ETSI TR 123 924 V18.0.0 (2024-04)

TECHNICAL REPORT

**Universal Mobile Telecommunications System (UMTS);
Feasibility study on Non-Access Stratum (NAS) node selection
function above Base Station Controller (BSC)
/ Radio Network Controller (RNC)
(3GPP TR 23.924 version 18.0.0 Release 18)**

Reference
RTR/TSGS-0223924vi00

Keywords
UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or
other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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.

Introduction

The solution for support of the Intra Domain Connection of RAN Nodes to Multiple CN Nodes for GSM and UMTS systems in TS 23.236 [2] has some issues for MSC Pool with existing deployments and implementations, e.g. upgrade of existing nodes. This TR studies whether these issues can be resolved by deploying a function above the BSC/RNC nodes which provides similar functions as the NNSF in BSC/RNC nodes that is specified in TS 23.236 [2].

1 Scope

This Technical Report evaluates the feasibility of implementing a function above the BSC/RNC nodes to provide similar functions as the NNSF function in BSC/RNC nodes that is specified in TS 23.236 [2]. This Technical Report also identifies the impacts on specifications.

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 23.236: "Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes".

[3]   3GPP TS 25.413: "UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling".

[4]   3GPP TS 23.251: "Network sharing; Architecture and functional description".

[5]   3GPP TS 48.008: "3GPP TS 48.008: "Mobile Switching Centre - Base Station System (MSC BSS) interface; Layer 3 specification".

[6]   ITU-T Recommendation Q.714: "Specifications of Signalling System No. 7 - Signalling connection control part (SCCP): Signalling connection control part procedures".

3 Definitions, symbols 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].

Serving Node Selection Function: A logical function above the BSC/RNC nodes used to assign an MSC Server to serve a mobile station and subsequently route the traffic to the assigned network resource.

3.2 Abbreviations

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and TS 23.236 [2] 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] and TS 23.236 [2].

SNRI   SCCP Network Resource Identifier
SNSF   Serving Node Selection Function

4 General Description

4.1 Architecture Assumptions

Figure 4.1-1 illustrates the set of network elements related to deploying the SNSF node for MSC Pool.
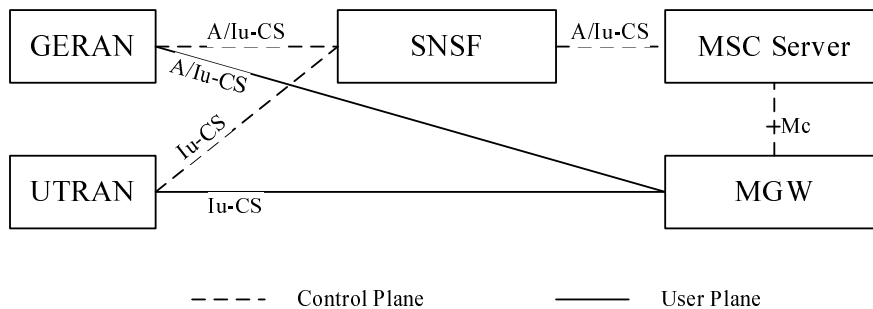
Figure 4.1-1: Network Architecture of deploying SNSF node for MSC Pool

Serving Node Selection Function is a newly introduced function which is between the BSC/RNC nodes with the MSC Servers for control plane. As implementation options, SNSF node is a logical function; it may be standalone or co-located with existing nodes. See clause 5.6 for the detail of the SNSF processing.

To resolve the issues identified from deploying NNSF within the BSC/RNC nodes for MSC pool illustrated in clause 4.2 and to avoid any potential update requirement on existing BSC/RNC equipments, the A/Iu-CS interface is used between BSC/RNC with SNSF.

4.2 Overview

4.2.1 Issues with deploying NNSF in BSC nodes for MSC pool

In certain networks and with certain implementations, some deployment issues have been identified relative to the deployment of the MSC Pool feature as specified in TS 23.236 [2]. Such issues associated with deploying NNSF in BSC/RNC for MSC pool are described in the following clauses.

4.2.1.1 In certain networks some existing BSC/RNC nodes do not support the feature

In certain networks, most of the existing BSC/RNC nodes do not support the feature, and it is not easy to update them to support the feature and to be maintained in the future. New BSC/RNC nodes can be required to support the function, but some of the existing BSC/RNC can not be upgraded. Therefore the advantage of deploying MSC Pool can not be fully exploited within certain networks.

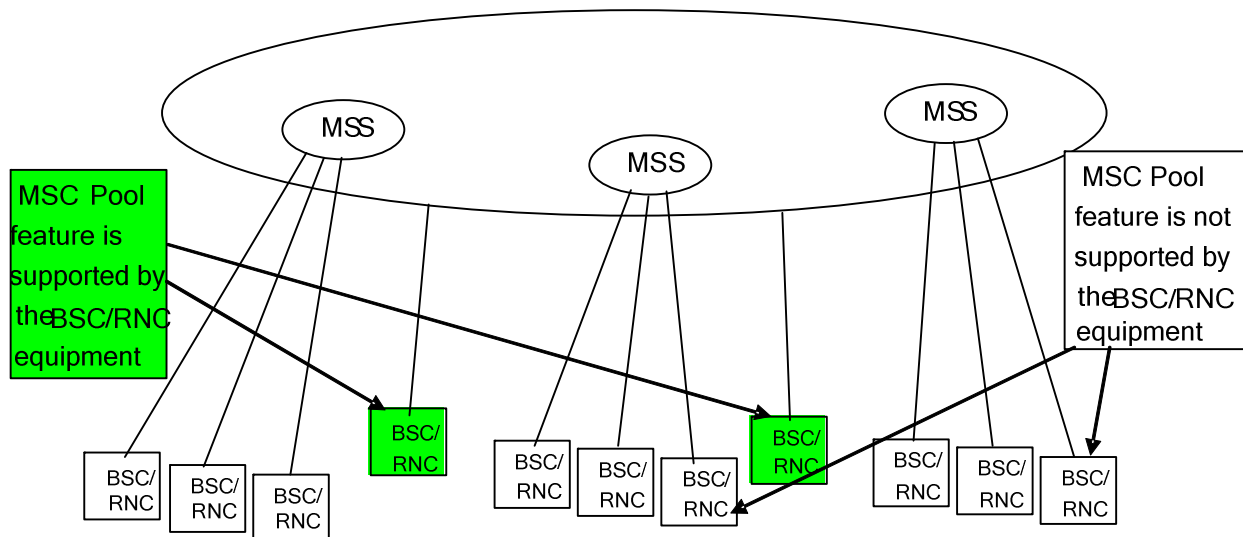**Figure 4.2.1.1.1: Part of BSC/RNC nodes support connecting to multiple MSS**

In the real-world example provided in Figure 4.2.1.1.1, nine BSC/RNC nodes do not support MSC Pool feature while two other ones support it. Only for mobile stations moving with the coverage of the 2 BSC/RNC nodes, which support NNSF and where the NNSF function is enabled, the interaction between MSC servers and HLR and inter-MSC handover are reduced, while moving to the coverage of any other BSC/RNC nodes, the interaction and the handover will still be required as if no MSC Pool feature is deployed. And when MS is in the coverage of one of the other 9 BSC/RNC nodes that do not support NNSF, only one MSC server that the BSC/RNC node connects to can serve for the subscriber, thus the resources of the MSC servers in this pool area cannot be shared. Very little advantages could be seen from the feature in such a network configuration.

4.2.1.2   Mesh TDM circuit connection between BSCs with MSCs is required

While deployment of AoIP (A interface bearer over IP) removes the mesh TDM connection of BSC nodes with MSC nodes, only TDM connections are supported by the existing BSC, and not all the existing BSC nodes can be updated to IP mode. The mesh TDM circuit connection between BSC nodes with MSC nodes is still a deployment issue in the absence of AoIP, and is described in this clause.

If the MSC Pool feature is deployed per TS 23.236 [2], the feature enabled BSC will be required to have signaling and bearer connection with all the MSCs in the pool area. Figure 4.2.1.2.1 shows the mesh connection between 3 BSC/RNC nodes and 3 MSCs.
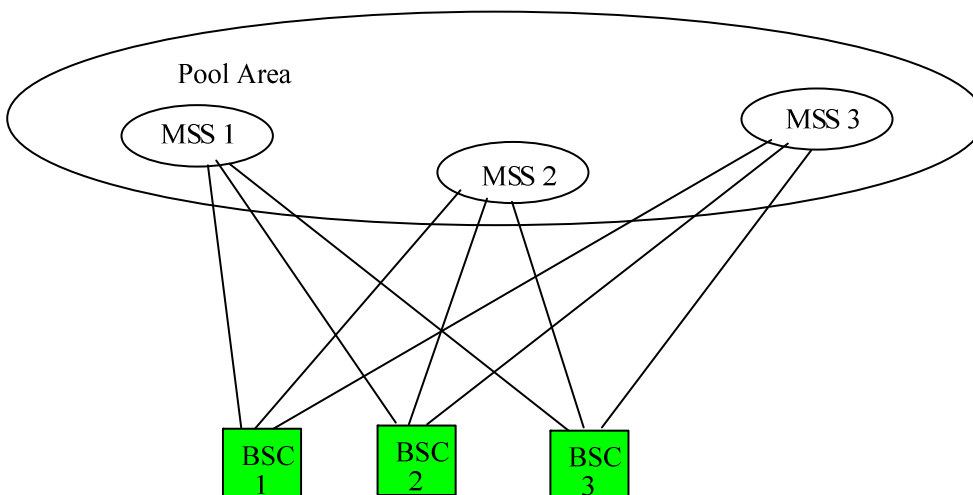

Figure 4.2.1.2.1: BSC/RNC connects to each MSS in the pool area

That is, the mesh TDM circuit connections between BSC with MSC Servers will be required because each BSC is needed to be able to connect to each MSC server in the pool area, and it will be extremely hard to implement as the POOL scale increases. When adding a new MSC into the pool area, the TDM circuit connection between all the BSCs with the new MSC must be installed (either by re-planing the TDM circuits between the BSCs with the MSCs or installing new circuits between the BSCs with the new MSC).

A physical mesh connection can be avoided by introducing virtual MGWs between BSCs and MSC servers, but the TDM circuit configuration between each pair of BSC and MSC is still required as shown in Figure 4.2.1.2.2. The TDM circuits between each pair of BSC and MSC can not be used by any other pair, e.g. circuits used for the pair BSC 1 and MSC 1 can not be re-used for the pair BSC 1 and MSC 2. Thus, the usage of the TDM circuits (specifically, the circuits in each BSC – virtual MGW pair) is limited by configuration. Any changes in the core network (e.g. adding a new MSC into the pool area) will require the TDM circuits between the BSCs with the virtual MGWs to be re-installed (either by re-planing the TDM circuit configuration between the BSCs with the virtual MGWs or by installing new TDM circuits, i.e. adding new TDM circuits between BSCs with the virtual MGW for the new MSC).
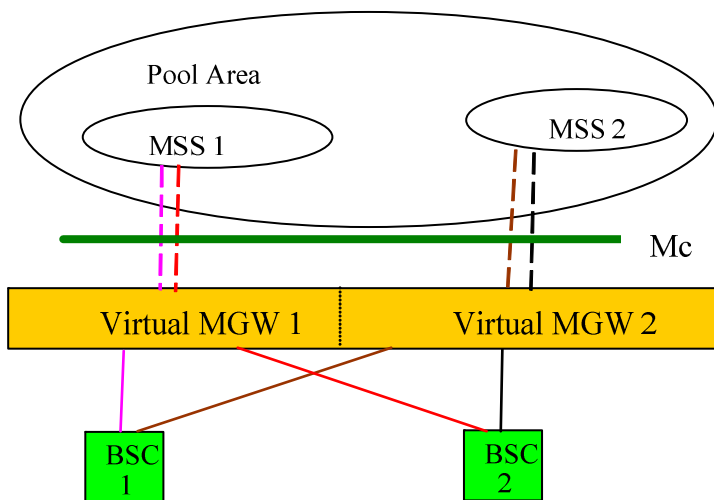
Figure 4.2.1.2.2: MGW between BSCs and MSC servers used as intermediary node

But if each BSC/RNC only connects with one or two intermediary nodes, thus keeping the number of intermediary nodes small, it will mitigate the abovementioned need as shown in figure 4.2.1.2.3 that illustrates just a single intermediary node..

See clause 4.9.1 for BSC/RNC is connected to several intermediate nodes for the control plane.
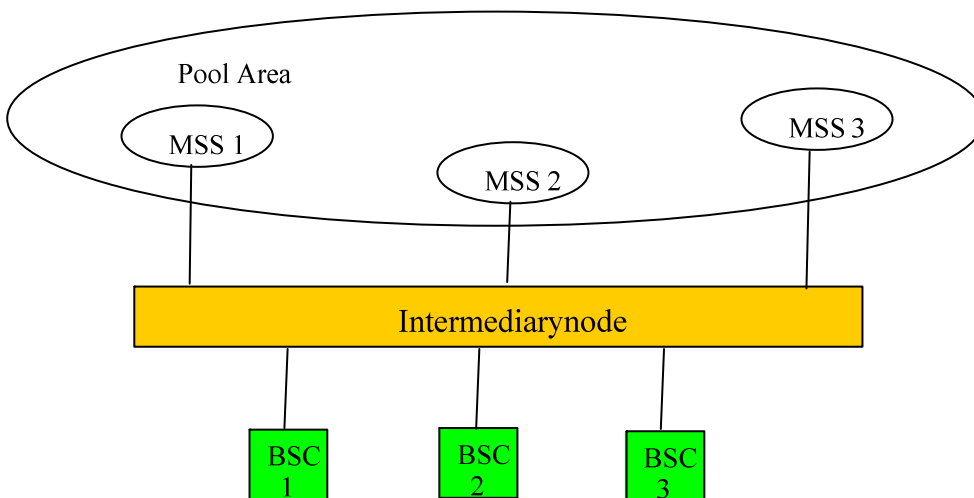
Figure 4.2.1.2.3: BSC and MSS connect to a single intermediary node

Furthermore, if the TDM circuits are reused between each pair of BSC and MSC, the likelihood of circuit exhaust will be much less, for example by means of managing the TDM circuits between the intermediary node and BSC nodes as normal resources and managed by the intermediary node itself.

