ETSI TS 148 016 V18.0.0 (2024-05)

**Digital cellular telecommunications system (Phase 2+) (GSM);
General Packet Radio Service (GPRS);
Base Station System (BSS) -
Serving GPRS Support Node (SGSN) interface;
Network service
(3GPP TS 48.016 version 18.0.0 Release 18)**

3GPP™ A GLOBAL INITIATIVE
GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Reference
RTS/TSGR-0048016vi00

Keywords
GSM

ETSI

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

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

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

Important notice

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

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

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

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

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

Notice of disclaimer & limitation of liability

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

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the Network Service used on the Base Station System (BSS) to Serving GPRS Support Node (SGSN) interface (Gb interface).

The protocol stack on the Gb interface is defined in the stage 2 Technical Specification 3GPP TS 43.060.

The Network Service entity provides network services to the BSSGP entity specified in 3GPP TS 48.018.

The layer 1 of the Gb interface is specified in 3GPP TS 48.014.

In the present document, the communication between adjacent layers and the services provided by the layers are distributed by use of abstract service primitives. But only externally observable behaviour resulting from the description is normatively prescribed by the present document.

The service primitive model used in the present document is based on the concepts developed in ITU-T Recommendation X.200.

2 References

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

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

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

[2] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service description; Stage 1".

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

[4] 3GPP TS 48.014: "General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Gb interface Layer 1".

[5] 3GPP TS 48.018: "General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP)".

[6] FRF 1.1 (1996): "User-to-Network Implementation Agreement (UNI)".

[7] (void).

[8] ITU-T Recommendation Q.921 (1997): "ISDN user-network interface - Data link layer specification".

[9] ITU-T Recommendation Q.922 (1992): "ISDN data link layer specification for frame mode bearer services".

[10] ITU-T Recommendation Q.931 (1998): "ISDN user-network interface layer 3 specification for Basic Call Control".

[11] ITU-T Recommendation Q.933 (1995): "Digital Subscriber Signalling System No. 1 (DSS 1) - Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring".

[12] ITU-T Recommendation I.370 (1991): "Congestion management for the ISDN Frame Relaying Bearer Service".

[13] ITU-T Recommendation X.200 (White Book): "Information technology - Open Systems Interconnection - Basic Reference Model: The basic model".

[14] ANSI T1.602: "ISDN - Data Link Layer Signalling Specification for Application at the User-Network Interface".

[15] ANSI T1.606 (1990): "Frame Relaying Bearer Service Architectural Framework and Service description (R 1996)".

[16] ANSI T1.617 (1991): "Digital Subscriber System No. 1 (DSS1) Signaling Specification for Frame Relay Bearer Service (R1997)".

[17] ANSI T1.618 (1991): "Digital Subscriber System No. 1 (DSS1) Core Aspects of Frame Relay Protocol for Use with Frame Relay Bearer Service (R1997)".

[18] IETF RFC 768 (1980): "User Datagram Protocol" (STD 6).

[19] IETF RFC 791 (1981): "Internet Protocol" (STD 5).

[20] IETF RFC 2460 (1998): "Internet Protocol, Version 6 (IPv6) Specification".

[21] 3GPP TS 23.236: "Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 22.060 and the following in apply:

BSSGP Virtual Connection (BVC): end-to-end virtual communication path between remote Network Service user entities

BSSGP Virtual Connection Identifier (BVCI): identifier of a BVC, having end-to-end significance across the Gb interface

IP endpoint: an endpoint defined by its IP address and UDP port. An IP endpoint can be a data endpoint and/or a signalling endpoint

Data IP endpoint: an IP endpoint used for Data traffic

Signalling IP endpoint: an IP endpoint used for Signalling traffic

Data traffic: data traffic for an IP Sub-Network is defined as NS SDUs for PTP and PTM functional entities (BVCI≥1)

Signalling traffic: signalling traffic for an IP Sub-Network is defined as NS SDUs for Signalling functional entities (BVCI=0) and all PDUs for IP Sub-Network Service Control

Full Mesh Connectivity: any IPv4 endpoint in an NSE is capable of communications with any IPv4 endpoint in its peer NSE. Also any IPv6 endpoint in an NSE is capable of communications with any IPv6 endpoint in its peer NSE

Network Service Entity Identifier (NSEI): identifier of an NS Entity having end-to-end significance across the Gb interface, i.e. the peer NSEs on the BSS side and the SGSN side are identified by the same NSEI value

Network Service Virtual Connection (NS-VC): end-to-end virtual communication path between Network Service peer entities

Network Service Virtual Connection Identifier (NS-VCI): identifier of an NS-VC having end-to-end significance across the Gb interface

Network Service Virtual Link (NS-VL): virtual communication path between the BSS or the SGSN and the intermediate network, or between the BSS and the SGSN in case of direct point-to-point configuration

Network Service Virtual Link Identifier (NS-VLI): identifier of an NS-VL, having local significance at the BSS or SGSN

Network Service Virtual Connection Group: groups all NS-VCs together which provide communication between the same peer NS entities. This grouping has local significance at the BSS or SGSN

Blocked / unblocked: when an NS-VC can not be used for NS user traffic, it is blocked. When an NS-VC can be used for NS user traffic, it is unblocked

Dead / alive: when an NS-VC is able to provide communication between remote NS entities, it is alive. When it is not able, it is dead. These states are supervised by means of a test procedure, as further described in the present document

Pool area: an area within which an MS may roam without need to change the serving SGSN. A pool area is served by one or more SGSNs in parallel. All the cells controlled by a BSC belong to the same one (or more) pool area(s).

3.2 Symbols

For the purposes of the present document, the symbols given in 3GPP TS 23.060 apply.

3.3 Abbreviations

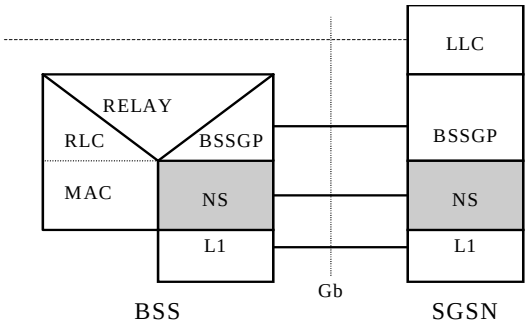
For the purposes of the present document, the abbreviations given in 3GPP TS 21.905 and the following apply:

BECN	Backward Explicit Congestion Notification
BSSGP	Base Station System GPRS Protocol
BVC	BSSGP Virtual Connection
BVCI	BSSGP Virtual Connection Identifier
CLLM	Consolidated Link Layer Management
DE	Discard Eligibility
FECN	Forward Explicit Congestion Notification
FR	Frame Relay
FRF	Frame Relay Forum
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LLC	Logical Link Control
LSP	Link Selector Parameter
MAC	Medium Access Control
NS	Network Service
NSEI	Network Service Entity Identifier
NS-SAP	Network Service Service Access Point
NS-VC	Network Service Virtual Connection
NS-VCI	Network Service Virtual Connection Identifier
NS-VL	Network Service Virtual Link
NS-VLI	Network Service Virtual Link Identifier
PDU	Protocol Data Unit
PTM	Point-To-Multipoint
PTP	Point-To-Point
PVC	Permanent Virtual Connection
RLC	Radio Link Control
SGSN	Serving GPRS Support Node
SNS	Sub-Network Service
UDP	User Datagram Protocol
UNI	User-to-Network Interface

4 Network Service general description

4.1 Overview

The position of the Network Service within the protocol stack of the Gb interface is shown in figure 4.1.1.



NOTE: BSSGP, L1, LLC, MAC, RELAY, RLC are outside the scope of the present document, refer to 3GPP TS 43.060 for further details.

Figure 4.1.1: Position of the NS within the Gb interface protocol stack

The Network Service performs the transport of NS SDUs between the SGSN and BSS. The services provided to the NS user shall be:

- Network Service SDU transfer. The Network Service entity shall provide network service primitives allowing for transmission and reception of upper layer protocol data units between the BSS and SGSN. The NS SDUs are transferred in order by the Network Service, but under exceptional circumstances order may not be maintained.
- Network congestion indication. Congestion recovery control actions may be performed by the Sub-Network Service (e.g. Frame Relay). Congestion reporting mechanisms available in the Sub-Network Service implementation shall be used by the Network Service to report congestion.
- Status indication. Status indication shall be used to inform the NS user of the NS affecting events e.g. change in the available transmission capabilities.

The Network Service entity is composed of an entity dependent on the intermediate transmission network used on the Gb interface, the Sub-Network Service, and of a control entity independent from that network, the Network Service Control. There is a hierarchical relationship between both entities. This is reflected in figure 4.1.2. The detailed communication mechanisms between both entities is an internal matter for the Network Service and is not further standardized.

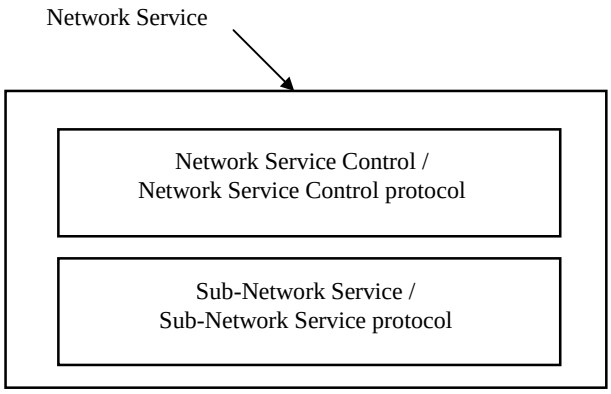


Figure 4.1.2: Internal architecture of the Network Service

The Sub-Network Service entity provides a communication service to Network Service Control peer entities. The Network Service Control peer entities use the Sub-Network Service for communication with each other. The peer-to-peer communication accross the Gb interface between remote Network Service Control entities is performed over Network Service Virtual Connections (NS-VCs). An NS-VC is a virtual communication path between Network Service Control peer entities.

The Network Service entity provides a communication service to NS user peer entities: the peer-to-peer communication between remote NS user entities is performed over BSSGP Virtual Connections (BVCs). A BVC is a virtual communication path between Network Service user peer entities. A Network Service Entity communicates with only one peer Network Service Entity.

Addressing across the Gb interface is further detailed in the rest of the present document.

The Network Service Control entity is responsible for the following functions:

- NS SDU transmission: The NS SDUs shall be transmitted on the NS-VCs. The NS SDUs are encapsulated into Network Service Control PDUs which in turn are encapsulated into Sub-Network Service PDUs.

- Load sharing: The load sharing function distributes the NS SDU traffic amongst the available (i.e. unblocked) NS-VCs of a group.

- NS-VC management: A blocking procedure is used by an NS entity to inform an NS peer entity when an NS-VC becomes unavailable for NS user traffic. An unblocking procedure is used for the reverse operation. A reset procedure is used between peer NS entities in order to set an NS-VC to a determined state, after events resulting in possibly inconsistent states of the NS-VC at both sides of the Gb interface. A test procedure is used to check that an NS-VC is operating properly between peer NS entities.

4.2 Addressing

The purpose of this sub-clause is to describe the addressing principles on the Gb interface in a generic way, i.e. irrespective of the exact configuration of the Gb interface and of the exact nature of the intermediate transmission network, when present. Therefore, this sub-clause provides an abstract description of the addressing principles. These principles are then applied to real networks in sub-clause "Sub-Network Service protocol".

In this sub-clause, addressing is considered in the general case where an SGSN is connected to several BSSs via an intermediate transmission network and in the specific case where a BSS is connected to several SGSNs within one or more pool areas, see 3GPP TS 23.236. Point-to-point physical connections may also be used, addressing in this special case can be derived from the general case.

4.2.1 Network Service Virtual Link (NS-VL)

An SGSN and a BSS may use different physical links for connecting to each other (e.g. because of intermediate equipment or transmission network). Each physical link is locally (i.e. at each side of the Gb interface) identified by means of a physical link identifier. The exact structure of the physical link identifier is implementation dependent.

Each physical link supports one or more Network Service Virtual Links (NS-VLs). Each NS-VL is supported by one physical link if the Frame Relay Sub-Network is employed. For an IP sub-network, the NS-VL is mapped to an IP endpoint. The exact nature of the NS-VL depends on the intermediate network used on the Gb interface. In the general case of an intermediate transmission network, the NS-VL is used to access the intermediate network. Communication means internal to the intermediate network are outside the scope of the present document. The NS-VLs may alternatively be used end-to-end between the BSS and SGSN, in case of a point-to-point configuration on the Gb interface.

Each NS-VL may be identified by means of a Network Service Virtual Link Identifier (NS-VLI). The significance (i.e. local or end-to-end) and the exact structure of the NS-VLI depends on the configuration of the Gb interface and on the intermediate network used. For example, in the case of a Frame Relay network, the physical link is the FR bearer channel, the NS-VL is the local link (at UNI) of the FR permanent virtual connection (PVC) and the NS-VLI is the association of the FR DLCI and bearer channel identifier.

4.2.2 Network Service Virtual Connection (NS-VC)

In order to provide end-to-end communication between the BSS and SGSN irrespective of the exact configuration of the Gb interface, the concept of Network Service Virtual Connection (NS-VC) is used. The NS-VCs are end-to-end virtual connections between the BSS and SGSN. In the case of a FR sub-network, at each side of the Gb interface there is a one-to-one correspondence between NS-VCs and NS-VLs. When employing an IP-sub-network one NS-VL may serve several NS-VCs (see figure 4.2.2.1).

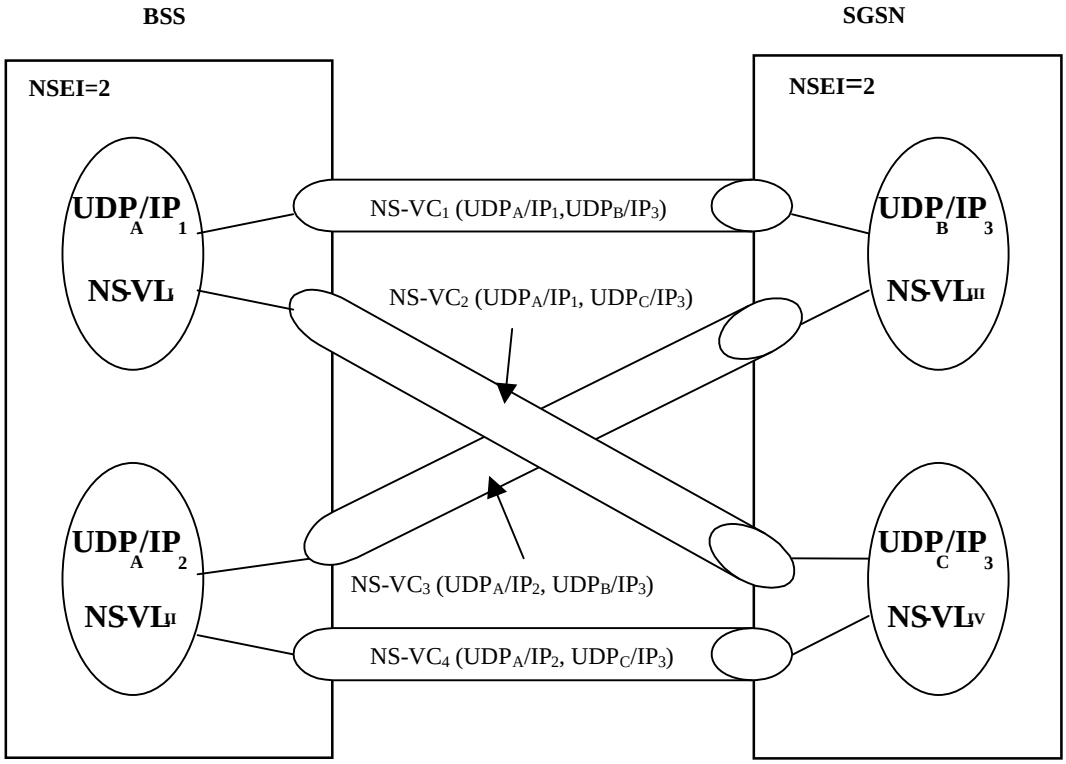


Figure 4.2.2.1: IP sub-network relationship between NS-VCs and NS-VLs

For example, in the case of a Frame Relay network, the NS-VC is the FR permanent virtual connection (PVC).

Figure 4.2.2.2 shows the relationship between NS-VCs and NS-VLs for a Frame Relay sub-network. In the case of an IP network, the NS-VC is given by a pair of IP endpoints at the BSS and SGSN. While Figure 4.2.2.1 illustrates a configuration with only one NSE, multiples NSE in either the BSS or SGSN are allowed.

At the BSS, the IP endpoints for each NSE shall not be shared among NSEs connected to the same SGSN. Howewer, an IP endpoint at the BSS may serve multiple NSEs when each of the NSEs is connected towards different SGSNs. At the SGSN, an IP endpoint may serve multiple NSEs; (i.e. IP endpoints may be shared among NSEs).

