

Source: TSG_SA WG5
Title: LS IN on UTRAN OAM Procedures (Feature-level Work Item: UOAM)
Agenda item: 5.2
Document for: INFORMATION

3GPP TSG-SA5 (Telecom Management)
Meeting #17, Sophia Antipolis, FRANCE, 18 – 26 January 2001

SA5#17(01)0012

Title: Feedback LS on UTRAN OAM Procedures (Feature-level Work Item: UOAM)
Source: SA5
TO: RAN3
Cc: RAN, SA, CN

Contact Person:

Name: Bert BODEN
E-mail Address: Bert.Boden@d2vodafone.de
Tel. Number: +49 211 533 2946

Attachments: 3GPP TR 32.800 v0.0.3

TSG SA5 thanks TSG RAN3 for the liaison on the UTRAN OAM Procedures work item. We have included the original questions from that liaison and TSG SA5's responses below. Also attached is the latest draft of 32.800.

We hope our responses address your concerns, and we look forward to continued co-operation between our working groups.

RAN3 Q1: RAN3 was unsure as to whether there would be changes to 25.433 and 25.430 specifications as a result of the work item (suggested by section 10), or if they were simply sources of information for the document 32.800 (suggested by section 15).

SA5 A1: The latter interpretation is correct, section 10 tries to capture the natural order for a top-down approach (as used by SA5 throughout its specifications), i.e. if the sequence had been correct, 32.800 would have been developed prior to the detailed Protocol and Interface specifications.

RAN3 Q2: The stated Release 4 deadline of June 2001 for changes to 25.433 and 25.430 is not aligned with the RAN3 target for Release 4 changes. RAN3 understands that the deadline for OAM specifications may be later, but is hoping to have completed its Release 4 work by TSG RAN/SA#11 (March 2001).

SA5 A2: No actual changes will be required (see 1 above), so there will be no alignment problems.

RAN3 Q3: RAN3 was unclear about the connection between the proposed SA5 work item and the RAN3 work items "RRM Optimisation" and "RAN Enhancements", as indicated in the work item sheet. RAN3 would appreciate some clarification about whether this implies that changes to the RAN3 work in these areas will be required.

SA5 A3: It is hoped that RAN3 may want to check the 32.800 report for consistency with their work, this is why these are listed as linked work items. During the development of the Release 4 work it is not expected that this should be a continuous activity but rather that the 32.800 work and the checks should be synchronised e.g. March-April timeframe for the next check.

RAN3 Q4: The indicated objectives appear to suggest that RNC behaviour with regard to NBAP may be specified in detail, which is not in-line with the Release '99 Iub protocol design. NBAP basically follows a client-server approach, with the Node B behaviour well-specified, leaving flexibility for the RNC to decide when to use specific procedures. It was also commented that it was not clear what the scope of the "solutions" referred to in the objectives would be.

SA5 A4: The 32.800 document will contain signalling examples and will not mandate the signalling to be used. We suggest that RAN3 may want to review the latest draft of the 32.800 report (attached) to clarify this point. It is not intended to change the level of detail already present in 32.800.

RAN3 Q5: In general, RAN3 would prefer to avoid external dependencies on its protocols, and believes that discussions on impacts to Iub signalling should occur in RAN3.

SA5 A5: We do not consider SA5 external to 3GPP. Where dependencies exist they need to be recognised and checked. We would also have been happy to have this report continue within RAN3. If RAN3 can suggest a better way of documenting the O&M aspects then SA5 would be more than happy to consider these proposals.



**3rd Generation Partnership Project;
Technical Specification Group Services and System
Aspects;
Management Level Procedures and Interaction with UTRAN
(Release 4)**

The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organisational Partners and shall not be implemented.

This Specification is provided for future development work within 3GPP only. The Organisational Partners accept no liability for any use of this Specification.

~~Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organisational Partners' Publications Offices~~

Keywords
UTRAN OAM

3GPP

Postal address

3GPP support office address

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

Internet

<http://www.3gpp.org>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2001, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Foreword	6
Introduction	6
1 Scope.....	7
2 References	7
3 Definitions and abbreviations.....	7
3.1 Definitions	7
3.2 Abbreviations.....	7
4 UTRAN O&M	8
4.1 UTRAN O&M overview	8
4.2 UTRAN O&M Procedures overview.....	9
4.2.1 Network Expansion Procedure.....	9
4.2.2 Cellular Network Configuration Procedure.....	9
4.2.3 Remote Software Update Procedure	9
4.2.4 Network Optimisation Procedure	9
4.2.5 Network Monitoring and Fault Management Procedures	10
4.3 Node B O&M Management Architecture	10
5 UTRAN O&M Procedures.....	10
5.2 Node B Installation and Initial Configuration.....	10
5.3 Cellular Network Configuration	11
5.3.1 Initial Cell Configuration	12
5.3.2 Cell Re-configuration	14
5.4 Network Optimisation Procedure.....	18
5.4.1 Reports relating to cell performance	18
5.4.2 Reports relating to Node B performance.....	18
5.4.3 Reports relating to Handover performance	19
5.4.4 Routing of the Performance Management (PM) reports	19
5.5 Remote Node B Software Update.....	19
5.5.1 Remote Software Update Procedure – Pull Method.....	20
5.5.2 Remote Software Update Procedure – Push Method	23
5.6 RNC Installation	26
5.7 Node B Expansion	26
5.7.1 Implementation Specific O&M Expansion	27
5.7.2 Logical Node B Expansion.....	28
5.7.3 Overall Node B Expansion.....	30
5.8 Node B Swap	30
5.8.1 Installation of a new RNC.....	31
5.8.2 Re-configuration of old RNC.....	31
5.8.3 Node B Detachment	32
5.8.4 New Installation	32
5.9 Network Monitoring and Fault Management Procedures	32
5.9.1 Implementation-specific Fault Management	33
5.9.2 Alarm Filtering and Correlation	33
5.9.3 NBAP alarm messages	33
History	37

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 present document describes procedures needed to manage a UTRAN Radio network. The purpose of these procedures is to ensure that the O&M functions supported via the IRPs and over the Iub interface are sufficient to allow a multi-vendor environment to be realised. To define this scope a proper understanding of the O&M functions in the network manager throughout the Node B is required. This will ensure that all O&M functions requiring interaction with the RNC and Node B are identified and specified accordingly.

1 Scope

The principle objective of the present document is to provide supporting information for the O&M standardisation of a (multi-vendor) UTRAN network. The actual specification work relating to the O&M interface between Network & Network Manager can be found in [9], [10] and [11] and for the Iub interface in [1]. For this reason the present document may contain information or working assumptions which are not a direct part of the specifications, but are essential to the progress and informed decision making.

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 TS 25.433: "NBAP Specification".
- [2] 3GPP TS 25.401: "UTRAN Overall Description".
- [3] 3GPP TS 25.442 "UTRAN Implementation Specific O&M Transport
- [4] 3GPP TS 25.432: "UTRAN Iub interface signalling transport".
- [5] 3GPP TS 25.832: "Manifestations of Handover and SRNS Relocation".
- [6] ITU-T Recommendation Q.821 (3/93): "Stage 2 and Stage 3 Description for the Q3 Interface – Alarm Surveillance".
- [7] ITU-T Recommendation X.721 (2/92): "Information Technology – Open Systems Interconnection – Structure of Management Information: Definition of Management Information".
- [8] ITU-T Recommendation X.731 (01/92): "Information Technology – Open Systems Interconnection – Systems Management: State Management Function".
- [9] 3GPP TS 32.106: "Configuration Management".
- [10] 3GPP TS 32.111: "Fault Management".
- [11] 3GPP TS 32.104: "Performance Management".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

- Logical O&M is defined in subclause 10.1.2 of [2].
- Implementation Specific O&M is defined in subclause 10.1.1 of [2].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAL5	ATM Adaptation Layer type 5
ATM	Asynchronous Transfer Mode
C-RNC	Controlling RNC
FDD	???
FFS	???
IP	Internet Protocol
NBAP	Node B Application Protocol
NE	Network Element
NM	Network Manager

O&M	Operation and Maintenance
PM	Performance Management
PVC	Permanent Virtual Circuit
RAKE	?????
RANAP	Radio Access Network Application Part
RF	?????
RNC	Radio Network Controller
RNSAP	Radio Network Subsystem Application Part
RSSI	Received Signal Strength Indicator
RxISCP	Received Interference Signal Code Power
SF	Spreading Factor
SVC	Switched Virtual Circuit
TDD	?????
UE	?????
HW	?????
SW	?????
UL	?????
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network

4 UTRAN O&M

4.1 UTRAN O&M overview

Figure 4.1.1 below shows a typical configuration of the O&M systems for UTRAN part. The figure also identifies all the interfaces between various management systems and NEs.

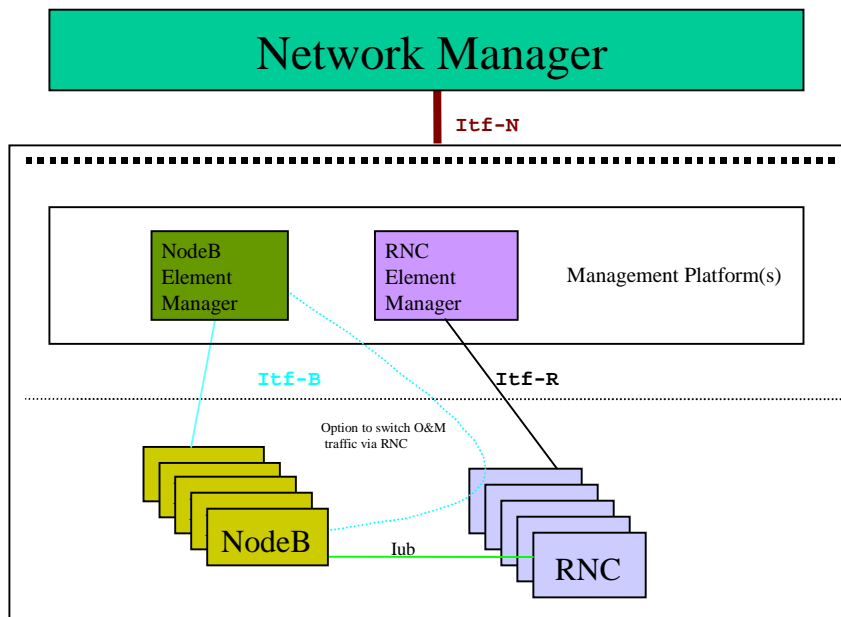


Figure 4.1.1: O&M Management Interfaces

The Management Interfaces are:

1. Itf-B - between Node B & its Manager (physically, this may be a direct connection or via the RNC [3]).
2. Itf-R - between RNC & its Manager.
3. Itf-N – between Network & Network Manager.

4.2 UTRAN O&M Procedures overview

This following list of UTRAN procedures should be used to derive requirements for the O&M functions of UTRAN elements, and to identify all information that has to be exchanged to provide the required functionality.

4.2.1 Network Expansion Procedure

Network Expansion in general includes expansion of existing elements and integration of new elements. These procedures can also be used to reduce the number of elements in the network. The most frequent expansion processes are:

Node B Expansion: The Node B Expansion means a modification of several Node B parameters that are provided by a previous planning process (see subclause 5.7).

Node B Installation: Installation of a new Node B including setting of all required parameters. Additionally the Node B is attached to the appropriate RNC and all links are dimensioned accordingly. Possibly causes Expansion/Modification of adjacent Node B's. An automatic configuration with the download of all the required (not vendor specific) data can reduce the required effort significantly. One possible example of such a configuration process is described in subclause 5.2.

Node B Swap: In case of integration of a new RNC one or more Node Bs are detached from neighbouring RNCs and attached to the new RNC. After configuration of the Node B and the new RNC and all according links, the Node B is detached from the old RNC and operates connected to the new RNC. Possibly Node B expansion procedures are triggered in all affected Node Bs (in the neighbouring cells, see subclause 5.8).

RNC Installation: Installation of a new RNC including setting of all required parameters. Additionally the RNC is attached to the appropriate Network Manager. One possible example of such a configuration process is described in subclause 5.6.

4.2.2 Cellular Network Configuration Procedure

Cellular Network Configuration processes deal with all modifications to NEs that have impact on the radio access network. For example parameters required for power management or synchronisation may be modified. A notification message to the according element indicating the planned configuration changes will be sent. For Implementation Specific O&M, both discreet message and file transfer methods should be supported for cellular network configuration, enabling the selected mechanism to be chosen dependent on the number of parameters to be configured. If the modification requires a larger amount of data to be transferred than the notification message may contain only the name and location of a required data file to be downloaded. Afterwards the affected NE(s) can integrate the supplied modifications and report the results of the performed parameter update. The element itself can choose the best time (in case of Node B in co-operation with the RNC) for the update according to its current load, etc. (see subclause 5.3).

4.2.3 Remote Software Update Procedure

Remote Software Update Procedure includes the remote Software Update of network elements. Within this Software Update process also self-checks and consistency checks are included. A status request message asking for a response from the affected network elements with the current release number can avoid release conflicts during the Software Update procedure. The Software Update procedure itself can be implemented with pull or with push technologies. A notification message to elements indicating a new software release (and the location of the required file) could be used to trigger an automatic download of the new release (pull technology). Or, the responses of the status request messages can be used to compose a multicast message carrying the new software release to all affected elements (push technology). See subclause 5.5.