4.2.1.3 Complex O&M

When NNSF is deployed within the BSC/RNC, any O&M operation related to NNSF functionality (e.g adding a new MSC into the pool area) will require the O&M centre to interact with each MSC Pool enabled BSC/RNC node individually. As the number of BSC/RNC nodes in a network increases, the complexity of O&M increases in proportion.
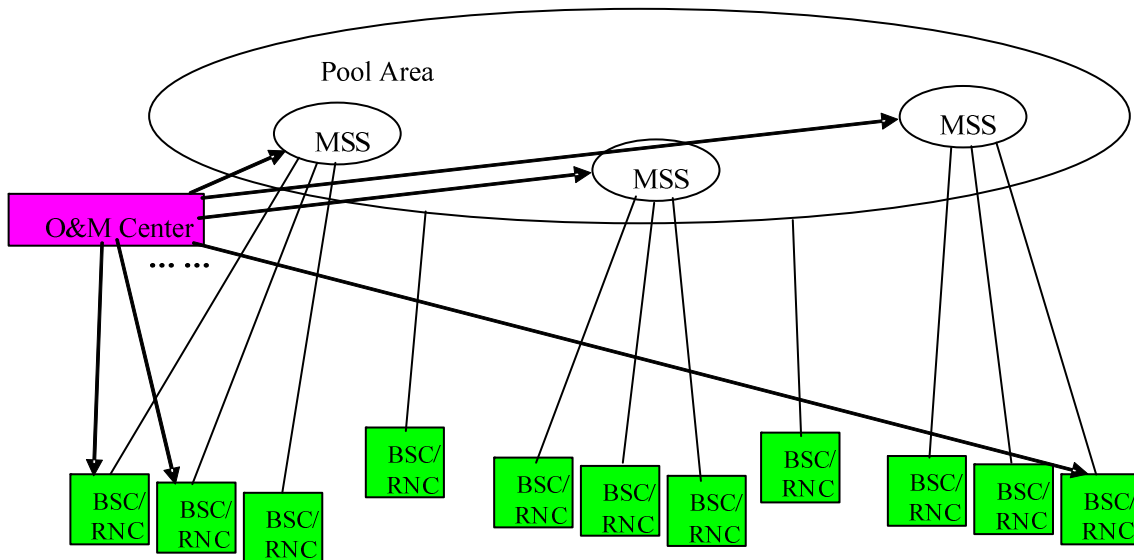
Figure 4.2.1.3.1: O&M centre send O&M command to all MSC Pool enabled BSCs/RNCs and MSSs

But if the NNSF is implemented in a small number of nodes, it will simplify the complexity of O&M.

4.2.2 Implementing SNSF outside of the BSC/RNC nodes

Deploying NNSF not in the BSC/RNC nodes but instead in standalone intermediary nodes as Serving Node Selection Function (SNSF) or co-locating with some other nodes as illustrated in figure 4.2.2.1, it will be much easier to resolve the problems captured in clause 4.2.1.
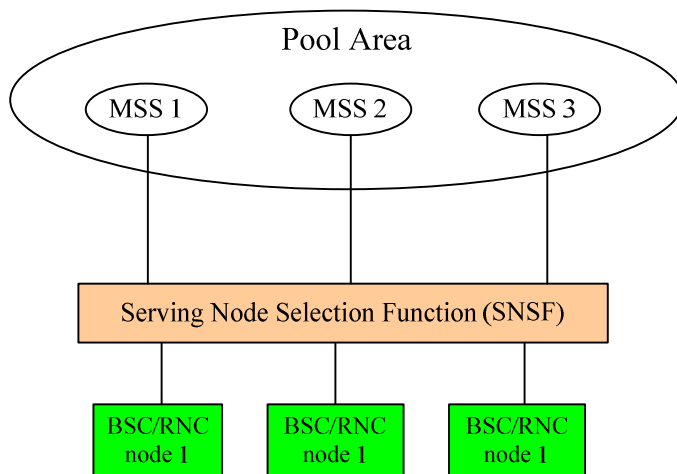
Figure 4.2.2.1: Deploying SNSF outside of the BSC/RNC nodes

The NAS Node Selection Function is as specified in TS 23.236 [2] to assign specific network resources (i.e. MSC or SGSN) to serve a mobile station and subsequently route the traffic to the assigned network resource. The NRI identifies the specific CN node. The Serving Node Selection Function (SNSF) is above the BSC/RNC nodes to provide similar functions with NNSF as specified in TS 23.236 [2], has a CN node address configured for the NRI derived from the initial NAS signalling message or from the LLC frame then this message or frame is routed to this address. If no CN

node address is configured for the derived NRI or if no NRI can be derived (e.g. the MS indicated an identity which contains no NRI) then the Serving Node Selection Function selects an available CN node (e.g. according to load balancing) and routes the message or LLC frame to the selected CN node.

4.2.3   Issues with deploying NNSF in BSC nodes for SGSN pool

In the progress of this study, there have been no contributions on the topic of SGSN Pool; as such, SGSN Pool is considered as being out of the scope of this feasibility study.

4.3   Load Balancing

The Serving Node Selection Function balances the signalling load between the available MSC Servers same as specified in clause 4.5 of TS 23.236 [2]. The load-balancing algorithm is implementation specific.

4.4   Load Re-Distribution

Signalling load re-distribution shall be performed as the procedures defined in clause 4.5a.1 of TS 23.236 [2] that the Serving Node Selection Function performs the same as the NAS Node Selection Function.

4.5   Mobility Management

No impacts upon mobility management result from the deployment of SNSF. See clause 4.6 of TS 23.236 [2].

4.6   Default CN node

No impacts to the default CN node concept result from the deployment of SNSF. See clause 4.7 of TS 23.236 [2].
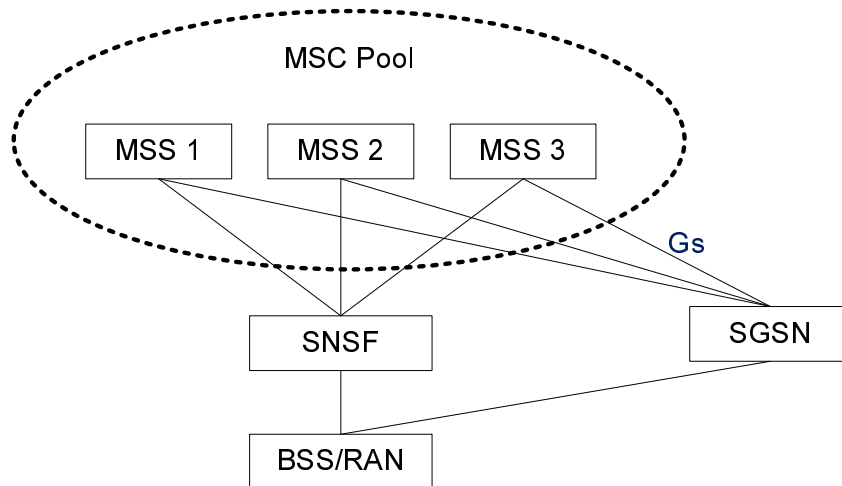
4.7   Support of combined mobility management procedures

No impacts to the support of combined mobility management procedures result from the deployment of SNSF. See clause 4.8 of TS 23.236 [2].

The configurations of the Gs interface are illustrated in figure 4.7-2.
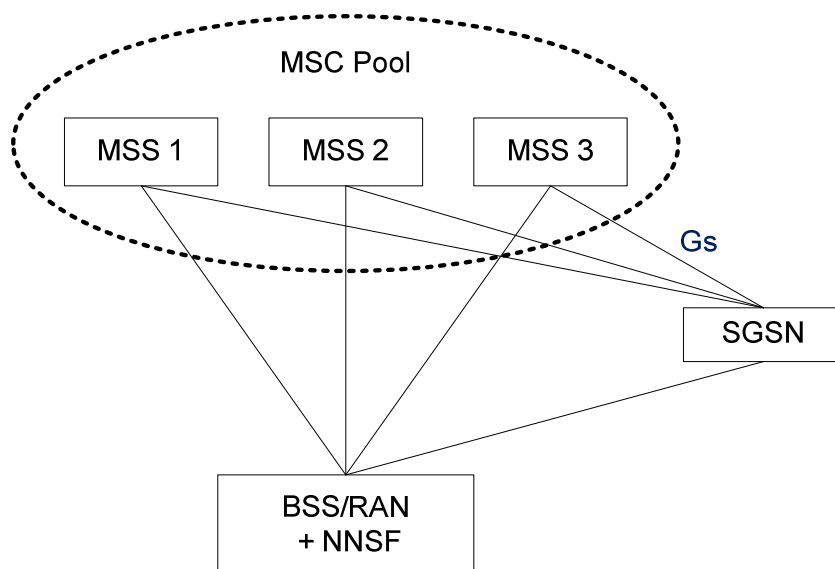
Deploying NNSF within the BSS/RAN nodes

Deploying SNSF above the BSS/RAN nodes

Figure 4.7-1: Network Model for using the combined mobility management

4.8   Re-use of A-Interface TDM circuits

The method of managing A-interface TDM circuits is independent with the feasibility study on deploying NNSF above the BSC/RNC nodes. The topic of re-use of A-Interface TDM circuits is considered as being out of the scope of this feasibility study.

4.9   Redundancy and failover

4.9.1   Redundancy and failover in signalling plane

The resilience of a network that is enabled for MSC Pool by means of the SNSF may be improved by the implementation of nodal redundancy and failover capabilities at the SNSF. Industry standard techniques that are specific to the transport type (e.g. SS7, IP) may be applied in order to achieve the objectives of SNSF redundancy and failover. These techniques typically imply:

1) real-time synchronization of transient data among multiple members of the redundancy set; and

2) automatic enabling of a back-up or standby member of the redundancy set when the active member fails.

The use of such techniques is intended to be transparent to the external nodes that communicate with the redundant node.

4.9.2   Redundancy and failover in user plane

The deployment of SNSF node above BSC/RNC has only impact on the control plane and has no impact on the redundancy and failover in the user plane.

5   Functional Description

5.1   MS function

The deployment of SNSF has no impact on the MS function. See clause 5.1 of TS 23.236 [2].

5.2   RNC Functions

The deployment of SNSF has no impact on the RNC functions, i.e. the RNC function does not provide the NAS Node Selection Function as specified in TS 23.236 [2].

5.3   BSC Functions

The deployment of SNSF has no impact on the BSC functions, i.e. the BSC function does not provide the NAS Node Selection Function as specified in clause 5.2 of TS 23.236 [2].

5.4   MSC Server Functions

In addition to the functions described in TS 23.236 [2], impacts to MSC Server functions due to the deployment of SNSF are described in clause 5.6 as summarized below:

- If SCCP Local Reference Based Handling of connection-oriented messages is applied, the MSC Server allocates the local SCCP reference which contains the local SNRI.

- If the solution of SNSF broadcasting TDM Circuit Management messages is applied, the MSC Server handles the received TDM Circuit Management message.

5.4a   MGW Functions

The deployment of SNSF above BSC/RNC places no requirement on the MGW.

NOTE: As an implementation option, SNSF may be co-located with MGW, and it does not create new requirements on the logical function of MGW.

5.5   SGSN Functions

The deployment of SNSF above BSC/RNC places no requirement on the SGSN.

NOTE: SGSN pools as specified in TS 23.236 [2] are not possible as SNSF does not provide the NNSF functionality for PS connections.

5.6   SNSF Functions

5.6.1   General

The SNSF node is used to select the specific MSC Server to which initial NAS signalling messages or LLC frames are routed. The NRI identifies the specific CN node. If the SNSF node has a CN node address configured for the NRI derived from the initial NAS signalling message, or from the LLC frame, then this message or frame is routed to this address. If no CN node address is configured for the derived NRI, or if no NRI can be derived (e.g. the MS indicated an identity which contains no NRI), then the SNSF node selects an available CN node (e.g. according to load balancing) and routes the message or LLC frame to the selected CN node.

The SNSF node derives the NRI from the TMSI when the MS is supported in either Iu-CS mode or A interface mode.

In A/Iu-CS mode, in the event that an MSS/VLR sends a paging-request/paging with IMSI (i.e. the paging message does not contain a TMSI), the SNSF node shall, upon reception, temporarily store the Global-CN-ID of the node that issued the paging-request/paging message. If the SNSF node in A/Iu-CS mode receives a paging-response with an IMSI, then it should check the temporarily stored Global-CN-ID on entries matching this IMSI, and forward the paging-response to the node identified by this Global-CN-ID.

All message sequence charts in the following clauses are examples and solutions may be implemented using different message sequences from what is illustrated here.

5.6.2   Handling of connection-oriented messages

5.6.2.1   Basic Handling of connection-oriented messages

On receipt the SCCP CR message from the BSC/RNC node, the SNSF node extracts the TMSI parameter from the layer-3 message and retrieves the NRI parameters from the TMSI, select and determine the CN node from the NRI parameter as per specified in clause 5.6.1 and distribute the message to the CN node as illustrated in figure 5.6.2.1.1. The layer-3 message in the SCCP CR message may be the Initial MS Message for the A interface mode or the Initial UE Message for the Iu mode.
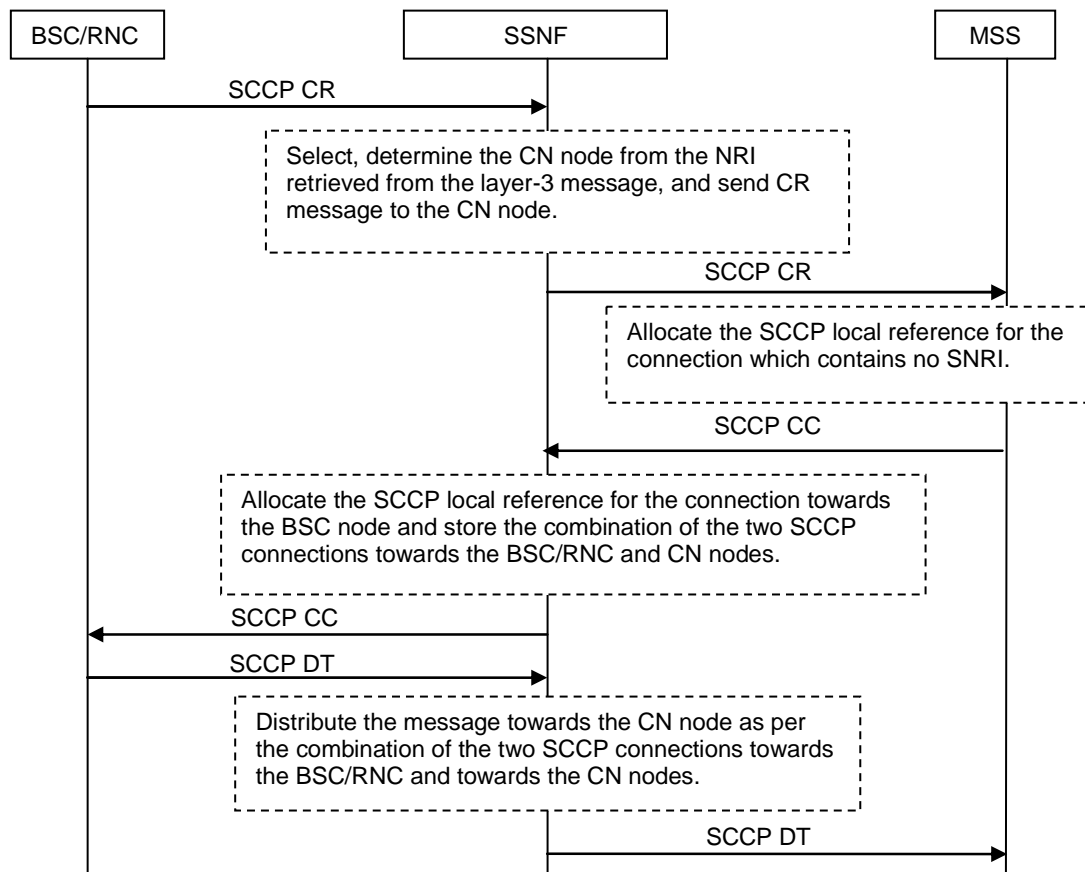

Figure 5.6.2.1.1: Service Flow for Basic Handling of connection-oriented messages

On receipt of the SCCP CC message from the MSS node, the SNSF node creates a local reference for the SCCP connection towards the BSC/RNC node and return SCCP CC message to the BSC/RNC node, and stores the combination of the two SCCP connections, one towards the BSC/RNC and one towards the MSS node.

For subsequent uplink and downlink messages, the SNSF node distributes the messages as per the combination of the two SCCP connections towards the BSC/RNC and the MSS nodes respectively, as illustrated in figure 5.6.2.1.1.

