International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2083

(08/2014)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

Multimedia telephony over distributed service networking

Recommendation ITU-T Y.2083

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	**Y.2000–Y.2099**
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2083

Multimedia telephony over distributed service networking

Summary

Recommendation ITU-T Y.2083 describes the distributed service networking (DSN) functional architecture intended to support multimedia telephony (MMTel) services based on the DSN service requirements. The main objective of this Recommendation is to define a high level MMTel service architecture over DSN and a set of capabilities and information flows which support MMTel services.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2083	2014-08-29	13	11.1002/1000/12280

Keywords

Distributed service networking, DSN, multimedia telephony, MMTel.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.2083

Multimedia telephony over distributed service networking

1 Scope

This Recommendation specifies a cost-effective, flexible, scalable and reliable system which provides multimedia telephony (MMTel) services to users connected to a distributed service networking (DSN) network. It describes the requirements and functional architecture for supporting MMTel services over DSN, defines detailed information flows related to MMTel service provisioning, node management and overload control. It also describes the support for supplementary services, mobility, interworking, charging, and network management in an MMTel system over DSN.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T M.3060] Recommendation ITU-T M.3060/Y.2401 (2006), *Principles for the Management of Next Generation Networks*.

[ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[ITU-T Q.1707] Recommendation ITU-T Q.1707/Y.2804 (2008), *Generic framework of mobility management for next generation networks*.

[ITU-T Q.1708] Recommendation ITU-T Q.1708/Y.2805 (2008), *Framework of location management for NGN*.

[ITU-T Q.1709] Recommendation ITU-T Q.1709/Y.2806 (2008), *Framework of handover control for NGN*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[ITU-T Y.2080] Recommendation ITU-T Y.2080 (2012), *Functional architecture for distributed service networking*.

[ITU-T Y.2173] Recommendation ITU-T Y.2173 (2008), *Management of performance measurement for NGN*.

[ITU-T Y.2206] Recommendation ITU-T Y.2206 (2010), *Requirements for distributed service networking capabilities*.

[ITU-T Y.2211] Recommendation ITU-T Y.2211 (2007), *IMS-based real-time conversational multimedia services over NGN*.

[ITU-T Y.2233] Recommendation ITU-T Y.2233 (2010), *Requirements and framework allowing accounting and charging capabilities in NGN*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendations uses the following terms defined elsewhere:

3.1.1 control node [b-ITU-T Y Suppl.10]: A DSN node which provides service control and transport control functionalities.

3.1.2 distributed service networking [ITU-T Y.2206]: An overlay network which provides distributed and manageable capabilities to support various multimedia services.

3.1.3 DSN node [ITU-T Y.2206]: A node used in DSN providing distributed functionalities, including distributed routing and distributed storage.

3.1.4 functional entity [ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.5 user profile [ITU-T Y.2080]: In the context of the DSN functional architecture, a collection of information that specifies the subscribed services and access privileges related to a DSN service user. The data in the user profile is called user profile data.

NOTE – A user profile may include the following attributes: user ID and other data related to authentication and authorization, user preferences, service status, service class, usage and/or contribution information, or subscriber accounting characteristics, etc.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 admitting node: During the process of node joining, the admitting node of the joining node is responsible for the portion of the namespace which will reside in the joining node.

3.2.2 bootstrap node: During the process of node joining, the bootstrap node of the joining node is the node that the joining node contacts. The bootstrap node validates the joining node's credentials and forwards the connecting request from the joining node to its admitting node.

3.2.3 proxy node: The proxy node of user equipment (UE) is the first contact point of UE. The proxy node locates the serving node and forwards session control messages between the serving node and UE.

3.2.4 responsible node: During the process of node leaving, the responsible node of the leaving node is the node that should take over the portion of the namespace that the leaving node is currently responsible for.

3.2.5 serving node: The serving node of UE is the DSN node which processes session control messages from UE. It is responsible for a range of user profile storage, and supports user authentication, session initiation and termination.

NOTE – The different descriptions of nodes are a relative concept; the DSN node is homogenous, and a node may act as different kinds of nodes depending on different sessions, different joining nodes, etc. For example, a node may act as a serving node to a certain end-user function (EF), but may also act as a proxy node to another EF.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DSN Distributed Service Networking

EF End-user Function

ID Identification

IMS IP Multimedia Subsystem

MMTel Multimedia Telephony

NEF Node Enrolment Function

NGN Next Generation Network

P2P Peer-to-Peer

QoS Quality of Service

RLF Resource Location Function

SCF Service Control Function

SIP Session Initiation Protocol

UE User Equipment

5 Conventions

Within this Recommendation, the keywords "multimedia telephony" and "MMTel" indicate the same service as "IP multimedia subsystem (IMS) based real time conversational multimedia services" defined in [ITU-T Y.2211].

6 Functional architecture

Figure 6-1 depicts a functional architecture, based on the distributed service networking (DSN) architecture of [ITU-T Y.2080], which can be used to support multimedia telephony (MMTel) services. The service control function (SCF) includes registration, authentication, authorization, media resources controlling and service user profiles, and it interacts with the resource location function (RLF) for resource location. All the DSN nodes in the MMTel service overlay have the same functional capabilities, including RLF and SCF. DSN nodes need to be enrolled by a node enrolment function (NEF) to construct the MMTel service overlay. The related functions and reference points are identified in [ITU-T Y.2080].

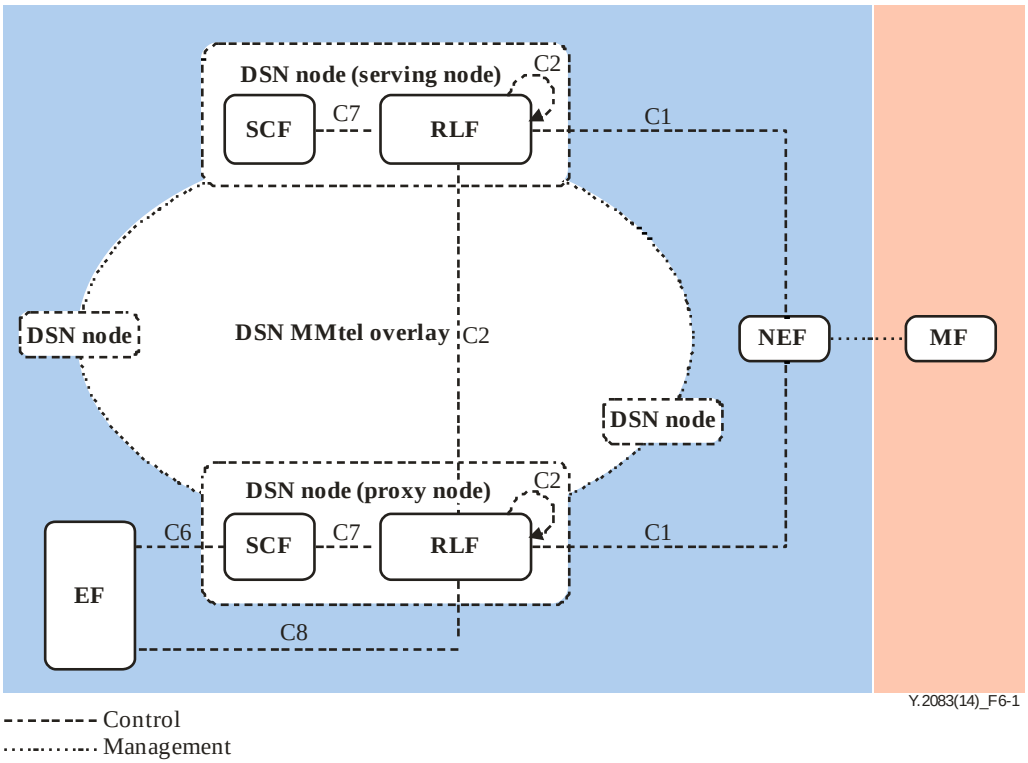

Figure 6-1 – MMTel service architecture over DSN

7 Basic communication procedures

The MMTel service allows multimedia conversational communications between two or more users. It provides for the real-time bidirectional conversational transfer of voice, video or optionally other types of data.

The MMTel communication is point to point between communicating terminals, or between a terminal and a network entity. This communication is usually symmetric, but in special cases the media components present in each direction may be different, or they may be the same, but with different bit rates and quality of service (QoS). Normally, the MMTel communication service is realised by a session control protocol.

According to whether a session control function is included, the procedures for MMTel communication can be categorized as application level procedures and overlay level procedures. The application level procedures consist of the user registration and session related procedures such as session initiation and session termination (release). The overlay level procedures contain the node management procedures which include node joining and node leaving.

7.1 Application level procedures

This clause describes the DSN application level procedures which implement the basic communication services including user registration, session initiation and session release.

NOTE 1 – The term "user" in the following procedure represents DSN user equipment (UE). The end-user function (EF) is a most primary function of DSN UE, which supports access to the DSN overlay network and service by exchanging session initiation protocol (SIP) messages with the SCF of a proxy node. UE may also include other functions.

