Generic IP Connectivity for PSTN / ISDN Services between Next Generation Networks
NOTICE OF COPYRIGHT AND LIABILITY

Copyright

All right, title and interest in this document are owned by Ofcom and/or the contributors to the
document unless otherwise indicated (where copyright be owned or shared with a third party). Such
title and interest is protected by United Kingdom copyright laws and international treaty provisions.

The contents of the document are believed to be accurate at the time of publishing, but no
representation or warranty is given as to their accuracy, completeness or correctness. You may freely
download, copy, store or distribute this document provided it is not modified in any way and it includes
this copyright and liability statement.

You may not modify the contents of this document. You may produce a derived copyright work based
on this document provided that you clearly indicate that it was created by yourself and that it was
derived from this document and provided further that you ensure that any risk of confusion with this
document is avoided.

Liability

Whilst every care has been taken in the preparation and publication of this document, NICC, nor any
committee acting on behalf of NICC, nor any member of any of those committees, nor the companies
they represent, nor any person contributing to the contents of this document (together the “Generators”)
accepts liability for any loss, which may arise from reliance on the information contained in this
document or any errors or omissions, typographical or otherwise in the contents.

Nothing in this document constitutes advice. Nor does the transmission, downloading or sending of this
document create any contractual relationship. In particular no licence is granted under any intellectual
property right (including trade and service mark rights) save for the above licence to copy, store and
distribute this document and to produce derived copyright works.

The liability and responsibility for implementations based on this document rests with the implementer,
and not with any of the Generators. If you implement any of the contents of this document, you agree
to indemnify and hold harmless the Generators in any jurisdiction against any claims and legal
proceedings alleging that the use of the contents by you or on your behalf infringes any legal right of
any of the Generators or any third party.

None of the Generators accepts any liability whatsoever for any direct, indirect or consequential loss or
damage arising in any way from any use of or reliance on the contents of this document for any
purpose.

If you have any comments concerning the accuracy of the contents of this document, please write to:

    The Technical Secretary,
    Network Interoperability Consultative Committee,
    Ofcom,
    2a Southwark Bridge Road,
    London SE1 9HA.
6. Packet / Frame Marking .................................................................................................................. 18
7. IP Addressing ................................................................................................................................. 18
8. Resilience ......................................................................................................................................... 18
  8.1 Definitions of Terms in this Section ............................................................................................... 18
  8.2 IP Connectivity Failure Detection ................................................................................................ 18
  8.3 Signalling Path Resilience ............................................................................................................. 19
  8.3.1 Signalling Resilience using SCTP .............................................................................................. 19
  8.3.2 Signalling Resilience using TCP ............................................................................................. 19
  8.3.3 Signalling Resilience using UDP ............................................................................................. 19
  8.4 Media Path Resilience .................................................................................................................. 19

Annex A (informative): Dynamic Behaviour of Architecture ............................................................ 21
Annex B (informative): Example of multi-path Signalling Resilience ................................................ 24
Annex C (informative): Example Schematic of SCTP Multi-PATH signalling Resilience .................... 25
Annex D (informative): Example Schematic of TCP Multi-PATH ........................................................ 26
Annex E (informative): Example Schematic of UDP Multi-Path signalling Resilience ....................... 27
Annex F (informative): Example of Media Route Resilience ............................................................... 28
Annex G (informative): Example of Inter-working of Distributed and Integrated Interconnection Solutions .................................................................................................................. 29

History ............................................................................................................................................... 30
Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC.

Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by NICC.

Introduction

This specification forms part of the Next Generation Network, Multi-Service Interconnect (MSI) Release Structure and ought to be read in conjunction with the associated releases of the standard ‘Multi-Service Interconnect of UK Next Generation Networks’ [36].

1 Scope

This specification defines the generic connectivity of PSTN/ISDN services between UK NGNs using IP technology. It is intended to support all PSTN / ISDN interconnect products such as, but not restricted to, geographic and non-geographic number range interconnect, geographic and non-geographic number portability, Carrier Pre-Select, Indirect Access, Directory Enquiries and Emergency services.

This specification defines the service architecture and how it is supported by the MSI Common Transport Specification [1] that supports logical network layer point-to-point connectivity with dedicated bandwidth as the transport between communications providers (CPs). The ongoing work in other standards areas on routed network interconnect is recognised but considered to be insufficiently mature to adopt. However, where possible, options that facilitate the transition to this type of architecture have been followed. This document does not cover the facilities to support a transport function that utilises an IP routed, multi-point, interconnect network.