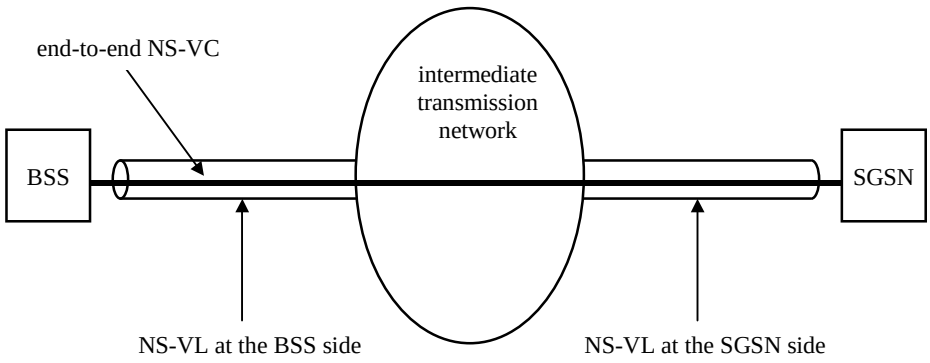


Figure 4.2.2.2: Frame relay sub-network relationship between NS-VCs and NS-VLs

Each NS-VC is identified by means of a Network Service Virtual Connection Identifier (NS-VCI) having end-to-end significance across the Gb interface. An NS-VCI uniquely identifies an NS-VC within an SGSN and within a BSS.

The establishment of an NS-VC includes the establishment of physical links, see 3GPP TS 48.014, and of NS-VLs.

In the case of an FR sub-network NS-VCs and NS-VLs are permanently established by means of administrative procedures, NS-VCIs are allocated by administrative means as well. The mapping of NS-VCIs on NS-VLIs and on physical link identifiers is held in non-volatile memory.

When employing an IP sub-network the NS-VCs and NS-VLs may be established by means of administrative means (static configuration) or by auto-configuration procedures (dynamic configuration).

4.2.3 Network Service Virtual Connection Group

The Network Service Virtual Connection Group groups together all NS-VCs providing communication between the same peer NS entities. One NS-VC group is configured between two peer NS entities. This grouping is performed by administrative means. At each side of the Gb interface, there is a one-to-one correspondence between a group of NS-VCs and an NSEI. The NSEI has an end-to-end significance across the Gb interface.

4.2.4 BSSGP Virtual Connection (BVC)

The Network Service provides communication paths between remote NS user entities. These communication paths are called BSSGP Virtual Connections (BVCs). Each BVC is used to transport NS SDUs between NS users.

A Network Service Entity provides one or more BVCs between peer NS user entities. Each BVC is supported by one group of NS-VCs. Each group of NS-VCs supports one or more BVCs. The NS entity maps between BVC and the related NS-VC group.

Each BVC is identified by means of a BSSGP Virtual Connection Identifier (BVCI) having an end-to-end significance across the Gb interface. The BVCI together with the NSEI uniquely identifies a BVC within an SGSN. The BVCI and NSEI are used on the Network Service-Service Access Point (NS-SAP) for layer-to-layer communication.

4.2.5 Use of Concepts on the Gb Interface when Intra Domain Connection of RAN Nodes to Multiple CN Nodes applies in the BSS

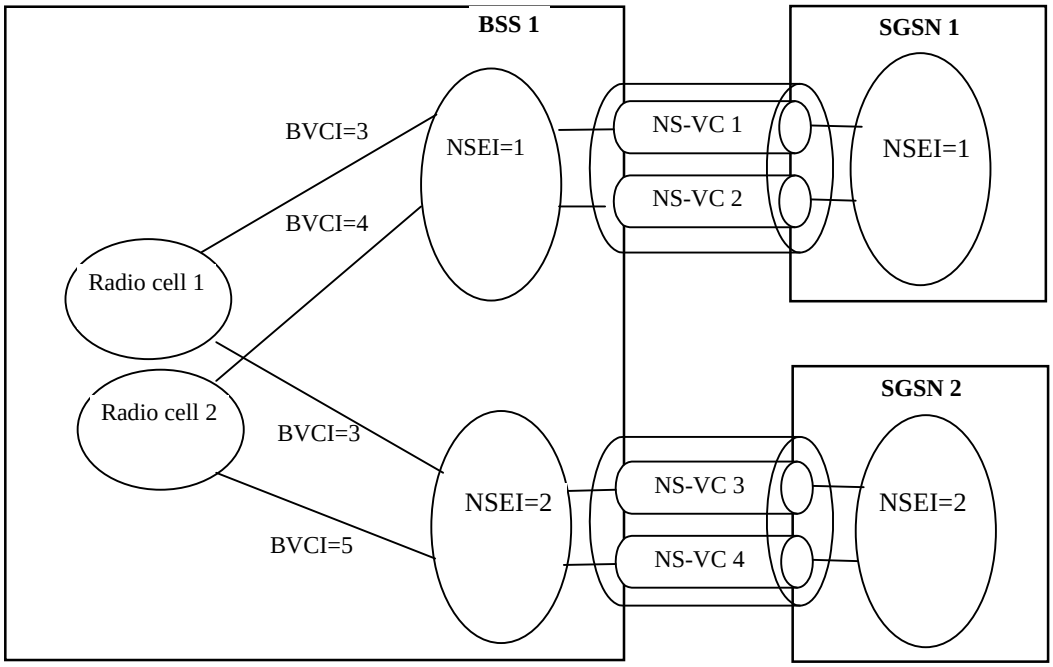


Figure 4.2.2.3: Use of Gb Concepts when Intra Domain Connection of RAN Nodes to Multiple CN Nodes applies in the BSS

For a pool area the BSS sets up several NSEs, and each of these NSEs goes towards different SGSNs. In this way the BSS have one NSE towards each of the connected SGSNs. Alternatively, several NSEs in the BSS are connected towards each of the SGSNs supporting the pool area.

One or more NS-VCs are set up between each of the NSEs in the BSS and the corresponding peer NSEs in the SGSNs. In an IP network, an NS-VC is identified by a pair of IP addresses and UDP ports at both the BSS and the SGSN. In a FR network, the identity of an NS-VC is unique within an NSEI.

4.3 Sub-Network Service functions

The Sub-Network Service functions of the Network Service shall provide access to the intermediate network (or to the peer entity in case of direct point-to-point configuration) by means of NS-VLs and shall provide NS-VCs between NS peer entities.

On each NS-VC, data are transferred in order by the Sub-Network Service.

When the Sub-Network Service entity detects that an NS-VC becomes unavailable (e.g. upon failure detection), or when the NS-VC becomes available again (e.g. after failure recovery), the Network Service Control entity shall be informed. Failures may occur due to protocol errors, intermediate transmission network failure, equipment or link failure or other reasons.

4.4 Load sharing function

4.4.1 Load Sharing function for the Frame Relay Sub-Network

4.4.1.1 Overview

The load sharing function distributes the NS SDU traffic among the unblocked NS-VCs of the same group on the Gb interface. The use of load sharing also provides to the upper layer seamless service upon failure by re-organizing the NS SDU traffic between the unblocked NS-VCs of the same group. The re-organization may disturb the order of transferred NS SDUs. The load sharing function should be implemented in both the BSS and the SGSN.

Load sharing applies only to NS SDUs, not to NS signalling such as NS-VC management PDUs.

4.4.1.2 Requirements on load sharing function

All NS SDUs to be transmitted over the Gb interface are passed to the load sharing function along with the Link Selector Parameter (LSP) , the BVCI and the NSEI. LSP and BVCI are used by the NS entity to select amongst the unblocked NS-VCs within the group, addressed by means of the NSEI, where to send the NS SDU. The mapping between LSP and NS-VC is based on an implementation dependent function that meets the following requirements:

- For each BVC and NSEI, the NS entity selects the NS-VC out of the group based on the LSP. This is an internal matter for the NS entity and it is not subject to further standardization.
- For each BVC and NSEI, NS SDUs with the same Link Selector Parameter shall be sent on the same NS-VC. Thus, the load sharing function guarantees that, for each BVC, the order of all NS SDUs marked with the same LSP value is preserved. In the event of a link failure and subsequent re-organization of the NS SDU traffic between the unblocked NS-VCs, the receiver may get out of order NS SDUs. Further actions implemented to prevent this error are outside the scope of the present document.
- Load sharing functions at the BSS and the SGSN are independent. Therefore, uplink and downlink NS SDUs for a subscriber may be transferred over different NS-VCs.
- A change in NS-VCs available for NS user traffic (i.e. one or more NS-VCs become blocked or unblocked) shall result in a re-organization of the NS SDU traffic amongst the unblocked NS-VCs of the same group.
- For a BVC, when there is no unblocked NS-VC of the group left between a BSS and a SGSN, the corresponding traffic is discarded by the NS at the sending side.

The Link Selector Parameter is locally used at the BSS and at the SGSN and shall not be transmitted across the Gb interface.

4.4.2 Load sharing function for the IP Sub-Network

4.4.2.1 Overview

The load sharing function distributes the NS SDUs and SNS PDUs traffic among the available IP endpoints on the Gb interface. The use of load sharing also provides to the upper layer seamless service upon failure by re-negotiating the NS SDU traffic between the remaining IP endpoints. The re-negotiation may disturb the order of transferred NS SDUs. The load sharing function shall be implemented in both the BSS and the SGSN.

The load sharing function for the IP sub-network determines the local IP endpoint locally and the remote IP endpoint based on weight information provided by the peer NSE. Each NSE shall use an implementation dependent load sharing function to determine the local IP endpoint associated with all NS SDU traffic related to an MS. The remote IP endpoint shall initially be determined by an implementation dependent load sharing function that distributes the traffic in equal proportion to the relative weights assigned to the peer NSE's endpoints. These relative weights are assigned by the peer NSE for both signalling traffic and data traffic and will be referred to as signalling weight and data weight respectively. (These relative weights are communicated using the SNS-CONFIG, SNS-ADD, and SNS-CHANGE-WEIGHT PDUs. Also, the remote IP endpoint can be changed by the peer NSE via the Resource Distribution Function (refer to sub-clause 4.4a.).

4.4.2.2 Selection of the local IP endpoint

The LSP is used by an NS entity to select amongst the available local IP endpoints for the given NSEI, from which the NS SDUs are sent. The association between an LSP and a local IP endpoint is based on an implementation dependent function that meets the following requirements:

- For each NS-SDU, an NS entity selects a local IP endpoint based on the LSP for sending the NS-SDU to the peer NSE. If the LSP has not been associated with a local IP endpoint, then a local IP endpoint shall be selected by a method that is implementation dependent. This is an internal matter for the NS entity and it is not subject to further standardisation.

- Once a local IP endpoint is selected for the LSP, the NSE should maintain a linkage between the LSP and the local IP endpoint so that NS SDUs with the same Link Selector Parameter shall be sent from the same local IP endpoint. The NSE may disassociate the MS from the last used local IP endpoint when an MS makes a cell change.

- If a local IP endpoint that has been mapped to an LSP is taken out of service, a new local IP endpoint shall be selected and associated with the LSP.

- Selection of the local IP endpoint occurs locally at each NSE.

- If there is no available local IP endpoint, the corresponding traffic is discarded by the NS at the sending side.

The Link Selector Parameter is locally used at the BSS and at the SGSN and shall not be transmitted across the Gb interface.

4.4.2.3 Selection of the remote IP endpoint

A remote IP endpoint is an IP address and UDP port that the peer NSE has made known to the local NSE (e.g. using the Configuration procedure). In addition to being used to select the local IP endpoint, the LSP is also used by the NS entity to select amongst the available remote IP endpoints for the given NSEI, to which the NS SDUs are sent. The selection of the remote IP endpoint for an LSP is initially based on the signalling weight and data weight of the remote IP endpoints. Also, the Resource distribution function can be used by the peer NSE to initially request or subsequently change the remote IP endpoint selection for an LSP.

4.4.2.3.1 Selection of remote IP endpoint for data traffic

For each NS-SDU, an NS entity selects a remote IP endpoint based on the LSP for sending the NS-SDU to the peer NSE. If the LSP has not been associated with a remote IP endpoint, then a remote IP endpoint shall be selected for the LSP according to the data-weights assigned to the peer NSE's IP endpoints. The remote IP endpoints shall be selected in equal proportion to the data-weights assigned to the peer NSE's endpoints. Data-weights are assigned by the peer NSE and have a value range of 0 to 255. A data weight of 0 assigned to an IP endpoint indicates that the load sharing function shall not initially associate this remote IP endpoint to an LSP. However, if an LSP has been previously associated with a remote IP endpoint, NS SDUs associated with this LSP shall be sent to this remote IP endpoint regardless of its data weight, i.e., even when the data weight has a value of 0. (This association of LSP to the IP endpoint with a data weight of 0 may have been requested by the remote NSE via the Resource Distribution Function.)

Examples of equal proportion selection:

- If IP endpoint (A) has data weight=5 and endpoint (B) has data weight=10, then endpoint (B) will be selected for initial association with an LSP twice as often as endpoint (A).

- If IP endpoint (A) has data weight=10 and endpoint (B) has data weight=10, then endpoint (A) and endpoint (B) will be selected for initial association with an LSP on an equal basis.

- If IP endpoint (A) has a data weight=0, then IP endpoint (A) will not be selected for initial association with an LSP. However, IP endpoint (A) may be associated with an LSP via the peer NSE's use of the Resource Distribution Function.

Once a remote IP endpoint is selected for the LSP, the NSE should maintain a linkage between the LSP and the remote IP endpoint so that NS SDUs with the same LSP shall be directed to the same remote IP endpoint. If a remote IP endpoint associated with an LSP is taken out of service, then another remote IP endpoint shall be selected according to the data-weights assigned by the peer NSE and associated with the LSP. The association of an LSP to a remote IP endpoint can be changed by the peer NSE using the Resource Distribution function (refer to sub-clause 4.4a).

The BSS may disassociate the LSP from the remote IP endpoint when an MS makes a cell change or when the MS context is deleted. The SGSN shall associate an MS with the last used remote IP endpoint as long as the SGSN has location information for the MS on cell level.

The Link Selector Parameter is locally used at the BSS and at the SGSN and shall not be transmitted across the Gb interface.

4.4.2.3.2 Selection of remote IP endpoint for signalling traffic

Outgoing BVCI=0 NS-SDUs, or SNS PDUs shall be sent to a remote IP endpoint according to the signalling weight assigned by the peer NSE. The sending NSE shall distribute these messages in equal proportion to the signalling weights assigned to the peer NSE's IP endpoints. The sending NSE may send the BVCI=0 NS-SDUs and all SNS PDUs from any IP endpoint.

NOTE: Load sharing endpoint selection does not apply to NS-SDUs or SNS PDUs subject to specific conditions stipulated elsewhere in the present specification, such as SNS-SIZE and SNS-CONFIG PDUs that need to be sent to an SGSN pre-configured endpoint, or any acknowledgement / response that needs to be sent back to the endpoint having originated the corresponding request.

Examples of equal proportion selection:

- If IP endpoint (A) has signalling weight=5 and IP endpoint (B) has signalling weight=10, then IP endpoint (B) will be selected as a signalling IP endpoint twice as often as IP endpoint (A).
- If IP endpoint (A) has signalling weight=10 and IP endpoint (B) has signalling weight=10, then IP endpoint (A) and IP endpoint (B) will be selected as a signalling IP endpoint on an equal basis.
- If IP endpoint (A) has a signalling weight=0, then IP endpoint (A) will not be selected as a signalling IP endpoint.

If there is no available remote IP endpoint, the corresponding traffic is discarded by the NS at the sending side.

The Link Selector Parameter is locally used at the BSS and at the SGSN and shall not be transmitted across the Gb interface.

4.4a Resource distribution function

The resource distribution function is only available for data traffic when an IP sub-network is used. This function allows the BSS or SGSN to explicitly change the IP endpoint at which it receives NS SDUs. The BSS or SGSN may choose not to initiate any request for change in IP endpoints for any MS or MBMS session and rely on the underlying load sharing function to properly distribute NS user traffic. However, if the BSS or SGSN receives a request to change the IP endpoint at which NS SDUs are received for an MS or MBMS session, then the higher layers shall be informed of this change by an indication in the Link Selector Parameter. That is, if the SGSN (BSS) receives a request to change the remote IP endpoint for an MS or MBMS session then subsequent downlink (uplink) data for the mobile or MBMS session shall be sent to that remote IP endpoint indicated by the request.

The Resource Distribution Function overrides the Load Sharing function for the selection of the remote IP endpoint. The Resource Distribution Function overrides the data weight of a remote IP endpoint (i.e. the Resource Distribution Function can request that data be sent to an IP endpoint that has a data weight=0).

4.4a.1 Requirements on resource distribution function

In an IP sub-network the BSS or SGSN may receive an NS SDU with a request to change the remote IP endpoint. The triggers for generating a request are implementation dependent and are not subject to further standardization. The behaviour on receipt of a request shall meet the following requirements:

- An NSE may change the IP endpoint at which the NS SDUs for an MS are received by setting the R-bit field to "1" (Request change flow) in the *NS SDU Control Bits* IE in the next NS SDU or in an NS SDU with no data.

