering range
        [local]qvpc-si#
```

Monitoring and Troubleshooting

Following are the show commands and outputs that enhance content filtering support to Insert device ID in EDNS0 records.

Show Commands and Outputs

Following are the show commands and outputs modified to show EDNS statistics and counters.

- **show active-charging trigger-condition name <tc>**: output is modified to include "app-proto = dns" and "external-content-filtering".
- **show active-charging trigger-action name <ta>**: output is modified to include "IP-addressing" and "edns encode".
- **show active-charging analyzer statistics name dns**: output is modified to include the "EDNS Encode Success Bytes" in the "EDNS Over UDP" section.
- **show active-charging session full all**: output is modified to include "GX CF Policy ID".
- **show active-charging service all**: output is modified to include "Range", "Start Value", and "End Value".
- **show active-charging subscribers full imsi <IMSI>**: output is modified to include the following parameters in the EDNS statistics per subscriber.
    - DNS-to-EDNS Uplink Pkts
    - DNS-to-EDNS Uplink Bytes
    - GX CF Policy ID

Note

- EDNS Encode success Bytes have extra added bytes added to convert the packet.
- DNS-to-EDNS Uplink Bytes have complete packet length along with extra bytes added.

CHAPTER 8

Diameter Route Table Entries Display Limit and Filtration Enhancement

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW • GGSN
Applicable Platform(s)	All
Feature Default	Not Applicable
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
Support for a limit and filtration on displaying route entries is added.	21.18.25

Feature Changes

Previous Behavior: The CLI output for the diameter route table does not have any limit and filtration on displaying route entries and this resulted to crash and restart of CLI task when there is a huge list of diameter route entries.

New Behavior: A limit is enforced and expired route entries are filtered while displaying the diameter route entries.

Impact on Customer: As the limit and filtration are enforced for the existing CLI **show diameter route table debug-info**, the changes introduced avoids the CLI task crash/reload for the cases where there is a huge list of diameter route entries to be shown/displayed. This limit is applicable for diameter route display during SSD collection and regular CLI **show diameter route table debug-info** execution.

CHAPTER 9

Enhancement to Data Record File Transfer in a Single SFTP Session

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GTPP Interface Administration and Reference*

Revision History

Revision Details	Release
First introduced.	21.18.15

Feature Changes

Previous Behavior: Each EDR, CDR, or UDR file is pushed to an external storage server through a single SFTP session.

In certain scenarios, it is possible for the file generation rate during busy hours to out-pace the push rate. This results in the development of a backlog that increases in `/hd-raid/` local storage utilization.

New Behavior: In the StarOS 21.18.15 release, new **push-count** keyword is added to the EDR Module Configuration Mode, UDR Module Configuration Mode, and GTPP Server Group Configuration Mode. The **push-count** keyword allows users to send higher quantities of files during a single SFTP session. Higher **push-count** values can significantly increase the rate at which files are pushed to the external storage server in a single session.

Customer Impact: Pushing more files through a single SFTP session reduces the overall number of SFTP sessions required thus saving the time it would take to establish those sessions. This is especially useful in networks where it takes significant time (For example, 1-2 seconds) to establish individual SFTP sessions.

Command Changes

The **push-count** keyword has been added to several commands to set the number of EDR/CDR/UDR files that are transferred to the external storage server during a single SFTP connection.

```
configure
   context context_name
      edr-module active-charging-service
         cdr push-count push_count
         default cdr push-count
         exit
```

The **push-count** keyword has been added to UDR Module Configuration mode command:

```
configure
   context context_name
      udr-module active-charging-service
         cdr push-count push_count
         default cdr push-count
         exit
```

Notes:

- **push-count** *push_count*: Specifies the number of EDR/CDR/UDR files transferred in each EDR/UDR push SFTP session. Default value is "1". *push_count* is configured as an integer value between 1 and 32, inclusive.

Important When *push_count* is set to “1”, file transfer operation is functionally identical to legacy behavior.

The **push-count** keyword has been added to GTPP Server Configuration mode command:

```
configure
   context context_name
      gtpp group group_name
         gtpp storage-server local file push-count push_count
         no gtpp storage-server local file push-count
         exit
```

Notes:

- **push-count** *push_count*: Specifies the number of EDR/CDR/UDR files transferred to remote system in each push to SFTP session. Default value is "1". *push_count* is configured as an integer value between 1 and 32, inclusive.

  > **Important** When *push_count* is set to “1”, file transfer operation is functionally identical to legacy behavior.

- **no**: Disables the push-count functionality.

CHAPTER 10

Events Monitoring

Feature Description

The Event Monitoring functionality allows monitoring of specific events in the 3GPP system and makes the event information available through either Service Capability Exposure Function (SCEF) or Home Subscriber Server (HSS). Allows the identification of the 3GPP network elements that are suitable for configuring specific events, detecting events, and reporting events to the authorized users.

The following example explains a specific use case for a individual subscriber.

A subscriber can track the following events:

- Location Reporting
- UE reachability
- Availability after DDN failure
- PDN Connectivity Status
- Loss of connectivity
- Communication failure
- Number of UEs available in a geographical location
- or Idle Status Indication for Availability after DDN failure for a specific subscriber (UE) from MME or HSS

  Once the tracking is initiated SCEF queries the MME service and reports the list of events failed or affected for that specific subscriber (UE).

In this release, MME supports monitoring events on s6a and t6a interfaces for monitoring the following events:

- **Number of UEs present in a geographical location** - This is triggered from SCEF to MME in Configuration information request message. MME responds with a configuration information Answer messages with the reports, status and supported AVPs. The following table describes the supported feature AVPs.

Table 3: Supported and Not Supported AVPs

AVPs	Parameters
Number-of-UE-Per-Location-Configuration	**{ EPS-Location-Information }** **[IMSI-Group-Id]**
MME-Location-Information	**[E-UTRAN-Cell-Global-Identity]** **[Tracking-Area-Identity]** **[User-CSG-Information]** **[eNodeB-ID]**

Number-of-UE-Per-Location-Report	**{ EPS-Location-Information }**
	{ UE-Count }
	IMSI-Group-Id
	{ Group-Service-Id }
	{ Group-PLMN-Id }
	{ Local-Group-Id }

Not Supported AVP	
Location Information	**[Geographical-Information]** **[Geodetic-Information]** **[Current-Location-Retrieved]** **[Age-Of-Location-Information]** **[Extended-eNodeB-ID]**

- **Location Reporting** - Montoring Events sends report when the MME detects that the UE changed location with the granularity as requested by the monitoring event configuration. If there is Minimum Reporting Interval, while the timer is running, the MME suppresses sending consecutive Location Reporting notification. On timer expiry MME sends location information that was contained in the latest suppressed Location Reporting notification and restarts the timer.

  Location Reporting is supported for Current Location or the Last Known Location of a UE. The Location Reporting type allows:

  - One Time Reporting: If request is for "Last known" of a UE the supported Accuracy in the network is at either cell level (CGI/ECGI), eNodeB, TA/RA level.
  - Periodic Reporting: Request is for current location type.
  - Continuous Location Reporting: Unless a Minimum Reporting Interval was provided, the serving node(s) sends a notification every time it becomes aware of a location change.

Table 4: Supported and Not Supported AVPs

AVPs	Parameters
Location-Information-Configuration	**[MONTE-Location-Type]** **[Accuracy]** **[Periodic-Time]**
MONTE-Location-Type	**CURRENT_LOCATION (0)** **LAST_KNOWN_LOCATION (1)** **Note** The default value, when this AVP is not included, is LAST_KNOWN_LOCATION (1).
Common Parameter	Maximum number of reports should not be greater than one if Monitoring-Type is LOCATION_REPORTING (2) and MONTE-Location-Type is LAST_KNOWN_LOCATION (1)
MME Location Information	**[E-UTRAN-Cell-Global-Identity]** **[Tracking-Area-Identity]** **[E-UTRAN-Cell-Global-Identity]** **[Current-Location-Retrieved]** **[User-CSG-Information]** **[eNodeB-ID]**
Not Supported AVP	
MME Location Information	**[Geographical-Information]** **[Geodetic-Information]** **[Current-Location-Retrieved]** **[Age-Of-Location-Information]** **[Extended-eNodeB-ID]**

- **UE Reachability** – Monitoring Events reports when UE transitions to ECM-CONNECTED mode (for a UE using Power Saving Mode or extended idle mode DRX) or when the UE reaches for paging (for a UE using extended idle mode DRX).

Table 5: Supported AVPs

AVPs	Parameters
UE-Reachability-Configuration	**[Reachability-Type]** **[Maximum-Response-Time** MME uses the Maximum Response Time as the Active Time for PSM UEs.
Event Reporting	**UE_REACHABILITY (1)** **REACHABLE_FOR_DATA(1)** **Maximum-UE-Availability-Time** **Maximum Latency:** : Sent by SCEF to HSS. HSS uses this Maximum Latency to calculate the subscribed periodic RAU/TAU timer.
Handover Scenatio	**Monitoring Event Information IE, NSR flag, SCEF Ref id, SCEF id, and Remaining number of reports.**

- **Availability after DDN failure** – MME triggers this event when the UE contacts the network. For example, to perform a TAU, or to executes a service request after DDN Failure.

  The SCEF sends Monitoring request without adding Max Number of Reports, since the "Availability after DDN Failure" is an ongoing event that needs explicit deletion to cancel further reports. The information is provided to the serving node (MME) at registration. The serving node notes this and sets a Notify-on-available-after-DDN-failure flag after a DDN failure. If the flag is set when the UE next contacts the network, the serving node notifies the SCEF that the UE is reachable, and clears the flag.

Note Not every DDN failure triggers this event. This event is triggered only when the UE is in PSM or eDRX mode.

Table 6: Supported AVPs

AVPs	Parameters
Event configuration	**Monitoring -Type: AVAILABILITY_AFTER_DDN_FAILURE (6)**
Event Reporting	**Monitoring-Type set to AVAILABILITY_AFTER_DDN_FAILURE (6)**
Handover Scenatio	**Monitoring Event Information IE, NSR flag, SCEF Ref id, SCEF id, and Remaining number of reports.**

- **PDN Connectivity Status** – The following AVPs are supported.

Table 7: Supported AVPs

AVPs	Parameters
Event configuration: HSS to MME	ULA / ISDR Monitoring-Type set to PDN_CONNECTIVITY_STATUS (10) PDN-Connectivity-Status-Configuration [Service-Selection] If the Service-Selection AVP is included, then the monitoring applies to that specific APN. if the If the Service-Selection is not available, the monitoring request applies to all APNs.
PDN-Connectivity-Status-Report	**{ Service-Selection }** **{ PDN-Connectivity-Status-Type }** **[PDN-Type]** **[Non-IP-PDN-Type-Indicator]** **[Non-IP-Data-Delivery-Mechanism]** **[Served-Party-IP-Address]**

- **Loss of Connectivity**– Event is triggered when UE's radio connectivity is lost. HSS configures events HSS through ULA/ISDR messages. Event reporting happens through RIR with event specific parameters. The following AVPs are supported. .

Table 8: Supported AVPs

AVPs	Parameters
Loss-Of-Connectivity-Reason - Identifies the reason of loss of connectivity	**UE_DETACHED_MME (0)** **UE_DETACHED_SGSN (1)** **MAX_DETECTION_TIME_EXPIRED_MME (2)** **MAX_DETECTION_TIME_EXPIRED_SGSN (3)** **UE_PURGED_MME (4)** **UE_PURGED_SGSN (5)**

- **Communication failure** – Event is triggered when the MME becomes aware of a RAN or NAS failure event. Event configuration by HSS through ULA/ISDR messages.

Important Handover and Roaming functions are not supported.

Table 9: Supported AVPs

AVPs	Parameters
Communication-Failure-Information	**[Cause-Type]** **[S1AP-Cause]**

- **Idle Status Indication for Availability after DDN failure and UE reachability** – MME supports Idle Status Indication when the UE transitions into idle mode. The MME includes the time at which the UE transitioned into idle mode, the active time, and the periodic TAU/RAU time granted to the UE by the MME in the notification towards the SCEF, the eDRX cycle length, and the suggested number of downlink packets if a value is provided to the S-GW.

Table 10: Supported AVPs

AVPs	Parameters
Idle-Status-Indication	**[Idle-Status-Timestamp]** – Time at which the UE transitioned into idle mode. **[Active-Time] d** – Shows the active time if PSM is enabled. **[Subscribed-Periodic-RAU-TAU-Timer]** – The periodic TAU/RAU time granted to the UE by the MME in the notification towards the SCEF. **[eDRX-Cycle-Length]** – Shows the eDRX cycle length if eDRX is enabled. **[DL-Buffering-Suggested-Packet-Count]** – Displays the Suggested number of downlink packets if a value is provided to the S-GW.
Handover Scenarois	**Monitoring Event Information IE, NSR flag, SCEF Ref id, SCEF id, and Remaining number of reports.**

- **External-identifier on MME for monitoring events**

  – The External-identifier feature is applicable for the ULR/ULA, DSR/DSA and IDR/IDA command pairs over S6a (and S6d), when the MME (or combined MME/SGSN) supports the External-identifer.

  - If the MME/SGSN includes the External-Identifier or the MSISDN if present in the subscription data received from the HSS, the UE contains the identity of the UE, which is a grouped AVP that contains MSISDN or the External-identifier.

Note If the MME or combined MME/SGSN does not support External-identifier:

- The HSS shall not send the External-Identifier subscription data to the MME or combined MME/SGSN within ULA.
- The HSS shall not send Monitoring Event configuration for UEs that are part of a group and have no MSISDN as part of its subscription data to the MME/SGSN.
- The HSS shall not indicate External-Identifier-Withdrawal in the DSR-Flags AVP of the DSR.

- Gtpv2 handover scenarios
- For adding **TAC** field in the Monitoring reporting information requests (RIR) from MME

How it Works

This section describes how montoring events work for the following two events:

- **Number of UEs present in a geographical location** – The UE information is exchanged by MME and SCEF based on the requested TAI through Configuration Information Request (CIR) and Configuration Information Answer (CIA) messages.
- **Communication failure** – Communication failure events that happend between MME and HSS can be monitored. The communication failure event is monitored when HSS sends a communication failure message in the monitoring event configuration. In MME, the message is received through Insert Subscriber Data Request (ISDR) on s6a interface. The MME sends the Monitoring Event Report for the communication failure event to SCEF over t6a interface through RIR (Reporting-Information-Request) messages.
- **External-identifier** – The External-identifier feature is applicable for the ULR/ULA, DSR/DSA and IDR/IDA command pairs over S6a (and S6d), when the MME (or combined MME/SGSN) supports the External-identifer.

  If the MME/SGSN includes the External-Identifier or the MSISDN if present in the subscription data received from the HSS, the UE contains the identity of the UE, which is a grouped AVP that contains MSISDN or the External-identifier.

Note

If the MME or combined MME/SGSN does not support External-identifier:

- The HSS shall not send the External-Identifier subscription data to the MME or combined MME/SGSN within ULA.
- The HSS shall not send Monitoring Event configuration for UEs that are part of a group and have no MSISDN as part of its subscription data to the MME/SGSN.
- The HSS shall not indicate External-Identifier-Withdrawal in the DSR-Flags AVP of the DSR.

Monitoring Events WorkFlow

This section describes the call flows in which the monitoring events procedure are performed.

Figure 3: Call Flow from SCEF to MME

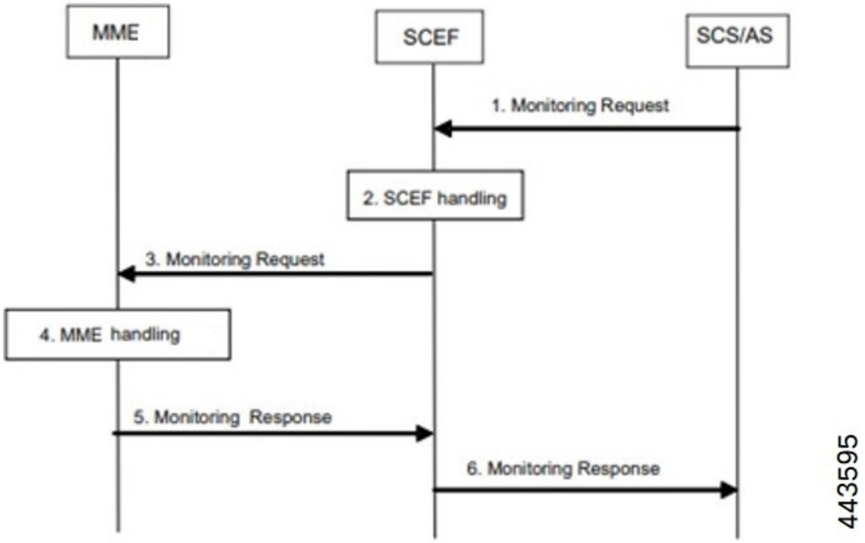


Table 11: Monitoring Event Configuration and Deletion through MME Procedure

Step	Description
1	The SCS/AS sends a Monitoring Request (SCS/AS Identifier, Monitoring Type, Monitoring Duration, Maximum Number of Reports, T8 Destination Address, TLTRI for Deletion) message to the SCEF. The SCEF assigns a TLTRI that identifies the Monitoring Request.

Step	Description
2	The SCEF stores the TLTRI, and also assigns it to an SCEF Reference ID.
3	The SCEF sends a Monitoring Request (SCEF ID, SCEF Reference ID, Monitoring Type, Monitoring Duration, Maximum Number of Reports, SCEF Reference ID for Deletion) message to the MME(s)/SGSN(s).
4	The MME/SGSN examines whether to accept the request from the SCEF based on operator configuration or whether it serves the SCEF Reference ID for Deletion and can delete it. If acceptable, the MME/SGSN stores SCEF ID, SCEF Reference ID, Monitoring Duration, Maximum Number of Reports and other relevant parameters unless it is a One-time request and the Monitoring Event is available to the MME/SGSN at this time. The MME/SGSN deletes the monitoring configuration identified by the SCEF Reference ID for Deletion, if provided.
5	The MME/SGSN sends a Monitoring Response (SCEF Reference ID, Cause) message to the SCEF to acknowledge acceptance of the Monitoring Request and to provide the requested monitoring information or to acknowledge the deletion of the identified monitoring event configuration, if it was requested.
6	The SCEF sends a Monitoring Response (TLTRI, Cause, Monitoring Event Report) message to the SCS/AS to acknowledge acceptance of the Monitoring Request and to provide the requested monitoring information in Monitoring Event Report parameter or to acknowledge the deletion of the identified monitoring event configuration at the time of request.

Figure 4: Monitoring Event Configuration and Deletion through HSS Call Flow

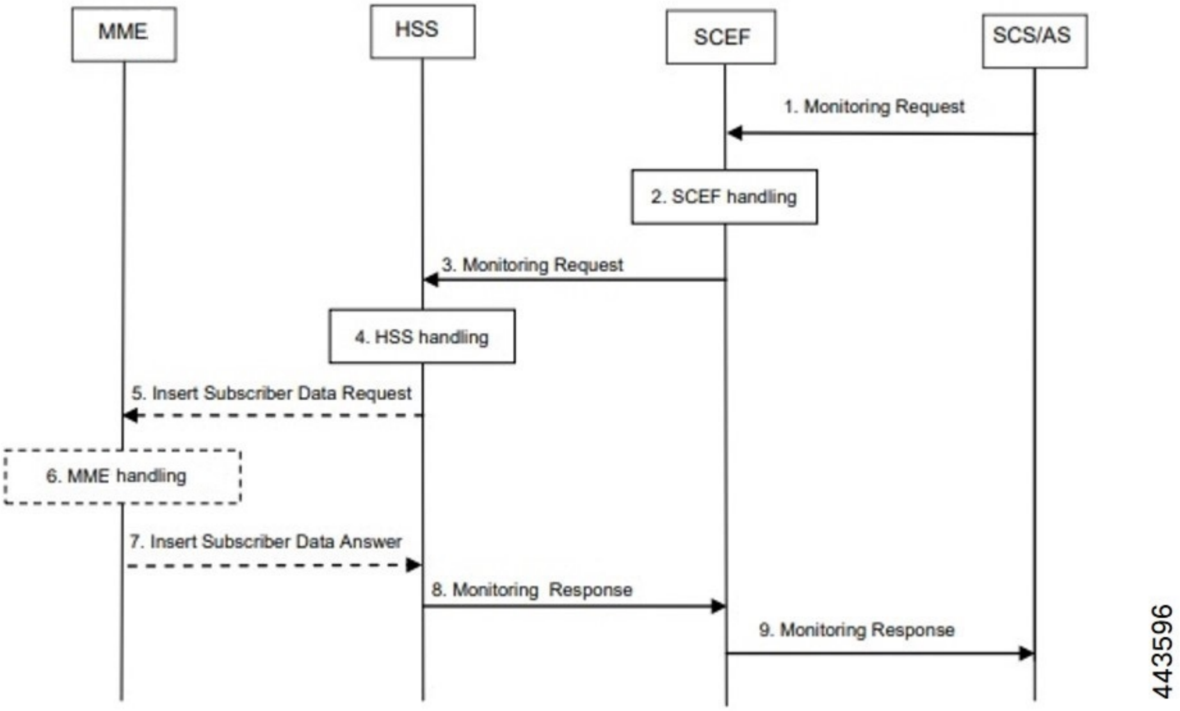


Table 12: Monitoring Event Configuration and Deletion through HSS Procedure

Step	Description
1	The Diamproxy client, which is running on the StarOS device receives Monitoring Event Configuration Requests from the HSS through s6a interface under Subscription data grouped AVP or from the SCEF through t6a in Configuration Information Request message.
2	AVP information received from the device is parsed and the message is sent to corresponding Session Manager for further handling.

Step	Description
3	The Session Manager parses the event message and decodes the appropriate event. **Important** MME running as part of Session Manager identifies if the message is synchronous and responds immediately or asynchronously. Requests from HSS are received in the Update Location Answer(ULA)/Insert Subscriber Data Request(ISDR). If the response is determined as asynchronous, then the response are notified through t6a to SCEF directly.
4	Event handling routine invokes handler for appropriate events.
5	After the event handling, the report is sent through Monitoring Event Report message on s6a and t6a interface. Based on the event type, MME choses to dispatch the report on S6a interface. The Subcriber Data Answer message and Subscription Data can contain the report on s6a interface. Configuration Information Answer and Reporting Information Request message can contain the report on t6a interface .

Configuring, monitoring, and reporting of new messages and AVPs for Home Subscribers are supported by following mechanisms:

- Monitoring Event Configuration AVP in CIR message from SCEF over t6a interface
- Monitoring Event Configuration in ULA/ISDR from HSS over s6a interface
- Monitoring Event Report AVP from MME over t6a interface through CIA for the number of UE in a geographical area event
- Monitoring Event Report AVP to MME over t6a interface through RIR message for any communication failure events under Subscription Data

Configuring MME Services and Call Control Profiles

This section describes how to configure monitoring events for a call control profile.

Important When you configure MME service for users, monitoring-events is disabled by default.

Enabling the CLI monitoring-events in a Call Control Profile

Use the following configuration to enable CLI monitoring-events for all users in a call control profile .