The SNSF node should only send SCCP Inactivity Test (IT) message towards the MSC Server on receipt of SCCP Inactivity Test (IT) message from the BSC/RNC node. The SNSF node shall not send SCCP Inactivity Test (IT) message towards the MSC Server if the corresponding SCCP connection towards the BSC/RNC node has been released. The SNSF node should only send SCCP Inactivity Test (IT) message towards the BSC/RNC node on receipt of SCCP Inactivity Test (IT) message from the MSC Server. And the SNSF node shall not send SCCP Inactivity Test (IT) message towards the BSC/RNC node if the corresponding SCCP connection towards the MSC Server has been released.

NOTE: On failure of receiving SCCP Inactivity Test (IT) message from the peer side (i.e. the SNSF node), the MSC Server and the BSC/RNC node will release the resources related to the SCCP connection.

5.6.2.2 SCCP Local Reference Based Handling of connection-oriented messages

Similar with distribute message as per the NRI parameter derived from the TMSI, SCCP Network Resource Identifier (SNRI) may be configured as several digits out of the SCCP local reference for identifying the MSC Server as illustrated in figure 5.6.2.2.1.
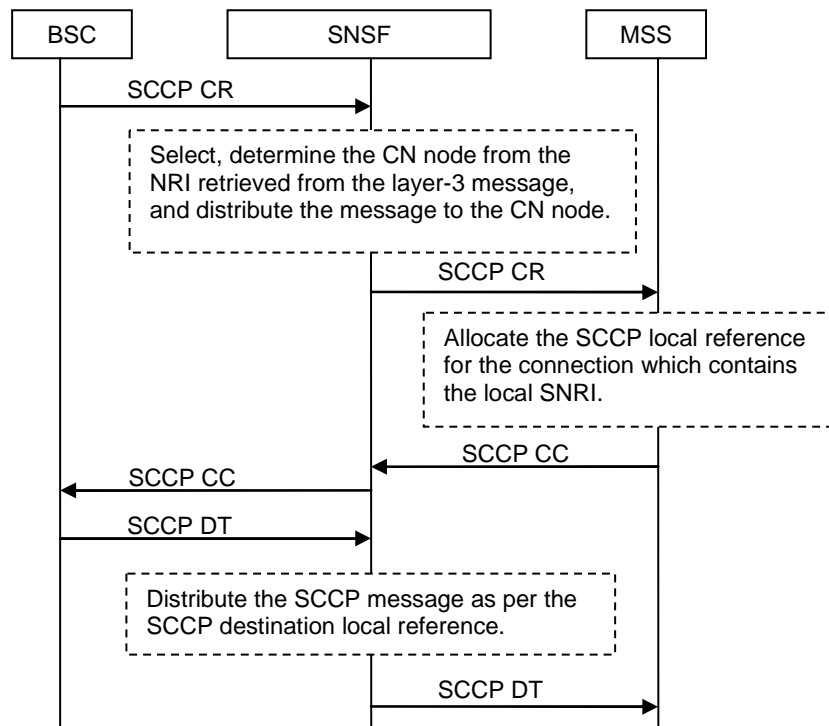

Figure 5.6.2.2.1: SNRI based distribution of uplink messages (SCCP connection established by the RAN)

On receipt of the initial SCCP CR message, the SNSF retrieves the NRI parameter from the TMSI from the layer 3 message and selects the MSC Server as specified in clause 5.6.1 and distribute the message to the destination MSC Server. The layer-3 message in the SCCP CR message may be the Initial MS Message for the A interface mode or the Initial UE Message for the Iu mode.

On receipt of the initial SCCP CR message, the MSC Server allocates the SCCP local reference for the connection which contains the local SCCP Network Resource Identifier (SNRI) as configured for the MSC Server, and returns the local reference by the source local reference to the BSC through the SNSF. The SNSF routes the message towards the BSC/RNC node as per the destination signalling point code retrieved from the SCCP CC message.

For subsequent uplink messages, the SNSF retrieves the SNRI parameter from the destination local reference and distributes the message as per the SNRI parameter. For subsequent downlink messages, the SNSF routes the message towards the BSC/RNC node as per the destination signalling point code retrieved from the SCCP message.

The SNSF shall not generate SCCP Inactivity Test (IT) messages by its own, but shall route uplink and downlink SCCP Inactivity Test (IT) messages as specified above for subsequent uplink and downlink messages.

  NOTE: On failure of receiving SCCP Inactivity Test (IT) message from the peer side (i.e. the SNSF), the MSC Server and the BSC/RNC node will release the resources related to the SCCP connection.

In this approach, the SNSF does not need to store or handle states of the SCCP connections established between the RAN node and the MSC server. SCCP messages for the same call may be distributed via different SNSFs (e.g. upon the failure of an SNSF).

The principles specified in this clause for SNRI based distribution of uplink connection oriented messages are also applicable to scenarios where the SCCP connection is established by the MSC Server, e.g. Handover Request procedure. In those scenarios, the MSC Server allocates and includes the SNRI within the SCCP local reference in the SCCP CR message (see figure 5.6.2.2.2). The SNSF distributes the SCCP CC message and subsequent uplink connection oriented messages as per the SCCP destination local reference.
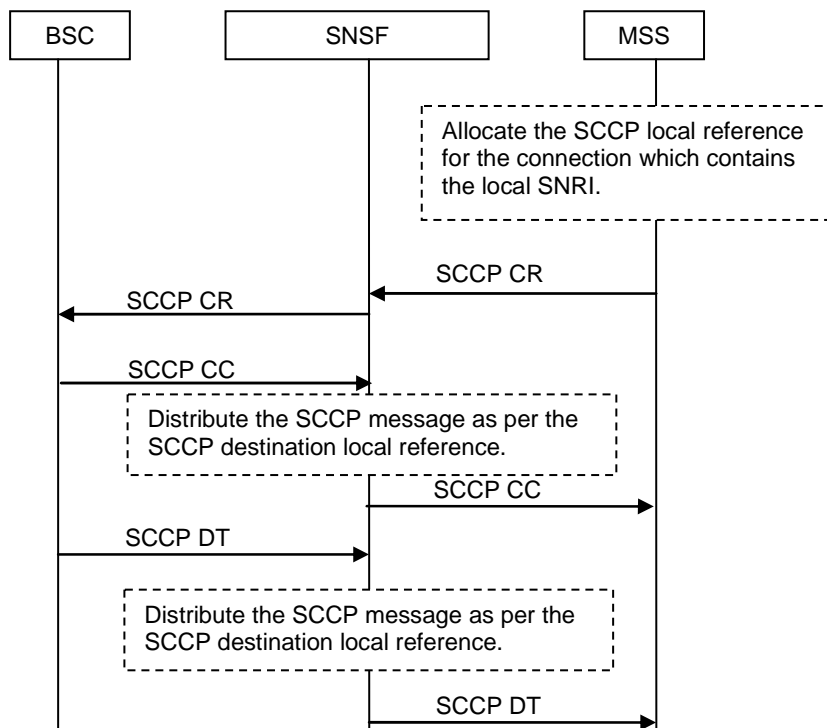
**Figure 5.6.2.2.2: SNRI based distribution of uplink messages
(SCCP connection established by the MSC Server)**

Basic configuration needed for one pool:

- For an MSC pool, the range of the SNRI bits out of the SCCP local reference shall be the same for SNSFs and MSC Servers. This range shall be configurable in SNSFs and MSC servers.

- The mapping from the SNRI to the MSC Servers shall follow the configuration in the MSC Servers.

- the SNRI should contain at most 5 bits (this allows the pool to contain up to 32 MSC Servers without impacting the maximum number of calls an MSC Server may support).

A sample of the range of the SNRI bits out of local reference in the CN side is illustrated in figure 5.6.2.2.

23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
				SNRI range																			

Figure 5.6.2.2: A sample of the range of the SNRI bits out of local reference in the CN side

NOTE: The configurations of NRI and SNRI are irrelative. With the nature both NRI and SNRI identifies the MSC Server, the two sets of identifiers may be unified or one set can be map to another one (e.g. several NRI map to one SNRI).

5.6.3 Handling of connectionless messages

Service flows are described in this clause for the BSSAP/RANAP connectionless messages.

5.6.3.1 UTRAN

5.6.3.1.1 Reset

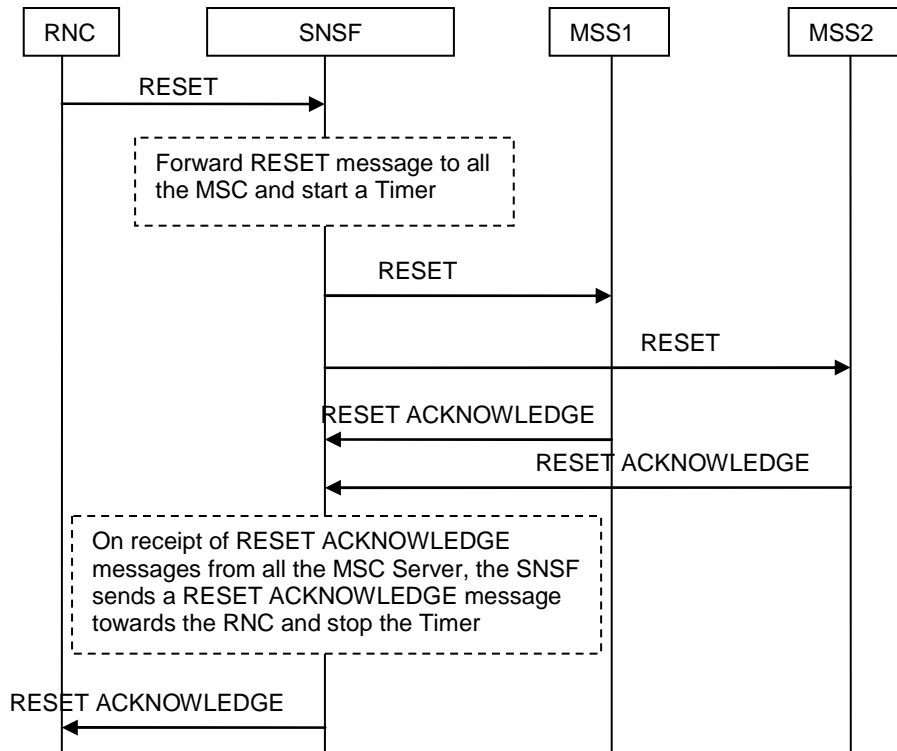##### 5.6.3.1.1.1 UTRAN Initiated RESET

Figure 5.6.3.1.1.1.1: UTRAN initiated RESET procedure

In the event of a failure at the UTRAN which has resulted in the loss of transaction reference information, a RESET message shall be sent to all MSC Servers towards which the RNC has Iu signalling connections established. This message is used by the MSC Server to release affected Radio Access Bearers and to erase all affected references for the sending RNC.

On receipt of the RNC initiated RESET message, the SNSF node forward the RESET message to all the MSC Servers and starts a Timer to waiting for the RESET ACKNOWLEDGE from the MSC Server. On receipt of the RESET ACKNOWLEDGE messages from all the MSC Server, the SNSF node sends a RESET ACKNOWLEDGE message towards the RNC and stops the Timer. If the Timer fires and the SNSF node has not received RESET ACKNOWLEDGE messages from all the MSC Servers, the SNSF node stops the timer and the RNC may re-send the RESET message as defined in clause 8.26.3.2 of TS 25.413 [3].
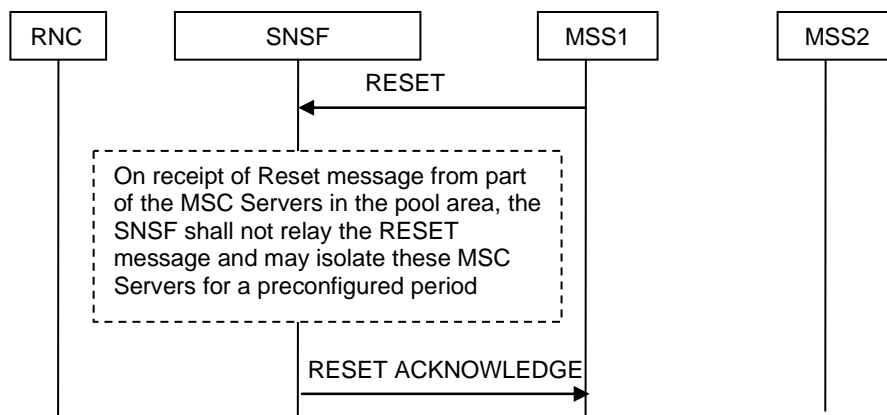
5.6.3.1.1.2 CN Initiated RESET

Figure 5.6.3.1.1.2.1: RESET procedure initiated from part of the MSC Servers

According to TS 25.413 [3], in the event of a failure at the CN, which has resulted in the loss of transaction reference information, a RESET message shall be sent to the RNC. On receipt of the RESET message, the UTRAN releases affected Radio Access Bearers and clears all the affected references.

The RNC should normally have Radio Access Bearers and Iu resources that are handled by other MSC Servers of the pool, and these resources shall not be released while resources handled by the resetting MSC Server should normally be released.

Based on that, the SNSF shall not relay towards the RNC the RESET message which is received from only part of the MSC Servers, and may isolate the MSC Servers for a preconfigured period. During that period, the SNSF does not transfer any message towards the isolated MSC Server. The affected Radio Access Bearers and the affected references with the isolated MSC Server will be release during the isolation period by some mechanisms, e.g. by the subscriber hanging up the call or by the SCCP Inactivity Test procedure. The SNSF shall then return a RESET ACKNOWLEDGE message to the resetting MSC.

NOTE 1: ITU-T Recommendation Q.714 [6] defines a range from 11 to 21 minutes for the SCCP T(iar) timer; in practice, all the calls should be released within few tens of seconds by subscribers hanging up the call.

NOTE 2: Immediately returning a RESET ACKNOWLEDGE message to the MSC Server without any isolation period prevents failure of subsequent mobile terminated calls or signalling (e.g. Short Message), as well as possible unbalanced load distribution on the MSC Servers of the pool. E.g. subscribers affected by the resetting MSC Server will hang up and re-establish a new call immediately, which will lead the SNSF to re-allocate the subscribers to other MSC Servers of the pool if the resetting MSC Server is isolated.

NOTE 3: Without an isolation period, the MSC Server may allocate to new calls an Iu signalling connection not yet freed in the RNC for earlier calls. This is not a concern if the RNC accepts the new call and releases the old call in that circumstances.

