3GPP TR 32.800 V5.0.0 (2002-03)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Telecommunication Management;
Management Level Procedures and Interaction with UTRAN
(Release 5)

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

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 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 and 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: "UTRAN Iub interface NBAP signalling".

[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 lub Interface: Signalling Transport".

[5] 3GPP TS 25.832: "Manifestations of handover and SRNS relocation".

[6] ITU-T Recommendation Q.821 (1993): "Stage 2 and Stage 3 description for the Q3 interface - Alarm Surveillance".

[7] ITU-T Recommendation X.721 (1992): "Information technology - Open Systems Interconnection - Structure of management information: Definition of management information".

[8] ITU-T Recommendation X.731 (1992): "Information technology - Open Systems Interconnection - Systems Management: State management function".

[9] 3GPP TS 32.6xx (32.106 old numbering scheme): "Configuration Management".

[10] 3GPP TS 32.111: "Fault Management".

[11] 3GPP TS 32.104: "3G Performance Management (PM)".

[12] 3GPP TS 25.215: "Physical layer - Measurements (FDD)".

[13] 3GPP TS 25.225: "Physical layer - Measurements (TDD)".

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 clause 10.1.2 of 3GPP TS 25.401 [2].
- Implementation Specific O&M is defined in clause 10.1.1 of 3GPP TS 25.401 [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
CRNC	Controlling RNC
DL	Downlink
DRNC	Drift RNC
FDD	Frequency Division Duplex
FFS	For Further Study
HW	Hardware
IP	Internet Protocol
NBAP	Node B Application Part
NE	Network Element
NM	Network Manager
O&M	Operation and Maintenance
PM	Performance Management
PVC	Permanent Virtual Circuit
RANAP	Radio Access Network Application Part
RF	Radio Frequency
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
SW	Software
TDD	Time Division Duplex
UE	User Equipment
UL	Uplink
UMTS	Universal Mobile Telecommunications System
UTRAN	Universal Terrestrial Radio Access Network

4 UTRAN O&M

4.1 UTRAN O&M overview

Figure 4.1.1 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.

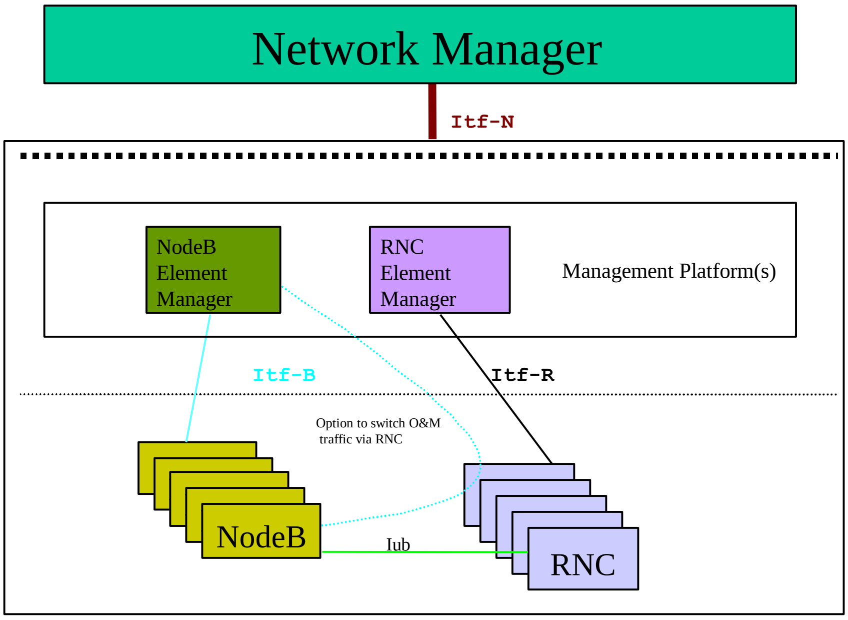


Figure 4.1.1: O&M Management Interfaces

The Management Interfaces are:

1. Itf-B - between Node B & its Manager (physically, this may be a direct connection or via the CRNC [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 clause 5.6).

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 clause 5.1.

Node B Swap: In case of integration of a new CRNC one or more Node Bs are detached from neighbouring CRNCs and attached to the new CRNC. After configuration of the Node B and the new CRNC and all according links, the Node B is detached from the old CRNC and operates connected to the new CRNC. Possibly Node B expansion procedures are triggered in all affected Node Bs.

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 clause 5.5.

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 discrete 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 CRNC) for the update according to its current load, etc. (see clause 5.2).

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 clause 5.4.

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.

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 clause 5.8)

4.3 Node B O&M Management Architecture

The working assumption for the Node B O&M management architecture is described in clause 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 clause 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 clause 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 examples 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.

Annex A contains a generic description of the processes 'blocking and unblocking of logical resources' which are used frequently in clause 5.

5.1 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 CRNC will be established. This includes the establishment of the NBAP signalling bearer (according to [4]).

NOTE 1: 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 CRNC, 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 CRNC about the completion of the Node B Initialisation by sending a RESOURCE STATUS INDICATION message. This provides the CRNC with the locally set parameters which are needed for the logical cell configuration, e.g. Local Cell Id(s) etc.

7. CRNC informs the CRNC Manager about the availability of the new Node B resources, and the CRNC Manager subsequently informs Network Manager (Step 7').

NOTE 2: The remaining logical cell configuration should be performed as described in clause 5.2.1.

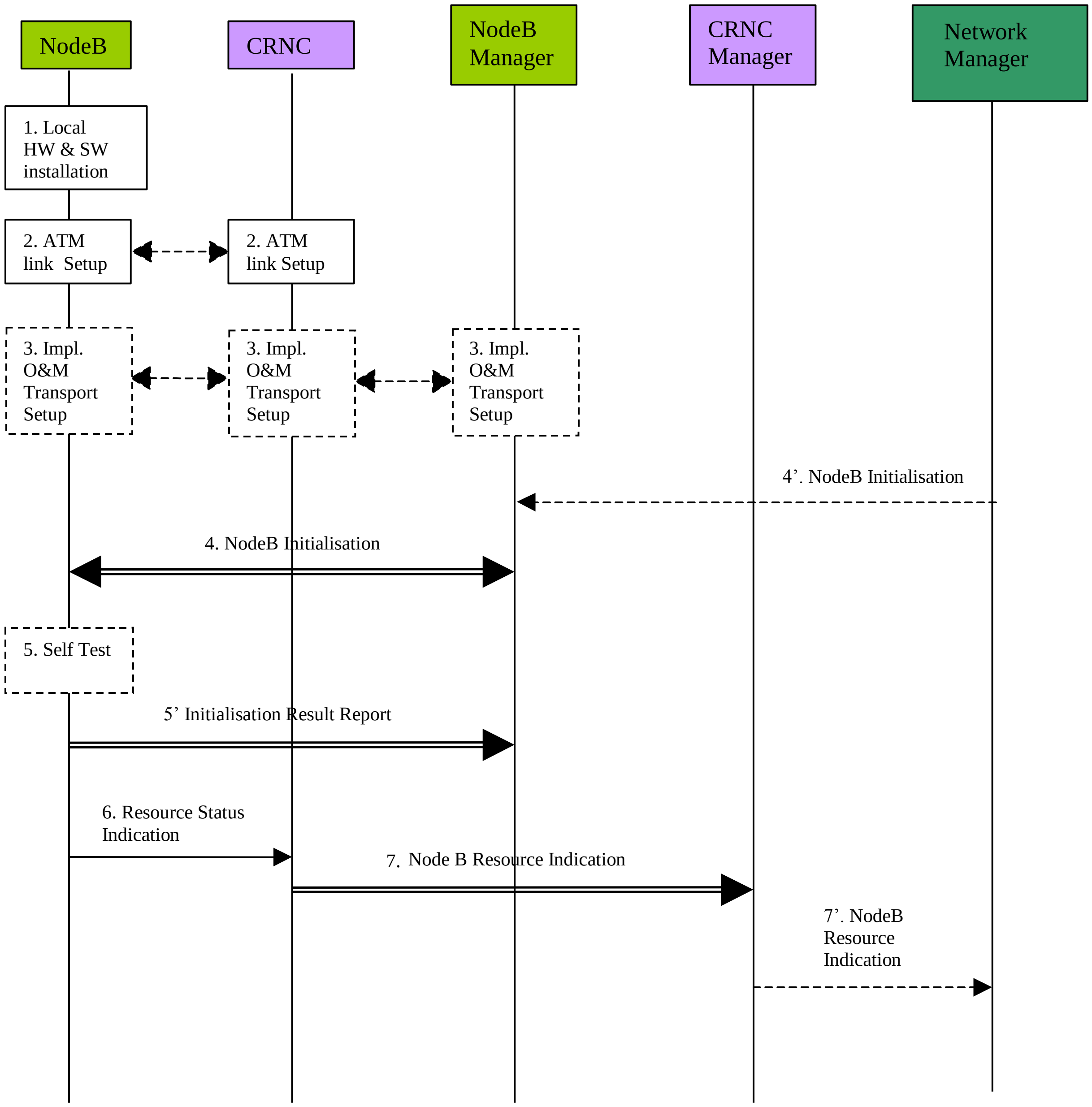

NodeB
CRNC
NodeB Manager
CRNC Manager
Network Manager
1. Local HW & SW installation
2. ATM link Setup
2. ATM link Setup
3. Impl. O&M Transport Setup
3. Impl. O&M Transport Setup
3. Impl. O&M Transport Setup
4'. NodeB Initialisation
4. NodeB Initialisation
5. Self Test
5' Initialisation Result Report
6. Resource Status Indication
7. Node B Resource Indication
7'. NodeB Resource Indication

Figure 5.1.1: Node B Installation and Initial Configuration Procedure

5.2 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.