The detailed procedures are described as follows. For easy understanding, the description of procedures in this Recommendation use the SIP protocol as an example, but are not limited to SIP.

NOTE 2 – Session initiation with supplementary services provisioning and session release due to abnormal reasons are similar to those specified in next generation network (NGN) IMS, so they are not defined in this Recommendation.

7.1.1 User registration

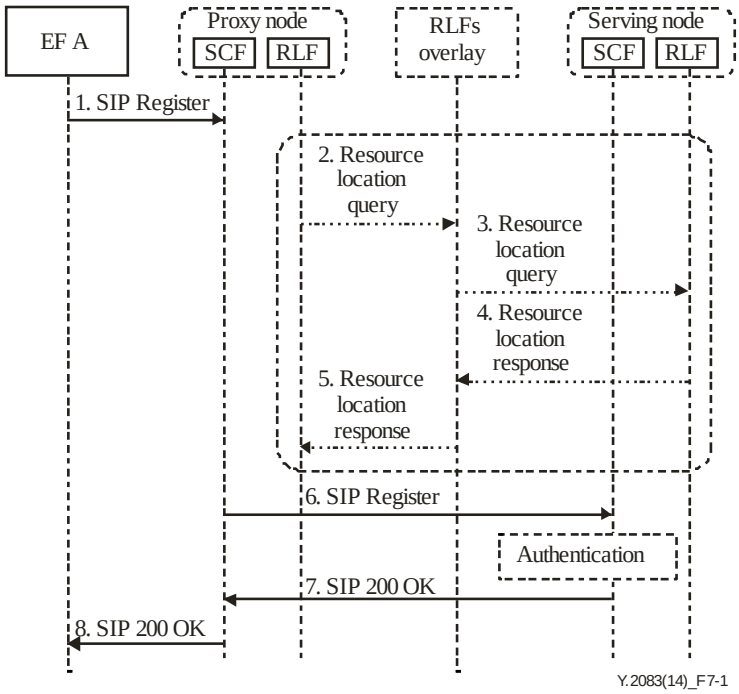

Figure 7-1 – User registration flow

NOTE – Both RLF and SCF are included in proxy node and serving node; they may exist in two separate physical entities in some deployment scenarios.

User registration flow, shown in Figure 7-1, is described as follows:

1) EF A sends a SIP register to the SCF of the proxy node;

2) The RLF of the proxy node locates the serving node for the user by using a peer-to-peer (P2P) overlay algorithm (e.g., Chord, Kademlia), and then sends a resource location query message to the overlay to find the address of the serving node;

3) The RLFs in the overlay route the resource location query message to the serving node;

4-5) When the serving node has received the resource location query message, its RLF will return a response to the RLF of the proxy node;

6) The SCF of proxy node records the address that is retrieved from the resource location query, and its SCF forwards the register message to the serving node directly;

7) The SCF of the serving node authenticates EF A by its user profile retrieved locally or remotely (e.g., from centralized user profile storage), and records registration data for EF A, and then returns a SIP 200 OK message to the proxy node indicating that registration was successful;

8) The proxy node forwards the SIP 200 OK message to EF A indicating that registration was successful.

7.1.2 Session related procedures

7.1.2.1 Session initiation

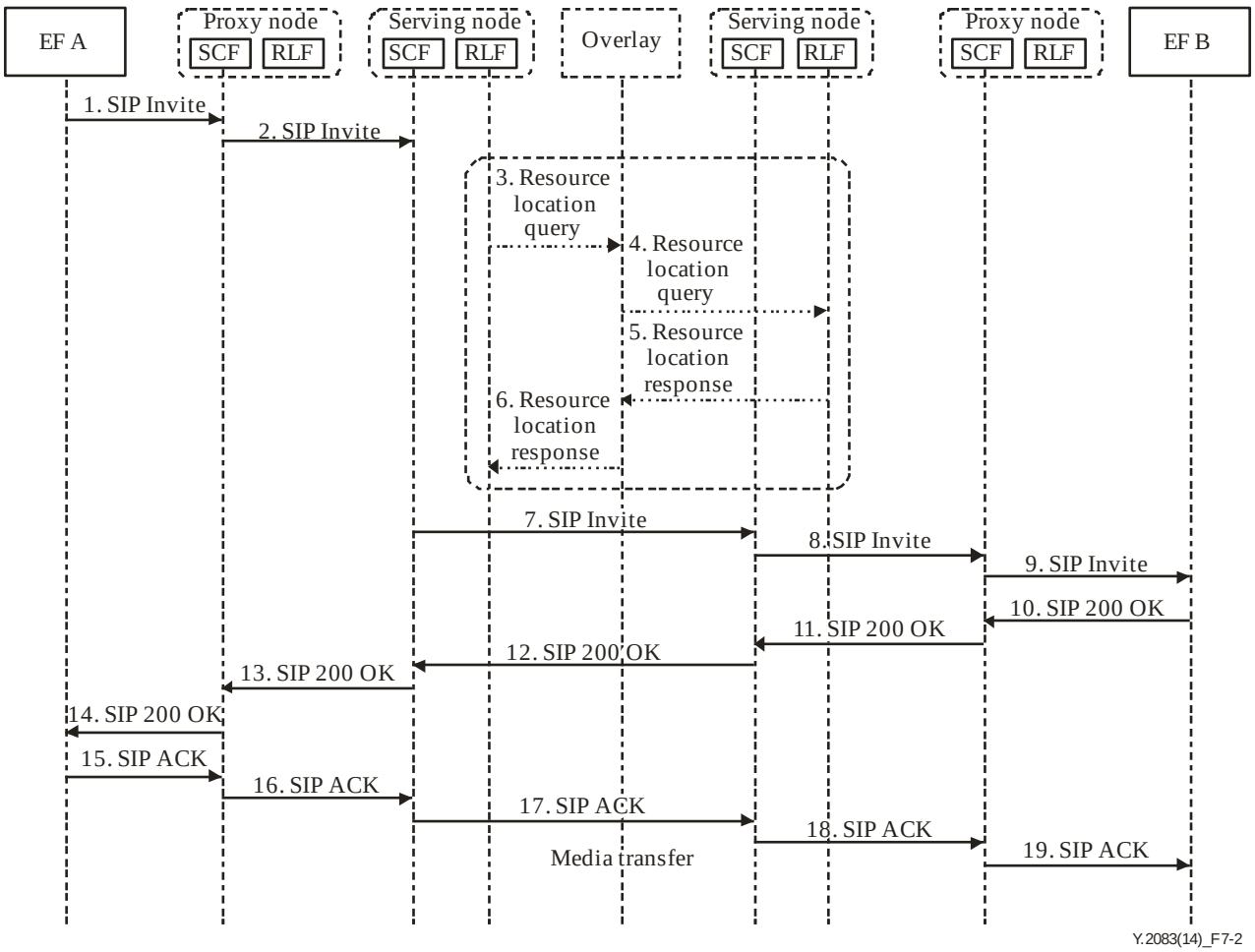

Figure 7-2 – General flow for session initiation

NOTE – Both RLF and SCF are included in proxy node and serving node.

General flow for session initiation, shown in Figure 7-2, is described as follows:

1) EF A sends a SIP invite message to its proxy node;

2) EF A's proxy node checks the address of EF A's serving node, and then forwards the SIP invite message to the serving node;

3) The RLF of EF A's serving node computes EF B's serving node ID, and sends a resource location query message to the overlay to find the address of the EF B's serving node;

4) The RLFs in the overlay route the resource location query message using a P2P routing algorithm to the serving node for EF B;

5-6) When EF B's serving node has received the resource location query message, its RLF will return its address to EF A's serving node;

7) EF A's serving node records the address of EF B's serving node in its connection table, which is the table to record other serving node's ID and address pairs, and then its SCF forwards the SIP invite message directly to EF B's serving node;

8) The SCF of EF B's serving node sends the SIP invite message to EF B's proxy node;

9) The SCF of EF B's proxy node forwards the request (SIP invite) to EF B;

10-11) Following the resource reservation and media negotiation, EF B returns a SIP 200 OK message to EF B's serving node;

12) EF B's serving node forwards the SIP 200 OK message to EF A's serving node directly;

13-14) EF A's serving node forwards the SIP 200 OK message to EF A;

15-19) After receiving the SIP 200 OK message, EF A returns a SIP ACK message to EF B, and then, EF A and EF B establish a connection.