NOTE: The BSSGP DL-UNITDATA (BSSGP UL-UNITDATA) and the BSSGP UL-MBMS-UNITDATA with an LLC-PDU Length Indicator set to 0 are given in 3GPP TS 48.018.

- An NSE shall only act on a request for change in IP endpoint if the new IP endpoint has previously been configured and is operational.
- For MBMS, the resource distribution function is only available at the BSS side. That is, it is only the BSS that can request a change of the IP endpoint to which the NS SDUs for an MBMS session are sent while MBMS data flows are only present in the downlink direction.
- Upon receiving a request for change in IP endpoint, an NSE shall notify the NS user entity of the change by an indication in the Link Selector Parameter (that is, the IP endpoint at the peer entity) and direct subsequent NS SDUs for the given MS or MBMS session to the new IP endpoint.
- The resource distribution functions are independent at the BSS and the SGSN. That is, each entity may independently choose the IP endpoint at which NS SDUs for an MS or MBMS session are received.
- An NSE shall obtain the new IP endpoint from the source IP endpoint (i.e. in the UDP/IP header) of the NS SDU in which the Request Change Flow bit was set. The new IP Endpoint is not explicitly transmitted over the Gb.
- The BSS shall associate an MS with the last used remote IP endpoint as long as the MS context exist in the BSS or until the MS makes a cell change.
- The SGSN shall associate an MS with the last used remote IP endpoint as long as the SGSN has location information for the MS on cell level.
- The SGSN shall associate an MBMS session with the last used remote IP endpoint for the duration of the MBMS session.

4.5 NS-VC management function

The NS-VC management function is responsible for the blocking / unblocking, reset and test of NS-VCs.

4.5.1 Blocking / unblocking of an NS-VC

The blocking / unblocking procedures shall not be used for an IP Sub-network.

When a condition making an NS-VC unavailable for NS user traffic is locally detected at the BSS or at the SGSN, the NS-VC shall be marked as blocked by the local NS entity and the remote NS peer entity shall be informed by means of a blocking procedure. The remote NS entity shall then mark the NS-VC as blocked and shall consider it as unavailable for NS user traffic.

A BSS or SGSN may block an NS-VC because of:

- Operation and Maintenance intervention at the Gb interface making the NS-VC unavailable for NS user traffic;
- equipment failure at a BSS or an SGSN entity;
- equipment or link failure on a BSS or an SGSN site;
- failure in the transit network; or
- other causes.

When the NS-VC becomes available again for NS user traffic, the NS entity which initiated the blocking procedure may inform the remote NS peer entity by means of an unblocking procedure. The remote NS entity shall then mark the NS-VC as unblocked and shall consider it as available for NS user traffic.

The blocking / unblocking procedures are further detailed in the rest of the present document.

4.5.2 Reset of an NS-VC

The reset procedure shall not be used for an IP Sub-network.

This procedure is used to reset one NS-VC to a determined state between remote entities. This procedure is performed:

- when a new NS-VC is set-up;

- after a processor re-start;
- after a failure recovery when the state of an NS-VC must be set to blocked and alive; or
- at any local event restoring an existing NS-VC in the dead state or in an undetermined state.

When a reset procedure is initiated, data in transfer may be lost.

4.5.3 Test of an NS-VC

The test procedure is used to check that end-to-end communication exists between peer NS entities on a given NS-VC. When end-to-end communication exists, the NS-VC is in the "alive" state, otherwise it is in the "dead" state. A dead NS-VC can not be in the "unblocked" state.

5 Elements for layer-to-layer communication

This sub-clause presents the Network Service in a generic way, no assumptions are made regarding the real protocols providing the network services.

5.1 Service primitive model

The service primitive model shown in figure 5.1.1 is applicable to both BSS and SGSN.

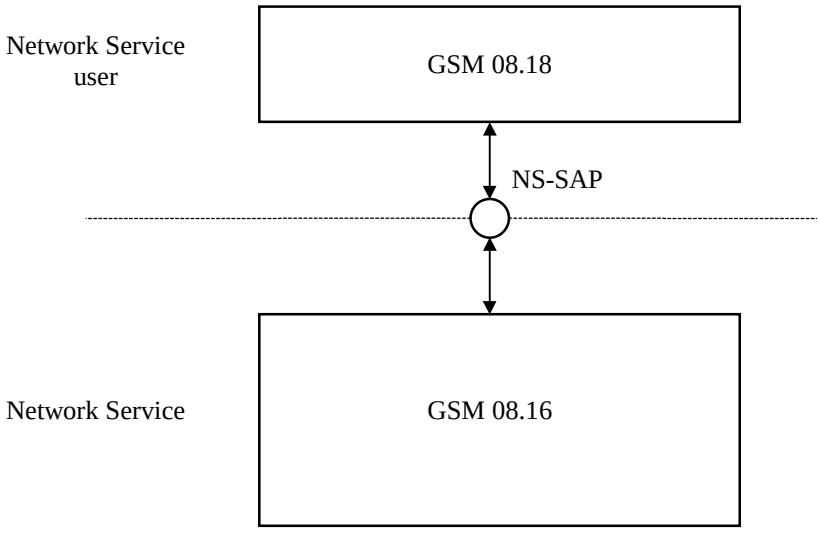


Figure 5.1.1: Network Service primitive model

The network services are provided at the Network Service-Service Access Point (NS-SAP).

5.2 Service primitives and parameters

The Network Service primitives are summarized in table 5.2.1. The general syntax of the Network Service primitives is:

NS - Generic name - Type (Parameters).

Table 5.2.1: Network Service primitives

Generic name	Type				Parameters
	Request	Indication	Response	Confirm	
UNITDATA	X	X			- BVCI and NSEI - NS SDU - NS Change IP endpoint - Link Selector Parameter
CONGESTION		X			- BVCI and NSEI - congestion cause
STATUS		X			- BVCI and NSEI - NS affecting cause - transfer capability

5.2.1 Primitives

5.2.1.1 NS-UNITDATA-Request

This primitive is used by the NS user entity to send a NS SDU to its peer entity via a BVC. The NS entity sends the NS SDU in unacknowledged mode. The Link Selector Parameter is used to identify the NS SDUs which must be sent in order relatively to each other. The NSEI is used by the NS entity to select the group of NS-VCs corresponding to the addressed remote entity. The NS Change IP endpoint is used to request the NS entity to indicate whether a "request change flow" or "confirm change flow" indication needs to be sent to its peer entity.

5.2.1.2 NS-UNITDATA-Indication

This primitive is used by the NS entity to provide the NS user entity with a NS SDU received on a virtual connection. The NS SDU are received in unacknowledged mode. BVCI together with NSEI indicate which BVC the NS SDU was received on. The NS Change IP endpoint is used to indicate to the user of the NS entity whether a "request change flow" or "confirm change flow" indication was received from the peer entity. In case a "request change flow" is received from the peer entity the Link Selector Parameter on which the NS SDU was received is sent to the higher layer.

5.2.1.3 NS-CONGESTION-Indication

The NS entity shall be able to detect when a congestion situation starts and ends on an NS-VC.

This primitive is used by the NS entity to report to the NS user entity that congestion is detected or that the congestion situation has disappeared. The BVCI and NSEI of the affected BVC and the congestion cause are reported to the NS user entity. Typically, the cause indicates the direction of transmission affected by the congestion.

5.2.1.4 NS-STATUS-Indication

There may be situations where an NS-VC becomes unavailable for NS user traffic. When this occurs, the NS user is informed of the degradation of the transfer capacity by means of this primitive including the "transfer capability" parameter.

When an NS-VC previously unavailable for NS user traffic becomes available again, the NS user entity is also informed by means of this service primitive, indicating the current transfer capability.

This primitive may be used in response to an NS-UNITDATA-Request primitive which the NS is unable to serve because of e.g. NS-VC failure.

This primitive may also be used upon recovery after a failure affecting the NS.

5.2.2 Parameters

5.2.2.1 NS SDU

The NS SDUs are specified in 3GPP TS 48.018. They shall never be inspected by the Network Service entity.

5.2.2.2 Link Selector Parameter

The Link Selector Parameter is included in the NS-UNITDATA-Request primitive for load sharing purposes as described in sub-clause "Requirements on load sharing function".

The Link Selector Parameter is included in the NS-UNITDATA-Indication primitive and in the NS-UNITDATA-Request primitive for resource distribution purposes as described in sub-clause 4.4a.1. The Link Selector Parameter shall include a reference to the local IP endpoint and the remote IP endpoint for resource distribution purposes if the NS Change IP endpoint parameter has the cause value of "request change flow".

5.2.2.3 BVCI I and NSEI

BVCI and NSEI parameters are included in the service primitives to identify the BVC for which the service is provided. These parameters are used by the NS entity to multiplex the NS SDUs over the NS-VCs.

5.2.2.4 Congestion cause

The congestion cause shall indicate the affected direction of transmission and may be set to the following values:

a) congestion detected, backward;

b) end of congestion, backward;

c) congestion detected, forward;

d) end of congestion, forward.

5.2.2.5 Transfer capability

This parameter is used to report to the NS user entity the current transfer capacity available for a BVC, in terms of bandwidth. This parameter may be set to any value from "0" (zero) to the maximum bandwidth provided by the complete set of NS-VCs associated to the BVC.

5.2.2.6 NS affecting cause

This parameter is used to indicate to the NS user entity the reason which caused the NS-STATUS-Indication primitive to be used. The cause values are:

NS-VC failure: a failure is affecting one or more NS-VCs, the NS is still available.

NS-VC recovery: one or more NS-VCs which were in failure are available again.

NS failure: the NS can not provide data transfer services to the NS user.

NS recovery: the NS can provide data transfer services again.

5.2.2.7 NS change IP endpoint

The NS change IP endpoint parameter is included in the NS-UNITDATA-Request and NS-UNITDATA-Indication primitive for resource distribution purposes. This parameter is used in an IP sub-network to indicate to the NS user entity a request for change in IP endpoint or a response to a change in IP endpoint. The cause values are:

Request change flow: Request to change the IP endpoint at which to receive NS SDUs associated with a subscriber or MBMS session.

Confirm change flow: Confirmation to a request for change of IP endpoint of NS SDUs associated with a subscriber or MBMS session.

6 Sub-Network Service protocol

6.1 Frame Relay support of the Sub-Network Service protocol

6.1.1 Overview

The Gb interface may consist of direct point-to-point connections between the BSS and the SGSN, or an intermediate Frame Relay network may be placed between both ends of the Gb interface. Other intermediate equipments may be traversed. Several configurations are possible, the detail of which is outside the scope of the present document. For the purposes of the present document the following two types of configurations have to be considered:

- Point-to-point physical connections.
- Intermediate Frame Relay network.

In case of an intermediate Frame Relay network, both BSS and SGSN shall be treated as the user side of the user-to-network interface. The network-to network interface is outside the scope of the present document.

Only Frame Relay permanent virtual connections (PVCs) shall be used on the Gb interface. Therefore ITU-T Recommendation Q.922 Annex A or T1.618 for PCS1900 and ITU-T Recommendation Q.933 Annex A or T1.617 for PCS1900, permanent virtual connection procedures, shall be supported. Switched virtual connection procedures in ITU-T Recommendation Q.922 or T1.618 for PCS1900 and ITU-T Recommendation Q.933 or T1.617 for PCS1900 shall not be supported. ITU-T Recommendation Q.921 or T1.602 and ITU-T Recommendation Q.931 procedures shall not be applicable.

The Frame Relay user-to-network interface (UNI) shall be implemented on the Gb interface according to the FRF 1.1 agreement, unless otherwise stated in the present document. Selected options or deviations from FRF 1.1 are specified in the rest of this Frame Relay chapter. Where discrepancies arise between the present document and the above mentioned recommendations, the present document takes precedence.

The rest of this Frame Relay sub-clause applies only to PVC usage.

The Gb interface addressing principles shall be applied as follows:

- The physical link is the Frame Relay bearer channel.
- The NS-VL is the local link in one end (at UNI) of the Frame Relay PVC.
- The NS-VLI is the Frame Relay DLCI together with the bearer channel identifier.
- The NS-VC is the Frame Relay PVC.
- The Sub-Network Service entity is the Frame Relay entity.

6.1.2 Network configuration

The Gb interface is a User-to-Network (UNI) interface, as defined in FRF 1.1. Two configurations are possible, either a direct link configuration or PVC(s) via a Frame Relay network.

Annex A shows an example of each type of configuration.

In case of point-to-point connections, the BSS shall be considered as the user side of the user-to-network interface, the SGSN shall be considered as the network side, see figure 6.1.2.1.

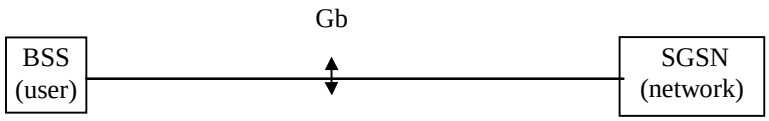


Figure 6.1.2.1: Direct link configuration

In case of an intermediate Frame Relay network, both BSS and SGSN shall be treated as the user side of the user-to-network interface, see figure 6.1.2.2. The network-to network interface is outside the scope of the present document.

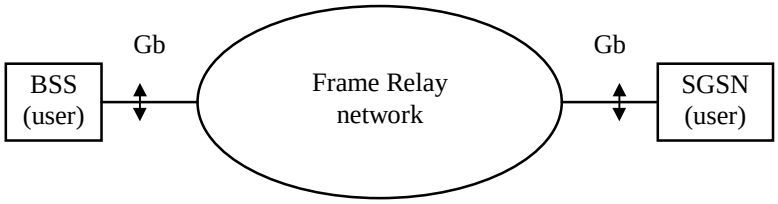


Figure 6.1.2.2: PVC via a Frame Relay Network

6.1.3 Services expected from layer 1

In the context of Frame Relay, the physical link is referred to as the bearer channel.

The Frame Relay protocol shall be run across permanently reserved bearer channels on the Gb interface, see 3GPP TS 48.014.

6.1.4 Options selected from FRF 1.1

6.1.4.1 Support of DL-CONTROL sub-layer

No end-to-end DL-CONTROL sub-layer shall be implemented on the Gb interface.

6.1.4.2 Frame length

The default maximum information field size of 1 600 octets shall be supported on the Gb interface. Maximum information field sizes greater than 1 600 octets may be agreed to between Frame Relay network operators and users at subscription time.

6.1.4.3 Congestion control procedures

Congestion control is defined in FRF 1.1 and consists of congestion avoidance and congestion recovery mechanisms.

Congestion control on the Gb interface consists of congestion avoidance based on the DE bit and on explicit notifications via the FECN and BECN bits within the address field of the Frame Relay frame.

Congestion avoidance based on the CLLM message (see ITU-T Recommendation Q.922 sub-clause A.7 or T1.618 for PCS1900 and FRF 1.1 sub-clause 2.2.5) is not required at the BSS and SGSN sides.

No congestion control mechanism based on implicit congestion detection (see ITU-T Recommendation Q.922 sub-clause A.6.1) or T1.618 for PCS1900 is required at the BSS and SGSN sides.

6.1.4.3.1 DE bit usage

The BSS and the SGSN shall always set the DE bit to 0 (zero).

6.1.4.3.2 FECN and BECN bit usage

Setting of the FECN and BECN bits:

The FECN and BECN bits shall be set to 0 by the BSS and the SGSN.

Reaction upon receipt of FECN or BECN marked frames:

The reaction of the BSS and the SGSN upon reception of FECN or BECN marked frames is implementation dependent.

It is recommended to implement ITU-T Recommendation Q.922 appendix I.2 or T1.618 for PCS1900 procedures or similar procedures, so that the NS entity can reduce or increase the transmission rate, depending on the FECN or BECN bits received.

The NS entity shall be able to report the congestion situation to the upper layer. The criteria to be met for congestion being reported to the upper layer are implementation dependent. The upper layer is expected to reduce or increase its transmission rate as appropriate. It shall be up to the upper layer to perform further appropriate actions e.g. flow control with its peer entity, see ITU-T Recommendation I.370 or T1.606 for PCS1900.

6.1.4.4 Signalling procedures

ITU-T Recommendation Revised Q.933 annex A or T1.617 for PCS1900 procedures shall be implemented at the BSS and the SGSN sides as recommended in FRF 1.1 sub-clause 2.3.

On the Gb interface, these procedures shall be initiated by the user side of the UNI, reverse procedures shall not be used.

Only periodic polling shall be used, asynchronous status message needs not to be supported.

Switched virtual connection procedures , see FRF 1.1 sub-clause 2.3.2, shall not be implemented.

6.1.4.5 C/R bit usage

The C/R bit shall not be used and shall be set to 0 by the sending entity. It shall not be checked by the receiving entity.

6.1.5 Abnormal conditions

Upon detection of the unavailability of a PVC by the Frame Relay entity or when a PVC becomes available again, the Network Service Control entity shall be informed. Unavailability cases are described in Recommendations ITU-T Recommendation Q.922 or T1.618 for PCS1900 and ITU-T Recommendation Q.933 annex A or T1.617 for PCS1900.