```
configure
  call-control-profile profile_name
    [ no ] monitoring-events
    end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of the call control profile as an alphanumeric string of 1 to 64 characters.
- **monitoring-events**: Monitors an event under the call control profile mode.
- **no**: Disables CLI monitoring-events in a Call-Control-Profile for an MME service.

Configuring Monitoring Events for an MME Service

Use the following configuration to monitor events for an MME service:

```
configure
  context context_name
    mme-service service_name
      [ no ] monitoring-events
      end
```

NOTES:

- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service must be a string from 1 to 63 characters.
- **monitoring-events**: Configures monitoring events for MME service users.
- **no**: Disables CLI monitoring-events in an MME Service.

Verifying the CLI monitoring-events in an MME Service

The following command is used to verify the parameters for Event Monitoring in an MME service:

```
show mme-service all | grep Monitor
Monitoring Events : Enabled
```

CHAPTER 11

GTPV1/V2 Echo Support for Peer MME and SGSN

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	**Release**
This feature is fully qualified in this release.	21.18

Revision Details	Release
First introduced. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account representative.	21.17

Feature Description

MME supports path management status of MME (S10) and SGSN (Gn/Gp). MME sends and receives GTP V2 Echo Message for Peer Node status in S10 Interface and GTP V1 Echo Message for Peer node status in Gn/Gp Interface. MME sends and receives the Echo message for Configured peer Node in MME regardless of GTP session. When **peer-sgsn echo-params** CLI is enabled under mme-service, MME will initiate Echo to peer Gn/Gp SGSNs configured under mme-service and also to peer SGSNs added/created during 3G-4G/4G-3G Gn/Gp Handover.

Path failure is detected when there is no response to Echo Request even after max retransmissions. Path failure detection is not done based on "Restart counter value change in echo response".

GTP V1 Echo Message is supported in compliance with the 3GPP 29.060 7.2 Path Management Messages operation and GTP V2 Echo Message is supported in compliance with the 3GPP 29.274, 7.1 Path Management Messages operation.

Existing traps SGSNGtpcPathFailure, SGSNGtpcPathFailureClear, EGTPCPathFail, and EGTPCPathFailClear are used by this feature.

Configuring GTPV1/V2 Echo Support for Peer MME and SGSN

This section provides information on the CLI commands to configure GTPV1/V2 Echo Support for Peer MME and SGSN feature.

Configuring Path Management for Peer MME

Use the following configuration to configure the path management for Peer MME.

```
configure
   context context_name
      mme-service mme_service_name
         peer-mme echo-params interval interval retransmission-timeout
retransmission_timeout max-retransmissions max_retransmissions reconnect-interval
 reconnect_interval
            [ no ] peer-mme echo-params
            end
```

NOTES:

- **no**: Removes the path management configuration for peer MME with Gn/Gp capability.
- **peer-mme**: Configures a Peer MME for inter-MME relocations.

- **echo-params** : Configures echo parameters for peer MME with GN/GP capability.
- **interval** *interval*: Configures echo interval in seconds. *interval* must be an integer from 60 to 300.
- **retransmission-timeout** *retransmission_timeout*: Configures echo retransmission timeout in seconds. *retransmission_timeout* must be an integer from 1 to 20.
- **max-retransmissions** *max_retransmissions*: Configures maximum retries for echo request. *max-retransmissions* must be an integer from 0 to 15.
- **reconnect-interval** *reconnect_interval*: Configures echo interval to be used once a peer node is detected to be unreachable. Retransmission is not applicable in this time. *reconnect_interval* must be an integer from 60 to 86400.

Configuring Path Management for Peer SGSN

Use the following configuration to configure the path management for Peer SGSN.

```
configure
   context context_name
      mme-service mme_service_name
         peer-sgsn echo-params interval interval retransmission_timeout
retransmission_timeout max-retransmissions max-retransmissions reconnect-interval
 reconnect_interval
               no peer-sgsn echo-params
               end
```

NOTES:

- **no**: Removes the path management configuration for peer SGSN with Gn/Gp capability.
- **echo-params** : Configures echo parameters for peer SGSN with GN/GP capability.
- **interval** *interval*: Configures echo interval in seconds. *interval* must be an integer from 60 to 300.
- **retransmission-timeout** *retransmission_timeout*: Configures echo retransmission timeout in seconds. *retransmission_timeout* must be an integer from 1 to 20.
- **max-retransmissions** *max-retransmissions*: Configures maximum retries for echo request. *max-retransmissions* must be an integer from 0 to 15.
- **reconnect-interval** *reconnect_interval*: Configures echo interval to be used once a peer node is detected to be unreachable. Retransmission is not applicable in this time. *reconnect_interval* must be an integer from 60 to 86400.

Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor this feature.