4.2.4 Network Optimisation Procedure

In order to identify possible modifications that allow an improvement of the overall network performance this process type consists of the collection of measurement data and of the decision process to trigger network expansion and/or configuration procedures to optimise the network. Since expansion and configuration processes are handled separately (see above) the network optimisation process deals in this context only with the collection of measurement data (see subclause 5.4).

4.2.5 Network Monitoring and Fault Management Procedures

This process observes the status of network elements and handles alarm and event notifications. Additionally customer complaints are considered. (see subclause 5.9)

4.3 Node B O&M Management Architecture

The working assumption for the Node B O&M management architecture is described in subclause 10.1 of [2].

This architecture defines two categories of O&M functions at Node B – Logical O&M and Implementation Specific O&M. Logical O&M functions are supported over the Iub interface in NBAP – see subclause 10.1.2 of [2].

It should be possible to route the Implementation Specific O&M via the same physical bearer as the Iub interface – see

subclause 10.1.1 of [2], where the transport layer for this scenario is specified in [3].

5 UTRAN O&M Procedures

This clause provides procedure examples for the UTRAN O&M. These shall include management level procedures based on a scenario diagram of their execution, to clarify interaction between various NEs and Managers. The scenarios shall describe both Logical O&M and Implementation Specific O&M procedures, thus ensuring that a comprehensive description of the procedure is provided to clearly define the scope of that procedure. This should facilitate a better understanding of the scope of each procedure.

5.2 Node B Installation and Initial Configuration

The detailed steps of this procedure are given below. It describes the scenario where a new Node B is installed into the network, and the initial implementation specific configuration of the Node B is performed.

1. The Node B hardware will be installed at the Node B site, as well as software to be installed locally and setting of parameters.
2. The ATM link between the Node B and C-RNC will be established. This includes the establishment of the NBAP signalling bearer (according to [4]).

NOTE: It is **FFS** whether the signalling bearers have to be established manually or whether an automatic establishment is possible.

3. The transport channel for the Implementation Specific O&M will be established. If the Implementation Specific O&M is to be routed via the C-RNC, one or several AAL5/ATM PVCs or SVCs for the transport of O&M IP packets will be established (according to [3]). Otherwise a direct IP transport channel to the Node B Manager will be established.
4. A Node B initialisation procedure will be performed by means of Implementation Specific O&M functions (this could possibly be initiated from the NM). It includes downloading of software from the Node B Manager (which can be done automatically or manually), and the setting of all implementation specific configuration parameters. Having completed this procedure all the necessary conditions to allow the configuration of logical resources in one or several cells in the Node B will be fulfilled.
5. Following the Node B implementation specific initialisation some self-tests may be performed. The result of these self-tests should be communicated to the Node B manager via implementation specific O&M.
6. The Node B informs the C-RNC about the completion of the Node B Initialisation by sending a *Resource Status Indication* message. This provides the C-RNC with the locally set parameters which are needed for the logical cell configuration, e.g. Local Cell Id(s), number of carriers etc.
7. C-RNC informs the C-RNC Manager about the availability of the new Node B resources, and the C-RNC Manager subsequently informs Network Manager (**Step 7**).

NOTE: The remaining logical cell configuration should be performed as described in subclause 5.3.1.

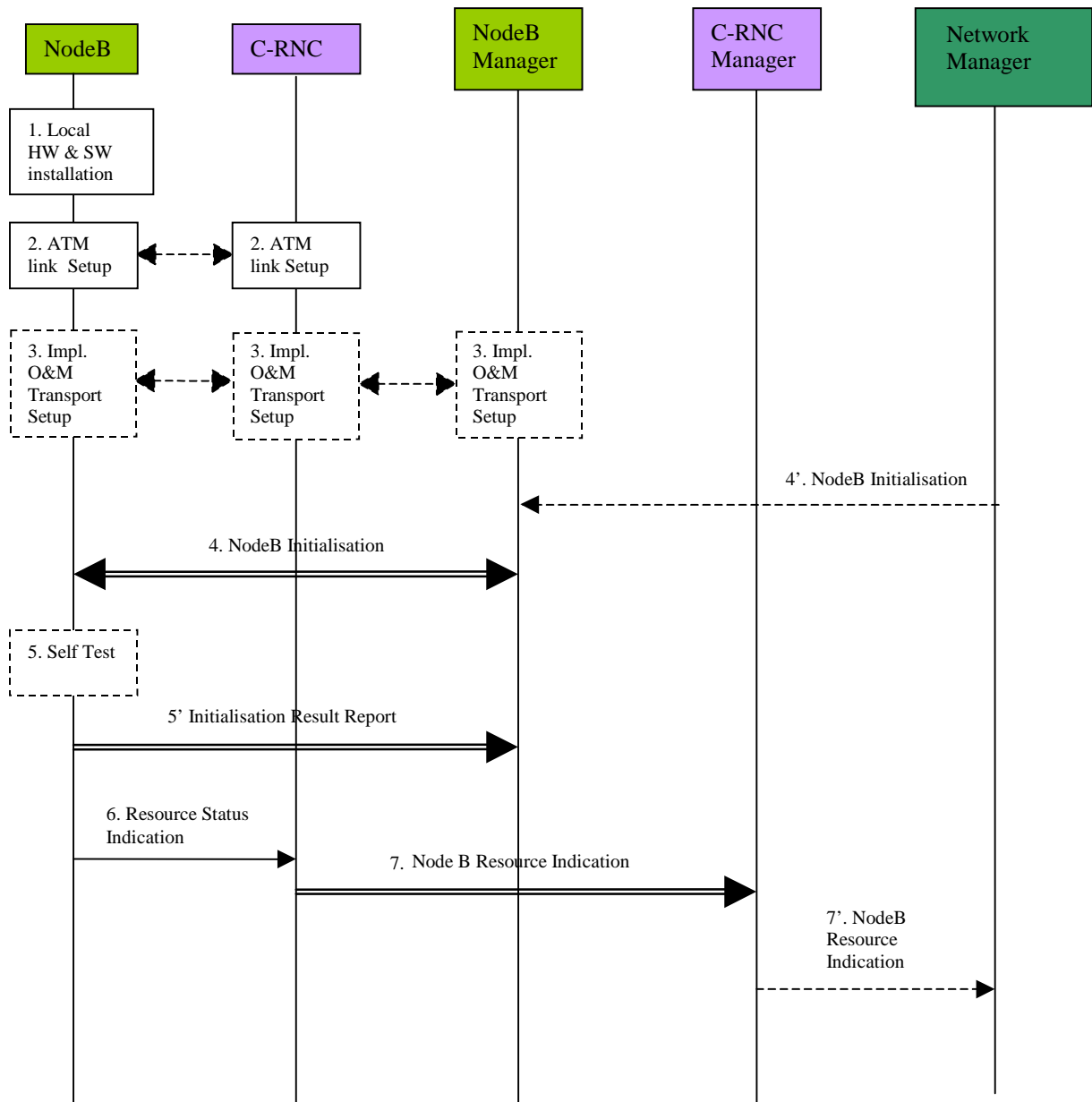


Figure 5.2.1: Node B Installation and Initial Configuration Procedure

5.3 Cellular Network Configuration

The cellular network configuration procedure describes all the required Node B parameter modifications associated with the definition of the Radio Access Network (RAN). The configuration of Node B incorporates both configuration of the logical resources supported at Node B, and configuration of the Implementation Specific aspects of Node B to support these resources. In addition, in order to allow the RAN to be optimised on an ongoing basis (depending on the traffic conditions), both initial configuration and ongoing configuration shall be supported.

5.3.1 Initial Cell Configuration

The definition of a cell in the UMTS system will originate from the management system. In order to make this process as simple as possible for the network operator, automation should be used and standardised entities addressed wherever possible. As such, the focus for creation of a cell should be the standardised cell model defined within the UTRAN. The creation of this Logical traffic carrying entity should be the trigger for the overall cell creation process, since this enables the network operator to deal only in standardised entities and not manufacturer specific aspects.

The Logical cell entity itself is resident in the RNC, since the cell is a logical traffic carrying entity and the RNC is the traffic controlling entity. The cell shall be as defined in [1]. The creation of the Node B control port shall be achieved via Implementation Specific O&M.

The following procedure represents one possible method by which a cell can be configured within the UTRAN. This procedure assumes that the associated Node B has already been installed using the procedure described in subclause 5.2, and that both Iub and Implementation Specific O&M communications are established.

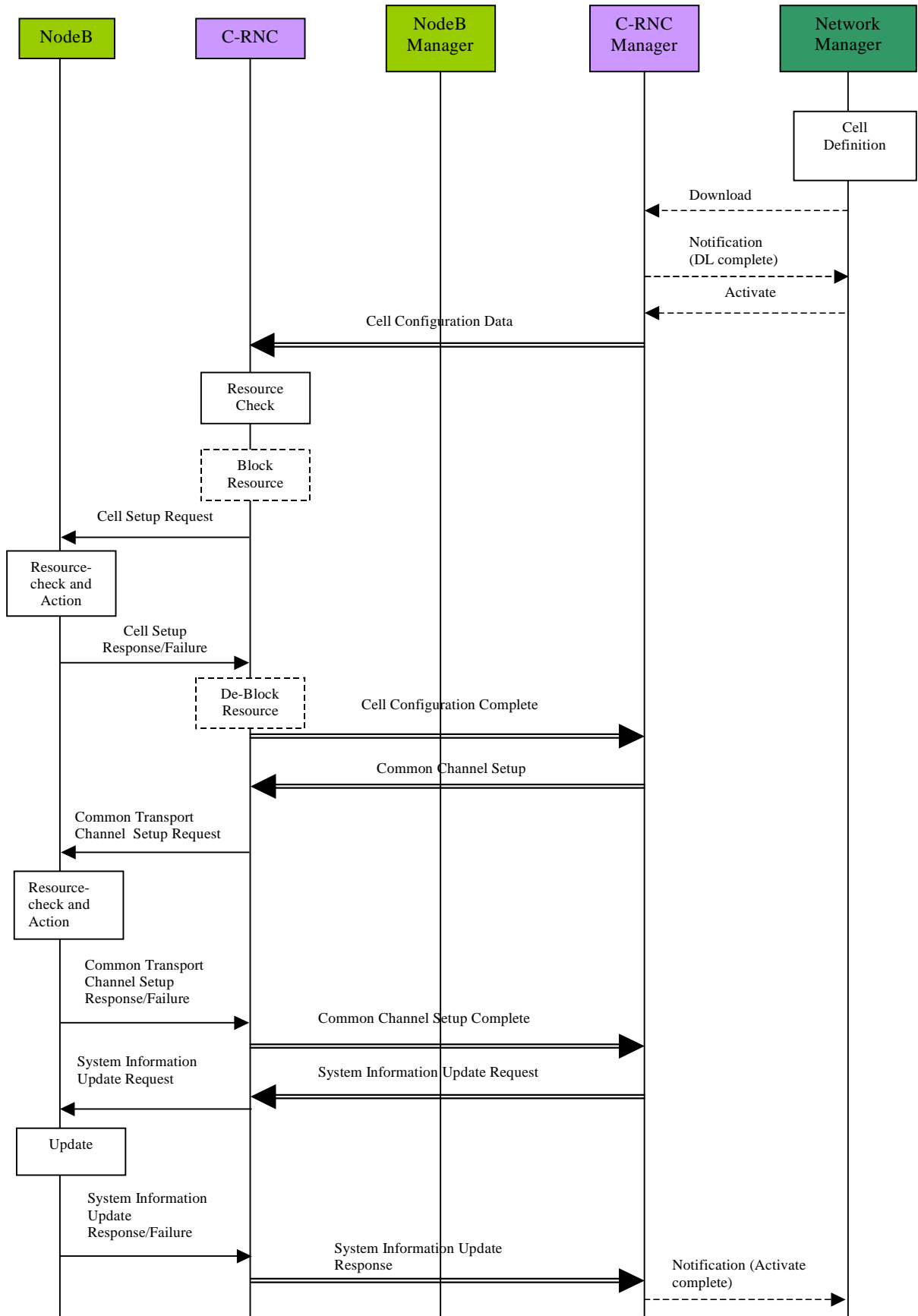


Figure 5.3.1.1: Initial Cell Configuration

The procedure above consists of the following steps:

1. The cell is defined and created in the Network Manager by the operator. This may be by manual means or as an output from a network optimisation tool. The definition should include all identifiers for the Node B required for creation of this cell and the associated C-RNC. These identifiers are FFS.
2. The operator initiates the creation of the cell, and the Network Manager initiates the cell configuration data Download to the appropriate C-RNC manager.
3. The C-RNC manager returns a Notification (DL Complete) to the Network Manager to indicate successful data transfer.
4. The operator then initiates the activation of the new cell from the Network Manager by sending an Activate message to the C-RNC manager.
5. The C-RNC manager passes the cell configuration data to the C-RNC for creation.
6. The C-RNC performs a resource check to ensure it has sufficient physical resources to support the new cell it has been instructed to define. This resource check applies only to the RNC's capabilities and not the Node B.
7. If required the RNC blocks any resources that may be affected by the cell configuration e.g. adjacent cells that may need re-configuration after the set-up of the new cell.
8. The C-RNC invokes the Cell Set-up Request message to carry all the required configuration information for mapping of the logical cell to the local cell in Node B.
9. Node B then performs the configuration of the new cell.
10. Once complete, the Node B advises the C-RNC that the configuration of the new cell has been successful using the Cell Set-up Response message. In the case of a failure, Node B invokes the Cell Set-up Failure message.
11. The C-RNC **unblocks** any resources that have been previously blocked. The Node B is not involved in this blocking/**unblocking**, since it only affects logical resources.
12. The RNC then advises the C-RNC manager that the configuration of the new cell has been successful (Cell Configuration Complete).
13. The C-RNC manager initiates the establishment of the required common transport channels and provides Node B with the appropriate System Information for that cell.
14. After the Node B has received the Common Transport Channel Setup Request(s), it checks the available resources (e.g. Iub link capacity, etc.) and establishes the requested channel(s).
15. Success is reported back to the RNC using the according response message, while in case of failure the Common Transport Channel Set-up Failure message will be used.
16. After successful establishment of the required common transport channels the RNC invokes the System Information Update procedure in order to start transmission of system information in the established cell.
17. Where the cell successfully begins operating, the C-RNC reports successful cell establishment (and operation) to its manager.
18. The C-RNC manager finally reports successful cell establishment and activation to the Network Manager by sending the Notification (Activate complete).

