3GPP TR 23.812 V11.0.0 (2011-12)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on IP Multimedia Subsystem (IMS) evolution (Release 11)

Keywords

3GPP, Architecture, IMS

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The scope of the technical report is to capture the results of a study into the feasibility of enhancing IMS network architecture. This report intends to study the feasibility of enhancing IMS network architecture as follows,

- Investigating architectural improvements to reduce the complexity of signalling procedures by reducing the signalling hops, or the number of options and combinations (by looking at different groupings of combining existing entities);
- Investigating means to improve system-level load balancing and reliability;
- Investigating possibilities for reducing configuration workload to save OPEX.
- Investigating the introduction of IMS Overload Control mechanisms.

Backward compatibility with current IMS specifications shall be ensured.

NOTE: overlap with SA5 and CT4 work need to be monitored.

This report is intended to explore potential architecture improvements and also provide conclusions on the above aspects with respect to potential future normative specification work.

There are a number of functions involved in call session setup in IMS network. Interfaces and interactions between network elements may be a little complicated and not that efficient. It is deemed beneficial to review the current IMS architecture including aspects such as the possible optimization of interfaces/reference points (by looking at different groupings of combining existing entities), reducing options of solutions for the same issues, relevancy of certain functions etc.

IMS network service availability largely relies on the reliability of network entities. If some network elements implementing critical functions (e.g. S-CSCF, HSS) fail, service availability may be impacted. Moreover network elements may not be fully utilized because network load may not be well distributed, e.g. some nodes may be overloaded due to sudden traffic increase, while others may be under loaded to some extent. Though there are some element level approaches to solve these problems, some system level solutions should be studied, for example, the method to distribute load between network elements in different geographical locations especially when a disaster happens, such as earthquake.

Network expansion may require significant manual configurations, and the network maintenance and upgrade may be time-consuming and also may be costly for operators. Introducing self-organization features may improve the network intelligence and reduce the efforts of manual configuration.

The objectives of the study for investigating the introduction of IMS Overload Control mechanisms are to:

- Determine the parts of IMS architecture for which overload control mechanisms are needed;
- Evaluate the applicability of candidate solutions for Overload Control to the SIP entities of the IP multimedia core network architecture, including:
    - mechanisms having already been specified or studied within 3GPP and their possible enhancements,
    - mechanisms specified or studied by other bodies (e.g. ETSI TISPAN, IETF) and their possible enhancements,
    - other mechanisms, if proposed within this work item;
- Provide recommendations based on analysis.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[3] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[4] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[5] ETSI ES 283 034-2 V3.1.1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Congestion and Overload Control; Part 2: Core GOCAP and NOCA Entity Behaviours".

[6] IETF draft, draft-ietf-soc-overload-control-01: "Session Initiation Protocol (SIP) Overload Control".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[7] IETF draft, draft-ietf-soc-load-control-event-package: "A Session Initiation Protocol (SIP) Load Control Event Package".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[8] IETF RFC 2136: "Dynamic Updates in the Domain Name System (DNS UPDATE)".

[9] IETF RFC 1034: "Domain Names - Concepts and Facilities".

[10] IETF RFC 1995: "Incremental Zone Transfer in DNS".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Load Balancing: technique to distribute workload evenly across two or more network nodes implementing the same functions, in order to get optimal resource utilization.

Overload Control: technique to detect and react to the near-congestion state of a network /node.

Congestion Control: a set of actions taken to relieve congestion by limiting the spread and duration of it. (ITU-T Recommendation I.113, definition 703).

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] apply.

4 Analysis of IMS architecture

Editors note: This clause analyzes IMS architecture and identifies some problems from architectural level.

4.1 Session setup efficiency

4.1.1 Problems description

Editors note: This clause illustrates standard IMS session setup flows and identifies the complexity of P/I/S-CSCF interaction.

4.1.2 Summary

4.2 Load Balancing

4.2.1 Problems description

Editors note: This clause analyzes IMS Load Balance mechanism (e.g. P/S/I-CSCF/SLF/HSS) and identifies potential load balance problems (e.g. how to handle explosive traffic) under IMS architecture.

4.2.1.1 General

Load Balancing is an important mechanism in telecommunication networks. In general, we can adopt DNS technology in IMS to achieve limited Load Balancing. However, current DNS cannot coordinate with IMS to achieve real-time and more dynamic Load Balancing. Specifically, it is difficult to handle explosive traffic growth when a part of the IMS network is overloaded. This section analyzes IMS Load Balancing mechanisms (e.g. P-CSCF/S-CSCF/I-CSCF/SLF/HSS) and identifies potential Load Balancing problems (e.g. how to handle explosive traffic growth).

4.2.1.2 Analysis of P-CSCF Load Balancing

Generally, there are three methods used by the UE to discover P-CSCF addresses:

1) The UE shall request the P-CSCF address(es) from the GGSN when activating the PDP context. The GGSN shall send the P-CSCF address(es) to the UE when accepting the PDP context activation.

2) Use of DHCP to provide the UE with the domain name and/or IP address of a P-CSCF and the address of a DNS that is capable of resolving the P-CSCF name.

3) The UE may be configured with the fully qualified domain name (FQDN) of a P-CSCF or its IP address.

As stated above, IMS does not provide any mechanism for Load Balancing among P-CSCFs, allowing to direct the UE to a low loaded P-CSCF. 3GPP specifications, such as TS 23.060 [2], do not explicitly define how a GGSN obtains a P-CSCF address. Generally, a GGSN may be configured statically with a P-CSCF address. It is similar to DHCP, where P-CSCF domain names are configured statically.

Currently, a P-CSCF may reject a registration request from a UE when it is overloaded. This mechanism may not be sufficient in order to handle explosive traffic growth or to distribute the load between P-CSCFs.

4.2.1.3 Analysis of S-CSCF Load Balancing

When a UE initially registers in the IMS, a S-CSCF shall be assigned to serve the UE. S-CSCF assignment is performed by the I-CSCF, but the S-CSCF selection policy of the I-CSCF mainly depends on the capabilities, topological information and the availability of the S-CSCF (See TS 23.228 [3] for details). The I-CSCF does not have Load Balancing information related to the S-CSCFs, which may result in a bad distribution of the load between the S-CSCF of an IMS network.

When a UE re-registers, the S-CSCF, which was assigned at initial registration, may no longer be the optimal choice with regard to load balance and/or availability of alternative S-CSCFs. S-CSCF re-selection may not be done during re-registration, which may lead to sub-optimal S-CSCF allocations for a long time period.

For incoming SIP requests other than SIP REGISTER, the choice for an S-CSCF that shall handle this requests is based on the S-CSCF that is selected during registration, for those cases where registration is applicable. For cases where registration is not applicable (such as IMS as "transit" network, and peering based business trunking), the S-CSCF (or Transit Function) selection is based on pre-configured static information e.g. information stored in an HSS. This static information may not always be the optimal choice.

4.2.1.4 Analysis of SLF Load Balancing

The SLF supports HSS address queries for the I-CSCF or S-CSCF when there are multiple HSSs in an IMS network. In a large-scale network, the SLF may become a bottleneck of the system.

4.2.1.5 Analysis of HSS Load Balancing

HSS Load Balancing involves knowledge of the capacities of different HSS entities and data storage planning. Because different HSSs have different capacities, an imbalance of user data storage may result and it is not easy to guarantee the well-distributed traffic among the HSSs.

4.2.1.6 Analysis of I-CSCF Load Balancing

Load Balancing between I-CSCF entities can be achieved by means of DNS, based on existing Load Balancing algorithms. This capability will not be further investigated.

4.3 Recovery and Load Balancing

4.3.1 Problems description

4.3.1.1 General

This clause analyzes current IMS Recovery and Load Balancing mechanisms.

4.3.1.2 Analysis of current entity-level redundancy/restoration mechanism

Generally in IMS network, entity-level redundancy mechanism can be used to survive entity failures without the co-operation with IMS core. This mechanism uses additional entities and backs up all data locally during running time. Pre-configuration is done for the pair of the original entity and a backup one. When the original one breaks down, the backup one will take over its task at once. This method does not handle the case where both the original entity and the backup one are both down due to e.g. an earthquake.

4.3.1.3 Analysis of current system-level reselection/restoration mechanism

Currently, 3GPP CT4 has specified restoration procedures for S-CSCF restoration in TS 23.380 and is doing additional study on other system-level IMS restoration in TR 23.820 (e.g. P-CSCF and HSS) to enhance the network restoration capabilities. These solutions are all based on the reassignment of a new entity taking over the load from the failed one. However, it is not specified today how the load status of the new entity could be taken into account when performing a re-selection. If the load status is not taken into account during e.g. the S-CSCF re-selection process of the restoration procedures, this could in a worst case scenario result in that the load of the failed entity is transferred to other entities and those newly selected entities may get overloaded. The situation may get even worse when a regional disaster happens, which may cause an explosive traffic load.

4.3.2 Summary

As for initial registration and re-registration, a proper S-CSCF Load Balancing mechanism may be needed when performing restoration procedures. S-CSCF restoration is built up in two steps, the I-CSCF procedure of re-selecting a S-CSCF, and the procedure of restoring the data in the S-CSCF. The (re-)selection mechanism used for S-CSCF restoration procedures, are basically the same as the normal S-CSCF selection mechanism for initial registration. Hence, the restoration procedures could benefit of the S-CSCF (re-)selection mechanisms being studied in this TR.

4.4 Scalability

4.4.1 Problems description

Editor's note: This section analyzes IMS scalability mechanism and identifies potential scalability problems (e.g. how to reduce OPEX upon SLF/HSS and P/I/S-CSCF expansion).

The network scalability is a critical point for the network expansion ability and maintenance of an IMS network. The problem of scalability includes several aspects. How to preserve the efficiency of locating user data is one of them if the number of subscribers grows a lot.

When the number of subscribers increases continuously, operators usually need to deploy multiple HSSs that may be distributed geographically. SLF is thus deployed to handle the selection of multiple HSSs. The size of the SIP URI based index table in SLF will become bigger and bigger which may as result cause the inefficiency of addressing the right HSS through querying SLF via Dx and Dh interface. These inefficiencies may be implementation dependent rather than standardization related.

Another aspect relates to the synchronization amongst distributed SLFs. If distributed SLFs are utilized to, e.g. improve the efficiency of locating the right HSS or handle restoration issues, every time a new HSS equipment is added to expand the user capacity, all distributed SLFs may have to be synchronized with the new index information. The larger the user capacity becomes, the larger the number of SLFs needs to be, and the more time-consuming the synchronization will be.

4.4.2 Summary

5 Applicability of Overload Control and Load Balancing

Editor's note: This clause aims to determine the parts of IMS architecture and the operational use cases for which Overload Control and Load Balancing mechanisms are needed.

5.1 Overload Control

5.1.1 Overload Control at the UNI

5.1.1.1 P-CSCF overload control

The P-CSCF overload control may happen during the registration or re-registration process. The solution alternatives are described in clause 6.2.1.

Impacts on the UE should be minimized.

5.1.2 Overload Control at the NNI

5.1.3 Overload Control of Application Servers

5.1.4 S-CSCF overload control

The S-CSCF overload control happens during registration/re-registration process. The solution alternatives are described in clause 6.2.2.

5.2 Load Balancing

5.2.0 General

The IMS Load Balancing can be applicable to:

- dynamically monitor and balance the load between entities of the same kind to reduce the load gaps;
- automatically balance load when a new entity is added to the network or a working entity is removed;
- automatically or in a manual way balance the load between different regions or entity pools.

5.2.1 P-CSCF Load Balancing

The P-CSCF Load Balancing happens during registration process.

P-CSCF Load Balancing can be executed either with a mapping from domain name to IP address, or with reconfiguration at IP-CAN or UE.

Impact on UE should be minimized.

5.2.2 S-CSCF Load Balancing

The S-CSCF Load Balancing happens during registration/re-registration process.

S-CSCF Load Balancing can be executed either with a mapping from domain name to IP address or with reconfiguration at I-CSCF (or maybe at HSS).

5.2.3 Applicability of P/S-CSCF Load Balancing based on periodic monitoring to massive restart of UEs

The following discusses how a Load Balancing mechanism based on periodic monitoring of the CSCF load may be applicable to the following cases:

1) Massive restart of UEs served by a pool of load-balanced P-CSCF nodes.
2) Massive restart of UEs served by a pool of load-balanced S-CSCF nodes.

Such massive restart of a large number of UEs may for example happen:

- when an IMS node serving these UEs goes down,
- when an access network or power outage occurs in a given regional area,
- following the distribution of an OS patch causing the UEs to reboot.

In the above cases, the rapidity and the intensity of the load fluctuation depends on:

a) the UE restart algorithm;

NOTE: The following is mandated in TS 24.229, clause 5.1.1.2.1, in Rel-9 onwards, but we cannot assume that all deployed UEs comply to this algorithm: "*After a maximum of 2 consecutive unsuccessful initial registration attempts, the UE shall implement the mechanism defined in clause 4.5 of RFC 5626 [92] for new registration attempts. The UE shall use the values of the parameters max-time and base-time, of the algorithm defined in clause 4.5 of RFC 5626 [92]. If no values of the parameters max-time and base-time have been provided to the UE by the network, the default values defined in clause 4.5 of RFC 5626 [92] shall be used.*"

b) the choice the operator has made to configure the restart timers;

c) aspects of the DNS behaviour not currently specified.

In typical IMS deployments it is expected that the periodicity between initial registration attempts will be less or equal to the re-registration periodicity. A re-registration periodicity of 1 hour is expected to be a widespread order of magnitude in current IMS deployments.

When the respective loads of the P-CSCF or S-CSCF nodes in a pool are nearly equal, which is for instance the case when the P-CSCF or S-CSCF pool receives no traffic for some time following a network failure or a power failure affecting the served UEs, there is currently no guarantee that the initial registration traffic following the end of the failure will not be directed to a single P-CSCF or S-CSCF node within the pool until the next load information update. This is for instance the case when the DNS Server or the UEs resolve the P-CSCF pool FQDN into a single IP address (assuming the loads of the P-CSCF in pool are nearly equal).

Therefore, the load monitoring periodicity needs to be shorter than the initial registration attempt periodicity divided by the number of P-CSCF nodes or S-CSCF in the considered pool.

The following figure represent the behaviour **at the limit**, taking as an example the case of 4 nodes in a pool, to which a load-balancing mechanism based on periodic monitoring as applied, after a massive restart, with an initial registration periodicity of 1 hour and a monitoring periodicity of 15 minutes (assuming the case where the DNS Server of the UE resolves the P-CSCF pool FQDN into a single IP address among the set of less-loaded nodes).

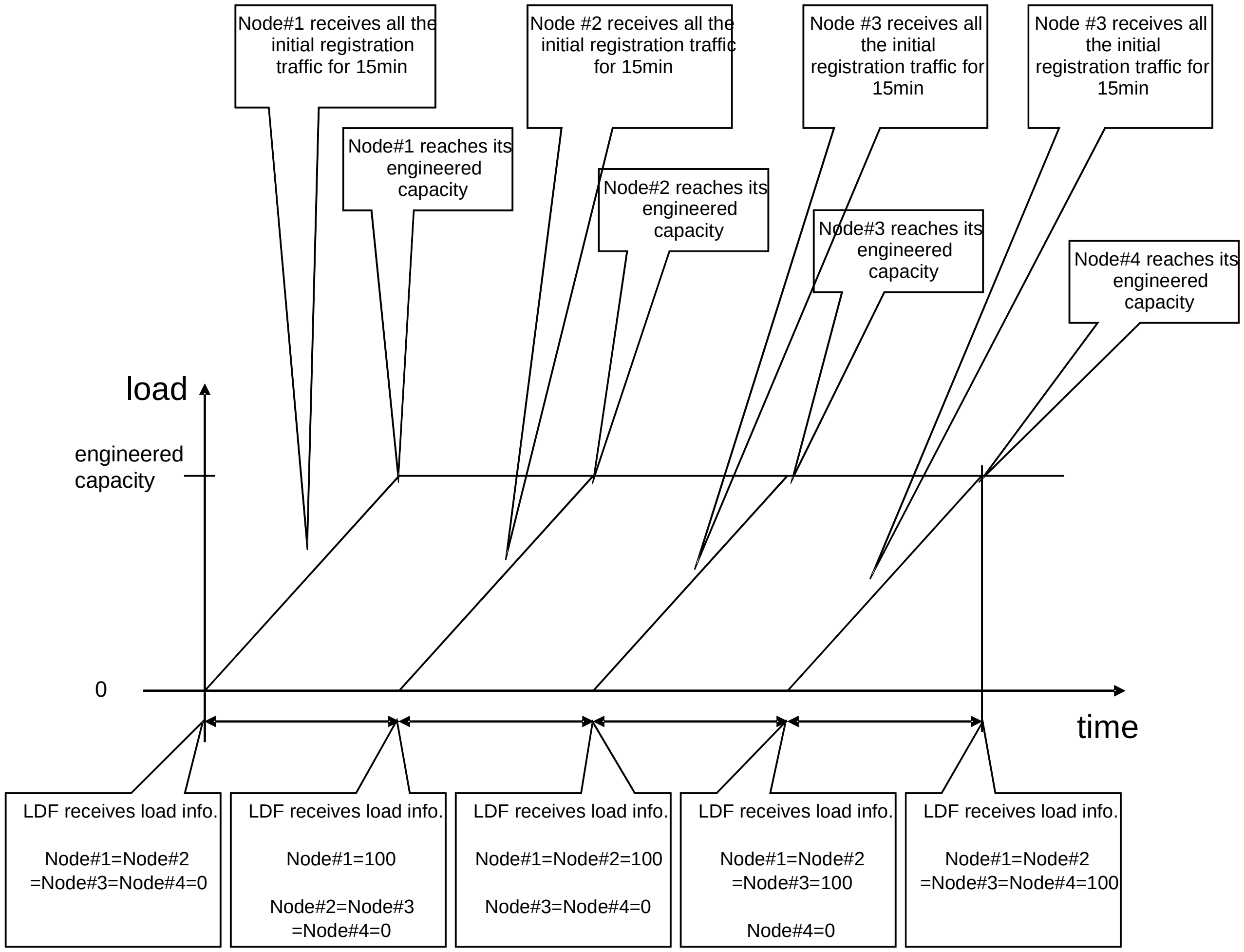

Node#1 receives all the initial registration traffic for 15min
Node#1 reaches its engineered capacity
Node #2 receives all the initial registration traffic for 15min
Node#2 reaches its engineered capacity
Node #3 receives all the initial registration traffic for 15min
Node#3 reaches its engineered capacity
Node #3 receives all the initial registration traffic for 15min
Node#4 reaches its engineered capacity
load
engineered capacity
0
time
LDF receives load info. Node#1=Node#2 =Node#3=Node#4=0
LDF receives load info. Node#1=100 Node#2=Node#3 =Node#4=0
LDF receives load info. Node#1=Node#2=100 Node#3=Node#4=0
LDF receives load info. Node#1=Node#2 =Node#3=100 Node#4=0
LDF receives load info. Node#1=Node#2 =Node#3=Node#4=100

Figure 5.2.3-1

5.2.4 AS Load Balancing

6 Architecture alternatives

Editor's note: This clause aims to come up with solutions from architecture's point of view to resolve the problems described in clause 4.

6.1 Architecture alternatives for Load Balancing

6.1.1 Load Balancing based on Load Detection Function

6.1.1.1 Load Detection Function (LDF)

6.1.1.1.1 General

In order to perform overload detection and resolution and/or Load Balancing between P-CSCFs or S-CSCFs, a new function called the Load Detection Function (LDF) is proposed to monitor and store the load information of all P-CSCFs and S-CSCFs, (e.g. CPU and Memory Usage, currently supported number of users, or service related factors) and execute policies based on that to, e.g. select P/S-CSCFs.

The functions of the LDF include:

- Monitor and store the load information of network entities(e.g. P-CSCF, S-CSCF) in an operator's domain;

NOTE: Periodic monitoring can be used by the LDF to obtain load information of network entities; this is particularly applicable when the LDF is used for Load Balancing. A threshold crossing indication mechanism can be used by the LDF to obtain load information of P/S-CSCFs, for example, when their load exceeds a pre-defined threshold. This is particularly applicable when the LDF is only used for Overload Control.

- Make Load Balancing or Overload Control decision/policy such as triggering a proper network re -configuration with a certain pre-tested configuration or performing a purely dynamic Load Balancing algorithm;
- Download the load balance decision/policy to related network entities (e.g. IP-CAN related entities, I-CSCF, or DNS) to execute.

Editor's note: Whether LDF is used to perform Overload Control is dependent on the assessment of all Overload Control alternatives.

6.1.1.1.2 Alternative 1 for LDF architecture

The figure below illustrates the reference points of the LDF in this alternative.

- The LDF monitors the load of IMS entities via the Lm reference point. The load information required by LDF can be as stated in Annex X.
- The LDF downloads the load balance decision/policy to DNS via the Ln reference point, and DNS UPDATE mechanism defined in RFC 2136 can be reused to implement this functionality (Refer to Annex A). If DNS is not enabled for selection of IMS entities in practice, Ln reference point is used to transfer configuration parameters to I-CSCF for S-CSCF selection and to IP-CAN for P-CSCF selection. The Ln reference point can also be used to inform IMS entities, such as P-CSCFs and S-CSCFs, their backup entities for Overload Control.

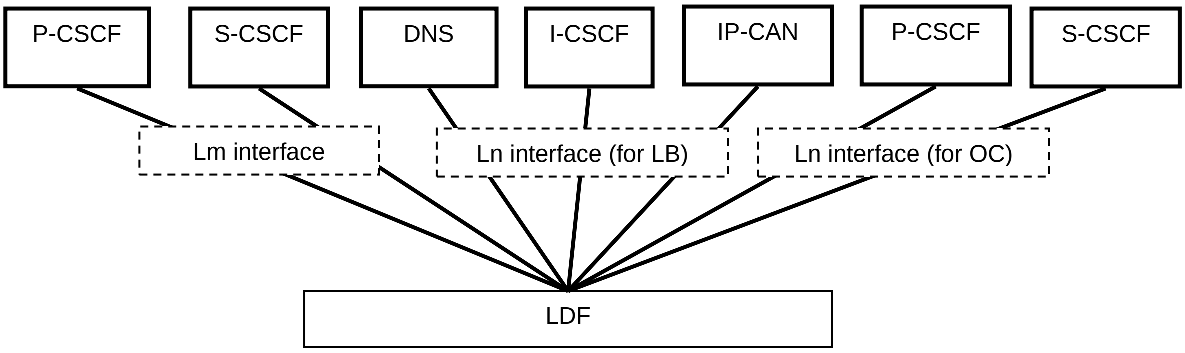


Figure 6.1-1: LDF Interfaces without EMS/NMS

6.1.1.1.3 Alternative 2 for LDF architecture

The interconnection between LDF and other Load Balancing/Overload Control involved entities can be through EMS/NMS as shown below.