Show Commands and Outputs

show mme-service all name

The output of this command includes the following fields:

- PEER MME Echo Parameters :
  - interval
  - retransmission timeout
  - max retransmissions
  - reconnect interval
- PEER GN/GP SGSN Echo Parameters:
  - interval
  - retransmission timeout
  - max retransmissions
  - reconnect interval

show egtpc statistics

The output of this command includes the following fields:

Path Management Messages:

PEER MME Echo Request

- Total TX
- Initial TX
- Retrans TX

PEER MME Echo Response:

- Total RX

show egtpc peers mme

```
+----Status:   (D) - Dead    (A) - Alive
 |
 |+---IP Type:     (S) - Static  (D) - Dynamic
 ||  Service               Echo Req           Echo Req   Echo Rsp
 vv  ID      Peer Address  Time of Creation   Sent       Retransmitted  Received
 -- --- ---------------    ------------------ --------  ---------------
```

Total Peers:

Show sgtpc statistic

Path Management Messages:

Echo Request:

```
  Total   Echo-Req TX:     Total   Echo-Req RX:
  Initial Echo-Req TX:     Initial Echo-Req RX:
  Retrans Echo-Req TX:
```

Echo Response:

```
Total Echo-Rsp TX:    Total Echo-Rsp RX:
```

show sgtpc peers

```
Path     Service               Echo Req       Echo Req        Echo Rsp
Status   ID      Peer Address            Sent         Retransmitted     Received
----     --- -----------------------  -----------   ---------------   ---------
```

CHAPTER 12

Handling User Session During CCR-RAR Collision

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• MME
Applicable Platform(s)	• ASR 5500
Feature Default	Enabled - Always-on Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
Documentation update: Detailed information is provided for the change in behaviour.	21.19
First introduced.	

Feature Changes

Previous Behavior: In case of Credit Control Request - Re-Auth Request (CCR-RAR) collision for a user session supporting multiple services, ASR 5500 did not initiate a new CCR message to perform re-authorization for the remaining services/rating-groups (RG).

New Behavior: In 17.1 and later releases, generic support is provided to re-authorize the remaining services/rating-groups, post CCR-RAR collision, for a user session supporting multiple services to complete the credit re-authorization process.

For user sessions supporting multiple services (RG1, RG2, and RG3), the following call flows show different methods to complete the credit re-authorization process during a CCR-RAR collision.

ASR 5500 Gateway Receives Pending Response from OCS Before Time-Out

This section describes how the ASR 5500 gateway (P-GW/GGSN) receives pending response from the Online Charging System (OCS) server before time-out. In this case, the ASR 5500 gateway receives RAR when Credit Control Answer Update (CCA-U) is pending from the OCS server.

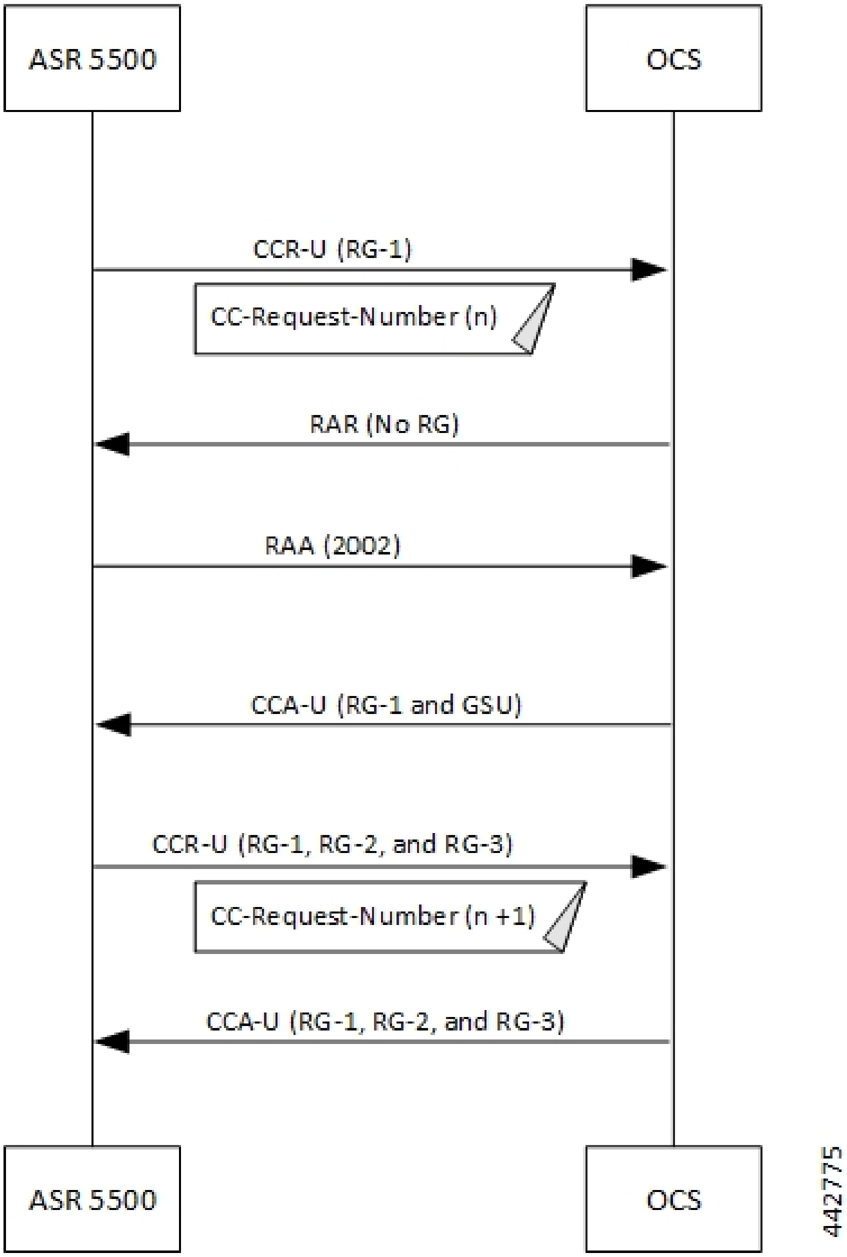


Table 13: ASR 5500 Gateway Receives Pending Response from OCS Before Time-Out Call Flow

Step	Description
1	Upon exhausting quota for RG-1, the ASR 5500 gateway sends a CCR-U message with CC-Request-Number (n) to the OCS server with Reporting Reason as Quota Exhausted. The ASR 5500 gateway waits for response from the OCS server for RG-1.
2	The ASR 5500 gateway receives an RAR message without any RG from OCS when CCA-U for RG1 is pending.
3	The ASR 5500 gateway immediately sends a Re-Auth Answer (RAA) message with the Result-Code as 2002 to OCS.
4	OCS sends a CCA-U message with Granted Service Unit (GSU) for RG1 to the ASR 5500 gateway.
5	Once the ASR 5500 gateway receives the CCA-U message, it sends the CCR-U message with CC-Request-Number (n+1) and Reporting-Reason as Forced-Reauthorization for all the active RGs, they are, RG-1, RG-2, and RG-3.
6	OCS acknowledges the CCR-U message and sends a CCA-U message with GSU for RG-1, RG-2, and RG-3 to the ASR 5500 gateway.

ASR 5500 Gateway Receives Pending Response from the Secondary OCS Server After Time-Out at the Primary OCS Server

This section describes how the ASR 5500 gateway receives the CCA-U message from the secondary OCS server after CCR-U time-out at the primary OCS server with Credit Control Failure Handling (CCFH) retry and terminate. In this case, the ASR 5500 gateway receives RAR when the CCA-U message is pending from the primary OCS server.

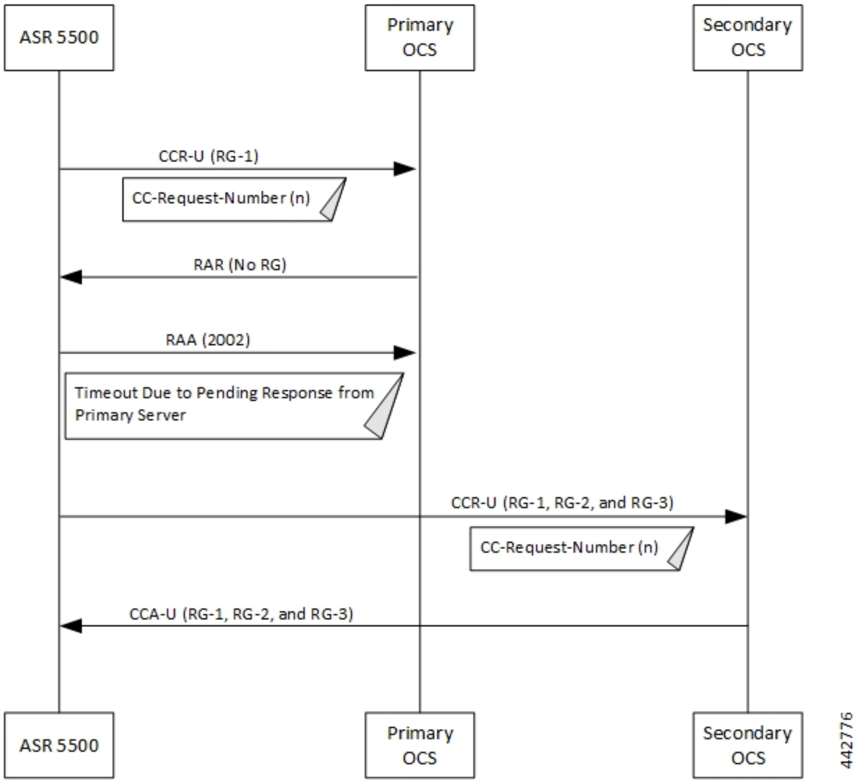


Table 14: ASR 5500 Gateway Receives Pending Response from the Secondary OCS Server After Time-Out at the Primary OCS Server

Step	Description
1	Upon exhausting quota for RG-1, the ASR 5500 gateway sends a CCR-U message with CC-Request-Number (n) to the primary OCS server with Reporting Reason as Quota Exhausted. The ASR 5500 gateway waits for response from the primary OCS server for RG-1.
2	The ASR 5500 gateway receives an RAR message without any RG from the primary OCS server when CCA-U for RG1 is pending.
3	The ASR 5500 gateway immediately sends an RAR message with the Result-Code as 2002 to the primary OCS server.
4	The ASR 5500 gateway retries to send the CCR-U message with CC-Request-Number (n) to the secondary OCS server with all the active RGs after there is a CCR-U time-out at the primary OCS server. The CCR-U message contains RG-2 and RG-3 with Reporting-Reason as Forced-Reauthorization and RG-1 with Reporting-Reason as Forced-Reauthorization and Quota-Exhausted.