5.2.1 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 clause 5.1, and that both Iub and Implementation Specific O&M communications are established. This procedure is also used when reconfiguring a cell (or cells) in the case that cell transmissions were switched off as part of the blocking process.

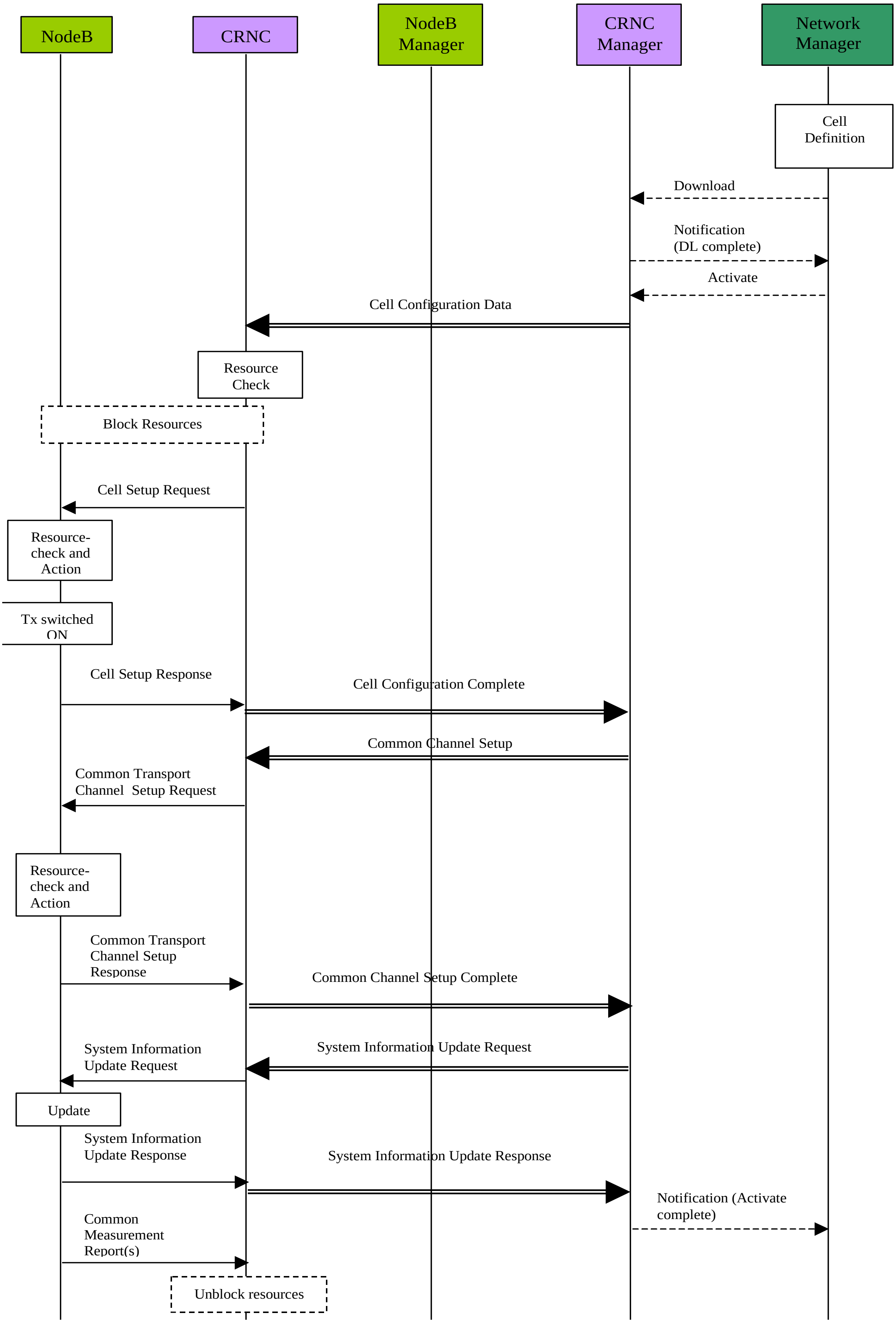

NodeB
CRNC
NodeB Manager
CRNC Manager
Network Manager
Cell Definition
Download
Notification (DL complete)
Activate
Cell Configuration Data
Resource Check
Block Resources
Cell Setup Request
Resource-check and Action
Tx switched ON
Cell Setup Response
Cell Configuration Complete
Common Channel Setup
Common Transport Channel Setup Request
Resource-check and Action
Common Transport Channel Setup Response
Common Channel Setup Complete
System Information Update Request
System Information Update Request
Update
System Information Update Response
System Information Update Response
Notification (Activate complete)
Common Measurement Report(s)
Unblock resources

Figure 5.2.1.1: Initial Cell Configuration

The procedure above shows an example for an initial cell configuration. Descriptions, which distinguishes between Bulk CM and Basic CM may be given after the related TSes are available. The procedure 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 CRNC. The identifiers are specified in 3G TS 25.401.
2. The operator initiates the creation of the cell, and the Network Manager initiates the cell configuration data Download to the appropriate CRNC manager.
3. The CRNC 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 CRNC manager.
5. The CRNC manager passes the cell configuration data to the CRNC for creation.
6. The CRNC 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 CRNC's capabilities and not the Node B.
7. If required the CRNC initiates blocking of any resources that may be affected by the cell configuration e.g. adjacent cells that may need a new configuration after the set-up of the new cell.
8. The CRNC invokes the CELL SETUP 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, and the subsequent configurations of other affected cells, which were blocked as part of this procedure, are modified, the Node B may switch on the transmission to all of these newly configured cells.
11. The Node B then advises the CRNC that the configuration has been successful using the CELL SETUP RESPONSE message for each new cell.
12. The CRNC then advises the CRNC manager that the configuration of the new cell(s) has been successful (Cell Configuration Complete).
13. The CRNC manager initiates the establishment of the required common transport channels and provides CRNC with the appropriate System Information for that cell.
14. The CRNC sends the COMMON TRANSPORT CHANNEL SETUP REQUEST message(s) to the Node B for each new cell.
15. Upon reception of this message, the Node B checks the available resources (e.g. Iub link capacity, etc.) and establishes the requested channel(s).
16. Success is reported back to the CRNC using the COMMON TRANSPORT CHANNEL SETUP RESPONSE message.
17. After successful establishment of the required common transport channels the CRNC invokes the System Information Update procedure in order to start the broadcast of system information in the established cells. The procedure is initiated with a SYSTEM INFORMATION UPDATE REQUESTmessage sent from the CRNC to the Node B, and followed by a SYSTEM INFORMATION UPDATE RESPONSE message being returned.
18. Common Measurement reports may be required to be sent to the CRNC from the Node B of the concerning cell(s). This is done by a COMMON MEASUREMENT INITIATION REQUEST being sent from the CRNC to the Node B, and followed by COMMON MEASUREMENT REPORT message(s) being returned from Node B to CRNC.
19. The CRNC internally unblocks the resources that have been previously blocked.
20. When the cell successfully begins operating, the CRNC reports successful cell establishment (and operation) to its manager.

21. The CRNC manager finally reports successful cell establishment and activation to the Network Manager by sending the Notification (Activate complete).

5.2.2 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 CRNC 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 CRNC giving the CRNC 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 CRNC does not include any Node B Implementation Specific parameters that 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 CRNC.

It should be noted that the blocking used in this case does not cause cell transmission to be switched off, and uses the System Information Update procedure to block the cell from the Node B. If cell transmission was required to be switched off, then the Initial Cell Configuration example (clause 5.2.1) would be carried out instead.