5.3.2 Cell Re-configuration

In order to enable the traffic environment to be optimised, the ongoing re-configuration of cell parameters shall be supported within UMTS. To ensure that both long-term and real-time optimisation can be applied to the UTRAN, the RNC controls the traffic carrying entity (i.e. the cell) and its associated parameters. In applying this philosophy, the generic cell model is held at the RNC giving the RNC access to all parameters for any required modification. This is essential if the cell parameters are to be altered on a real-time basis in order to optimise the traffic environment, since the RNC is the only UTRAN entity with real-time knowledge of the traffic conditions. This generic cell model controlled by the RNC does not include any Node B Implementation Specific parameters which may be interpreted as 'cell parameters'.

Therefore, two categories of cell re-configuration shall be supported – that which is initiated from the management system (operator or optimisation tool), and that which is automatically initiated by the radio resource algorithms in the RNC.

The procedure below represents one possible method by which a cell can be re-configured from the management system.

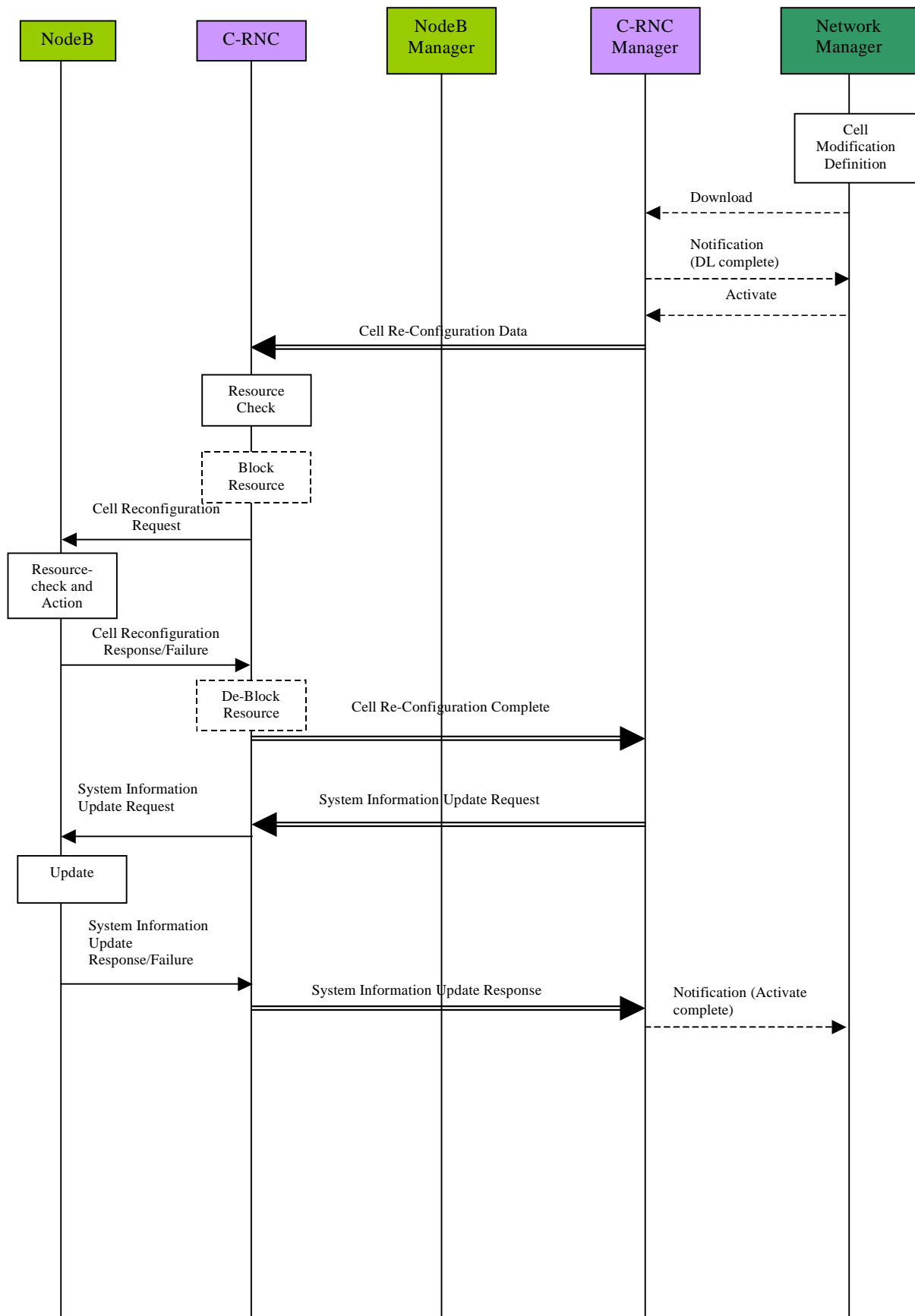


Figure 5.3.2.1: Cell Re-configuration Initiated by the Management System

The procedure above consists of the following steps:

1. The change to the cell configuration is defined and created in the Network Manager by the operator. This may be by manual means or as an output from a network optimisation tool. The definition should include the cell identifier and the associated C-RNC identifier.
2. The operator initiates the re-configuration of the cell, and the Network Manager initiates the cell re-configuration data Download to the appropriate C-RNC manager.
3. The C-RNC manager returns a Notification (DL Complete) to the Network Manager to indicate successful data transfer.
4. The Network Manager then initiates the activation of the re-configured cell by sending an Activate message to the C-RNC manager.
5. The C-RNC manager passes the cell re-configuration data to the C-RNC.
6. The C-RNC performs a check on the requested configuration changes to ensure they are compatible with the remaining cell configuration and capabilities.
7. If required, the RNC blocks resources that may be affected by the cell re-configuration, e.g. the cell itself or adjacent cells that may also need re-configuration.
8. The C-RNC issues a Cell Re-configuration Request to the target Node B.
9. The Node B performs a check on the requested configuration changes to ensure they are compatible with the remaining Node B configuration and capabilities.
10. Node B then performs the re-configuration of the cell and/or transport channels, including any implementation specific re-configuration (between Node B and its manager – not shown).
11. Once complete, the Node B advises the C-RNC that the configuration of the cell has been successful with the Cell Re-configuration Response message. In the case of a failure the Cell Re-configuration Failure message will be issued.
12. The RNC de-blocks any resources that have previously been blocked. The Node B is not involved in this blocking/de-blocking, since it only affects logical resources within the RNC.
13. The RNC then advises the C-RNC manager that the reconfiguration of the cell has been successful (cell Re-configuration Complete).
14. After successful cell re-configuration the RNC may invoke the System Information Update procedure (if the system information has changed during the cell re-configuration).
15. The RNC invokes the System Information Update procedure in order to start transmission of system information in the re-configured cell.
16. When the cell is successfully operating, the C-RNC reports successful cell operation to its manager.
17. The C-RNC manager finally reports successful cell establishment and activation to the Network Manager by sending the Notification (Activate complete).

The procedure below represents one possible method by which a cell can be automatically reconfigured from the RNC.

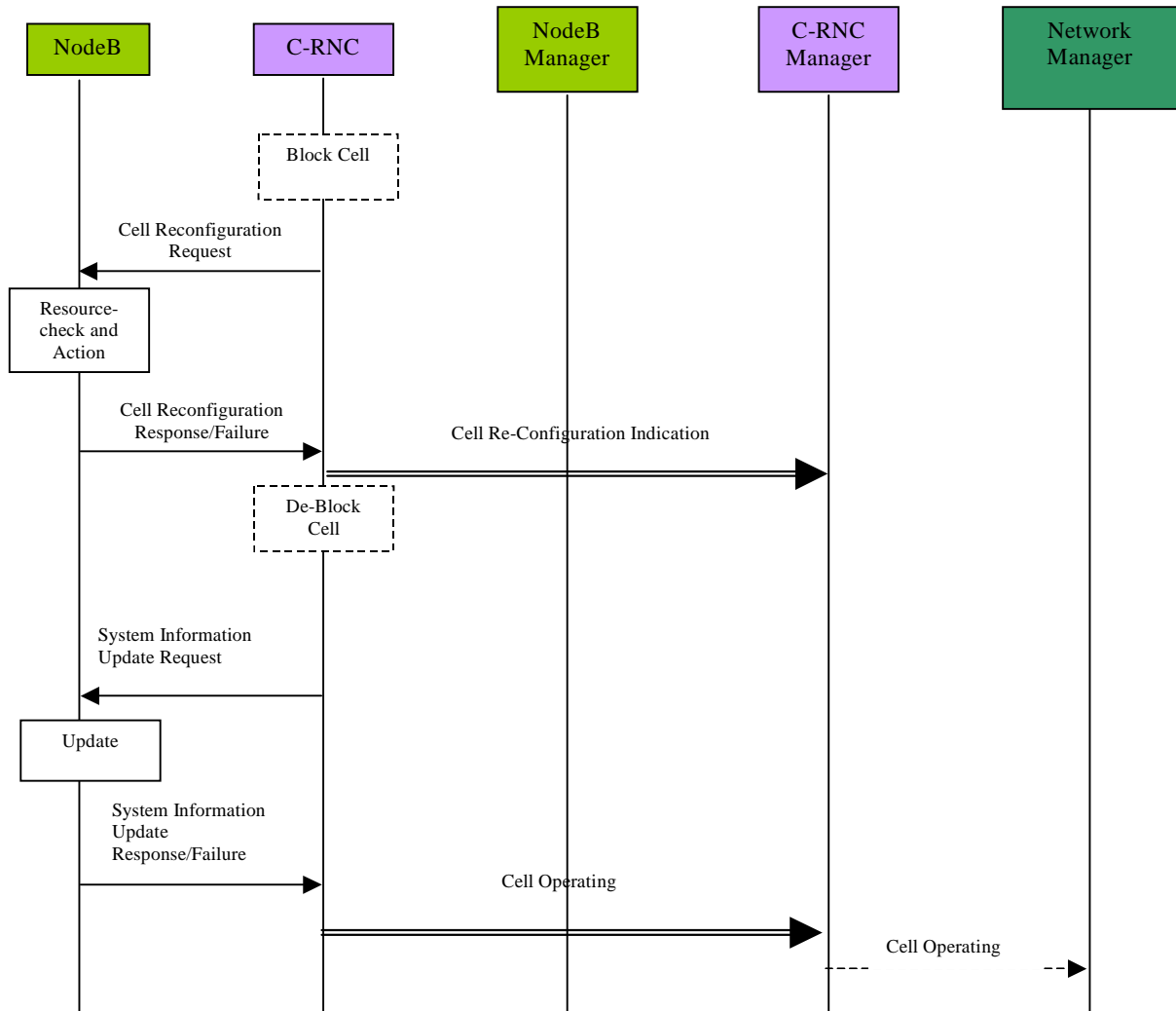


Figure 5.3.2.2: Cell Re-configuration Initiated by the RNC

The procedure above consists of the following steps:

1. Following a decision in the radio resource algorithms to perform a cell re-configuration (due to the traffic conditions), the C-RNC blocks any resources, which may be affected by the procedure e.g. the cell itself or adjacent cells that may also need re-configuration.
2. The C-RNC sends a cell re-configuration request to the target Node B.
3. The Node B performs a check on the requested configuration changes to ensure they are compatible with the remaining Node B configuration and capabilities.
4. Node B then performs the reconfiguration of the cell, including any implementation specific reconfiguration (between Node B and its manager – not shown).
5. Once complete, the Node B advises the C-RNC that the re-configuration of the cell has been successful.
6. The C-RNC then advises its manager (which in turn advises the Network Manager) of the cell re-configuration that has been executed, for updating of the management system cell database. In the meantime the RNC de-blocks any resources that have previously been blocked. The Node B is not involved in this blocking/de-blocking, since it only affects logical resources within the RNC.
7. After successful cell re-configuration the RNC may invoke the System Information Update procedure (if the system information has changed during the cell re-configuration).
8. The RNC invokes the System Information Update procedure in order to start transmission of system information in the re-configured cell.
9. When the cell is successfully operating, the C-RNC reports successful cell operation to its manager.
10. The C-RNC manager reports successful cell operation to the Network Manager.