Step	Description
5	The secondary OCS server acknowledges the CCR-U message and sends a CCA-U message with GSU for RG-1, RG-2, and RG-3 to the ASR 5500 gateway.

ASR 5500 Gateway Receives No Response After Time-Out at Both the Secondary OCS Server and the Primary OCS Server

This section describes how the ASR 5500 gateway receives no response after CCR-U time-out at both the primary and secondary OCS servers with CCFH retry and terminate. In this case, the ASR 5500 gateway receives RAR when the CCA-U message is pending from the primary OCS server.

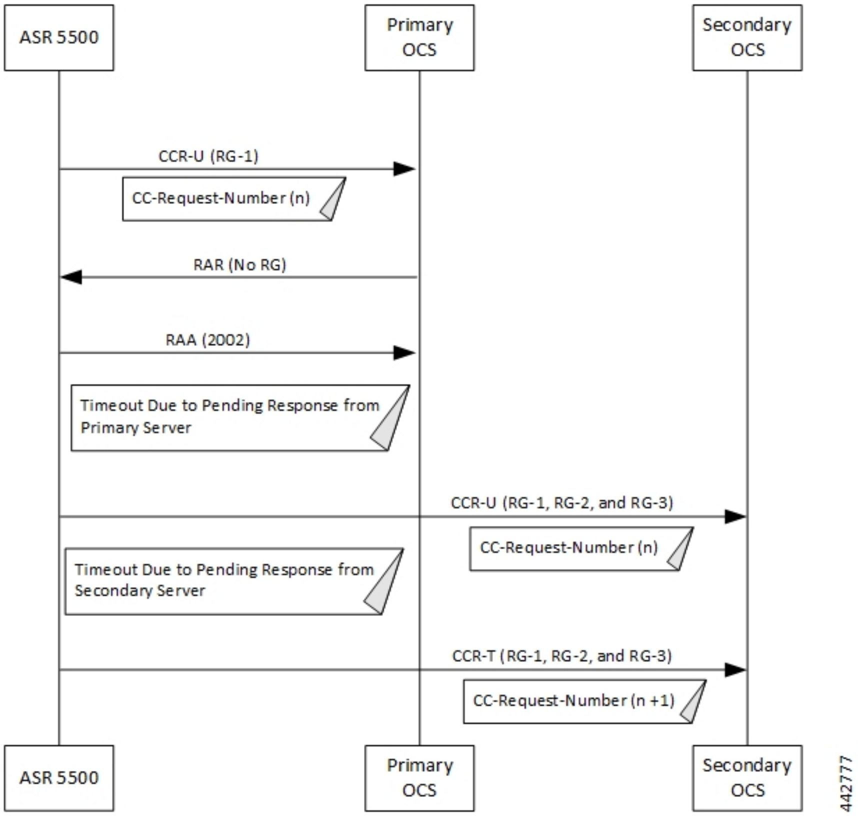


Table 15: ASR 5500 Gateway Receives No Response After Time-Out at Both the Secondary OCS Server and the Primary OCS Server

Step	Description
1	Upon exhausting quota for RG-1, the ASR 5500 gateway sends a CCR-U message with CC-Request-Number (n) to the primary OCS server with Reporting Reason as Quota Exhausted. The ASR 5500 gateway waits for response from the primary OCS server for RG-1.
2	The ASR 5500 gateway receives an RAR message without any RG from the primary OCS server when CCA-U for RG1 is pending.

Step	Description
3	The ASR 5500 gateway immediately sends an RAR message with the Result-Code as 2002 to the primary OCS server.
4	The ASR 5500 gateway retries to send the CCR-U message with CC-Request-Number (n) to the secondary OCS server with all the active RGs after there is a CCR-U time-out at the primary OCS server. The CCR-U message contains RG-2 and RG-3 with Reporting-Reason as Forced-Reauthorization and RG-1 with Reporting-Reason as Forced-Reauthorization and Quota-Exhausted.
5	The ASR 5500 gateway sends a Credit Control Request Terminate (CCR-T) message with CC-Request-Number (n+1), which contains RG-1, RG-2, and RG-3 with Reporting-Reason as Final to the secondary OCS server to terminate the session.

ASR 5500 Gateway Session Enters the Server Unreachable State After Time-Out at the Primary OCS Server

This section describes how the ASR 5500 gateway enters a server unreachable state after CCR-U time-out at the primary OCS server. In this case, the ASR 5500 gateway receives RAR when the CCA-U message is pending from the primary OCS server.

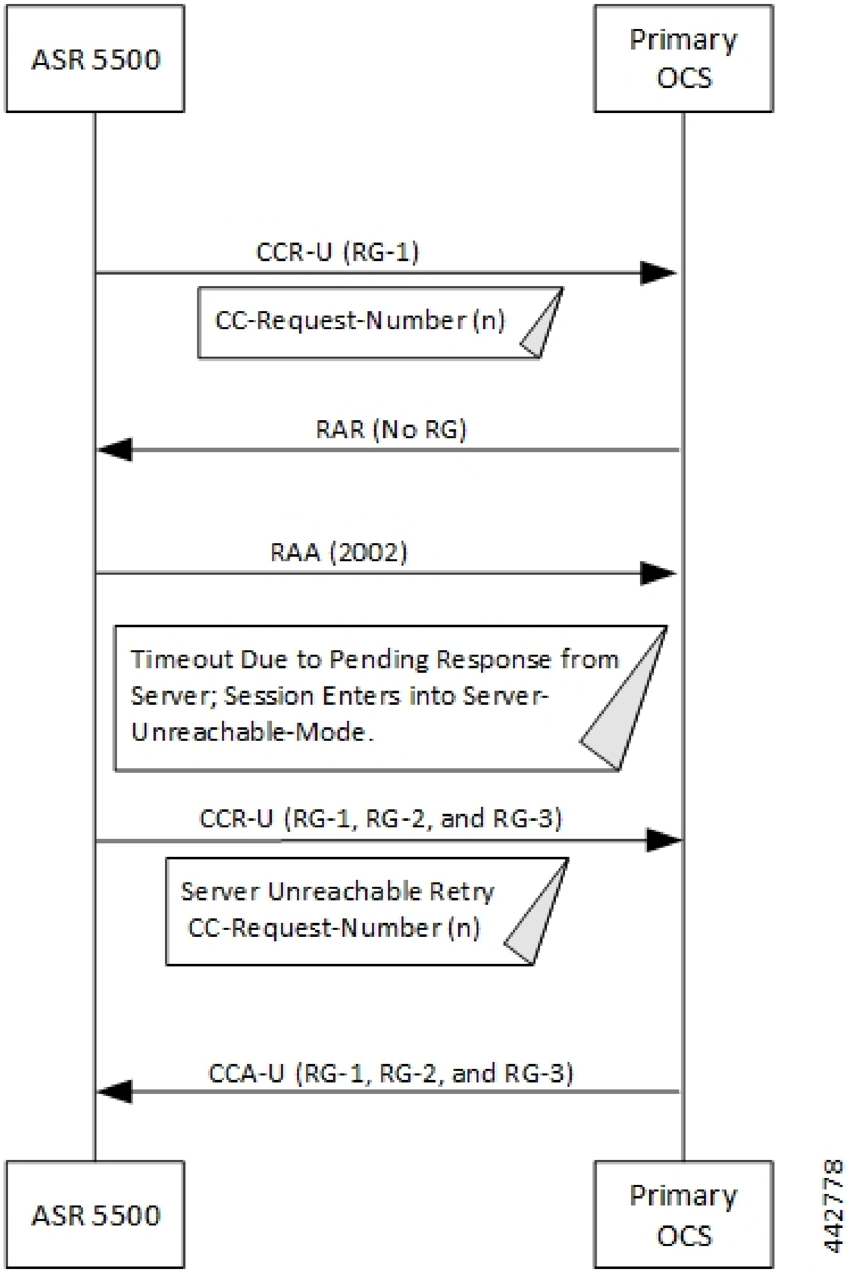

ASR 5500
Primary OCS
CCR-U (RG-1)
CC-Request-Number (n)
RAR (No RG)
RAA (2002)
Timeout Due to Pending Response from Server; Session Enters into Server-Unreachable-Mode.
CCR-U (RG-1, RG-2, and RG-3)
Server Unreachable Retry CC-Request-Number (n)
CCA-U (RG-1, RG-2, and RG-3)
ASR 5500
Primary OCS
442778

Table 16: ASR 5500 Gateway Session Enters the Server Unreachable State After Time-Out at the Primary OCS Server

Step	Description
1	Upon exhausting quota for RG-1, the ASR 5500 gateway sends a CCR-U message with CC-Request-Number (n) to the primary OCS server with Reporting Reason as Quota Exhausted. The ASR 5500 gateway waits for response from the primary OCS server for RG-1.