If the SNSF received RESET messages from all the MSC Servers towards a RNC node within the MSC Pool Area during the period of the isolation, the SNSF may send a RESET message to the destination RNC. On receipt of the RESET ACKNOWLEDGE message from the RNC, the SNSF forwards the RESET ACKNOWLEDGE message to all the MSC Servers.
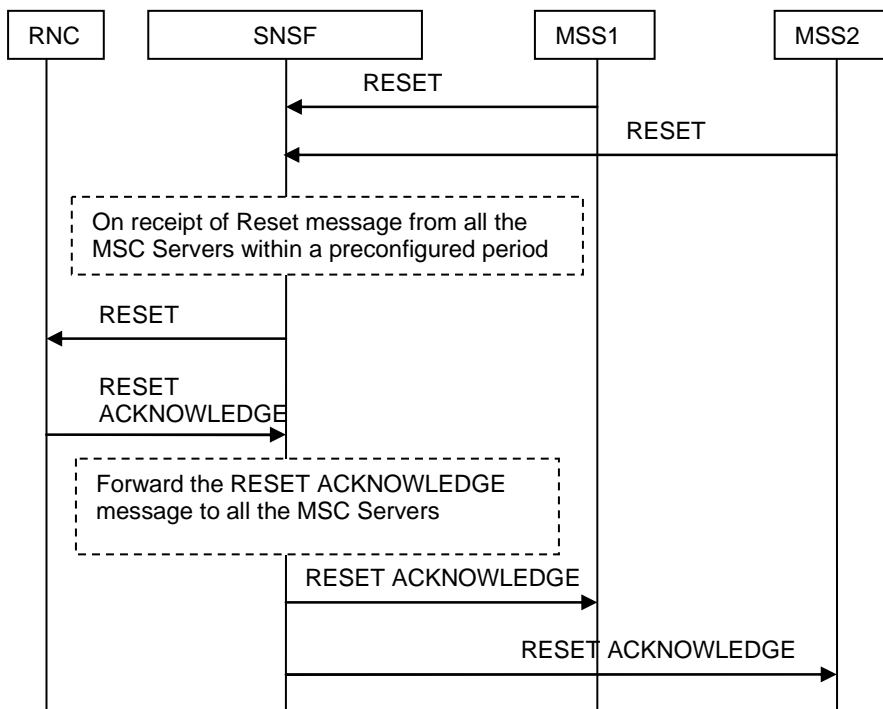
Figure 5.6.3.1.1.2.2: RESET procedure initiated from all the MSC Servers

NOTE 4: If a RNC connects with multiple SNSFs, the MSC Servers shall be configured to one of the SNSFs that the MSC Servers shall send the RESET messages to. The MSC Servers should only send the RESET message to the preconfigured SNSF when the RESET procedure is initiated towards the RNC.

NOTE 5: Since it is unlikely that all the MSC Servers of the pool reset at the same time (i.e. during the same short period), an SNSF can handle this scenario as it handles RESET initiated by part of the MSC Servers of the pool.

5.6.3.1.2 Overload Control

The Overload Control procedure is defined to give some degree of signalling flow control according to TS 25.413 [3]. See clause 8.25 of TS 25.413 [3] for detail of the philosophy and the algorithm used.

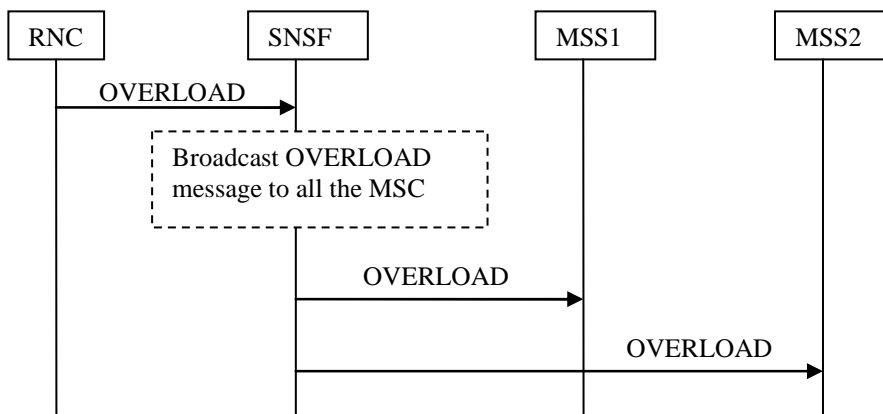#### 5.6.3.1.2.1 UTRAN Initiated Overload Control

Figure 5.6.3.1.2.1.1: Overload at the UTRAN

If the UTRAN is overloaded, it will send an OVERLOAD message towards the MSC Servers which the RNC node connects with. On receipt of the RNC initiated OVERLOAD message, the SNSF node should broadcast this message to all the MSC Servers.

5.6.3.1.2.2   CN Initiated Overload Control

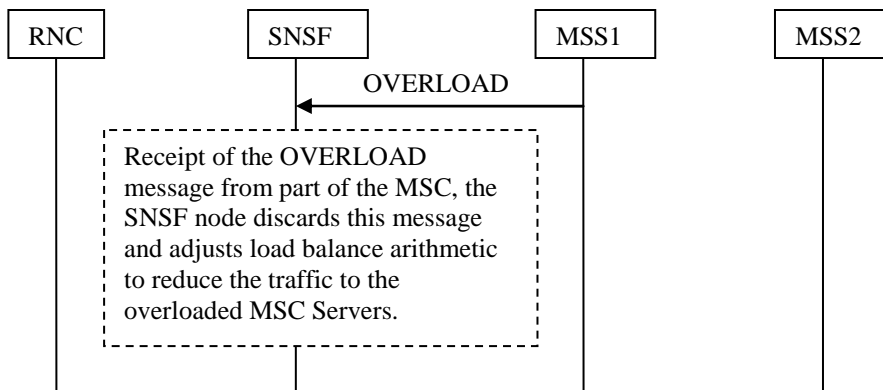5.6.3.1.2.2.1   Overload at parts of the MSC Servers

Figure 5.6.3.1.2.2.1.1: Overload at parts of the MSC Servers

The MSC Server should indicate to the RNC that it is in a congested state by sending an OVERLOAD message. On reception of the message, the UTRAN should cause reduction of signalling traffic towards the MSC Server. When the SNSF is deployed above the UTRAN, if only part of the MSC Servers are in a congested state, the OVERLOAD message should not be sent to the RNC nodes, otherwise, the RNC will reduce signalling traffic towards all the MSC Servers. The SNSF node should adjusts load balance arithmetic to reduce congested MSC Server traffic and add other normal MSC Server traffic.

5.6.3.1.2.2.2   Overload at all the MSC Servers
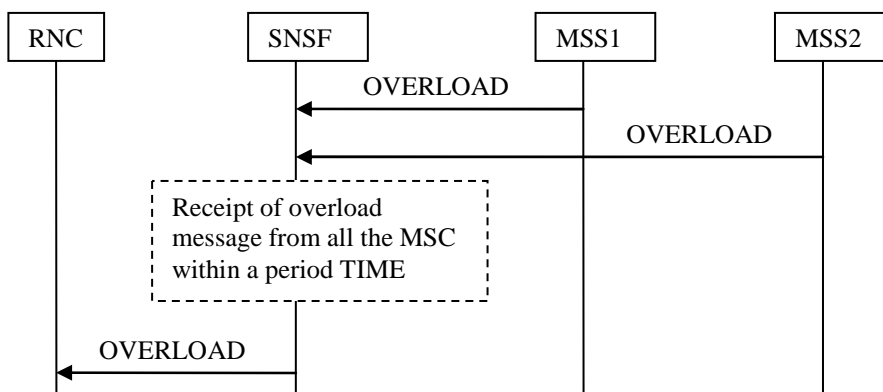
Figure 5.6.3.1.2.2.2.1: Overload at all of the CN

On receipt of all OVERLOAD messages from all the MSC Servers within a period TIMER (the TIMER is configurable with operator's decision), the SNSF node relays one of the received OVERLOAD messages to the destination RNC node. On reception of the message, the UTRAN will reduce signalling traffic towards the CN.

NOTE: If an RNC node connects with multiple SNSF nodes, the MSC Servers shall be configured to one of the SNSF nodes that the MSC Servers shall send the OVERLOAD messages to. The MSC Servers should only send the OVERLOAD message to the preconfigured SNSF node when the OVERLOAD procedure is initiated towards the RNC.

5.6.3.1.3 Reset Resource

5.6.3.1.3.1 UTRAN Initiated Reset Resource

Figure 5.6.3.1.1.2.1: UTRAN initiated RESET RESOURCE procedure
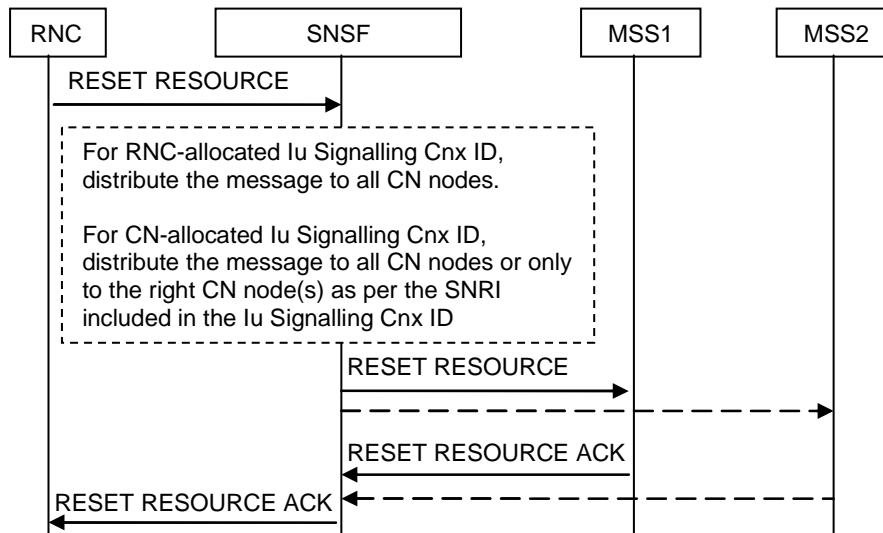
According to TS 25.413 [3], in the event of an abnormal failure, the RNC may send a RESET RESOURCE message (including the list of Iu Signalling Connection Identifiers) to release the corresponding CN resources.

The Iu Signalling Connection Identifiers may have been allocated by the RNC or the MSC Server.

The MSC Server should include the SNRI in the Iu signalling connection ID it allocates.

Upon receipt of a RESET RESOURCE message from the RNC, the SNSF should broadcast the RESET RESOURCE message including RNC-initiated or/and MSC-initiated Iu Signalling Connection Ids to all MSC Servers. At the expiration of a guard timer, the SNSF returns a RESET RESOURCE ACK to the RNC.

As an implementation option, the SNSF may distribute a RESET RESOURCE message including only MSC-initiated Iu Signalling Connection Ids only to the right MSC Server(s) using the SRNI contained within the Iu Signalling Connection Ids.

In this approach, the SNSF does not need to store call related information.

NOTE: Including the SNRI in an MSC-initiated Iu signalling connection ID enables the SNSF to route the RESET RESOURCE message to the right MSC Server(s), but also the MSC Servers to recognize their own MSC-initiated Iu signalling connection Ids if the RESET RESOURCE message is distributed to all MSC Servers.

5.6.3.1.3.2 CN Initiated Reset Resource

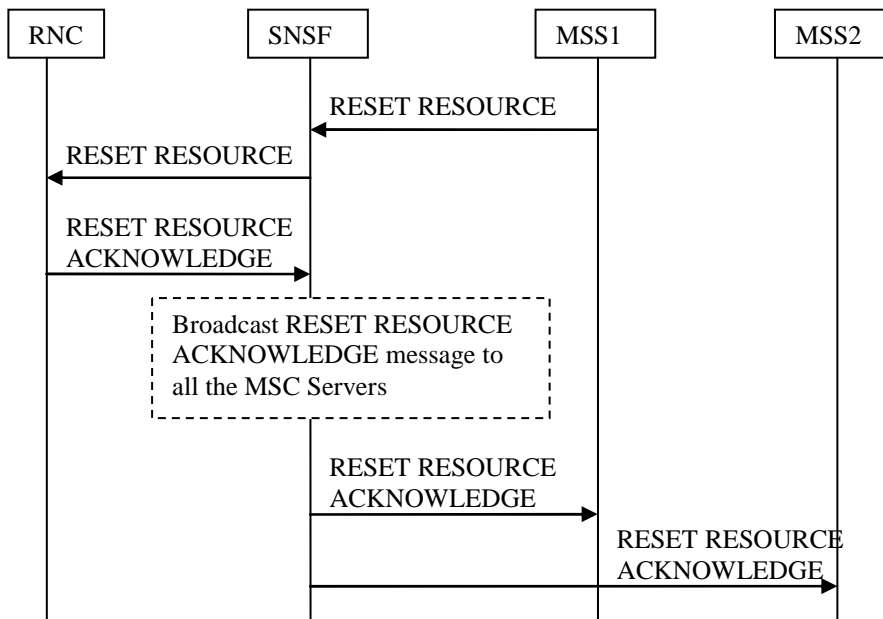5.6.3.1.3.2.1 Alternative 1: Broadcast Based

Figure 5.6.3.1.3.2.1.1: MSC Server initiated Reset Resource Procedure

The MSC Server initiates the procedure by sending a RESET RESOURCE message to the RNC. On receipt of the MSC RESET RESOURCE message, the SNSF node transfers this message to the destination RNC.

On reception of this message the RNC shall release the local resources and references (i.e. radio resources and Iu signalling connection identifiers) associated to the specific MSC Server and Iu signalling connection identifiers indicated in the received message. The RNC shall always return the RESET RESOURCE ACKNOWLEDGE message to the MSC Server when all Iu-related resources and references have been released. On receipt of the RNC RESET RESOURCE ACKNOWLEDGE message, the SNSF node broadcasts this message to all the MSC Servers. The MSC Servers shall ignore the RESET RESOURCE ACKNOWLEDGE message if no corresponding pending RESET RESOURCE procedures are matched locally.

5.6.3.1.3.2.2 Alternative 2: Mapping RESET to RESET Resource

For RANAP RESET message from MSC-S, the handling is similar to BSSAP as described in clause 5.6.3.2.1.2.2 but instead of mapping the RESET to RESET Circuit including CIC, the SNSF maps the RESET from MSC-S to RESET Resource message including the Iu Signalling Connection Identifier.

5.6.3.1.4 ERROR INDICATION

5.6.3.1.4.1 UTRAN Initiated Error Indication
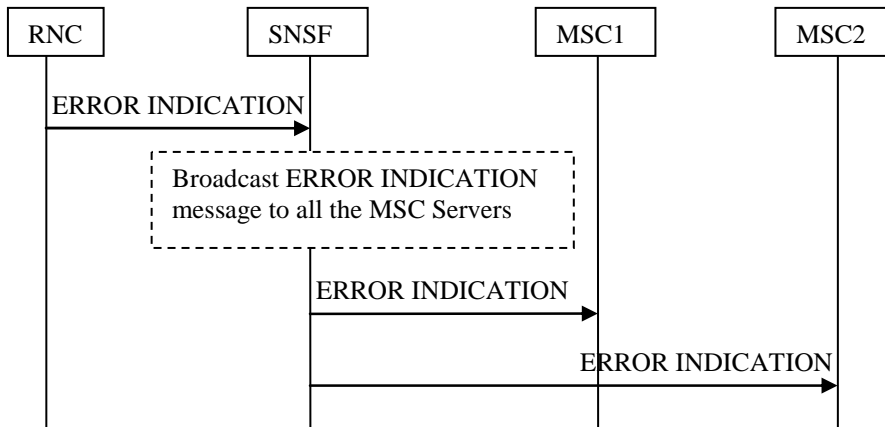
Figure 5.6.3.1.4.1.1: Error Indication procedure, RNC originated

The Error Indication procedure is initiated by an RNC node to report detected errors in one incoming message, provided they cannot be reported by an appropriate failure message. On receipt of the RNC ERROR INDICATION message, the SNSF broadcasts this message to all the MSC Servers in the Pool Area.

5.6.3.1.4.2 CN Initiated Error Indication

Figure 5.6.3.1.4.2.1: CN initiated Error Indication procedure

On receipt of the MSC Server initiated ERROR INDICATION message, the SNSF transfers this message to the destination RNC as per the destination Signalling Point Code received from the MSC Server.