7.1.2.2 Session release

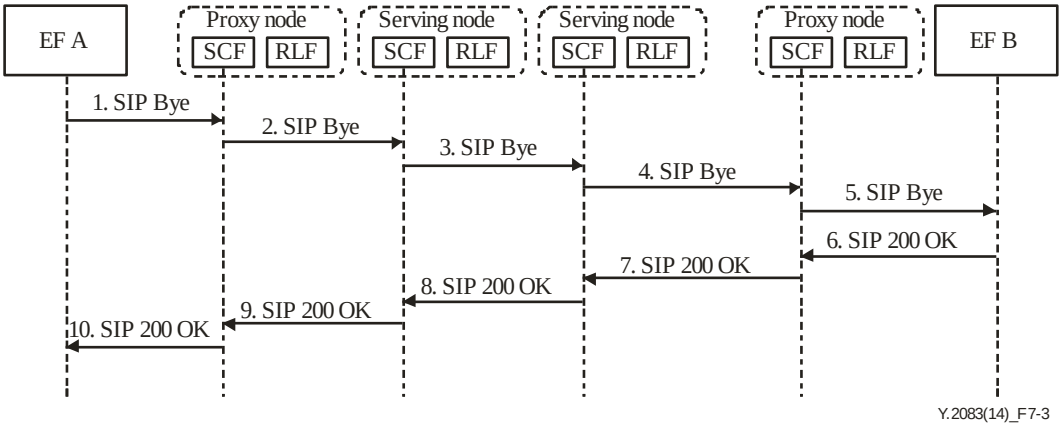

Figure 7-3 – General flow for session release

To release the session in the DSN overlay, a SIP Bye is initiated by EF A and traverses the overlay to the other end of communication, EF B, as shown in Figure 7-3.

7.2 Overlay level procedures

This clause describes the node management procedures in the overlay level when there is a node joining or leaving the DSN.

7.2.1 Node joining

7.2.1.1 Node joining without on-going and new sessions in the admitting node

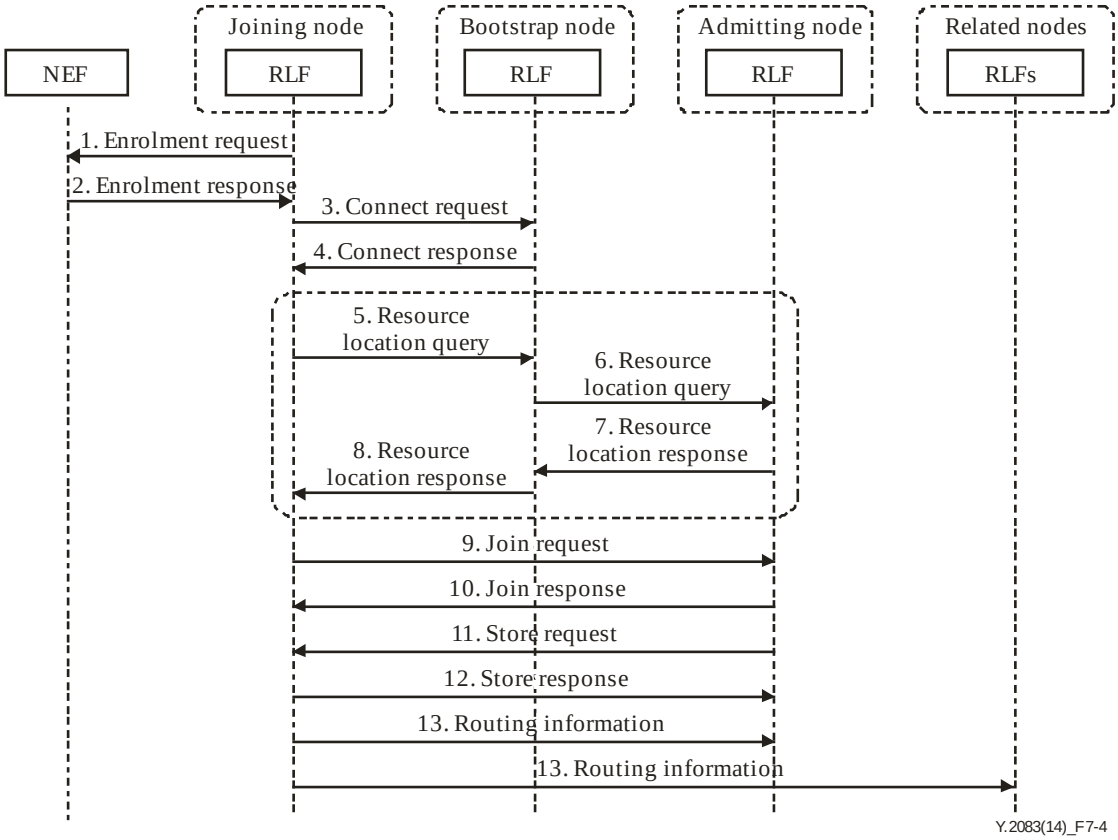

Figure 7-4 – Node joining flow without on-going and new sessions in the admitting node

Node joining flow without on-going and new sessions in the admitting node, shown in Figure 7-4, is described as follows:

1) The joining node sends an enrolment request to the NEF to request configuration and bootstrap information to join the DSN overlay;

2) The NEF authenticates the joining node and assigns a node ID for it, then returns the necessary configuration and bootstrap information;

3) The joining node tries to connect to one or more bootstrap nodes to join the DSN overlay. The address of the bootstrap node can be provided by the NEF, pre-stored in the joining node, or looked up through a DNS service;

4) The bootstrap node returns a response to set up the connection with the joining node;

5) The joining node record the address of the bootstrap node in its connection table, then according to a specific P2P algorithm, the joining node sends a resource location query request through the bootstrap node to connect to the admitting node which is currently responsible for the namespace that the joining node should take over;

6) The bootstrap node forwards the resource location query to the admitting node;

7-8) The admitting node responds to the resource location query request through the bootstrap node;

9) After received resource location response, the joining node sets up a direct connection with the admitting node. The joining node sends a join request to the admitting node to announce it will join into the overlay;

10) The admitting node checks that the joining node will take over part of its own name space and returns a response;

11) The admitting node starts transferring the data to the joining node;

12) The joining node responds for successful store action. Step 11 and 12 repeat until all necessary data are successfully transferred;

13) The joining node sends its routing information to the admitting node and other related DSN nodes which should update their routing information.

7.2.1.2 Node joining with on-going sessions in admitting node

On-going sessions are maintained by the admitting node, while user profiles are transferring from the admitting node to the joining node. In order to maintain the continuity of session control, the session control is left in the admitting node until the current session is terminated.

The following flow in Figure 7-5 shows the example of node joining with the consideration of on-going sessions.

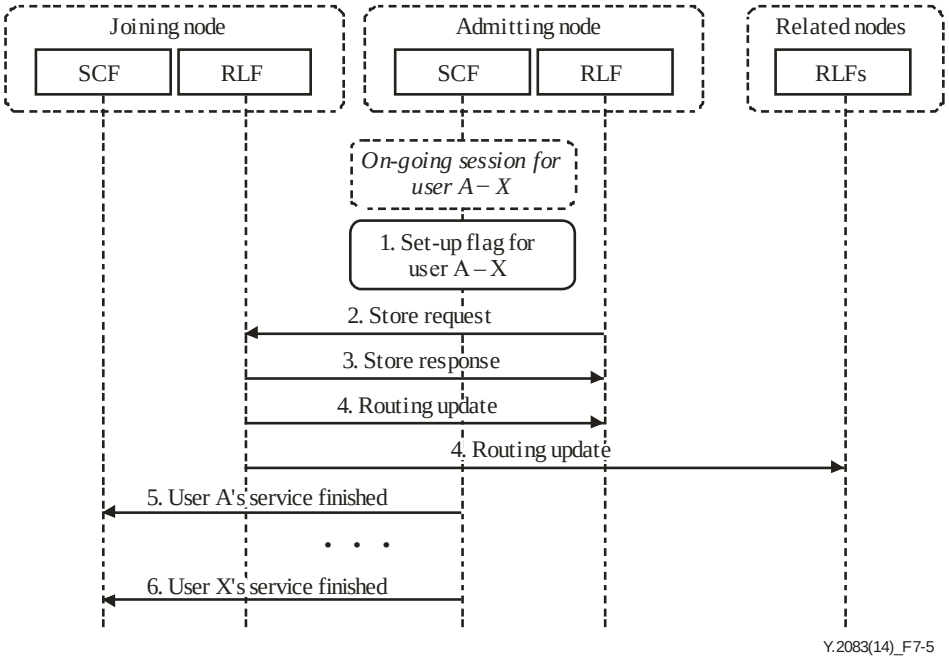

Figure 7-5 – Node joining flow with on-going sessions in the admitting node

1) On-going sessions for users A through X are maintained on the admitting node while data is transferred; flags are set in the user's profile to denote that their session control will remain in the admitting node;

2-4) Data transfers from the admitting node to the joining node, and the joining node send its routing information to the admitting node and other related DSN nodes which should update their routing information;

5) When user A's service is finished in the admitting node, an inform message is sent to the joining node to change the flag for user A's profile. Subsequently, a new service of user A can be handled in the joining node;

6) Step 5) repeats when service is finished in the admitting node until the last user (i.e., user X) finishes its service transfer.

7.2.1.3 Node joining with new session establishment in the admitting node

This clause describes the scenario in which a user, e.g., user A, sends a request to connect to user B, even though the user profile has been transferred to the joining node and user B still has an on-going session in the admitting node.

