

# Function Specification Administration of Multi Regions and BSS Capacity

Ericsson Dynamic Activation 1

---

## FUNCTION SPECIFICATION

**Copyright**

© Ericsson AB 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

**Disclaimer**

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

**Trademark List**

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Purpose and Scope	1
1.2	Target Group	1
1.3	Typographic Conventions	1
<b>2</b>	<b>General</b>	<b>1</b>
<b>3</b>	<b>Administration of Multi Regions</b>	<b>3</b>
3.1	Management of Administration Domains	3
3.2	Use of Administration Domains in Provisioning	4
3.2.1	Individual Provisioning	4
3.2.2	Massive Provisioning	7
<b>4</b>	<b>Administration of BSS Capacity</b>	<b>11</b>
4.1	Connection Restriction Control	12
4.2	Sustainable Provisioning Throughput Restriction Control	13
	<b>Reference List</b>	<b>19</b>





# 1 Introduction

This section is an introduction to this document. It contains information about the prerequisite, purpose, scope, and target group for the document. This section also contains explanations of typographic conventions used in this document.

## 1.1 Purpose and Scope

This document describes the Administration of Multi Regions and BSS Capacity feature in the Ericsson™ Dynamic Activation (EDA).

## 1.2 Target Group

The target group for this document is as follows:

- Network Administrator
- Application Administrator
- Other

For information about the different target groups, see *Library Overview*, Reference [1]

## 1.3 Typographic Conventions

Typographic conventions are described in *Library Overview*, Reference [1].

# 2 General

Administration of Multi Regions and Administration of Business Support System (BSS) Capacity are two features in the Dynamic Activation Provisioning Manager functional group. These two features have technical dependency with other features in Dynamic Activation and in the layered HLR.