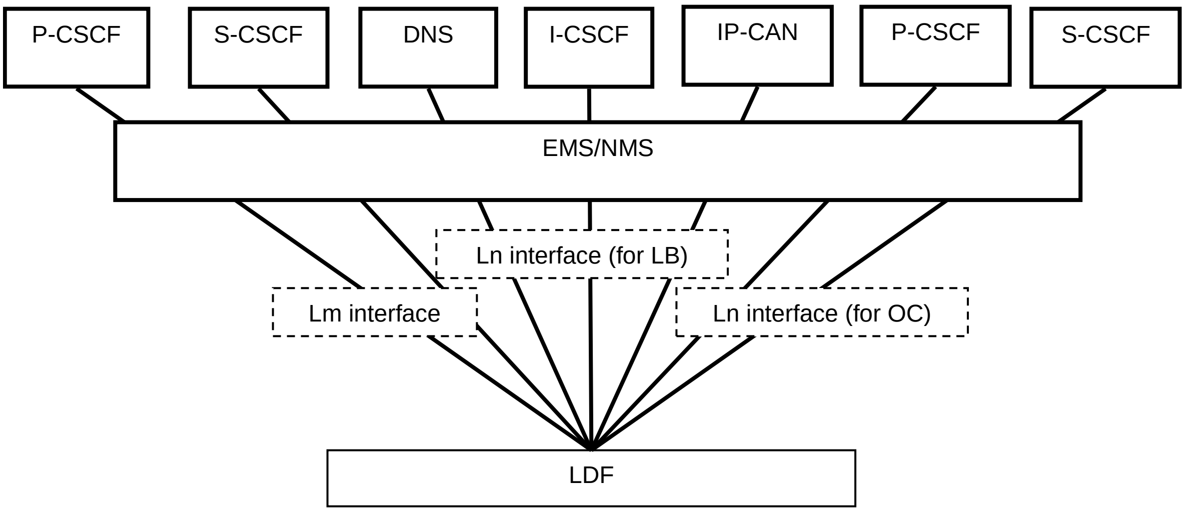


Figure 6.1-2: LDF Interfaces with EMS/NMS

NOTE: Considerations need to be made for the redundancy and reliability mechanisms for the LDF to ensure the availability of the LDF.

Periodic monitoring of a CSCF's load induces an additional workload on this CSCF. Monitoring shall be designed in such a way that such added workload is negligible compared to the workload caused by normal operations of the CSCF such as SIP routing.

Editor's note: The network management related issues should be transferred to SA5 for discussion. The relation between the LDF based Load Balancing mechanism and the existing network management system is for future study.

6.1.1.1.4 Alternative 3 for LDF architecture

This alternative is a specific form of Alternative 2, where:

- The LDF retrieves the load information from the EMs through the management interface Itf-N (type 2) specified in TS 32.101, and is seen as an NM by the EMs.

- The load balancing decision/policy is provided by the LDF to DNS via a non-standardized interface. This can be achieved by co-locating the DNS with the LDF.

This is depicted on the figure below.

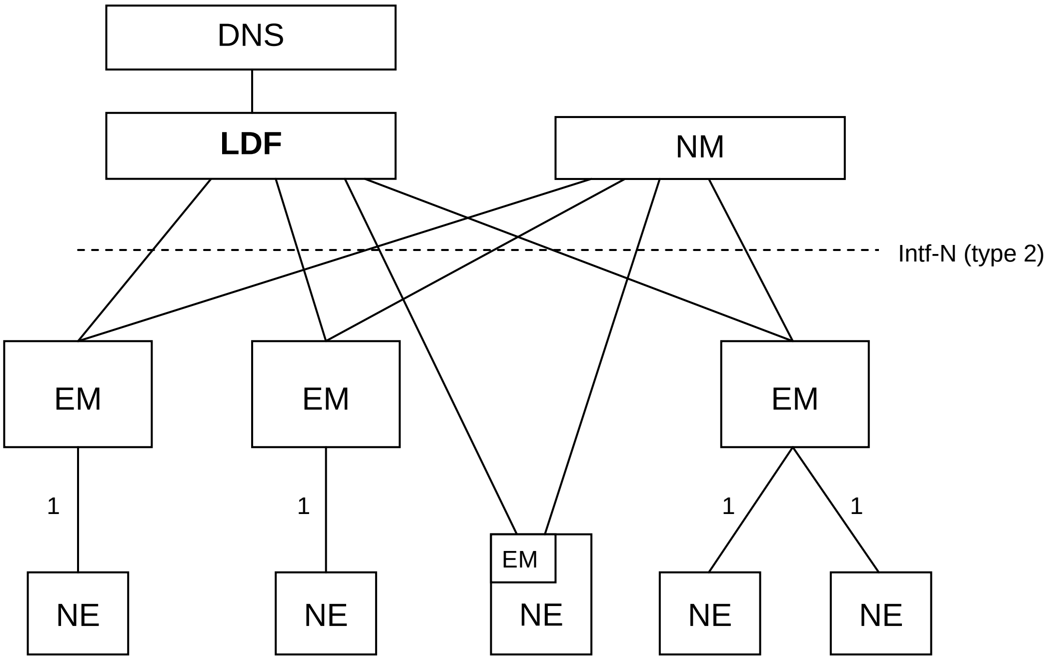


Figure 6.1-3: LDF interfaces with EMS

6.1.1.1.5 Alternative 4 for LDF architecture

This minimalist LDF architecture is a subset of Alternative 1, where only the Lm reference point is considered:

- The LDF monitors the load of IMS entities via the Lm reference point, which can thus be seen as a Type 1 interface from a telecom management perspective. The load information required by LDF can be as stated in Annex C.
- The load balancing decision/policy is provided by the LDF to DNS via a non-standardized interface. This can be achieved by co-locating the DNS with the LDF.

This is depicted on the figure below.

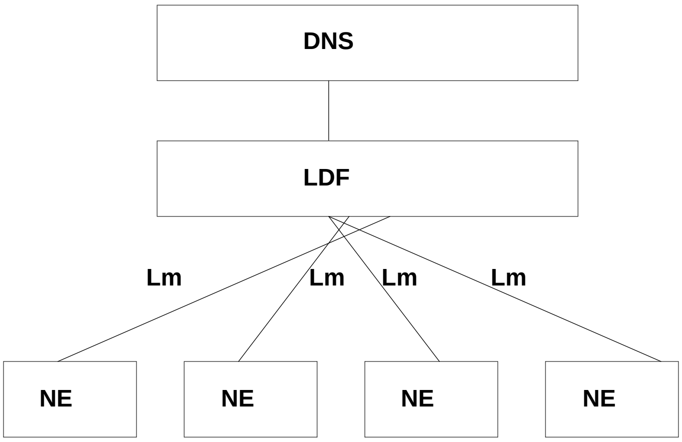


Figure 6.1-4: LDF interfaces for load monitoring

6.1.1.2 P-CSCF Load Balancing with LDF

6.1.1.2.1 General

In order to achieve Load Balancing between P-CSCFs, the Load Detection Function (LDF) is utilized to monitor and store the load information of all P-CSCFs.

The P-CSCF Load Balancing mechanisms implemented by the LDF are:

- Monitor and store the load information of P-CSCFs. This is achieved either by querying each P-CSCF, or by collecting information reported by the P-CSCFs.

- Update the load information of P-CSCFs periodically to DNS.

6.1.1.2.2 Information flow

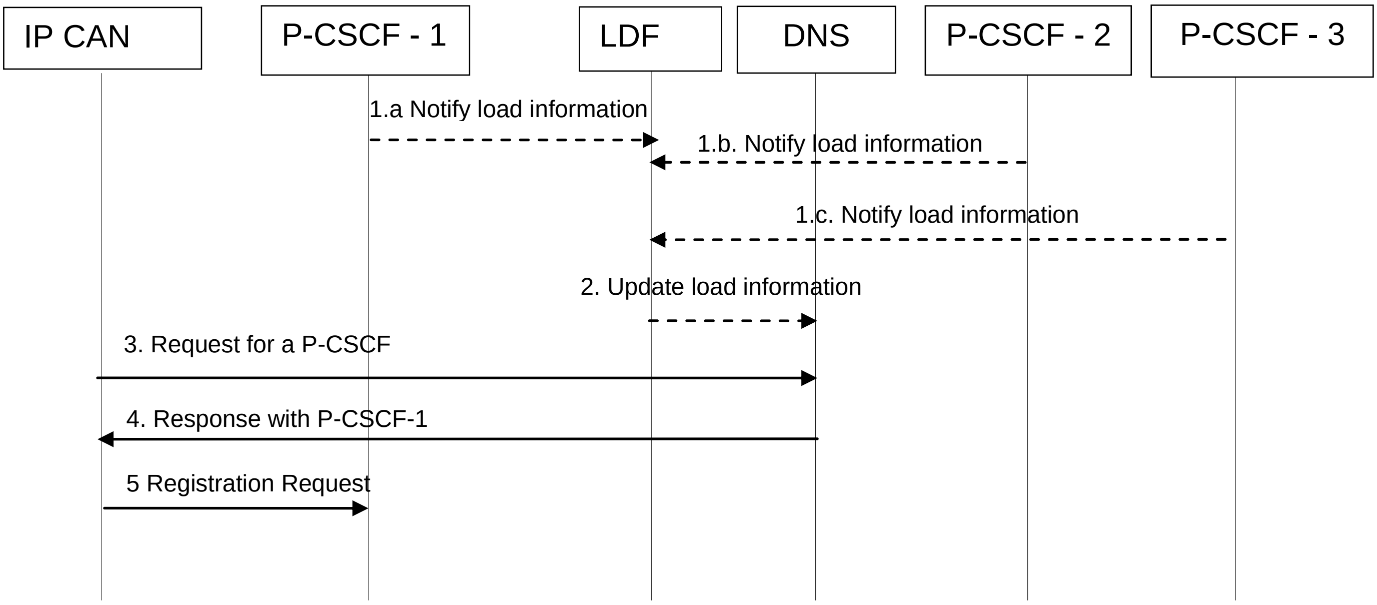

IP CAN
P-CSCF - 1
LDF
DNS
P-CSCF - 2
P-CSCF - 3
1.a Notify load information
1.b. Notify load information
1.c. Notify load information
2. Update load information
3. Request for a P-CSCF
4. Response with P-CSCF-1
5 Registration Request

Figure 6.1-5: Information flow for P-CSCF Load Balancing

1. P-CSCF-1, P-CSCF-2 and P-CSCF-3 notify the load information to LDF(e.g. periodically).

2. LDF updates the load state of the relevant P-CSCFs to DNS at a given interval.

NOTE 1: For Alternative 2 of LDF architecture, EMS/NMS is used for information delivery between LDF and P-CSCF as well as between LDF and DNS as shown in figure 6.1-2.

3. UE initiates an address query for P-CSCF to DNS.

4. DNS implements a Load Balancing algorithm and return the address of a relatively low-load P-CSCF-1. If all available LDFs go out of service for some reason, DNS is required to be aware of this failure and fall back to the static P-CSCF assignment mechanism (e.g. round robin) without considering load information.

5. UE sends IMS registration request to P-CSCF-1.

NOTE 2: DNS caching may break this Load Balancing mechanism, if the TTL of DNS entries is not set to zero or a very small value (e.g. a value that is close to the load probing period). It is up to the operator to define the TTL of DNS entries, e.g. by making a trade-off between the cost of extra DNS queries induced by lowering the TTL, and the benefits provided by this Load Balancing mechanism.

6.1.1.3 S-CSCF Load Balancing during initial registration

6.1.1.3.1 General

The load information of S-CSCFs is beneficial to improve the Load Balancing across S-CSCFs. If the load state of S-CSCFs is considered when selecting S-CSCF during the initial registration, load imbalance amongst S-CSCFs might be alleviated to some extent and S-CSCFs might be utilized more efficiently. The LDF (Load Detection Function) could be introduced to help implement S-CSCF Load Balancing for certain scenarios.

The following observations can be made:

- When performing Load Balancing for the S-CSCF during initial registration, it is not only the current traffic load of the S-CSCFs that is of interest, but the maximum expected load that the registered users will create during busy hours.
- Different users imply different expected load on the system at different periods of times. A business user generates different load than residential users. A user with only one terminal using MMTEL, will have quite different behaviour than a user with multiple terminals, using MMTEL, Push-to-talk, Messaging, IMS based mobile TV, and enabled for ICS/SRVCC/Inter-UE transfer.

NOTE: Different IMS subscriptions may have different load caracteristics (such as IP PBX). This can be taken into account by the operator by configuring specific server capabilities in the user profile of users that have specific characteristics (e.g. to direct IP PBX registrations to S-CSCFs that are dimensionned to serve IP PBXs).

6.1.1.3.2 Information flow

Figure 6.1-6 shows an information flow where a relatively low-load S-CSCF is selected during IMS initial registration.

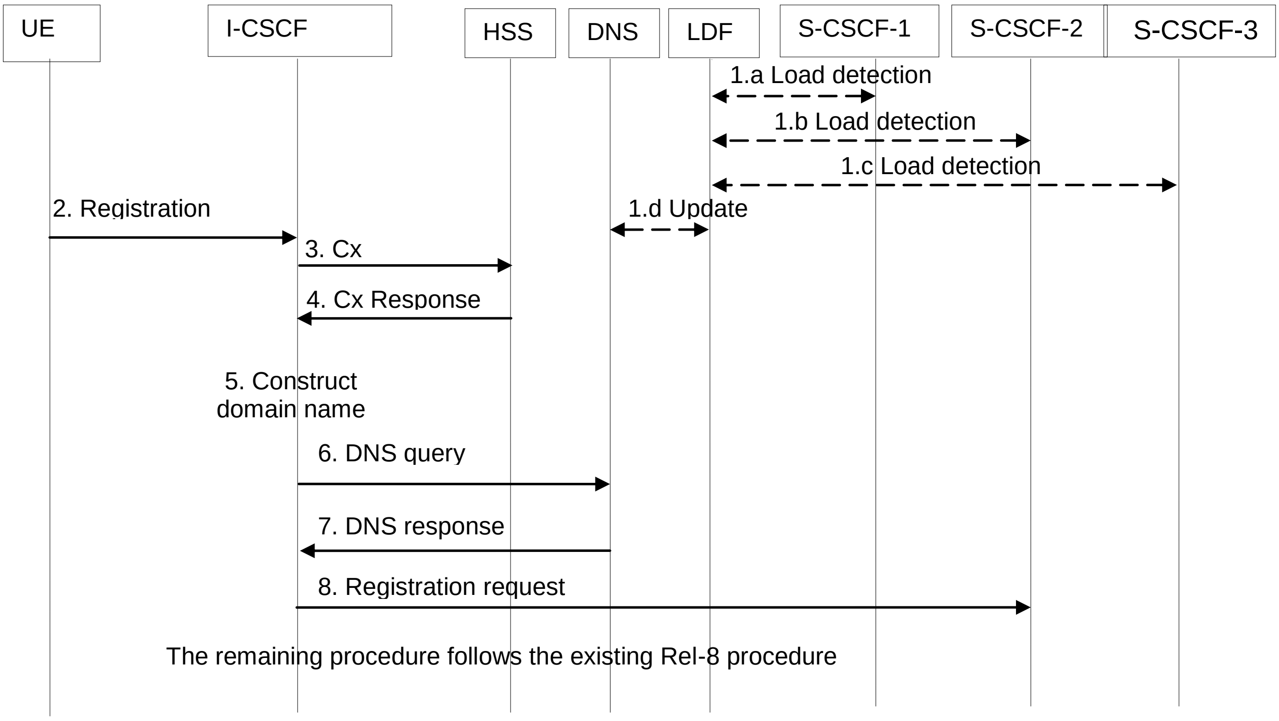


Figure 6.1-6: Information flow for S-CSCF Load Balancing at initial registration

1. The LDF interacts with the S-CSCFs in the same domain to obtain load information of S-CSCFs, and updates the DNS accordingly.. This is achieved either by querying each S-CSCF, or by collecting information reported by the S-CSCFs.

NOTE: For Alternative 2 of LDF architecture, EMS/NMS is used for information delivery between LDF and S-CSCF as well as between LDF and DNS as shown in figure 6.1-2.

2. The I-CSCF receives a IMS registration request from a UE.
3. The I-CSCF sends the Cx query to the HSS to find an appropriate S-CSCF.
4. The I-CSCF receives a Cx response, which contains the server capabilities, from HSS if no S-CSCF is assigned to the user.
5. In the case where Cx response contains server capabilities, the I-CSCF constructs a domain name from these capabilities, using a deterministic algorithm and local configuration.
6. The I-CSCF performs a DNS query to resolve the domain name constructed at step 5 or the S-CSCF address received by the HSS at step 4.

7. The I-CSCF receives a response containing address(es) of preferable S-CSCFs from the LDF.

8. The I-CSCF sends the IMS registration request to the S-CSCF.

6.1.1.4 S-CSCF Load Balancing during re-registration

Figure 6.1-7 shows an information flow where a more preferable S-CSCF is selected during IMS re-registration. LDF is involved to offer load information. It's assumed that S-CSCF re-selection should not impact service continuity. Thus, S-CSCF re-selection only applies to the registered UEs without ongoing services.

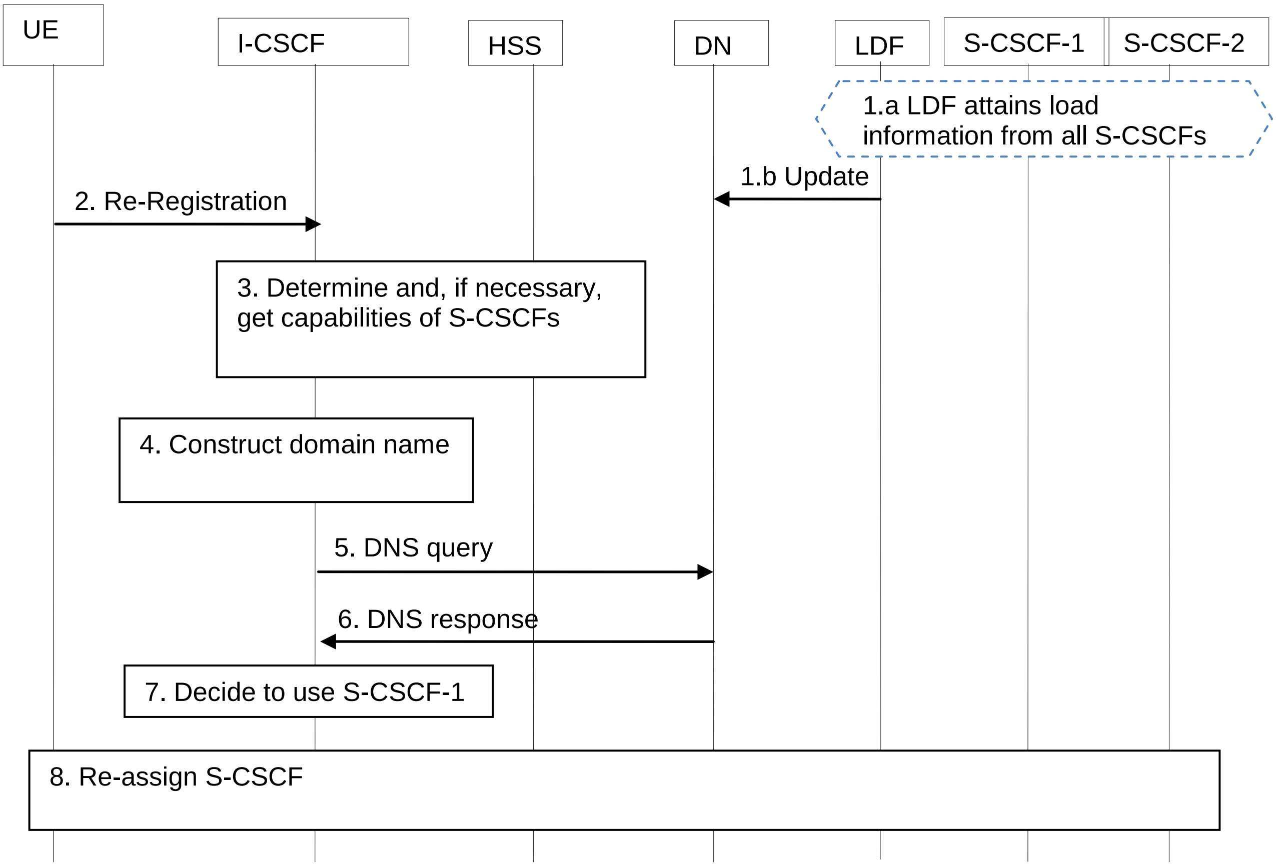

UE
I-CSCF
HSS
DN
LDF
S-CSCF-1
S-CSCF-2
1.a LDF attains load information from all S-CSCFs
1.b Update
2. Re-Registration
3. Determine and, if necessary, get capabilities of S-CSCFs
4. Construct domain name
5. DNS query
6. DNS response
7. Decide to use S-CSCF-1
8. Re-assign S-CSCF

Figure 6.1-7: Information flow for S-CSCF load balancing at re-registration

1. LDF interacts with the S-CSCFs in the same domain to obtain dynamic load information of S-CSCFs, and updates the DNS accordingly.

NOTE: For Alternative 2 of LDF architecture, EMS/NMS is used for information delivery between LDF and S-CSCF as well as between LDF and DNS as shown in figure 6.1-2.

2. I-CSCF receives a IMS re-registration request from UE.

3. I-CSCF determines and, if necessary, gets capabilities of S-CSCFs from HSS using step 2-6 of Detection Mechanism 1 (in clause 6.3.1.2) or step 2-5 of Detection Mechanism 2 (in clause 6.3.1.3).

4. In the case where Cx response contains server capabilities, I-CSCF constructs a domain name from these capabilities, using a deterministic algorithm and local configuration.

5. I-CSCF performs a DNS query to resolve the domain name constructed at step 4 or the S-CSCF address received from the HSS at step 3.

6. I-CSCF receives a response containing address(es) of preferable S-CSCF(s) from DNS.

7. The I-CSCF calculates the best suited S-CSCF based on the received capabilities and load information. If the best suited S-CSCF is the currently assigned S-CSCF (S-CSCF 2) or the best suited S-CSCF is currently not available, existing Rel-8 procedure is followed. Otherwise, go to Step 8.