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

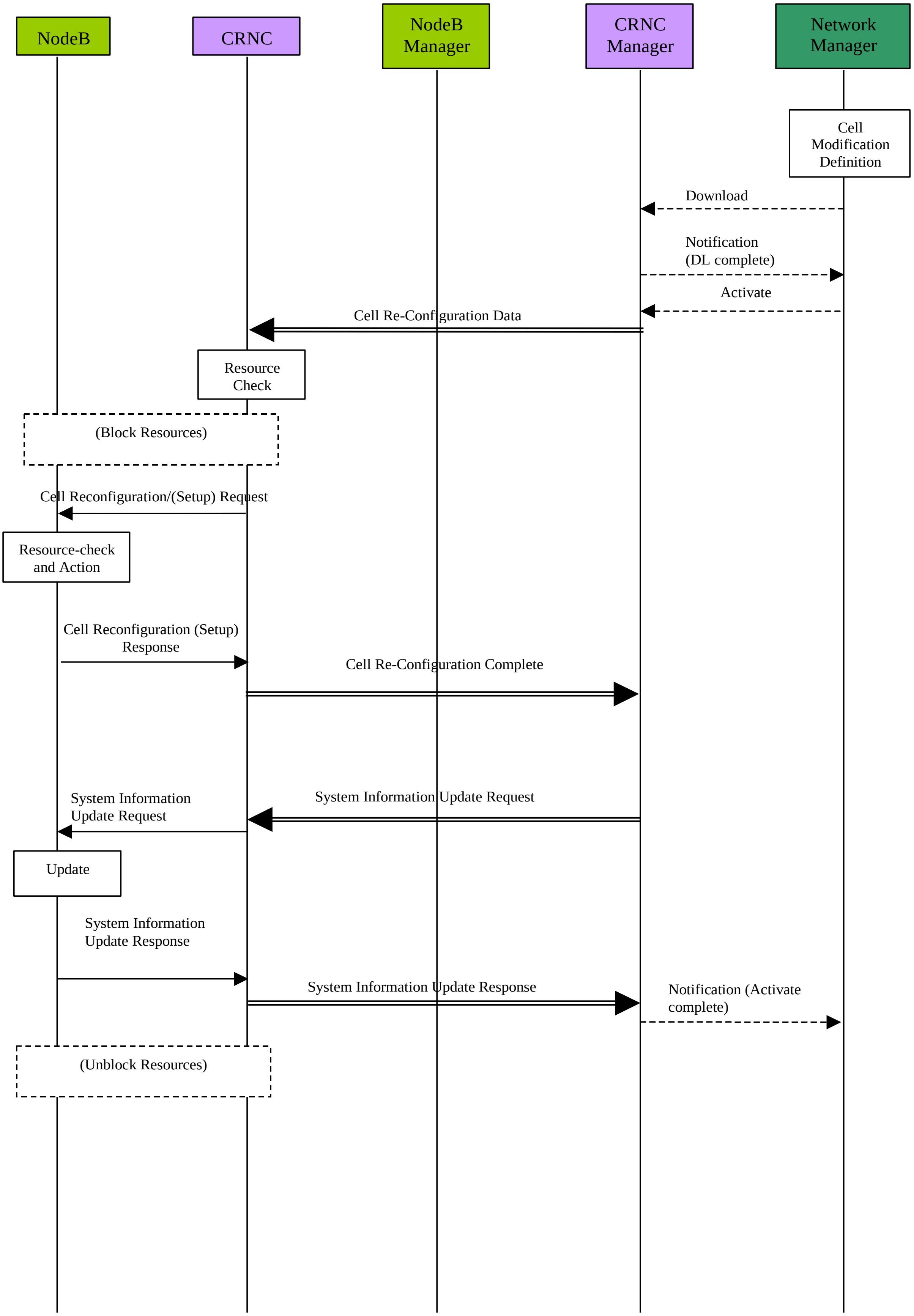

NodeB
CRNC
NodeB Manager
CRNC Manager
Network Manager
Cell Modification Definition
Download
Notification (DL complete)
Activate
Cell Re-Configuration Data
Resource Check
(Block Resources)
Cell Reconfiguration/(Setup) Request
Resource-check and Action
Cell Reconfiguration (Setup) Response
Cell Re-Configuration Complete
System Information Update Request
System Information Update Request
Update
System Information Update Response
System Information Update Response
Notification (Activate complete)
(Unblock Resources)

Figure 5.2.2.1: 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 CRNC 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 CRNC manager.

3. The CRNC 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 CRNC manager.

5. The CRNC manager passes the cell re-configuration data to the CRNC.

6 The CRNC performs a check on the requested configuration changes to ensure they are compatible with the remaining cell configuration and capabilities.

7. If required, the CRNC initiates the blocking of 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 CRNC issues a CELL RECONFIGURATION REQUEST message to the target Node B.

9. When the CELL RECONFIGURATION REQUEST message is received, 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 CRNC that the configuration of the cell has been successful with the CELL RECONFIGURATION RESPONSE message.

12. The unblocking of any resources that have previously been blocked is then completed.

13. The CRNC then advises the CRNC manager that the reconfiguration of each cell has been successful (Cell Re-configuration Complete).

14. After successful cell (re)-configuration, the CRNC may invoke the System Information Update procedure (if the system information has changed during the cell reconfiguration). The procedure is initiated with a SYSTEM INFORMATION UPDATE REQUEST message sent from the CRNC to the Node B.

15. The CRNC invokes the System Information Update procedure in order to start transmission of system information in the reconfigured cell.

16. When the cell is successfully operating, the CRNC reports successful cell operation to its manager.

17. The CRNC 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 CRNC.

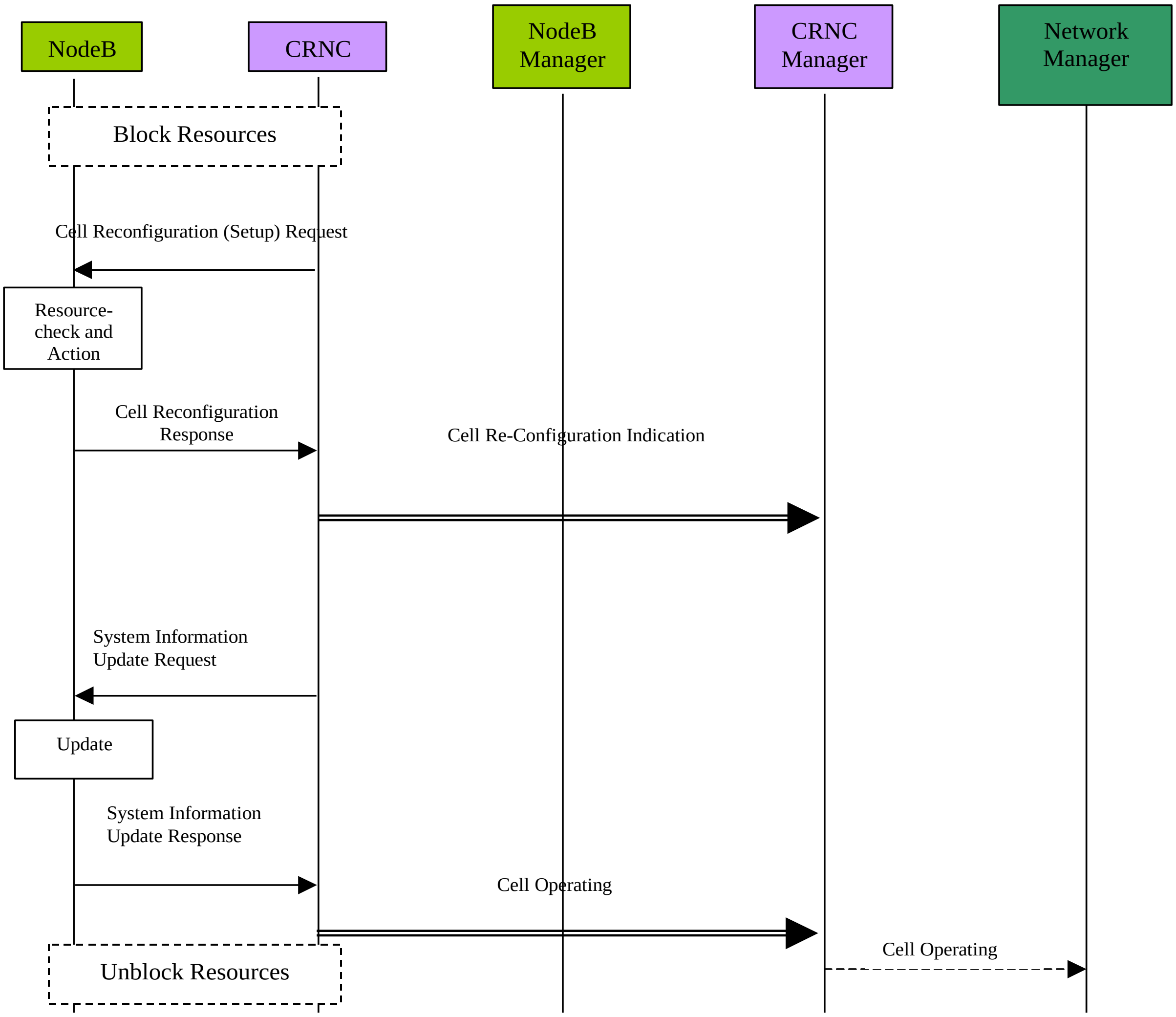

NodeB
CRNC
NodeB Manager
CRNC Manager
Network Manager
Block Resources
Cell Reconfiguration (Setup) Request
Resource-check and Action
Cell Reconfiguration Response
Cell Re-Configuration Indication
System Information Update Request
Update
System Information Update Response
Cell Operating
Cell Operating
Unblock Resources

Figure 5.2.2.2: Cell Re-configuration Initiated by the CRNC

A decision has been made in the radio resource algorithms to perform a cell reconfiguration (due to the traffic conditions). The procedure used to carry this out is shown above, and consists of the following steps:

1. The CRNC may block any resources that may be affected by the procedure e.g. the cell itself or adjacent cells that may also need re-configuration.
2. The CRNC sends a CELL RECONFIGURATION REQUEST message 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. The Node B then performs the (re)-configuration of the cell, including any implementation specific reconfiguration (between Node B and its manager - not shown).
5. Once complete, the Node B advises the CRNC that the reconfiguration of the cell has been successful, by sending a CELL RECONFIGURATION RESPONSE message to the CRNC.
6. The CRNC then advises its manager (which in turn advises the Network Manager) of the cell reconfiguration that has been executed, for updating of the management system cell database. (In the meantime the CRNC unblocks any resources that have previously been blocked.)
7. After successful cell (re)-configuration, the CRNC may invoke the System Information Update procedure (if the system information has changed during the cell re-configuration).