2 References

For the particular version of a document applicable to this release see ND1610 [36].

2.1 Normative references

[1] ND1611 "Multi-Service Interconnect Common Transport for UK NGNs".
[3] ND1614 "Management of General Connectivity of PSTN/ISDN Service Interconnect for UK NGNs ".
[5] ND1636 : " NGN Interconnect - IP Address Allocation ".
[6] ND1620 "Interconnect architecture for Voice Line Control Service between UK NGNs”.

[7] ND1633 "Next Generation Networks; Element Naming Framework”

[8] ND1628 “Security”


[10] ND1007 “ISDN User Part (ISUP)”


[12] ND1621 “Generic Overload Control for use on Interconnect of UK NGNs”


[14] ND1017 “Interworking between Session Initiation Protocol (SIP) and UKISDN User Part (UK ISUP)”


[16] ND1409 "Guidelines on PSTN/ISDN IP Interconnect Pre-operational Testing”


[18] ND1411 ”Signalling Operational Test Manual”

[19] ND1412 ”ISUP Services Operational Test Manual”

[20] ND1615 ”NGN Interconnect; Voice Line Control Service; General Connectivity Management”


[22] IETF RFC 2474: “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”


[25] IETF RFC 3551: “RTP Profile for Audio and Video Conferences with Minimal Control” Schulzrinne, H. and Casner, S

[26] IETF RFC 792: “Internet Control Message Protocol”

[27] ETSI TS 01 025: “TISPAN NGN Service and Capabilities Requirements; Release 1.”

[28] IEEE STD 802.1q: “Virtual Bridged Local Area Networks”


[31] IETF RFC3490, section 2: “IETF, Internationalizing Domain Names in Applications (IDNA)”
2.2 Informative references

[37] SR 001 262 (V2.0.0): "ETSI drafting rules Section 23:- Verbal Forms For The Expression Of Provisions ".

3 Definitions, symbols and abbreviations

3.1 Key Words
The key words “shall”, “shall not”, “must”, “must not”, “should”, “should not”, “may”, “need not”, “can” and “cannot” in this document are to be interpreted as defined in the ETSI Drafting Rules [37].

3.2 Abbreviations

CP .................................................. Communications Provider
DNS ............................................... Domain Name Service
DSCP ............................................. Differentiated Service Code Point
ETSI .............................................. European Telecommunication Standards Institute
ICMP ............................................. Internet Control Message Protocol
IETF .............................................. Internet Engineering Task Force
IP ................................................... Internet Protocol
ISDN ............................................ Integrated Services Digital Network*
ISUP ............................................ ISDN User Part of C7 signalling
kbps ............................................. Kilobits per second
kHz .............................................. Kilohertz
ms ................................................. milliseconds
MSI .............................................. Multi-Service Interconnect
NAT .............................................. Network Address Translation
NGN ............................................. Next Generation Network
NNI .............................................. Network Network Interface
PSTN ............................................. Public Switched Telephone Network*
PT ................................................ Payload Type
RTCP ............................................. Real Time Control Protocol
RTP ............................................... Real Time Protocol
SBC ............................................... Session Border Controller
SIP ................................................. Session Initiation Protocol
SIP-I .............................................. SIP with Encapsulated ISUP
SCTP ............................................. Stream Control Transmission Protocol
SDP ................................................ Session Description Protocol
TCP ............................................... Transmission Control Protocol
UDP ............................................... User Datagram Protocol
UNI ................................................ User Network Interface
URI ................................................ Uniform Resource Indicator

* PSTN and ISDN when used with the term ‘service’ define the replication of the service set applied to NGNs rather than the legacy networks themselves.
4 PSTN / ISDN Service Level Functional Architecture

The PSTN/ISDN Functional Architecture defines the interconnect interfaces between two UK Next Generation Networks (NGN) with relationship to the NGN’s internal logical network functions.