6.2 IP Support of the Sub-Network Service Protocol

6.2.1 Overview

The IP Sub-Network shall use the Internet Protocol (IP) as defined in either RFC 791 or RFC 2460 and the User Datagram Protocol (UDP) as defined in RFC 768.

The connections between the BSS and the SGSN may consist of point-to-point connections or of an intermediate IP network. Several configurations are possible, the details of which are outside the scope of the present document. For the purposes of the present document the following characteristics have to be considered:

1) The Sub-Network Service (SNS) may be configured by administrative means (i.e. static configuration) or by auto-configuration procedures (i.e. dynamic configuration). In the case of auto-configuration the operator shall ensure, in advance, that each NSE can fulfil its peer NSE requirements (e.g. maximum number of NS-VCs, maximum number of IP-endpoints).

2) Administrative configuration means the administration of the NSEs' IP endpoints (including the Signalling Weight and Data Weight).

3) In the case of a point-to-point connection, the administrative configuration shall be used. In the case of an intermediate IP network connection, then either the administrative means or the auto-configuration procedures may be used.

4) The BSS NSE has no knowledge of the configuration of any other BSS NSEs.

5) The auto-configuration procedures are used to exchange configuration information between the BSS and the SGSN. The client/server principle applies: the SGSN is the server, while the BSS is a client. The BSS shall have knowledge of at least one SGSN IP endpoint, referred to as pre-configured endpoint hereafter, to initiate the procedures. The auto-configuration procedures consist of the following:

a) After start-up the BSS NSE reports to the peer-SGSN NSE by initiating the Size procedure.

b) Then, the BSS initiates the Configuration Procedure in which a sequence of messages are exchanged between the BSS and the SGSN containing signalling endpoints, data endpoints, and initial weights.

A pre-configured endpoint shall not be used for NSE data or signalling traffic (with the exception of Size and Configuration procedures) unless it is configured by the SGSN using the auto-configuration procedures.

6) A network connection as part of the intermediate IP network between the NSEs shall be terminated by the same type of IP addresses (e.g. IPv4 or IPv6).

7) For dynamic configurations the change of initially configured parameters shall be supported by the Add procedure, Delete procedure and ChangeWeight procedure.

8) The SNS messages (SNS SIZE, SNS CONFIG, SNS ADD, SNS DELETE, SNS CHANGEWEIGHT) serving to support the configuration, Size, Add, Delete and ChangeWeight procedures shall only be used in the case of dynamic configuration.

6.2.1a Abnormal Conditions

If the BSS or SGSN NSE receives at a given IP endpoint an SNS PDU containing an unknown NSEI or an NSEI associated to a different local IP endpoint, the BSS or SGSN NSE may simply discard such SNS PDU without further action.

6.2.2 IP Fragmentation

Fragmentation should be avoided if possible. Examples of fragmentation drawbacks are, e.g.:

- Fragmentation is inefficient, since the complete IP header is duplicated in each fragment.
- If one fragment is lost, the complete packet has to be discarded. The reason is that no selective retransmission of fragments is possible.

Mechanisms used to avoid fragmentation are outside the scope of the present document.

6.2.3 Services expected from layer 1 and layer 2

Layer one and two are unspecified. No services are defined in the present document.

6.2.4 Size Procedure

This procedure is initiated by the BSS. The Size procedure shall be performed to:

- Reset all information maintained by the BSS NSE and its peer prior to the configuration procedure.
- Verify that the number of NS-VCs that can be supported by the BSS NSE is greater than or equal to the number of NS-VCs required for full mesh connectivity to the peer SGSN NSE.
- Verify that the number of IP endpoints indicated by the BSS NSE can be supported by the SGSN NSE.
- Verify the compatibility between the type of IP addresses (IPv4/IPv6) supported by the peer NSEs.

The BSS NSE shall send an SNS-SIZE PDU to the SGSN using any of the pre-configured SGSN IP endpoints (configuring of any pre-configured SGSN IP endpoints is out of the scope of the present document). The BSS shall start timer Tsns-prov. The SNS_SIZE PDU shall contain the following information elements:

- NSEI: NSE Identifier.
- Maximum Number of NS-VCs: maximum number of NS-VCs the BSS NSE can support.
- Reset Flag: indicates whether all configuration information between the BSS NSE and its peer SGSN NSE shall be cleared prior to a forthcoming initiation of the configuration procedure by the BSS NSE (Reset-bit field of the

Reset Flag IE set to "1"), or if the procedure is only initiated to ascertain the ability of the SGSN NSE to support the requested capabilities (Reset-bit field of the *Reset Flag* IE set to "0").

- Number of IP4 Endpoints: maximum number of BSS NSE IPv4 addresses that the BSS NSE is allowed to configure through the forthcoming configuration procedure and/or

- Number of IP6 Endpoints: maximum number of BSS NSE IPv6 addresses that the BSS NSE is allowed to configure through the forthcoming configuration procedure.

Upon receipt of an SNS-SIZE PDU, the SGSN shall:

- If the Reset-bit field of the *Reset Flag* IE is set to "1", clear all previous operating information about the BSS NSE (no operating information shall be affected in the SGSN if the Reset-bit field of the *Reset Flag* IE is set to "0").

- Send an SNS-SIZE-ACK PDU to the source IP endpoint. The SNS-SIZE-ACK PDU shall contain the NSEI IE. The SNS-SIZE-ACK PDU may contain the *Cause* IE as specified in sub-clause 6.2.4.1.

Upon receipt of an SNS-SIZE-ACK PDU the BSS shall:

- Stop timer Tsns-prov.

- If the Reset-bit field of the *Reset Flag* IE was set to "1" in the SNS-SIZE PDU sent by the BSS, initiate the configuration procedure (see sub-clause 6.2.5).

6.2.4.1 Abnormal Conditions

If the maximum number of NS-VCs indicated in the SNS-SIZE PDU is less than the number of NS-VCs required for full mesh connectivity between the peer NSEs, the SGSN shall send an SNS-SIZE-ACK PDU with a cause code "Invalid number of NS-VCs". The number of NS-VCs required for full mesh connectivity between peer NSEs is the product of the number of IPv4 endpoints supported on each of the peer NSEs plus the product of the number of IPv6 endpoints supported on each of the peer NSEs.

Upon receiving the SNS-SIZE-ACK PDU with a cause code "Invalid number of NS-VCs" the BSS NSE may notify the O&M system and abort the procedure.

If the SGSN does not support the type of IP addresses (IPv4/IPv6) offered by the BSS, the SGSN shall send an SNS-SIZE-ACK PDU with a cause code "Invalid number of IP4 Endpoints" or "Invalid number of IP6 Endpoints". Upon receiving the SNS-SIZE-ACK PDU with a cause code "Invalid number of IP4 Endpoints" or "Invalid number of IP6 Endpoints" the BSS NSE may notify the O&M system and abort the procedure.

If the SGSN does not support the number of IPv4 endpoints indicated in the SNS-SIZE PDU, the SGSN shall send an SNS-SIZE-ACK PDU with a cause code set to "Invalid number of IP4 Endpoints". If the SGSN does not support the number of IPv6 endpoints indicated in the SNS-SIZE PDU, the SGSN shall send an SNS-SIZE-ACK PDU with a cause code set to "Invalid number of IP6 Endpoints". Upon receiving the SNS-SIZE-ACK PDU with a cause code set to "Invalid number of IP4 Endpoints" or "Invalid number of IP6 Endpoints", the BSS NSE may notify the O&M system and abort the procedure.

Upon expiry of timer Tsns-prov the NSE may retry the operation SNS-SIZE-RETRIES times. If the operation has been attempted SNS-SIZE-RETRIES times without acknowledgement from the peer NS entity, then the NS entity may notify the O&M system and abort the procedure. Whether the NS entity would restart the size procedure using any pre-configured SGSN IP endpoints after abortion is left implementation dependent. Further actions are outside the scope of the present document.

6.2.5 Configuration Procedure

The configuration procedure is used on the Gb interface to exchange configuration information between an NSE and its peer NSE. To start the configuration procedure, the client/server principle is used, with the BSS as the client. Upon start-up/restart of a BSS NSE or following the detection of a restart of a peer SGSN NSE (e.g. by means of the test procedure - see sub-clause 7.4b), the Size procedure with the Reset-bit field of the *Reset Flag* IE set to "1" in the SNS-SIZE PDU shall be performed upon initiation by the BSS NSE before the configuration procedure is started.

After completion on the BSS side of the Size procedure having indicated a reset, the BSS NSE shall send an SNS-CONFIG PDU to the same pre-configured SGSN IP endpoint used in the Size procedure.

NOTE: This does not imply that the SNS-CONFIG PDU has to be sent from the same IP endpoint used in the Size procedure.

The BSS shall start timer Tsns-prov. The SNS-CONFIG PDU shall contain the following information elements:

NSEI: NSE Identifier.

End Flag: identifies the last SNS-CONFIG PDU sent by the BSS NSE.

List of IP4 Elements: one or more IPv4 endpoints, or

List of IP6 Elements: one or more IPv6 endpoints.

Upon receipt of an SNS-CONFIG PDU sent by the BSS, the SGSN shall send an SNS-CONFIG-ACK PDU to the source IP endpoint.

Upon receipt of an SNS-CONFIG-ACK PDU sent by the SGSN, the BSS shall:

- Stop timer Tsns-prov.
- Repeat the above SNS-CONFIG PDU sequence to the SGSN if the BSS has more IP endpoints to configure.

After completion on the SGSN side of the Size procedure, the SGSN shall send an SNS-CONFIG PDU to the BSS NSE using any known signalling IP endpoints (i.e., from information contained within an SNS-CONFIG PDU sent by the BSS). The SGSN shall start timer Tsns-prov. The SNS-CONFIG PDU shall contain the following information elements:

NSEI: NSE Identifier.

End Flag: identifies the last SNS-CONFIG PDU sent by the SGSN NSE.

List of IP4 Elements: one or more IPv4 endpoints, or

List of IP6 Elements: one or more IPv6 endpoints.

Upon receipt of an SNS-CONFIG PDU sent by the SGSN, the BSS shall send an SNS-CONFIG-ACK PDU to the source IP endpoint.

Upon receipt of an SNS-CONFIG-ACK PDU sent by the BSS, the SGSN shall:

- Stop timer Tsns-prov.
- Repeat the above SNS-CONFIG PDU sequence to the BSS if the SGSN has more IP endpoints to configure. The SGSN shall start timer Tsns-prov.

Neither the SGSN nor the BSS shall initiate any other procedure before receiving the peer's end-flag.

6.2.5.1 Abnormal Conditions

Upon receiving an SNS-CONFIG PDU with the E-bit field in the *End Flag* IE set to "1", if the total number of IPv4 elements sent to the SGSN by the BSS NSE is greater than the number of IPv4 endpoints sent by the BSS NSE in the SIZE PDU, the SGSN shall send an SNS-CONFIG-ACK PDU with a cause code of "Invalid number of IP4 Endpoints". The SGSN shall clear all information associated with the peer BSS NSE.

Upon receiving an SNS-CONFIG-ACK PDU with a cause code set to "Invalid number of IP4 Endpoints" the BSS may notify the O&M system and abort the procedure. Further actions are outside the scope of the present document. The BSS shall clear all information associated with the peer SGSN NSE.

Upon receiving an SNS-CONFIG PDU with the E-bit field in the *End Flag* IE set to "1", if the total number of IPv6 elements sent to the SGSN by the BSS NSE is greater than the number of IPv6 endpoints sent by the BSS NSE in the SIZE PDU, the SGSN shall send an SNS-CONFIG-ACK PDU with a cause code of "Invalid number of IP6 Endpoints". The SGSN shall clear all information associated with the peer BSS NSE.

Upon receiving an SNS-CONFIG-ACK PDU with a cause code set to "Invalid number of IP6 Endpoints" the BSS may notify the O&M system and abort the procedure. Further actions are outside the scope of the present document. The BSS shall clear all information associated with the peer SGSN NSE.

Upon receiving an SNS-CONFIG PDU with the E-bit field in the *End Flag* IE set to "1", if the total number of IPv4 elements sent to the BSS by the SGSN NSE is greater than the number of IPv4 endpoints supported by the BSS NSE, the BSS shall send an SNS-CONFIG-ACK PDU with a cause code set to "Invalid number of IP4 Endpoints" and clear all information associated with the peer SGSN NSE.

Upon receiving an SNS-CONFIG PDU with the E-bit field in the *End Flag* IE set to "1", if the total number of IPv6 elements sent to the BSS by the SGSN NSE is greater than the number of IPv6 endpoints supported by the BSS NSE, the BSS shall send an SNS-CONFIG-ACK PDU with a cause code set to "Invalid number of IP6 Endpoints" and clear all information associated with the peer SGSN NSE.

Upon receiving an SNS-CONFIG-ACK PDU with a cause code set to "Invalid number of IP4 Endpoints" or "Invalid number of IP6 Endpoints" the SGSN may notify the O&M system and abort the procedure. Further actions are outside the scope of the present document. The SGSN shall clear all information associated with the peer BSS NSE.

Upon receiving an SNS-CONFIG PDU with the E-bit field in the *End Flag* IE set to "1", if the resulting sum of the signalling weights of all the peer IP endpoints configured for this NSE is equal to zero or if the resulting sum of the data weights of all the peer IP endpoints configured for this NSE is equal to zero the NSE shall send an SNS-CONFIG-ACK PDU with a cause code of "Invalid weights". The NSE shall clear all information associated with the peer NSE. Upon receiving an SNS-CONFIG ACK PDU with cause code set to "Invalid weights" the NSE shall clear all information associated with the peer NSE and may notify the O&M system.

Upon expiry of timer Tsns-prov the NSE may retry the operation SNS-CONFIG-RETRIES times. If the operation has been attempted SNS-CONFIG-RETRIES times without acknowledgement from the peer NSE, then the NSE may notify the O&M system and abort the procedure. Further actions are outside the scope of the present document.

6.2.6 Add Procedure

The Add procedure is used by an NSE to configure additional IP endpoints.

To add new IP endpoints, the NSE shall send an SNS-ADD PDU to a peer NSE signalling endpoint. Upon sending the SNS-ADD PDU the NSE shall start timer Tsns-prov. The SNS-ADD PDU shall contain the following information elements:

NSEI: NSE Identifier.

Transaction ID: identifies a unique transaction within an NSE.

List of IP4 Elements: one or more IPv4 endpoints, or.

List of IP6 Elements: one or more IPv6 endpoints.

Upon receipt of an SNS-ADD PDU the NSE shall send an SNS-ACK PDU to the source IP endpoint from which the SNS-ADD PDU was sent. The SNS-ACK PDU shall contain the Transaction ID set to the same value as that in the SNS-ADD PDU.

Upon receipt of an SNS-ACK PDU the NSE shall stop timer Tsns-prov.

6.2.6.1 Abnormal Conditions

Upon receiving an SNS-ADD PDU, if the consequent number of NS-VCs exceeds the maximum own supported number of NS-VCs then the NSE shall send an SNS-ACK PDU with cause code set to "Invalid number of NS-VCs".

Upon receiving an SNS-ADD PDU, if the consequent number of IPv4 endpoints exceeds the number of IPv4 endpoints supported by the NSE, the NSE shall send an SNS-ACK PDU with a cause code set to "Invalid number of IP4 Endpoints".

Upon receiving an SNS-ADD PDU, if the consequent number of IPv6 endpoints exceeds the number of IPv6 endpoints supported by the NSE, the NSE shall send an SNS-ACK PDU with a cause code set to "Invalid number of IP6 Endpoints".

Upon receiving an SNS-ADD PDU containing an already configured IP endpoint the NSE shall send an SNS-ACK PDU with the cause code "Protocol error - unspecified".

For any of the abnormal cases specified above:

- The whole content of the received SNS-ADD PDU shall be ignored.
- The SNS-ACK PDU shall be sent to the source IP endpoint from which the SNS-ADD PDU was sent. The SNS-ACK PDU shall contain the Transaction ID set to the same value as that in the SNS-ADD PDU.

Upon expiry of timer Tsns-prov the NSE may retry the operation SNS-ADD-RETRIES times. If the operation has been attempted SNS-ADD-RETRIES times without acknowledgement from the peer NSE, then the NSE may notify the O&M system and abort the procedure. Further actions are outside the scope of the present document.

6.2.7 Delete Procedure

The delete procedure is used by an NSE to remove previously configured IP endpoints from service.

To delete IP endpoints, the NSE shall send an SNS-DELETE PDU to a peer NSE signalling endpoint. Upon sending the SNS-DELETE PDU the NSE shall start timer Tsns-prov. The SNS-DELETE PDU shall contain the following information elements:

NSEI: NSE Identifier.

Transaction ID: identifies a unique transaction within the NSE.

IP Address: all IP endpoints that use this IP address shall be deleted or

List of IP4 Elements: one or more IPv4 endpoints, or

List of IP6 Elements: one or more IPv6 endpoints.

Upon receipt of an SNS-DELETE PDU the NSE shall send an SNS-ACK PDU to the source IP endpoint from which the SNS-DELETE PDU was sent. The SNS-ACK PDU shall contain the Transaction ID set to the same value as that in the SNS-DELETE PDU.