8. The CRNC invokes the System Information Update procedure in order to start transmission of system information in the reconfigured cell. The procedure is initiated with a SYSTEM INFORMATION UPDATE message sent from the CRNC to the Node B.
9. When the cell is successfully operating, the CRNC reports successful cell operation to its manager.
10. The CRNC manager reports successful cell operation to the Network Manager.

5.3 Network Optimisation Procedure

This clause is under rework of SA5 for Release 5.

5.4 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 CRNC to be involved in this process to enable the traffic handling to be optimised during such procedures.

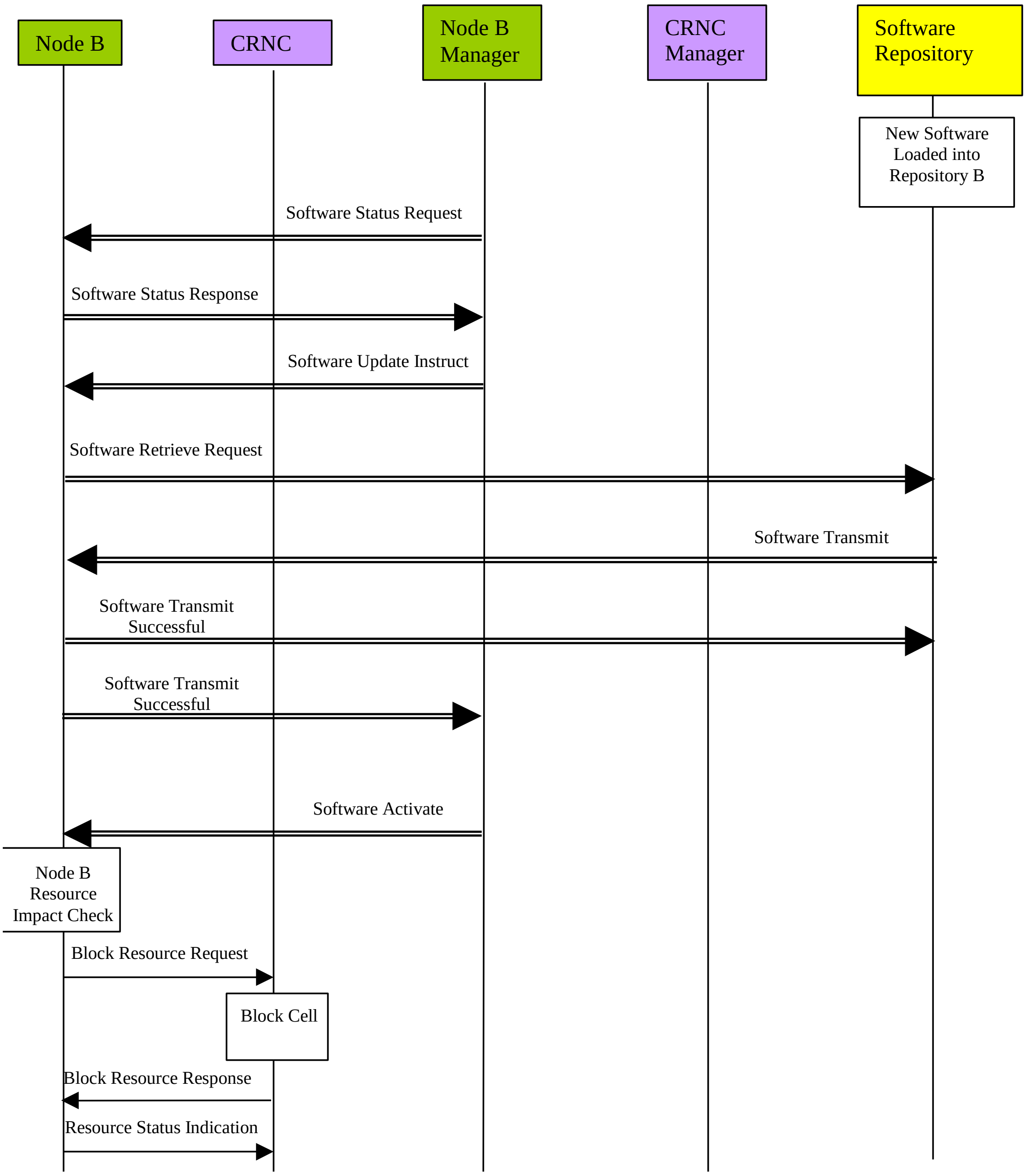
Two possible mechanisms to initiate the transfer of new software to the Node B are as follows. Firstly, the software may be located in a remote node and the Node B provided with an appropriate address to retrieve the software - this is referred to as a 'pull method'. Also, it is possible for the management 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.

5.4.1 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 CRNC 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 (in case configuration data are not effected) 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.


Node B
CRNC
Node B Manager
CRNC Manager
Software Repository
New Software Loaded into Repository B
Software Status Request
Software Status Response
Software Update Instruct
Software Retrieve Request
Software Transmit
Software Transmit Successful
Software Transmit Successful
Software Activate
Node B Resource Impact Check
Block Resource Request
Block Cell
Block Resource Response
Resource Status Indication

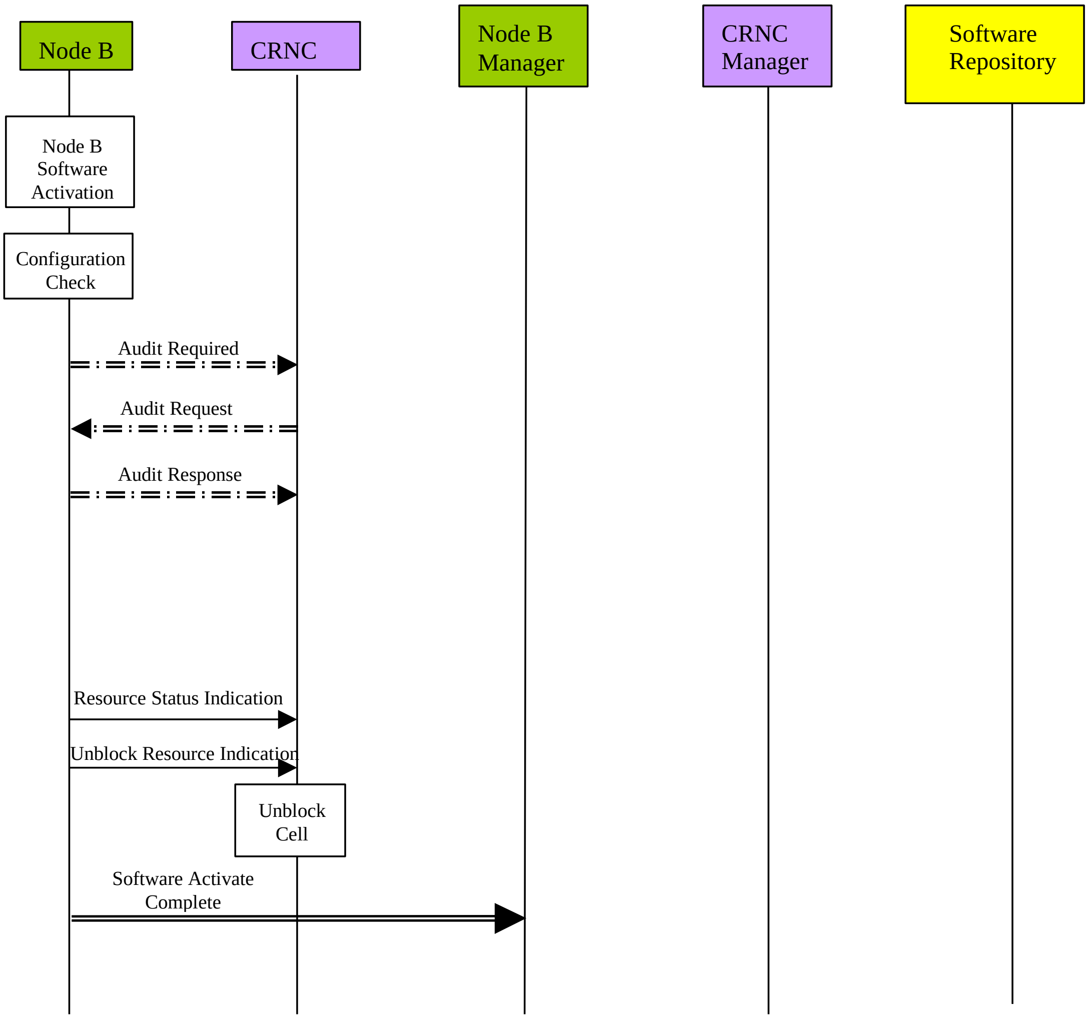


Figure 5.4.1.1: Remote Node B Software Update (Pull)

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 the CRNC to block the associated resources (see Annex A.1 for message flows). 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 CRNC whether it should block the resources immediately (high priority shutdown) or whether it may 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 CRNC of the time available to perform the blocking. The priority indicator should be derived from the initial operator request.