5.4 Network Optimisation Procedure

5.4.1 Reports relating to cell performance

In order to identify possible modifications that allow an improvement of the overall network performance this procedure describes the collection of measurement data within the cell. The resulting measurement reports are discussed below.

- **No. of active channels per cell**

In order to compare the planned cell capacity with the real traffic load, the number of active channels within the cell has to be measured. This has to be done at least in a statistical way, e.g. n active channels per measurement time period (e. g. 15 minutes). The operator has to know the data rates/services of these channels. For example, the output of this collection could be:

```
12:00 - 12:15
  8k circuit switched service:    16
 16k circuit switched service:    12
128k circuit switched:           2
358k packet switched:            1

12:15 - 12:30
  8k circuit switched service:    12
128k circuit switched:           1
358k packet switched:            2
```

It is FFS if some information is also necessary regarding the Spreading Factor (SF) and the use of multi-code transmission.

- **Sector call Set-up**

The number of call set-up attempts within a cell **shall has to** be measured, together with the number of call set-up failures and the reasons for these failures. These measurements **should** distinguish between UE originated and UE terminated calls.

The sector call set-up failures **shall** distinguish between failures which occur at Node B (i.e. before channel requests have been sent to the RNC) and those which occur in the RNC.

- **RF Loss**

The number of RF losses per cell **shall has to** be counted. It shall be possible to combine the result with a failure indicator.

- **Total Transmitted Power**

The output power of a Node B depends on the number of active channels and the location of the UEs. That means that the overall output power of a Node B varies. For network planning purposes, the interference given to the neighbour cells is required. So the distribution of the overall output power of a Node B (per sector) **shall has to** be reported to the Management Platform.

- **RSSI (FDD)/RxISCP (TDD)**

For the calculation of the UL interference level at the Node B (antenna connector) the overall received power **shall** be measured.

- **Received Signal Code Power**

The distribution of the received signal code power at the antenna connector **should** be measured.

- **Transmitted Code power**

The distribution of the transmitted code power at antenna connector **should be measured.**

- **Event Triggered Measurements**

It **shall be possible to define event-triggered measurements, where the triggers are used to initiate/terminate the reporting of the measurements. For these types of measurements, the actual measured entity **shall** be used as the reporting trigger.**

5.4.2 Reports relating to Node B performance

Node B hardware report

The Node B hardware report shall include the following:

- an overview of the share of the traffic load on the different hardware components (e.g. cards, RAKE receivers, etc.)
- stability report (e. g. out of service time)
- busy time of the different hardware components

Node B resource report

This report shall include the usage of the physical L1 resources (e.g. channel number, code number, etc.).

5.4.3 Reports relating to Handover performance

The number of successful / unsuccessful handover attempts is required for the optimisation of UTRAN, as well as the Core Network (CN).

The following cases **should** be included in the handover report (refer to [5]):

- softer handover
- intra RNC soft handover
- inter RNC soft handover
- intra cell hard handover
- inter cell hard handover
- inter Node B hard handover
- inter RNC hard handover
- handover from UMTS to GSM
- handover from GSM

The number of the branches should be part of these statistics.

It is FFS if there is any time information needed, e.g. how long a UE is in the handover case (i.e. average time).

5.4.4 Routing of the Performance Management (PM) reports

The RNC should be able to make traffic-handling decisions which best suit the system conditions at that time. Therefore some key statistics should be routed to the RNC. These key statistics should be common to all Node Bs and available to the RNC on a real-time basis. The Iub interface should be capable of supporting **their** transfer to allow the quality of service to be maximised.

Table 1 lists the PM reports. Besides these reports there will exist implementation specific reports.

Table 1: PM reports contents

Node B parameter / report	Node B to NM	Node B to RNC	RNC to NM
No. of active channels per cell			X
Sector call set-up	FFS		X
RF Loss			X
Total Transmitted Power	X	real-time meas.	
RSSI (FDD)	X	real-time meas.	
RxISCP (TDD)	X		
Received signal code power	X	real-time meas.	
Transmitted code power	X	real-time meas.	
Event triggered measurements	X	real-time meas.	
Node B hardware report	X		
Node B resource report	X		
Softer handover			X
Intra RNC soft handover			X
Inter RNC soft handover			X
Intra sector hard handover			X
Inter sector hard handover			X
Inter Node B hard handover			X
Handover UMTS to GSM			X
Handover from GSM			X
Inter RNC soft handover			X
Inter RNC hard handover			X
Data rates			X
Multi code usage			X
NOTE:	These counters are for information only, the normative list can be found in 3GPP TS 32.104 [11] annex C.		

The real-time measurements can be used for admission control. To avoid collision of the PM measurements in the Node B done in parallel by the NM and the RNC (real-time measurements) the NM starts the measurements in the Node B. The RNC can request these measurements.

5.5 Remote Node B Software Update

The remote Software Update procedure shall enable the software used by Node B to be updated remotely from the management system. The actual software used by Node B will be specific to a particular vendor implementation, and its

transfer should therefore be supported via Implementation Specific O&M. However, it is possible that the process of updating and/or activation of Node B software may impact on the logical resources within Node B. It is therefore necessary for the RNC to be involved in this process to enable the traffic handling to be optimised during such procedures.

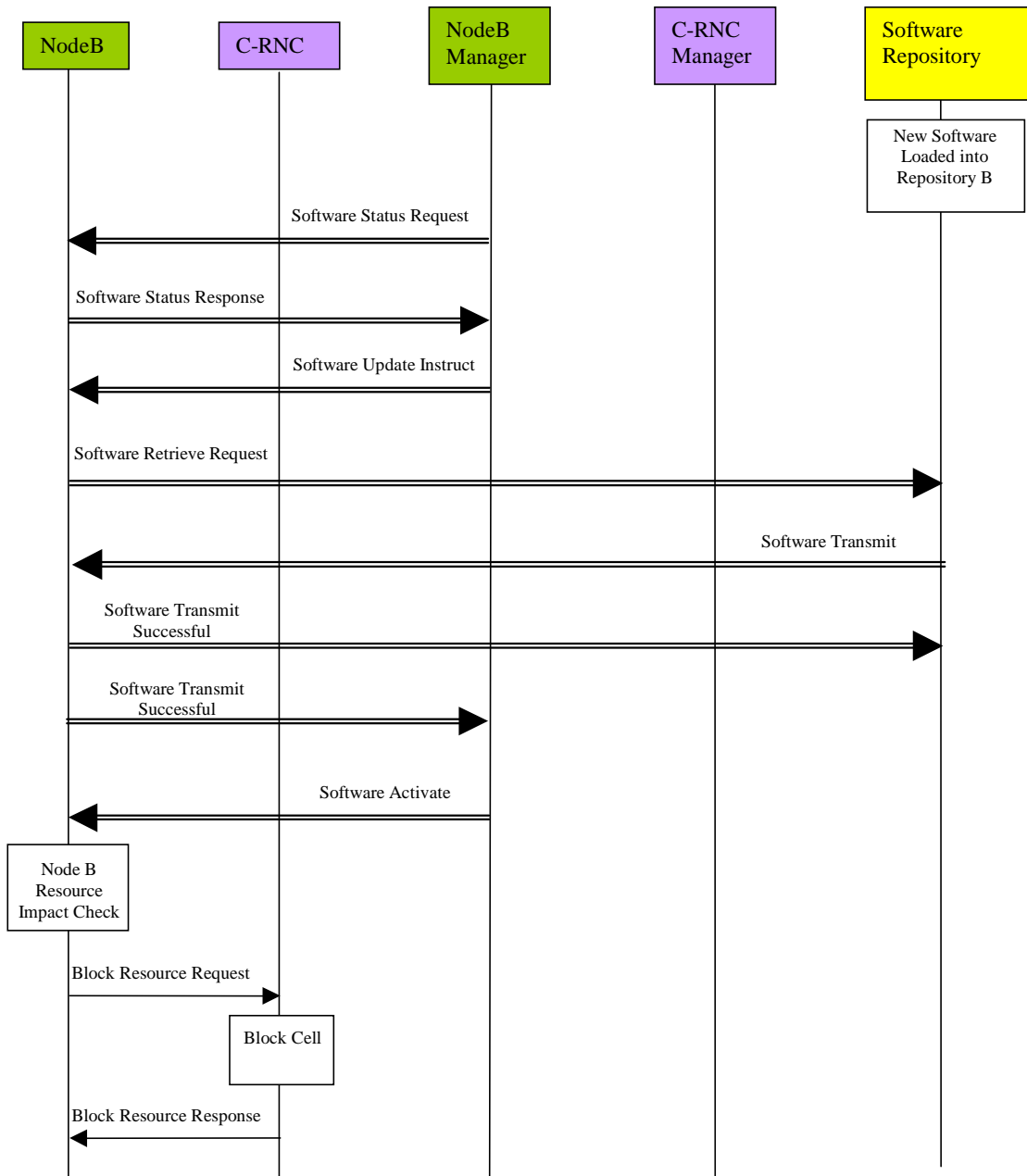
Two possible mechanisms to initiate the transfer of new software to the Node B are as follows. Firstly, the software may be located in a remote node and the Node B provided with an appropriate address to retrieve the software – this is referred to as a 'pull method'. Also, it is possible for the management system to provide the software directly to the Node B – this is referred to as a 'push method'. Both mechanisms should be supported in the standards, with the choice of which method to implement (or both) being left to vendor implementations and operator requirements.

5.5.1 Remote Software Update Procedure – Pull Method

The initiation of the remote upgrade of a Node B will originate from the management system. However, in a mature network a large number of Node Bs are installed and the process of simultaneously upgrading all Node Bs places great demands on the bandwidth requirements to the management system and the processing capability within it. To overcome this, the management system can manage the Software Update process in the normal way, however the actual software can be stored in remote software repositories, which can be accessed by the Node Bs. These software repositories are logical entities, which can be physically located anywhere in the UMTS.

In addition, the actual process of downloading software and/or activating it may impact on the logical resources supported in Node B. It is therefore necessary to ensure the RNC is advised of such impact and provided with the opportunity to defer the operation based on the traffic conditions.

The following procedure represents one possible method by which a Node Bs software can be remotely upgraded using a pull method. This procedure assumes that the associated Node B has already been installed and configured using separate procedures, and that both Iub and Implementation Specific O&M communications are therefore established.



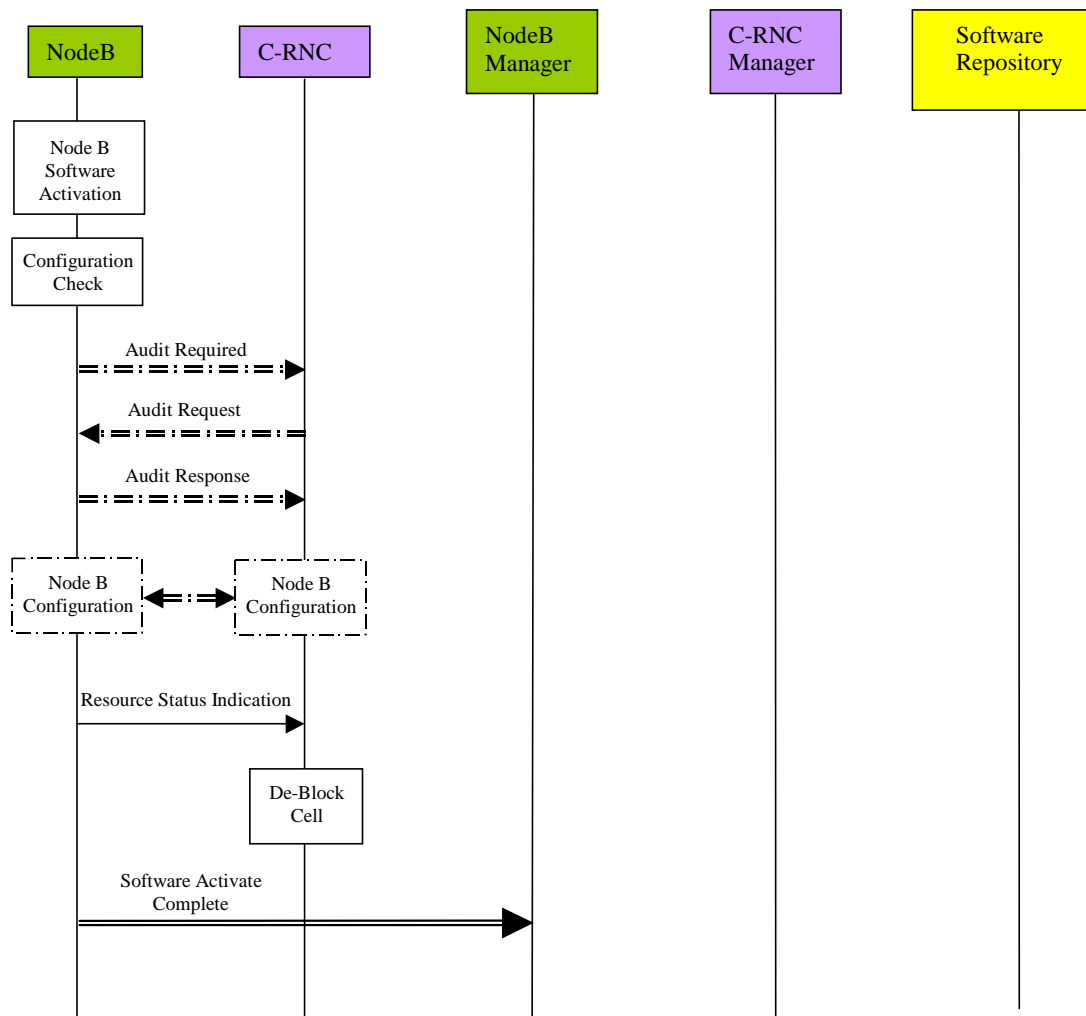


Figure 5.5.1.1: Remote Node B Software Update (Pull)

The procedure above consists of the following steps:

1. The new Node B software is loaded onto the software repository. A unique address is assigned to its location. This loading process may be performed remotely from the management system or manually by the operator.
2. The Node B management system requests the current software status of the target Node B.
3. The Node B responds providing its software status to its management system. The Node B management system is then able to determine whether a software update is required.
4. The Node B management system instructs the Node B to perform a software update. The address of the new software (located in the software repository) is provided.
5. The Node B then requests transmission of the new software from the software repository, using the address provided from the management system.
6. The software repository responds by transmitting the new software.
7. Node B confirms the successful receipt of the software to the repository.
8. Node B then advises its management system that the software transfer from the software repository was successful.
9. The Node B management system then instructs the Node B to activate the new software.
10. The Node B then determines whether the software activation process to follow will impact on the logical resources it is currently supporting. If logical resources are impacted, the Node B requests permission to block the associated resources from the RNC. The resources described should anticipate any requirement for a Node B restart to facilitate the activation process (if necessary). This request should carry a priority indicator (as defined in [1]) to indicate to the RNC whether it shall block the resources immediately (high priority shutdown) or whether it can delay or prevent the block (normal/low priority shutdown). For a normal shutdown, the request should also include a shutdown timer parameter (see [1]) to inform the RNC of the time available to perform the blocking. The priority indicator should be derived from the initial operator request.
11. The RNC will attempt to block the resources as requested by the Node B.