Upon receipt of an SNS-ACK PDU the NSE shall stop timer Tsns-prov.

6.2.7.1 Abnormal Conditions

Upon receiving an SNS-DELETE PDU containing one or more IP endpoints that has not been previously configured with an SNS-ADD PDU or an SNS-CONFIG PDU, the NSE shall send an SNS-ACK PDU with a cause code of "Unknown IP endpoint" to the source IP endpoint from which the SNS-DELETE PDU was sent. The SNS-ACK PDU shall contain the Transaction ID set to the same value as that in the SNS-DELETE PDU. The NSE shall also include, in the SNS-ACK PDU, all IPv4 endpoints in the SNS-DELETE PDU that have not been previously configured in the *List of IP4 Elements* IE, or all IPv6 endpoints in the SNS-DELETE PDU that have not been previously configured in the *List of IP6 Elements* IE. All previously configured IP endpoints contained in the SNS-DELETE PDU shall be deleted.

Upon receiving an SNS-DELETE PDU containing an IP address for which no IP endpoints have been previously configured with an SNS-ADD PDU or an SNS-CONFIG PDU, the NSE shall send an SNS-ACK PDU with a cause code of "Unknown IP address" to the source IP endpoint from which the SNS-DELETE PDU was sent. The SNS-ACK PDU shall contain the Transaction ID set to the same value as that in the SNS-DELETE PDU. The NSE shall also include, in the SNS-ACK PDU, the IP address received in the SNS-DELETE PDU.

Upon expiry of timer Tsns-prov the NSE may retry the operation SNS-DELETE-RETRIES times. If the operation has been attempted SNS-DELETE-RETRIES times without acknowledgement from the peer NSE, then the NSE may notify the O&M system and abort the procedure. Further actions are outside the scope of the present document.

6.2.8 ChangeWeight Procedure

The ChangeWeight procedure is used by an NSE to change the signalling weight and/or data weight of the specified IP endpoints.

To change the signalling weight and/or data weight of an IP endpoint, the NSE shall send an SNS-CHANGEWEIGHT PDU to a peer NSE signalling endpoint. Upon sending the SNS-CHANGEWEIGHT PDU the NSE shall start timer Tsns-prov. The SNS-CHANGEWEIGHT PDU shall contain the following information elements:

NSEI: NSE Identifier.

Transaction ID: identifies a unique transaction within the NSE.

List of IP4 Elements: one of more IPv4 endpoints, or

List of IP6 Elements: one or more IPv6 endpoints.

Upon receipt of an SNS-CHANGEWEIGHT PDU the NSE shall send an SNS-ACK PDU to the source IP endpoint from which the SNS-CHANGEWEIGHT PDU was sent. The SNS-ACK PDU shall contain the Transaction ID set to the same value as that in the SNS-CHANGEWEIGHT PDU.

Upon receipt of an SNS-ACK PDU the NSE shall stop timer Tsns-prov.

6.2.8.1 Abnormal Conditions

Upon receiving an SNS-CHANGEWEIGHT PDU, if the resulting sum of the signalling weights of all the peer IP endpoints configured for this NSE is equal to zero or if the resulting sum of the data weights of all the peer IP endpoints configured for this NSE is equal to zero, the BSS/SGSN shall send an SNS-ACK PDU with a cause code of "Invalid weights". The whole content of that SNS-CHANGEWEIGHT PDU shall be ignored.

Upon receiving an SNS-CHANGEWEIGHT PDU containing one or more IP endpoints that has not been previously configured with an SNS-ADD PDU or an SNS-CONFIG PDU, the NSE shall send an SNS-ACK PDU with a cause code of "Unknown IP endpoint" to the source IP endpoint from which the SNS-CHANGEWEIGHT PDU was sent. The SNS-ACK PDU shall contain the Transaction ID set to the same value as that in the SNS-CHANGEWEIGHT PDU. The NSE shall also include, in the SNS-ACK PDU, all IPv4 endpoints sent in the SNS-CHANGEWEIGHT PDU that have not been previously configured in the *List of IP4 Elements* IE, or all IPv6 endpoints sent in the SNS-CHANGEWEIGHT PDU that have not been previously configured in the *List of IP6 Elements* IE. The NSE shall discard the information in the SNS-CHANGEWEIGHT PDU associated with all IP endpoints that have not been previously configured. All previously configured IP endpoints contained in the SNS-CHANGEWEIGHT PDU shall be changed.

Upon expiry of timer Tsns-prov the NSE may retry the operation SNS-CHANGEWEIGHT-RETRIES times. If the operation has been attempted SNS-CHANGEWEIGHT-RETRIES times without acknowledgement from the peer NSE, then the NSE may notify the O&M system and abort the procedure. Further actions are outside the scope of the present document.

7 Network Service Control protocol

7.1 Procedures for the transmission of NS SDUs

NS SDUs are transmitted in unacknowledged mode across the Gb interface by means of an NS-UNITDATA PDU.

The NS-UNITDATA PDU is used in both BSS-to-SGSN and SGSN-to-BSS directions.

For an IP sub-network, an NS-UNITDATA PDU for a PTP BVC may indicate a request to change the IP endpoint and/or a response to a change in the IP endpoint.

If the BSS or SGSN receives an NS-UNITDATA PDU for a signalling BVC or a PTM BVC then the BSS or SGSN shall ignore the coding of the C-bit and R-bit.

7.1.1 Abnormal Conditions

If the BSS receives an NS-UNITDATA PDU including a BVCI not associated to the NS-VC where the PDU was received, the BSS shall return an NS-STATUS PDU on that NS-VC, cause "BVC unknown on that NSE". Depending on the implementation, the BSS may then ignore the BVCI and treat the rest of the NS-UNITDATA PDU.

7.2 Blocking / unblocking procedures

The Blocking/Unblocking procedures shall not be used for an IP Sub-network.

When a BSS (or SGSN) wishes to block an NS-VC between a BSS and SGSN, the following shall be performed:

- The transmitting side at the BSS (or SGSN) shall mark the NS-VC as blocked and shall inform the load sharing function. This results in the redistribution of NS-UNIDATA PDUs to other unblocked NS-VCs of the same group, as described in the "Load sharing function" sub-clause. The NS user entity shall also be informed of the new transfer capability by means of an NS-STATUS-Indication primitive for each affected BVC. A BSS (or SGSN) then sends an NS-BLOCK PDU to the peer entity and starts timer Tns-block.

- The NS-BLOCK PDU contains the NS-VCI and a Cause element indicating the reason for blocking (typical cause values: Transit network failure, O&M intervention, Equipment failure). The NS-BLOCK PDU may be sent in any alive (blocked or unblocked) NS-VC pertaining to the same group as the NS-VC to be blocked, unless otherwise required for particular cases which may be further described in the rest of the present document.

- At the sending side of the NS-BLOCK PDU, if no failure has occurred in the receive direction (e.g. O&M intervention), the originator of the NS-BLOCK PDU shall continue to accept NS-UNITDATA PDUs received on the NS-VC being blocked, until an NS-BLOCK-ACK PDU is received for this NS-VC. The originator of the NS-BLOCK PDU shall stop to accept NS-UNITDATA PDUs, if the number of retries of the blocking procedures is exceeded.

- Upon Receipt of an NS-BLOCK PDU at an SGSN (or BSS) the NS-VC shall be marked as blocked. The SGSN (or BSS) shall immediately inform the load sharing function. The NS user entity shall also be informed of the new transfer capability by means of an NS-STATUS-Indication primitive for each affected BVC. The SGSN (or BSS) then sends in any alive (blocked or unblocked) NS-VC of the relevant group an NS-BLOCK-ACK PDU, for the blocked NS-VC, to the BSS (or SGSN).

- On receipt of an NS-BLOCK-ACK PDU or NS-BLOCK PDU, the originator of the NS-BLOCK PDU stops timer Tns-block.

The NS-VC shall remain blocked until an NS-UNBLOCK PDU is received indicating that the NS-VC's state has been changed.

When a BSS (or SGSN) wishes to unblock an NS-VC between a BSS and SGSN, the following shall be performed:

- The BSS (or SGSN) sends an NS-UNBLOCK PDU to the peer entity and starts timer Tns-block. The NS-UNBLOCK PDU shall be sent on the NS-VC to be unblocked (the NS-VC must be alive, see check procedure in sub-clauses "Test of an NS-VC"). The BSS or SGSN may discard any NS-UNITDATA PDU received on the concerned NS-VC until the reception of the NS-UNBLOCK-ACK PDU.

- If an NS-UNBLOCK PDU is received by an SGSN (or BSS) for an NS-VC and the SGSN (or BSS) is able to unblock the NS-VC, the SGSN (or BSS) shall return an NS-UNBLOCK-ACK PDU on the NS-VC where the NS-UNBLOCK PDU was received, then the NS-VC shall be marked as unblocked. The load sharing function shall be informed. The NS user entity shall also be informed of the new transfer capability by means of an NS-STATUS-Indication primitive for each affected BVC.

- A BSS (or SGSN) shall stop timer Tns-block on receipt of an NS-UNBLOCK-ACK or NS-UNBLOCK PDU, shall mark the NS-VC as unblocked and shall inform the load sharing function in order to allow transmission of NS-UNITDATA PDUs on this NS-VC. The NS user entity shall also be informed of the new transfer capability by means of an NS-STATUS-Indication primitive for each affected BVC. An NS-UNBLOCK PDU received while a BSS (or SGSN) is waiting for an NS-UNBLOCK-ACK PDU shall be acknowledged with an NS-UNBLOCK-ACK PDU.

- If an NS-UNBLOCK PDU is received by an SGSN (or BSS) and the SGSN (or BSS) is not able to unblock the NS-VC, the NS-VC shall remain blocked and the NS-VC blocking procedure shall be initiated by returning an NS-BLOCK PDU to the BSS (or SGSN). This NS-BLOCK PDU shall be sent on the NS-VC where the NS-UNBLOCK PDU was received.

- If a BSS (or SGSN) receives an NS-BLOCK PDU while waiting for an NS-UNBLOCK-ACK PDU, it shall stop timer Tns-block and the NS-VC shall remain blocked. An NS-BLOCK-ACK PDU shall be returned. An indication shall be issued towards the O&M system, announcing that the unblocking of the NS-VC was not possible at the peer entity. Further actions of the O&M system are out of the scope of the present document.

7.2.1 Abnormal Conditions

If an NS-BLOCK-ACK PDU is not received for an NS-BLOCK PDU within Tns-block seconds, then the NS-BLOCK PDU procedure shall be repeated a maximum of NS-BLOCK-RETRIES attempts. After NS-BLOCK-RETRIES unsuccessful retry attempts the procedure is stopped and the O&M system is informed that the blocking procedure has failed. Further actions of the O&M system are out of the scope of the present document. The NS-VC shall be marked as blocked at the originating side of the blocking procedure.

If an NS-UNBLOCK-ACK PDU is not received for an NS-UNBLOCK PDU within Tns-block seconds, the NS-UNBLOCK PDU procedure shall be repeated a maximum of NS-UNBLOCK-RETRIES attempts. After NS-UNBLOCK-RETRIES unsuccessful retry attempts the procedure is stopped and the O&M system is informed that the unblocking procedure has failed. Further actions of the O&M system are out of the scope of the present document. The NS-VC shall be marked as blocked at the originating side of the unblocking procedure.

If an NS-UNITDATA PDU is received on an NS-VC that is marked at a BSS or an SGSN as blocked and no NS-VC unblocking procedure is pending, then an NS-STATUS PDU (Cause value: NS-VC blocked) shall be returned to the peer entity.

If an NS-BLOCK PDU is received by a BSS or an SGSN for a blocked NS-VC, an NS-BLOCK-ACK PDU shall be returned.

If an NS-UNBLOCK PDU is received by a BSS or an SGSN for an unblocked NS-VC, an NS-UNBLOCK-ACK PDU shall be returned.

If an unexpected NS-BLOCK-ACK PDU is received by a BSS or an SGSN and it is related to an NS-VC that is locally blocked, the NS-BLOCK-ACK PDU is discarded. If the NS-BLOCK-ACK PDU is related to an NS-VC that is not locally blocked, then an NS-VC unblocking procedure is initiated.

If an unexpected NS-UNBLOCK-ACK PDU is received by a BSS or an SGSN and it is related to an NS-VC that is not locally blocked, the received NS-UNBLOCK-ACK PDU is discarded. If the NS-UNBLOCK-ACK PDU is related to an NS-VC that is locally blocked, then an NS-VC blocking procedure is initiated.

If the NS-VCI received in an NS-BLOCK or NS-BLOCK-ACK PDU is unknown, then the error shall be reported to the originator of the PDU by means of an NS-STATUS PDU including the unknown NS-VCI, with the Cause value set to "NS-VC unknown", the O&M system shall be informed, then the NS-BLOCK or NS-BLOCK-ACK PDU shall be ignored. Further actions of the O&M system are out of the scope of the present document.

7.3 Reset procedure

The reset procedure shall not be used for an IP Sub-network.

The reset procedure shall be used when a new NS-VC is set-up between a BSS and an SGSN, after processor re-start, after failure recovery or any local event restoring an existing NS-VC in the dead state or when its state is undetermined between remote NS entities. Upon completion of the reset procedure, the successfully reset NS-VC is marked as blocked and alive at both sides of the Gb interface.

When a BSS (or SGSN) wishes to reset an NS-VC, the following shall be performed:

- The NS entity at the BSS (or SGSN) informs the NS user entity of the new transfer capability by means of an NS-STATUS-Indication primitive for each affected BVC. The BSS (or SGSN) then sends an NS-RESET PDU to its peer entity indicating the NS-VCI and the NSEI. The NS-RESET PDU is sent on the NS-VC being reset. The NS-RESET PDU includes a Cause information element.

- The sending entity of the NS-RESET PDU then marks the NS-VC as blocked and dead and starts timer Tns-reset.

- Receipt of an NS-RESET PDU at an SGSN (or BSS) shall be acknowledged with an NS-RESET-ACK PDU including the NS-VCI and the NSEI, provided that the receiving side is able to reset the NS-VC (i.e. no local condition prevents the receiving side from resetting the NS-VC). The NS-RESET-ACK PDU shall be sent on the NS-VC being reset.

- The entity receiving the NS-RESET PDU then marks the acknowledged NS-VC as blocked and alive and informs the NS user entity of the new transfer capability by means of an NS-STATUS-Indication primitive for each affected BVC. The test procedure is then initiated on this NS-VC.

- When the sending entity of an NS-RESET PDU receives the NS-RESET-ACK PDU, it stops timer Tns-reset, marks the NS-VC as blocked and alive and initiates the test procedure on this NS-VC. The originator of the NS-RESET PDU is then responsible for unblocking this NS-VC.

In case of collision between reset procedures initiated at both sides of the Gb interface, the following shall apply:

- When an NS entity awaiting an NS-RESET-ACK PDU in response to an NS-RESET PDU receives an NS-RESET PDU, it shall acknowledge it as described above, and in addition, it shall treat it as an NS-RESET-ACK PDU.

When an NS entity is awaiting an NS-RESET-ACK PDU, any PDU other than NS-RESET or NS-RESET-ACK received on one of the NS-VCs being reset shall be ignored.

The reset procedure overrides any other pending procedure on the affected NS-VC i.e. other pending procedures are stopped, other running timers are stopped.

7.3.1 Abnormal conditions

If the sending entity of an NS-RESET PDU receives no NS-RESET-ACK PDU before timer Tns-reset expires the corresponding NS-VCs shall remain blocked and dead and the entire reset procedure shall be repeated. If the reset procedure remains unsuccessful for a period of time established by the operator, the O&M system shall be informed, and the reset procedure shall be stopped. Further actions of the O&M system are out of the scope of the present document.

If the NS-VCI received in an NS-RESET PDU is different from the NS-VCI locally associated to this NS-VC, the O&M system shall be informed, an NS-RESET-ACK PDU shall be returned including the NS-VCI locally associated to this NS-VC, then the NS-RESET PDU shall be ignored as if not received.

If the NSEI received in an NS-RESET PDU is different from the NSEI locally associated to this NS-VC, the O&M system shall be informed, an NS-RESET-ACK PDU shall be returned including the NSEI locally associated to this NS-VC, then the NS-RESET PDU shall be ignored as if not received.

If the NS-VCI received in an NS-RESET-ACK PDU is different from the NS-VCI locally associated to this NS-VC or if the NSEI received in an NS-RESET-ACK PDU is different from the NSEI locally associated to this NS-VC, the O&M system shall be informed, then the reset procedure shall be stopped. Further actions of the O&M system are out of the scope of the present document.

If an NS-RESET-ACK PDU is received when not expected, it shall be ignored.

7.4 Test procedure for a Frame Relay Sub-network

The test procedure shall be used when a BSS (or SGSN) wishes to check that end-to-end communication with its peer entity exists on an NS-VC.

Both sides of the Gb interface may initiate this procedure independently from each other. This procedure shall be initiated upon successful completion of the reset procedure (as specified in sub-clause "Reset procedure") and shall then be periodically repeated.