11. The CRNC then attempts to block the resources as requested by the Node B.

12. The CRNC then responds to the Node B advising of the success of the resource block, with the BLOCK RESOURCE RESPONSE message. In this way the CRNC 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 Resource Status Indication is sent from the Node B to the CRNC, disabling the necessary resources.

14. 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.

15. 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 CRNC to perform a configuration audit by issuing an AUDIT REQUIRED INDICATION message.

16. The CRNC initiates a configuration audit of the Node B in response by sending an AUDIT REQUEST message to the Node B.

17. The Node B responds with the AUDIT RESPONSE message, which includes its configuration status. On receipt of this message, the CRNC compares this with the configuration record in its database.

18. With the RESOURCE STATUS INDICATION message the Node B then indicates to the CRNC the "enabled" resources now available.

19. If there were any resources blocked as part of the procedure, the Node B sends the UNBLOCK RESOURCE INDICATION message to the CRNC, to inform it that it may now permit the use of those resources.

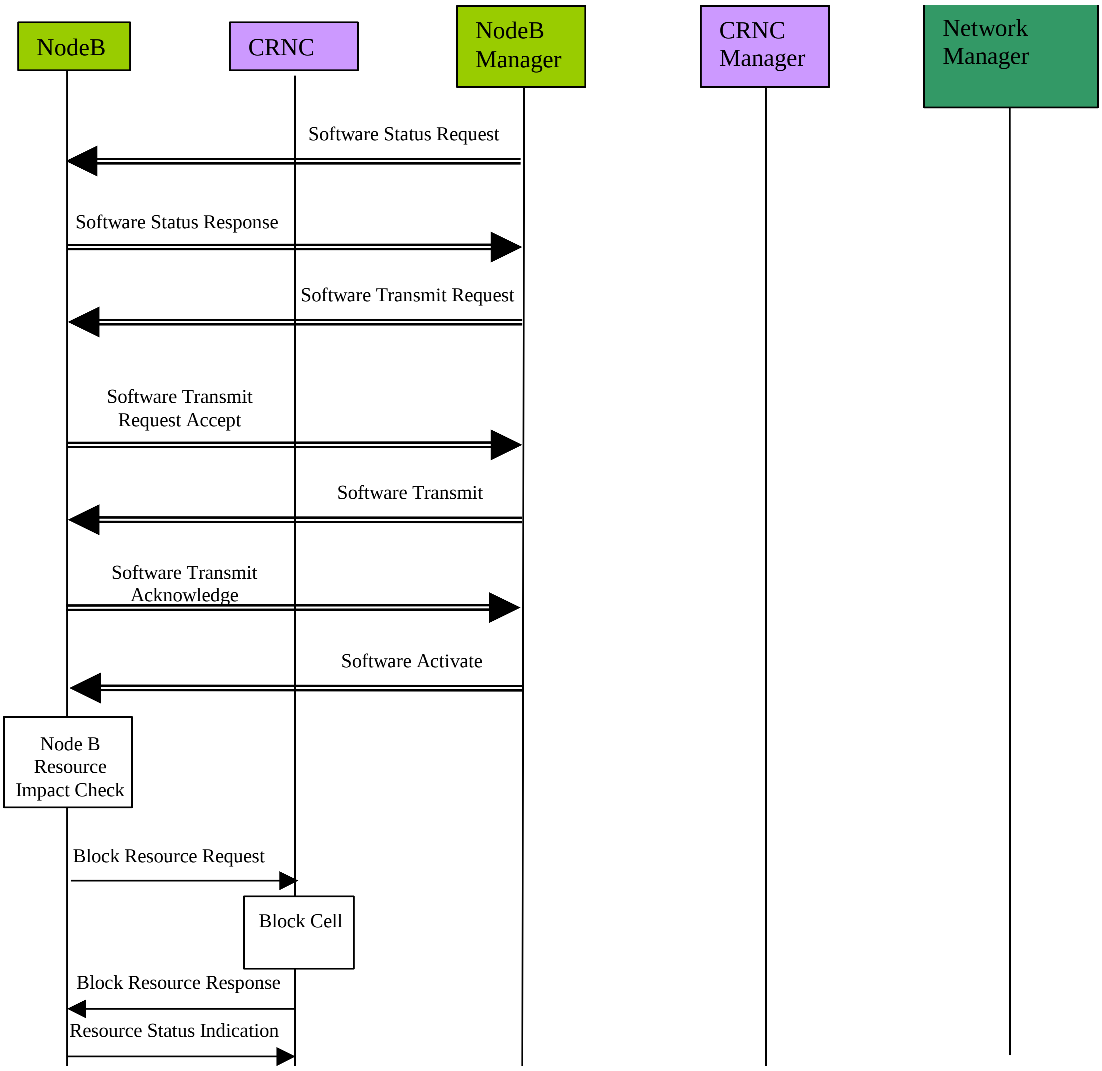
20. The Node B confirms to the management system that the software activation is complete.

5.4.2 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 CRNC 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.


NodeB
CRNC
NodeB Manager
CRNC Manager
Network Manager
Software Status Request
Software Status Response
Software Transmit Request
Software Transmit Request Accept
Software Transmit
Software Transmit Acknowledge
Software Activate
Node B Resource Impact Check
Block Resource Request
Block Cell
Block Resource Response
Resource Status Indication

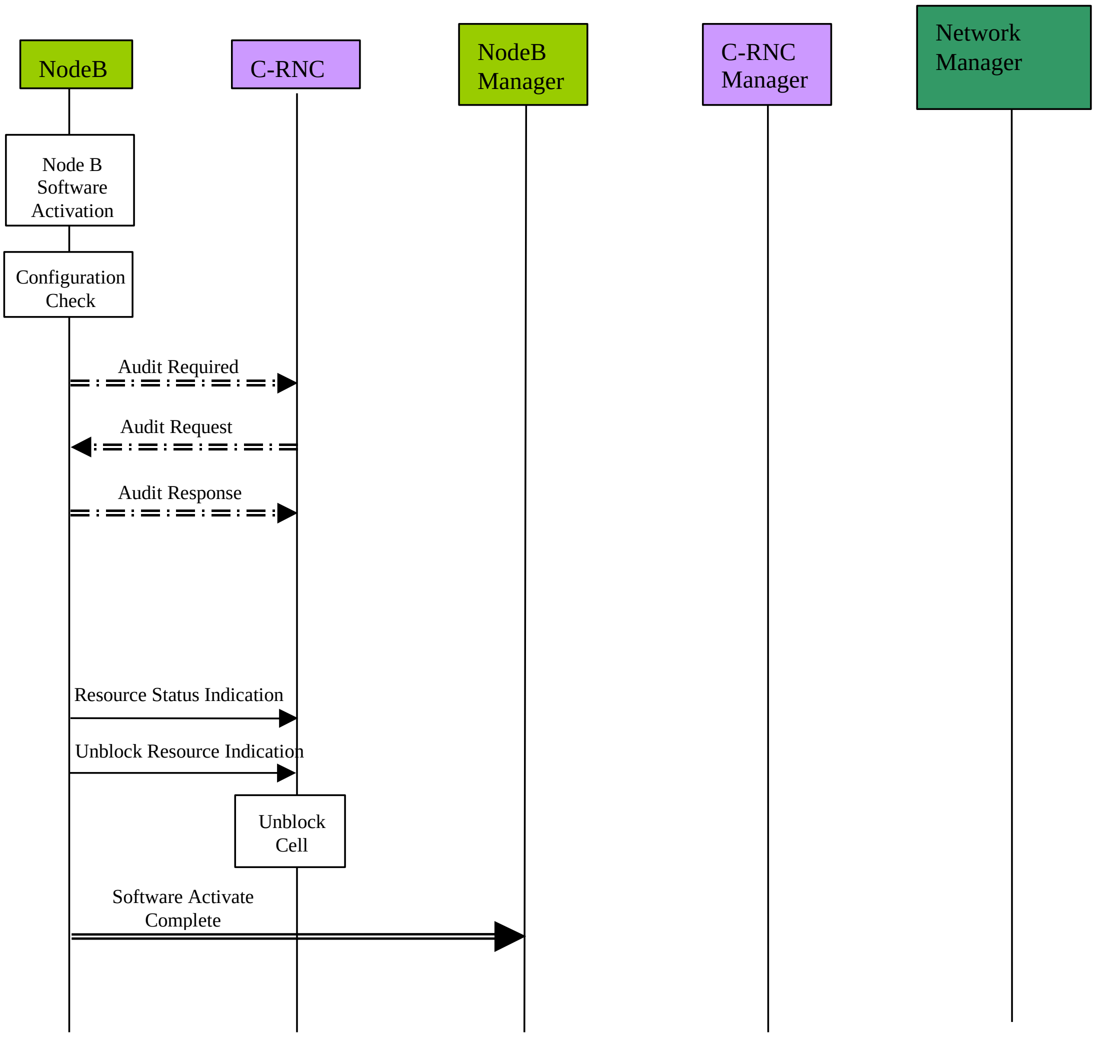


Figure 5.4.2.1: Remote Node B Software Update (Push)

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 the CRNC to block the associated resources. 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 CRNC whether it should block the resources immediately (high priority shutdown) or whether it may 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 CRNC of the time available to perform the blocking. The priority indicator should be derived from the initial operator request.
8. The CRNC then attempts to block the resources as requested by the Node B.