8. The re-assignment of S-CSCF follows Re-Selection Mechanism 1 (in clause 6.3.2.2) or Re-Selection Mechanism 2 (in clause 6.3.2.3)

6.1.1.5 Load Balancing during S-CSCF restoration

6.1.1.5.1 General

Current solution of S-CSCF system-level restoration proposed by CT4 is based on the reselection of new S-CSCF to take over the load of the failed one. But the solution doesn't consider the dynamic load status of newly selected S-CSCF. Thus, the newly selected S-CSCF may get overloaded or even crashed because of the transferring-in of load from the failed S-CSCF. In order to solve this problem, LDF can be used to select one or more low-load S-CSCF to share the redundant load transferred from the failed S-CSCF.

6.1.1.5.2 Load Balancing during S-CSCF restoration (originating procedure)

When a S-CSCF fails, a backup S-CSCF will take the place of the disabled one during an originating procedure as depicted in TS 23.380. That S-CSCF will download user backup data from HSS that helps continue setting up the session. A LDF based Load Balancing mechanism can be used to improve this procedure.

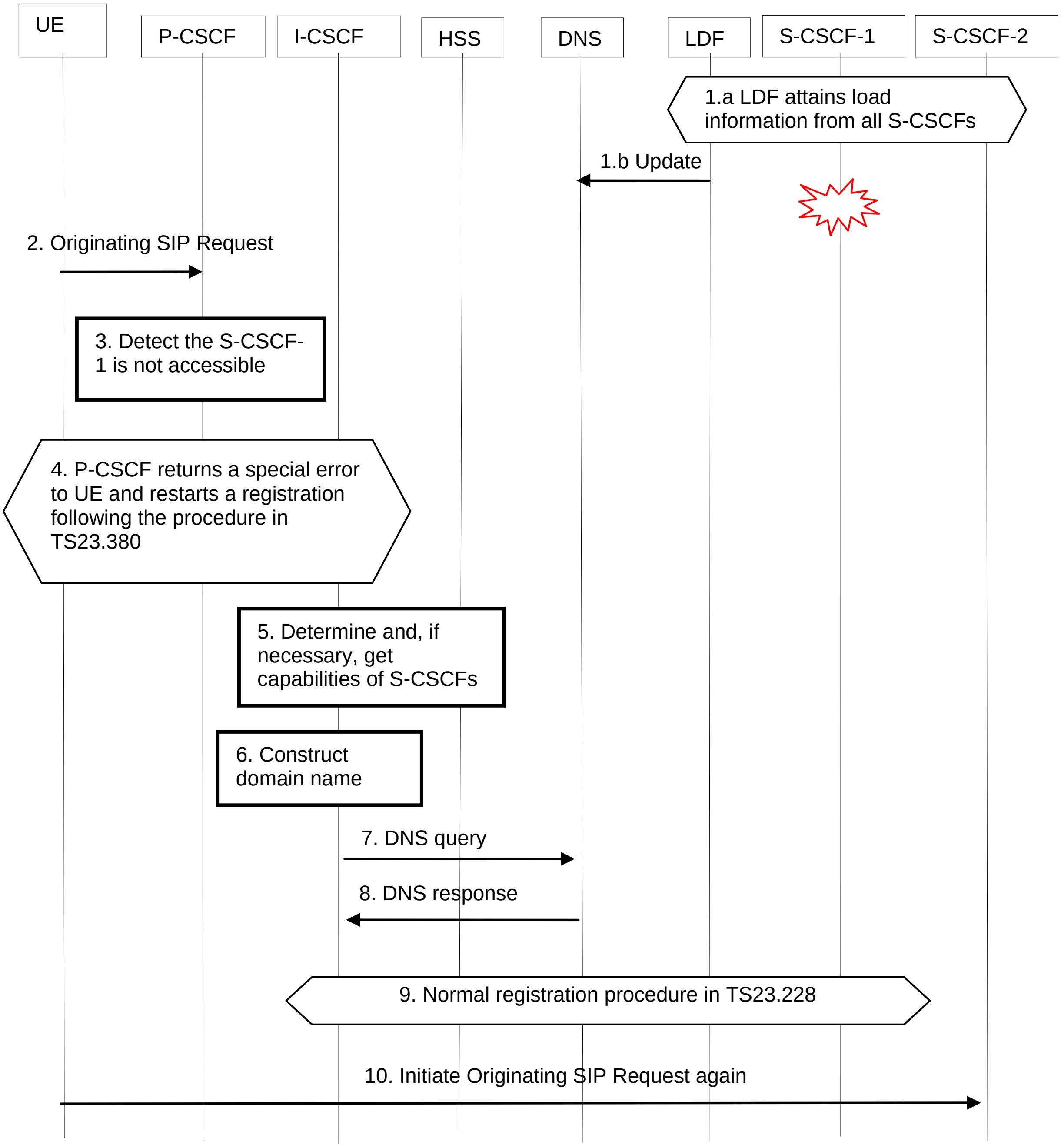

UE
P-CSCF
I-CSCF
HSS
DNS
LDF
S-CSCF-1
S-CSCF-2
1.a LDF attains load information from all S-CSCFs
1.b Update
2. Originating SIP Request
3. Detect the S-CSCF-1 is not accessible
4. P-CSCF returns a special error to UE and restarts a registration following the procedure in TS23.380
5. Determine and, if necessary, get capabilities of S-CSCFs
6. Construct domain name
7. DNS query
8. DNS response
9. Normal registration procedure in TS23.228
10. Initiate Originating SIP Request again

Figure 6.1-8: Information flow for Load Balancing during S-CSCF restoration (originating procedure)

1. LDF interacts with the S-CSCFs in the same domain to obtain dynamic load information of S-CSCFs, and updates the DNS accordingly.

NOTE: For Alternative 2 of LDF architecture, EMS/NMS is used for information delivery between LDF and S-CSCF as well as between LDF and DNS as shown in figure 6.1-2.

2. P-CSCF receives an originating SIP request for a user who has registered on S-CSCF-1.

3. P-CSCF detects S-CSCF-1 is not accessible.

4. P-CSCF returns a special error to UE and restarts a registration following the procedure in TS 23.380.

5. I-CSCF determines and, if necessary, gets capabilities of S-CSCFs from HSS using step 2-6 of Detection Mechanism 1 (in clause 6.3.1.2) or step 2-5 of Detection Mechanism 2 (in clause 6.3.1.3).

6. In the case where Cx response contains server capabilities, I-CSCF constructs a domain name from these capabilities, using a deterministic algorithm and local configuration.

7. I-CSCF performs a DNS query to resolve the domain name fetched at step 4 or constructed at step 5 or the S-CSCF address received from the HSS at step 4.

8. I-CSCF receives a response containing address(es) of preferable S-CSCF(s) from DNS.

9. I-CSCF forwards the message to a selected S-CSCF-2 and the normal registration procedure follows.

10. UE sends the originating SIP Request again.

6.1.1.5.3 Load Balancing during S-CSCF restoration (terminating procedure)

When a S-CSCF fails, a backup S-CSCF will take the place of the disabled one during a terminating procedure as depicted in TS 23.380. That S-CSCF will download user backup data from HSS that helps continue setting up the session. A LDF based Load Balancing mechanism can be used to improve this procedure. This clause describes an alternative that the backup S-CSCF fetches user backup data one at a time when a session setup request comes.

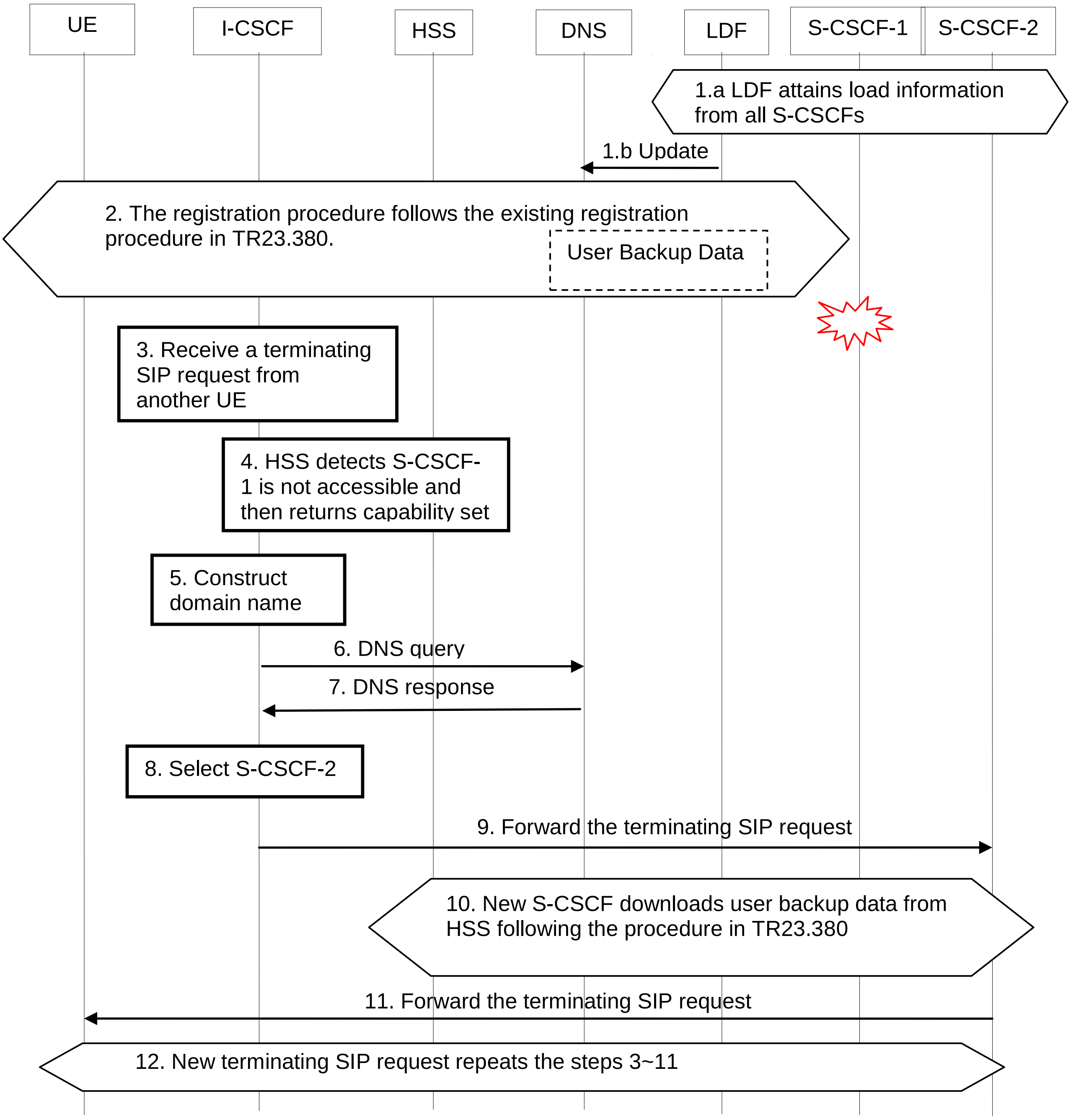

UE
I-CSCF
HSS
DNS
LDF
S-CSCF-1
S-CSCF-2
1.a LDF attains load information from all S-CSCFs
1.b Update
2. The registration procedure follows the existing registration procedure in TR23.380.
User Backup Data
3. Receive a terminating SIP request from another UE
4. HSS detects S-CSCF-1 is not accessible and then returns capability set
5. Construct domain name
6. DNS query
7. DNS response
8. Select S-CSCF-2
9. Forward the terminating SIP request
10. New S-CSCF downloads user backup data from HSS following the procedure in TR23.380
11. Forward the terminating SIP request
12. New terminating SIP request repeats the steps 3~11

Figure 6.1-9: Information flow for Load Balancing during S-CSCF restoration (terminating procedure)

1. LDF interacts with the S-CSCFs in the same domain to obtain dynamic load information of S-CSCFs, and updates the DNS accordingly.

NOTE: For Alternative 2 of LDF architecture, EMS/NMS is used for information delivery between LDF and S-CSCF as well as between LDF and DNS as shown in figure 6.1-2.

2. The registration procedure follows the existing registration procedure where S-CSCF backs up user data in HSS in TS 23.380.

3. I-CSCF receives a terminating SIP request for a user who has registered on S-CSCF-1.

4. I-CSCF sends LIR message to HSS in order to obtain the address of S-CSCF-1. HSS detects S-CSCF-1 is not accessible. I-CSCF receives LIA message, which contains the capability set, from HSS.

5. In the case where Cx response contains server capabilities, I-CSCF constructs a domain name from these capabilities, using a deterministic algorithm and local configuration.

6. I-CSCF performs a DNS query to resolve the domain name fetched at step 4 or constructed at step 5 or the S-CSCF address received from the HSS at step 4.

7. I-CSCF receives a response containing address(es) of preferable S-CSCF(s) from DNS.

8. I-CSCF selects S-CSCF-2 from the returned S-CSCFs.

9. I-CSCF forwards the terminating SIP request to S-CSCF-2.

10. S-CSCF-2 downloads the user backup data from the HSS.

11. S-CSCF-2 forwards the terminating SIP request to UE.

12. If another terminating SIP request comes for another called user, who also used to register on S-CSCF-1, the restoration procedure repeats the steps 3~11.

6.1.2 S-CSCF Load Balancing at Initial Registration based on HSS

This alternative proposes to re-use existing signalling mechanisms, but where the HSS, with its current information and knowledge, selects the appropriate S-CSCF based on different information it has. This information could include:

- Number of current registered user at the S-CSCF
- Type of provisioned services of each of those users
- Number of expected terminals each of those user may have
- Type of user (residential or business)
- Additional policies and information received from support system (which could include current status of the S-CSCFs, such as it is under maintenance and should not be selected etc.).

6.1.3 Load balancing using IETF SOC Overload Control

Some aspects of system load can be planned for or anticipated either because the there is some degree of predictability, or the rate which load is changing across the system is changing in a relatively gradual way. Existing OA&M solutions are able to handle this, but the centralized nature of an OA&M system is likely to limit what is achievable to be in the order of 10 or 15 minutes.

Similarly, it can be expected that any other centralized load balancing solution will have similar limitations. It seems very likely that "real-time" load balancing, where the load through elements in the network might need to change from session to session, will need to occur as a result of information exchanged in the signalling that occurs between elements, and as the result of load balancing decisions that occur in the network elements themselves.

The IETF SOC overload control mechanism described in clause 6.2.4 also has the effect of re-distributing load between network entities. The oc value propagated to upstream servers doesn't directly represent how much a downstream server is loaded, but instead represents how much the traffic to it should be reduced by. Load balancing can be achieved by configuring the thresholds at which different oc values are sent, and by configuring the normal load distribution algorithm in the upstream server.

It is expected that this load balancing mechanism could be used in conjunction with OA&M mechanisms and DNS to provide a system that can handle anticipated or regular load changes across a network as well as rapidly changing local load conditions.

6.1.4 Load Balancing based on dynamic DNS

6.1.4.1 Introduction

This clause describes the use of existing DNS standards in support of load balancing.

Existing DNS standards provide several ways to adjust and exchange load information, including in "near real time".

There are several methods for a centralized DNS server to obtain load information from the CSCFs from different vendors, and make them available as SRV records to the whole (or part of the) IMS network, as described below.

The proposed options have the following characteristics:

- Use DNS SRV records:
  - SRV records provided the list of hosts available to a given destination;
  - SRV records provide the weight information for optimal distribution;
  - Load Balancing is performed by the DNS client, by selecting amongst the SRV records.
- In Method 2 and Method 3 each system has its own Local Zone Domain.
- The weights of the records for each system in DNS are constantly adjusted, based on proprietary implementations of load measurement and reporting in each system.
- If all systems do the same then DNS will implicitly have load information for every host. There is no need then for any new inter-vendor interfaces (and the new development costs and inter-op testing that they would require) since existing DNS and SIP routing standards would be followed.

When the DNS load distribution scheme as proposed above is applied, the load information from any destination is always available to any other system, just by using the existing DNS mechanism. Therefore, it is always possible to calculate an optimal distribution from anywhere over multiple "multi-vendors" destinations, providing that the meaning of the weights is understood.

Editor's note: Investigation is required regarding whether there are issues of stability in this system wide control system.

6.1.4.2 Method 1 Dynamic DNS

A centralized DNS may be updated by each of the IMS network elements using a standard DNS mechanism such as Dynamic DNS (RFC 2136 [5]).

This solution requires some network domain naming coordination, but does not involve any new protocol. Each network entity must implement RCF 2136 [5] to provide weight updates to the centralized DNS.

Alternatively, multiple network entities from the same vendor could provide a common DNS agent in order to update the centralized "inter-vendor" DNS server using RFC 2136 [5]. This means that the way the DNS agent is fed with the weights from its own network entities can be proprietary.

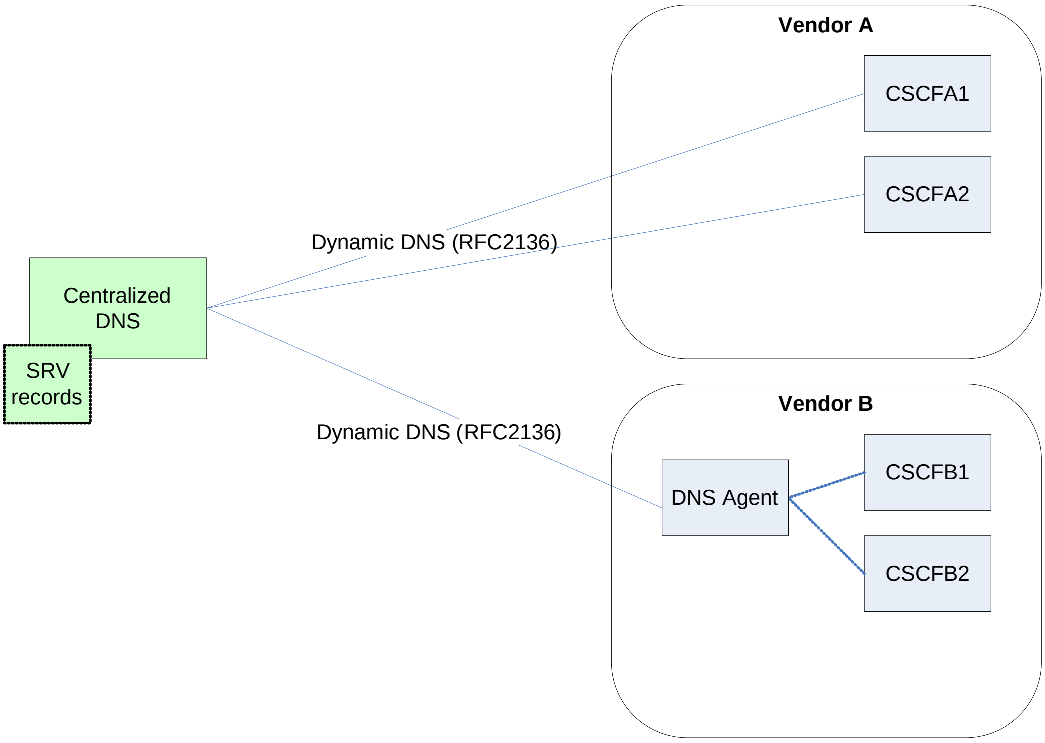


Figure 6.1.4.2-1: Dynamic DNS method

6.1.4.3 Method 2: Zone transfer

A centralized DNS may be updated by each IMS network elements using zone transfers and incremental zone transfer (RFC 1034 [6] and RFC 1995 [10] respectively).

This solution does not involve any new protocol, but does require that network elements define their own local zone domain and implement their own local DNS as the authoritative DNS of this local zone.

Alternatively, multiple network elements from the same vendor could define a common local zone domain and provide a common DNS authoritative domain server in order to update the centralized "inter-vendor" DNS server using RFC 1034 [6] and RFC 1995 [10]. This means that the way the DNS authoritative domain server is fed with the weights from its own network elements can be proprietary.

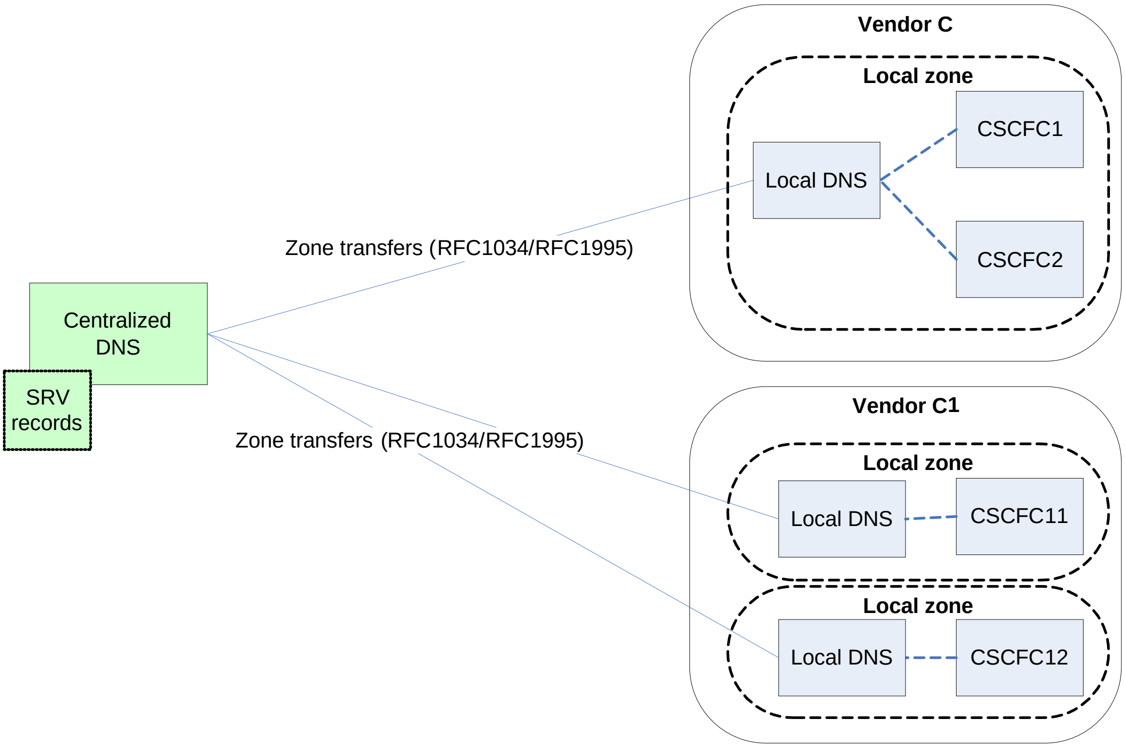


Figure 6.1.4.3-1: Zone transfer method

6.1.4.4 Method 3: SRV DNS resolution requests

A centralized DNS may simply update the weights by sending SRV DNS resolution requests to each IMS Network Elements for which it needs to provide a common consolidated domain.

This solution does not involve any new protocol, but does require that each network element defines its own local zone domain and implements its own local DNS as the authoritative DNS of this local zone. This option is the safest and easiest to set up, since the centralized DNS does not need to authorize network elements to access and change it.