Upon successful completion of an NS-VC reset procedure, a BSS (or SGSN) shall start timer Tns-test, then:

- Upon Tns-test expiry, a BSS (or SGSN) sends an NS-ALIVE PDU on the NS-VC to be checked, starts timer Tns-alive and waits for an NS-ALIVE-ACK PDU on this NS-VC.

- Upon receipt of an NS-ALIVE PDU on an alive NS-VC, an SGSN (or BSS) shall return an NS-ALIVE-ACK PDU on the NS-VC where the NS-ALIVE PDU was received.

- Upon receipt of the NS-ALIVE-ACK PDU in response to an NS-ALIVE PDU, the originator of the NS-ALIVE PDU, shall stop timer Tns-alive and shall start again timer Tns-test.

The procedure is repeated each time Tns-test expires.

7.4.1 Abnormal conditions

If an NS-ALIVE-ACK PDU is received when not expected, it shall be ignored.

If no NS-ALIVE-ACK PDU is received before Tns-alive expires, the test procedure shall be repeated a maximum of NS-ALIVE-RETRIES attempts. After NS-ALIVE-RETRIES unsuccessful retry attempts, the procedure is stopped, the NS-VC is marked as dead and blocked, the O&M system and the load sharing function are informed, and an NS-STATUS-Indication is sent to the NS user entity. If the NS-VC is not already blocked, a blocking procedure is initiated using an alive NS-VC, if any. Further actions of the O&M system are out of the scope of the present document.

7.4b Test Procedure for an IP Sub-network

The test procedure is used on the Gb interface to verify the communications paths between the SGSN and the BSS. At least one of the signalling endpoints of the SGSN shall be tested by the BSS, by sending the NS-ALIVE PDU on any NS-VC terminating at any of the SGSN signalling endpoints. An NSE may test any peer NSE IP endpoint at any time.

It is recommended that all remote IP endpoints of an NSE (signalling and data endpoints) are tested periodically, regardless of their operational status (operational or non-operational).

Upon successful completion of the Size and configuration procedures when configured by auto-configuration procedures, or upon completion of administrative configuration, the NSE shall start timer Tns-test. Upon expiry of the timer Tns-test the NSE shall:

- send an NS-ALIVE PDU to a peer IP endpoint.
- start timer Tns-alive.
- upon receiving an NS-ALIVE-ACK PDU from the peer NSE IP endpoint, the NSE shall stop timer Tns-alive and shall start again timer Tns-test.

The procedure is repeated each time that the Tns-test expires.

Upon receipt of an NS-ALIVE PDU, on any configured IP endpoint, the NSE shall send an NS-ALIVE-ACK PDU to the source UDP/IP endpoint of the NS-ALIVE PDU.

Upon receipt of an NS-ALIVE-ACK PDU, on an IP endpoint marked as non-operational, the NSE communication path is marked as operational.

7.4b.1 Abnormal Conditions

If an NS-ALIVE-ACK PDU is received when not expected, it shall be discarded.

7.4b.1.1 Abnormal Conditions for signalling endpoints

If the NSE timer Tns-alive expires, the test procedure shall be repeated a maximum of NS-ALIVE-RETRIES times. After NS-ALIVE-RETRIES unsuccessful attempts the NSE communication path is marked as non-operational.

The O&M system and the load sharing function are informed, and an NS-STATUS-Indication is sent to the NS user entity. If more than one signalling endpoint is available at the SGSN, an NS-STATUS PDU may be sent to the SGSN using one of the available signalling endpoints of the peer NSE. The NS-STATUS includes the two IP endpoints that comprise the NS-VC and a cause code "IP test failed". Further actions of the O&M system is out of the scope of the present document.

If more than one signalling endpoints are available at the SGSN the test procedure shall continue on one or more of these endpoints.

If all signalling UDP/IP endpoints of a peer SGSN NSE are marked non-operational and if the NSE is configured by auto-configuration procedures, then the BSS NSE shall start the Size procedure with the Reset-bit field of the *Reset Flag* IE set to "1" followed by the configuration procedure.

If an SGSN tests IP endpoints of a peer BSS NSE and all signalling IP endpoints of a peer BSS NSE are marked non-operational and if the NSE is configured by auto-configuration procedures, then the SGSN NSE shall not respond to NS-ALIVE messages from that BSS NSE. If the NSE is configured by administrative means, then the SGSN NSE shall respond to NS-ALIVE messages from that BSS NSE.

When the SGSN recovers after a restart or a network failure and if the NSE is configured by auto-configuration procedures, it shall not respond on any NS-PDUs until the Size and configuration procedures have been completed successfully.

7.4b.1.2 Abnormal Conditions for data endpoints

If the test procedure is being performed on a data IP endpoint and timer Tns-alive expires, depending on the implementation, the test procedure may be repeated. After NS-ALIVE-RETRIES unsuccessful retry attempts, the O&M system and the load sharing function are informed, and an NS-STATUS-Indication is sent to the NS user entity. An NS-STATUS procedure may be initiated towards a signalling IP endpoint. The NS-STATUS includes the two IP endpoints that comprise the NS-VC and a cause code "IP test failed". Further actions of the O&M system is out of the scope of the present document.

When an NS-ALIVE fails for a path, the sending side is allowed to change both the local IP endpoint and the remote IP endpoint.

Traffic may be processed if received on an IP endpoint after an unsuccessful test procedure.

7.5 Procedure for error reporting

The reporting of protocol errors to the remote entity is done by means of the NS-STATUS PDU, as further described in the rest of the present document.

Upon receipt of an NS-STATUS PDU, the O&M system is informed. Further actions of the O&M system are out of the scope of the present document.

7.5.1 Abnormal conditions

If an error is detected in a received NS-STATUS PDU, then the error shall not be reported to the remote NS entity.

7.6 Resource Distribution Procedure

Each NS entity is responsible for determining when to trigger the Resource Distribution Function and to which IP endpoint resource distribution can occur. This sub-clause only describes the mechanism for informing the peer NS entity the IP endpoint at which NS user data for an MS or for an MBMS session is to be received. Recommended usage of the Resource Distribution Function for an IP sub-network when Resource Distribution is to be performed on a data flow concerning an MS can be found in annex B.

The resource distribution function at an NSE may choose to change the IP endpoint at which it receives NS user data for an MS or MBMS session. To achieve this, the NS user entity shall notify the load sharing function and subsequently the NS entity to send an NS-UNITDATA with the R-bit field set to "1" in the *NS SDU Control Bits* IE from the new IP endpoint. Note: the BSS may set the R-bit field to "1" in the initial PDU for NS user data for an MS. If an NSE has no NS SDU to send for some period of time, or if Resource Distribution is to be performed on a data flow concerning an MBMS session, then the NSE shall send an NS-UNITDATA PDU containing a BSSGP DL-UNITDATA (BSSGP UL-UNITDATA) or, in case of an MBMS session, a BSSGP UL-MBMS-UNITDATA with an LLC-PDU Length Indicator set to 0 (see 3GPP TS 48.018).

When the NSE receives an NS-UNITDATA PDU with R-bit field set to "1" in the *NS SDU Control Bits* IE, it shall inform the higher layers to change the destination IP endpoint for that MS or MBMS session. All subsequent NS SDUs for the same MS or MBMS session shall be sent to this destination. The receiving NSE may optionally send an NS-UNITDATA PDU with the C-bit field set to "1" in the *NS SDU Control Bits* IE to confirm acknowledgement of the request to change the IP endpoint.

The NSE initiating the Resource Distribution Function for an MS shall not set the R-bit field to "1" in an NS-UNITDATA PDU for this MS once it has received an NS-UNITDATA PDU for the same MS, irrespective of the C-bit field value, at the requested IP endpoint.

7.6.1 Abnormal Conditions

If a peer NSE continues to send NS-UNITDATA for a given MS or MBMS session to an IP endpoint after receipt of a NS-UNITDATA with R-bit that directs traffic to a different IP endpoint, then the action taken by the NSE is implementation dependent.. The BSS maintains the MS context for a subscriber for a finite period of time. When uplink data is received for a mobile and the BSS has no MS context with the SGSN preferred IP endpoint then the BSS may choose to send the NS user data on one of the IP endpoints determined by the load sharing function. However, the SGSN maintains the MS context for as long as it has location information for the MS on cell level.

8 General protocol error handling

This sub-clause is not applicable to the Sub-Network Service protocol.

The following "General case" sub-clause applies unless otherwise stated in the "Special cases" sub-clause.

8.1 General case

This sub-clause specifies procedures for the handling of unknown, unforeseen, and erroneous protocol data by the receiving entity. These procedures are called "error handling procedures", but in addition to providing recovery mechanisms for error situations they define a compatibility mechanism for future extensions of the protocol.

Most error handling procedures are mandatory for a BSS and SGSN.

Detailed error handling procedures are implementation dependent and may vary from PLMN to PLMN. However, when extensions of this protocol are developed, networks shall be assumed to have the error handling that is indicated in this sub-clause as mandatory ("shall") and that is indicated as strongly recommended ("should").

In this sub-clause the following terminology is used:

- **Syntactical error:** an IE is defined to be syntactically incorrect in a PDU if it contains at least one value defined as "reserved" or "reserved for future use", or if its value part violates coding rules specified in the relevant protocol specification, e.g. a too short IE (the length indicator shall be used to determine the boundary of the IE). However, it is not a syntactical error that an IE specifies in its length indicator a greater length than defined in the relevant protocol specification; and

- **Semantic error:** a PDU is defined to have semantically incorrect contents if it contains information which, possibly dependent on the state of the receiver, is in contradiction to the resources of the receiver and/or to the procedural part of the relevant protocol specification.

To allow for the introduction of new functions the following rules shall be used to determine the actions of a receiving entity when it receives a PDU, part or all of which it is unable to understand. As the recipient is unable to tell the difference between a new, previously unspecified coding and an erroneous coding, the recipient also uses the same rules for error handling.

The robustness of a recipient in handling erroneous PDUs does not relax the requirement that the transmitter shall obey the present document. However, it is intended that functionality can be gradually added to an entity, and no obstacle to intermediate phase equipment is intended.

8.1.1 Presence requirements of Information Elements

There are three different presence requirements (M, C, or O) for an IE within a given PDU:

- **M ("Mandatory")** means that the IE shall be included by the sending side, and that the receiver diagnoses a "missing essential IE" error when detecting that the IE is not present.

- **C ("Conditional")** means:

- that inclusion of the IE by the sender depends on conditions specified in the relevant protocol specification;
- that there are conditions for the receiver to expect that the IE is present and/or conditions for the receiver to expect that the IE is not present; these conditions depend only on the PDU itself, and not on the state in which the PDU was received; they are known as static conditions;
- that the receiver detecting that the IE is not present when sufficient static conditions are fulfilled for its presence, shall diagnose a "missing essential IE" error;
- that the receiver detecting that the IE is present when sufficient static conditions are fulfilled for its non-presence, shall treat the IE as an optional one, see below.

- **O ("Optional")** means that the receiver shall never diagnose a "missing essential IE" error or shall never diagnose an error because it detects that the IE is present or that the IE is not present. There may however be conditions depending on the states, resources, etc. of the receiver to diagnose other errors.

In addition, the following definitions apply:

- **Essential Elements:** These are the conditional (C) elements when the condition for their reception is fulfilled, plus the mandatory (M) elements. Any exception to this rule is explicitly stated in the relevant protocol specification.
- **Non-Essential Elements:** Non-essential elements are all the information elements that are not defined as essential.

8.1.2 Erroneous events

The following events shall be regarded as errors by the recipient and shall be treated as specified below. Certain types of error shall be reported to the sending side, in that case the erroneous PDU and the error cause shall be returned to the sending side by means of the appropriate error reporting PDU. The following rules shall be applied in order of precedence:

1) a PDU whose type is non-existent or unrecognisable: the error shall not be reported, the PDU shall be ignored;
2) a PDU not consistent with the recipient's state: the error shall be reported with cause "PDU not compatible with the protocol state", the PDU shall be ignored;
3) a PDU sent in the wrong direction: the error shall be reported with cause "Protocol error - unspecified", the PDU shall be ignored;
4) a missing essential information element: the error shall be reported with cause "Missing essential IE", the PDU shall be ignored;
5) syntactical error in an essential IE: the error shall be reported with cause "Invalid essential IE", the PDU shall be ignored.

8.1.3 Non-erroneous events

The following events shall not be regarded as errors by the recipient:

1) spare bits with an unexpected value in any information element;
2) the use of additional octets in any information element with a length indicator, that is: when the indicated length is greater than defined in the relevant protocol specification (the length indicatorl shall be used to determine the boundary of the IE);
3) a missing non-essential information element;
4) an unknown information element identifier;
5) any unexpected information element; and
6) a syntactical error in any non-essential information element.

When the recipient detects one or more of these events the receiving entity shall ignore the information that it is unable to understand and treat the PDU on the basis of the information that remains.

Additionally, when more information elements of a particular type are received than are expected, the last one(s) shall be ignored.

If, because information was ignored, the rest of the PDU can no longer be handled then the receiving entity shall report the error to the sending side by means of the appropriate error reporting PDU including the incorrect PDU received and the cause "semantically incorrect PDU".

8.1.4 Other events

The following events should be treated on a case by case basis and the outcome may depend upon the capabilities of the recipient.

1) The recipient may accept PDUs that contain information elements that do not appear to be in the correct sequence. Elements that occur more than once in a PDU shall be assumed to have been transmitted in the correct order. Recipients that do not accept out of sequence information elements shall regard the PDU as containing unexpected and/or missing information elements and follow the procedures defined in the rest of this "General case" sub-clause.

2) When any IE with semantically incorrect contents is received, the receiving entity shall react according to the relevant protocol specification. If however no such reactions are specified, the receiving entity shall ignore that IE and treat the rest of the PDU. If, because this IE was ignored, the rest of the PDU can no longer be handled then the receiving entity shall report the error to the sending side by means of the appropriate error reporting PDU including the incorrect PDU received and the cause "semantically incorrect PDU".

8.2 Special cases

In case of conflict between this sub-clause and the above "General case" sub-clause, this sub-clause takes precedence.

In case of conflict between this sub-clause and the specific "Abnormal conditions" sub-clauses in sub-clause "Network Service Control protocol", the "Abnormal conditions" sub-clauses take precedence over this "Special cases" sub-clause.

8.2.1 Deviations from the "General case" sub-clause

The Cause information element (see sub-clauses "General PDU definitions and contents" and "General information elements coding") shall be considered as a non-essential information element even when mandatory in a PDU.

8.2.2 Error reporting

The NS-STATUS PDU shall be used to report error to the remote NS entity, see sub-clause "Procedure for error reporting". The NS-STATUS PDU shall never be used to report an error detected in a received NS-STATUS PDU.

9 General PDU definitions and contents

This sub-clause is not applicable to the Sub-Network Service protocol.

9.1 General structure of a PDU

This sub-clause defines the general structure of the PDUs on the Gb interface.

The general PDU structure is composed of:

a) a PDU type information element; and

b) other information elements, as required.

The PDU type IE occupies the first octet position in the PDU.

This general structure and the numbering convention used on the Gb interface are illustrated in figure 9.1.1. The bits are grouped into octets. The bits of an octet are shown horizontally and are numbered from 1 to 8. Multiple octets are shown vertically and are numbered from 1 to n.

The octets shall be transmitted by increasing order of octet number. Within each octet, the bits shall be transmitted by increasing order of bit number i.e. bit 1 of octet 1 shall be transmitted first, bit 8 of octet n shall be transmitted last.

	8	7	6	5	4	3	2	1
octet 1	PDU type							
octets 2, 3, ...n	other information elements							

Figure 9.1.1: General PDU structure and numbering convention

Each PDU definition includes a table listing the information elements (IEs) known in the PDU and the order of their appearance in the PDU. Unless specified otherwise in the PDU descriptions, a particular information element shall not be present more than once in a given PDU. All information elements that may be repeated are explicitly indicated.

For each information element the table indicates:

a) The name of the information element (which may give an idea of the semantics of the element).

b) Possibly a reference to another GSM Technical Specification where the information element is described.

c) The presence requirement indication (M, C, or O) for the IE as defined in sub-clause "General protocol error handling".

d) The format (T, L, V) of the information element. See further description of the type (T), length (L) and V (value) fields in sub-clause "General structure of the information elements".

e) The length of the information element (or permissible range of lengths), in octets, in the PDU, where "?" means that the maximum length of the IE is only constrained by the lower layer protocol. This indication is non-normative. The indicated length includes all the T, L, V fields present in the IE.

f) Sub-clauses specifying, where appropriate, conditions for IEs with presence requirement C or O in the relevant PDU which together with other conditions specified in 3GPP TS 48.016 define when the information elements shall be included or not, what non-presence of such IEs means, and - for IEs with presence requirement C - the static conditions for presence and/or non-presence of the IEs, see sub-clause "General protocol error handling".

9.2 Network Service Control PDUs

The Network Service Control PDUs are also referred to as NS PDUs in the rest of the present document.