The following flow in Figure 7-6 shows the influence of node joining on such kinds of session establishment.

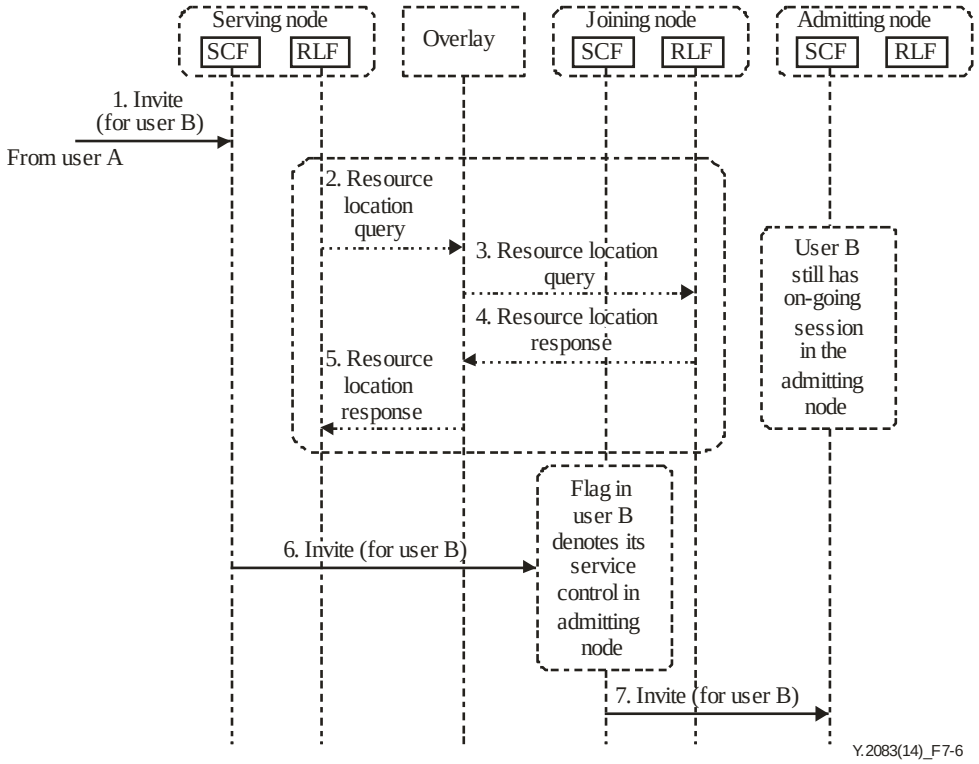

Figure 7-6 – Node joining flow with new session establishment in the admitting node

1) After the node join, there is a session request from user A to user B. An invite message is sent to user A's serving node;

2-6) The joining node that is responsible for the user profile of user B is found using an overlay algorithm. A connection is set up and the invite message is forwarded to the joining node;

7) The flag in the user profile denotes that the service control is still on the admitting node, the invite message is forwarded to the admitting node, and the admitting node will handle the invite message.

7.2.2 Node leaving

Node leaving includes graceful leaving and ungraceful leaving. Graceful leaving means that before leaving, the leaving node will send an announcement to the other nodes, so that the work or data in the leaving node will be transferred to the other nodes. Ungraceful leaving means that the node leaves without informing the other nodes and the work or data cannot be transferred from the leaving node to the other nodes.

7.2.2.1 Graceful leaving

Flows of graceful leaving for different cases are illustrated in this clause.

7.2.2.1.1 Graceful leaving without on-going and new session establishment request in the leaving node

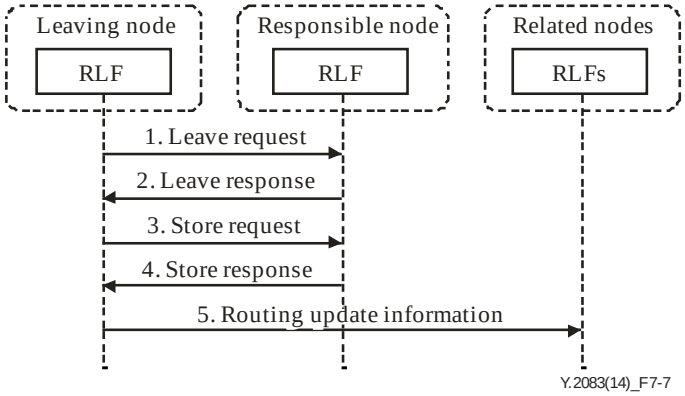

Figure 7-7 – Graceful leaving flow without on-going and new sessions in the leaving node

Graceful leaving flow without on-going and new sessions in the leaving node, shown in Figure 7-7, is described as follows:

1) The leaving node sends a leave request to the responsible node; this node will be responsible for the name space of the leaving node after it leaves;

NOTE 1 – The leaving node uses the overlay algorithm to determine the ID of the responsible node.

2) The responsible node responds to the leave request;

3) The leaving node stores its resource information to the responsible node;

4) The responsible node responses for successful store;

NOTE 2 – Step 3 and 4 can repeat until all necessary data are successfully transferred;

5) The leaving node sends its routing update information to other related DSN nodes which should update their routing information.

NOTE 3 – The update message can also be sent by the responsible node.

7.2.2.1.2 Graceful leaving with on-going sessions in the leaving node

When a node choses to leave the overlay gracefully, it transfers the entire user profile to a responsible node. However, there could still be on-going sessions maintained by the leaving node. In order to maintain the continuity of session control, the session control remains in the leaving node until the current session is terminated.

The following flow in Figure 7-8 shows the example of node graceful leaving with the consideration of on-going sessions.

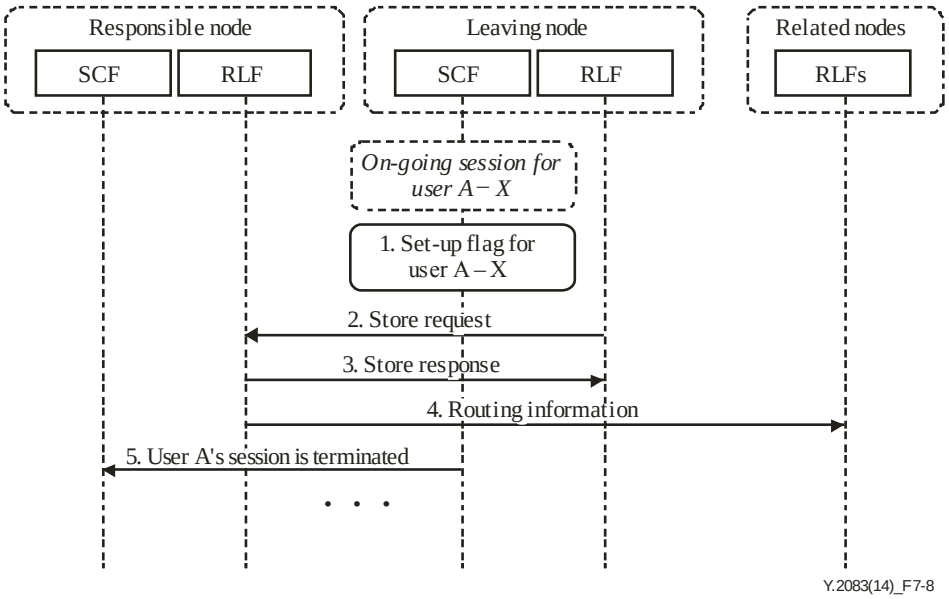

Figure 7-8 – Graceful leaving with on-going sessions in the leaving node

1) For on-going sessions for user A through X on the leaving node while data is transferred, flags are set in their user profiles to denote that their session control will remain in the leaving node;

2-4) The user profiles are transferred from the leaving node to the responsible node and the responsible node sends its routing information to its related DSN nodes which should update their routing information;

5) When user A's session is terminated in the leaving node, an inform message is sent to the responsible node to change the flag for user A's profile. Therefore, the new service of user A can be handled in the responsible node.

NOTE – Step 5) repeats when there is a session terminated in the leaving node, until the last user (i.e., user X) finishes its session in the leaving node.

7.2.2.1.3 Graceful leaving with new session establishment in the leaving node

The following flow in Figure 7-9 shows the case when there is an on-going session to the user on the leaving node, and at the same time there is a new session establishment request to the user.