It is also possible that multiple network elements from the same vendor define a common local zone domain and provide a common DNS authoritative domain server in order to resolve SRV records requests from the centralized "inter-vendor" DNS server. Similarly, the way by which the DNS authoritative domain server is fed with the weights from its own network elements may be proprietary

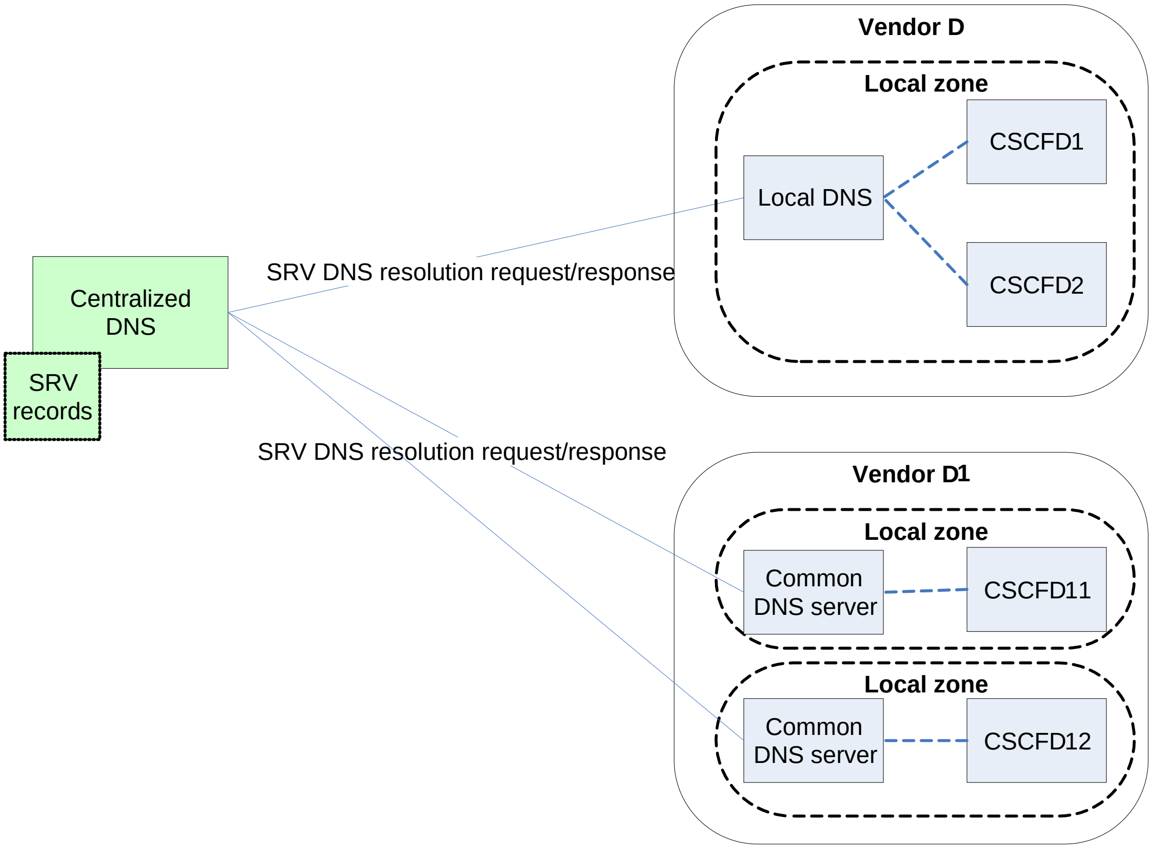


Figure 6.1.4.4-1: SRV DNS resolution requests method

6.1.5 Registration independent Serving Node Load Balancing based on HSS

6.1.5.1 General

Load Balancing of a Serving Node (i.e. S-CSCF or Transit Function) can be obtained in a registration independent way by having the entry point of a network (e.g. I-CSCF, IBCF, or P-CSCF) make a Location Info Request to an HSS. The HSS will respond with an optimal Serving Node in the Location Info Response based on a selection policy functionality operating in the HSS. The selection policy function may make use of load information provided to the HSS, either directly or via an intermediate load information function (where the load information function collects information about load on a regular basis). The selection policy function may also make use of other information, e.g. about planned maintenance of a Serving Node, about Serving Node capabilities, and/or customer based policies.

For an I-CSCF used as entry point this can schematically be depicted as indicated in Figure 6.1.5.1-1. In this diagram the HSS is making use of a Selection Policy Function (SPF) which gets its information from a Load Information Function (LIF) and other sources.

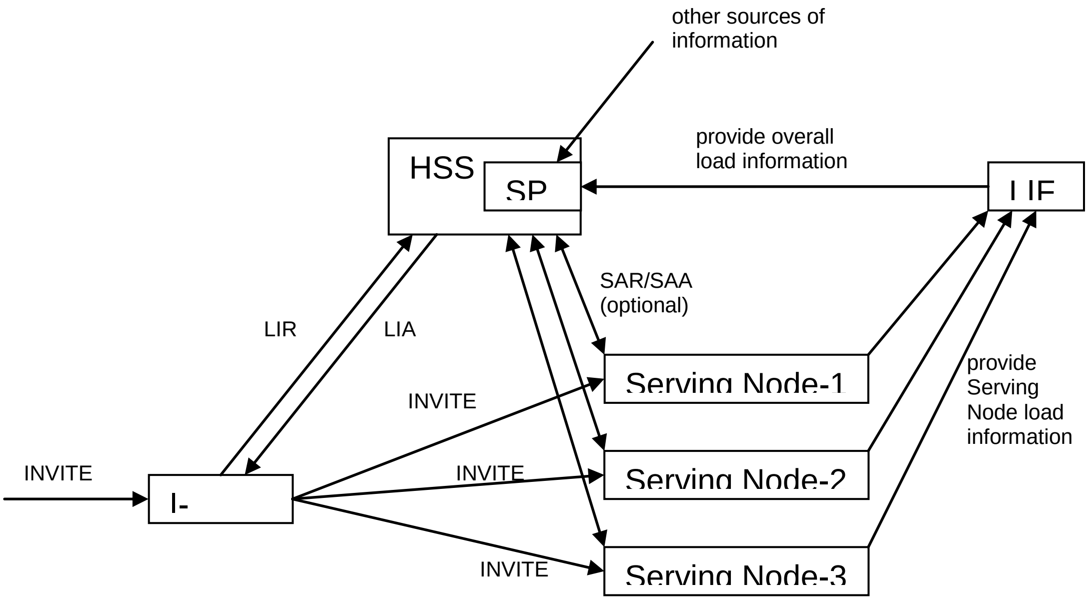


Figure 6.1.5.1-1: Registration independent Serving Node Load Balancing

NOTE: Alternative implementations are possible. The SPF may be implemented as a standalone entity not integrated with the HSS. The combination of SPF and LIF provide similar functionality to an LDF.

6.1.5.2 Information flow for registration independent Serving Node Load Balancing by I-CSCF

Fig 6.1.5.2-1 shows an information flow where an INVITE message is handled by an I-CSCF and Serving Node Load Balancing is performed by a query to the HSS from this I-CSCF.

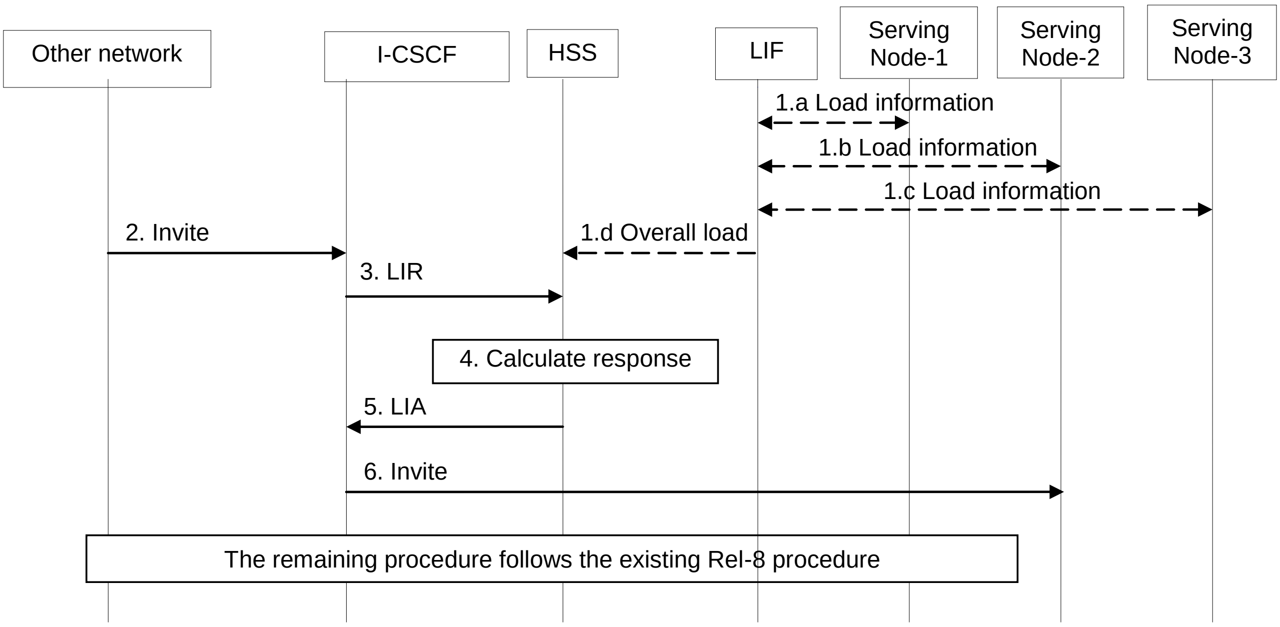


Figure 6.1.5.2-1: Information flow for registration independent Serving Node Load Balancing by I-CSCF

1. LIF interacts with the Serving Nodes in the same domain (1a, 1b, 1c) to obtain dynamic load information of Serving Nodes, and informs the HSS accordingly (1d).

2. I-CSCF receives an invite request from another network.

3. I-CSCF issues a standard Location Info Request to the HSS in order to obtain a Serving Node identity for further handling of the invite request.

4. HSS executes internal selection policy function based on information provided to the HSS and internal logic.

5. I-CSCF receives a Location Info Answer from the HSS indicating a specific Serving Node address (Serving Node-2 in this case).

6. I-CSCF sends the invite request to the Serving Node address received.

6.2 Architecture alternatives for Overload Control

6.2.1 P-CSCF Overload Control

6.2.1.1 P-CSCF redirects to another P-CSCF

6.2.1.1.1 Description

If overload conditions are detected in P-CSCF it may redirect a UE (which is trying to perform IMS Registration) to another P-CSCF. Such a network based redirect facilitation will aid the UE in finding another P- CSCF in a more deterministic fashion.

6.2.1.1.2 Information flow

Fig 6.2-1 shows an information flow where a UE is redirected to another P-CSCF during IMS registration.

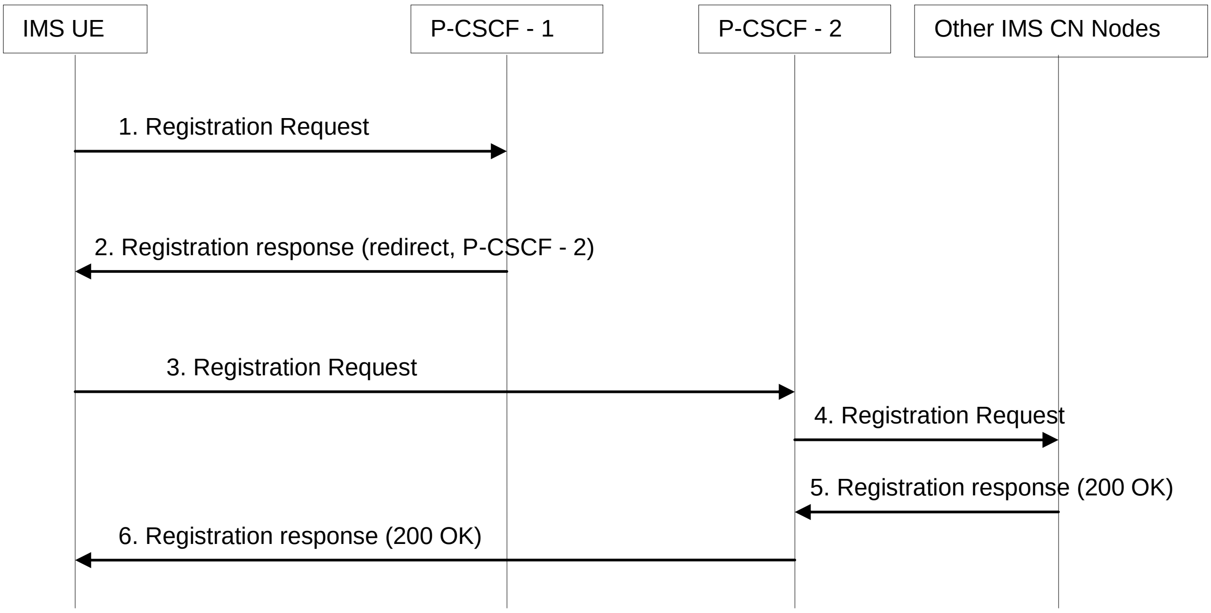

IMS UE
P-CSCF - 1
P-CSCF - 2
Other IMS CN Nodes
1. Registration Request
2. Registration response (redirect, P-CSCF - 2)
3. Registration Request
4. Registration Request
5. Registration response (200 OK)
6. Registration response (200 OK)

Figure 6.2-1: Information flow for IMS Registration redirection

1. UE sends a IMS Registration request to P-CSCF -1 that is experiencing overload condition.

2. P-CSCF - 1 sends a Registration redirection response with a redirect address of P-CSCF - 2.

NOTE: The P-CSCF-2 can be configured in P-CSCF-1.

3. UE sends IMS registration request to P-CSCF-2..

4. P-CSCF-2 forwards the registration requests to IMS CN for further processing.

5. P-CSCF-2 receives successful registration response.

6. P-CSCF-2 sends successful IMS registration response to the UE.

6.2.1.1.3 Co-existence with earlier releases

Editor's note: This section will analyze how the new solution will impact on IMS network. (e.g. how to interwork and get compatible with IMS earlier releases).

6.2.1.2 Using DNS to select another P-CSCF

6.2.1.2.1 Description

This alternative relies on existing mechanisms to re-select another P-CSCF, when the P-CSCF to which a UE has requested a registration, is overloaded.

6.2.1.2.2 Information flow

Figure 6.2-2 shows an information flow where a UE attempts registration with a P-CSCF, which rejects the registration because of overload, and the UE subsequently performs a DNS query to obtain the address of another P-CSCF.

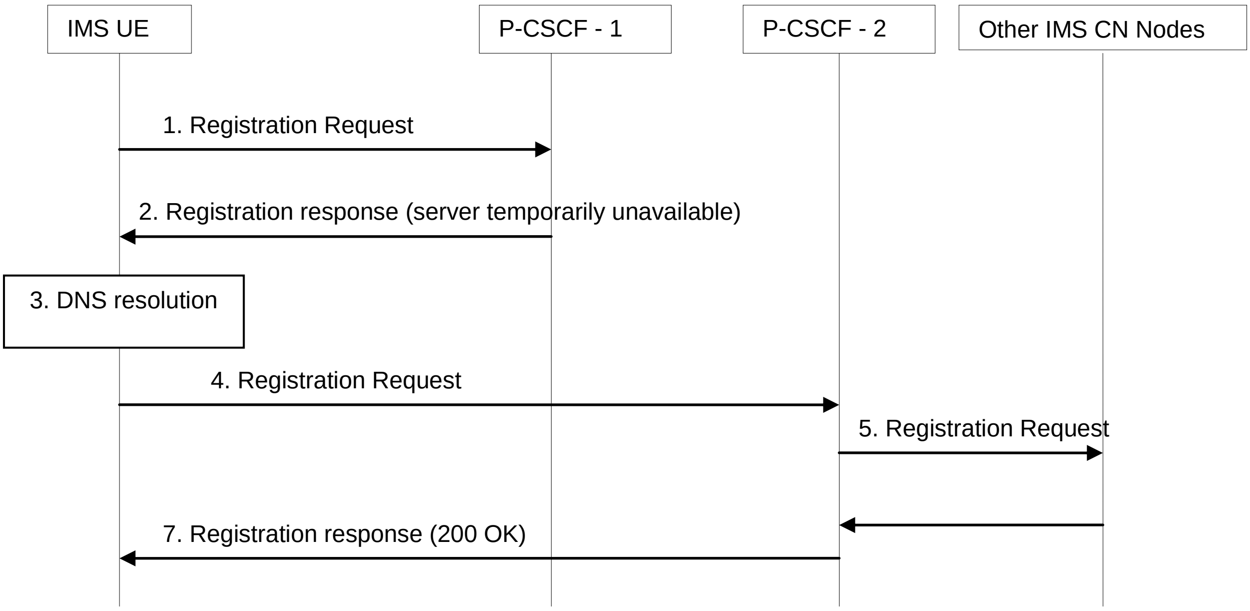


Figure 6.2-2: Information flow for IMS Registration redirection

1. UE sends a IMS Registration request to P-CSCF -1 that is experiencing overload condition.
2. P-CSCF-1 sends a Registration response indicating that it is temporarily unavailable.
3. UE performs a DNS resolution and selects another P-CSCF.

NOTE: P-CSCF Load Balancing as described in clause 6.1.1.2 may be used to select a relatively low-loaded P-CSCF.

4. UE sends IMS registration request to P-CSCF-2.
5. P-CSCF-2 forwards the registration requests to IMS CN for further processing.
6. P-CSCF-2 receives successful registration response.
7. P-CSCF-2 sends successful IMS registration response to the UE.

6.2.1.3 P-CSCF Overload Control based on LDF

6.2.1.3.1 General

In order to achieve Overload Control between P-CSCFs, the Load Detection Function (LDF) is utilized to monitor and store the load information of all P-CSCFs.

The P-CSCF Overload Control mechanisms implemented by the LDF are:

- Monitor and store the load information of P-CSCFs. This is achieved either by querying each P-CSCF, or by collecting information reported by the P-CSCFs.

- Provide a P-CSCF with the address of a low-load P-CSCF to redirect initial registration.

6.2.1.3.2 Information flow

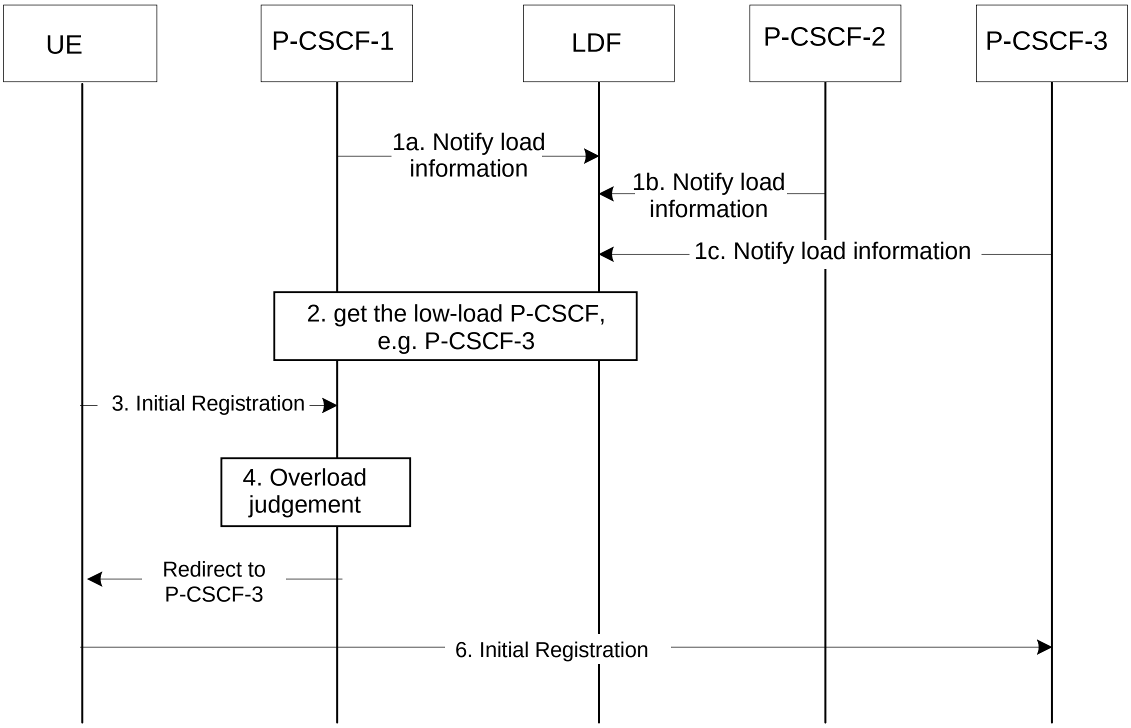

UE
P-CSCF-1
LDF
P-CSCF-2
P-CSCF-3
1a. Notify load information
1b. Notify load information
1c. Notify load information
2. get the low-load P-CSCF, e.g. P-CSCF-3
3. Initial Registration
4. Overload judgement
Redirect to P-CSCF-3
6. Initial Registration

Figure 6.2-3: Information flow for P-CSCF Overload Control

1. P-CSCF-1, P-CSCF-2 and P-CSCF-3 notify the load information to LDF(e.g. periodically).

NOTE: For Alternative 2 of LDF architecture, EMS/NMS is used for information delivery between LDF and P-CSCF as shown in figure 6.1-2.

2. P-CSCF-1 gets the low-load P-CSCF address, eg. P-CSCF-3.

3. P-CSCF-1 receives the initial registration of UE.

4. P-CSCF-1 finds that it is in overload condition.

5. P-CSCF-1 sends a Registration redirection response with a redirect address of P-CSCF-3.

6. UE sends IMS registration request to P-CSCF-3.

6.2.1.4 UE selects another P-CSCF upon negative response from P-CSCF

6.2.1.4.1 General

This alternative relies on existing 24.229 procedures in order to handle overload situations during initial registration and suggests reusing those mechanisms for the re-registration scenario.

6.2.1.4.2 During Initial Registration Procedure

Figure 6.2.1.4.2-1 shows an information flow where a UE attempts registration with a P-CSCF, which rejects the registration because of overload, and the UE subsequently selects another P-CSCF. The whole procedure is already defined in TS 24.229.