5.6.3.1.5 INFORMATION TRANSFER

Figure 5.6.3.1.5.1: Information Transfer Procedure

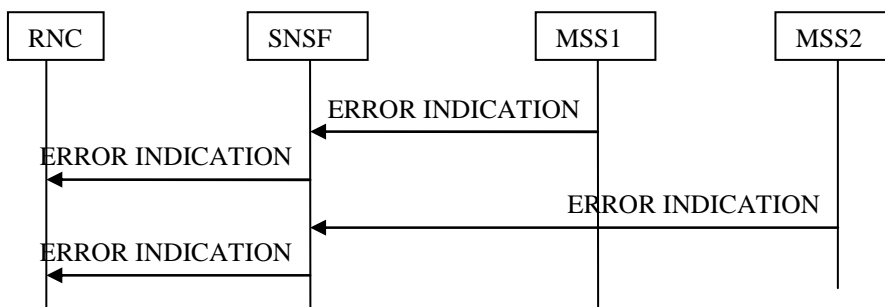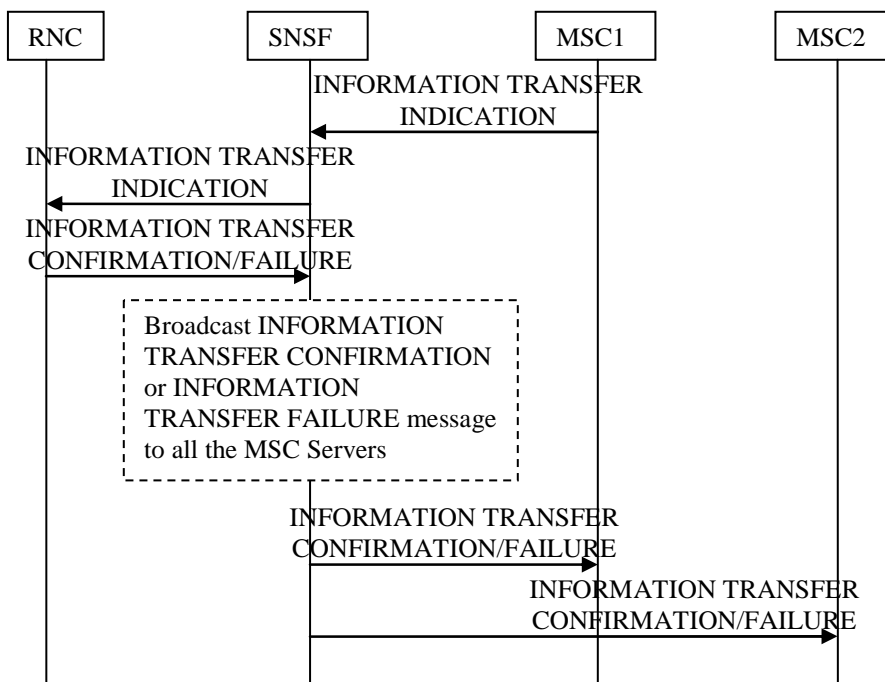On receipt of the MSC INFORMATION TRANSFER INDICATION message, the SNSF transfers this message to the destination RNC. On receipt of INFORMATION TRANSFER CONFIRMATION or INFORMATION TRANSFER FAILURE message from the RNC, the SNSF broadcasts this message to all the MSC Servers in the Pool Area. The MSC Server shall ignore this message if no corresponding pending Information Transfer procedures are matched locally by checking if the *Information Transfer ID* is allocated locally.

5.6.3.1.6 Direct Information Transfer

5.6.3.1.6.1 UTRAN Initiated Direct Information Transfer

Figure 5.6.3.1.6.1.1: Direct Information Transfer initiated from the RNC

The purpose of the Direct Information Transfer procedure is to transfer some information from the RNC to the CN. The procedure is initiated with a DIRECT INFORMATION TRANSFER message sent from the RNC to the CN. On receipt of the RNC DIRECT INFORMATION TRANSFER message, the SNSF broadcasts this message to all the MSC Servers in the Pool Area.

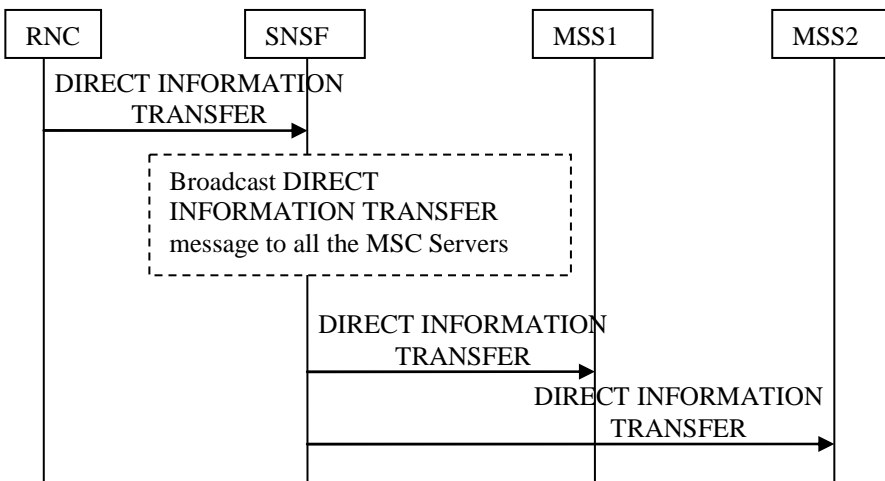5.6.3.1.6.2   CN Initiated Direct Information Transfer
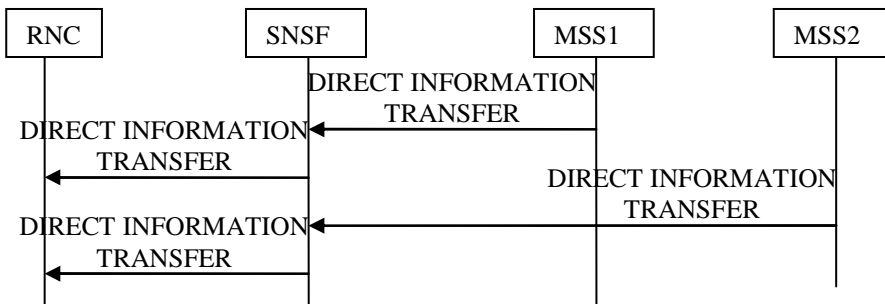
Figure 5.6.3.1.6.2.1: Direct Information Transfer initiated from the CN

The purpose of the Direct Information Transfer procedure is to transfer some information from the CN to the RNC. The procedure is initiated with a DIRECT INFORMATION TRANSFER message sent from the CN to the RNC. On receipt of the MSC DIRECT INFORMATION TRANSFER message, the SNSF transfers this message to the destination RNC.

5.6.3.1.7   Uplink Information Exchange
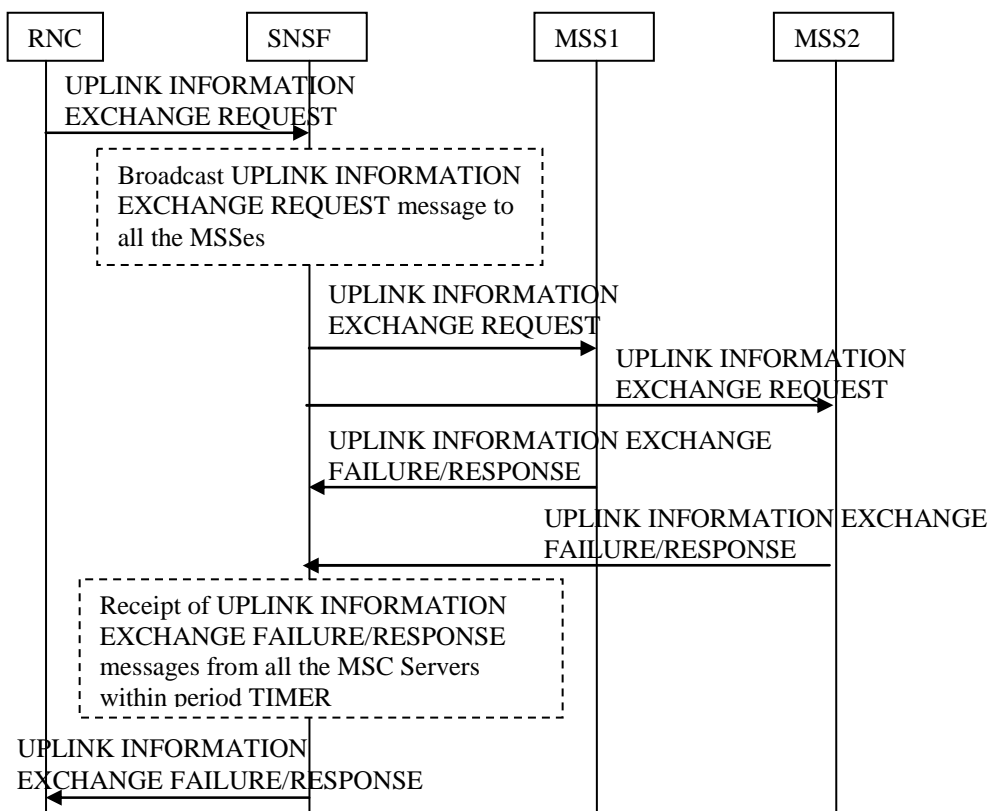
Figure 5.6.3.1.7.2: Uplink Information Exchange procedure

On receipt of the RNC UPLINK INFORMATION EXCHANGE REQUEST message, the SNSF broadcasts the message to all the MSC Servers in the Pool Area. On receipt of an MSC UPLINK INFORMATION EXCHANGE FAILURE/RESPONSE message from all the MSC Servers in the Pool Area within a period TIMER (where TIMER is an operator matter), the SNSF transfers the latest UPLINK INFORMATION EXCHANGE FAILURE/RESPONSE message to the destination RNC.

5.6.3.1.8   Paging

5.6.3.1.8.1   Paging when RNC connects with one SNSF node
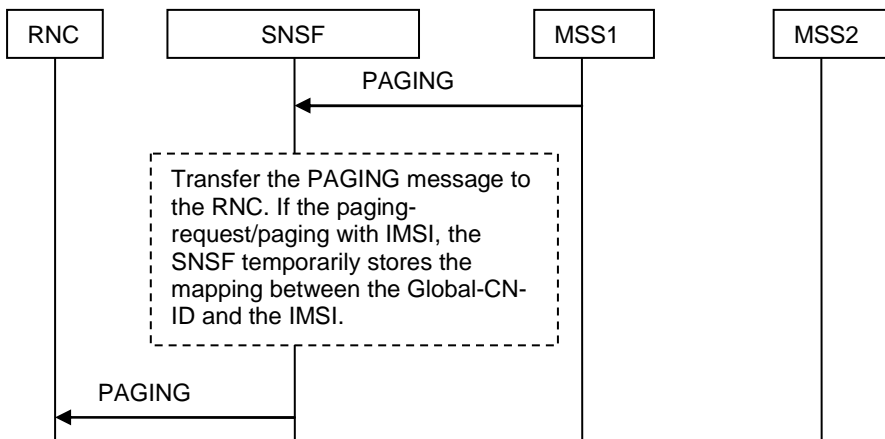
Figure 5.6.3.1.8.1.1: Paging procedure. RNC connect with one SNSF node

On receipt of the PAGING message, the SNSF node transfers this message to the destination RNC.

5.6.3.1.8.2   Paging with TMSI when RNC connects with multiple SNSF nodes

Figure 5.6.3.1.8.2.1: the paging-request/paging with TMSI procedure. RNC connect multiple SNSF nodes

On receipt of the PAGING message, if the paging type is TMSI paging, the SNSF node transfers this message to the destination RNC.

5.6.3.1.8.3   Paging with IMSI when RNC connects with multiple SNSF nodes

Figure 5.6.3.1.8.3.1: Procedure for Paging with IMSI (RNC connects to multiple SNSF nodes)

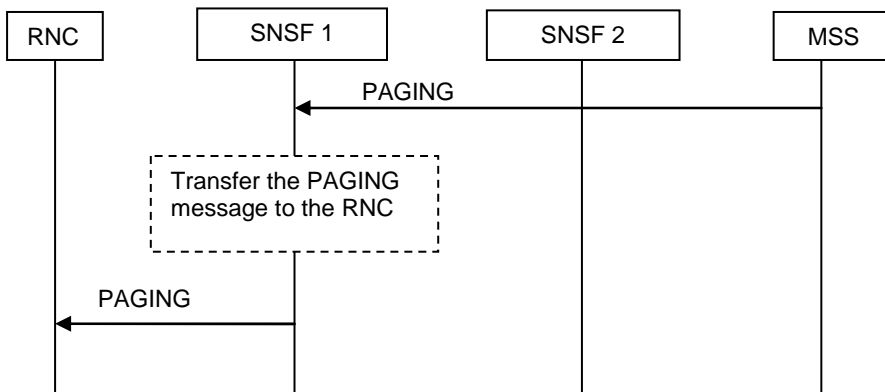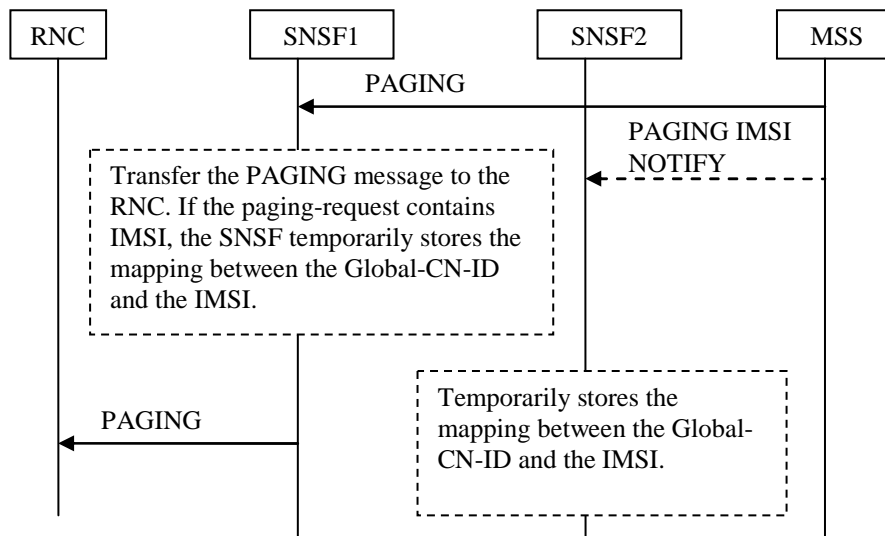On receipt of the PAGING message, the SNSF transfers this message to the destination RNC. In case the PAGING message contains IMSI, the SNSF temporarily stores the mapping between the Global-CN-ID of the node that issued the paging message and the IMSI.

If the MSS connects with multiple SNSF nodes, the PAGING IMSI NOTIFY message should be sent to the other SNSF nodes in the Pool Area, and all these SNSF nodes should temporarily store the mapping between the Global-CN-ID of the node that issued the paging message and the IMSI.

NOTE 1:   The Paging response message may be reported via an SNSF node other than the one that received the original PAGING request message. To ensure that all SNSF nodes are able to route the PAGING response message correctly, it is proposed to notify the other SNSF nodes by means of the PAGING IMSI NOTIFY message.

NOTE 2:   The PAGING_IMSI_NOTIFY message may be a RANAP message and an option whether it needs to be sent or not. It is implementation specific how this may be done.