Step	Description
2	The ASR 5500 gateway receives an RAR message without any RG from the primary OCS server when CCA-U for RG1 is pending.
3	The ASR 5500 gateway immediately sends an RAR message with the Result-Code as 2002 to the primary OCS server.
4	The ASR 5500 gateway session enters the server unreachable state after there is a CCR-U time-out at the OCS server. The ASR 5500 gateway retries CCR-U with CC-Request-Number (n). The CCR-U contains all the active RGs; RG-1 and RG-2 with Reporting-Reason as Forced-Reauthorization and RG-3 with Reporting-Reason as Forced-Reauthorization and Quota-Exhausted.
5	OCS acknowledges the CCR-U message and sends a CCA-U message with GSU for RG-1, RG-2, and RG-3 to the ASR 5500 gateway.

ASR 5500 Gateway Receives RAR from Secondary Server Before Time-Out

This section describes how the ASR 5500 gateway receives the RAR message from the secondary OCS server before a CCR-U time-out. In this case, the ASR 5500 gateway receives RAR when the CCA-U message is pending from the primary OCS server.

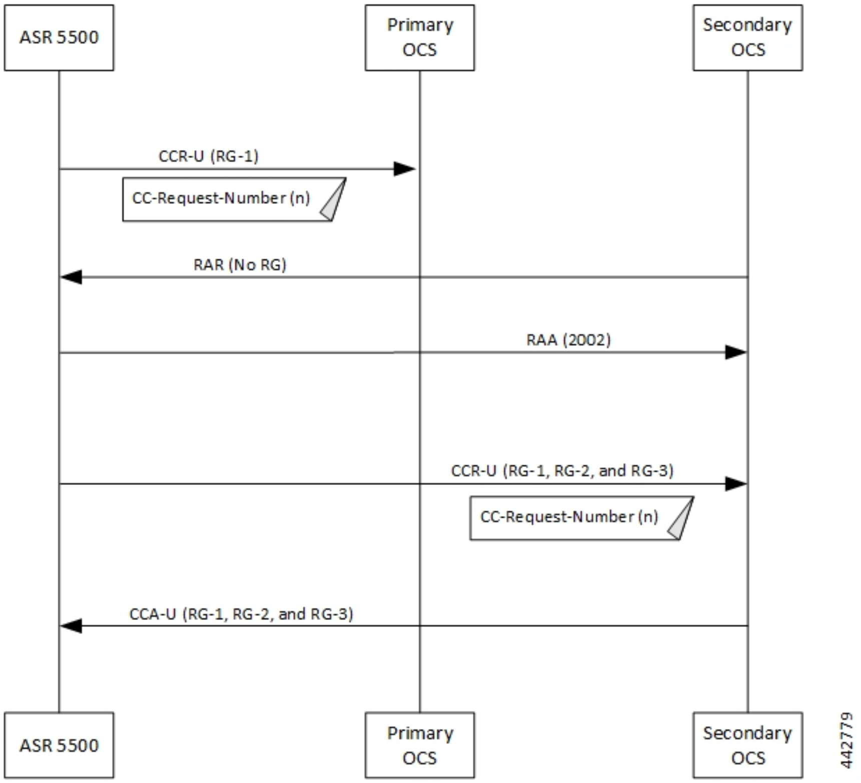


Table 17: ASR 5500 Gateway Receives RAR from Secondary Server Before Time-Out

Step	Description
1	Upon exhausting quota for RG-1, the ASR 5500 gateway sends a CCR-U message with CC-Request-Number (n) to the primary OCS server with Reporting Reason as Quota Exhausted. The ASR 5500 gateway waits for response from the primary OCS server for RG-1.
2	The ASR 5500 gateway receives an RAR message without any RG from the primary OCS server when CCA-U for RG1 is pending.
3	The ASR 5500 gateway immediately sends an RAR message with the Result-Code as 2002 to the primary OCS server.
4	The ASR 5500 gateway sends the CCR-U message with CC-Request-Number (n) to the secondary OCS server with all the active RGs. The CCR-U message contains RG-2 and RG-3 with Reporting-Reason as Forced-Reauthorization and RG-1 with Reporting-Reason as Forced-Reauthorization and Quota-Exhausted.
5	The secondary OCS acknowledges the CCR-U message and sends a CCA-U message with GSU for RG-1, RG-2, and RG-3 to the ASR 5500 gateway.

Customer Impact: Not applicable

CHAPTER 13

IPv4/IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled-Always on
Related Changes in This Release	Not Applicable
Related Documentation	*P-GW Administration Guide*

Revision History

Revision Details	**Release**
The P-GW supports IPv4/IPv6 address encoding change in Flow-Description AVP under Application-Detection-Information AVP for APPLICATION-START event trigger.	21.18.25
The StarOS 21.15.52 is enhanced with IPv4/IPv6 address encoding change in Flow-Description AVP under Application-Detection-Information AVP for APPLICATION-START event trigger from P-GW.	21.15.52

Feature Changes

Previous Behavior: In CCR-U for APPLICATION-START event trigger from P-GW, Flow-Description AVP under Application-Detection-Information AVP towards PCRF was encoded as:

- For ipv4 flows a netmask of /0 was used
- For ipv6 flows prefix length of 0 was used

New Behavior: In CCR-U for APPLICATION-START event trigger from P-GW, Flow-Description AVP under Application-Detection-Information AVP towards PCRF is encoded as:

- For ipv4 flows a netmask of /32 is used
- For ipv6 flows prefix length of 128 is used

Customer Impact: PCRF receives flow description value with 32/128 netmask/prefix. If PCRF rejects the value, ADC over Gx will not work.

CHAPTER 14

MME Support for EN-DC SON Configuration Transfer IE on S1-AP

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Configuration Not Required
Related Changes in This Release	Not Applicable
Related Documentation	*MME Administration Guide*

Revision History

Revision Details	**Release**
This feature is fully qualified in this release.	21.18
First introduced. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account representative.	21.17

Feature Description

Configuration Transfer enables the transfer of information between two eNodeBs at any time via S1 interface and the Core Network.

MME supports EN-DC SON Configuration Transfer IE in eNB Configuration Transfer Message and MME Configuration Transfer Message in compliance with specification 36.413 V15.6.0.

eNB Configuration Transfer procedure is initiated with eNB configuration transfer message sent from the eNB to the MME. If the MME receives the EN-DC SON Configuration Transfer IE, it transparently transfers the EN-DC SON Configuration Transfer IE either towards the eNB indicated in the Target eNB-ID IE or towards an eNB connected to the en-gNB indicated in the Target en-gNB-ID IE which is included in the EN-DC SON Configuration Transfer IE. MME sends EN-DC SON Configuration information through Configuration Transfer Tunnel Message to the peer MME.

MME identifies the dynamic eNB to en-gNB mapping entries through the Connected en-gNB List IE in S1 Setup Request message. The connected en-gNB List IE includes Connected en-gNB To Be Added List IE and Connected en-gNB To Be Removed List IE in eNB Configuration Update message. MME maintains eNB and en-gNB mapping entries to handle enb config transfer messages that are received with target engnb-id but without target enb-id.

Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the MME feature.

Show Commands and Outputs

show mme-service enodeb-association connected-en-gnb all

The output of this command includes the following field:

- connected-en-gnb all — Shows all the en-gNBs connected to all eNodeBs.

  The sample configuration output is an example for the **show mme-service enodeb-association connected-en-gnb all** command :

```
asr5500# show mme-service enodeb-association connected-engnb all
  MMEMgr                         : Instance 1
  Peerid                         : 17301506
  Global ENodeB ID        : 123:123:456
    Connected engNB ID : 4194306
    Broadcast PLMNs       :123:456
                          123:455
    TAC                   : 2400
```

show mme-service enodeb-association connected-en-gnb enodeb-name <enb name>

The output of this command includes the following field::

- connected-en-gnb enodeb-name <enb name> — Shows en-gNBs connected to specific eNodeB.

The sample configuration output is an example for the **show mme-service enodeb-association connected-en-gnb enodeb-name <enb name>** command

```
]asr5500# show mme-service enodeb-association connected-engnb enodeb-name enb1
MMEMgr                        : Instance 1
  Peerid                      : 17301506
  Global ENodeB ID    : 123:123:456
     Connected engNB ID     : 4194306
    Broadcast PLMNs          :123:456
                              123:455
    TAC                       : 2400
```

CHAPTER 15

Routing Based on Realm name MME

Feature Summary and Revision History

Summary Data

Table 18: Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5000 • ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• AAA Interface Administration and Reference • Command Line Interface Reference • MME Administration Guide • Statistics and Counters Reference

Table 19: Revision History

Revision Details	Release
First introduced	21.18

Introduction to Routing based on Realm name MME

In the Mobility Management Entity-Diameter Routing Agent (MME-DRA) Home Subscriber Server (HSS) network setup, the Diam:AIR message DRA searches for the correct destination realm of the Diameter message and sends back Diam:AIA as a response message to MME.