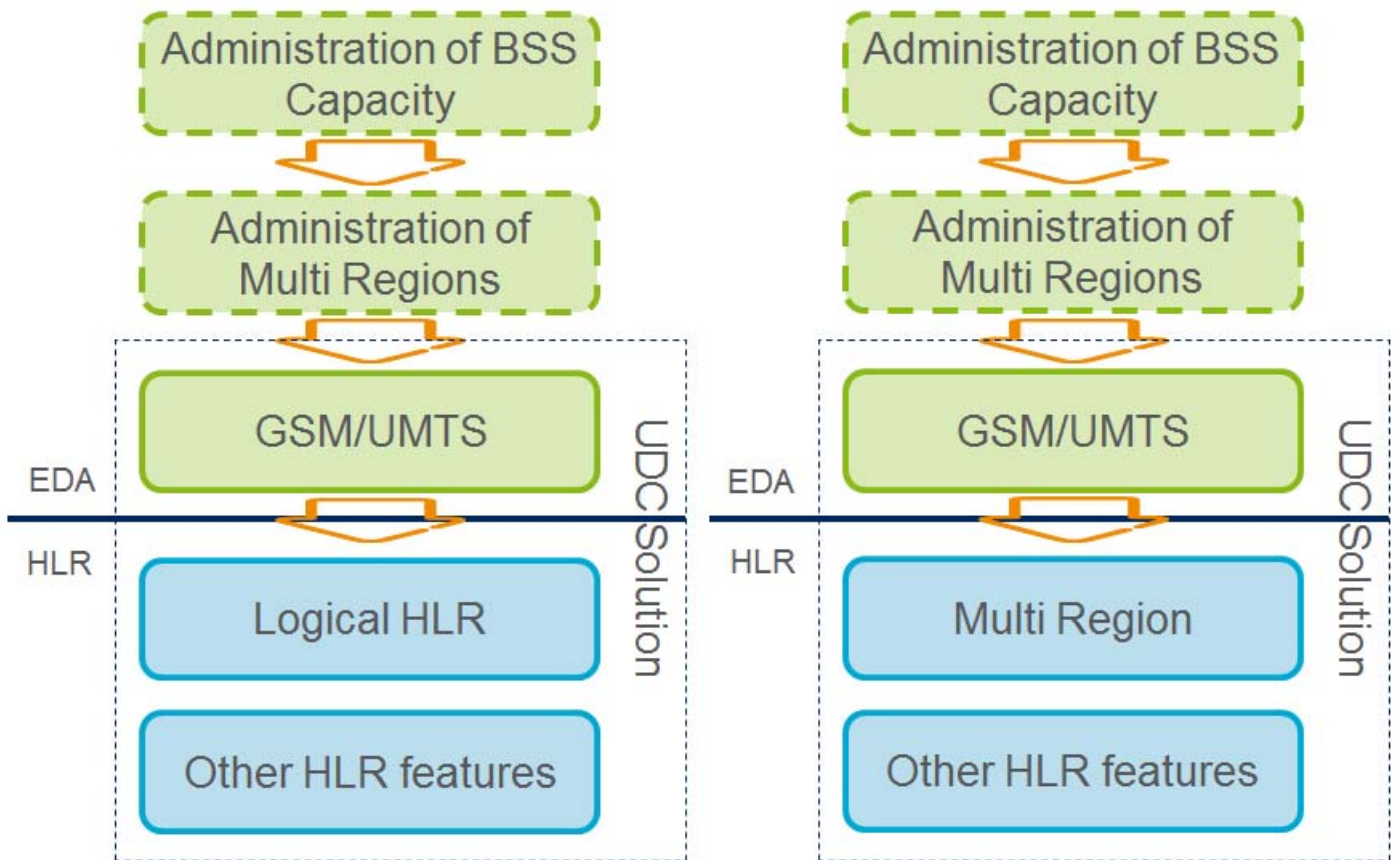


Figure 1 Feature Dependency

As illustrated in Figure 1, the GSM/UMTS feature in Dynamic Activation is one of the three mandatory components in the UDC solution for the HLR application. Logical HLR and Multi Region are two HLR optional features. These features are aiming for segmenting the HLR capacity in the UDC solution for the operator but in different flavors. With either of them, operators can introduce the optional feature Administration of Multi Regions in the network. Therefore operators can manage subscriber data in a segmented manner. On top of this, another optional feature Administration of BSS Capacity can be deployed, providing the mechanism to regulate provisioning capacity use between the provisioning clients. The Administration of Multi Regions feature is the prerequisite for the Administration of BSS Capacity feature.

For more information about the provisioning solution for HLR in data layered architecture, see *Function Specification Layered HLR*, Reference [2]. For more information about the software platform Provisioning Server that hosts these two features, see *Function Specification Resource Activation*, Reference [3]. For information about configuring these features, see *Configuration Manual for Resource Activation*, Reference [4].



## 3 Administration of Multi Regions

This feature enables sharing of UDC HLR network infrastructure among different regions/countries/service providers. The key functions are:

- **Management of Administration Domains (then called Admin Domains):** This is the foundation for the next two functions. Defined Admin Domains must reflect the service agreement between the network infrastructure owner and the region/countries/service providers.
- **Access control:** This function ensures that each region/country/service provider only can administer its own subscribers; other subscribers served by the same network infrastructure are not accessible. Every provisioning request is evaluated towards the restriction rules defined in the Admin Domain. Provisioning requests that violate the restriction rules are rejected. This also ensures that a subscriber only can access the services provided within its region/countries/service providers, regardless of the network capability.
- **Manage Region Identifier (RID) for BSS during provisioning:** The attribute RID can be handled transparently by Dynamic Activation. Thus the BSS is not affected.

### 3.1 Management of Administration Domains

An Admin Domain is a special provisioning role with mandatory restriction rules. An Admin Domain is defined with the purpose to group subscribers within a network. It is possible to:

- Add/Edit/View an Admin domain
- Compare two Admin Domains
- Associate an Admin Domain to a user. For information about user authorization, see *Function Specification Resource Activation*, Reference [3].

When defining an Admin Domain, the following rules must be considered:

- Up to 32 Admin Domains are supported.
- Each Admin Domain can be associated with one or more users.
- Each Provisioning Client can be associated with one or more Admin Domains. The following is valid within the Admin Domain context:
  - A user having access to only one Admin Domain is called a Provisioning Client.