5.6.3.2   GSM

5.6.3.2.1   Reset

5.6.3.2.1.1   GERAN Initiated RESET

The procedure is similar to the procedure specified in clause 5.6.3.1.1.1, with the following differences according to TS 48.008 [5]:

-    A RESET message is used by the BSS to indicate the MSC Server to release affected calls and erase all affected references and to put all circuits into the idle state;

-    Upon receipt of a RESET message from BSS, the MSC Server that does not allocate the circuits send block messages (BLOCK or CIRCUIT GROUP BLOCK) for all circuits that were previously locally blocked on the MSC Server side;

On receipt of the RESET message from the BSS via the SNSF, the MSC Server will release the affected calls and circuits, and will initiate BLOCK or CIRCUIT GROUP BLOCK procedures for circuits locally blocked on the MSC Server side as per TS 48.008 [5].

5.6.3.2.1.2 CN Initiated RESET

5.6.3.2.1.2.1 Alternative -1: Broadcast Based

The procedure is similar to the procedure specified in clause 5.6.3.1.1.2, with the following differences: according to TS 48.008 [5],

- A RESET message is used by the BSS to release affected calls and erase all affected references and to put all circuits into the idle state;

- Upon receipt of a RESET message from the MSC a BSS that does not allocate the circuits send block messages (BLOCK or CIRCUIT GROUP BLOCK) for all circuits that were previously locally blocked on the BSS side;

Since the SNSF will not pass the RESET message to the BSC (at least when part of the MSC Servers only are resetting), the BSC will not release the affected calls and circuits, and will not initiate any BLOCK or CIRCUIT GROUP BLOCK procedures for circuits locally blocked on the BSS side.

As a consequence, the BSS may not be able to use the terrestrial resource that the reset MSC Server indicates for subsequent call establishments or handovers:

- If the MSC indicates a circuit not yet released, the BSC will return an ASSIGNMENT FAILURE or HANDOVER FAILURE message with the cause set to "terrestrial resource already allocated";

- If the MSC indicates a circuit locally blocked on the BSS side, the BSC will return an ASSIGNMENT FAILURE or HANDOVER FAILURE message with the cause "requested terrestrial resource unavailable" and send a single global BLOCK message for that concerned terrestrial circuit.

The MSC may initiate a new assignment procedure using a new terrestrial resource.

NOTE: Without an isolation period, the MSC Server may allocate to new calls an AoIP Call Identifier not yet freed in the BSC for earlier calls. This is not a concern if the BSC accepts the new call and releases the old call in that circumstances.

5.6.3.2.1.2.2 Alternative -2: Mapping RESET to RESET Circuit

When a Reset message from an MSC-S is received in the SNSF (which forwards to BSC), this indicates to the BSC that all circuits controlled by that MSC-S have to be reset. However, since all the circuits from the BSC are distributed among the MSC-S's in the pool, the sending of a Reset message to the BSC would cause reset of calls to the other MSC-S's.

A Reset message received from an MSC-S is mapped to dedicated Reset Circuit messages towards the BSC's, see Figure 5.6.3.2.1.2.2.1 below.

However the Reset Circuit releases all the sessions which have TDM circuit connected.

The SNSF has supervision timers in order to supervise the responses from the BSC and the MSC-S, these are required for a fault tolerant implementation.
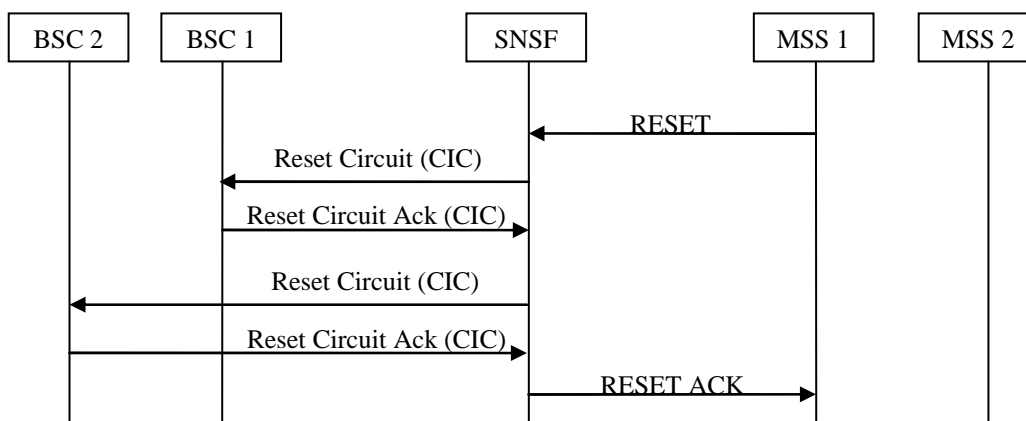

Figure 5.6.3.2.1.2.2.1:: RESET procedure initiated from part of the MSC Servers-Alt 2

NOTE: This solution applies to single SNSF scenario.

5.6.3.2.2 Overload

The procedure is similar to the procedure specified in clause 5.6.3.1.2, with the "BSC" replacing the "RNC".

5.6.3.2.3 Reset IP Resource

The procedure is similar to the procedure specified in clause 5.6.3.1.3.1, with the "AoIP Call Identifier" replacing the "Iu Signalling Connection Id" and the BSSAP "RESET IP RESOURCE" message replacing the RANAP "RESET RESOURCE" message.

Since the AoIP Call Identifiers are always allocated by the MSC, the SNSF may distribute the RESET IP RESOURCE messages only to the right MSC Servers.

5.6.3.2.4 Paging

Same as Paging procedure for RANAP (See clause 5.6.3.1.8).

5.6.3.2.5 Resource Request
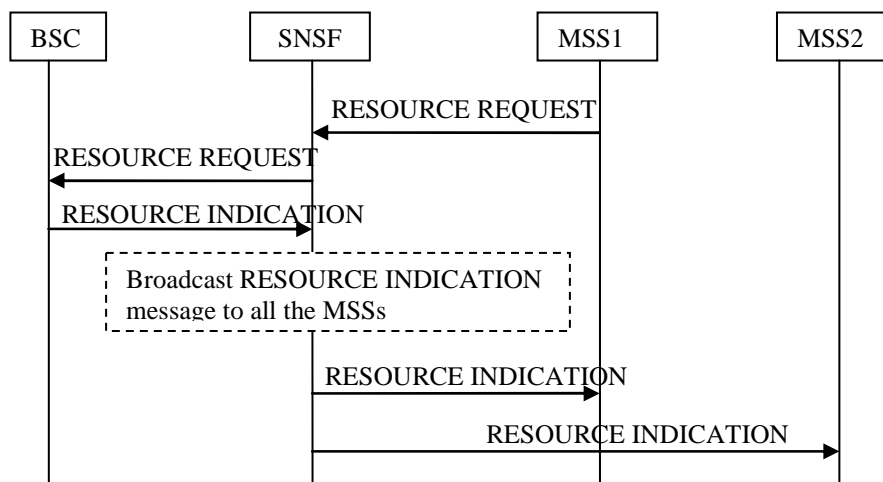
Figure 5.6.3.2.5.1: Resource Request Procedure

The RESOURCE REQUEST message is sent from the MSC to the BSS and requests the current spare and optionally the total accessible resource on a particular cell. On receipt of the RESOURCE REQUEST message, the SNSF node transfers this message to the destination BSC.

The RESOURCE INDICATION message is sent from the BSS to the MSC in response to a resource request message, the message includes an explicit indication of the cell concerned. On receipt of the RESOURCE INDICATION message, the SNSF node broadcast the message to all the MSC Servers. The MSC Servers which do not sent RESOURCE REQUEST message should ignore RESOURCE INDICATION message. The MSC Servers shall ignore the message if no corresponding pending RESOURCE REQUEST procedures are matched locally.

5.6.3.2.6 Handover Candidate Enquire

Figure 5.6.3.2.6.1: Handover Candidate Enquire Procedure

The purpose of this procedure is to allow the MSC Server to ascertain if it is possible to handover any MSs that are currently being served by a particular cell to another nominated cell.

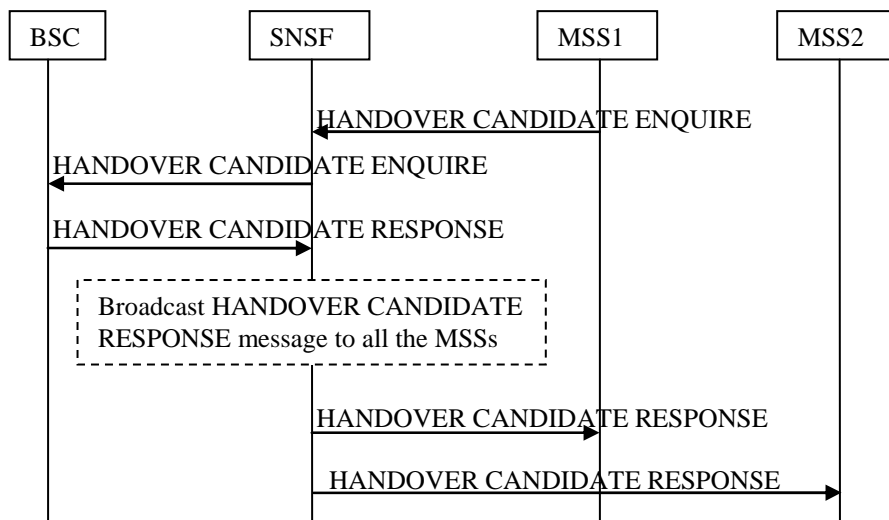The MSC Server sends a HANDOVER CANDIDATE ENQUIRE message towards a BSS. On receipt of the HANDOVER CANDIDATE ENQUIRE message, the SNSF node transfers this message to the destination BSC.

On receipt of the HANDOVER CANDIDATE RESPONSE message, the SNSF node broadcasts the response message to all the MSC Servers. Only the MSC Server that sends the HANDOVER CANDIDATE ENQUIRE message will handle the response message. The other MSC Servers in the Pool Area shall ignore the response message per procedures specified in TS 48.008 [5].

5.6.3.2.7 Confusion

This message is sent in either direction in response to a message which cannot be treated correctly for some reason, and for which another failure message cannot substitute. The use of this message may be under operator control.
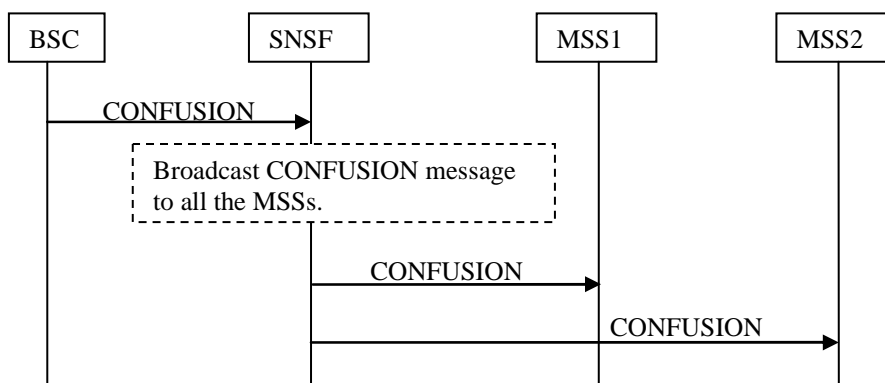
5.6.3.2.7.1 Confusion from the BSS

Figure 5.6.3.2.7.1.1: Confusion procedure, BSC originated

The CONFUSION message is sent from the BSC to the MSC Server. On receipt of the BSC CONFUSION message, the SNSF node broadcasts this message to all the MSC Servers.
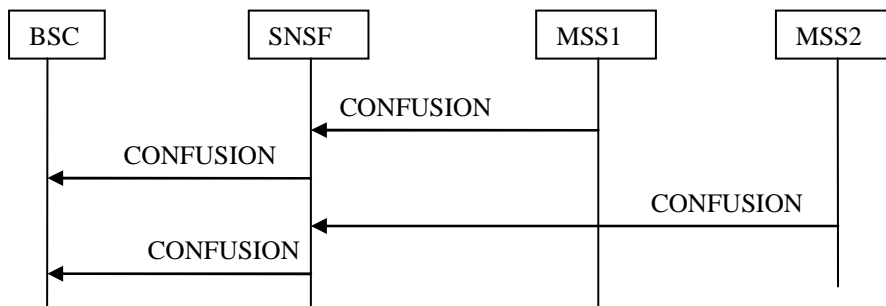
5.6.3.2.7.2 Confusion from the CN

Figure 5.6.3.2.7.2.1: Confusion procedure, CN originated

The CONFUSION message is sent from the MSC to the BSC. On receipt of the MSC Server initiated CONFUSION message, the SNSF node transfers the message to the destination BSC.

5.6.3.2.8 Load Indication

The purpose of the load indication procedure is to inform all neighbour BSS's about the traffic situation of a cell.

The philosophy is to control the incoming handover traffic at the source, i.e. the BSS of the concerned cell informs all its neighbour BSSs about the load situation. This is achieved by sending a LOAD INDICATION message to the neighbour BSSs. On receipt of the LOAD INDICATION message the BSS may analyse the load information and take the traffic load into consideration when deciding a handover.

The algorithm in which the BSS decides on starting a Load Indication procedure is operator dependent.

The implementation of the Load Indication procedure shall be regarded as optional, that means, if this procedure is not used, the Load Indication message may be ignored by these network elements.

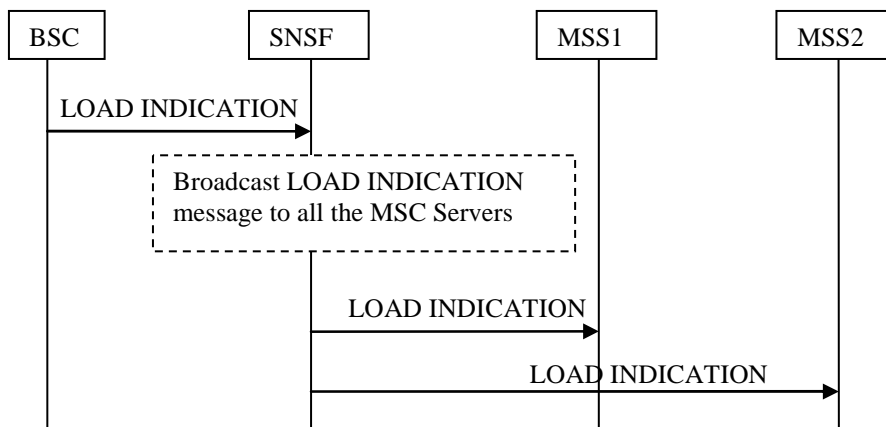5.6.3.2.8.1 BSS Initiated Load Indication

Figure 5.6.3.2.8.1.1: Load Indication procedure, BSC originated

The LOAD INDICATION message is sent from the BSS to the MSC Server. It indicates to the receiving entity that the transmitting BSS has detected a load situation in the concerned cell. On receipt of the BSC LOAD INDICATION message, the SNSF node broadcasts this message to all the MSC.

5.6.3.2.8.2 CN Initiated Load Indication
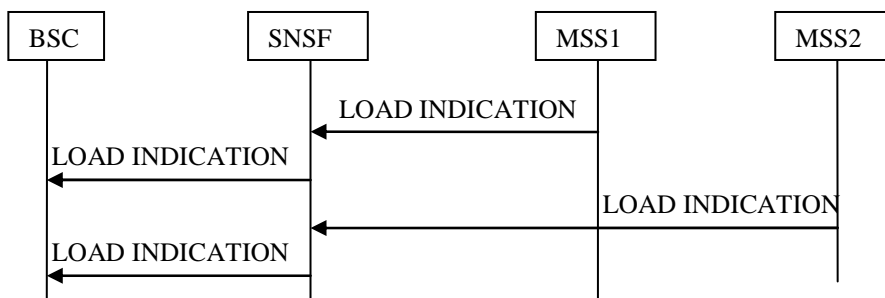
Figure 5.6.3.2.8.2.1: Load Indication procedure, MSC originated

The LOAD INDICATION message is sent from the MSC Server to the BSC. It indicates to the receiving entity that the transmitting MSS has detected a load situation in the concerned cell. On receipt of the MSC LOAD INDICATION message, the SNSF node transfers this message to the destination BSC node.