Similarly, in the MME-DRA Equipment Identity Register (EIR) network setup, the Diam:MICR (ME Identity-Check Request)message DRA searches for the correct destination realm of the Diameter message and sends back Diam:MICA (ME Identity-Check Identity Answer)as a response message to MME.

This process creates a load in DRA. In order to reduce the load, a new functionality has been added in MME. As per the new functionality, the operator can manually define the destination realm that needs to be used on the following interfaces S6A and S13. The destination realm can be given statically at two places: One Call-control-profile and MME-Service.

Note When specifyling Realm name at MME-service level, the Realm override takes effect only for S6a Diameter messages.

How it works

The operator can manually create an impact in both the diameter interfaces S6A and S13. The operator can use the new CLI configuration "diameter-destination-realm" under call-control-profile associate CLI, to define the destination realm name used for call-control-profile on the specific "peer-hss-service" to identify the diameter endpoint and the interface.

Similarly, in MME service level a CLI is used to define the destination realm in associating along with “peer-hss-service”.

The Destination realm can be provided at multiple places.

This feature works in the following order of priority:

Priority	Destination realm used from (if defined)
1 (Highest)	CallControlProfile – Associate- hss-peer-service Realm
2	Operator Profile: realm generated by “Dynamic Destination realm “option **Note** Not applicable to Home Subscribers.

Priority	Destination realm used from (if defined)
3	MME Service – Associate – hss-peer-service Realm **Note** Applicable to S6a interface only.
4 (Lowest)	Default Destination realm by MME

Enabling and Disabling Destination Realm at Call Control Profile Level on S6A and S13 Interface

Use the following configuration command to associate the hss-peer-service with the endpoint interface along with destination realm name at call-control-profile level on S6A and S13 interface:

```
configure
   context context_name
      call-control-profile profile_name
         [ remove ]associate hss-peer-service service_name
              { s13-interface |  s6a-interface }
              [diameter-destination-realm  realm_name ]
         end
```

Enabling and Disabling Destination Realm at MME-Service Level

Use the following configuration command to enable and disable destination realm at MME-Service level

```
configure
   context context_name
      mme-service mme_service_name
        [ no ] associate hss-peer-service service_name
            diameter-destination-realm  realm_name
         end
```

CHAPTER 16

RTLLI Management for 2G M2M Devices

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *SGSN Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
Counter enhancements on TAC and LAC levels are introduced	21.17.9

Feature Description

Fixed Random TLLI (RTLLI) Management for 2G M2M devices is intended to expand the operator's control of TLLI (temporary logical link identifier) in the following scenario:

When multiple M2M devices attempt PS Attaches, with the same fixed RTLLI coming from different NSEIs (network service entity identifier), the SGSN cannot distinguish between the devices. The SGSN functions ***as if*** the first device bearing an RTLLI is no longer attached and begins to communicate with the next device using that same RTLLI. With multiple M2M devices attempting attaches - all with the same RTLLI - the result is TLLI collision and dropped calls.

Counter Enhancements on TAC and LAC Levels

In StarOS 21.17 and later releases, the existing bulk statistics counters, 2G-simple-attach-rej-randomtlli-collision and 2G-combined-attach-rej-randomtlli-collision are updated at LAC level.

How It Works

This feature deals with Attach problems due to simultaneous IMSI attaches, all with the same fixed RTLLI.

Configure the SGSN to discard/drop Attach Request messages received from an MS with an RTLLI already in use on the SGSN by adding validation of the NSEI. Attach gets processed if the attach is coming from a different NSEI. This functionality is disabled by default.

The Fixed Random TLLI Handling mechanism extends the functionality to reduce jumbling of authentication vectors across subscribers,. A new verification table has been added to the GbMgr. The table maintains a list of TLLI + NSEI and if an incoming Attach Request includes a TLLI + NSEI already on the table then the call is dropped. This functionality is disabled by default.

Configuring RTLLI Management

No new commands or keywords have been added to the CLI in support of Fixed Random TLLI Management. Enabling / Disabling this mechanism is integrated into existing CLI.

For information about the commands, parameters and parameter values, please check your *Command Line Interface Reference* manual for each of the commands listed below.

Important The following configurations should be performed during system boot up. It is not advisable to enable/disable this TLLI management functionality during runtime.

Verifying Both the RTLLI and the NSEI

To enable the SGSN to handle Attach Requests with the same fixed RTLLI by verifying both the RTLLI and the NSEI, use the following configuration:

```
config
  sgsn-global
    gmm-message attach-with-tlli-in-use discard-message only-on-same-nsei
```

```
      old-tlli invalidate tlli hex_value
      old-tlli hold-time time
      end
```

Notes:

- **only-on-same-nsei** - This keyword is required to enable this new verification mechanism.

Verifying Only the RTLLI

To enable the SGSN to handle Attach Requests with the same fixed RTLLI by verifying only the RTLLI, use the following configuration:

```
config
  sgsn-global
    gmm-message attach-with-tlli-in-use discard-message
    old-tlli invalidate tlli hex_value
    old-tlli hold-time time
    end
```

Notes:

- **only-on-same-nsei** - Do not include this keyword to disable this new verification mechanism. The system defaults to the verification mechanism provided with Release 16.3 (see *How It Works*).

Verifying Configuration

To verify if the functionality is enabled or disabled, use the following commands from the Exec mode:

```
show configuration | grep gmm-mess
show configuration | grep old-
show configuration verbose | grep old-
```

Monitoring and Troubleshooting

This section provides information for monitoring and/or troubleshooting the RTLLI Management functionality.

To see the statistics of attach drops that are due to same-RTLLI collisions, execute the show commands listed below. When you are looking at the generated statistics, consider the following:

- If the generated counter values are not increasing then collisions are not occurring.
- If the generated counter values are increasing then it means collisions are occurring and attaches were dropped.

Configured to Verify Both RTLLI and NSEI

If **gmm-message attach-with-tlli-in-use discard-message only-on-same-nsei** is configured then the following show command can give the drop count of attaches caused by same RTLLI and NSEI:

```
show gbmgr all parser statistics all | grep use

IMSI Key: 1487 P-TMSI Key: 0 attach with tlli in use : 592 <-- drops from existing table
with RTLLI+NSEI
```

```
Add P-TMSI Key: 0 attach drop tlli in use(pre tlli check): 297 <-- drops from new table
with RTLLI

IMSI Key : 1190 P-TMSI Key : 594 attach with tlli in use : 395
Add P-TMSI Key : 0 attach drop tlli in use(pre tlli check) : 198
```

Configured to Verify Only RTLLI

If "gmm-message attach-with-tlli-in-use discard-message" is configured then the following show command can give the drop count of attaches caused by same RTLLI:

```
show gbmgr all parser statistics all | grep use

 IMSI Key: 1487 P-TMSI Key: 0 attach with tlli in use : 592 <-- drops from existing table
with RTLLI
Add P-TMSI Key: 0 attach drop tlli in use(pre tlli check): 297 <-- drops from new table
with RTLLI

IMSI Key : 1190 P-TMSI Key : 594 attach with tlli in use : 395
Add P-TMSI Key : 0 attach drop tlli in use(pre tlli check) : 198
```

Verify Attach Rejects due to Same RTLLI

The following show command generates SessMgr counters that track the Attach Rejects due to same RTLLI collision:

```
show gmm sm stats | grep Same random tlli collision

Same random tlli collision: 10
```

The 'sgsn-implicit-detach(237)' session disconnect reason pegs when the 2G-SGSN rejects the Attach Request due to same RTLLI collision.

The following show command identifies the two bulk statistics the SGSN uses to track the number of times the SGSN rejects Attach Requests or Combined Attach Requests due to same RTLLI collision.

```
show bulkstats variables sgsn | grep colli
%2G-simple-attach-rej-randomtlli-collision%                  Int32     0   Counter
%2G-combined-attach-rej-randomtlli-collision%                Int32     0   Counter
```

In StarOS 21.17 and later releases, the existing bulkstats counters (%2G-simple-attach-rej-randomtlli-collision% , %2G-combined-attach-rej-randomtlli-collision%) are updated at LAC level. Existing counters are added as part of recovery, **gprs-bk schema**:

```
show bulkstats variables gprs-bk | grep tlli
%2G-simple-attach-rej-randomtlli-collision-bk%               Int32     0   Counter
%2G-combined-attach-rej-randomtlli-collision-bk%             Int32     0   Counter
```

To print the recovered statistics, run the following show command:

```
show gmm-sm statistics recovered-values verbose
    2G Attach Rejects due to same rtlli collisions:
      Simple :           0
      Combined :           0
```

CHAPTER 17

TAI-based Routing for 20-bit and 28-bit eNB ID

This feature enables MME to perform TAI-based routing for both 20-bit and 28-bit eNB IDs.

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide* • Statistics and Counters Reference

Revision History

Revision Details	Release
HeNBGW Selection Enhancement in MME.	21.18
HeNBGW Selection Enhancement in MME.	21.15

Revision Details	Release
First introduced.	21.1

Feature Description

MME supports TAI-based routing of handover (HO) and configuration transfer messages towards Pico controller/HeNBGW when the target eNB ID is 28 bits, but it could not support TAI-based routing when the target Pico eNB ID is 20 bits.

Pico controller can transfer the target Pico eNB ID to 28 bits from 20 bits if the handover is Pico-to-Pico, but it could not handle Macro-to-Pico handover as there is no Pico Controller for Macro.

In releases 21.1 and beyond, the behavior of MME is modified so that it can perform TAI-based routing even if target home-eNB ID is 20 bits.