9.2.1 NS-ALIVE

This PDU is used to test an NS-VC.

PDU type: NS-ALIVE

Direction: BSS to SGSN, SGSN to BSS

Table 9.2.1.1: NS-ALIVE PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1

9.2.2 NS-ALIVE-ACK

This PDU acknowledges a received NS-ALIVE PDU and is sent on the NS-VC where the NS-ALIVE PDU was received.

PDU type: NS-ALIVE-ACK

Direction: SGSN to BSS, BSS to SGSN

Table 9.2.2.1: NS-ALIVE-ACK PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1

9.2.3 NS-BLOCK

This PDU indicates that an NS-VC shall be blocked at the recipient entity.

PDU type: NS-BLOCK

Direction: BSS to SGSN, SGSN to BSS

Table 9.2.3.1: NS-BLOCK PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
Cause	10.3.2	M	TLV	3
NS-VCI	10.3.5	M	TLV	4

9.2.4 NS-BLOCK-ACK

This PDU acknowledges that an NS-VC has been blocked for use.

PDU type: NS-BLOCK-ACK

Direction: SGSN to BSS, BSS to SGSN

Table 9.2.4.1: NS-BLOCK-ACK PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
NS-VCI	10.3.5	M	TLV	4

9.2.5 NS-RESET

This PDU indicates that the NS peer entity is trying to reset one NS-VC.

PDU type: NS-RESET

Direction: BSS to SGSN, SGSN to BSS

Table 9.2.5.1: NS-RESET PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
Cause	10.3.2	M	TLV	3
NS-VCI	10.3.5	M	TLV	4
NSEI	10.3.6	M	TLV	4

Typical cause values are: O&M intervention, Equipment failure.

9.2.6 NS-RESET-ACK

This PDU acknowledges the reset of the indicated NS-VC.

PDU type: NS-RESET-ACK

Direction: BSS to SGSN, SGSN to BSS

Table 9.2.6.1: NS-RESET-ACK PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
NS-VCI	10.3.5	M	TLV	4
NSEI	10.3.6	M	TLV	4

9.2.7 NS-STATUS

This PDU is used to report error conditions.

PDU type: NS-STATUS

Direction: SGSN to BSS, BSS to SGSN

Table 9.2.7.1: NS-STATUS PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
Cause	10.3.2	M	TLV	3
NS-VCI	10.3.5	C	TLV	4
NS PDU	10.3.3	C	TLV	3-?
BVCI	10.3.1	C	TLV	4
List of IP4 Elements	10.3.2c	C	TLV	10-?
List of IP6 Elements	10.3.2d	C	TLV	22-?

9.2.7.1 Static conditions for NS-VCI

The *NS-VCI* IE shall be included when the *Cause* IE is set to one of the following values:

a) "NS-VC blocked";

b) "NS-VC unknown";

and shall not be included otherwise.

9.2.7.2 Static conditions for NS PDU

The *NS PDU* IE shall be included if the NS-STATUS message is sent in response to a received NS PDU within which an error was detected i.e. when the *Cause* IE is set to one of the following values:

a) "Semantically incorrect PDU";

b) "PDU not compatible with the protocol state";

c) "Protocol error - unspecified";

d) "Invalid essential IE";

e) "Missing essential IE";

and shall not be included otherwise.

This is the whole PDU received with error. This PDU may be truncated if it exceeds the information carrying capacity of the NS.

9.2.7.3 Static conditions for BVCI

The *BVCI* IE shall be included when the *Cause* IE is set to one of the following values:

a) "BVCI unknown on that NSE";

and shall not be included otherwise.

9.2.7.4 Static conditions for List of IP4 Elements

The *List of IP4 Elements* IE shall be included when the *Cause* IE is set to one of the following values:

a) " IP test failed";

and the IP endpoints of the NS-VC that failed are IPv4 endpoints. The *List of IP4 Elements* IE shall be the only conditional IE sent in a NS-STATUS PDU.

The *List of IP4 Elements* IE shall not be included otherwise.

9.2.7.5 Static conditions for List of IP6 Elements

The *List of IP6 Elements* IE shall be included when the *Cause* IE is set to one of the following values:

a) " IP test failed";

and the IP endpoints of the NS-VC that failed are IPv6 endpoints. The *List of IP6 Elements* IE shall be the only conditional IE sent in a NS-STATUS PDU.

The *List of IP6 Elements* IE shall not be included otherwise.

9.2.8 NS-UNBLOCK

This PDU indicates that an NS-VC shall be unblocked at the recipient entity.

PDU type: NS-UNBLOCK

Direction: BSS to SGSN, SGSN to BSS

Table 9.2.8.1: NS-UNBLOCK PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1

9.2.9 NS-UNBLOCK-ACK

This PDU acknowledges that an NS-VC has been unblocked.

PDU type: NS-UNBLOCK-ACK

Direction: SGSN to BSS, BSS to SGSN

Table 9.2.9.1: NS-UNBLOCK-ACK PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1

9.2.10 NS-UNITDATA

This PDU transfers one NS SDU between the BSS and SGSN.

PDU type: NS-UNITDATA

Direction: BSS to SGSN, SGSN to BSS

Table 9.2.10.1: NS-UNITDATA PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
NS SDU Control Bits	10.3.9	M	V	1
BVCI	10.3.1	M	V	2
NS SDU	10.3.4	M	V	1-?

The length of the *NS SDU* information element shall be derived by the Network Service Control entity from the length of the complete NS-UNITDATA PDU provided by the Sub-Network Service entity to the Network Service Control entity.

9.3 Sub-Network Service Control PDUs

The Sub-Network Service Control PDUs are also referred to as SNS PDUs in the rest of the present document. The Sub-Network Service Control PDUs are only used in an IP sub-network.

9.3.1 SNS-ACK

The SNS-ACK PDU is used to acknowledge the SNS-ADD PDU, the SNS-DELETE PDU, or the SNS-CHANGEWEIGHT PDU.

PDU type: SNS-ACK

Direction: BSS to SGSN, SGSN to BSS

Table 9.3.1.1: SNS-ACK PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
NSEI	10.3.6	M	TLV	4
Transaction ID	10.3.10	M	V	1
Cause	10.3.2	O	TLV	3
IP Address a)	10.3.2b	C	TV	6-18
List of IP4 Elements b)	10.3.2c	C	TLV	10-?
List of IP6 Elements b)	10.3.2d	C	TLV	22-?
a) the IP Address IE shall only be present if the "Cause" value is set to "Unknown IP address". b) one or more of these conditional IEs shall be present if the "Cause" value is set to "Unknown IP endpoint".				

9.3.2 SNS-ADD

The SNS-ADD PDU is used to add additional IP Endpoints.

PDU type: SNS-ADD

Direction: BSS to SGSN, SGSN to BSS

Table 9.3.2.1: SNS-ADD PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
NSEI	10.3.6	M	TLV	4
Transaction ID	10.3.10	M	V	1
List of IP4 Elements a)	10.3.2c	C	TLV	10-?
List of IP6 Elements a)	10.3.2d	C	TLV	22-?
a) one and only one of the conditional IEs shall be present.				

9.3.3 SNS-CHANGEWEIGHT

The SNS-CHANGEWEIGHT PDU is used to change the signalling weight and/or data weight of an IP endpoint.

PDU type: SNS-CHANGEWEIGHT

Direction: BSS to SGSN, SGSN to BSS

Table 9.3.3.1: SNS-CHANGEWEIGHT PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
NSEI	10.3.6	M	TLV	4
Transaction ID	10.3.10	M	V	1
List of IP4 Elements a)	10.3.2c	C	TLV	10-?
List of IP6 Elements a)	10.3.2d	C	TLV	22-?
a) one and only one of the conditional IEs shall be present.				

9.3.4 SNS-CONFIG

The SNS-CONFIG PDU is used to configure a NSE to a peer NSE.

PDU type: SNS-CONFIG

Direction: BSS to SGSN, SGSN to BSS

Table 9.3.4.1: SNS-CONFIG PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
End Flag	10.3.2a	M	V	1
NSEI	10.3.6	M	TLV	4
List of IP4 Elements a)	10.3.2c	C	TLV	10-?
List of IP6 Elements a)	10.3.2d	C	TLV	22-?
a) one and only one of the conditional IEs shall be present.				

9.3.5 SNS-CONFIG-ACK

The SNS-CONFIG-ACK PDU is used to acknowledge an SNS-CONFIG PDU. The SNS-CONFIG-ACK PDU shall be sent to the source IP Endpoint of the corresponding SNS-CONFIG PDU.

PDU type: SNS-CONFIG-ACK

Direction: BSS to SGSN, SGSN to BSS

Table 9.3.5.1: SNS-CONFIG-ACK PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
NSEI	10.3.6	M	TLV	4
Cause	10.3.2	O	TLV	3

9.3.6 SNS-DELETE

The SNS-DELETE PDU is used to delete previously configured IP Endpoints.

PDU type: SNS-DELETE

Direction: BSS to SGSN, SGSN to BSS

Table 9.3.6.1: SNS-DELETE PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
NSEI	10.3.6	M	TLV	4
Transaction ID	10.3.10	M	V	1
IP Address a)	10.3.2b	C	TV	6-18
List of IP4 Elements a)	10.3.2c	C	TLV	10-?
List of IP6 Elements a)	10.3.2d	C	TLV	22-?
a) one and only one of the conditional IEs shall be present.				

9.3.7 SNS-SIZE

The SNS-SIZE PDU is used to indicate to the peer NSE the maximum number of NS-VCs or a change in the NS-VC capacity. The SNS-SIZE PDU is used to signal the restart of a NSE to a peer NSE.

PDU type: SNS-SIZE

Direction: BSS to SGSN

Table 9.3.7.1: SNS-SIZE PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
NSEI	10.3.6	M	TLV	4
Reset Flag		M	TV	2
Maximum Number of NS-VCs	10.3.2e	M	TV	3
Number of IP4 Endpoints a)	10.3.2f	C	TV	3
Number of IP6 Endpoints a)	10.3.2g	C	TV	3
a) At least one of these conditional IEs shall be present.				

9.3.8 SNS-SIZE-ACK

The SNS-SIZE-ACK PDU is used to acknowledge an SNS-SIZE PDU. The SNS-SIZE-ACK PDU shall be sent to the source IP Endpoint of the corresponding SNS-SIZE PDU.

PDU type: SNS-SIZE-ACK

Direction: SGSN to BSS

Table 9.3.8.1: SNS-SIZE-ACK PDU contents

Information element	Reference	Presence	Format	Length
PDU type	10.3.7	M	V	1
NSEI	10.3.6	M	TLV	4
Cause	10.3.2	O	TLV	3

10 General information elements coding

This sub-clause is not applicable to the Sub-Network Service protocol.

10.1 General structure of the information elements

The general information element structure is composed of (see figure 10.1.1):

a) an Information Element Identifier (also referred to as the T field);

b) a length indicator (also referred to as the L field);

c) the information element value (also referred to as the V field).

Information elements have the TLV, the TV or the V format, as specified in the relevant protocol specification. The format of any given information element may depend on the context e.g. on the message type.

	8	7	6	5	4	3	2	1
octet 1	Information Element Identifier (IEI)							
octets 2, 2a	length indicator							
octet 3 ... octet ... n	information element value							

Figure 10.1.1: Information element structure, TLV format

	8	7	6	5	4	3	2	1
octet 1	information element value							
...								
octet ... n								

Figure 10.1.2: Information element structure, V format

When a field extends over more than one octet, the order of bit values progressively decreases as the octet number increases. The least significant bit of the field is represented by the lowest numbered bit of the highest numbered octet of the field.

10.1.1 Information Element Identifier

The first octet of an information element having the TLV format contains the IEI of the information element. If this octet does not correspond to an IEI known in the PDU, the receiver shall assume that the next octet is the first octet of the length indicator field and shall interpret it as described in the "Length indicator" sub-clause.

This rule allows the receiver to skip unknown information elements and to analyse any following information elements.

10.1.2 Length indicator

The length indicator shall be included in all information elements having the TLV format.

Information elements may be variable in length. The length indicator is one or two octet long, the second octet may be absent. This field consists of the field extension bit, 0/1 ext, and the length of the value field which follows, expressed in octets. The field extension bit enables extension of the length indicator to two octets.

Bit 8 of the first octet is reserved for the field extension bit. If the field extension bit is set to 0 (zero), then the second octet of the length indicator is present. If the field extension bit is set to 1 (one), then the first octet is the final octet of the length indicator.

The length of the value field of the IE occupies the rest of the bits in the length indicator.

	8	7	6	5	4	3	2	1
octet 2	0/1 ext	length						
octet 2a	length							

Figure 10.1.2.1: Length indicator structure

The BSS or SGSN shall not consider the presence of octet 2a in a received IE as an error when the IE is short enough for the length to be coded in octet 2 only.

10.2 Information element description

The descriptions of the information elements are organized in alphabetical order of the IE name. Each IE is described in one sub-clause.

A figure of the sub-clause defines the structure of the IE indicating:

- the position of the IEI, when present;
- the fields the IE value part is composed of;
- the position of the length indicator, when present;
- possibly octet numbers of the octets that compose the IE.

Finally, the sub-clause may contain figures defining the structure and value range of the fields that compose the IE value part.

Where the description of information elements in the present document contains bits defined to be "spare bits", these bits shall set to zero by the sending side, and their value shall be ignored by the receiving side.

The term "default" may be used, implying that the value defined shall be used in the absence of any assignment, or that this value allows negotiation of alternative values in between the two peer entities.

10.3 Information elements

The IEI values are indicated in table 10.3.1:

Table 10.3.1: IEI coding

IEI coding								Information element name
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	0	Cause
0	0	0	0	0	0	0	1	NS-VCI
0	0	0	0	0	0	1	0	NS PDU
0	0	0	0	0	0	1	1	BVCI
0	0	0	0	0	1	0	0	NSEI
0	0	0	0	0	1	0	1	List of IP4 Elements
0	0	0	0	0	1	1	0	List of IP6 Elements
0	0	0	0	0	1	1	1	Maximum Number of NS-VCs
0	0	0	0	1	0	0	0	Number of IP4 Endpoints
0	0	0	0	1	0	0	1	Number of IP6 Endpoints
0	0	0	0	1	0	1	0	Reset Flag
0	0	0	0	1	0	1	1	IP Address
other values								reserved for future use

10.3.1 BVCI

This IE is used for multiplexing BVCs on NS-VCs.

	8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
octet 1	IEI							
octets 2, 2a	length indicator							
octet 3	most significant octet of BVCI							
octet 4	least significant octet of BVCI							

Figure 10.3.1.1: BVCI information element

10.3.2 Cause

This IE may be used to indicate to the peer NS entity the reason which triggered a procedure, or the reason of an abnormal condition.

	8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
octet 1	IEI							
octets 2, 2a	length indicator							
octet 3	cause value							

Figure 10.3.2.1: Cause information element

The cause values are indicated in table 10.3.2.1:

Table 10.3.2.1: Cause values

Cause value coding								Cause name
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	Transit network failure
0	0	0	0	0	0	0	1	O&M intervention
0	0	0	0	0	0	1	0	Equipment failure
0	0	0	0	0	0	1	1	NS-VC blocked
0	0	0	0	0	1	0	0	NS-VC unknown
0	0	0	0	0	1	0	1	BVCI unknown on that NSE
0	0	0	0	1	0	0	0	Semantically incorrect PDU
0	0	0	0	1	0	1	0	PDU not compatible with the protocol state
0	0	0	0	1	0	1	1	Protocol error - unspecified
0	0	0	0	1	1	0	0	Invalid essential IE
0	0	0	0	1	1	0	1	Missing essential IE
0	0	0	0	1	1	1	0	Invalid number of IP4 Endpoints
0	0	0	0	1	1	1	1	Invalid number of IP6 Endpoints
0	0	0	1	0	0	0	0	Invalid number of NS-VCs
0	0	0	1	0	0	0	1	Invalid weights
0	0	0	1	0	0	1	0	Unknown IP endpoint
0	0	0	1	0	0	1	1	Unknown IP address
0	0	0	1	0	1	0	0	IP test failed
other values								reserved for future use

10.3.2a End Flag

This IE is used to indicate last SNS-CONFIG PDU to be sent to the peer NS entity. All unused bits are spare.

	8	7	6	5	4	3	2	1
octet 1	spare							E-bit

Figure 10.3.2a.1: End Flag information element

The "E-bit" is coded as shown below:

0 Additional PDUs will be sent.

1 Last PDU sent.

10.3.2b IP Address

This IE identifies an IP address.

	8	7	6	5	4	3	2	1
Octet 1	IEI							
Octet 2	Address Type							
Octets 3 -n	Address value							

Figure 10.3.2b.1: IP Address information element

Where "n" is 6 if the Address Type is IPv4 and "n" is 18 if the Address Type is IPv6.

The "Address Type" is coded as shown in table 10.3.2b.1.

Table 10.3.2b.1: "Address Type" coding

coding	Address Type
0	Reserved
1	IPv4
2	IPv6
Reserved	All values not explicitly shown are reserved for future use.