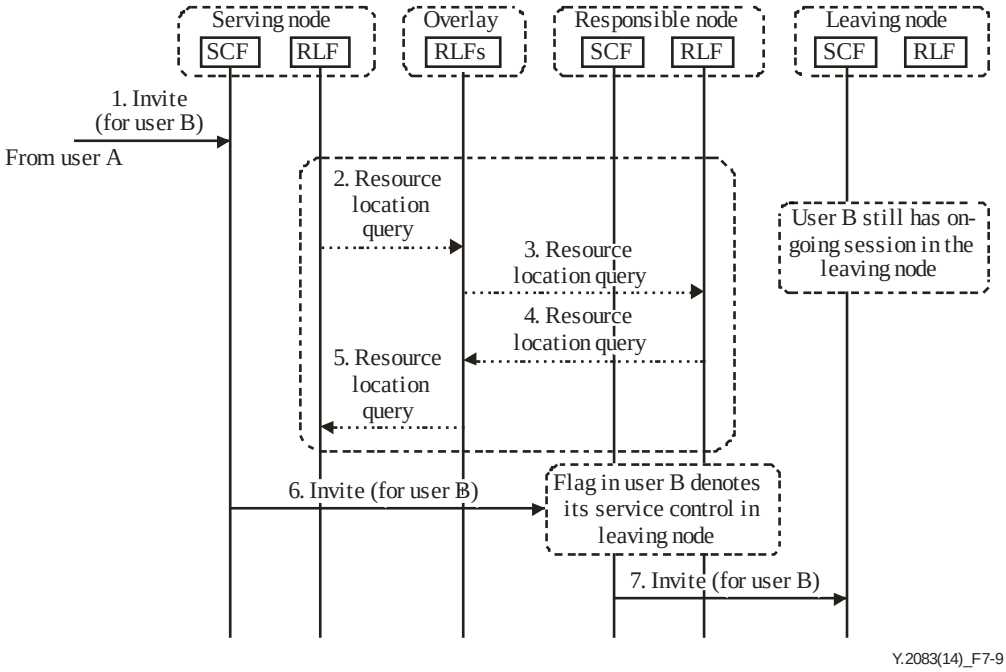

Figure 7-9 – Graceful leaving with new session establishment in the leaving node

1) During the process of node leaving, there is a session request from user A to user B. An invite message is sent to user A's serving node;

2-6) The responsible node is found responsible for the user profile of user B using the overlay algorithm. Connection is set up and the invite message is forwarded to the responsible node as described in session initiation flow;

7) The flag in the user profile denotes that the service control is still on the leaving node, then the invite message is forwarded to the leaving node.

7.2.2.2 Ungraceful leaving

In ungraceful leaving, data cannot be transferred from the leaving node to the responsible node. In order to avoid data loss due to ungraceful leaving, DSN requires a backup algorithm to keep at least one extra copy of data for each DSN node. Therefore, the resource of the leaving node can be fetched from its backup node to its responsible node when ungraceful leaving occurs, although in some special cases, the responsible node itself acts as the backup node at the same time. In addition to the leaving node's own data, the backup data stored in the leaving node will be lost as well. Therefore, the related nodes should re-back up their data.

7.2.2.2.1 Node ungraceful leaving procedure without on-going sessions and new sessions establishment request on the leaving node

If the leaving node recovers in a short time, the backup node can handle the sessions and there is no need to perform data moving. A failover timer is set up and data moving occurs only when the failover timer expires. See Figure 7-10 below.

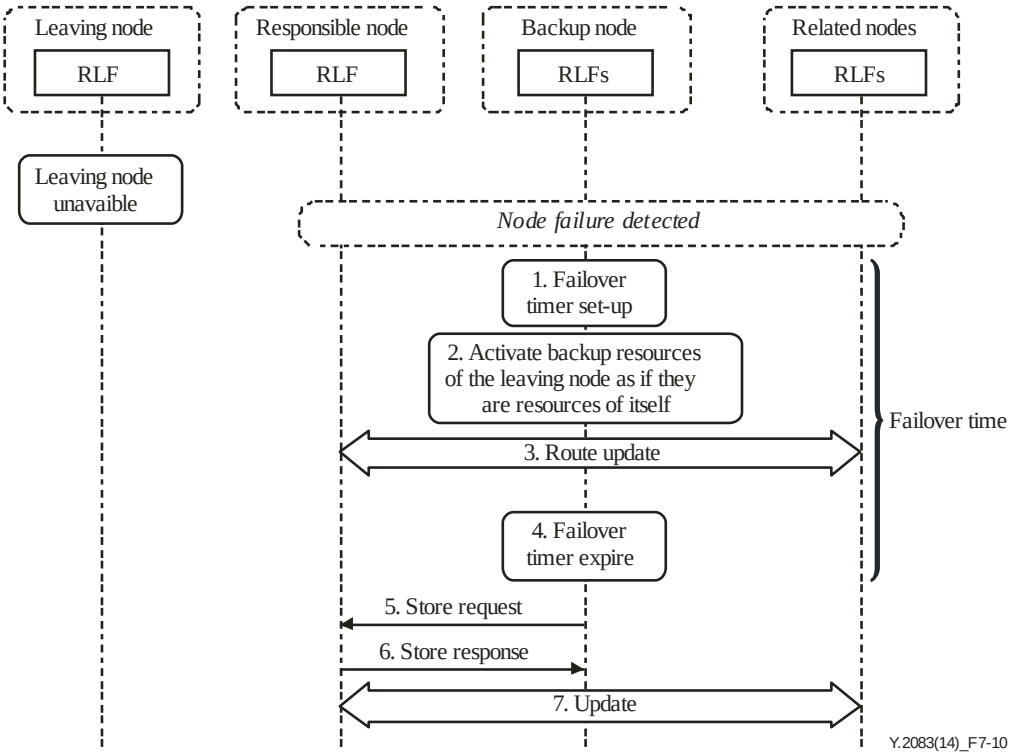

Figure 7-10 – Node ungraceful leaving flow without on-going and new sessions in the leaving node

1) Once a node leaving has been detected, a failover timer is set up in the backup nodes which have the backup of the resource for the leaving node;

2) Backup nodes activate the backup resources to handle the request for these resources during the failover time;

3) Route updates among the overlays are initiated to set up the paths to the backup nodes for the backup resource access. If the leaving node recovers during this time, it will take over the resources again;

4) The failover timer expires;

5-7) Data is transferred from the backup nodes to the responsible node and updates among overlays about the topology change are made. Note that if the backup node is the responsible node, the data transfer is not needed.

7.2.2.2.2 Node ungraceful leaving with on-going sessions in the leaving node

The node's ungraceful leaving may seriously influence the on-going sessions controlled by the leaving node. All the dynamic status data for these sessions will be lost. For example, the charging information will be corrupted as it only refers to the last updated version of the leaving node.

7.2.2.2.3 Node ungraceful leaving with new session establishment in the leaving node

The following flow in Figure 7-11 shows the case of a new session establishment request, to the users in the leaving node, before the overlay topology updated is finished.

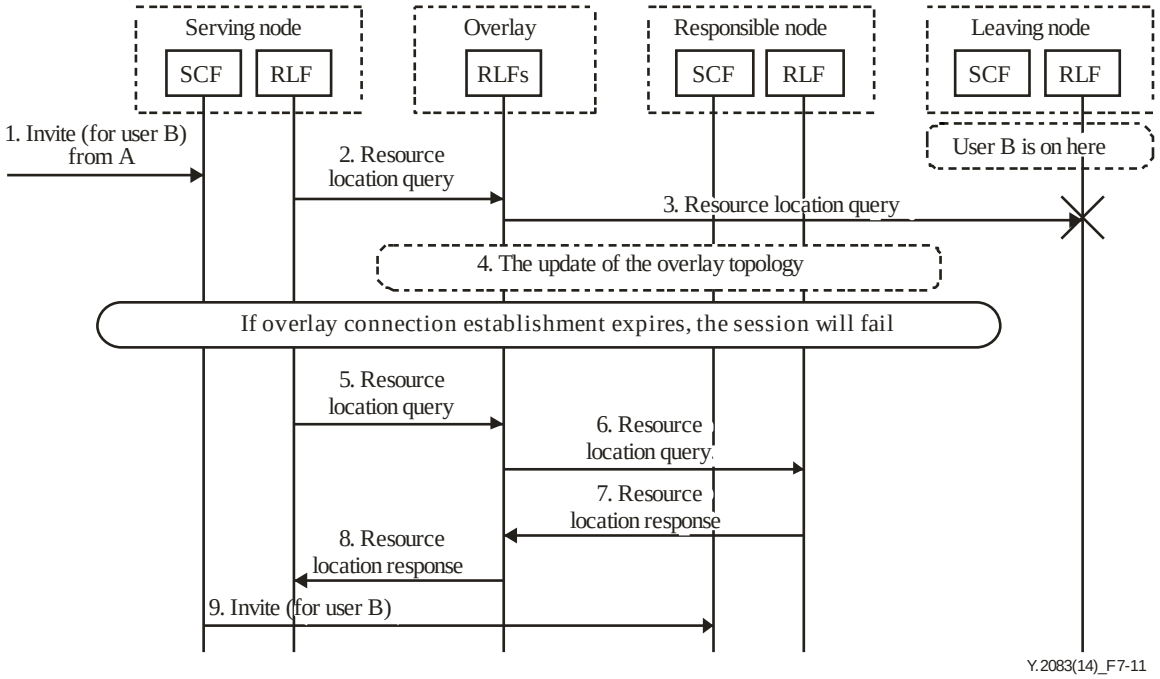

Figure 7-11 – Node ungraceful leaving with new session establishment in the leaving node

1) After node ungraceful leaving, there is a session request from user A to user B. An invite message is sent from user A's serving node;

2-3) Before the overlay topology update is finished, the resource location query message is sent to the leaving node, but there is no reply;

4) While waiting for the reply, the overlay topology detects the node failure and is updated and the responsible node takes the place of the leaving node. The summation of the failover time and the overlay topology update time must be less than the overlay connection establishment time (this time includes the retransmission interval and final set-up time);

5-8) If the overlay connection establishment does not expire before the network update finishes, the resource location query message is resent and the responsible node replies and the overlay connection is set up;

9) The invite message is forwarded to responsible node.