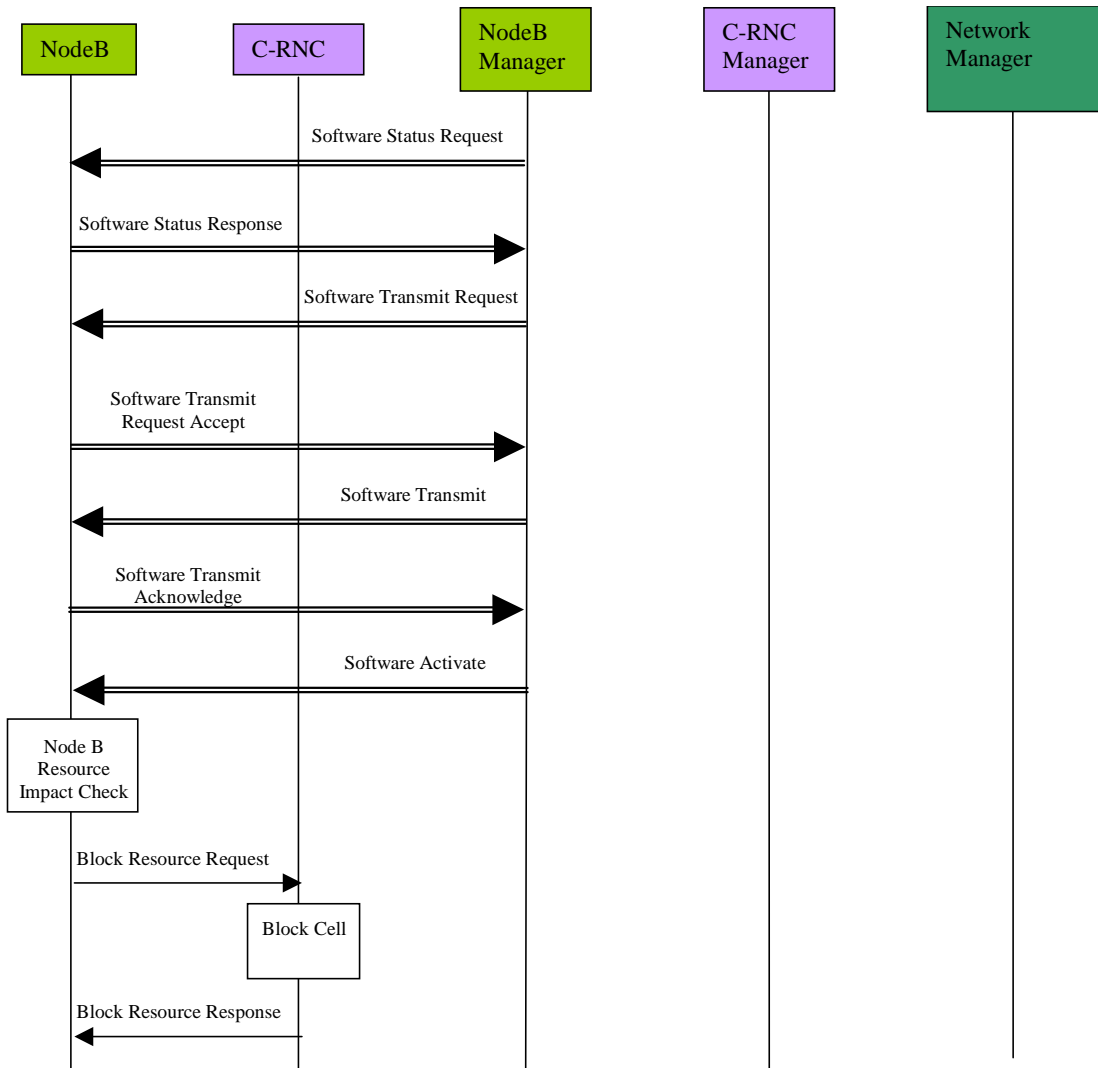
12. The RNC will respond to the Node B advising of the success or rejection of the block resource request. In this way the RNC may delay the blocking of the resources based on the traffic conditions, unless it is instructed to block them immediately (see above). This process will be repeated until all necessary resources have been blocked.
13. The Node B then activates the new software. Any loss/re-establishment of communication between the RNC and the Node B (for instance due to a possible restart) shall be performed by the transport protocols.
14. The Node B then performs a configuration check to determine whether any data may have been lost as a result of the software activation. If the Node B detects the possibility that data may have been lost, it requests the RNC to perform a configuration audit by issuing an audit-required message.
15. The RNC initiates a configuration audit of the Node B in response by issuing an audit request.
16. The Node B responds with its configuration status, and the RNC compares this with the configuration record in its database.
17. If a configuration error is identified, the RNC initiates corrective configuration measures. These may include the set-up, re-configuration or deletion of cells and common transport channels.
18. The Node B then indicates to the RNC the (restored) resources now available.
19. The RNC is then able to de-block any resources previously blocked as part of the procedure.
20. The Node B confirms to the management system that the software activation is complete.

5.5.2 Remote Software Update Procedure – Push Method

The initiation of the remote upgrade of a Node B will originate from the management system. Furthermore, the management system may also directly transfer new software to the Node B as part of the procedure. This approach is referred to as a push method.

In addition, the actual process of downloading software and/or activating it may impact on the logical resources supported in Node B. It is therefore necessary to ensure the RNC is advised of such impact and provided with the opportunity to defer the operation based on the traffic conditions.

The following procedure represents one possible method by which a Node B's software can be remotely upgraded using a push method. This procedure assumes that the associated Node B has already been installed and configured using separate procedures, and that both Iub and Implementation Specific O&M communications are therefore established.



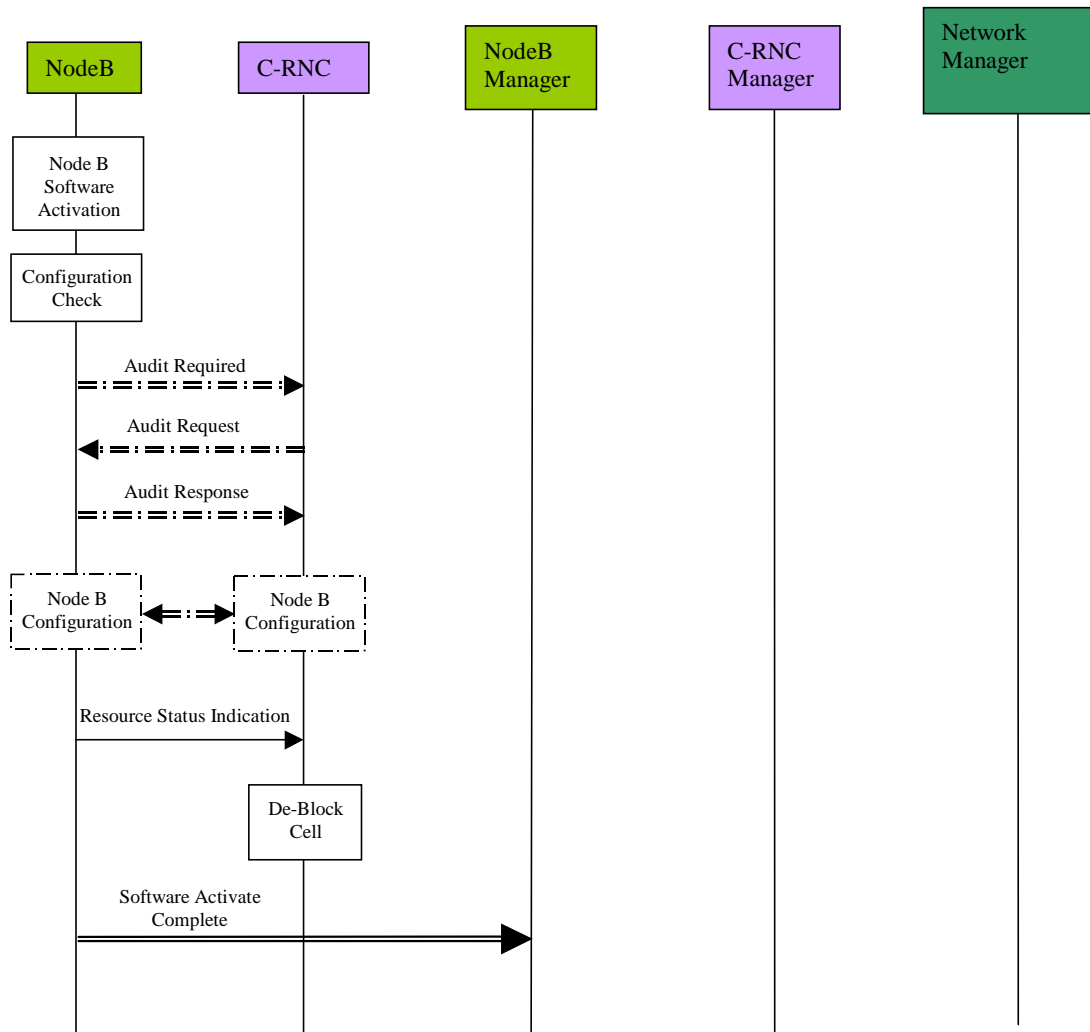


Figure 5.5.2.1: Remote Node B Software Update (Push)

The procedure above consists of the following steps:

1. The Node B management system requests the current software status of the target Node B.
2. The Node B responds providing its software status to its management system. The Node B management system is then able to determine whether a software update is required.
3. The Node B management system instructs the target Node B that a software update shall be performed.
4. The Node B accepts the software update instruction from the Node B management system, which responds by transmitting the new software.
5. Node B acknowledges to its management system the successful transmission of the new software.
6. The Node B management system then instructs the Node B to activate the new software.
7. The Node B then determines whether the software activation process to follow will impact on the logical resources it is currently supporting. If logical resources are impacted, the Node B requests permission to block the associated resources from the RNC. The resources described should anticipate any requirement for a Node B restart to facilitate the activation process (if required). This request should carry a priority indicator (as defined in [1]) to indicate to the RNC whether it shall block the resources immediately (high priority shutdown) or whether it can delay or prevent the block (normal/low priority shutdown). For a normal priority shutdown, the request should also include a shutdown timer parameter (see [1]) to inform the RNC of the time available to perform the blocking. The priority indicator should be derived from the initial operator request.
8. The RNC will attempt to block the resources as requested by the Node B.
9. The RNC will respond to the Node B advising of the success or rejection of the block resource request. In this way the RNC may delay the blocking of the resources based on the traffic conditions, unless it is instructed to block them immediately (see above). This process will be repeated until all necessary resources have been blocked.
10. The Node B then activates the new software. Any loss/re-establishment of communication between the RNC and the Node B (for instance due to a possible restart) shall be performed by the transport protocols.

21. The Node B then performs a configuration check to determine whether any data may have been lost as a result of the software activation. If the Node B detects the possibility that data may have been lost, it requests the RNC to perform a configuration audit by issuing an audit-required message.
22. The RNC initiates a configuration audit of the Node B in response by issuing an audit request.
23. The Node B responds with its configuration status, and the RNC compares this with the configuration record in its database.
11. If a configuration error is identified, the RNC initiates corrective configuration measures. These may include the set-up, re-configuration or deletion of cells and common transport channels.
12. The Node B then indicates to the RNC the (restored) resources now available.
13. The RNC is then able to de-block any resources previously blocked as part of the procedure.
14. The Node B confirms to the management system that the software activation is complete.