- A user having access to more than one Admin Domain is called a Local Administrator.
- A user having access to all Admin Domains and the System Administrator Admin Domain is called a System Administrator.
- All Admin Domains must have restriction rules for the mandatory key parameters - RID and IMSI.
- MSISDN number series restriction rule is a special rule.
  - If Mobile Number Portability (MNP) is used in the network, MSISDN number series must not be defined as a restriction rule.
  - If MNP is not used in the network, MSISDN number series must be defined in the Admin Domain to avoid the unnecessary CUDb-lookup.
- Admin Domains can never have overlapping IMSI number series, MSISDN number series or RID values. Thus a subscriber belongs to only one Admin Domain.
- In addition to the key parameters, Admin Domains can contain restriction rules for other attributes, for example, Subscriber Data Profile IDs attribute.

## 3.2 Use of Administration Domains in Provisioning

The following two chapters describe how Admin Domain and RID are used in Individual provisioning requests and Massive provisioning requests. CAS backwards compatibility is achieved by not including RID.

### 3.2.1 Individual Provisioning

Individual provisioning request scenarios are outlined in Figure 2.



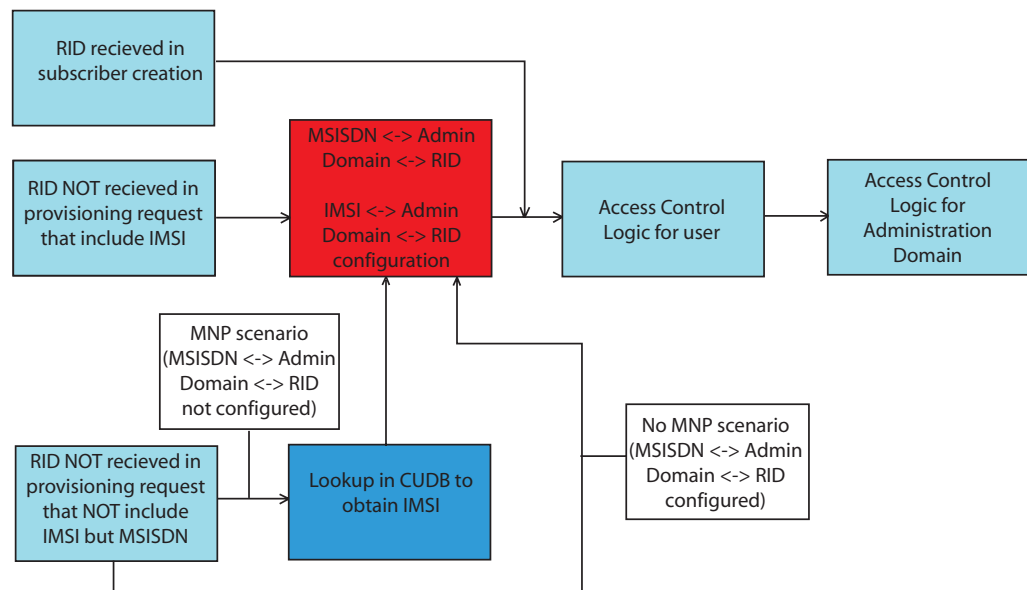


Figure 2 Individual Provisioning Requests Scenarios

BSS can choose to include or exclude the RID in the provisioning requests. When RID is not included in the provisioning requests, the logic locates it and maps it to the request:

- The provisioning requests contain IMSI: As IMSI is one of the mandatory attributes in Admin Domains, it points to one Admin Domain and thus the RID.
- The provisioning requests contain only the MSISDN as identity: The logic first uses the MSISDN to locate the Admin Domain. If the MSISDN is not found (because of the presence of MNP), a CUDB lookup based on MSISDN is initiated to find the IMSI. The returned IMSI is then used to locate the Admin Domain and then the RID.