4.1 Conventions used in the Architecture Figures

The convention used in labelling the functional architecture is as follows:-

- All logical functions and interfaces are labelled with an alpha/numeric identifier.
- All logical functions’ identifiers begin with the letter ‘f’.
- All interconnect interfaces’ identifiers begin with the letter ‘i’.
- The second letter of an identifier (function or interface) indicates if it is associated with the Control plane (C) or the Bearer plane (B). ‘T’ denotes functions or interfaces associated with the MSI Common Transport Specification [6]. E.g. iC5 is control plane interface number 5.
- All functions and interfaces that have their own separate technical definition are labelled with a number unique to the identifier type. E.g. fC1 and iC1 are different defined entities as are iB1 and iB2.
- Multiple instances of separate functions or interfaces that have the same definitions have the same identifier root but are differentiated by appending an alpha letter to the root identifier. e.g. Interfaces with the same root identifier and number and a different suffix letter such as iB1a, iB1b, etc indicate separate instances of the same interface type and definition.
- Green lines between functions indicate logical internal relationships within the NGN which are not defined.
- Red lines indicate interconnect interfaces for the common transport capabilities in the bearer plane.
- Blue lines indicate service level interfaces that sit on top of the associated underlying common transport capabilities.

4.2 Interconnect Architecture Definition

The PSTN/ISDN Functional Architecture defines logical network functions and interconnect interfaces between two Next Generation Networks, NGN A and NGN B. It shows the static relationships between functions and the interconnect interfaces between NGNs. The functional architecture is divided into control and bearer planes and defines the properties of the functions and interfaces (see Figure 1). Note that the functional architecture is capable of being realised within a NGN in a number of ways and that no physical implementation is implied.

Typical outline message flows are provided in Annex A to show the dynamic behaviour of the architecture.
4.3 Functional Component Description

4.3.1 Control Plane Functions

4.3.1.1 Source Session Control Function (fC3)

This function controls the originating terminal that is setting up a session. It receives signalling from the terminal function within its network and if it determines that the routing requires to be passed through an interconnect point, it signals to the Edge Session Control Function within its own network. It sends the information on the session that is being set-up and its subsequent status and also sends the IP address and port number to be used by packets sent in the backward bearer path within its own network.

4.3.1.2 Edge Session Control Function (fC1)

The Edge Session Control Function provides the co-ordination intelligence for controlling the other functional elements associated with the interconnection.

The Edge Session Control Function:

a) may interact with other session control functions within its own network in order to manage session egress or ingress for the interconnection point it controls. e.g. Source and Destination Session Control Functions (fC3 & fC4).
b) **shall** interact with its peer Session Control Functions in another network, acting as a SIP Back-to-Back User Agent, managing session egress or ingress for the interconnection point(s) it controls.

c) **may** provide the IP address translations for the signalling stream between the two different address spaces, if the IP address space within its own network is different to the address space used across the interconnection.

d) **shall** ensure that the media type and characteristics that are requested in the signalling, (Session Description Protocol RFC 2327 [23]), are compatible with the PSTN/ISDN service as defined in the media stream definition and announcement section (see section 4.4.4). New session requests that do not have compliant SDP parameters **shall** be rejected in line with section 4.4.2.6 to ensure compliance with End-to-End Network Performance Rules & Objectives for the Interconnection of NGNs [13] and the ETSI NGN Service & Capabilities Requirements [28].

e) **shall**, during session establishment, determine that there is the required bandwidth for the bearer session as requested in the signalling by making requests for bandwidth allocation from the Bandwidth Management Function (fC2).

f) **shall** control the use of the Media Border Function (fB3) when present. See section 4.3.2.3.

g) **shall** provide the correct IP / port translations, as required, in the signalling streams associated with the media streams if the CP’s NGN and the interconnected network have different IP address spaces.

h) **shall** not depend upon the topology information received within the session control messages from the peer network. This applies to all SIP messages received which have headers that are capable of containing topology information such as Via, Route, Record Route and Service-Route.

i) **shall** prevent unconstrained circular routeing by supporting the Request Validation of the **Max-Forwards** SIP header field ([21] Section 16.3 step 3). To enable this mechanism to be used, the edge session controller **shall** support the Max-Forwards header field ([21] Section 8.1.1.6 Max-Forwards) and decrement this field when forwarding messages.

j) **should** produce call detail records which **may** contain any of the following:--
   i. Session time and date.
   ii. SIP Global reference in its P-charging Vector [14]
   iii. Session duration.
   iv. Source and destination IP addresses between the IP Media Border Function (fB3) and the termination inside the NGN as well as the IP address between the IP Media Border Functions of the peer networks (fB3-fB3) for fault analysis between CPs.