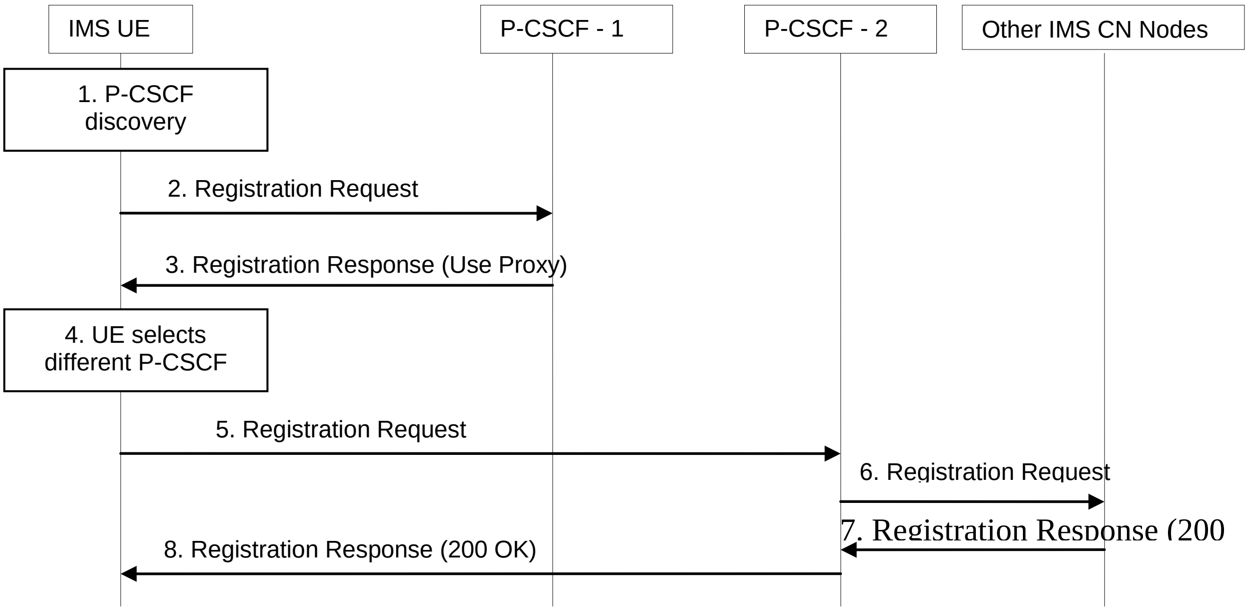


Figure 6.2.1.4.2-1: UE selects another P-CSCF during initial registration

1. UE performs P-CSCF discovery as defined in TS 24.229.

2. UE sends a registration request to P-CSCF -1 that is experiencing overload condition.

3. P-CSCF-1 sends a registration response indicating to select a different P-CSCF.

4. UE selects a P-CSCF address, which is different from the previously used address.

5. UE sends IMS registration request to P-CSCF-2.

6. P-CSCF-2 forwards the registration requests to IMS CN for further processing.

7. P-CSCF-2 receives successful registration response.

8. P-CSCF-2 sends successful IMS registration response to the UE.

6.2.1.4.3 During Re-Registration Procedure

Figure 6.2.1.4.3-1 shows an information flow where a UE attempts re-registration with a P-CSCF, which rejects the registration because of overload, and the UE subsequently performs P-CSCF discovery and selects a different P-CSCF previously used.

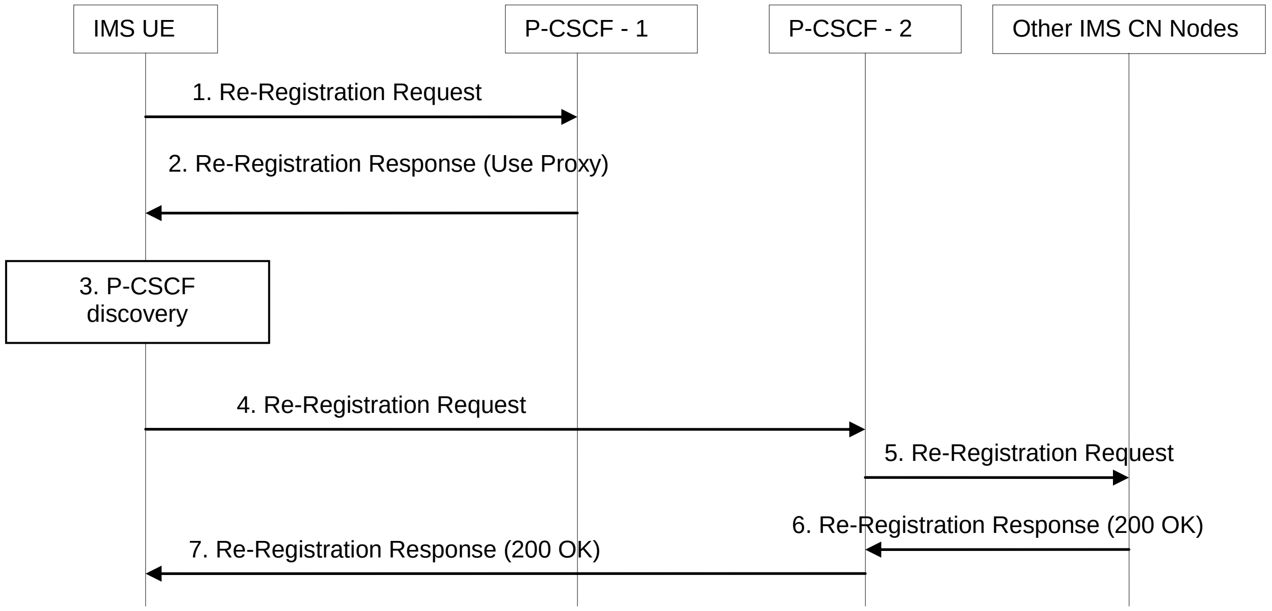

IMS UE
P-CSCF - 1
P-CSCF - 2
Other IMS CN Nodes
1. Re-Registration Request
2. Re-Registration Response (Use Proxy)
3. P-CSCF discovery
4. Re-Registration Request
5. Re-Registration Request
6. Re-Registration Response (200 OK)
7. Re-Registration Response (200 OK)

Figure 6.2.1.4.3-1: UE selects another P-CSCF during re-registration

1. UE sends a re-registration request to P-CSCF -1 that is experiencing overload condition.
2. P-CSCF-1 sends a re-registration response indicating to select a different P-CSCF.
3. UE performs P-CSCF discovery procedure as described in 24.229 and selects a P-CSCF address, which is different from the previously used address.
4. UE sends IMS re-registration request to P-CSCF-2.
5. P-CSCF-2 forwards the re-registration requests to IMS CN for further processing.
6. P-CSCF-2 receives successful re-registration response.
7. P-CSCF-2 sends successful IMS re-registration response to the UE.

6.2.2 S-CSCF Overload Control

6.2.2.1 S-CSCF Overload Control based on LDF

6.2.2.1.1 General

The load information of S-CSCFs is beneficial to improve Overload Control. If the load state of S-CSCFs is considered when selecting an S-CSCF during the initial registration, load imbalance amongst S-CSCFs due to the overload of an S-CSCF might be alleviated to some extent and S-CSCFs might be utilized more efficiently. The LDF (Load Detection Function) could be introduced to help implement S-CSCF Overload Control for certain scenarios.

The observations in clause 6.1.1.3 are also applicable to Overload Control.

6.2.2.1.2 Information flow

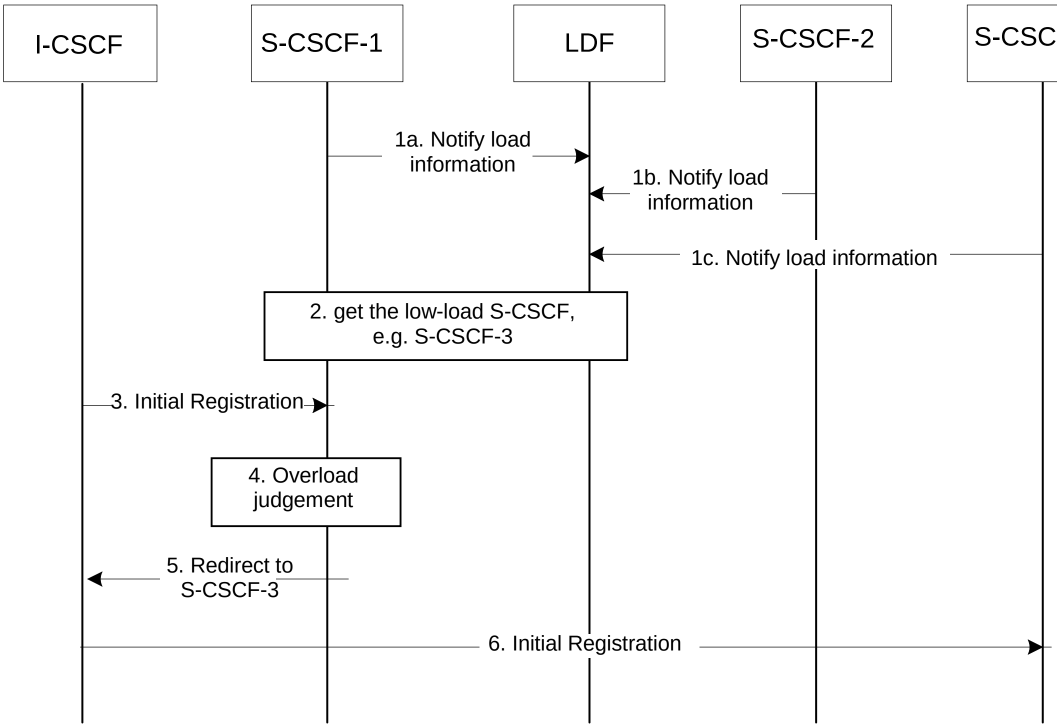


Figure 6.2-6: Information flow for S-CSCF Overload Load at initial registration

1. The LDF interacts with the S-CSCFs in the same domain to obtain load information of S-CSCFs. This is achieved either by querying each S-CSCF, or by collecting information reported by the S-CSCFs.

NOTE: For Alternative 2 of LDF architecture, EMS/NMS is used for information delivery between LDF and S-CSCF as shown in figure 6.1-2.

2. S-CSCF-1 gets a low-load S-CSCF address, eg. S-CSCF-3.

3. The I-CSCF sends the IMS initial registration request to the selected S-CSCF, i.e. S-CSCF-1.

4. S-CSCF-1 finds that it is in overload condition.

Editor's note: It is FFS whether S-CSCF or I-CSCF should perform the Overload Control.

5. S-CSCF-1 sends a Registration redirection response to I-CSCF with a redirect address of S-CSCF-3.

6. The I-CSCF sends the IMS initial registration request to S-CSCF-3.

6.2.3 Overload Control based on GOCAP

6.2.3.1 Overview

GOCAP (Generic Overload Control Application Protocol) is a protocol standardised by ETSI in ES 283 034-2 [5]. Its purpose is to provide a general mechanism for protecting hosts and servers (e.g. SIP Servers) in Next Generation Networks against processing overload. This protocol enables a host to protect itself from overload by sending to traffic sources load control filters known as "restrictions". GOCAP assumes a rate-based model, more specifically a leaky bucket model. GOCAP does not place any restrictions on the type of traffic to be restricted. A profile specification is required to make it applicable to a particular type of traffic.

A GOCAP Master is a host that uses GOCAP to protect itself from overload by sending restrictions to traffic sources known as GOCAP slaves. An XML document is exchanged between the master and the slaves to create, update or delete restrictions. GOCAP Masters and Slaves do not need to be adjacent. A GOCAP Master can send preventive restrictions to GOCAP Slaves that do not send any traffic as long as they are known to be potential traffic sources.

The GOCAP specification does not place any restriction on the protocol used to carry XML documents. However, the current version of this specification provides mapping to both Diameter and SIP. The SIP solution is primarily - but not exclusively - intended for use between entities that are already supporting the SIP protocol for other purposes (e.g. SIP Application Servers). However, GOCAP does not prevent using Diameter as means to convey overload control information between two SIP servers. In all cases the structure of the XML document is governed by the same XML schema.

When Diameter is used, GOCAP slaves act as Diameter servers in the sense that they handle restriction requests. A GOCAP Master acts as a Diameter client in the sense that it is the element requesting restrictions to be instantiated. The XML document is included in the GOCAP-Body AVP of the Profile-Update-Request Diameter command.

When SIP is used, GOCAP slaves subscribe to a specific SIP event (congestion_control) with GOCAP Masters. Restriction information is sent from the GOCAP Master to the GOCAP slaves using NOTIFY requests embedding an XML document as a message body.

A Restriction includes a list of flow descriptions, a duration and a leak rate. Flow descriptions characterize the type of traffic to be restricted. A flow description includes a destination application layer address (which may be a Telephone Number or a URI, possibly Wildcarded) and one or more application labels. The specification of application labels is outside the scope of the GOCAP specification and needs to be further specified in application documents.

6.2.3.2 Applicability to the IMS

GOCAP could be used to protect any SIP and Diameter servers in the IMS. This would require specifying a GOCAP profile for filtering SIP and Diameter traffic. Application labels would typically have to be defined to represent particular SIP messages (e.g. SIP.INVITE) to be filtered or particular Diameter messages to be filtered (e.g. Diameter.AAR).

The following IMS entities could play the role of a GOCAP Master:

- An Application Server, in which case the role of the GOCAP Slave would be played by the S-CSCFs;
- An S-CSCF, in which case the role of the GOCAP Slave would be played by the P-CSCFs, I-CSCFs, the IBCFs, the MGCFs, some AS;
- An IBCF, in which case the role of the GOCAP Slave would be played by the S-CSCFs, the I-CSCFS, other IBCFs, the MGCFs, some AS;
- An HSS, in which case the role of the GOCAP Slave would be played by the I/S-CSCFs and some AS.

Identified issues of the solution:

- It would not be appropriate for a collection of UE instances to play the role of a GOCAP Slaves, as the GOCAP Master (P-CSCF) would have to spend a significant amount of its processing resources to send restrictions to all registered UEs while each of them would account for a small amount of traffic. Complex UE playing the role of an externally attached network and generating a large amount of traffic might be an exception.
- GOCAP relies on a non-IANA registered event package.

Identified benefits of the solution:

- This mechanism provides the functionality required to control overload of SIP servers in IMS.

6.2.4 Overload Control based on IETF SOC WG solution as described in draft-ietf-soc-overload-control-01

6.2.4.1 General

In IETF, work on SIP overload control has been moved from SIPPING to SOC (SIP Overload Control) WG. The former Hilt Overload ID has been split into:

- draft-ietf-soc-overload-design, describing basic principles of overload control (IETF status: working group draft)
- draft-ietf-soc-overload-control-01 [6], describing a protocol solution (IETF status: working group draft)

A SIP server, e.g. I-CSCF, that supports this functionality adds an "oc" parameter to the Via headers it inserts into SIP requests. This provides an indication to its neighbours that it supports overload control.

A SIP server, e.g. S-CSCF, can provide overload control feedback to its neighbours by providing a value for the "oc" parameter to the topmost Via header field of a SIP response. The topmost Via header is determined after the SIP server has removed its own Via header.

Since the topmost Via header of a response will be removed by the neighbour after processing it, overload control feedback contained in the "oc" parameter will not travel beyond a SIP entity. A Via header parameter therefore provides hop-by-hop semantics for overload control feedback even if the next hop neighbour does not support overload control.

The "oc" parameter can be used in all response types including provisional, success and failure responses. A SIP server may update the "oc" parameter to all responses it is sending.

The "oc" parameter value specifies the percentage by which the load forwarded to this SIP server should be reduced. Possible values range from 0 (the traffic forwarded is reduced by 0%, i.e., all traffic is forwarded) to 100 (the traffic forwarded is reduced by 100%, i.e., no traffic is forwarded). The default value of this parameter is 0.

Policies based on the content of the Resource-Priority header or other indicators, such as the SOS URN, allow emergency requests to be forwarded despite of an overload condition.

6.2.4.2 Applicability to the IMS

Identified issues of the solution:

- This mechanism is applicable to IMS SIP servers only.
- This mechanism is not well suited for certain types of application servers hosting multiple applications or applications where overload conditions can be created by calls with specific properties. For example, an Application Server hosting a 800 application overloaded by mass calling to a particular destination (e.g. people call a particular number to vote during a TV show) would return a loss rate to all CSCFs, which would apply it to all 800 calls regardless of the called number.
- Because this mechanism works hop-by-hop, it is not suitable in configurations where a B2BUA that is not overload control aware is on the signalling path between the overloaded server and the actual traffic sources (e.g. an AS acting as a B2BUA between the S-CSCF and another AS).

It would be inefficient to rely on this mechanism to prevent P-CSCF overload, except for the case of complex UE playing the role of an externally attached network and generating a large amount of traffic.

Identified benefits of the solution:

- This mechanism is well suited for preventing overload of core network servers (CSCF) where overload is not due to calls to a specific application/destination.

6.2.4.3 Example Information flow

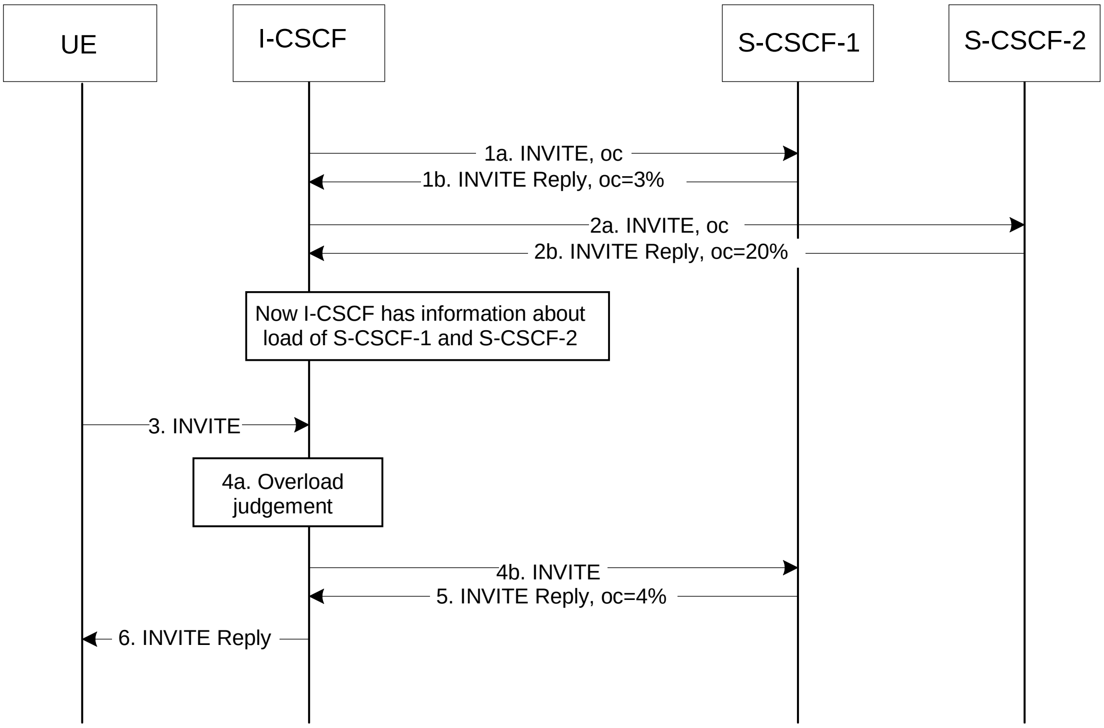


Figure 6.2.4.3-1: Information flow for S-CSCF Overload Control according to draft-ietf-soc-overload-control

1. During a past INVITE, the I-CSCF get feedback about the load situation of S-CSCF-1.

2. During a past INVITE, the I-CSCF get feedback about the load situation of S-CSCF-2.

3. Incoming INVITE from UE.

4. With these information, the I-CSCF can either:

    a. Forward the INVITE either to S-CSCF-1 or S-CSCF-2, or

    b. Refuse the INVITE request because of overload situation.

5. The Reply to the INVITE can contain an updated "oc" value.

6. INVITE Reply is sent to UE.

6.2.5 Overload Control based on IETF SOC WG solution as described in draft-ietf-soc-load-control-event-package

6.2.5.1 General

In IETF, work on SIP overload control has been moved from SIPPING to SOC (SIP Overload Control) WG. The new name for this ID is therefore draft-ietf-soc-load-control-event-package [7] (IETF status: working group draft).

As shown in figure 6.2.5.2-1 the proposed mechanism is built upon the existing SIP event framework. Traffic sources act as SIP event subscribers and hosts protecting themselves from overload are acting as SIP event notifiers. They do not need to be adjacent. For example the I-CSCF subscribes to a load control event package and receives filters and thresholds from the S-CSCF depending on load conditions. A host can send preventive restrictions to potential sources that do not send any traffic as long as they are known to be potential traffic sources.

This mechanism is based on load filters. A load filter contain:

- filter conditions, including the type of SIP request (e.g. INVITE) to which the filter applies, calling and called identities (possibly wildcarded) the period of time during which the control should be activated;
- an action, specified using one of the the following elements depending on the overlaod control model used:
  - *rate-based model*: the <rate> element denotes an absolute value of the maximum acceptable request rate in requests per second;
  - *loss-based model*: the <percent> element specifies the relative percentage of incoming requests that should be accepted;
  - *windows-based model*: the <win> element describes the acceptable window size supplied by the receiver, which is applicable in window-based load control.
- optionally, an explicit indication of the desired action in case a request cannot be accepted:
  - "drop" for simple drop, or
  - "reject" for explicit rejection (e.g., sending a "500 Server Internal Error" response message to an INVITE request), or
  - "forward" to an alternate destination (e.g., an answering machine with explanation of why the request cannot be accepted).

Policies based on the content of the Resource-Priority header or other indicators, such as the SOS URN, allow emergency requests to be forwarded despite of an overload condition.

6.2.5.2 Applicability to the IMS

This mechanism would be applicable to IMS SIP servers only. Whether extensions to filter conditions (e.g. IFC-like) would be required need to be evaluated.

The following IMS entities could play the role of a SIP Notifier

- An Application Server, in which case the role of the traffic source would be played by the S-CSCFs;
- An S-CSCF, in which case the role of the traffic source would be played by the P-CSCFs, I-CSCFs, the IBCFs, the MGCFs, some AS;
- An IBCF, in which case the role of the traffic source would be played by the S-CSCFs, the I-CSCFS, other IBCFs, the MGCFs, some AS;

Identified issues of the solution:

As for GOCAP, it would not be appropriate to protect the P-CSCF from overload by the UEs, as the P-CSCF would have to spend a significant amount of its processing resources to send restrictions to all registered UEs while each of them would account for a small amount of traffic. Complex UE playing the role of an externally attached network and generating a large amount of traffic might be an exception.

Identified benefits of the solution:

- This mechanism provides the functionality required to control overload of SIP servers in IMS.
- This mechanism is well suited for application servers when the source of overload is due to calls to a specific destination (e.g. a 800 application overloaded by mass calling to a particular destination) or specific message types (e.g. MESSAGE). It can however be used in other cases as well by using empty (unconditional) filters.