During the access control process:

- If both user and Admin Domains restriction rules exist, the request is evaluated towards the user restriction rules, and then the Admin Domain ones.
- An attribute validated against the User authority is not validated against the Admin Domain authority. In other words, user restriction rules override the Admin Domain restriction rules.
- If a user is associated to more than one Admin Domain, access control validates the request against the authority of all the Admin Domains. The request must match the authority of one of the Admin Domains.
- A user can only administer the subscribers defined in the Admin Domain to which it belongs.



- Requests are rejected if the RID/MSISDN/IMSI combination in the request conflicts with that defined in the Admin Domain.

This is an example of how the Admin Domain can be used. Table 1 defines a setup for a small operator with restriction rules and its associated users.

*Table 1 Example of Admin Domains with Restriction Rules and Associated Users*

Name	Restriction Rules	Capacity Attributes and other Attributes	Users
Administration Domain 1	RID=1 IMSI=123456* CSP=11 # Camel Profile ID profile=11 # Subscriber Data profile ID		user_one_prov, user_11_IN, user_21_OSS, user_localadm, user_sysadm
Administration Domain 2	RID=2 IMSI=123457* CSP=12 # Camel Profile ID profile=12 # Subscriber Data profile ID		user_two_prov, user_12_OSS, user_localadm, user_sysadm
Administration Domain 3	RID=3 IMSI=123458* CSP=13 # Camel Profile ID profile=13 # Subscriber Data profile ID		user_three_prov, user_13_OSS, user_localadm, user_sysadm
Administration Domain 4	RID=4 IMSI=123459* CSP=14 # Camel Profile ID profile=14 # Subscriber Data profile ID		user_four, user_14, user_sysadm
Administration Domain System Administrator		sysadm	user_sysadm

Examples of Individual provisioning request behavior:

**Example 1.** Create subscriber without RID

log in as: **user\_one\_prov**

```
> HGSUI:IMSI=123456789012345,MSISDN=345678901234567;
```

<OK - Subscriber created>

The request is associated with Admin Domain 1 because of matching IMSI. The command passes Admin Domain ACL because user\_one\_prov is associated with Admin Domain 1.

**Example 2.** Create subscriber without RID and wrong user

log in as: **user\_12\_OSS**



```
> HGSUI:IMSI=123456789012345,MSISDN=345678901234567;
```

```
<Error message - user has no access to Admin Domain 1>
```

The request is associated with Admin Domain 1 because of matching IMSI. The command fails in Admin Domain ACL because `user_12_OSS` is associated with Admin Domain 2.

### Example 3. Create subscriber with RID

```
log in as: user_one_prov
```

```
> HGSUI:IMSI=123456789012345,MSISDN=345678901234567,RID=2;
```

```
<Error message - RID mismatch>
```

The request is associated with Admin Domain 1 because of matching IMSI. The command fails in Admin Domain ACL because `RID=2` mismatch with `RID=1` from Admin Domain 1.

### Example 4. Print Subscriber Data with MSISDN

Subscriber with `MSISDN=345678901234567` and `IMSI=123456789012345` exists in CUDB.

```
log in as: user_one_prov
```

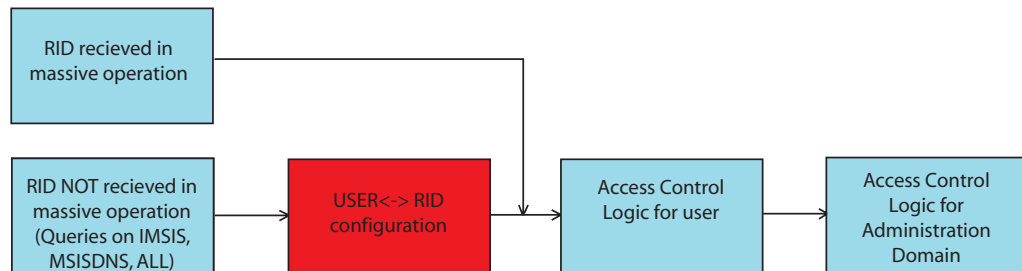
```
> HGSDP:MSISDN=345678901234567;
```

```
<OK - prints data of subscriber>
```

As MNP is presented in the network, MSISDNS is not configured in the Admin Domains. A CUDB lookup is performed to get the IMSI. The request is associated with Admin Domain 1 based on the retrieved IMSI. The command passes Admin Domain ACL because `user_one_prov` is associated with Admin Domain 1.