9. .The CRNC then responds to the Node B advising of the success of the resource block, with the BLOCK RESOURCE RESPONSE message. In this way the CRNC 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 RESOURCE STATUS INDICATION message is sent from Node B to the CRNC, disabling the necessary resources.

11. The Node B then activates the new software. Any loss/re-establishment of communication between the CRNC and the Node B (for instance due to a possible restart) shall be performed by the transport protocols.

12. 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 CRNC to perform a configuration audit by issuing an AUDIT REQUIRED message.

13. The CRNC initiates a configuration audit of the Node B in response by sending an AUDIT REQUEST message to the Node B.

14. The Node B responds with the AUDIT RESPONSE message, which includes its configuration status. On receipt of this message, the CRNC compares this with the configuration record in its database.

15. The Node B then indicates to the CRNC, with the RESOURCE STATUS INDICATION message, that the (restored) resources are now available.

16. If there were any resources blocked as part of the procedure, the Node B sends the UNBLOCK RESOURCE INDICATION message to the CRNC, to inform it that it may now permit the use of those resources.

17. The Node B confirms to the management system that the software activation is complete.

5.5 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.

Establishment of necessary parts of the transport layer of the Iu and Iur interfaces, e.g. any ATM PVCs.

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.

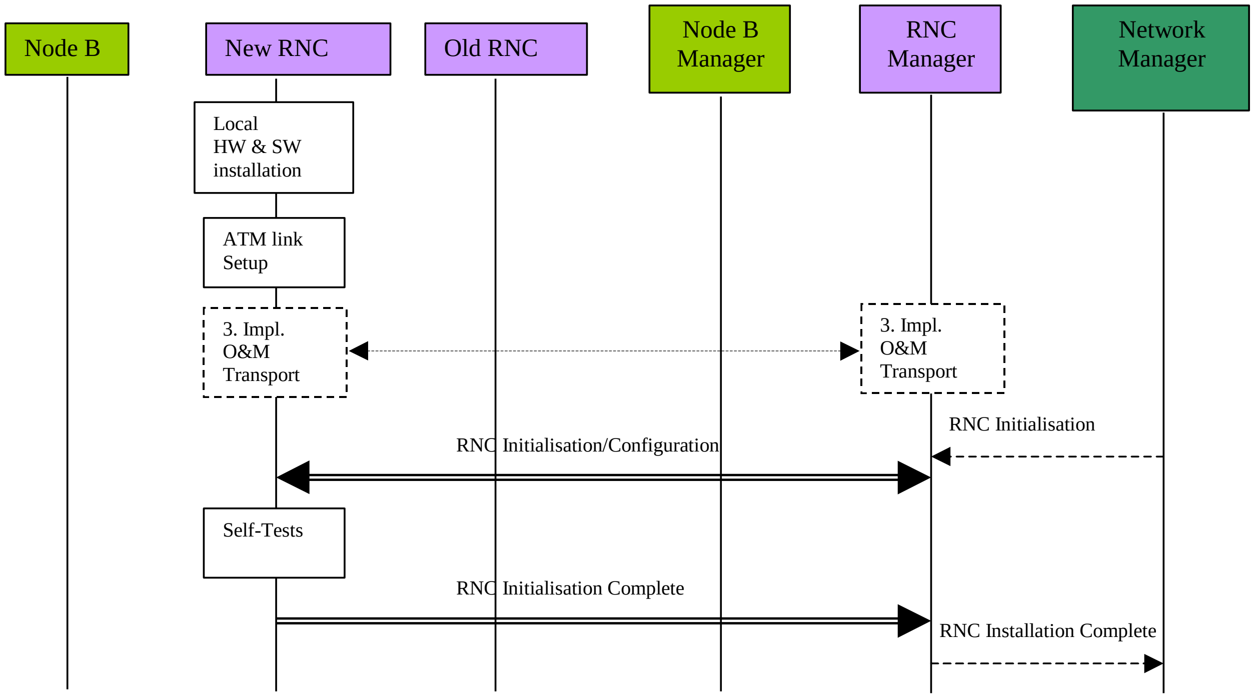


Figure 5.5.1: RNC Installation

5.6 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 (same as Radio Network 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 CRNC 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.

5.6.1 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 CRNC and the Node B (and their management entities). The CRNC is only involved in the case where the availability of logical resources owned by the CRNC (but physically located in the Node B) is impacted.

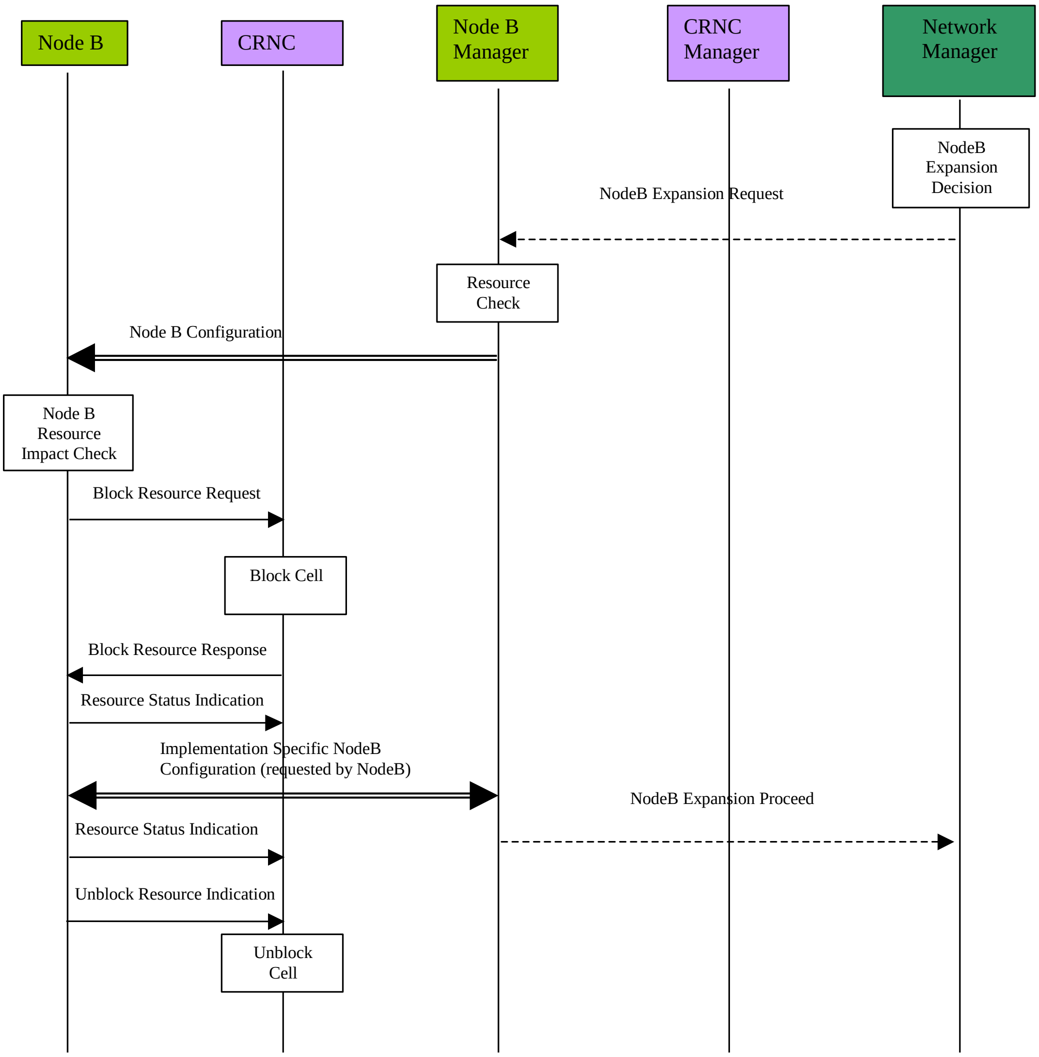


Figure 5.6.1.1: Implementation Specific Node B Expansion

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 CRNC 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 CRNC to block the associated resources. This request should carry a priority indicator (see [1]). By interpreting the requested priority the CRNC decides whether the resource shall be blocked immediately (high priority shutdown) or whether the CRNC may delay the blocking (normal/low priority shutdown). The priority indicator should be derived from the operator expansion request. After blocking any impacted resources, the CRNC sends a BLOCK RESOURCE RESPONSE message to the Node B indicating that the associated resources are blocked. The Node B in return sends a RESOURCE STATUS INDICATION message to the CRNC to disable the necessary resources.

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 CRNC 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. If there are any blocked resources, the Node B sends the UNBLOCK RESOURCE INDICATION message to the CRNC. This informs the CRNC that it may now permit the use of those resources.

5.6.2 Logical Node B Expansion

The logical Node B expansion includes the re-configuration of logical resources owned by the CRNC 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. It should be noted that if the reconfiguration requires cell transmissions to be switched off, then the Initial Cell Configuration procedure is used instead.