NOTE 1 – There is an assumption in the above flow that the overlay topology update time must be less than the time of the overlay connection establishment. Moreover, the time of the overlay connection establishment must be less than the time of the invite message retransmission. If these two assumptions cannot be satisfied, the session will fail.

NOTE 2 – The overlay topology update is triggered by the overlay routing maintenance algorithm. For example, if a node does not receive the heart-beat message from its neighbour in the routing table for a certain period of time, it will assume this neighbour has left the overlay and will initiate the topology update.

7.2.3 Session set-up procedure when serving node changes

Node joining and leaving will cause serving nodes to change for some users. The following flows in Figure 7-12 and Figure 7-13 show two kinds of solutions for session set-up when the serving node changes.

7.2.3.1 Previous serving node locates the new serving node

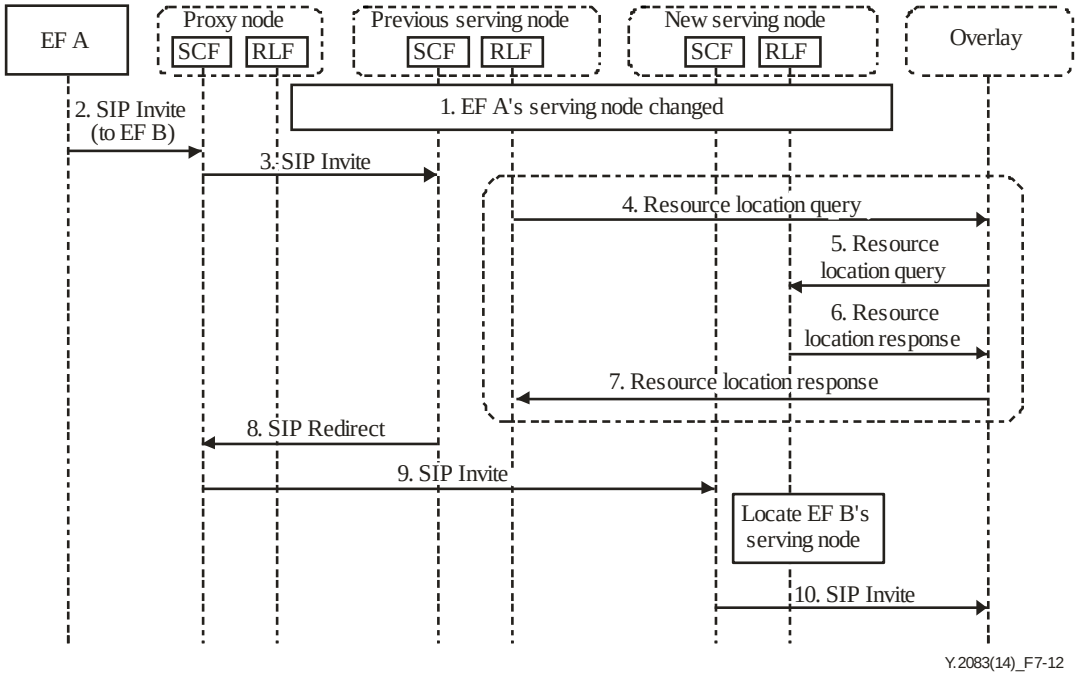

Figure 7-12 – Previous serving node locates the new serving node

1) EF A's serving node changed due to node joining or leaving;

2) EF A sends a SIP invite request to its proxy node in order to establish session with EF B;

3) Since the proxy node has no information about the change of EF A's serving node, it will forward the request to the previous serving node;

4-7) The previous serving node finds that it no longer serves EF A. Then it initiates a resource location query in the overlay to obtain EF A's current serving node;

8) The previous serving node returns a SIP Redirect message which includes the address of the current serving node to the proxy node;

9) EF A's proxy node forwards the SIP invite request to the new serving node;

10) EF A's new serving node locates EF B's serving node and forwards the SIP invite request to EF B's serving node.

7.2.3.2 Proxy node locates the new serving node

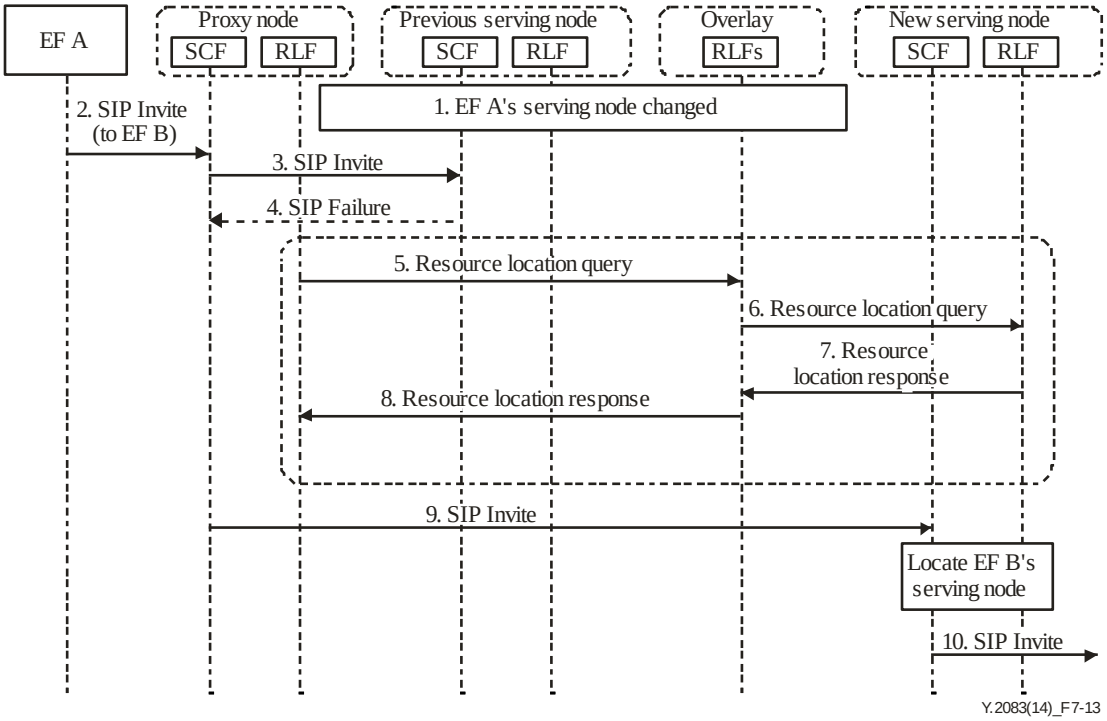

Figure 7-13 – Proxy Node locates the new serving node

Proxy node locates the new serving node flow, shown in Figure 7-13, is described as follows:

1) EF A's serving node changed due to node joining or leaving;

2) EF A sends an SIP invite request to its proxy node in order to establish a session with EF B;

3) EF A's proxy node forwards the request to the previous serving node;

4) The previous serving node finds that it no longer serves EF A, then it returns a SIP failure message which notifies EF A that its serving node has changed;

5-8) The proxy node initiates a resource location query in the overlay to obtain EF A's new serving node;

9) EF A's proxy node forwards the SIP invite request to the new serving node;

10) EF A's new serving node locates EF B's serving node and forwards the SIP invite request to EF B's serving node.

8 Overload control considerations in MMTel

When an overload happens, the overloaded node can be offloaded by using a backup node or by adding a new node when all the backup nodes are unavailable to offload the traffic. This clause describes these procedures only in the context of recommended solutions.

8.1 Overload control flows by using a backup node

When using a backup node, the backup node will ask for permission to handle the calls which should be handled by the overloaded node. The way of asking for permission can be proactive or reactive; proactive means that the backup node asks for permission in advance, while reactive means that the backup node asks for permission when new call arise.

8.1.1 Proactively overload control flows

8.1.1.1 Offloading by a backup node

This procedure applies when the serving node is overloaded; it chooses an available backup node and offloads its traffic to it.

This procedure, shown in Figure 8-1, describes the offloading flow of an overloaded node.