10.3.2c List of IP4 Elements

This IE identifies a list of IPv4 elements.

	8	7	6	5	4	3	2	1
octet 1	IEI							
octet 2, 2a	Length Indicator							
octets 3-10	IP4 Element 1							
octets … - (2+8n)	IP4 Element n							

Figure 10.3.2c.1: List of IP4 Elements information element

The length depends on the number of IP4 Elements: n. The coding of an IP4 Element is:

	8	7	6	5	4	3	2	1
octet (x+1)-(x+4)	IPv4 Address							
octet (x+5)-(x+6)	UDP Port Value							
octet (x+7)	Signalling Weight							
octet (x+8)	Data Weight							

where x = 8i - 6 ($1 \leq i \leq n$).

10.3.2d List of IP6 Elements

This IE identifies a list of IPv6 elements.

	8	7	6	5	4	3	2	1
octet 1	IEI							
octet 2, 2a	Length Indicator							
octets 3- 22	IP6 Element 1							
octets … - (2+20n)	IP6 Element n							

Figure 10.3.2d.1: List of IP6 Elements information element

The length depends on the number of IP6 Elements: n . The coding of an IP6 Element is:

	8	7	6	5	4	3	2	1
octet (x+1)-(x+16)	IPv6 Address							
octet (x+17)-(x+18)	UDP Port Value							
octet (x+19)	Signalling Weight							
octet (x+20)	Data Weight							

where x = 20i - 18 ($1 \leq i \leq n$).

10.3.2e Maximum Number of NS-VCs

This IE identifies the maximum number of NS-VCs.

	8	7	6	5	4	3	2	1
octet 1	IEI							
octet 2 **octet 3**	most significant octet of Maximum Number of NS-VCs least significant octet of Maximum Number of NS-VCs							

Figure 10.3.2e.1: Maximum Number of NS-VCs information element

10.3.2f Number of IP4 Endpoints

This IE identifies the number of IPv4 endpoints.

	8	7	6	5	4	3	2	1
octet 1	IEI							
octet 2 **octet 3**	most significant octet of Number of IP4 Endpoints least significant octet of Number of IP4 Endpoints							

Figure 10.3.2f.1: Number of IP4 Endpoints information element

10.3.2g Number of IP6 Endpoints

This IE identifies the number of IPv6 endpoints.

	8	7	6	5	4	3	2	1
octet 1	IEI							
octet 2 **octet 3**	most significant octet of Number of IP6 Endpoints least significant octet of Number of IP6 Endpoints							

Figure 10.3.2g.1: Number of IP6 Endpoints information element

10.3.3 NS PDU

This IE is included in the NS-STATUS PDU sent in answer to an erroneous NS PDU. This IE contains the erroneous PDU received. The erroneous PDU may be truncated in order to fit in the maximum size of the NS-STATUS PDU.

	8	7	6	5	4	3	2	1
octet 1	IEI							
octets 2, 2a	length indicator							
octet 3	NS PDU							
...								
octet n								

Figure 10.3.3.1: NS PDU information element

10.3.4 NS SDU

This IE contains one and only one NS SDU transmitted across the Gb interface.

	8	7	6	5	4	3	2	1
octet 1	NS SDU							
...								
octet n								

Figure 10.3.4.1: NS SDU information element

In this "NS SDU" information element, bit i of octet j is equal to bit i of octet j of the NS SDU, as defined in the NS user protocol specification.

10.3.5 NS-VCI

This IE unambiguously identifies one NS-VC amongst all the NS-VCs used between one SGSN and the connected BSSs.

	8	7	6	5	4	3	2	1
octet 1	IEI							
octets 2, 2a	length indicator							
octet 3	most significant octet of NS-VCI							
octet 4	least significant octet of NS-VCI							

Figure 10.3.5.1: NS-VCI information element

10.3.6 NSEI

This IE unambiguously identifies one NSE.

	8	7	6	5	4	3	2	1
octet 1	IEI							
octets 2, 2a	length indicator							
octet 3	most significant octet of NSEI							
octet 4	least significant octet of NSEI							

Figure 10.3.6.1: NSEI information element

10.3.7 PDU type

Table 10.3.7.1: PDU type coding

PDU type coding								PDU name
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	0	NS-UNITDATA
0	0	0	0	0	0	1	0	NS-RESET
0	0	0	0	0	0	1	1	NS-RESET-ACK
0	0	0	0	0	1	0	0	NS-BLOCK
0	0	0	0	0	1	0	1	NS-BLOCK-ACK
0	0	0	0	0	1	1	0	NS-UNBLOCK
0	0	0	0	0	1	1	1	NS-UNBLOCK-ACK
0	0	0	0	1	0	0	0	NS-STATUS
0	0	0	0	1	0	1	0	NS-ALIVE
0	0	0	0	1	0	1	1	NS-ALIVE-ACK
0	0	0	0	1	1	0	0	SNS-ACK
0	0	0	0	1	1	0	1	SNS-ADD
0	0	0	0	1	1	1	0	SNS-CHANGEWEIGHT
0	0	0	0	1	1	1	1	SNS-CONFIG
0	0	0	1	0	0	0	0	SNS-CONFIG-ACK
0	0	0	1	0	0	0	1	SNS-DELETE
0	0	0	1	0	0	1	0	SNS-SIZE
0	0	0	1	0	0	1	1	SNS-SIZE-ACK
other values								reserved for future use

10.3.7a Reset Flag

This IE is used to indicate if the peer NS entity shall reset all configuration information. All unused bits are spare.

	8	7	6	5	4	3	2	1
octet 1	IEI							
octet 2	Spare							Reset-bit

Figure 10.3.7a.1: Reset Flag information element

The "Reset-bit" is coded as shown below:

0 Do not reset.

1 Reset.

10.3.8 (void)

10.3.9 NS SDU Control Bits

This IE is used to indicate additional information about the NS-SDU to the user of the NS entity. All unused bits are spare.

	8	7	6	5	4	3	2	1
octet 1	spare						C-bit	R-bit

Figure 10.3.9.1: NS SDU Control Bits information element

The "R-bit" is coded as shown below:

0 No request for change flow;

1 Request change flow.

The "C-bit" is coded as shown below:

0 No confirmation for change flow;

1 Confirm change flow.

10.3.10 Transaction ID

This IE provides an identifier for SNS PDUs.

	8	7	6	5	4	3	2	1
octet 1	Value							

Figure 10.3.10.1: Transaction ID information element

11 List of system variables

Table 11.1: System timers

Timer name	Timer value	Notes	Relation to other timers
Tns-block	1s to 120s	Guards the blocking and unblocking procedures	none
Tns-reset	1s to 120s	Guards the reset procedure	none
Tns-test	1s to 60s	Periodicity of the NS-VC test procedure	none
Tns-alive	3s	Guards the NS-VC test procedure	none
Tsns-prov	1s-10s	Guards the SNS procedures	none

Table 11.2: System counters

Counter name	Value	Notes
NS-BLOCK-RETRIES	3	recommended value
NS-UNBLOCK-RETRIES	3	recommended value
NS-ALIVE-RETRIES	10	recommended value
SNS-ADD-RETRIES	3	recommended value
SNS-CONFIG-RETRIES	3	recommended value
SNS-CHANGEWEIGHT-RETRIES	3	recommended value
SNS-DELETE-RETRIES	3	recommended value
SNS-SIZE-RETRIES	3	recommended value

Annex A (informative): Recommended usage of BVCI and NSEI

This annex recommends a way to use BVCIs and NSEIs, avoiding huge and unflexible configuration data at the SGSN. This annex uses concepts defined in 3GPP TS 48.018.

The key points are:

- A BVCI needs not to be unique within an SGSN, a BVCI is unique within an NS Entity. BVCI together with NSEI uniquely identify a BVC within an SGSN (the global identifier within an SGSN is BVCI+NSEI).

- BVCIs corresponding to PTP functional entities need not to be statically configured at the SGSN side: no fixed, permanent relationship is required in the SGSN between PTP BVCIs and NS-VCs.

With the NSEI, the SGSN needs not to be updated when a new cell (BVCI) is added to a BSS (NSEI). The pre-configuration of a cell in the SGSN and the constraint in the number of BVCs in an SGSN are not needed:

- The SGSN keeps detailed MM information about an MS while the MS is in the READY state, i.e. the SGSN knows the BVCI and NSEI which can be used to contact the MS for downlink transmission. The BVCI and NSEI are passed from NS to BSSGP and from BSSGP to the upper layers as a primitive parameter in every uplink packet received by the SGSN. Subsequent downlink LLC frames to this MS shall be transmitted by the SGSN over the BVC identified by this BVCI+NSEI.

- An SGSN in STANDBY state will page an MS before sending downlink traffic. The MS will respond with an LLC packet that will put the MM context in READY state and will deliver the BVCI and NSEI to the user of BSSGP.

For paging purposes, the SGSN only needs to know the correspondence between each Routeing Area and one or more NSEI(s) where to send the corresponding paging messages. Paging messages for a mobile in STANDBY state shall always be sent over BVCI=0 of an NSEI and for a mobile in READY state the circuit page is sent over the PTP BVC identified by the BVCI+NSEI. There may be NSEI(s) where BVCI=0 is not used.

Annex B (informative): Recommended usage of Resource Distribution for IP

This annex recommends a way to support resource distribution over the Gb in an IP sub-network. Resource distribution provides a means to control the IP endpoint at which the NS user traffic for a mobile is received.

Some examples of resource distribution over the Gb:

Example 1: Both NS entities trigger resource distribution (refer to figure B.1).

The BSS receives an uplink LLC PDU from the mobile and creates a mobile context. Now the BSS selects the source IP/UDP$_1$ endpoint (internal implementation dependent) and a destination IP/UDP$_3$ endpoint (IP load sharing dependent) on which to send NS SDUs associated with the mobile.

The BSS sends the uplink NS-UNITDATA (with R-bit set and the LSP corresponding to the IP endpoints selected) to the SGSN from IP/UDP$_1$ to IP/UDP$_3$. On receipt of uplink NS-UNITDATA for the mobile the SGSN may also choose to change the IP endpoint at which it wishes to receive uplink NS-UNITDATA for the mobile to IP/UDP$_4$. The SGSN responds by sending a downlink NS-UNITDATA with R-bit and C-bit set to 1 from the IP/UDP$_4$ at to IP/UDP$_1$.

Subsequent uplink and downlink NS-UNITDATA for the mobile shall follow the dotted path (IP/UDP$_1$ and IP/UDP$_4$) through the IP sub-network.

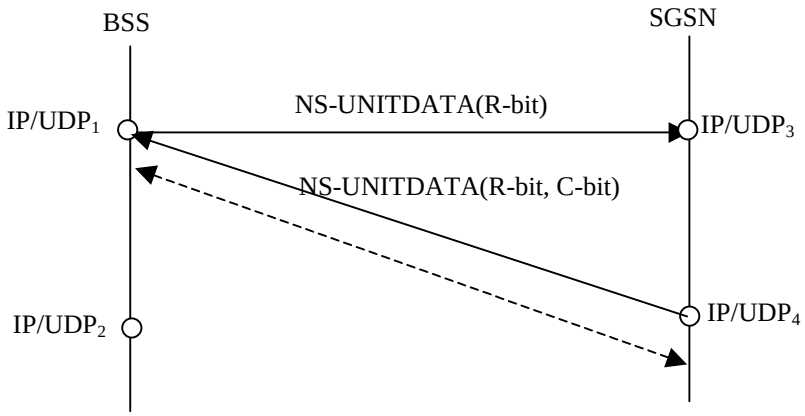


Figure B.1: Example 1 of both NS entities requesting change flow

Example 2: Only one NS entity triggers resource distribution (refer to figure B.2).

The BSS sends an uplink NS-UNITDATA with R-bit set from IP/UDP$_1$ to IP/UDP$_3$ at the SGSN. The SGSN may choose not to trigger resource distribution, but the SGSN confirms receipt of the "request change flow" by sending the in the next downlink NS-UNITDATA with C-bit set to IP/UDP$_1$.

Subsequent uplink data transfer for the mobile will follow the dotted paths from IP/UDP$_1$ to IP/UDP$_3$ and downlink data transfer from IP/UDP$_4$ to IP/UDP$_1$.

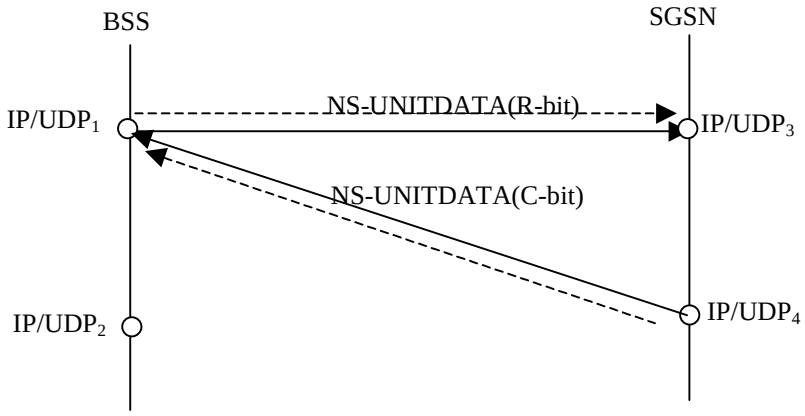


Figure B.2: Example 2 of only one NS entity requesting change flow

Example 3: NS entity triggering resource distribution without data (refer to figure B.3).

The SGSN may wish to receive uplink data for a mobile at IP/UDP$_4$ and not IP/UDP$_3$. The SGSN may not have downlink data, in which case the SGSN may send a downlink NS-UNITDATA (with R-bit set) containing a BSSGP DL-UNITDATA with an LLC PDU of length 0.

Subsequent uplink data transfer for the mobile will follow the dotted path from IP/UDP$_1$ to IP/UDP$_4$ through the IP sub-network.

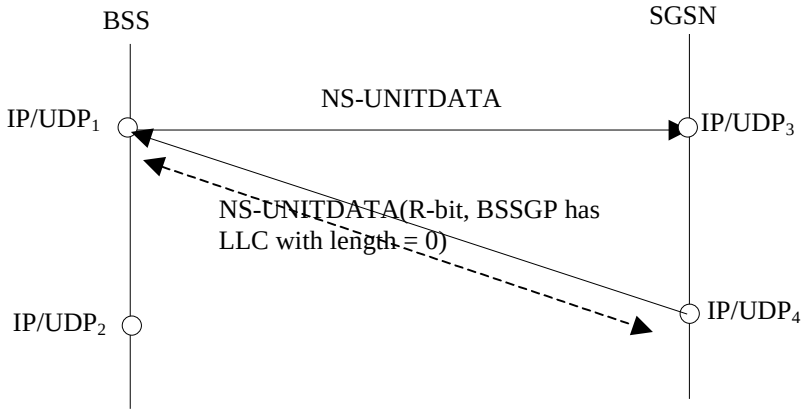


Figure B.3: Example 3 of NS entity requesting change flow without data

Example 4: NS entities without any resource distribution function (refer to figure B.4).

The BSS and SGSN may not care which IP endpoint data arrives at as long as the requirements for the load sharing function are met.

In this case the paths taken by the uplink and downlink data are independent.

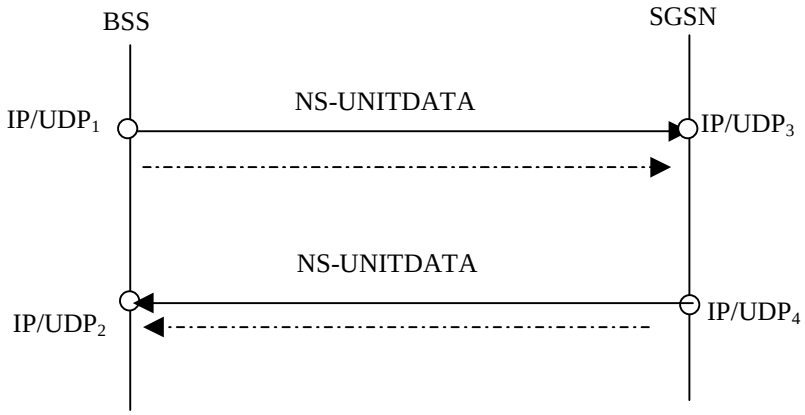


Figure B.4: Example 4 of NS entity not requesting change flow

Annex C (informative): Change History

Meeting / Date	Doc	CR	Rev	Subject/Comment	New version
January 2016	-	-	-	Creation of Rel-13 version based on version 12.0.0	13.0.0

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2017-03	RP-75	-	-	-	-	Version for Release 14 (frozen at TSG-75)	14.0.0
2018-06	RP-80	-	-	-	-	Update to Rel-15 version (MCC)	15.0.0
2020-07	RP-88e	-	-	-	-	Upgrade to Rel-16 version without technical change	16.0.0
2022-03	RP-95e	-	-	-	-	Upgrade to Rel-17 version without technical change	17.0.0
2024-03	RP-103	-	-	-	-	Upgrade to Rel-18 version without technical change	18.0.0

History

Document history		
V18.0.0	May 2024	Publication