## 3.2.2 Massive Provisioning

Massive provisioning Admin Domain association and Access Control flow are described in figure Figure 3. There are only two variants of Massive provisioning requests - with RID and without RID.



**Figure 3** Massive Provisioning Requests Scenarios

Massive provisioning requests have the following characteristics:

- A Massive request is associated with one or several Admin Domains based on the logged-in user or RID provided in the request, not the IMSI, or MSISDN keys as in Individual provisioning. If RID is omitted, the request is associated with all Admin Domains the logged-in user is associated with, see **Example 1** Page 8 and **Example 4** on Page 9.
- If RID values and key values, for example MSISDN or IMSI, mismatch in the Admin Domain ACL, the requests is not blocked. The purpose is to maintain a strong search flexibility regarding combinations of RID and key values, for example IMSIS and MSISDNS. However, if the RID value mismatch with the logged-in user values, the Admin Domain ACL blocks the request, see **Example 2, 3, and 5** on Page 9.
- A user can be associated to more than one Admin Domain. The user can:
  - Use both the RID and the key parameters (MSISDNS or IMSIS) to set a definite search.
  - Update scope on Massive provisioning requests.

There are several examples of Massive provisioning requests, which clarify Admin Domain association and Access Control behavior.

Admin Domain configurations in these examples are the same as in the Individual provisioning examples, see Table 1.

**Example 1.** Massive search for all subscribers that match IMSIS=12345688

log in as: **user\_one\_prov**

> **HEMSSDP: IMSIS=12345688, SSDA;**

<OK, Returns a number of users matching IMSIS=12345688 and RID=1>

> **HEMSSDP: IMSIS=12345688, SSDA, RID=1;**

<OK, Returns a number of users matching IMSIS=12345688 and RID=1>



Both the requests print subscribers from Admin Domain 1 with IMSIS=12345688. The first request is assigned to RID=1 during processing because user\_one\_prov is associated with Admin Domain 1. The second request has an explicit RID=1.

**Example 2.** Print all subscribers that match IMSIS=222222

log in as: user\_one\_prov

> HEMSSDP:IMSI=222222,SSDA;

<OK, Does not return any users>

> HEMSSDP:IMSI=222222,SSDA,RID=1;

<OK, Does not return any users>

Both requests do not print any users because the CUDB combined search criteria IMSI and RID do not match any users.

**Example 3.** Print all subscribers that match IMSIS=123456 and RID=2 (Admin Domain 2)

log in as: user\_one\_prov

> HEMSSDP:IMSI=123456,SSDA,RID=2;

<Error message - user has no access to Admin Domain 2>

Returns an error because of RID=2 and associated Admin Domain 2 is not associated with logged in user user\_one\_prov.

**Example 4.** Change all subscribers that belong to Admin Domain 1

log in as: user\_one\_prov

> AEMSSUC:IMSIALL,AMF=14532,FSETIND=2;

<OK, Change subscribers that belong to Admin Domain 1>

> AEMSSUC:IMSIALL,AMF=14532,FSETIND=2,RID=1;

<OK, Change subscribers that belong to Admin Domain 1>

Both requests change all subscribers that are associated with Admin Domain 1 which is associated with user\_one\_prov.

**Example 5.** Change all subscriber that belongs to Admin Domain 1 and 2

log in as: user\_one\_prov

> AEMSSUC:IMSIALL,AMF=14532,FSETIND=2,RID=1&2;



<Error message - user has no access to Admin Domain 2>

Requests return an error because `user_one_prov` have no access to Admin Domain 2.

The following examples show how System Administrator and Local Administrator can use RID and number series to define search scope to cover more than one Admin Domain. Admin Domain configurations in these examples are the same as in the Individual provisioning examples, see Table 1.