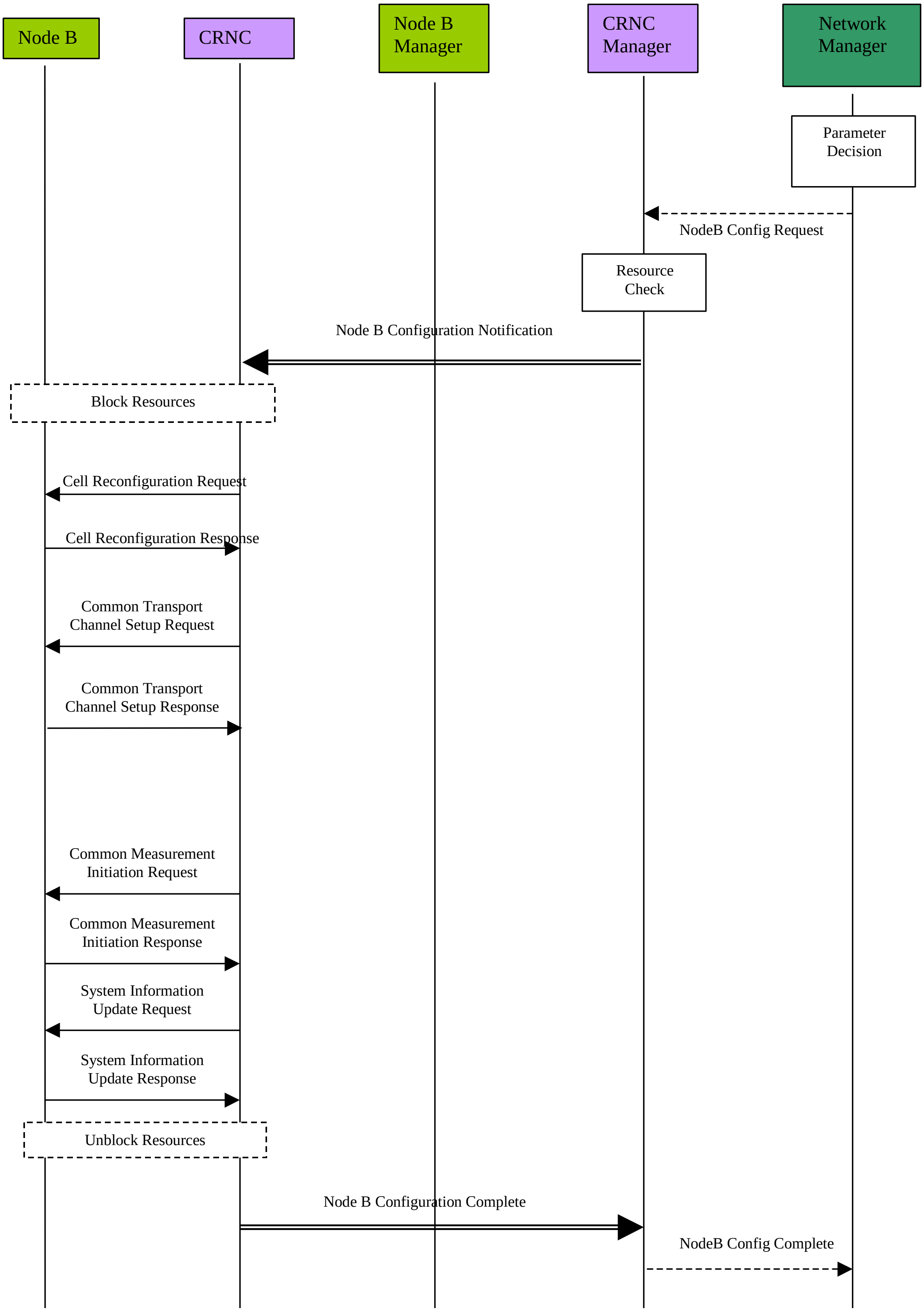

Node B
CRNC
Node B Manager
CRNC Manager
Network Manager
Parameter Decision
NodeB Config Request
Resource Check
Node B Configuration Notification
Block Resources
Cell Reconfiguration Request
Cell Reconfiguration Response
Common Transport Channel Setup Request
Common Transport Channel Setup Response
Common Measurement Initiation Request
Common Measurement Initiation Response
System Information Update Request
System Information Update Response
Unblock Resources
Node B Configuration Complete
NodeB Config Complete

Figure 5.6.2.1: 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, CRNC and the Network Manager, a configuration request may be issued from the Network Manager to the CRNC 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 clause 5.6.1), sent as a final result of the implementation specific expansion.

2. The CRNC Manager performs a resource check for the required expansion, and initiates the Node B logical expansion by sending the new parameters to the associated CRNC and requesting the reconfiguration of the Node B.

3. The CRNC may initiate the blocking of any resources 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 CRNC sends a CELL SETUP REQUEST message to the Node B. In the successful case the Node B will respond with a CELL SETUP RESPONSE message. The CRNC initiates a reconfiguration of a cell, using a CELL RECONFIGURATION REQUEST message.

5. In order to perform a common transport channel set-up, the CRNC requests the establishment of all required channels using a COMMON TRANSPORT CHANNEL SETUP REQUEST message to the Node B. The successful establishment is reported back to the CRNC by a COMMON TRANSPORT CHANNEL SETUP RESPONSE message. The CRNC may also perform changes using a COMMON TRANSPORT CHANNEL RECONFIGURATION REQUEST message.

6.System information messages may now be updated from the CRNC, and new measurement tasks may be initiated (or existing ones terminated) by the CRNC.

7. The CRNC can then unblock both the resources previously blocked as part of the procedure, and those newly configured resources resulting from the Node B expansion.

8. The result of the Node B logical configuration procedure is reported to the CRNC Manager. The complete Node B Configuration (both implementation specific and logical) may then be reported to the Network Manager.

5.6.3 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, CRNC and Management System:

- The reconfiguration 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 CRNC.

- 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 CRNC has to be notified about the status of the available resources.

- In order to configure the logical resources owned and controlled by the CRNC (but physically supported by the Node B) the CRNC 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 CRNC. This shall constitute a request for the configuration.

- After receiving the configuration request from the Management System, the CRNC has to perform all required tasks to configure the Node B properly, (i.e. cell set-up, reconfiguration, or deletion; set-up, reconfiguration 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 CRNC Manager by the CRNC.

5.7 Node B Swap

This clause is under rework of SA5 for Release 5.

5.8 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 Recommendation X.731 [8].

In the case where failures impact on the services supported the CRNC should report these service failures to the Management System.

It should be noted that the Management System 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.

5.8.1 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 CRNC, 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.

5.8.2 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 CRNC and Node B have to perform alarm correlation and filtering. The mechanism used by the Node B and the CRNC 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 CRNC 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.

5.8.3 NBAP alarm messages

With respect to Node B failures, it is necessary to inform the CRNC 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 CRNC 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 CRNC 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 CRNC about the available resources using a RESOURCE STATUS INDICATION message. The CRNC/management system may then re-configure the Node B to restore the previous configuration (i.e. before the failure).