6.2.5.3 Example Information flow

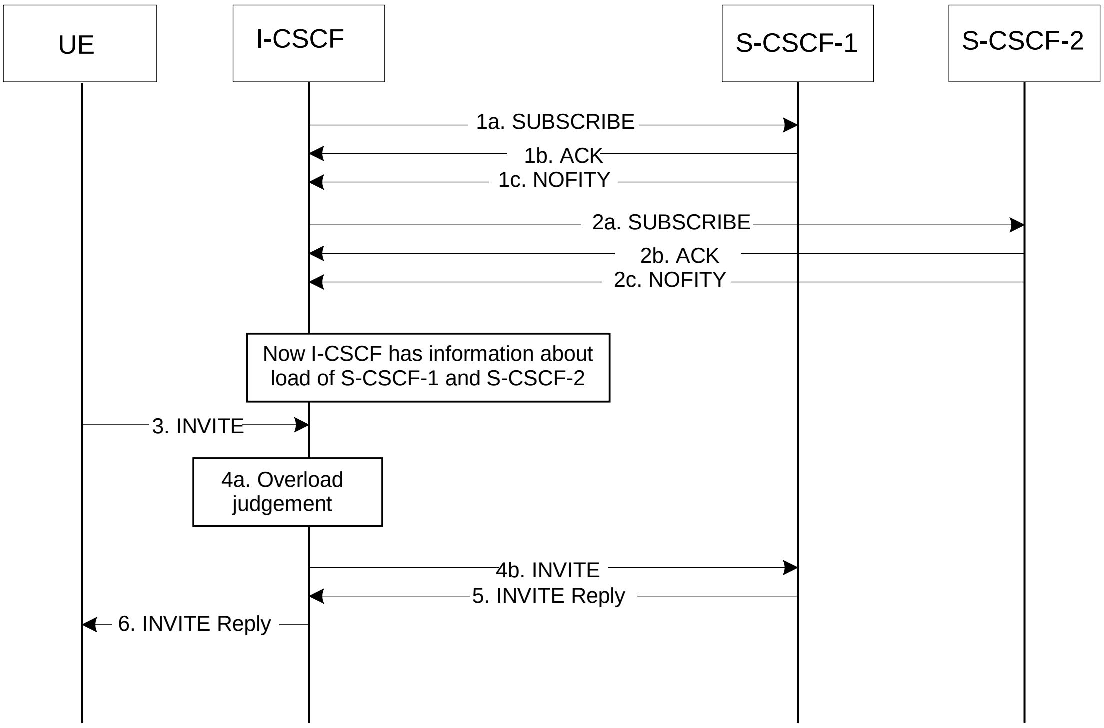


Figure 6.2.5.3-1: Information flow for S-CSCF Overload Control according to draft-ietf-soc-load-control-event-package

1. I-CSCF SUBSCRIBE to overload event notification of S-CSCF-1.

2. I-CSCF SUBSCRIBE to overload event notification of S-CSCF-2.

3. A User INVITE comes to I-CSCF.

4. The I-CSCF has actual information about the overload in S-CSCF-1 and -2 and can:

   a. Refuse the INVITE request because of overload situation, or

   b. Forward the INVITE either to S-CSCF-1 or S-CSCF-2.

5. INVITE Reply is sent to I-CSCF.

6. INVITE Reply is sent to UE.

6.2.6 High Level Summary

The following table provides a high level summary of the key properties of the overload control mechanisms described in clause 6.2.3, 6.2.4 and 6.2.5.

Table 6.2.1-1

	GOCAP	draft-ietf-soc-overload-control	draft-ietf-soc-load-control-event-package
Applicability	Any type of traffic	SIP traffic	¨SIP traffic
Restriction Type	Filter-based restrictions	Global Restrictions	Filter-based restrictions or global restrictions
Mode of operation	Traffic Independent	Feedback	Traffic Independent
Model	Rate-based (leaky bucket)	Loss-based	Rate-based (call gap) Loss-based Windows-based
Transport	XML embedded in SIP NOTIFY request or Diameter PUR command	Parameters in the Via header field of SIP responses	XML embedded in SIP NOTIFY request

6.3 S-CSCF re-selection

6.3.1 Architectural alternatives to detect whether S-CSCF re-selection may be desired

6.3.1.1 General

This clause describes mechanisms aiming to detect whether a UE is registered with a sub-optimal S-CSCF due to the fact that the most preferred S-CSCF was not available (or highly loaded) during registration and a more optimal S-CSCF becomes available.

The detection mechanisms do not support a check on whether there are any on-going dialogs for the subscription, which should not be released by triggering S-CSCF re-selection. However, this check may be done as part of the re-selection mechanism as described in clause 6.3.2.

NOTE: Clause 6.3.1 does not discuss the mechanisms for how the I-CSCF obtains information (load or availability) from the S-CSCFs to make the decision on re-selection.

6.3.1.2 Detection mechanism 1

6.3.1.2.1 Architectural details

This architectural alternative adds additional functionality and signalling load compared to Rel-8 to the I-CSCF. Message contents of SIP or Cx messages are not modified.

At UE re-registration, when the I-CSCF receives the currently assigned S-CSCF name within Cx-UAA, it may decide to check whether the currently assigned S-CSCF is the most preferred S-CSCF for the UE based on capabilities. If so, the I-CSCF sends another Cx-UAR command to the HSS, explicitly requesting capabilities. When receiving the response Cx-UAA from the HSS containing capabilities, the I-CSCF calculates the best suited S-CSCF based on capabilities, compares it with the currently assigned S-CSCF, and if different, checks whether it is available (and not highly loaded).

6.3.1.2.2 Information flow

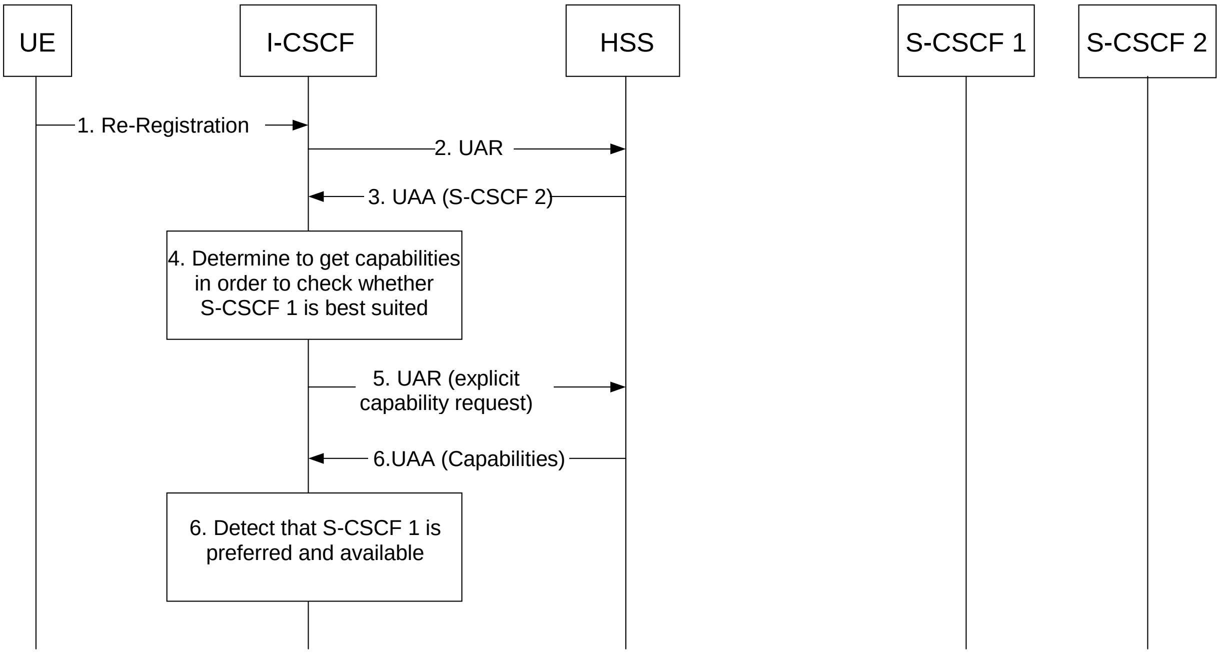

UE
I-CSCF
HSS
S-CSCF 1
S-CSCF 2
1. Re-Registration
2. UAR
3. UAA (S-CSCF 2)
4. Determine to get capabilities in order to check whether S-CSCF 1 is best suited
5. UAR (explicit capability request)
6.UAA (Capabilities)
6. Detect that S-CSCF 1 is preferred and available

Figure 6.3.1.2.2-1

1. - 3. Existing Rel-8 procedures are followed.

4. When the I-CSCF receives the current S-CSCF name within Cx-UAA it may decide to check, based on operator configuration (e.g. always, during the night), whether the currently assigned S-CSCF is not the preferred S-CSCF. If I-CSCF decides not to check, existing Rel-8 procedure is followed; re-selection is not performed. If I-CSCF decides to check; the procedure is continued with step 5.

5. I-CSCF explicitly requests capabilities from the HSS by sending a second Cx-UAR command. Note that parameters in Cx-UAR to explicitly request capabilities were already defined in Rel-8.

6. Capabilities are returned from the HSS (existing Rel-8 procedure).

7. The I-CSCF calculates the best suited S-CSCF based on the received capabilities. If the best suited S-CSCF is the currently assigned S-CSCF (i.e. S-CSCF 2) or the best suited S-CSCF is currently not available, existing Rel-8 procedure is followed. If the best suited S-CSCF is different from the currently assigned S-CSCF and is available, the I-CSCF may take additional steps towards S-CSCF re-selection. I-CSCF may rely on information provided by LDF in order to get the load and availability of the S-CSCF.

NOTE 1: This procedure is similar to a procedure documented in TS 29.228 [4], where the I-CSCF generates a timeout when no response to the SIP Register was received.

NOTE 2: The described detection mechanism extends the duration of the re-registration process and the number of messages between the I-CSCF and the HSS.

6.3.1.3 Detection mechanism 2

6.3.1.3.1 Architectural details

This architectural alternative adds additional functionality (compared to Rel-8) to the I-CSCF and the HSS. It extends Message content of Cx-UAR to allow requesting both together, the current S-CSCF name and the capabilities.

At UE re-registration, when the I-CSCF receives the SIP REGISTER message, the I-CSCF may decide to check whether the currently assigned S-CSCF (if any) is the most preferred S-CSCF for the UE based on capabilities. If so, the I-CSCF sends Cx-UAR command to the HSS, indicating that the HSS, when it returns the current S-CSCF name shall in addition also return capabilities. When receiving the response Cx-UAA from the HSS containing the current S-

CSCF name and the capabilities, the I-CSCF calculates the best suited S-CSCF based on the capabilities, compares it with the currently assigned S-CSCF, and - if different - checks whether it is available (and not highly loaded).

6.3.1.3.2 Information flow

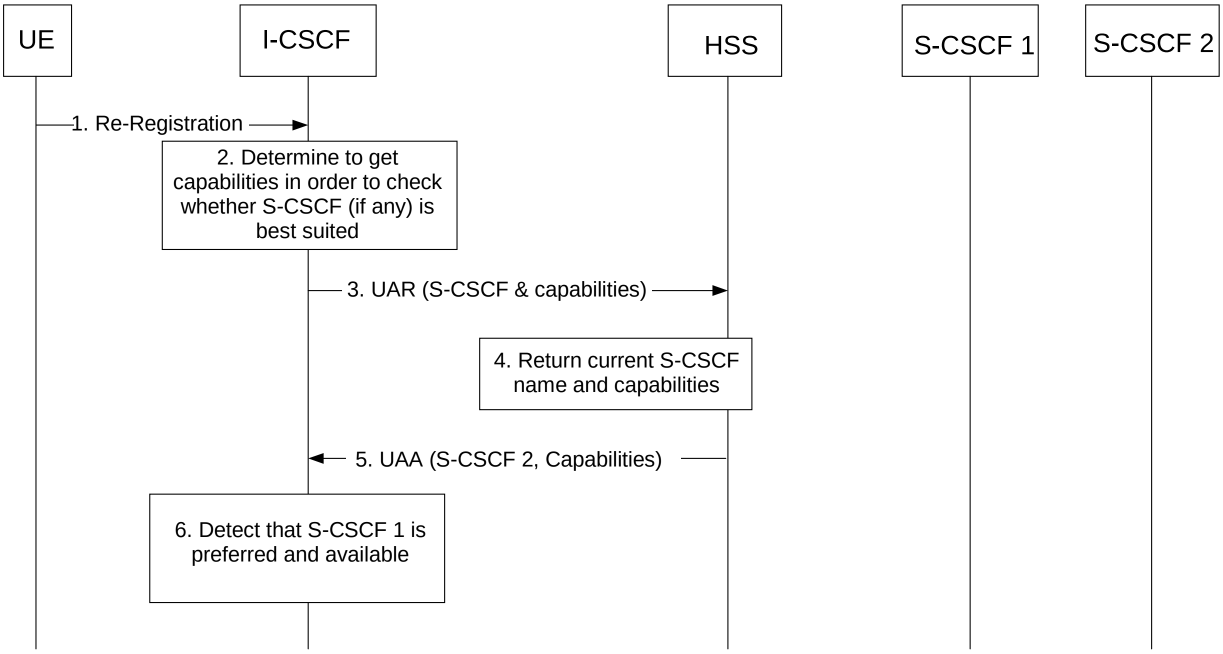

UE
I-CSCF
HSS
S-CSCF 1
S-CSCF 2
1. Re-Registration
2. Determine to get capabilities in order to check whether S-CSCF (if any) is best suited
3. UAR (S-CSCF & capabilities)
4. Return current S-CSCF name and capabilities
5. UAA (S-CSCF 2, Capabilities)
6. Detect that S-CSCF 1 is preferred and available

Figure 6.3.1.3.2-1

1. I-CSCF receives SIP REGISTER.
2. I-CSCF may determine, based on operator configuration (e.g. always, during the night), to get capabilities in order to check whether the currently assigned S-CSCF (if any) is not the preferred S-CSCF. If it decides not to do so, existing Rel-8 procedure is followed (not shown in the figure); re-selection will not be done. If it decides to perform the check, the procedure is continued with step 3.
3. I-CSCF indicates to the HSS by means of a new parameter within Cx-UAR that S-CSCF name (if any) and capabilities are requested.
4. If the HSS does not support the new indication in Cx-UAR, the new indication is ignored and the HSS follows existing Rel-8 procedure (not shown in the figure). In this case the I-CSCF may fall back to detection mechanism 1 (see 6.3.1.2.2) step 5. Otherwise the procedure is continued with step 5.
5. HSS returns the currently assigned S-CSCF name (S-CSCF 2) and capabilities to the I-CSCF.
6. The I-CSCF calculates the best suited S-CSCF based on the received capabilities. If the best suited S-CSCF is the currently assigned S-CSCF (S-CSCF 2) or the best suited S-CSCF is currently not available, existing Rel-8 procedure is followed (not shown in the figure). If the best suited S-CSCF is different from the currently assigned S-CSCF and it is available, the I-CSCF takes additional steps towards S-CSCF re-selection. I-CSCF may rely on information provided by LDF in order to get the load and availability of the S-CSCF.

6.3.1.4 Detection mechanism 3

6.3.1.4.1 Architectural details

This architectural alternative adds additional functionality (compared toRel-8) to the I-CSCF, the HSS, and the S-CSCF. It extends the functionality of the SIP REGISTER message sent from I-CSCF to S-CSCF and the Cx-SAR command sent from S-CSCF to HSS.

NOTE: It is a stage 3 issue as to how the functionality of the SIP REGISTER is extended.

A preparation step is performed at initial registration; when the I-CSCF selects a S-CSCF that is not the preferred S-CSCF (e.g. because the preferred S-CSCF is not available or highly loaded), the I-CSCF indicates to the selected (but not preferred) S-CSCF that a better S-CSCF may become available later. The S-CSCF forwards this information with Cx-SAR to the HSS which stores the information against the current S-CSCF name.

The actual detection step is then triggered by the HSS which - based on the stored information ("better S-CSCF may become available") - returns current S-CSCF name and additionally capabilities within Cx-UAA after receiving Cx-UAR from the I-CSCF. I-CSCF then may calculate the best suited S-CSCF based on capabilities and checks whether it is available (and not highly loaded).

6.3.1.4.2 Information flow (preparation step)

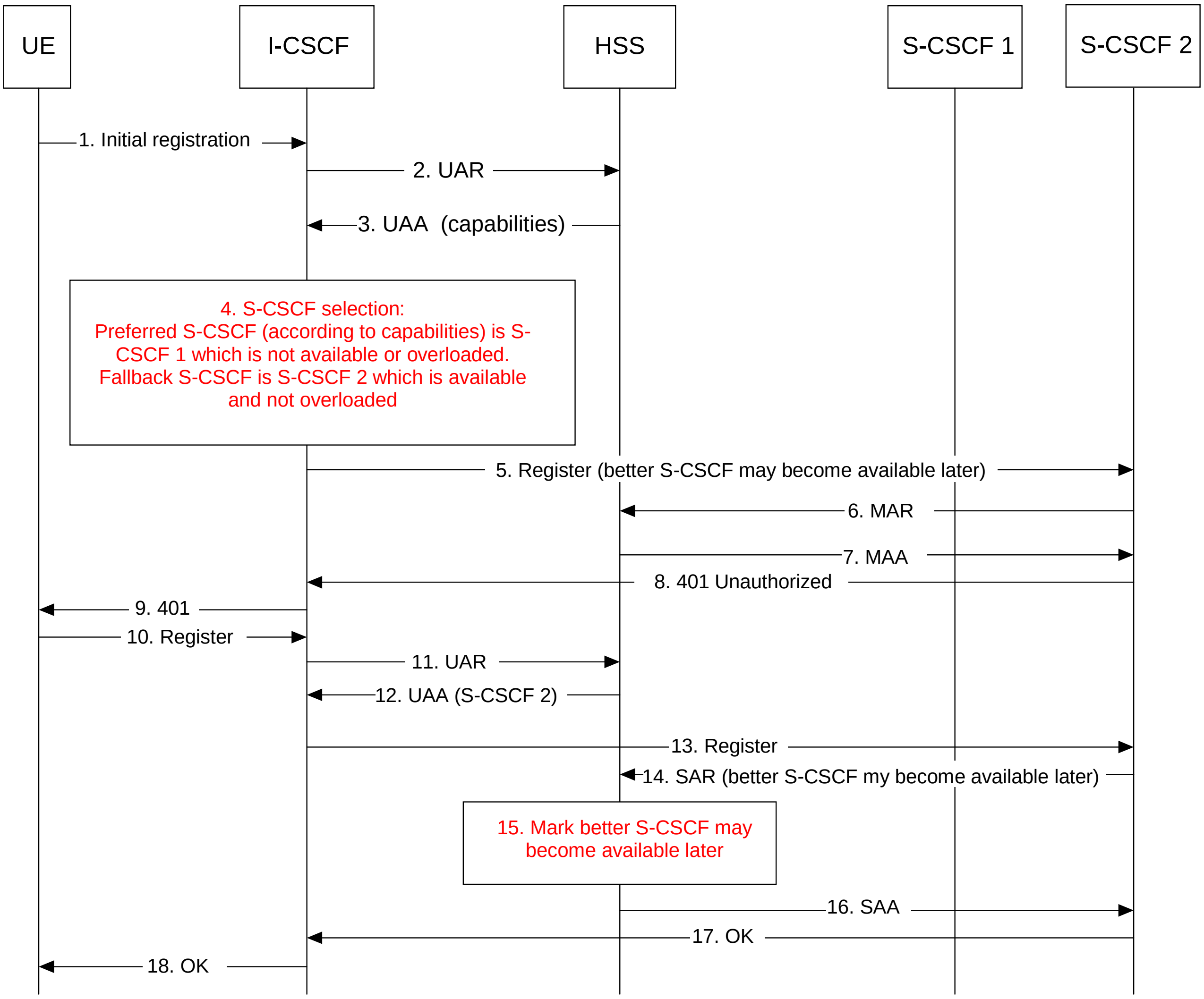

UE
I-CSCF
HSS
S-CSCF 1
S-CSCF 2
1. Initial registration
2. UAR
3. UAA (capabilities)
4. S-CSCF selection:
Preferred S-CSCF (according to capabilities) is S-CSCF 1 which is not available or overloaded.
Fallback S-CSCF is S-CSCF 2 which is available and not overloaded
5. Register (better S-CSCF may become available later)
6. MAR
7. MAA
8. 401 Unauthorized
9. 401
10. Register
11. UAR
12. UAA (S-CSCF 2)
13. Register
14. SAR (better S-CSCF my become available later)
15. Mark better S-CSCF may become available later
16. SAA
17. OK
18. OK

Figure 6.3.1.4.2-1

1.- 3. Existing Rel-8 procedures are followed.

4. I-CSCF selects a less preferred S-CSCF (e.g. because the preferred S-CSCF is not available or highly loaded).

5. I-CSCF indicates to the less preferred but selected S-CSCF that a better S-CSCF may become available later.

6. - 13. Existing Rel-8 procedures are followed. Note that in step 11 the HSS has not yet stored the information that a better S-CSCF may become available later and therefore does not return capabilities in addition to the S-CSCF name in step 12 (see 6.3.1.4.3 step 4).

14. Based on the received information in step 5 the S-CSCF forwards this information in Cx-SAR to the HSS.

15. The HSS stores the information "better S-CSCF may become available later" against the S-CSCF name.

16.- 18. Existing Rel-8 procedures are followed.