5.6 RNC Installation

The installation of the new RNC consists of the following steps:

1. Establishment of the connection to the management system.
2. Implementation specific initialisation of the RNC including the start of all functional entities residing in the RNC.
3. Establishment of all required Iu connections, e.g. signalling bearer for RANAP.
4. Establishment of possible Iur connections, e.g. signalling bearer for RNSAP.

After the local HW/SW installation, the (possibly) manual establishment of all ATM links, and the connection to the RNC Manager, the new RNC is initialised and configured by its Manager (possibly initiated from the NM). Similar to the Node B installation, the RNC may request its initialisation from the RNC Manager. After the initialisation/configuration some self-tests shall be performed. The results of these self-tests are reported back to the RNC Manager. Since the installation of a new RNC does not affect the NBAP messages, and most of the performed actions are implementation specific, the RNC installation will not be described further.

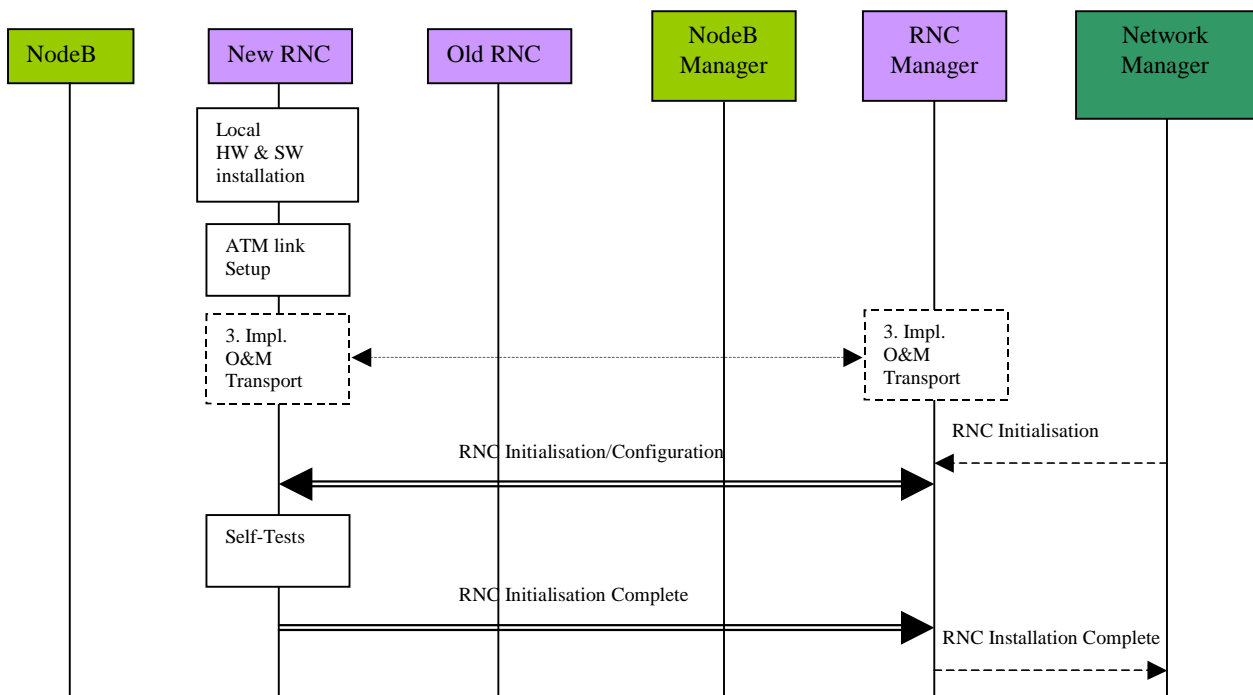


Figure 5.6.1: RNC Installation

5.7 Node B Expansion

The Node B Expansion procedure describes the integration/modification of equipment in Node B and the subsequent modification/configuration of the vendor independent parameters that have to be provided by the Management system (possibly as result of a previous planning process). The Node B expansion procedure applies whenever new or additional hardware/software modules have to be installed into a previously installed Node B.

In principle, the Node B Expansion procedure can be separated into two steps:

1. Implementation Specific O&M Expansion
2. Logical O&M Expansion

The above steps relate to the configuration of resources in Node B directly by the Management System, and the configuration of logical resources owned by the RNC residing in Node B, respectively. Assuming that the required configuration data (i.e. the parameters to be modified and their according value) have already been provided by a previous planning process, the procedure involves different entities for both expansion types.

5.7.1 Implementation Specific O&M Expansion

The Node B Expansion includes re-configuration of vendor dependent Node B parameters and/or the exchange/installation of hardware modules. The pre-requisite for the Implementation Specific Node B Expansion is a completely installed and configured Node B with an existing implementation specific O&M transport channel. The details of this expansion procedure are out of the scope of the present document, and the following figure intends only to clarify the involvement of the affected entities and the information flow between the RNC and the Node B (and their management entities). The RNC is only involved in the case where the availability of logical resources owned by the RNC (but physically located in the Node B) is impacted.

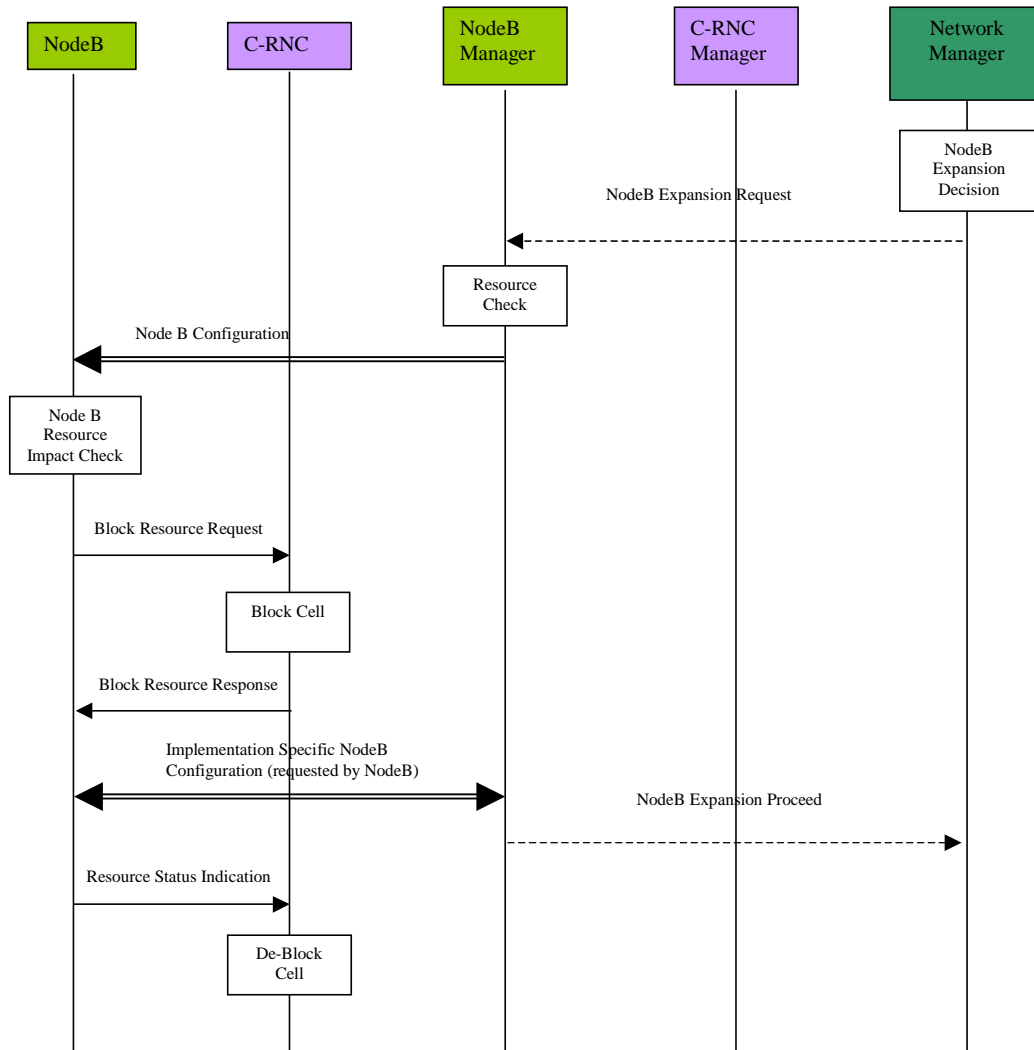


Figure 5.7.1.1: Implementation Specific Node B Expansion

1. The decision to perform a Node B expansion is derived in the Management System by the operator. A network optimisation tool can possibly be used to do this. In the case where there are separate sub-systems for the RNC and Node B management systems, and a separate Network Manager exists, there may be a *Node B Expansion Request* message from the Network Manager to the Node B Manager.
2. The Node B Manager checks the resources required to support this expansion (link capacity, etc.) and sends a *Node B Configuration* message via the implementation specific O&M channel. It should be noted that this procedure could be replaced by a technician pressing a button on the hardware module to be exchanged (for example). The following steps are still applicable where such manual triggering is used.
3. The Node B determines whether the expansion process to follow will impact on the logical resources it supports. The Node B may determine that itself or the Node B manager may provide this information. If logical resources are impacted, the Node B requests the RNC to block the associated resources. . This request should carry a priority

indicator (see [1]). By interpreting the requested priority the RNC can decide whether the resource shall be blocked immediately (high priority shutdown) or whether the RNC can delay the blocking (normal/low priority shutdown). The priority indicator should be derived from the operator expansion request. After blocking any impacted resources, the RNC sends a *Block Resource Response* message to the Node B indicating that the associated resources are blocked.

4. The necessary implementation specific configuration is then initiated/requested by the Node B (i.e. after it has received the *Node B Block Response* message). The implementation specific configuration (not depicted in detail) includes self-tests of Node B, and the report of these self-tests to the Node B Management System. After successful implementation specific Node B expansion, the Node B informs the RNC about the available resource via the *Resource Status Indication* message. Where a separate Node B Manager and Network Manager exist, the Node B Manager informs the Network Manager about the successful implementation specific expansion. The Node B Manager then indicates to the Network Manager that the remaining expansion processes may precede **i.e.** the logical expansion.
5. After receiving the *Resource Status Indication* the RNC de-blocks any previously blocked resources and resumes normal operation.

5.7.2 Logical Node B Expansion

The logical Node B expansion includes the re-configuration of logical resources owned by the RNC that might be physically supported by the Node B. This procedure shall be used to configure new Node B elements previously integrated by the Implementation Specific Node B Expansion. This expansion procedure contains no hardware modifications or any other implementation specific change. This procedure is comparable to the Cellular Network Configuration Procedure.