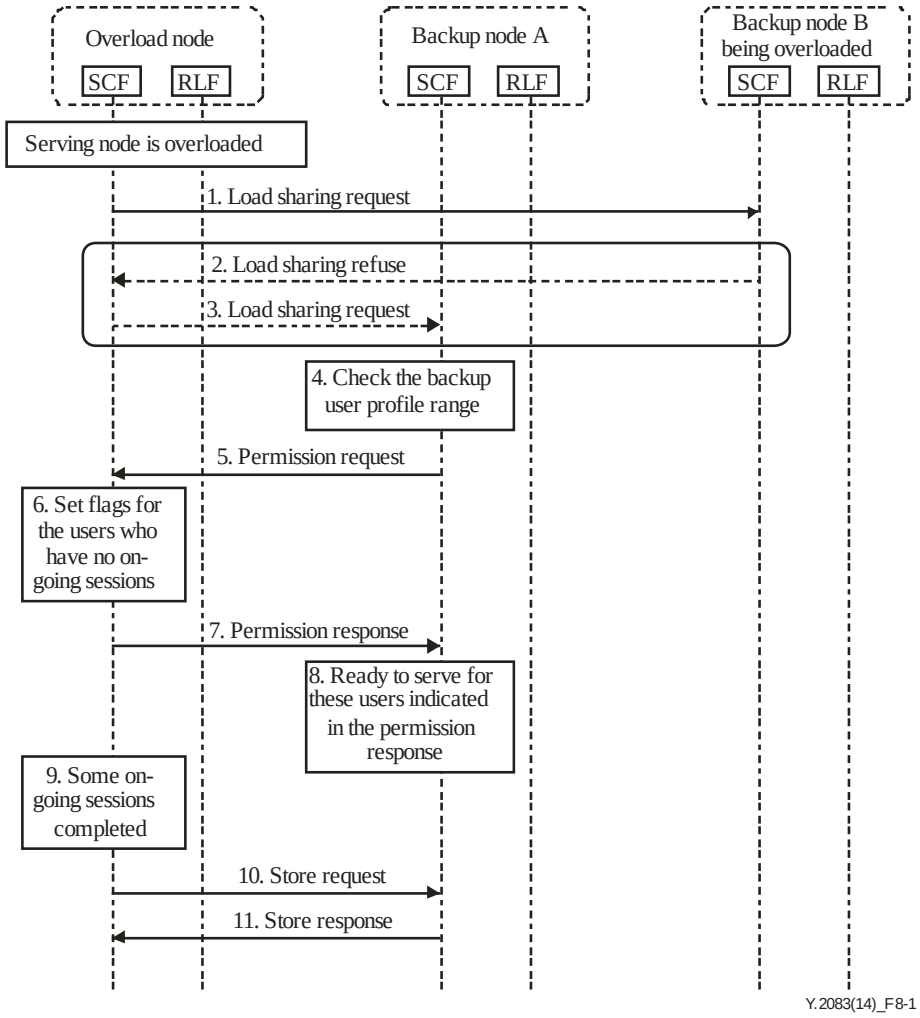

Figure 8-1 – Overload control by informing backup node to offload on overloaded node

1) If the serving node is overloaded, it sends a load sharing request message to one of its backup nodes (e.g., backup node B);

2) If backup node B cannot support the request, it refuses the offload request;

NOTE – The serving node may have more than one backup node, and if one of the backup nodes whose load is close to a threshold or has already reached it, it should refuse the load sharing request.

3) The serving node chooses another backup node (e.g., backup node A) and sends it a load sharing request message;

4) If backup node A is not overloaded, it checks its backup user profile range;

5) Backup node A sends a permission request to the overloaded serving node with a request to serve all the users whose user profiles are stored in the backup nodes;

6) The overloaded serving node sets flags for the users who have no on-going sessions indicating they will be served by the backup node. The flags may include the address of the backup node;

7) The overloaded serving node sends a permission response to the backup node which includes the user identities the backup node should be responsible for;

8) The backup node is ready to serve the users indicated in the permission response;

9-11) When on-going sessions have finished on the serving node, and it is still overloaded, the serving node transfers the profiles of the users whose sessions have just finished to the backup node and those users will be served in the backup nodes after their user profiles have transferred.

8.1.1.2 Session establishment during offloading

Figure 8-2 shows the session establishment procedure after the overloaded node has offloaded part of the user profile to its backup nodes as described in clause 8.1.1.1.

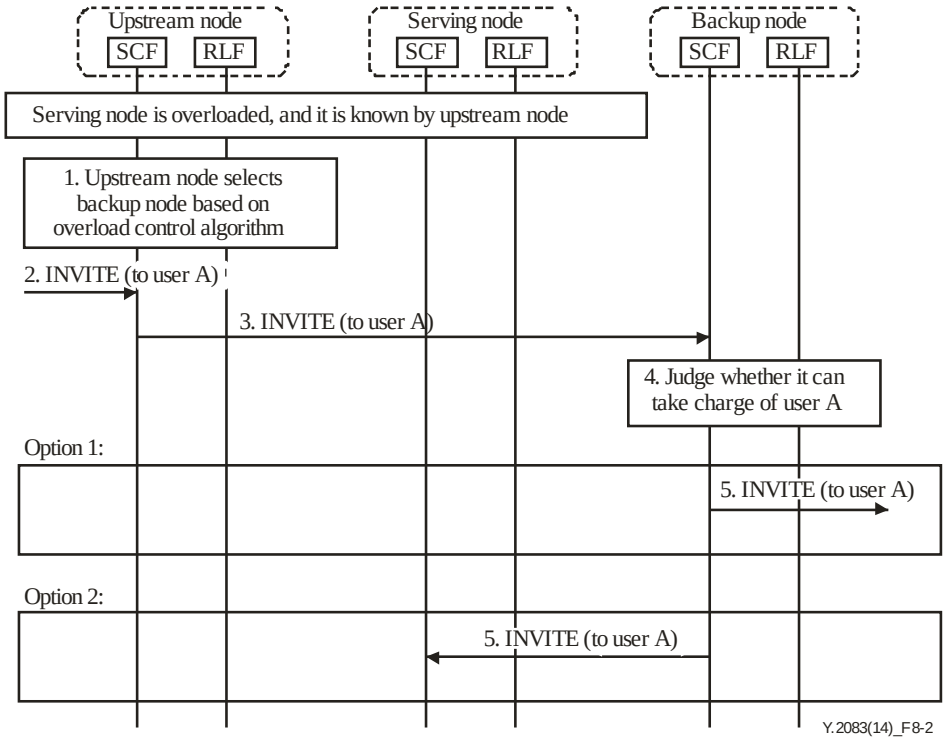

Figure 8-2 – Session establishment procedure on overloaded node with pre-informing backup node

1) The serving node which is responsible for user A's profile is overloaded and the overload status of the serving node is known by the upstream node. According to the overload control mechanism, the upstream node selects the backup node(s) of the serving node using the overlay algorithm;

NOTE 1 – Based on the load information that is carried in the keep-alive messages (i.e., the heartbeat message), the upstream node can be aware of the overload status of the serving node.

NOTE 2 – If the serving node has more than one backup node and each backup node is only responsible for some of the users, the upstream node should be aware of the range of users which each backup node is responsible for. There may be different approaches, e.g., exchange keep-alive message between the upstream node and the downstream node which carries the range information among several backup nodes. Another method is that the upstream node could calculate the target backup node of the serving node by using the global unified routing algorithm.

2) The upstream node receives an invite message designated to user A;

3) The upstream node forwards the invite message to the backup node;

4) The backup node judges whether user A should be taken charge of based on the range information it received from the overloaded serving node;

There will be two possibilities depending on whether user A is under the control of the backup node. Following are the flows for the two different cases.

Option 1:

5) The backup node finds itself responsible for user A, and then the backup node will handle the invite message.

Option 2:

5) If the backup node is not responsible for user A, it forwards the invite message to the overloaded serving node and the serving node will handle the invite message;

8.1.2 Reactive overload control flows

Figure 8-3 shows the session establishment procedure. When the target serving node is overloaded, the overloaded node prepares to offload to the backup nodes after it receives the session establishment requests.