**Example 1.** Print all subscribers that `user_localadm` has access to

log in as: `user_localadm`

> `HEMSSDP:IMSI=1234,SSDA;`

<OK, Output>

Prints all subscribers `user_localadm` has access to which are Admin Domain 1, 2 and 3. `RID=1&2&3` is associated with the request because `user_localadm` is associated with Admin Domain 1, 2 and 3 and thus limits the number of returned subscribers. The `IMSI=1234` would include all subscribers in the network defined in Table 1, but the result is limited which is based on what Admin Domain associations `user_localadm` has.

**Example 2.** Print all subscribers from Admin Domain 1 and 3

log in as: `user_localadm`

> `HEMSSDP:IMSI=1234,SSDA,RID=1&3;`

<OK, Prints subscribers from Admin Domain 1 and 3>

Prints all subscribers from Admin Domain 1 and 3.

**Example 3.** Change all subscribers from Admin Domain 1 and 3 using `IMSIALL` instead of `IMSI`

log in as: `user_localadm`

> `AEMSSUC:IMSIALL,AMF=14532,RID=1&3;`

<OK, Changed subscribers from Admin Domain 1 and 3>

**Example 4.** Change all subscribers `user_localadm` has access to

log in as: `user_localadm`

> `AEMSSUC:IMSIALL,AMF=14532;`

<OK, Changed subscribers from Admin Domain 1, 2 and 3>



Changes all subscribers `user_localadm` has access to, which are from Admin Domain 1, 2 and 3.

**Example 5.** Change users with IMSIS=1234 and RID=2&4

log in as: `user_sysadm`

> `HEMSSDP:IMSI=1234,SSDA,RID=2&4;`

<OK, Prints all subscribers from Admin Domain 2 and 4>

Prints all subscribers from Admin Domain 2 and 4. RID is provided, that limits the resulting scope of subscribers.

**Example 6.** Print all subscribers with IMSIS=1234, whole network

log in as: `user_sysadm`

> `HEMSSDP:IMSI=1234,SSDA;`

<OK, Prints subscribers from the whole network>

Prints all subscribers in the whole network. The IMSIS=1234 include all subscribers in the network defined in Table 1.

## 4 Administration of BSS Capacity

This feature ensures fair provisioning capacity sharing between regions/countries/service providers, thus avoiding Denial of Service.

Fair capacity sharing is enforced by introducing Capacity Attributes that define restrictions on the provisioning resources which a provisioning client or provisioning role can utilize. Two Capacity Attributes are used in Dynamic Activation:

- **Connection Restriction Control:** Defines the maximum number of allowed parallel logons on the provisioning interfaces. When the configured limit on a given interface is exceeded, new logon attempts are rejected with an error message.
- **HLR Sustainable Provisioning Throughput Restriction Control:** Defines the minimum HLR Sustainable Customer Service Orders per second. Can also be described as Maximum Allowed HLR Customer Service Orders per second under saturated traffic conditions. The enforcement mechanism is only enabled during saturated traffic conditions.



Feature administration of BSS Capacity depends on feature administration of Multi Regions.

## 4.1 Connection Restriction Control

The feature enables the possibility to configure the Capacity Attribute "maximum number of allowed parallel logons" on the MML and CAI3G interfaces. The restrictions apply per user and Dynamic Activation system.

One limit can be configured for MML (includes both TELNET and SSH), and CAI3G (includes both HTTP and HTTPS). They are mutually independent. One user can be allowed to have, for example five parallel logons on the MML interface, and 10 parallel logons on the CAI3G interface simultaneously.

When the configured limit on a given interface is reached, a new logon attempt is rejected with an error message.

The configuration and restriction check is system wide, which means that all logons on different cluster nodes add up towards the configured maximum limit.

For example, if `user_one_prov` has maximum five MML sessions, the sixth time logon attempt to the Dynamic Activation over the MML interface is rejected.

When defining connection restrictions, all provisioning clients must be considered. This means that the connection capacity of a system must be shared by users not only provisioning the HLR, but also other applications, such as IMS.