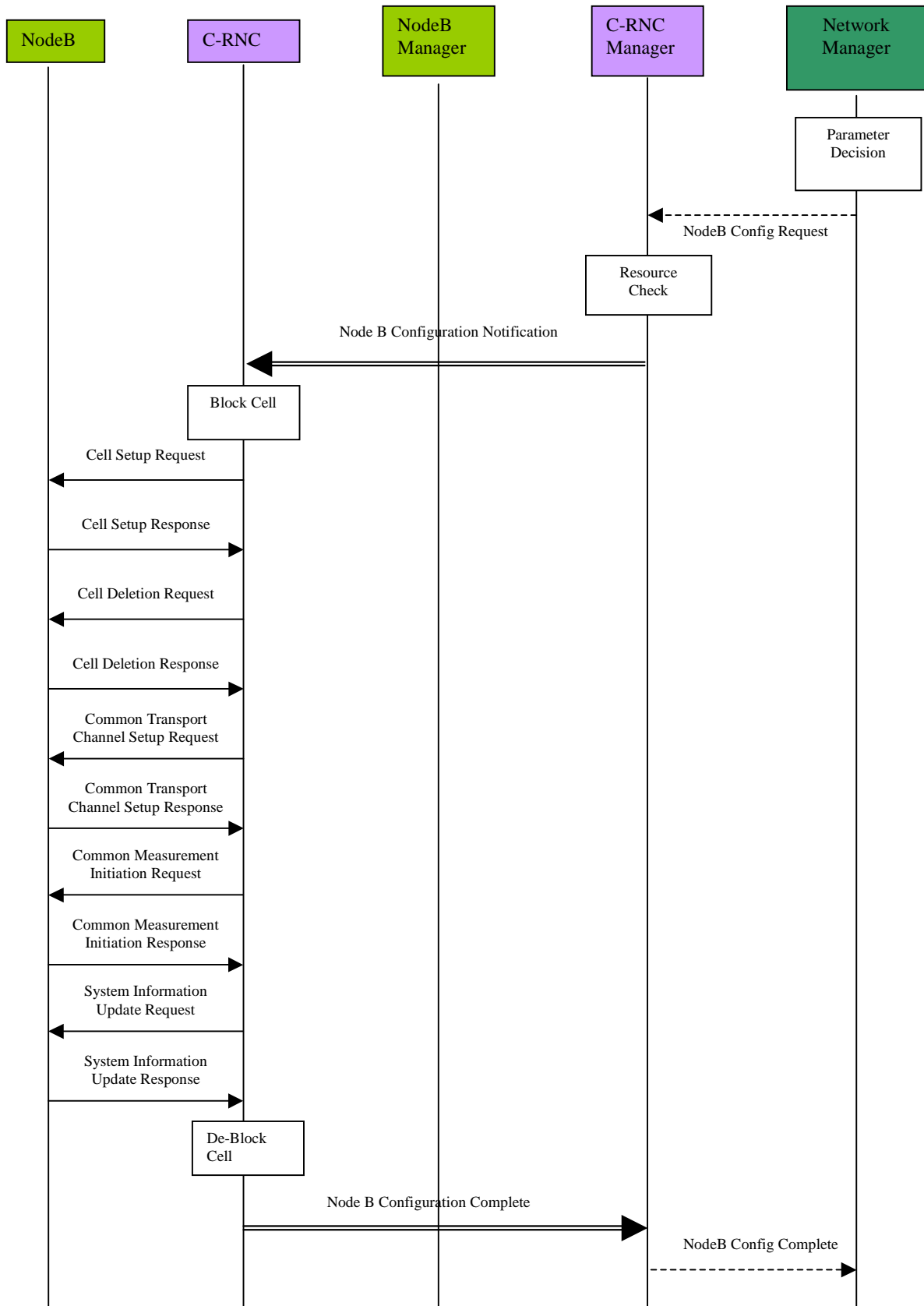


Figure 5.7.2.1: Logical Node B Expansion

1. The new cell parameters or common transport channel configuration is defined by the Network Manager as a result of a previous network optimisation process. Where separated sub-systems exist for Node B, RNC and the Network Manager, a configuration request may be issued from the Network Manager to the RNC Manager with all the required information to establish the new logical resources in the expanded Node B. It should be noted that the above procedure might be triggered by the Node B Expansion Proceed message (see subclause 5.7.1), sent as a final result of the implementation specific expansion.
2. The RNC Manager performs a resource check for the required expansion, and initiates the Node B logical expansion by sending the new parameters to the associated RNC and requesting the re-configuration of the Node B.
3. The RNC may block any logical resource supported by the Node B, which are impacted by the expansion process, e.g. a cell.
4. To perform the required changes to the configuration of a cell, the RNC sends a cell set-up request message to the Node B. The Node B will respond with a cell set-up response or with a failure notification (cell set-up failure). The same principle is applicable for the deletion of a cell. The RNC may also perform changes using a cell re-configuration request, as required.
5. In order to perform a common transport channel set-up, the RNC requests the establishment of all required channels using a common transport channel set-up request message to the Node B. The successful establishment or possible failure is reported back to the RNC by a Common Transport Channel Set-up Response message or common transport channel set-up failure message respectively. The RNC may also perform changes using a common transport channel re-configuration request, as required.
6. New measurement tasks may then be initiated (or existing ones terminated) by the RNC, and system information messages updated from the RNC. The RNC can then unblock both the resources previously blocked as part of the procedure, and those newly configured resources resulting from the Node B expansion.
7. The result of the Node B logical configuration procedure is reported to the RNC Manager. The complete Node B Configuration (both implementation specific and logical) may then be reported to the Network Manager.

5.7.3 Overall Node B Expansion

From the above descriptions the required actions that have to be fulfilled by the affected NEs can be derived. The following list represents a summary of the above procedure descriptions, with respect to the actions to be performed in the Node B, RNC and Management System:

- The re-configuration of implementation specific parameters and equipment shall be triggered by a request message from the Node B Manager to the Node B via the implementation specific O&M signalling channel. Alternatively a manual trigger should be also possible.
- After receiving the configuration request (including any parameters required to indicate which Node B parts are involved) the Node B may request the blocking of the affected logical resource(s) in the RNC.
- After the implementation specific configuration the Node B performs a self-test and sends a report of the results to the Management System via the implementation specific O&M signalling channel.
- Following the implementation specific Node B expansion, the RNC has to be notified about the status of the available resources.
- In order to configure the logical resources owned and controlled by the RNC (but physically supported by the Node B) the RNC Manager has to be notified of the required Node B expansion, and shall then send all the required logical configuration information (e.g. new cell parameters) to the associated RNC. This shall constitute a request for the configuration.
- After receiving the configuration request from the Management System, the RNC has to perform all required tasks to configure the Node B properly, (i.e. cell set-up, re-configuration, or deletion; set-up, re-configuration or deletion of common transport channels; initiation or termination of measurement tasks in Node B).
- The completion of the logical Node B expansion (and the result) shall then be reported back to the RNC Manager by the RNC.

5.8 Node B Swap

Within the Node B Swap Procedure one or more Node Bs might be detached from existing RNCs and attached to other RNCs. For example the installation of a new RNC can trigger the Node B Swap procedure. There are five possible steps to be performed:

1. Physical installation of the new RNC and of all links.
2. Configuration of the new RNC.
3. Re-configuration of the old RNC (including possible re-configuration of adjacent Node B's attached to this RNC).
4. Detachment of the Node B from the existing RNC.
5. Attachment of the Node B to the new RNC.

The Node B Swap is one of the most labour intensive procedures, and optimisation of this procedure is a valuable improvement of the overall network O&M. For operators it is important to minimise the interruption time of the Node B swap operation. In particular, this procedure consists of several other procedures. The (re-)configuration of RNCs and Node Bs can be included in the Cellular Network Configuration procedure and the Node B Expansion procedure. The

attachment of the Node B to the new RNC is comparable to a Node B installation. These procedures will not be described in detail; only possible trigger messages or result messages will be considered. Assuming that all physical links and the site for the new RNC are prepared, the description starts with the installation of a new Node B.

5.8.1 Installation of a new RNC

See subclause 5.6.

5.8.2 Re-configuration of old RNC

The old RNC has to be re-configured in order to adapt it to the change of resources caused by the detachment. Therefore within the Node B Swap procedure the Network Manager sends an RNC re-configuration request to the Manager of the old RNC. In the described example the RNC Manager for the old and the new RNC reside in the same entity. It should be noted that there may be separate Managers, e.g. in case of RNCs from different manufacturers. Since it is likely the radio parameters in the cells of the old RNC will change by detaching one Node B, the RNC re-configuration should re-configure the data in its Node Bs that is not implementation specific. Therefore, the RNC re-configuration consists of the configuration of the RNC and several other Cellular Network Configuration procedures. The Network Manager may send an RNC Re-configuration Request to the RNC Manager (in the case that both management entities exist separately). The RNC Manager then performs a modification check (taking into account the capabilities of the old RNC) and performs the RNC re-configuration. After some self-tests the RNC Re-configuration Complete message is sent to the RNC Manager. Following the RNC re-configuration the RNC Manager that also has control over the logical RNC resources (i.e. cells) performs one or more cell re-configuration procedures (refer to subclause 5.3). The finalisation of the whole re-configuration, i.e. RNC and associated cell re-configuration(s), is reported to the Network Manager. If any inconsistency of the configuration data in the RNC and Node B is detected, the RNC invokes the Audit procedure to check the configuration status.

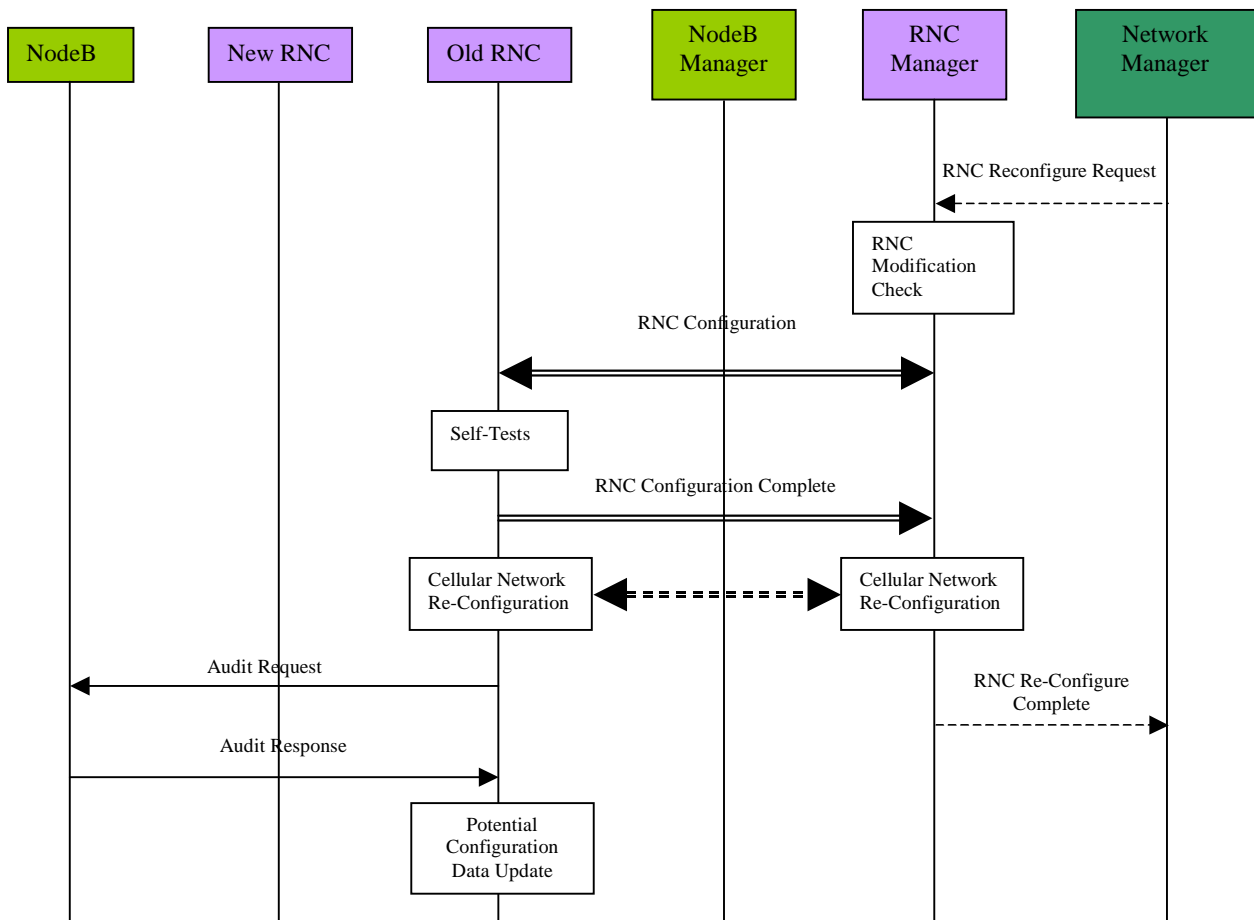


Figure 5.8.2.1: RNC Re-configuration

5.8.3 Node B Detachment

First the Network Manager requests the detachment from the according Node B Manager. The Node B Manager informs the Node B (via implementation specific O&M signalling) that the Node B will be detached. After receiving the detach request, the Node B asks the RNC to block the logical resources it supports. This step may be performed as part of the re-configuration of the old RNC. When the Node B receives the result of the blocking procedure from the RNC, it reports its blocked-state back to the Node B Manager and initiates its detachment. The subsequent implementation specific detachment includes the release of established connections (signalling bearer for NBAP and implementation specific O&M). The completion of the detachment should be reported to the Network Manager by the Node B manager.

5.8.4 New Installation

As soon as the Network Manager receives the Node B Detach Complete message, it may trigger the installation of the detached Node B to the new RNC. For example, the Network Manager may inform the installation technician to install the Node B. The remaining installation process is the same as for the normal Node B installation. Refer to the Node B installation procedure for details (see subclause 5.2).

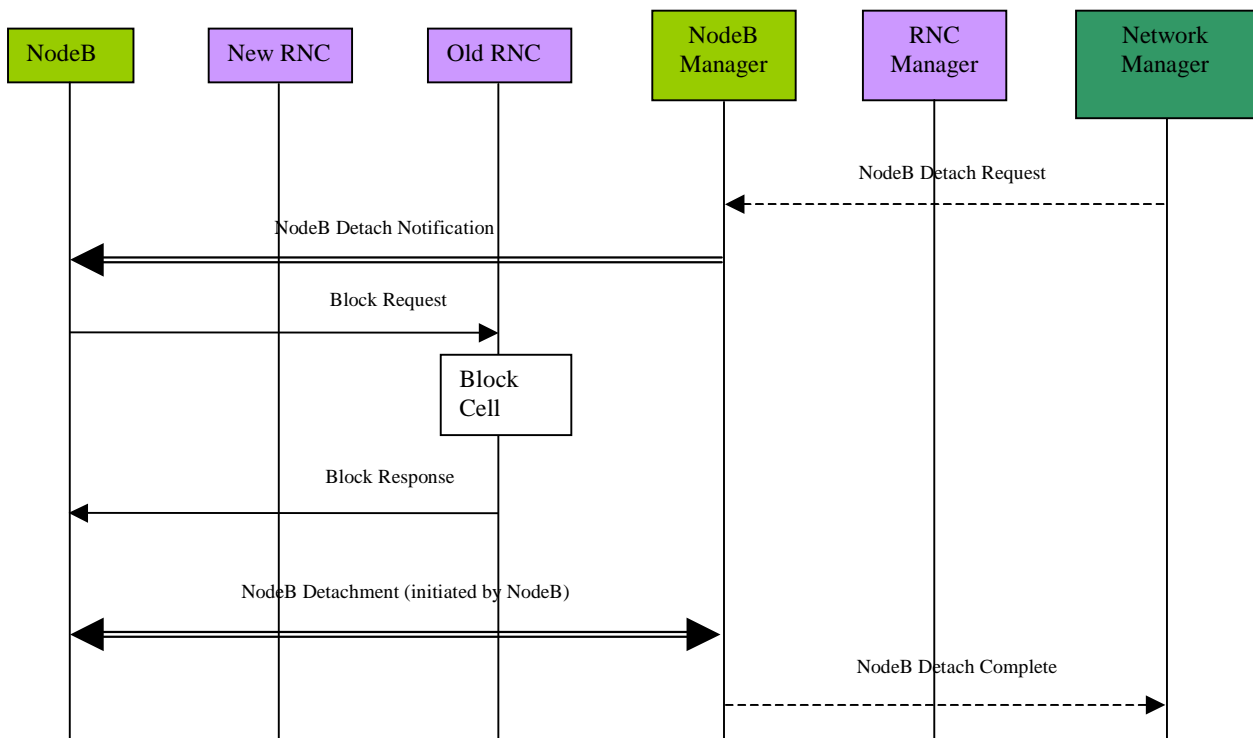


Figure 5.8.4.1: Node B Detach

- Since the Management System receives separate reports for each sub-procedure, i.e. for RNC installation, Node B installation and RNC re-configuration the whole procedure can be seen as successful if all sub-reports indicate successful sub-procedures.