5.6.3.2.9 Connectionless Information Transfer

5.6.3.2.9.1 BSS Initiated Connectionless Information Transfer
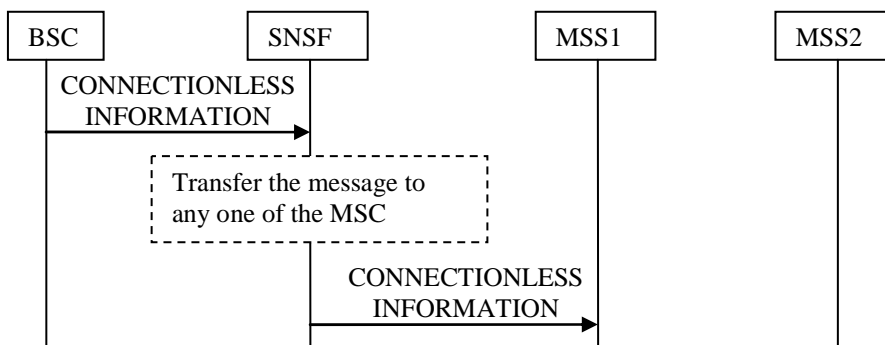
Figure 5.6.3.2.9.1.1: Connectionless Information sent from the BSC

On receipt of the CONNECTIONLESS INFORMATION message from the BSC, the SNSF node transfers this message to any one of the MSC Servers in the Pool Area.

5.6.3.2.9.2 CN Initiated Connectionless Information Transfer
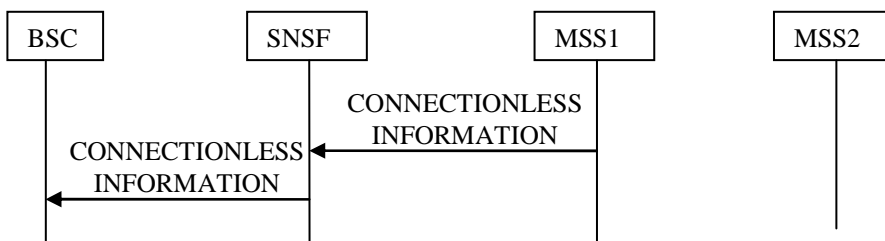
Figure 5.6.3.2.9.2.1: CN Initiated Connectionless Information

On receipt of the CONNECTIONLESS INFORMATION message from the MSC Server, the SNSF node transfers this message to the destination BSC.

5.6.3.2.10 TDM Circuit Management

This clause describes message handling procedures at the SNSF for uplink TDM circuit management-related messages. Two alternatives have been captured as summarized below with the corresponding pros and cons:

- Message distribution based on **circuit mapping data**: in this method, the SNSF determines the destination MSC Server(s) on the basis of the combination of the identity (code) of the affected circuit(s) and the network address of the sending BSC. A configured mapping between this information and the network address of the destination MSC Server(s) is assumed to exist in the SNSF.

    - **Pros**: The circuit mapping data method permits precise identification of the destination MSC Server(s), yet requires the configuration of mapping data in the SNSF.

    - **Cons**: If much data configuration is required on the SNSF node together with the MSC Server, any change on the configuration will be very complicated.

- Message distribution based on **broadcast mechanism**: in this method, the SNSF sends the message to each MSC Server in the MSC Pool.

    - **Pros**: This alternative requires no configured data in the SNSF or data synchronization between MSC Servers and SNSF nodes, yet its use results in the sending of messages to MSC Servers that do not manage the indicated circuit(s).

    - **Cons**: MSC Server may receive TDM circuit management messages to operator circuits which are not locally configured and it is required to discard these messages in these cases.

The use of the alternatives is implementation specific and there is no recommendation in the present document.

5.6.3.2.10.1 Message Distribution Based on Circuit Mapping Data

Optionally, the SNSF may have the configuration data of the mapping from the circuit identity (e.g. Circuit Identity Code and the Signalling Point Code of the BSC) to the MSS node. On receipt of the circuit management messages from the BSC node, the SNSF handle the message as per the message type listed below:

- On receipt of the BSC initiated (Un)Block or Reset Circuit message, the SNSF determines the MSS node as per the Circuit Identity Code extracted from the received message and the Source Signalling Point Code, and distributes the message to the MSS node. On receipt the (Un)Blocking Acknowledgement or Reset Circuit Acknowledge message, the SNSF relays the message to the BSC as per the destination Signalling Point Code.

- On receipt of the MSS initiated (Un)Block or Reset Circuit message, the SNSF relays the messages towards the BSC as per the destination Signalling Point Code. When received the (Un)Block Acknowledgement or Reset Circuit Acknowledge message, the SNSF determines the MSS node as per the Circuit Identity Code extracted from the received message and the Source Signalling Point Code, and distributes the message to the MSS node.

- On receipt of the BSC initiated Circuit Group (Un)Block message, the SNSF extracts the sub-set of circuits configured for each MSS node and specified in the received message, relays the message with this sub-set circuits towards the MSS node. The MSSs shall (Un)Block the circuits locally configured and return a Circuit Group (Un)Block message by setting the Status Bits with the value of "1" (*(un)blocking acknowledgement*) for the (Un)Blocked circuits. The SNSF will receive multiple Circuit Group (Un)Blocking Acknowledgement messages (one from each MSS node) and the SNSF shall aggregate the Status Bits of this IE with value of "1" ((un)blocking acknowledgement) and send the message with the aggregated Status Bits of the Circuit Identity Code List IE to the BSC node. Figure 5.6.3.2.10.1.1 illustrates the procedures for BSC initiated Circuit Group Block messages to block circuits configured to MSS1 and MSS2.

NOTE 1: As specified in TS 48.008 [5], "*The CIRCUIT GROUP UNBLOCKING ACKNOWLEDGEMENT message is accepted as the appropriate acknowledgement only if the indicated Circuit Identity Code and the returned Range field of the Circuit Identity Code List match the corresponding parameter values of the respective initiating message. Otherwise the message is considered as not expected.*" The MSC Server shall return the acknowledgement messages responding to the Circuit Group (Un)Block message with the same Circuit Identity Code and the same Range Field of the Circuit Identity Code List IE.
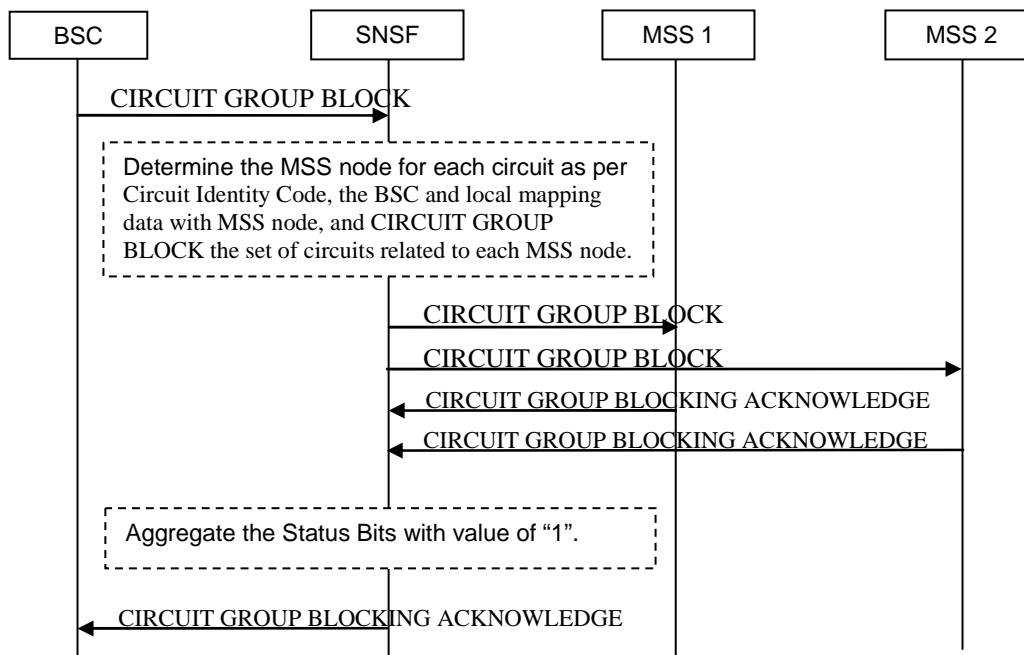
**Figure 5.6.3.2.10.1.1: Uplink TDM Circuit Management Message Handling at the SNSF
(SNSF distributes the messages as per circuit identity)**

- On receipt of the MSS initiated Circuit Group (Un)Block message, the SNSF relays the messages towards the
  BSC as per the destination Signalling Point Code. When received the Circuit Group (Un)Blocking
  Acknowledgement message (all the circuits will map to the same MSS node), the SNSF distributes the message
  received from the BSC node to the MSS node as per the Circuit Identity Code extracted from the received
  message and the Source Signalling Point Code.

- For the BSC initiated Unequipped Circuit message, the SNSF extracts the sub-set of circuits configured for each
  MSS node and specified in the received message, relays the message with this sub-set circuits towards the MSS
  nodes.

NOTE 2: If MSS connects to multiple SNSF nodes, the MSS shall only return the acknowledgement messages
         towards the SNSF node which the corresponding Reset Circuit, (Un)Block, and Circuit Group (Un)Block
         received from.

5.6.3.2.10.2   Message Distribution Based on Broadcast Mechanism

Alternatively, The SNSF may distribute the uplink message towards to each MSS node. In this approach, the SNSF will
no need keep any data related to the mapping from the Circuit Identity to the MSS node. On receipt of the circuit
management messages from the BSC node, the SNSF handle the message as per the message type listed below:

- On receipt of the BSC initiated (Un)Block or Reset Circuit message, the SNSF relay a copy of the message to
  each MSS node. The MSS shall only handle the message if the circuit is configured locally. On receipt the
  (Un)Blocking Acknowledgement or Reset Circuit Acknowledge message, the SNSF relays the message to the
  BSC as per the destination Signalling Point Code. To avoid unnecessary UNEQUIPPED CIRCUIT messages
  from the MSC Servers, the MSC Servers shall ignore the (Un)Block or Reset Circuit message that the circuit
  indicated in the message is not configured locally and shall not send an UNEQUIPPED CIRCUIT message in
  these cases.- On receipt of the MSS initiated (Un)Block or Reset Circuit message, the SNSF relays the
  messages towards the BSC as per the destination Signalling Point Code. When received the (Un)Block
  Acknowledgement or Reset Circuit Acknowledge message from the BSC, the SNSF relay a copy of the message
  to each MSS node. The MSS shall ignore the message if the circuits is not configured locally.

- On receipt of the BSC initiated Circuit Group (Un)Block message, relay a copy of the message to each MSS
  node. The MSS shall ignore the circuits specified in the message but not configured locally, (Un)Block the
  circuits locally configured and return a Circuit Group (Un)Block message by setting the Status Bits with the
  value of "1" (*(un)blocking acknowledgement*) for the (Un)Blocked circuits and with the value of "0" (*no
  indication*) for the others. The SNSF will receive multiple Circuit Group (Un)Blocking Acknowledgement
  messages and all the messages shall have the same content with the exception of the Circuit Identity Code List

IE. The SNSF shall aggregate the Status Bits of this IE with value of "1" ((un)blocking acknowledgement) and send the message with the aggregated Status Bits of the Circuit Identity Code List IE to the BSC node. Figure 5.6.3.2.10.2.1 illustrates the procedures for BSC initiated Circuit Group Block messages to block circuits configured to MSS1 and MSS2. To avoid unnecessary UNEQUIPPED CIRCUIT messages from the MSC Servers, the MSC Servers shall not send UNEQUIPPED CIRCUIT messages for the circuits indicated in the Circuit Group (Un)Block message but not locally configured.

NOTE 1: As specified in TS 48.008 [5], "*The CIRCUIT GROUP UNBLOCKING ACKNOWLEDGEMENT message is accepted as the appropriate acknowledgement only if the indicated Circuit Identity Code and the returned Range field of the Circuit Identity Code List match the corresponding parameter values of the respective initiating message. Otherwise the message is considered as not expected.*" The MSC Server shall return the acknowledgement messages responding to the Circuit Group (Un)Block message with the same Circuit Identity Code and the same Range Field of the Circuit Identity Code List IE.
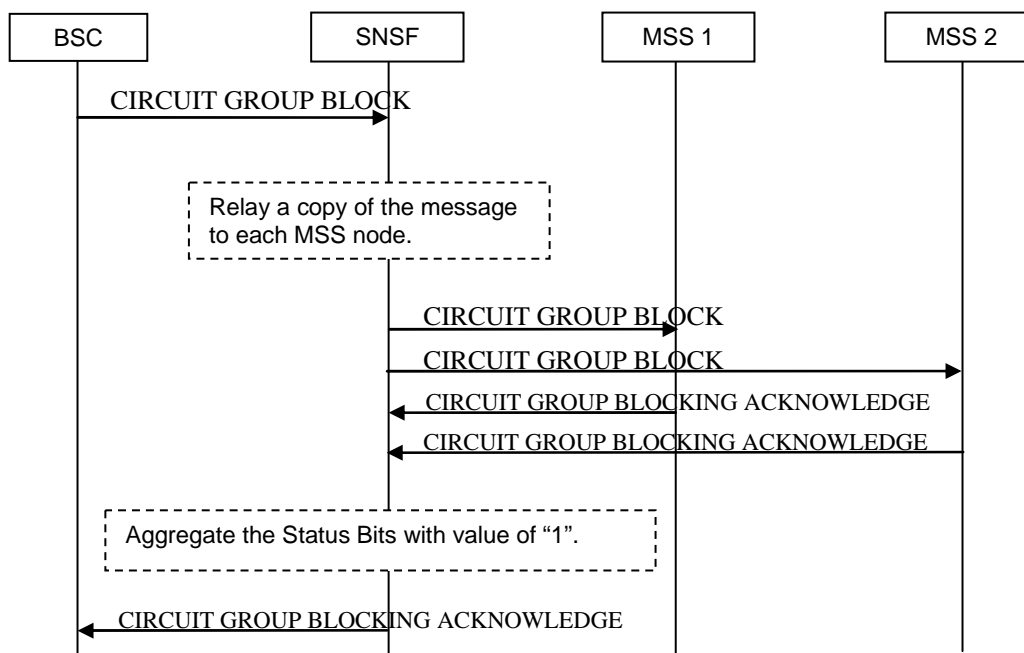

Figure 5.6.3.2.10.2.1: Uplink TDM Circuit Management Message Handling at the SNSF (SNSF Relay the Message to each MSS node a copy)

- On receipt of the MSS initiated Circuit Group (Un)Block message, the SNSF relays the messages towards the BSC as per the destination Signalling Point Code. When received the Circuit Group (Un)Blocking Acknowledgement message, the SNSF relay a copy of the message to each MSS node. The MSS shall ignore the message if the circuits specified in the message are not configured locally.

- For the BSC initiated Unequipped Circuit message, the SNSF relays a copy of the message to each MSS node.