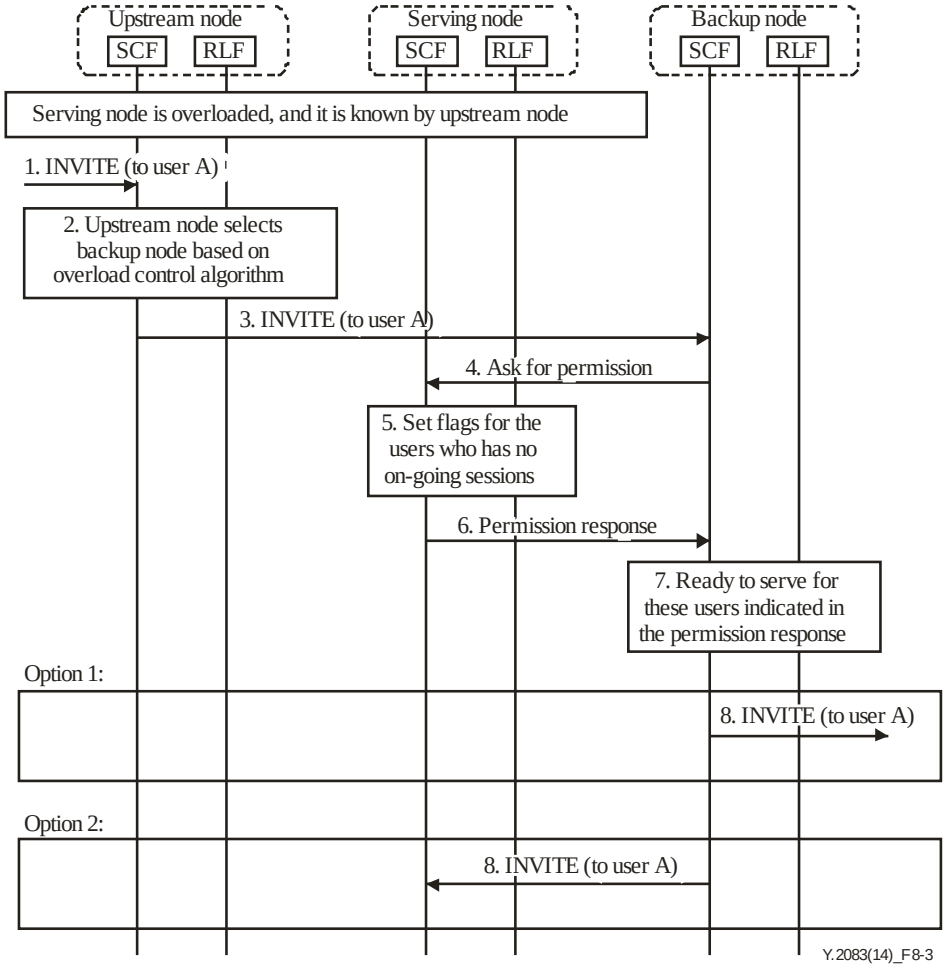

Figure 8-3 – Session establishment procedure on overloaded node without pre-informing backup node

1-2) The serving node which is responsible for user A is overloaded, and the overload status of the serving node was known by the upstream node; the upstream node receives a invite message designated to user A, according to the overload control mechanism; the upstream node selects a backup node of the serving node using the overlay algorithm;

3) The upstream node forwards the invite message to the backup node;

4) The backup node receives the invite message, then sends a permission request message to the overloaded serving node for permission to serve all the users whose user profiles are stored as backup in it;

5) The overloaded serving node sets flags for these users who have no on-going sessions and indicates that they will be served by the backup node;

NOTE – The flags may include the address of the backup node. If the serving node has more than one backup node, the flags will be synchronized to all backup nodes. When the serving node is in full-load state it cannot reply to any messages, so the backup node may refuse the invite according to local policy when time has expired.

6) The overloaded serving node sends a response to the backup node which includes the user identities the backup node should be responsible for;

7) The backup node is ready to serve the users indicated in the permission response;

There will be two possibilities depending on whether user A is served by the backup node. Following are the flows for the two different cases.

Option 1:

8) The backup node finds it is responsible for user A and it will handle the invite message.

Option 2:

8) If the backup node is not responsible for user A, it forwards the invite message to the overloaded serving node and the serving node will handle the invite message.

8.1.3 User profile synchronization after overloaded node recovery

This procedure, shown in Figure 8-4, applies when the serving node has recovered from an overloaded state.

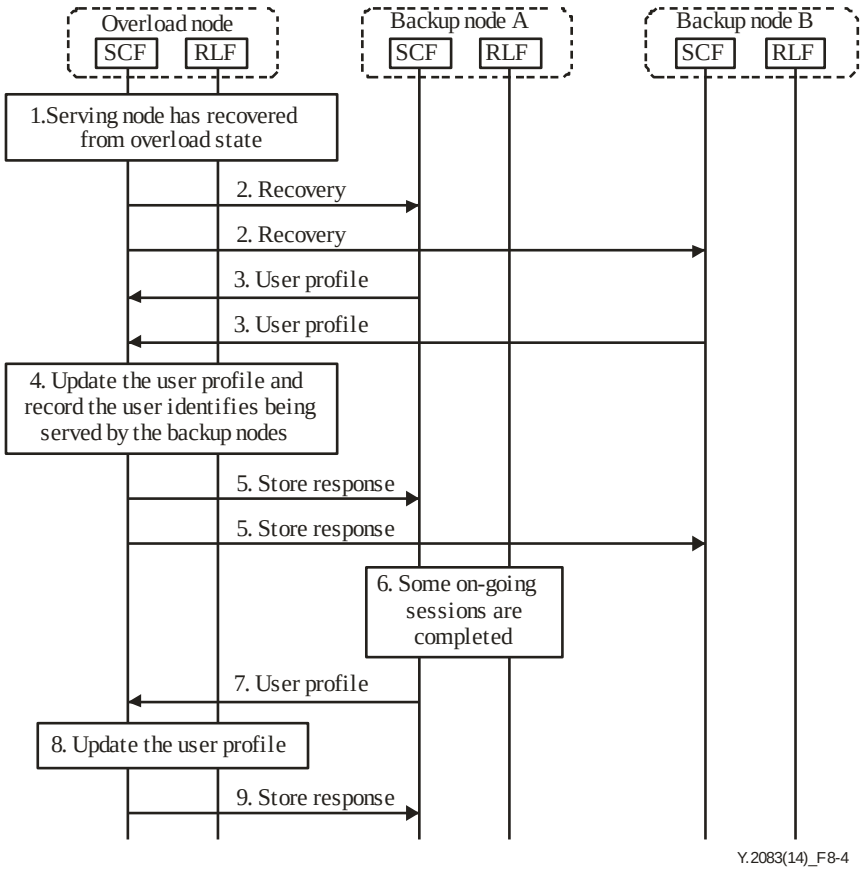

Figure 8-4 – User profile synchronization flow after overloaded node recovery

1) The serving node has recovered from an overloaded state;

2) The recovered node sends a message with recovery information to all its backup nodes in order to get the user profiles which may be updated during the overloading period;

3) The backup nodes acknowledge the recovery messages by transferring the updated user profiles to the serving node. The message also includes information about the identifiers of those users being served by the backup nodes;

4) The serving node receives and stores the latest user profiles, and records the identifies of those users being served by the backup nodes;

5) The serving node sends the store response to the backup nodes;

6-7) After the on-going sessions have finished on the backup nodes, the backup nodes send the user profiles which are updated in the on-going sessions to the serving node;

8) The serving node receives and stores the latest user profile;

9) The serving node sends the store response to the backup nodes.

8.2 Overload control by initiating a node joining

If all the backup nodes are not available to offload the traffic for the serving node, a joining node will be added to offload the traffic. The procedures for node joining are illustrated in clause 7.2.1.

9 Supplementary services support

There is no difference between NGN IMS and DSN in supporting supplementary services and services interaction which provides the relationship between different services. Detailed definition and description of the supplementary services are specified in [ITU-T Y.2211]. In DSN MMTel, the SCF in the serving node with user profile is aware of the supplementary service subscription of a user and provides access to the supplementary services. The SCF works in conjunction with the specified application server to provide the supplementary service to the user.

10 Mobility support

According to [ITU-T Y.2206], mobility in DSN can be categorized as terminal mobility and personal mobility. Terminal mobility is the ability of a terminal to access DSN services from different locations while in motion, and the capability of the network to identify and locate that terminal. Personal mobility is the ability of a user to access DSN services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.

Basically, there is no difference between NGN IMS and DSN in mobility support.

Detailed definition and description of the terminal mobility are specified in [ITU-T Q.1706], [ITU-T Q.1707], [ITU-T Q.1708] and [ITU-T Q.1709].

Detailed definition and description of the personal mobility are specified in [ITU-T Q.1706], [ITU-T Q.1707].

11 Interworking

Under the control of SCF, DSN can reuse the gateway functions (e.g., IBG-FE, TMG-FE, SG-FE) defined in NGN to interwork with networks including DSN, NGN, PSTN/ISDN, etc.

12 Charging

[ITU-T Y.2233] provides charging functions which can be used by DSN MMTel. The DSN node and interfaces between DSN MMTel system and charging system should follow the principles in [ITU-T Y.2233].

13 Security considerations

Security considerations are not addressed in this Recommendation.

14 Network management

[ITU-T M.3060] contains the management requirements, general principles and architectural requirements for managing NGNs to support business processes to plan, provision, install, maintain, operate and administer NGN resources and services. The management requirements for MMTel identified in this clause can be viewed as specialized functions of the network management function (NMF) block defined in [ITU-T M.3060].

[ITU-T Y.2173] specifies requirements, reference measurement network model, high-level and functional architectures, and procedures for performance measurement management. Data collection and measurement functions, such as configuration data collection, fault information collection, performance data collection and MMTel service QoS measurement can be viewed as specialized functions of NGN performance measurement defined in [ITU-T Y.2173].

Bibliography

[b-ITU-T Y Suppl.10] ITU-T Y-series Recommendations – Supplement 10 (2010), *ITU-T Y.2000-series – Supplement on distributed service network (DSN) use cases*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015