5.9 Network Monitoring and Fault Management Procedures

The Network Monitoring and Fault Management Procedures observe the status of NEs and handle alarm and event notifications. In addition to network generated information customer complaints may be considered. Since most faults and alarms are inherently related to vendor specific hardware and software failures, the functions of Fault Management are implementation specific and should be handled using implementation specific O&M. In order to exchange failure information between Node B and RNC, the logical O&M shall also support Fault Management. As defined in [1], this shall be achieved using state management of the logical resources, which shall be compliant with ITU-T X.731 [8]. In the case where failures impact on the services supported the RNC should report these service failures to the Management System. The interaction between the UTRAN nodes (with respect to the entire UTRAN Network Monitoring and Fault Management) is depicted in figure 5.9.1 below.

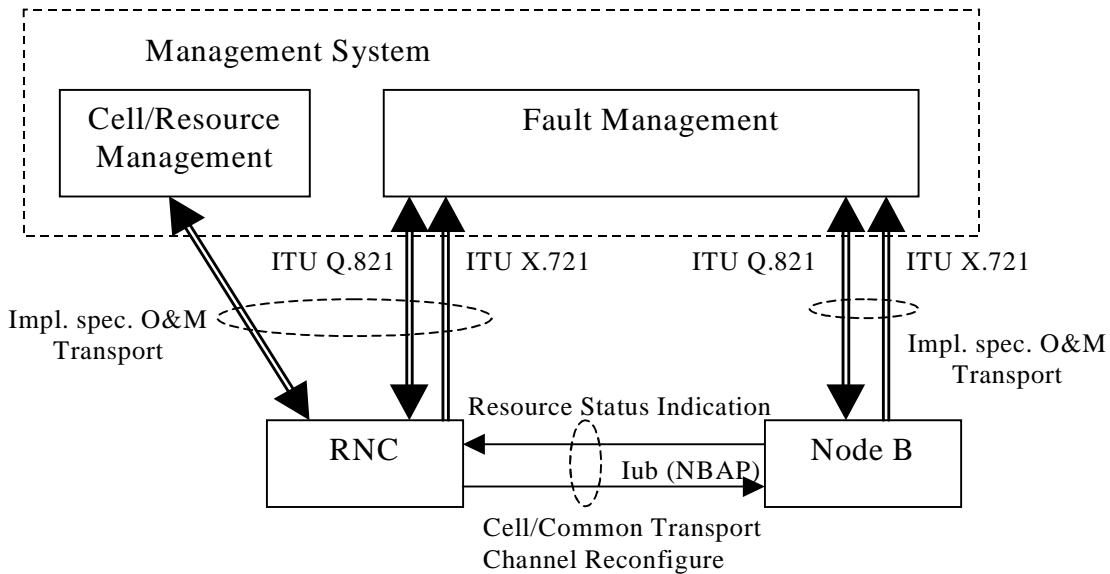


Figure 5.9.1: UTRAN Fault Management

It should be noted that the Management System shown above represents the management of the whole UTRAN and this may consist of a number of sub-systems with different functionality. As such the Management System should not be seen as one physical element, but as a logical entity that may be distributed over several physical network nodes. As part of the overall Fault Management process, a number of individual NBAP messages may be initiated (e.g. cell/common transport channel re-configure). These procedures will not be described in detail.

5.9.1 Implementation-specific Fault Management

For hardware or software failures appropriate alarms should be sent to the Fault Management sub-system of the Management System. One supported alarm message format could be based on [7]. It should be noted that the Q3 interface [6] should not necessarily be used; the alarm signalling should only be backwards compatible to the Q3 interface. The alarm signalling traffic should be carried by the implementation specific O&M transport from Node B and the RNC, to the Fault Management sub-system. The information contained in the alarm messages shall be used to locate the failure and to repair or replace the faulty modules.

5.9.2 Alarm Filtering and Correlation

The correlation of alarms is crucial to reduce the alarm signalling traffic between the network nodes and the Management System. Therefore both RNC and Node B have to perform alarm correlation and filtering. The mechanism used by the Node B and the RNC to perform alarm correlation/filtering to the management system shall be an implementation matter. The issue of *Resource Status Indication* messages from the Node B to the RNC shall be as defined in [1].

In addition to correlation and filtering, a record of UTRAN alarms (possibly contained in a database) may be beneficial in order to determine the reason for certain faults, and to facilitate comprehensive responses to customer complaints. This database should provide information about failure causes, time and date, location, and the affected logical resource and service. It should also be possible to correlate a specific user identity with a failure event, and the management system should therefore be capable of associating alarms received against both implementation specific and logical resources. To enable this, the UTRAN shall therefore support all the necessary identifiers to ensure a given event can be uniquely identified. The support of this failure database within the management system shall be an implementation issue.

5.9.3 NBAP alarm messages

With respect to Node B failures, it is necessary to inform the RNC about the unavailability of logical resources due to Node B hardware/software faults. For major failures, i.e. failures that significantly limit the operation of one cell or an entire Node B, the RNC should inform the Management System. However, it may also be possible for there to be two stages in handling major failures.

In the first stage the RNC performs emergency action(s) for immediate failure handling. Then in the case of permanent failures of non-redundant elements, the Management System may initiate a second stage such as the re-configuration of

cells or possibly a whole Node B. As soon as the failure in Node B has been removed (and the affected resource is ready to operate) the Node B notifies the RNC about the available resources using a *Resource Status Indication* message. The RNC/management system may then re-configure the Node B to restore the previous configuration (i.e. before the failure).

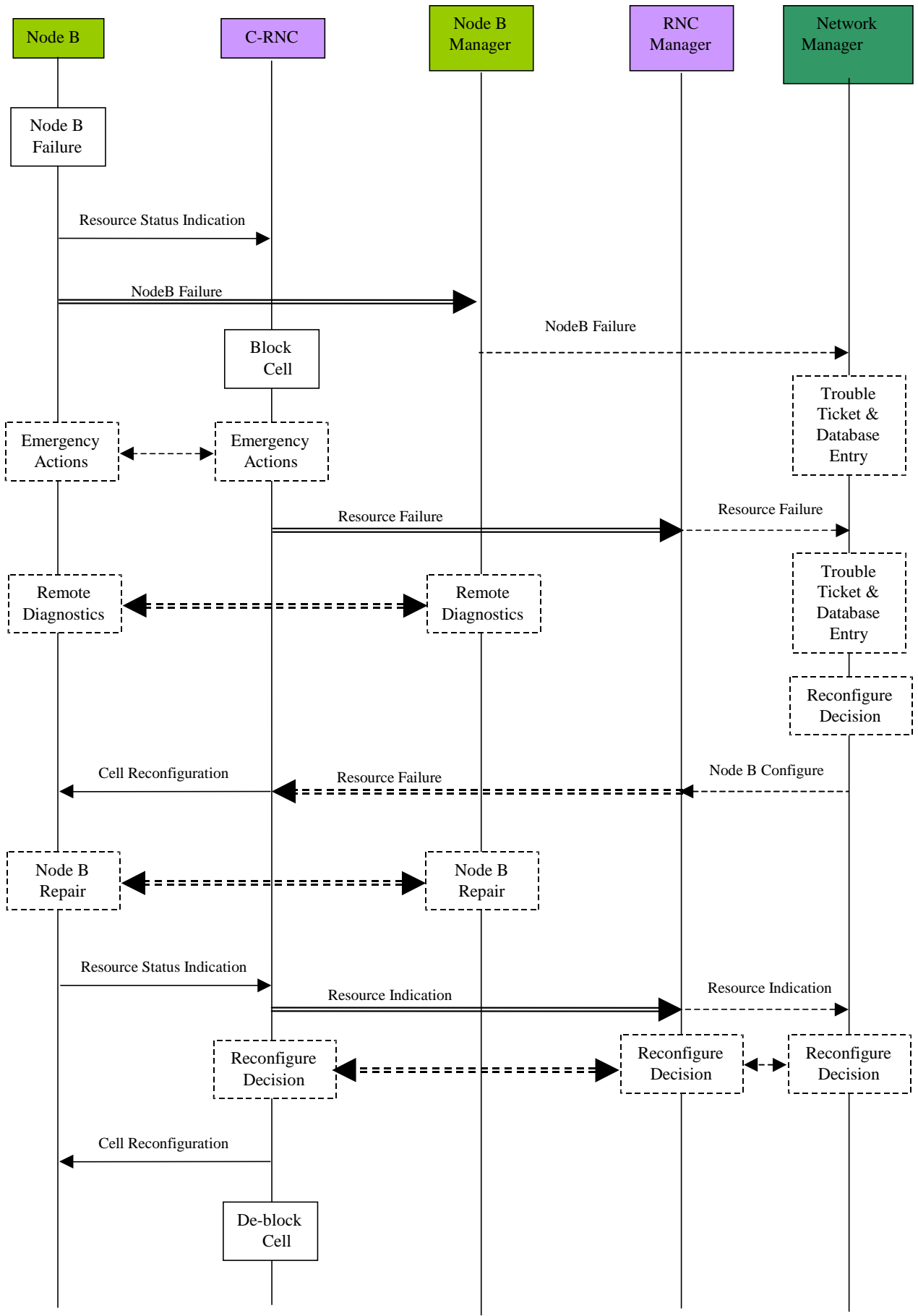


Figure 5.9.3.1: Node B Fault Handling Procedure

From the above diagram the actions that have to be performed by the affected NEs can be derived. The following list represents a summary of the procedure with respect to the actions to be performed by Node B, the RNC and the Management System:

1. In the case of a failure in Node B, the RNC and the Management System shall be notified by the Node B. The RNC may block the logical resource affected.
2. The RNC performs some immediate action to reduce the impact of the failure on logical resources and services (emergency actions). This is stage one of the fault handling and is marked with the dashed line in figure 5.9.3.1 above.
3. The Management System initiates the appropriate procedure to handle the failure. Additionally, a failure database entry can be created.
4. The fault handling function in the Management System should trigger a remote diagnostics procedure.
5. For major failures that significantly and permanently limit the operation of the affected resource, (e.g. a cell), the Management System can decide to take this resource out of order due to failure and repair. In this case a Node B or one or more cell re-configuration procedures shall be triggered by the Management System.

NOTE: Other cells than the affected cell could also be re-configured, for example to extend their coverage in order to cover the affected cells area.

This is stage two of the fault handling and might be performed in addition to the emergency handling.

6. After the failure in Node B is removed, the Node B shall send a notification to the Management System (via the implementation specific O&M signalling channel) and a *Resource Status Indication* to the RNC informing about the availability of the repaired cell.

If (as a result of the failure) a re-configuration was performed, the RNC/management system may decide to restore the old Node B configuration by performing a further Node B re-configuration.

History

Document history		
TR01 v 0.0.1	2000-05	Initial Version based on I3.05 version 0.2.2 Document according to NBAP Specification 3GPP TS 25.433 v3.1.0
TR01 v 0.0.2	2000-07	Chapter level removed in chapter 5. Document layout changed according to template TR. Introduction and scope aligned to contents of document. Subclause 5.3.1 and 5.3.2 updated, changed "cell" to resource, added message towards NM. Subclause 5.5.1 and 5.5.2 updated, blocking cell during software download removed. Subclause 5.7.1 Node B Expansion Notification changed to Node B Expansion Request
TR01 v 0.0.3	2000-10	Rephrased Introduction Changed Network Management Center (NMC) to Network Manager (NM) Updated figure 4.1.1 to match 3GPP TS 32.101 figure. Removed Itf-N abbreviation in scope chapter. Subclause 3.1: renamed procedures to message flows Added item RNC installation in 4.2.1. Removed chapter 5.1 (NBAP message overview) Installation of new RNC added also as separate chapter (5.6) Chapter 5.3.1. updated according to Common Configuration Management Chapter 5.3.2. updated according to Common Configuration Management
v 0.0.1	2000-10	Document number changed
v 0.0.2	2000-12	Minor editorial changes
v 0.0.3	2001-01-17	Zoicas/MCC: Converted to 3GPP layout/rules. Editing, etc.
Editor for 3GPP TR 32.800 is:		
Martijn HIJDRA Mannesmann Mobilfunk GmbH Tel.: +49 211 533 3973 Fax : +49 Email : iu.consultant@d2mannesmann.de		
This document is written in Microsoft Word version 97.		