This feature provides a configurable option within MME service to configure target HeNB type (home or macro or both) behind HeNBGW. Based on this configuration, MME allows TAI-based lookup of target eNB, if target eNB ID is not found by MME during handover. By default, TAI-based lookup is performed only for home eNB ID (28-bits).

This feature is also introduced to support identification of target eNB using target TAI for target eNB type Macro or Pico nodes or both so that handover to such eNB can be supported if it is connected to MME through Pico controller/HeNBGW. From MME point of view, Pico controller is a Macro eNB which is using 20 bit eNB ID to support multi-cell.

Along with S1 based intra-MME HO, this feature can be applied to inter MME S1 HO procedures (inbound S10, S3 and Gn handovers). Please note that, in Gn case, MME converts target RNC ID to macro eNB ID so target TAI-based lookup for macro eNB works fine.

This feature allows operators to configure the global eNodeB IDs of HeNBGWs in the MME service. The MME uses this information to perform HeNBGW related functions. In case of S1-based handovers to home eNodeBs served by a HeNBGW, the lookup at MME for the target eNodeB based on global eNB ID will fail, as MME is aware of only the HeNBGW. In those cases, additional lookup needs to be done based on TAI to find the HeNBGW serving the home eNodeB.

Since TAI-based lookup for home or macro eNBs is supported for HeNBGWs, all such HeNBGWs should be defined in HeNBGW management database (HeNBGW-mgmt-db). The HeNBGW-mgmt-db should be associated within mme-service.

The number of HeNBGW entries in the HeNBGW-mgmt-db has been increased from 8 to 512.

HeNBGW Selection Enhancement

TAI is unique and it is not shared across multiple HeNBGWs. If the TAIs are shared, then any one of the target eNBs sharing the TAC under consideration will be selected during TAI-based target eNB selection and handed over to the eNB may fail. To overcome this failure, HeNBGW matched with MSB 10 bits of Target HeNB ID (macro-enb 20 bit or home-enb 28 bits) and eNB ID of HeNBGW must be selected. If no match is found, then any one of the target eNBs sharing the TAC under consideration is selected during the TAI-based target eNB selection and handover to the eNB may ultimately fail.

Note If there are several HeNBGW with same TAI, CISCO MME supports selection of HeNBGW with MSB 10 bits (macro-enb 20 bit or home-enb 28 bits)) of HeNB ID.

Limitations

The following are the limitations of this feature:

- TAI-based lookup is performed only for home eNB.
- TAI should be unique and should not be shared across multiple HeNBGWs. If the TAIs are shared, then any one of the target eNBs sharing the TAC under consideration will be chosen during TAI-based target eNB selection and handover to the eNB might fail.

Configuring TAI-based Lookup of eNB

The following section provides the configuration commands to enable the TAI-based lookup of eNB.

Configuring Target eNB Type for TAI-based Lookup

Use the following configuration commands to configure the target eNB type or target henb-type as home or macro.

```
configure
   context context_name
      mme-service service_name
         henbgw henb-type { macro-enb | home-enb | all }
         end
```

Notes:

- The **henbgw henb-type { macro-enb | home-enb | all }** is a new CLI command introduced in 21.1 release to support TAI-based lookup functionality.
- **henbgw**: Configures Home eNodeB gateway options.
- **henbgw-type**: Configures HeNB type. TAI-based lookup depends on HeNB type.
  - **home-enb**: Configures HeNB type home-enb (28-bits)
  - **macro-enb**: Configures HeNB type macro-enb (20-bits)
  - **all**: Configures HeNB type both macro-enb (20-bits) and home-enb (28-bits)
- By default, when the **henbgw henb-type** command is not applied explicitly, target eNB type is set as home-enb.
- Use the **no henbgw henb-type** command to delete the existing configuration, if previously configured.

- The target eNB type configuration is effective only when the **henbgw henb-type** CLI command is configured within mme-service and the HeNBGW-mgmt-db is associated with HeNBGWs inside mme-service.

Verifying the Target eNB Type Configuration

Use the following commands to verify the configuration status of this feature.

```
show mme-service all
```

- or -

```
show mme-service name service_name
```

service_name must be the name of the MME service specified during the configuration.

This command displays all the configurations that are enabled within the specified MME service.

The following is a sample configuration of this feature.

```
configure
   lte policy
      mme henbgw mgmt-db db_name
         henbgw-global-enbid mcc 123 mnc 456 enbid 12345
         henbgw-global-enbid mcc 123 mnc 456 enbid 12543
         end
configure
   context context_name
      mme-service service_name
         henbgw henb-type macro-enb
         associate henbgw-mgmt-db henbdb
         end
```

NOTES:

- By default, when the **henbgw henb-type** command is not configured, target eNB type is set as **home-enb**.

Configuring HeNBGW msb-10-bits Selection

Use the following commands to configure HeNBGW selection using HeNB MSB 10 bits for the same TAI.

```
configure
  context context_name
    mme-service service_name
      henbgw selection msb-10-bits
      no henbgw selection
      end
```

NOTES:

- **no** : Removes the configured HeNBGW selection for the same TAI.
- **henbgw**: Configures HeNBGW options.
- **selection**: Configures HeNBGW selection for same TAI.

- **msb-10-bits** Configures HeNBGW selection using HeNB MSB 10 bits for same TAI. By default this is disabled.

Note HeNBGW selection using HeNB MSB 10 bits is performed only when TAIs are shared across multiple HeNBGWs.

The TAI lookup happens only in the following instance:

- When henb-type {all | macro-enb} for handover to target Henbgw macro 20 bits.
- When henb-type **{all | home-enb}** is configured for handover to target HeNBGW home 28 bits. However, when henb-type {macro} is configured for handover to target HeNBGW home 28 bits, the lookup at MME for the target eNodeB will fail in handover preparation.

Monitoring and Troubleshooting the TAI-based Lookup

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show mme-service all** CLI command. If not enabled, configure the **henbgw henb-type** CLI command in MME service Configuration mode and check if it works.
- Collect and analyze the output of **show configuration**, **show support details**, **show mme-service name** *service_name* and **show mme-service statistics handover** commands. Also, check the reported logs, if any. For further analysis, contact Cisco account representative.
- Check and analyze the debug logs for mme-app, s1ap, mmemgr, and mmedemux facilities to determine if TAI-based lookup fails for a particular TAI.

show mme-service all

The following field is added to the output of the **show mme-service all** command in support of this feature.

```
HENBGW HeNodeB Type: macro-enb
```

*Table 20: **show mme-service all** Command Output Descriptions*

Field	Description
HENBGW HeNodeB Type	Displays the configured type for HeNodeB gateway. HENBGW HeNodeB Type can be one of the following: • macro-enb • home-enb • all

Field	Description
HeNBGW selection using HeNodeB MSB 10 bits for same TAI	• Enabled • Disabled

show mme-service name *service_name*

The following field is added to the output of the **show mme-service name** *service_name* command in support of this feature.

```
HENBGW HeNodeB Type: macro-enb
```

*Table 21: **show mme-service name** service_name Command Output Descriptions*

Field	Description
HENBGW HeNodeB Type	Displays the configured type for HeNodeB gateway. HENBGW HeNodeB Type can be one of the following: • macro-enb • home-enb • all

show mme-service statistics handover

The following fields are added to the output of the **show mme-service statistics handover** command in support of this feature.

```
Handover Statistics:
  Intra MME Handover
    .
    .
    Target TAI based S1 handover
      Attempted:       4
      Success:         3
      Failures:        1
.
.
  EUTRAN<-> EUTRAN using S10 Interface:
    .
    .
    Inbound relocation using Target TAI based S1 HO procedure:
      Attempted:       0
      Success:         0
      Failures:        0
```

*Table 22: **show mme-service statistics**Command Output Descriptions*

Field	Description
Target TAI based S1 handover	
Attempted	Displays the total number of attempted intra MME S1 handovers that used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Inbound relocation using Target TAI based S1 HO procedure	
Attempted	Displays the total number of attempted inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.

show mme-service statistics peer-id

The following fields are added to the output of the **show mme-service statistics peer-id** *peer_id* **handover** command in support of this feature.

```
Handover Statistics:
  Intra MME Handover
    .
    .
    Target TAI based S1 handover
      Attempted:       4
      Success:         3
      Failures:        1
.
.
  EUTRAN<-> EUTRAN using S10 Interface:
    .
    .
    Inbound relocation using Target TAI based S1 HO procedure:
      Attempted:       0
      Success:         0
      Failures:        0
```

*Table 23: **show mme-service statistics** Command Output Descriptions*

Field	Description
Target TAI based S1 handover	
Attempted	Displays the total number of attempted intra MME S1 handovers that used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Inbound relocation using Target TAI based S1 HO procedure	
Attempted	Displays the total number of attempted inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.

Bulk Statistics

MME Schema

The following bulk statistics have been added to the MME schema to track the TAI-based lookup attempts, successes and failures during intra-MME S1 and inter-MME inbound S10 handovers:

- emmevent-s1ho-target-tai-attempt
- emmevent-s1ho-target-tai-success
- emmevent-s1ho-target-tai-failure
- in-s1-ho-4gto4g-s10-target-tai-attempted
- in-s1-ho-4gto4g-s10-target-tai-success
- in-s1-ho-4gto4g-s10-target-tai-failures

For detailed information on these bulk statistics, refer to the **BulkstatStatistics_documentation.xls** spreadsheet that is included as part of the software companion package for this release.