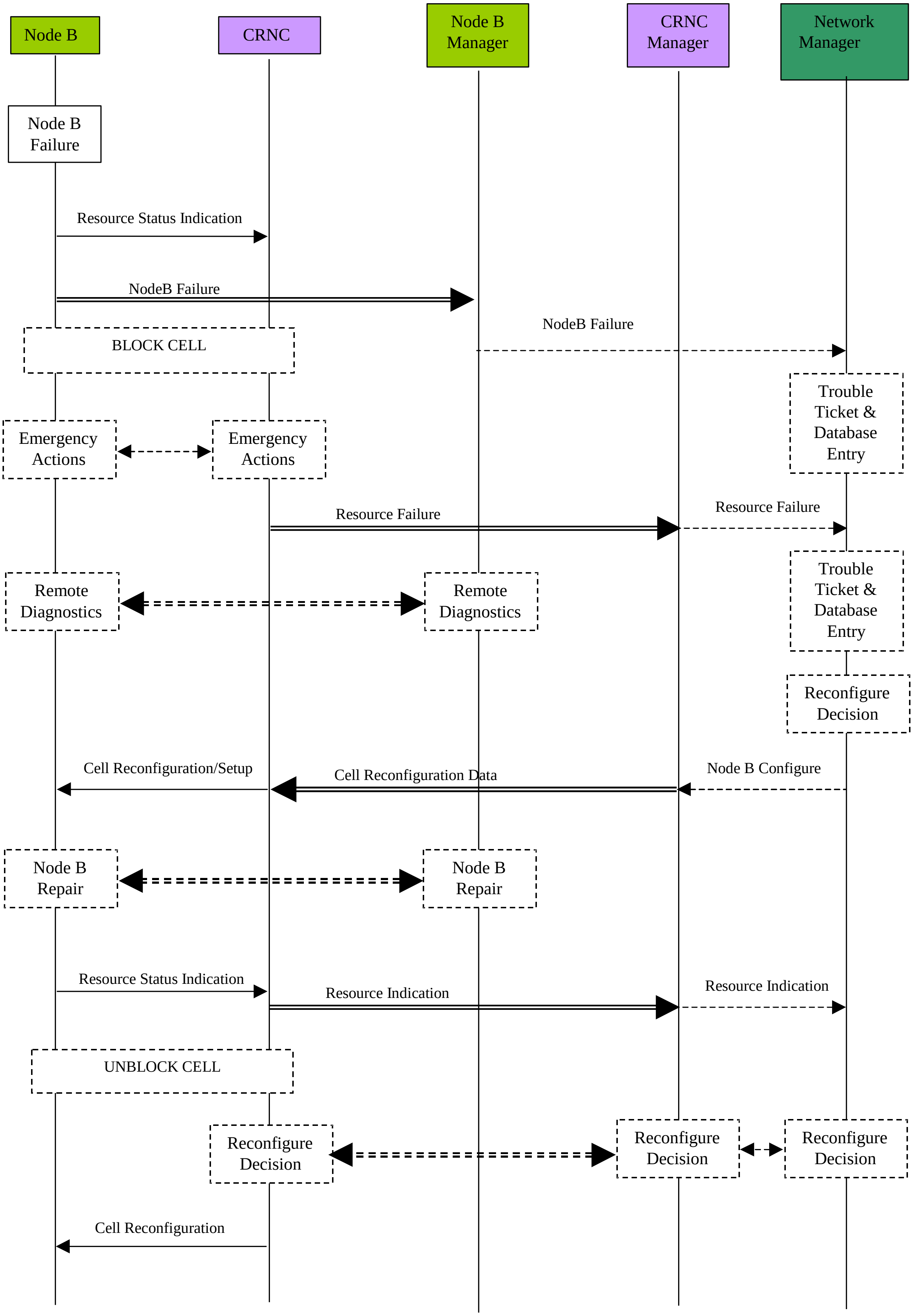


Figure 5.8.3.1: Node B Fault Handling Procedure (HW problem)

The above diagram shows an example for a Fault Handling Procedure in case of a HW problem. 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 CRNC and the Management System:

1. In the case of a failure in Node B, the CRNC and the Management System shall be notified by the Node B. The CRNC may block the logical resource affected.

2. The CRNC 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 the figure 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. The CRNC may block the logical resource affected.

6. 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 one or more cell re-configuration procedures shall be triggered by the Management System.

NOTE: (If cells other than the affected cell were required to be re-configured, for example to extend their coverage in order to cover the affected cells area, these cells would also have been blocked.

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

7. After the failure in the Node B is removed, the Node B sends a notification to the Management System (via the implementation specific O&M signalling channel)., It also sends a RESOURCE STATUS INDICATION message to the CRNC informing about the availability of the repaired cell.

8. The cells that have been blocked as a result of the failure are now unblocked.

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.

Annex A: Blocking/Unblocking of Logical Resources (Cells)

The blocking and unblocking of logical resources is used frequently in UTRAN O&M procedures. There are two ways in which the blocking and unblocking of a logical resource (cell) can be initiated. These are:

- Node B initiated blocking and unblocking;
- CRNC initiated blocking and unblocking.

These two methods are shown in annex A, clauses A.1 and A.2, and are used whenever resources (cells) need to be blocked. The entity (CRNC or Node B) that initiates the blocking of a logical resource must also initiate the unblocking of a logical resource.

Resources are desired to be blocked when they need to be modified, as a result of a direct reconfiguration, failure, or an indirect reconfiguration (i.e. a reconfiguration because a new neighbouring cell has been set-up). It may be desirable to turn off the cell transmissions of blocked cells to stop unnecessary interference to UEs in neighbouring cells. Then after the modification to the resources has taken place, all of the affected cell transmissions may be switched back on together, and the corresponding logical resources in the CRNC unblocked.

A.1 Node B Initiated Resource (Cell) Blocking and Unblocking

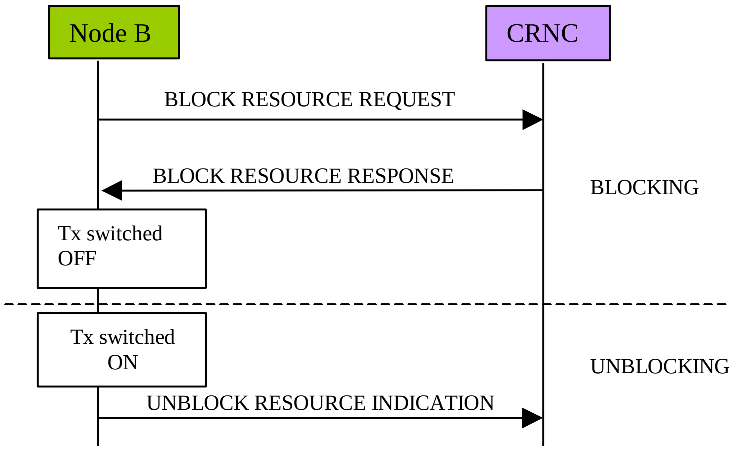


Figure A.1: Node B Initiated Blocking and Unblocking: Successful Operation

The procedure above consists of the following steps:

- For the blocking case:

  1. The Node B decides that some of its resources should be blocked. It sends the BLOCK RESOURCE REQUEST message to the CRNC to request it to block the corresponding logical resources (cells) in the CRNC.

  2. Upon receipt of this message, the CRNC decides whether or not to block the affected logical resources (cells). If it decides to block these logical resources (cells), the CRNC may remove any existing traffic and system information in the CRNC that is for these resources (cells), and prohibit any more traffic from being admitted at the CRNC, and system information from being broadcast from the CRNC, for these resources (cells).

  3. The CRNC sends the BLOCK RESOURCE RESPONSE message to the Node B.

4. Upon receipt of the BLOCK RESOURCE RESPONSE message, the Node B may immediately switch off the transmission to the affected cells.

- For the unblocking case:

1. When the Node B decides that the affected cells are available again, it may turn on the corresponding transmission, and send the UNBLOCK RESOURCE INDICATION message to the CRNC.

2. Upon receipt of this message, the CRNC decides whether or not to unblock the affected logical resource (cell). If it decides to unblock the resources (cell), normal operation may be resumed.

A.2 CRNC Initiated Resource (Cell) Blocking and Unblocking

CRNC Initiated Blocking is used when the CRNC decides that logical resources should be blocked. In the worst case, the cell transmission at the Node B may need to be switched off. In this case, the Cell Deletion is used to carry out this action (see figure A.2). In order to "unblock" the blocked resources, for this case, the signalling in the Initial Cell Configuration procedure (clause 5.2.1) is used after resources have been blocked. In the case of a cell being reconfigured, it should be noted that if the cell transmission is switched off, that the Initial Cell Configuration must instead take place to effectively "unblock" the cell after gaining the new configuration.

NOTE 1: In the present document it is assumed that any other affected resources that are blocked belong to the same Node B as the concerning resource that is being acted upon.

If it is not required to switch the cell transmission off, then the CRNC may only block the resource (cell) internally, and remove traffic for that cell. However, the cell still exists in the Node B, which does not prohibit UEs from attempting to attach to it, and also causing possible interference to neighbouring cells. For the unblocking case, the (resource) cell is "unblocked" internally in the same way.

Alternatively the CRNC may send the SYSTEM INFORMATION UPDATE REQUEST message to the Node B, requesting it to bar the concerning cell(s) from being used by UEs, and acknowledged with a SYSTEM INFORMATION UPDATE RESPONSE message. However, in this case, the common transport channels may continue transmitting to the cell(s), causing possible interference to neighbouring cells. In order to "unblock" resources in this case, the CRNC would have to send another SYSTEM INFORMATION UPDATE REQUEST message unbarring the blocked cells(s).

NOTE 2: For the purposes of the present document, in the case that a Cell Reconfiguration is carried out and cell transmission is not switched off, then the CRNC Initiated Blocking using the SYSTEM INFORMATION UPDATE REQUEST is used.

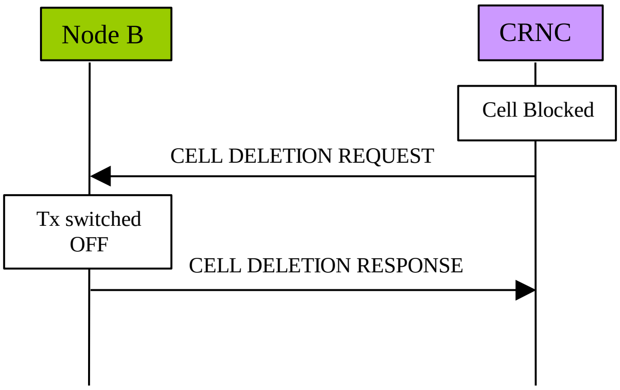


Figure A.2: CRNC Initiated Blocking: Successful Operation

The procedure above consists of the following steps:

1. The CRNC decides that logical resources (cells) should be blocked, so internally blocks these resources (cells).

2. The CRNC may then send the CELL DELETION REQUEST message to the Node B. It sends this message in order to inform the Node B to remove the corresponding cell resources.

3. Upon receipt of this message, the Node B removes the corresponding cell resources, including any common and dedicated channels and any user plane transport bearers for the corresponding cell.

4. The Node B then sends the CELL DELETION RESPONSE to the CRNC, to inform it that the cell resources are no longer available, and it may consider the cell as "not existing".

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Jun 2001	S_12	SP-010233	--	--	Approved at TSG SA #12 and placed under Change Control	1.0.0	4.0.0
Mar 2002	S_15	--	--	--	upgraded without change to Rel-5 (no CR)	4.0.0	5.0.0