6.3.1.4.3 Information flow (actual detection step)

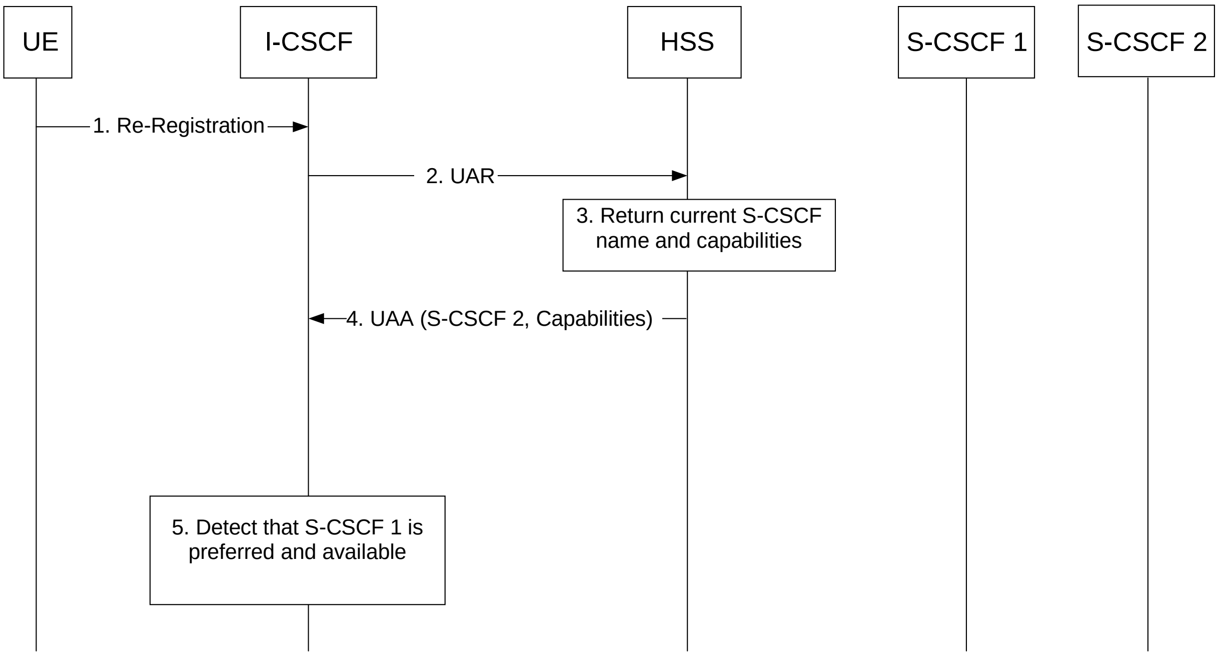

UE
I-CSCF
HSS
S-CSCF 1
S-CSCF 2
1. Re-Registration
2. UAR
3. Return current S-CSCF name and capabilities
4. UAA (S-CSCF 2, Capabilities)
5. Detect that S-CSCF 1 is preferred and available

Figure 6.3.1.4.3-1

1-2. Existing Rel-8 procedures are followed.

3. The HSS detects that it has stored the information "better S-CSCF may become available later" against the current S-CSCF.

4. The HSS returns capabilities in addition to the current S-CSCF name to the I-CSCF.

5. The I-CSCF, when receiving the current S-CSCF name and in addition also the capabilities, calculates the best suited S-CSCF based on the received capabilities. If the best suited S-CSCF is currently not available, existing Rel-8 procedure is followed (not shown in the figure). If the best suited S-CSCF is available, the I-CSCF may take additional steps towards S-CSCF re-selection.

6.3.1.5 Detection Mechanism 4

The detection for need of S-CSCF re-selection is done by either

- the interaction between the management system and the HSS. No need for interaction with other network functions. Whenever the management system detects that a subscriber needs to be moved, and based on other policies of whether it is appropriate to move the subscriber at that point in time, the management system can initiate the re-selection procedures as proposed in clause 6.3.1.3.

- local configurations and policies in HSS may also result in triggering of re-selection. This could e.g. in the case a UAR command is sent, the HSS checks whether a more "optimal" S-CSCF is available based on local configuration. This is then similar to previous alternatives, but with the decision in the HSS rather than the I-CSCF.

6.3.2 Alternatives to re-select the S-CSCF

6.3.2.1 General

The following requirements need to be fulfilled by the S-CSCF reselection mechanism:

- It shall be possible for the operator to control the S-CSCF re-selection mechanism from the operator's management system.

- It shall be possible for the operator to trigger the S-CSCF re-selection mechanism for a given subscriber at any given time.

- The S-CSCF re-selection mechanism shall have the means to force re-selection only when no on-going dialogs/subscriptions exist.

- For unregistered users, where the S-CSCF has kept the user profile after de-registration, S-CSCF re-selection may be applied.

6.3.2.2 Re-Selection mechanism 1

This alternative adds additional functionality (compared to Rel-8) to the I-CSCF and the S-CSCF. In addition it extends the SIP REGISTER message sent from I-CSCF to S-CSCF and the SIP 480 message sent from S-CSCF to I-CSCF.

Message contents of messages via Cx are not modified.

When the decision to try S-CSCF re-selection is taken by the I-CSCF the I-CSCF forwards the SIP REGISTER message to the currently selected S-CSCF. A new (compared with Rel-8) indication within the REGISTER message asks the S-CSCF to reject the REGISTER message, if there are no active sessions for the UE (or any other UE within the user's subscription). If there are no active sessions, the S-CSCF returns a 480 message to the I-CSCF. I-CSCF then sends a REGISTER message to the preferred S-CSCF. Existing Rel-8 procedures then results in re-assignment of the S-CSCF. Active sessions will not be terminated, because there are no active sessions.

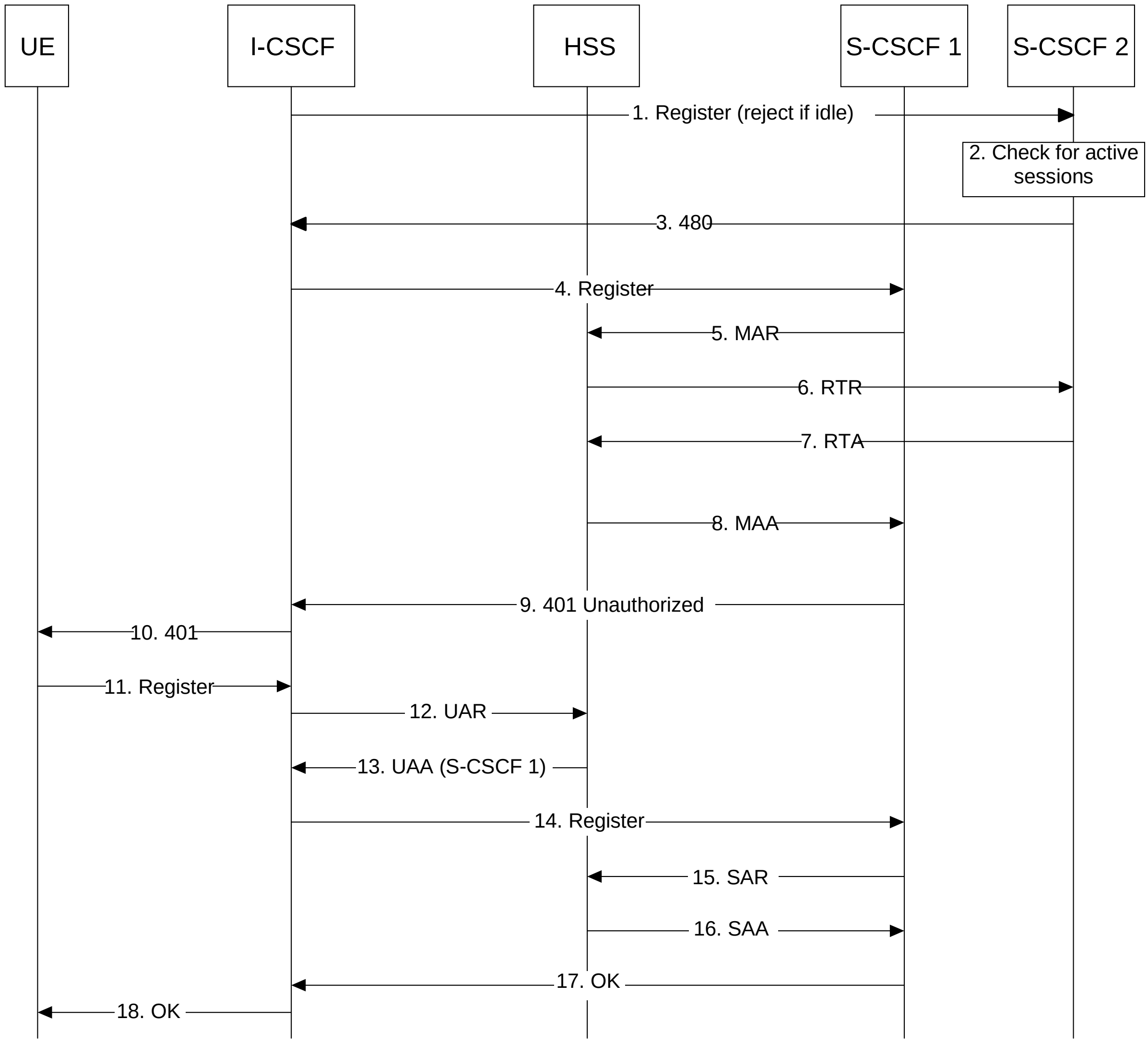


Figure 6.3.2.2-1

1. The I-CSCF sends SIP REGISTER with a new indication "reject if idle" to the assigned but less preferred S-CSCF (S-CSCF 2).

2. The S-CSCF 2 checks whether there are active sessions for any UE of the subscription. If there are active sessions (not shown in the figure) S-CSCF 2 continues according to existing Rel-8 procedures; S-CSCF re-assignment is not performed (delayed to next re-registration).

NOTE: If there are any ongoing sessions this procedure does not result in changing the S-CSCF, this includes for instance instant messaging sessions or presence subscriptions.

3. If there are no active sessions, S-CSCF 2 returns a 480 message to the I-CSCF indicating that S-CSCF re-assignment may be performed.

4. I-CSCF sends SIP REGISTER to the preferred S-CSCF (S-CSCF 1).

5. - 18. Existing Rel-8 procedures are followed and S-CSCF is changed.

6.3.2.3 Re-Selection mechanism 2

NOTE: Re-selection mechanism 2 is similar to re-selection mechanism 1. The only difference is that with mechanism 2 the S-CSCF de-registers itself from the HSS, whereas with mechanism 1 the HSS performs de-registration of the S-CSCF.

This alternative adds additional functionality (compared to Rel-8) to the I-CSCF and the S-CSCF. In addition it extends the SIP REGISTER message sent from I-CSCF to S-CSCF and the SIP 480 message sent from S-CSCF to I-CSCF.

Message contents of messages via Cx are not modified.

When the decision to try S-CSCF re-selection is taken by the I-CSCF the I-CSCF forwards the SIP REGISTER message to the currently selected S-CSCF. A new (compared with Rel-8) indication within the REGISTER message asks the S-CSCF to reject the REGISTER message, if there are no active sessions for the UE (or any other UE within the user's subscription). If there are no active sessions, the S-CSCF returns a 480 message to the I-CSCF and de-registers the user by sending SAR to the HSS. I-CSCF then sends a REGISTER message to the preferred S-CSCF. Existing Rel-8 procedures then results in re-assignment of the S-CSCF. Active sessions will not be terminated, because there are no active sessions.

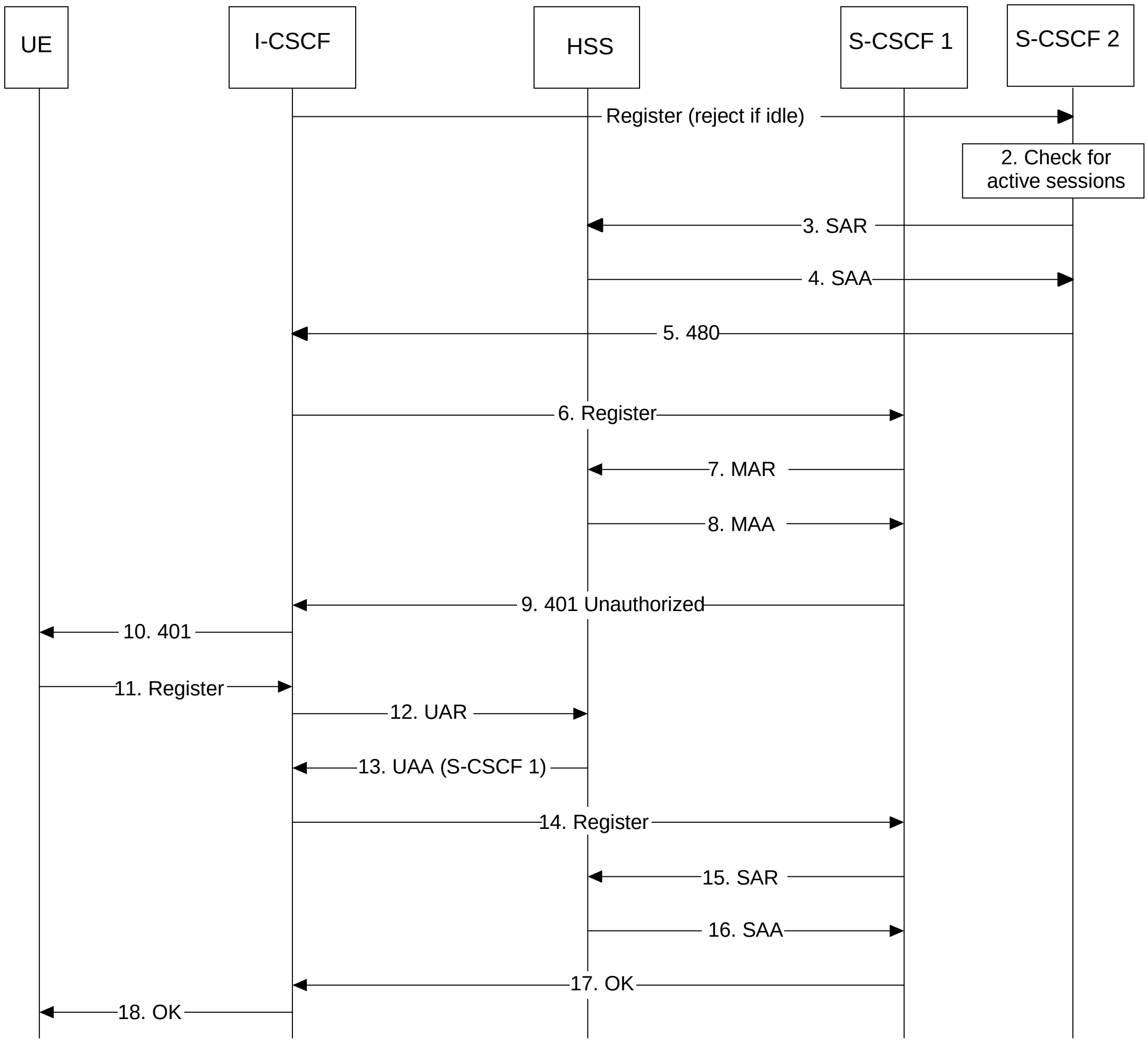


Figure 6.3.2.3-1

1. The I-CSCF sends SIP REGISTER with a new indication "reject if idle" to the assigned but less preferred S-CSCF (S-CSCF 2).

2. The S-CSCF 2 checks whether there are active sessions for any UE of the subscription. If there are active sessions (not shown in the figure) S-CSCF 2 continues according to existing Rel-8 procedures; S-CSCF re-assignment is not performed (delayed to next re-registration).

NOTE: If there are any ongoing sessions this procedure does not result in changing the S-CSCF, this includes for instance instant messaging sessions or presence subscriptions.

3. - 4. If there are no active sessions, S-CSCF 2 de-registers the user.

5. S-CSCF 2 returns a 480 message to the I-CSCF indicating that S-CSCF re-assignment shall be performed.

6. I-CSCF sends SIP REGISTER to the preferred S-CSCF (S-CSCF 1).

7. - 18. Existing Rel-8 procedures are followed and S-CSCF is changed.

6.3.2.4 Re-Selection mechanism 3

This alternative proposes to re-use the existing mechanism that allows S-CSCF re-selection. By using the Administrative de-registration procedure, the operator can force a subscriber to de-register and perform a new registration (at which time the subscriber will be allocated to the new S-CSCF).

This procedure can also be done automatically if either the management system has implemented such function or local policies exist in the HSS that can take such decision.. The Administrative de-registration procedure can be done at the time chosen by the operator if needed.

If it is required to do the S-CSCF re-selection when no active dialogs exist, the current procedures could easily be extended with including such additional criteria in the administrative de-registration command. In essence, this implies that the administrative de-registration command over Cx is extended with an indication that de-registration should only be done if no ongoing sessions exist. To solve the requirement to optionally allow S-CSCF re-selection also for un-registered user state in S-CSCF, a user de-assigning message could similar be sent also during the unregistered state from the HSS to the S-CSCF currently allocated.

7 Assessment

Editor's note: This section will assess all possible solutions and summarize the benefits and possibly the limitations of each solution.

7.1 Assessment of alternatives for Overload Control

7.1.1 P-CSCF Overload Control

There are four alternatives for P-CSCF Overload Control. Alternative 1 documented in clause 6.2.1.1 provides an Overload Control mechanism based on redirection. With this solution, P-CSCF needs to be enhanced to support feeding back other preferred P-CSCF(s). The list of backup P-CSCF(s) can either be pre-configured within each P-CSCF or fetched from LDF, which forms alternative 3 as documented in clause 6.2.1.3. With alternative 3, a new logical function, LDF, should be defined to collect dynamic load information from P-CSCFs and make appropriate P-CSCFs updated through a new interface.

Alternative 2 documented in clause 6.2.1.2 states a DNS re-request mechanism, which can be used if the UE acquires a list of SIP server domain names of P-CSCF(s) and the list of Domain Name Servers (DNS) via DHCP or has pre-configured domain names. The solution does not work if GPRS provisions P-CSCF address (es) or the UE uses pre-configured IP addresses or requests a list of SIP server IP addresses of P-CSCF(s) via DHCP. It also mentions that LDF based mechanism depicted in clause 5.2.2 can be used for DNS considering dynamic load information.

LDF may be co-located with P-CSCF or DNS server, but does not need to be implemented in a new physical entity.

Alternative 4 as described in clause 6.2.1.4 completes and is based on already existing 24.229 procedures (clause 6.2.1.4.1), which offer a mechanism to prevent the P-CSCF from getting overloaded during initial registration. There it is stated that if the UE receives 305 (Use Proxy) it shall perform initial registration with a P-CSCF address which is different from the previously used address. Alternative 4 proposes to extend this mechanism also for the re-registration procedure.

Table 7.1.1-1: P-CSCF Overload Control alternatives

Alternatives	Impact on P-CSCF	Impact on DNS	Impact on UE	Impact on SIP protocol	Restrictions
Alt 1 in clause 6.2.1.1 : overloaded P-CSCF returns the preferred P-CSCF	yes (Pre-configuration of alternative P-CSCF and redirect UE to other P-CSCF)	no	yes(Perform the registration to the redirected P-CSCF)	yes(Protocol extension for the redirection of P-CSCF)	not supported by Rel-9 UEs
Alt 2 in clause 6.2.1.2: DNS returns preferred P-CSCF	yes (only to report load info), if used with LDF	no	no	no	does not work if GPRS provides P-CSCF address or UE has pre-configured IP address or requests a list of SIP server IP addresses of P-CSCF(s) via DHCP
Alt 3 in clause 6.2.1.3: overloaded P-CSCF queries LDF and returns preferred P-CSCF	yes (Report its load info to LDF and retrieve load info of redirected P-CSCF from LDF and redirect UE to other P-CSCF)	no	yes(Perform the registration to the redirected P-CSCF)	yes (Protocol extension for the redirection of P-CSCF)	not supported by Rel-9 UEs
Alt 4 in clause 6.2.1.4 overloaded P-CSCF triggers UE to select another P-CSCF	yes (send 305 Use Proxy also for re-registration procedure)	no	yes (re-use initial registration behaviour also for re-registration)	no	not supported by Rel-9 UEs for re-registration

7.1.2 S-CSCF Overload Control during initial registration

Clause 6.2.2.1 proposes an S-CSCF Overload Control solution based on LDF, which is quite similar to that one for P-CSCF Overload Control.

LDF may be co-located with S-CSCF or DNS server, but does not need to be implemented in a new physical entity.

If Load Balancing is used from the I-CSCF, this solution is not needed as it is not likely that an overloaded S-CSCF gets selected.

Beside the described mechanism in this TR, TS 24.229 already describes S-CSCF overload protection handling within clause 5.3.1.3 abnormal cases. There is stated that if the selected S-CSCF does not respond to the REGISTER or sends back 3xx response or 480 (Temporarily Unavailable), the I-CSCF shall select a new S-CSCF based on the capabilities indicated from the HSS and shall not select one of any S-CSCFs selected previously during this same registration procedure.

Table 7.1.2-1: S-CSCF Overload Control alternatives

Alternatives	Impact on S-CSCF	Impact on DNS	Impact on I-CSCF	Impact on SIP protocol
Alt in clause 6.2.2.1: overloaded S-CSCF queries LDF and returns preferred S-CSCF	yes (Report its load info to LDF and retrieve load info of redirected S-CSCF from LDF, overload judgement and redirect to other S-CSCF)	no	yes (redirect to other S-CSCF as required)	yes (Protocol extension for the redirection of S-CSCF)
Alt2 as described in TS 24.229 clause 5.3.1.3	no	no	no	no

7.1.3 S-CSCF reselection during re-registration

Clause 6.3 proposes S-CSCF re-selection during re-registration alternatives by a two step approach:

- Step 1, as described in clause 6.3.1, checks whether S-CSCF is needed.
- Step2, as described in clause 6.3.2, performs the execution of the S-CSCF re-selection.

The following table compares the architectural alternatives to detect whether S-CSCF re-selection may be needed (step 1):

Table 7.1.3-1 Comparison of architectural alternatives to detect whether S-CSCF re-selection may be needed

	Impact on S-CSCF	Impact on I-CSCF	Impact on HSS/O&M centre
Mechanism 1 (clause 6.3.1.2): I-CSCF makes decision based on pre-configuration, unmodified Cx-UAR	No	Additional decision functionally in order to check whether the current S-CSCF is best suited	No
Mechanism 2 (clause 6.3.1.3): I-CSCF makes decision based on pre-configuration, modified Cx-UAR	No	New decision functionality, requests S-CSCF name and capabilities	Provides S-CSCF name and capabilities to I-CSCF
Mechanism 3 (clause 6.3.2): I-CSCF makes decision based on pre-configuration, 2-step approach	Stores in HSS an indication that a better suitable S-CSCF may become later	Indicates in REGISTER that a better suitable S-CSCF may become available later	Provides S-CSCF name and capabilities to I-CSCF
Mechanism 4 (clause 6.3.3): Triggered by interaction by the management system	No	Uses S-CSCF name and capabilities to select a S-CSCF	Requires additional interaction between the management system and the HSS, provides S-CSCF name and capabilities to I-CSCF

The following table compares the S-CSCF re-selection alternatives (step 2):

Table 7.1.3-2 Comparison of S-CSCF re-selection alternatives

	Impact on S-CSCF	Impact on I-CSCF	Impact on HSS/O&M centre
Mechanism 1 (clause 6.4.2): Register with Reject if Idle indication, HSS performs de-registration of the old S-CSCF	Checks if there are ongoing dialogs and indicates the current status to I-CSCF	REGISTER with "if idle" indication and performs registration with another S-CSCF	No
Mechanism 2 (clause 6.4.3): Register with Reject if Idle indication, S-CSCF de-registers itself	Checks if there are ongoing dialogs indicates the current status to I-CSCF	REGISTER with "if idle" indication and performs registration with another S-CSCF	No
Mechanism 3 (clause 6.4.4): Using administrative de-registration procedure to force new registration	Checks if there are ongoing dialogs and indicates status to HSS.	No	Extension to administrative de-registration command over Cx to avoid breaking ongoing sessions.