The MML and CAI3G protocol implementations are synchronous. This means that every MML client and CAI3G client have only one outstanding request per client. The following table illustrates the theoretical restriction figures that can be expected using the Connection Restriction feature.

*Table 2 Restriction Figures for Connection Restriction Control*

User	Number of MML Connections/Number of CAI3G HTTP Clients	Example of Latency in Milliseconds	Throughput per User and MML Connection or CAI3G HTTP Client (CSO/sec)
<code>user_one_prov</code>	10	100	100
<code>user_11_IN</code>	5	100	50
<code>user_localadm</code>	1	100	10
<code>user_two_prov</code>	20	100	200





## 4.2 Sustainable Provisioning Throughput Restriction Control

The purpose of the HLR sustainable throughput Restriction Control is to limit throughput on Individual Provisioning interfaces - MML and CAI3G. The feature has the following characteristics:

- The throughput restriction is set and measured in Customer Service Orders per second - CSO/sec.
- Restrictions can be set on both Provisioning Clients and Admin Domains, see Section 3 on page 2.
- The configuration and throughput restriction check is cluster wide, which means that all requests on different payload nodes add up towards the configured maximum throughput limit.
- Each system has a maximum traffic threshold which depends on the number of payload nodes in the system. The restriction is enabled only when maximum traffic threshold is reached. This means Provisioning Clients or Admin Domains could use more throughput than the configured values if the threshold is not reached.
- The total configured CSO/sec value for all Provisioning Clients belonging to one Admin Domain must never exceed the Administration Domain configured CSO/sec.
- The subscriber identifier MSISDN or IMSI defines which Admin Domain a request belongs to. Common Data or Massive Service DATA provisioning is not restricted.
- If there are other applications that provision through Dynamic Activation, such traffic is measured when calculating the maximum traffic threshold. However, when the threshold is reached, throughput control applies only on HLR and AUC individual provisioning requests.
- The Sustainable Provisioning Throughput Restriction Control is a best effort implementation. Configured throughput values and observed throughout values for a single user or domain can differ significantly when more than three users or domains are configured. Combine this feature with the Connection Restriction Control feature to fine-tune the throughput.

There are several examples that illustrate how previously characteristics behave.

**Example 1.** Throughput is lower than traffic threshold.

*Table 3 Configuration for the Example*

Number of Payload Nodes	Traffic Threshold CSO/sec	Admin Domain	Min. HLR Sustainable Throughput per Domain CSO/sec	User	Min. HLR Sustainable Throughput per User CSO/sec
4 nodes	1200	1	400	user_one_prov	- (not specified)
		2	800	user_two_prov	-

- user\_one\_prov sends 450 CSO/sec.
- user\_two\_prov sends 500 CSO/sec.

No restrictions are enforced because system has not reached traffic saturation.

**Example 2.** Admin Domain throughput restrictions enforced when throughput has reached traffic threshold.

*Table 4 Configuration for the Example*

Number of Payload Nodes	Traffic Threshold CSO/sec	Admin Domain	Min. HLR Sustainable Throughput per Domain CSO/sec	User	Min. HLR Sustainable Throughput per User CSO/sec
4 nodes	1200	1	400	user_one_prov	-
				user_11_IN	-
		2	800	user_two_prov	-

- user\_one\_prov sends 300 CSO/sec, the sum of CSO/sec for user\_one\_prov and user\_11\_IN is limited to 400.
- user\_two\_prov sends 800 CSO/sec.
- user\_11\_IN sends 150 CSO/sec, the sum of CSO/sec for user\_one\_prov and user\_11\_IN is limited to 400.

Restrictions are enforced because system has reached traffic saturation.