NOTE 2: If MSS connects to multiple SNSF nodes, the MSS shall only return the acknowledgement messages towards the SNSF node which the corresponding Reset Circuit, (Un)Block, and Circuit Group (Un)Block received from.

6 Interaction with other features

6.1 Interaction with Network Sharing

Network sharing is a way for operators to share the heavy deployment costs for mobile networks, especially in the roll-out phase. Multi-Operator Core Network (MOCN) is a network-sharing configuration in which only the RAN is shared and Gateway Core Network (GWCN) is a network sharing configuration that parts of the core network (MSC Servers or SGSN nodes) are also shared (see TS 23.251 [4]).

6.1.1 Interaction with MOCN

6.1.1.1 General

For MOCN network sharing, parts of RAN network are shared.

In a MOCN configuration without deploying the SNSF node above the RNC node, the RAN node routes the UE's initial access to the shared network to one of the available CN nodes which directly connected with the RAN node as per the PLMN-id and routes subsequent messages to the selected CN nodes as per the NRI parameters extracted from the (P-)TMSI.
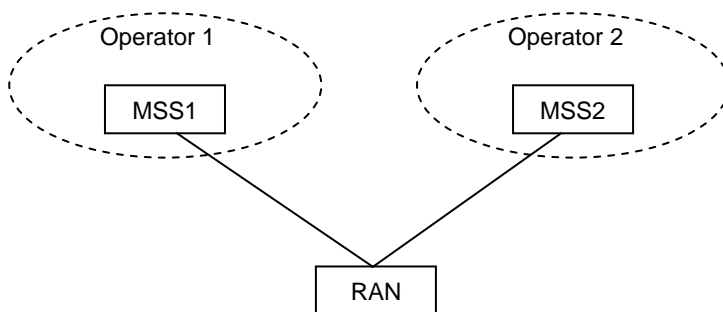

Figure 6.1.1.1.1: Network configurations for only MOCN is deployed

In an MOCN configuration with deploying the SNSF node above the RNC node, the RAN node may be fully configured to select and route the UE's initial access and subsequent messages to an available CN node directly, or the RAN node may be only configured to select and route the UE's initial access and subsequent messages to the SNSF node deployed above the RAN nodes and the SNSF node select and route the UE's initial access and subsequent messages to an available CN node as depicted in the following clauses.

6.1.1.2 RAN selects and distributes messages to CN nodes directly

In an MOCN configuration without deploying the SNSF node above the RNC node, the RAN node may be fully configured to select and route the UE's initial access and subsequent messages to an available CN node directly. As no SNSF node is deployed above the RAN nodes, no interaction is detected in this scenario.

6.1.1.3 SNSF node select and distribute messages to CN nodes

In a MOCN configuration with deploying the SNSF node above the RNC node, the RAN node may be only configured to select and route the UE's initial access and subsequent messages to the SNSF node deployed above the RAN nodes and the SNSF node select, determine and route the UE's initial access and subsequent messages to an available CN node as specified in clause 5.6 and illustrated in figure 6.1.1.3.1.
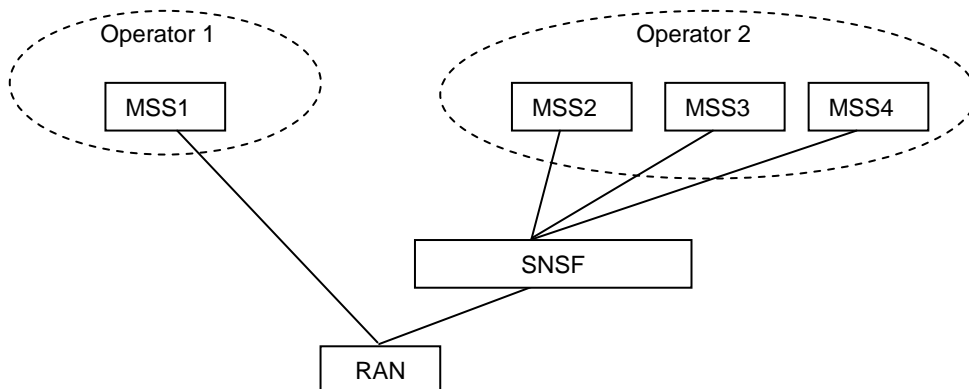

Figure 6.1.1.3.1: Network configurations for MOCN with MSC Pool

6.1.2 Interaction with GWCN

For GWCN network sharing, parts of the core network (MSC Servers or SGSN nodes) are also shared.

In a GWCN configuration without deploying the SNSF node above the RNC node, the RAN node routes the UE's initial access to the shared network to the directly connected CN node.

In a GWCN configuration with deploying the SNSF node above the RNC node, the RAN node routes the UE's initial access to the SNSF node shared between operators and the SNSF node select, determine and distribute the messages to a correct CN node as specified in clause 5.6 and illustrated in figure 6.1.2.1.

The network configurations of only GWCN and GWCN with MSC Pool are shown in figure 6.1.2.1.

Figure 6.1.2-1a: Only GWCN is configured

Figure 6.1.2-1b: Both GWCN and MSC Pool are configured
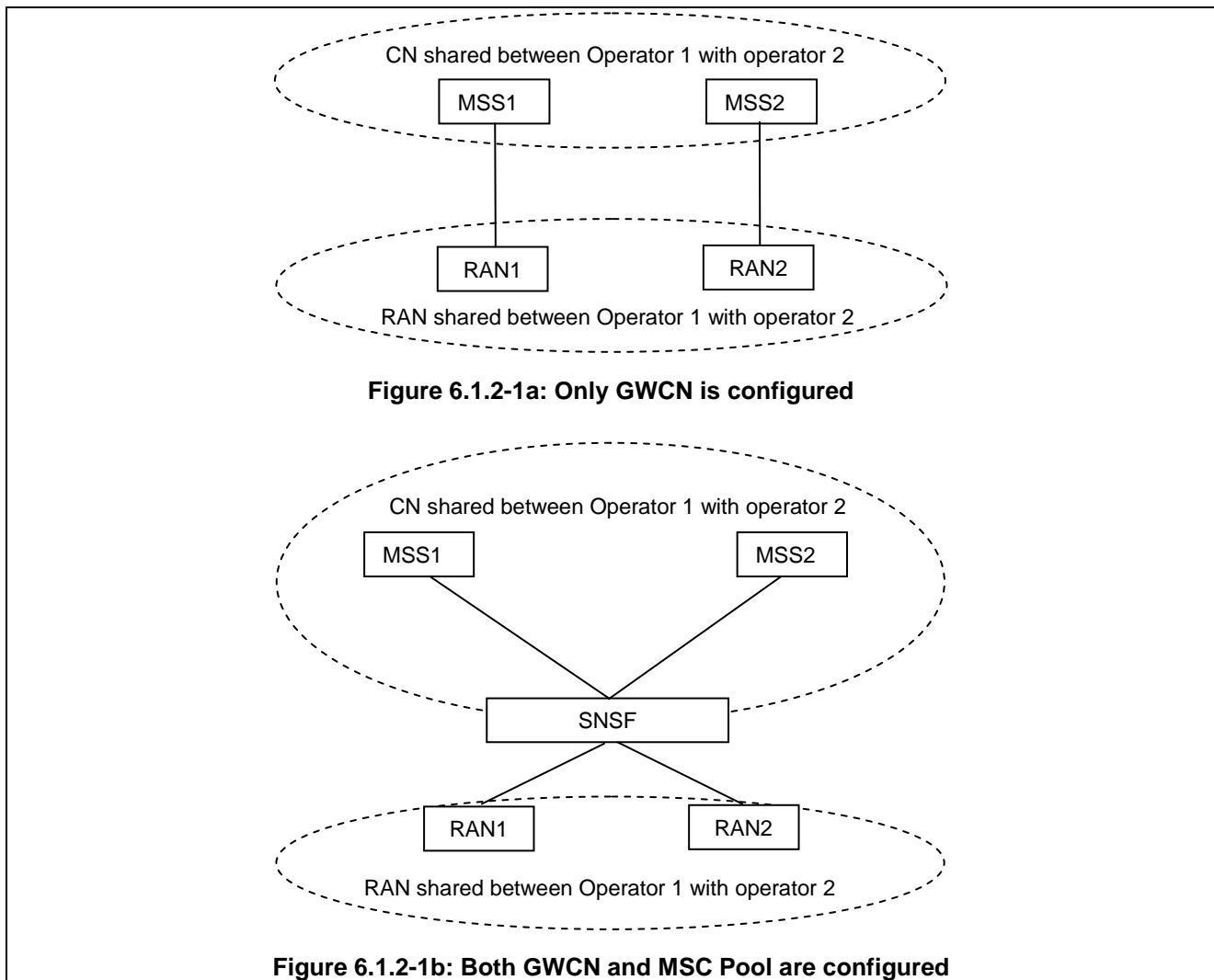
Figure 6.1.2.1: Network configurations for only GWCN and GWCN with MSC Pool

6.1.3 Conclusion

Deploying the SNSF node above the BSC/RNC node works well with the deploying of Network Sharing (MOCN or GWCN) feature and no impact on Network Sharing.

6.2 Interaction with A interface over IP

For the use of A interface control plane over IP with A interface user plane either over TDM or over IP, the A interface signalling is transported over SIGTRAN. With this configuration, the only consideration for the deployment of the SNSF nodes is related to SNSF node redundancy and failover. The procedures for such are described in clause 4.9.1.2.

7 Compatibility Issues

7.1 Co-existence of NNSF within BSC/RNC nodes with SNSF above BSC/RNC nodes

Using the NNSF within the BSC/RNC nodes has already been defined in TS 23.236 [2]. Deploying SNSF above the BSC/RNC nodes will co-exist with using the NNSF within the BSC/RNC nodes as described below.
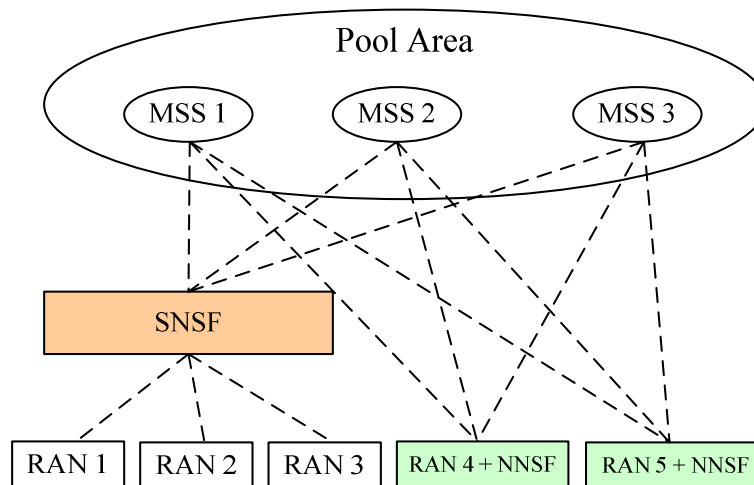

Figure 7.1.1: Co-existence of NNSF within BSC/RNC nodes with SNSF above BSC/RNC nodes

As shown in Figure 7.1.1, if part of the BSC/RNC nodes are capable of supporting the NNSF function as described in TS 23.236 [2] (RAN node 4~5) while the others are not (RAN node 1~3), the NNSF capable BSC/RNC nodes assign an MSC Server to serve a mobile station and subsequently route the signalling traffic to the assigned MSC Server whereas non-NNSF capable BSC/RNC nodes connect to SNSF node and the SNSF node is responsible for assigning an MSC Server to serve a mobile station and subsequently routing the signalling traffic to the assigned MSC Server.

In this situation, the MSC Server interacts with the SNSF node as described in clause 5 of the present document (e.g., allocate the SCCP local reference with SNRI as described in clause 5.6.2.2 if the SCCP Local Reference Based Handling of connection-oriented messages is used), and interacts with BSC/RNC nodes as specified in TS 23.236 [2].

8 Evaluation

The technical study verifies that it is feasible to support NNSF functionality above the RAN nodes. This has been studied for the circuit switched core network; the need for support of such function for the packet switched core network was removed during the execution of this study. The value of the SNSF function is based on not impacting 'old' RAN nodes. This also means that SNSF does not impact the existing A and Iu interfaces between the radio network and the CS core network.

This study has shown that the gain of independence from the RAN nodes requires:

- Either new standalone SNSF nodes must be introduced into the core network or the SNSF functionality must be collocated with already existing nodes, for example with the MGW. The latter may impact the capacity of the existing node due to the fact that functionality is added.

- It requires more signalling compared to when the NNSF functionality is applied in the RAN nodes, because connection to the SNSF function is forced, which are acting as proxies.

- If the SNSF functionality shall not be a single point of failure then additional complexity is required to realise redundancy mechanisms, including impacts on the MSC Server as well.

In many cases the SNSF functionality is an SNSF internal handling. For this internal handling it is possible to reuse what has been specified for NNSF in TS 23.236 [2], e.g. load balancing and load re-distribution. Other functionality does not impact SNSF at all, for example combined mobility management procedures. The only identified functionality which can't be inherited by existing specifications is the support for redundancy. A potential redundant solution is described in clause 5.6.2.2 of this TR. As vendors had to already cope with these situations early in the operational environment, vendor specific solutions already exist without impacting standards or existing NNSF functions.

In addition to the above analysis there are also other facts to be considered:

1. Vendors have already provided products to provide SNSF functionality collocated within MGWs by different means. They may come into conflict with a future normative specification.

2. As far as known, currently those MGWs interfacing the radio network and the MSC Servers are deployed by the same vendor. For these deployment scenarios there is no need for IOT testing.

3. MGW redundancy is also based on vendor specific implementations and is not specified by 3GPP. Specifying SNSF functionality may result into conflicts with already deployed MGW redundancy.

For the reasons listed above, the present TR concludes without a recommendation for normative specification of SNSF functionality.

9 Conclusions

Through the preceding technical investigation within this technical report, it is concluded that it is feasible to deploy SNSF nodes above the BSC/RNC nodes to provide functions similar to those of the NNSF in BSC/RNC nodes as specified in TS 23.236 [2]. The solution described in this TR is one of the possible solutions to resolve the implementation issues of deploying NNSF within the BSC/RNC nodes for MSC Pool.

The solutions described in this study may be used as guideline for implementations in cases where operator does not upgrade the radio networks.

Annex A:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2010-03	SP-47	SP-100173	-	-	MCC update to version 2.0.0 for presentation to TSG SA for approval: Requested Upgrade to TR 23.9XX.	1.2.0	2.0.0
2010-03	SP-47	-	-	-	MCC creation of **23.924** version 10.0.0 from **23.823** version 2.0.0 after TSG SA approval with the change of TR number.	2.0.0	10.0.0
2012-09	-	-	-	-	Update to Rel-11 version (MCC)	10.0.0	**11.0.0**
2014-09	SP-65	-	-	-	Update to Rel-12 version (MCC)	11.0.0	**12.0.0**
2015-12	-	-	-	-	Update to Rel-13 version (MCC)	12.0.0	**13.0.0**
2017-03	-	-	-	-	Update to Rel-14 version (MCC)	13.0.0	**14.0.0**
2018-06	SP-80	-	-	-	Update to Rel-15 version (MCC)	14.0.0	**15.0.0**
2020-07	SP-88E	-	-	-	Update to Rel-16 version (MCC)	15.0.0	**16.0.0**
2022-03	SP-95E	-	-	-	Update to Rel-17 version (MCC)	16.0.0	**17.0.0**
2024-03	-	-	-	-	Update to Rel-18 version (MCC)	17.0.0	**18.0.0**

History

Document history		
V18.0.0	April 2024	Publication