7.1.4 Exchange of Overload Control Information between IMS entities

Clauses 6.2.3, 6.2.4 and 6.2.5 describe alternative mechanisms for exchanging Overload Control Information between IMS entities, and clause 6.2.6 summarizes them.

These mechanisms can be grouped in two families:

- **Overload control based on explicit feedback:** draft-ietf-soc-overload-control (see clause 6.2.4). Considering the identified issues for traversal of B2BUA, this solution is only applicable to hop-by-hop cases in IMS.
- **Overload control based on traffic filters: GOCAP** (see clause 6.2.3) and draft-ietf-soc-load-control-event-package (see clause 6.2.5). Both of these solutions provide the functionality required to control overload of SIP servers.

There may be a need to select between GOCAP (see clause 6.2.3) and draft-ietf-soc-load-control-event-package (see clause 6.2.5). It is noted that there are no major technical differences between them.

However, considering that GOCAP relies on a non-IANA registered event package and that the standardization of the IETF solution is supported by a larger community than GOCAP, the latter solution is more likely to be widely supported in the industry.

7.2 Assessment of alternatives for Load Balancing

7.2.1 P-CSCF Load Balancing

Clause 6.1.1.2 gives a LDF based P-CSCF Load Balancing solution. LDF collects load information from P-CSCFs as it can do in P-CSCF Overload Control.

LDF may be co-located with P-CSCF or DNS server, but does not need to be implemented in a new physical entity.

Clause 6.1.3 proposes to reuse the IETF SOC overload control mechanism for IMS Load Balancing. The IETF SOC mechanism achieves Load Balancing by upgrading the SIP protocol for load related information transfer between UE and P-CSCF.

One problem of the IETF SOC solution is the security risk caused UE selecting P-CSCF according to P-CSCF's suggestion. Because UE is not reliable, it is possible that UE may not follow the suggestion from P-CSCF and even maliciously select reversely, causing security risks.

It is not easy for the IETF SOC solution to handle Load Balancing between P-CSCF pools.

The IETF SOC solution doesn't need to add new network entities, but it may have impacts on UE and P-CSCF because of the upgrading of SIP protocol.

The Load Balancing based on dynamic DNS (clause 6.1.4) relies on SRV DNS records. Load-balancing is therefore performed by the DNS client, which is the UE in this case. In consequence, in order to achieve efficient Load Balancing using such mechanism, requirements on the DNS Load-Balancing algorithm of the UE are needed.

Table 7.2.1-1: P-CSCF Load Balancing alternatives

Alternatives	Impact on P-CSCF	Impact on DNS	Impact on UE	Impact on SIP protocol
Alt in clause 6.1.1.2: UE queries DNS to get preferred P-CSCF	yes (only to report load info)	no	no	no
Alt2 in clause 6.1.3: SOC for Load Balancing	yes	no	yes	yes
Alt. in clause 6.1.4.2: Dynamic DNS Method 1	yes (need to implement RFC2136)	yes (need to implement RFC2136)	yes, need to implement RFC 3263	No
Alt. in clause 6.1.4.3: Dynamic DNS, Zone transfer	yes (need to implement a local DNS and RFC1034/1995)	yes (need to implement RFC1034/1995)	yes, need to implement RFC 3263	No
Alt. in clause 6.1.4.4: Dynamic DNS, SRV DNS resolution requests	yes (need to implement a local DNS).	no	yes, need to implement RFC 3263	no

7.2.2 S-CSCF Load Balancing

7.2.2.1 S-CSCF selection during initial registration

The solution documented in clause 6.1.1.3 provides a LDF based Load Balancing mechanism for selecting S-CSCF during initial registration. LDF collects load information from S-CSCFs as it can do in P-CSCF Overload Control and Load Balancing.

LDF may be co-located with S-CSCF or DNS server, but does not need to be implemented in a new physical entity.

Another solution documented in clause 6.1.2 proposes to re-use existing signalling mechanisms with the supporting system providing additional policy and information. This solution may require to specify the interface and signalling interaction between the supporting system and HSS.

Clause 6.1.3 proposes to reuse the IETF SOC overload control mechanism for IMS Load Balancing. The IETF SOC mechanism achieves Load Balancing by upgrading the SIP protocol for load related information transfer between I-CSCF and S-CSCF.

It is not easy for the IETF SOC solution to handle Load Balancing between S-CSCF pools.

The IETF SOC solution doesn't need to add new network entities, but it may have impacts on I-CSCF and S-CSCF because of the upgrading of SIP protocol.

Table 7.2.2.1-1: S-CSCF Load Balancing alternatives

Alternatives	Impact on S-CSCF	Impact on DNS	Impact on I-CSCF	Impact on SIP protocol	Impact on HSS
Alt1 in clause 6.1.1.3: I-CSCF constructs domain name	yes (only to report load info)	no	no	no	no
Alt 2 in clause 6.1.2: HSS returns preferred S-CSCF	no	no	no	no	yes (Implement optimal S-CSCF selection algorithm based on the information HSS and the supporting system have)
Alt3 in clause 6.1.3: SOC for Load Balancing	yes	no	yes	yes	no
Alt. in clause 6.1.4.2: Dynamic DNS Method 1	yes (need to implement RFC2136)	yes (need to implement RFC2136)	no	No	no
Alt. in clause 6.1.4.3: Dynamic DNS, Zone transfer	yes (need to implement a local DNS and RFC1034/1995)	yes (need to implement RFC1034/1995)	no	No	no
Alt. in clause 6.1.4.4: Dynamic DNS, SRV DNS resolution requests	yes (need to implement a local DNS).	no	no	No	no

7.2.2.2 S-CSCF re-selection during re-registration

There are two issues identified during the study for S-CSCF re-selection during re-registration. The first issue is to detect whether the S-CSCF re-selection is required. The other issue is to execute the re-selection.

There are five alternatives to handle the first issue. The assessment of them is as follows:

Alternative 1 documented in clause 6.3.1.2 adds additional functionality and signalling load (compared to Rel-8) to the I-CSCF. Message contents of SIP or Cx messages are not modified.

Alternative 2 documented in clause 6.3.1.3 adds additional functionality (compared to Rel-8) to the I-CSCF and the HSS. It extends Message content of Cx-UAR to allow requesting both together, the current S-CSCF name and the capabilities.

Alternative 3 documented in clause 6.3.1.4 adds additional functionality (compared toRel-8) to the I-CSCF, the HSS, and the S-CSCF. It extends the functionality of the SIP REGISTER message sent from I-CSCF to S-CSCF and the Cx-SAR command sent from S-CSCF to HSS.

Alternative 4 documented in clause 6.3.1.5 can provide load information via network management system. It can in such case be treated as LDF is integrated in OSS system.

Alternative 5 documented in clause 6.1.1.4 let I-CSCF determine and, if necessary, gets capabilities of S-CSCFs from HSS like Alternative 1 or Alternative 2. LDF collects load information from S-CSCFs and can be a function of S-CSCF.

Table 7.2.2.2-1: S-CSCF re-selection determining alternatives

Alternatives	Impact on S-CSCF	Impact on DNS	Impact on I-CSCF	Impact on SIP protocol	Impact on HSS	Impact on diameter protocol	Impact on ongoing sessions
Alt1 in clause 6.3.1.2: I-CSCF decides the preferred S-CSCF	yes (only to report load info)	no	yes(Check if the best S-CSCF is selected based on the first UAR/UAA and send the second UAR to get the S-CSCF capabilities)	no	no	no	no
Alt 2 in clause 6.3.1.3: I-CSCF queries HSS with S-CSCF name and capabilities	yes (only to report load info)	no	yes(Send UAR to get the current S-CSCF and capabilities and decide on the preferred S-CSCF)	no	yes (Return the current S-CSCF and capabilities at the same time)	yes UAR/UAA needs to be extended to contain S-CSCF and capabilities	no
Alt3 in clause 6.3.1.4: with fallback S-CSCF	yes (only to report load info)	no	yes(preferred S-CSCF selection and mark the indication of better S-CSCF in the forwarded REGISTER)	yes (REGISTER needs to be extended to indicate a better S-CSCF is available later)	No	yes (SAR needs to be extended to indicate a better S-CSCF might be available later)	no
Alt4 in clause 6.3.1.5: HSS based solution	yes (only to report load info)	no	no	no	yes (HSS may need to interact with O&M to get the status of S-CSCF)	don't know	don't know
Alt5 in clause 6.1.1.4: I-CSCF constructs Domain name	yes (only to report load info)	no	no	no	no	no	no

Three mechanisms for executing the re-selection are presented in this document. The assessment is as follows:

Both alternative 1 documented in clause 6.3.2.2 and alternative 2 documented in clause 6.3.2.3 will work, no matter taking the load information into account or not.

Alternative 1 adds additional functionality (compared to Rel-8) to the I-CSCF, the HSS, and the S-CSCF. In addition it extends the SIP REGISTER message sent from I-CSCF to S-CSCF and the SIP 480 message sent from S-CSCF to I-CSCF. Message contents of messages via Cx are not modified.

Alternative 2 adds additional functionality (compared to Rel-8) to the I-CSCF, the HSS, and the S-CSCF. In addition it extends the SIP REGISTER message sent from I-CSCF to S-CSCF and the SIP 480 message sent from S-CSCF to I-CSCF. Message contents of messages via Cx are not modified.

The only difference between the above two alternatives is that in alternative 2 the original S -CSCF deregisters itself from HSS whereas in alternative 1 it is HSS who deregister S-CSCF. But from S-CSCF re-selection point of view, these two alternatives are same.

Alternative 3 documented in clause 6.3.2.4 uses administrative mechanism to deregister S-CSCF. It may increase the complexity of OSS system if providing a per-user supervising and Load Balancing.

Table 7.2.2.2-2: S-CSCF re-selection execution alternatives

Alternatives	Impact on S-CSCF	Impact on DNS	Impact on I-CSCF	Impact on SIP protocol	Impact on HSS	Impact on diameter protocol
Alt1 in clause 6.3.2.2: overloaded S-CSCF returns preferred S-CSCF if there is no active session	yes (Send back 480 to I-CSCF if there is no active session)	no	yes (Registration to the preferred S-CSCF)	yes (REGISTER needs to be extended to indicate a better S-CSCF is available later)	no	no
Alt2 in clause 6.3.2.3: overloaded S-CSCF returns preferred S-CSCF if there is no active session, overloaded S-CSCF de-register itself	yes (Send back 480 to I-CSCF if there is no active session and then de-register itself	no	yes (Registration to the preferred S-CSCF)	yes (REGISTER needs to be extended to indicate a better S-CSCF is available later)	no	no
Alt3 in clause 6.3.2.4: using HSS based solution	yes (only to report load info)	no	no	no	yes (to get load information)	don't know

7.2.2.3 S-CSCF Load Balancing during restoration

The alternative documented in clause 6.1.1.5 proposes introducing LDF in the S-CSCF restoration procedure as depicted in TS 23.380. LDF collects load information from S-CSCFs and may be co-located with S-CSCF or DNS server.

7.2.2.4 Registration independent Serving Node Load Balancing

Clause 6.1.5 proposes a solution for Serving Node Load Balancing that is independent of the use of registrations. As such this makes this solution suitable for situations where no registrations occur, such as IMS transit networks and peering-based business trunking.

The solution proposed in clause 6.1.5 does not preclude other mechanisms for Serving Node load balancing that do not depend on registrations, such as the solution based on Dynamic DNS proposed in clause 6.1.4. Both solutions can coexist next to each other. They should not be considered mutually exclusive.

7.2.3 General consideration on Load Balancing

An additional advantage of the LDF-based solutions assessed in clauses 7.2.1 and 7.2.2 is that the LDF architecture is applicable to any entity, even those not documented in this TR.

7.2.4 LDF architecture assessment

7.2.4.1 Assessment on the utilization of EMS/NMS for the LDF architecture

Four LDF architectures are given in clause 6.1.1.1. In Alternative 1, direct interfaces are used between LDF and CSCF/DNS. In alternative 2, there are no direct interfaces between LDF and CSCF/DNS. EMS/NMS is used as an intermediary for information delivery between LDF and CSCF as well as between LDF and DNS. In Alternative 3, EMS is used as an intermediary for load monitoring. In Alternative 4, a direct interface is used for load monitoring.

The comparison of these two architectures is shown below:

Table 7.2.4.1-1

Alternatives	Impacts on CSCF	Create new function entity	Impacts on existing interface	New interface for CSCF	New interface for EMS/NMS
Alt 1 in clause 6.1.1.1.2: Direct interface	Yes (only to report load info)	Yes	No	Yes (only to report load info)	No
Alt 2 in clause 6.1.1.1.3: Indirect interface (through EMS/NMS)	No	Yes	No	No	Yes
Alt 3 in clause 6.1.1.1.x: Indirect interface (through EMS)	No	Yes	No	No	No
Alt 4 in clause 6.1.1.1.y: Direct interface, load monitoring only	Yes (only to report load info)	Yes	No	Yes (only to report load info)	No

Additional considerations related to these alternatives include:

- The OAM layer used in Alternatives 2 and 3 does not bring any added value to the communication between LDF and Network Elements.
- Alternative 2 relies on additional type 3 interfaces, although this type of management interfaces is outside the focus of 3GPP specifications.
- The only impact of Alternative 4 on Network Elements is to provide an interface to monitor load information. Although not standardized, this functionality is implemented in most modern network equipments (e.g. through SNMP).

7.2.4.2 Solution comparison between centralized LDF and distributed LDF

Three applicable scenarios for IMS Load Balancing are described in clause 5.2 of TR 23.812.

For the first scenario, i.e. "dynamically monitor and balance the load between entities of the same kind to reduce the load gaps", although each vendor can provide their own algorithms, when LDF is distributed to each IMS entity, to calculate the weights, it is necessary to share load information between IMS entities to reach a globally balanced state. This means new interfaces between IMS entities.

For the second scenario, i.e. "automatically balance load when a new entity is added to the network or a working entity is removed", if the functionality of LDF is distributed into each IMS entity, either a concentrated control is needed to lead the traffic to/from that moved entity by configuring each one's weight generating mechanism, or the sharing of load information between them is needed for self-adjustment.

For the third scenario, i.e. "automatically or in a manual way balance the load between different regions or entity pools", if the functionality of LDF is distributed into each IMS entity, when it is needed to adjust the load balancing method, e.g. to execute flexible Load Balancing between different pools, certain IMS entities need to be configured (i.e. the vendor's algorithm parameters need to be re-configured), which means a concentrated control, maybe through NMS/EMS and enhanced interfaces, is still a necessity.

The following table provides a summary of these two alternatives' impact to the network.

Table 7.2.4.2-1

Alternatives	New NE	Affected Existing NEs	New interface
Centralized LDF	LDF	P-CSCFs, S-CSCFs, etc, to respond to monitoring requests	LDF to NEs or existing EMS/NMS interfaces
Distributed LDF	no	P-CSCFs, S-CSCFs, etc.	no

8 Conclusion

Editor's note: This section will draw a conclusion on the potential alternative solutions after assessment.

It is recommended that no further work should be done within 3GPP as part of the IMS Evolution Study Item on the following aspects:

- Investigating architectural improvements to reduce the complexity of signalling procedures by reducing the signalling hops, or the number of options and combinations (by looking at different groupings of combining existing entities);
- Investigating possibilities for reducing configuration workload to save OPEX.

8.1 Load Balancing

It is recognized that an LDF architecture based on LDF as described in this TR is recommended for IMS Load Balancing.

It is recognized that the procedure described in clause 6.1.1.2.2 is able to be used for P-CSCF Load Balancing during initial registration.

It is recognized that the procedure described in clause 6.1.1.3.2 is able to be used for S-CSCF Load Balancing during initial registration.

Normative work should allow for the use of existing protocols and existing 3GPP management interfaces as much as possible.

SA WG2 has concluded that it does not have sufficient expertise to determine the best alternative architecture for this management capability and thus it is recommended that SA WG5 evaluate the different options for architectures documented in clause 6.1.1.1, recommend one of them, and progress any work if necessary.

8.2 Overload Control

In order to protect an individual P-CSCF from overload it is recommended to rely on the existing TS 24.229 procedure for initial registration as described in clause 6.2.1.4.2. It is also recommended to extend the usage of this procedure for IMS re-registration as described in clause 6.2.1.4.3.

It is recommended to restart the SA WG2 work on Overload Control mechanisms based on IETF SOC and other methods, after the related study in IETF gets mature.

Annex A:
DNS UPDATE Mechanism

DNS RR (Resource Record) has some attributes (e.g., weight parameter), which can be used to record network entities' dynamic load information. And RFC 2136 defines an UPDATE message to modify DNS RR. So a new interface could be added between DNS and LDF and the UPDATE message is used to periodically refresh the network entities' load state in order to assign a low-load network entity to the requester.

DNS periodic UPDATE messages might increase the pressure of DNS, and to relieve the pressure of DNS, the UPDATE interval could be prolonged to a certain extent and all P-CSCF load information can be batch updated from LDF to DNS.

Referring to RFC 2136, the UPDATE message can be used to update an existing RR or a group of RRs periodically. The real-time load information of P-CSCF detected by LDF can be transmitted to DNS every predefined interval. And the load message can be encapsulated in additional data of the UPDATE message.

```
+---------------------+

| Header |

+---------------------+

| Zone | specifies the zone to be updated

+---------------------+

| Prerequisite | RRs or RRsets which must (not) preexist

+---------------------+

| Update | RRs or RRsets to be added or deleted

+---------------------+

| Additional Data | additional data
```

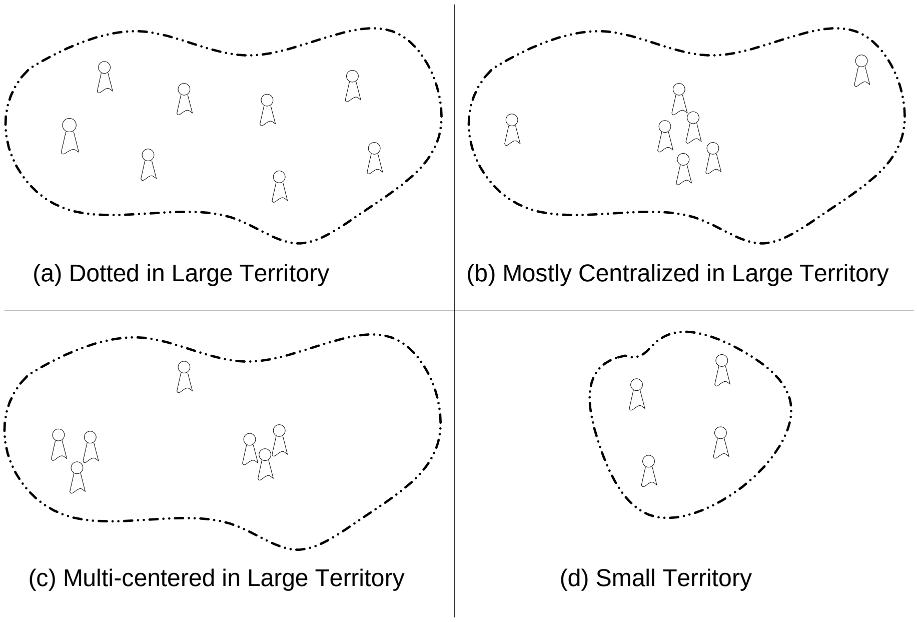
The load information contained in the additional data of UPDATE message can include the following factors:

- The current CPU and memory usage of P-CSCF;
- The number of current registered users in P-CSCF;
- The number of users with active sessions in P-CSCF;
- The maximum number of registered users in P-CSCF.

And all of the information is indicated by the weight parameter in the SRV RR. (See RFC 2782)

Annex B:
IMS Deployment Scenarios

When an operator deploys a core network, no matter whether it is IMS, the first thing to consider is the geographical distribution of its potential users. The user distribution is a key factor to influence the arrangement of the access network, which may in turn have major impact on the deployment of core network. To make things simple, some other factors, i.e. the provisioning of the carrier network and the interworking between different types of core network, are temporally put aside here.



(a) Dotted in Large Territory

(b) Mostly Centralized in Large Territory

(c) Multi-centered in Large Territory

(d) Small Territory

Figure B.1: User Distribution Scenarios

Figure B.1 illustrates four general user distribution scenarios that an operator may meet while deploying IMS. See the following explanations:

- Figure (a) illustrates the scenario that the potential users reside in a large area with no centralized characteristic
- Figure (b) illustrates the scenario that most of the potential users in a large area gathering at only one central place while a few users are dispersed.
- Figure (c) illustrates the scenario that most of the potential users in a large area gathering at more than one central place while a few users are dispersed.
- Figure (d) illustrates the scenario that the potential users are distributed in a small area.

A certain operator may care for only one or two of the above scenarios. Different scenarios, together with the operator's own operational requirements, will decide where the IMS functional entities should be located. Those logical entities located in the same place can be implemented together to save CAPEX and OPEX.

Key Issues for Operators While Deploying IMS

While deploying IMS, the operators need to take the following issues into consideration:

- The geographical positioning of IMS entities;
- The physical combination of IMS logical functional modules located in the same place, e.g. xCSCF;
- The organization of user data, which may deduce the positioning and organization of data related entities such as HSS;
- The organization of service platform, e.g., the positioning and organization of ASs;

- The interworking of IMS with other core networks, e.g. PLMN/PSTN;
- The entry to IMS (e.g. GGSN/PDN GW and SBC related issues).

For each user distribution scenario mentioned above, there may exist one most suitable solution, or there may exist general solutions for several scenarios or, ideally, even all scenarios. The last situation, obviously, will direct the optimization and evolution of IMS.

Annex C:
Example Load Information Required collected by LDF

Table C.1: Example Load Information Required collected by LDF

Data Type	Date name	Data description
CPU	CPU usage	CPU current average usage (%)
	CPU peak usage	CPU peak usage (%)
Memory	Memory usage	Memory current average usage (%)
	Peak memory usage	Memory peak usage (%)
System Load	Concurrent session number	Concurrent sessions number
	Peak concurrent session number	Peak concurrent session number
	Concurrent registrations	Concurrent Registrations
	Peak Concurrent Registrations	Peak Concurrent Registrations

Annex D: Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
12-2011	SP-54	SP-110760	-	-	-	MCC Update to version 2.0.0 for presentation to TSG SA for approval	1.2.0	2.0.0
12-2011	SP-54	-	-	-	-	MCC Update to version 11.0.0 after TSG SA approval	2.0.0	11.0.0