**Note:** The Connection Restriction Control feature is needed to get the exact Admin Domain throughput balance.

**Example 3.** One node stops to receive traffic.



Table 5 Configuration for the Example

Number of Payload Nodes	Traffic Threshold CSO/sec	Admin Domain	Min. HLR Sustainable Throughput per Domain CSO/sec	User	Min. HLR Sustainable Throughput per User CSO/sec
4 nodes	1200	1	400	user_one_prov	-
				user_11_IN	-
		2	800	user_two_prov	-

- user\_one\_prov sends 300 CSO/sec.
- user\_11\_IN sends 100 CSO/sec.
- user\_two\_prov sends 800 CSO/sec.

Node one stops receiving traffic reducing system-wide throughput to 900 CSO/sec.

Provisioning Client and Administration Domain throughput is reduced to 900 CSO/sec and user throughput decreases proportionally to the configured Admin Domain throughput restrictions.

**Note:** The Connection Restriction Control feature is needed to get the exact Admin Domain throughput balance.

**Example 4.** Provisioning Client throughput restriction when throughput has reached traffic threshold.

Table 6 Configuration for the Example

Number of Payload Nodes	Traffic Threshold CSO/sec	Admin Domain	Min. HLR Sustainable Throughput per Domain CSO/sec	User	Min. HLR Sustainable Throughput per User CSO/sec
4 nodes	1200	1	-	user_one_prov	300
				user_11_IN	100
		2	-	user_two_prov	800

- user\_two\_prov sends 800 CSO/sec.
- user\_one\_prov sends 300 CSO/sec
- user\_11\_IN tries to send 150 CSO/sec, but gets only 100 CSO/sec because the Admin Domain 1 CSO/sec = 400 and user restriction is set to CSO/sec = 100.

Restrictions are enforced because system has reached traffic saturation.

**Note:** The Connection Restriction Control feature needs to get the exact Admin Domain throughput balance.



**Example 5.** Throughput restriction for a user belonging to more than one Admin Domain when throughput has reached traffic threshold.

*Table 7 Configuration for the Example*

Number of Payload Nodes	Traffic Threshold CSO/sec	Admin Domain	Min. HLR Sustainable Throughput per Domain CSO/sec	User	Min. HLR Sustainable Throughput per User CSO/sec
4 nodes	1200	1	400	user_one_prov	300
				user_11_IN	50
		1, 2		user_localadm	-
		2	800	user_two_prov	800

- user\_two\_prov sends 750 CSO/sec, 50 CSO/sec left of Admin Domain 2 throughput.
- user\_one\_prov sends 300 CSO/sec, 100 CSO/sec left of Admin Domain 1 throughput.
- user\_localadm sends 100 CSO/sec, utilizing 50 CSO/sec from Admin Domains 1 and 50 CSO/sec from Admin Domain 2.
- user\_11\_IN sends 150 CSO/sec, but gets only 50 CSO/sec because the user restriction is set to CSO/sec = 50.

Restrictions are enforced because system has reached traffic saturation.

**Note:** The Connection Restriction Control feature needs to get the exact Admin Domain and user throughput balance.

**Example 6.** Admin Domain and Provisioning Client combination throughput restriction when throughput has reached traffic threshold.

*Table 8 Configuration for the Example*

Number of Payload Nodes	Traffic Threshold CSO/sec	Admin Domain	Min. HLR Sustainable Throughput per Domain CSO/sec	User	Min. HLR Sustainable Throughput per User CSO/sec
4 nodes	1200	1	400	user_one_prov	-
				user_11_IN	10
		2	800	user_two_prov	-

- user\_two\_prov sends 800 CSO/sec.
- user\_one\_prov sends 600 CSO/sec, gets 390 CSO/sec
- user\_11\_IN tries to send 20 CSO/sec, gets 10 CSO/sec



Restrictions are enforced because system has reached traffic saturation.

**Note:** The Connection Restriction Control feature needs to get the exact Admin Domain and user throughput balance.





## Reference List

- [1] *Library Overview*, 18/1553-CSH 109 628 Uen
- [2] *Function Specification Layered HLR*, 4/155 17-CSH 109 628 Uen
- [3] *Function Specification Resource Activation*, 3/155 17-CSH 109 628 Uen
- [4] *Configuration Manual for Resource Activation*, 2/1543-CSH 109 628 Uen