### 4.3.1.3 Bandwidth Management Function (fC2)

The Bandwidth Management Function within this architecture only relates to the transport trails in the bearer plane that carry the media stream (iT4b). In the general case this function will deal with requests for media sessions of varying bandwidth, but for PSTN / ISDN service, the media sessions are symmetric and of fixed bandwidth (e.g. RTP streams carrying 64kbps payload for PSTN / ISDN services and associated RTCP streams) and consequently simple call counting could suffice.
A bandwidth management function:

a) **should** hold a logical model of the bandwidth allocation of the transport trail that is related to the routing of the session (i.e. iT4b).

b) **should** have a near real time view of the transport operational status with regards to its ability to support the current overall bandwidth on the associated transport trails. i.e. the loss and re-establishment of the service offered on a transport VLAN is reflected into the Bandwidth Management Function.

c) **should** keep its bandwidth model in step with any fixed bandwidth policing performed by the transport function on its transport trails.

d) **should** process requests from the Edge Session Control Function for bandwidth allocation for a media session against the overall bandwidth on the transport trail across the interconnection.

### 4.3.1.4 Destination Session Control Function (fC4)

This function controls the end terminal receiving a session set-up. It receives signalling from the Edge Session Control Function within its network with information on the session that is being terminated (or being redirected) and sends back information related to the status of the terminal and the IP address and port number to be used by packets sent in the forward bearer within its own network.

Circular routeing checks **should** to be made in accordance with Inter-working between Session Initiation Protocol (SIP) and UK ISDN User Part (UK ISUP) [14].

### 4.3.2 Bearer Plane Functions

#### 4.3.2.1 Transport Function (fB1)

This service uses the IP capabilities (iT4) of the common transport specification as defined in ND1611 [1] and in accordance with clause 6 of the present document.

#### 4.3.2.2 Signalling Border Function (fB2)

The Signalling Border Function protects the signalling between edge session controllers in different networks which are connected via dedicated data channel(s) (iT4a) of fixed and policed bandwidth. Signalling Border Functions support connections that carry the signalling between one or more pairs of Edge Session Controllers.

The Signalling Border Function:

a) **should** provide a firewall between the NGN and the interconnection space applying policies that only allow IP address and port numbers from agreed sources into the network operator’s NGN and to ensure that only legitimate signalling exchanges are permitted from the CP’s NGN onto the interconnect link.

b) **may** provide translation of the signalling IP addresses.

c) **shall** perform the functions of a Security Gateway as defined in ETSI TS 133 210 [33] in accordance with sub-clause 4.4.1 of the present document.

d) **shall** detect the loss and reestablishment of communications with its peer Signalling Border Function and **shall** support monitoring requests from its peer. (See section 8.2).
e) **should**, if not provided elsewhere, provide the IP address translations for the signalling stream between the two different address spaces, if the IP address space within its own network is different to the address space used across the interconnection.

### 4.3.2.3 Media Border Function (fB3)

The IP Media Border Function provides policing of media streams between networks carried via transport interface iT4b.

The Media Border Function:

a) **may** open and close individual firewall pinholes for each IP address and port number pair for a RTP media stream on the establishment and termination of a session by the Edge Session Controller (fC1).

b) **may** provide network topology concealment of the CP’s NGN.

c) **should** allow the connection of RTP streams, within its own network (with associated IP address space and UDP port numbers) and the RTP streams at the interconnect, with different or overlapping IP address spaces and sets of UDP port numbers.

d) **should** enforce the bandwidth of each media stream as requested in the associated signalling message.

e) **shall** detect the loss and reestablishment of communications with its peer Media Border Function and **shall** support monitoring requests from its peer (See section 8.2).

### 4.4 Interface Definitions

#### 4.4.1 Signalling Transport Interfaces

##### 4.4.1.1 Signalling Interconnect Use of the Common Transport Function (iT4a)

The signalling interface **shall** be carried over the IP capability of the common transport function (iT4a) on one or more individual VLANs reserved for signalling only.

Traffic carried on one such VLAN **shall not** affect the capacity of other VLANs. Each VLAN may convey messages associated with one or more signalling associations. The dimensioning of each VLAN **shall** take account of the capacity required for peak load and loads encountered under fault conditions.

#### 4.4.1.2 Signalling IP Addressing

An IP subnet **shall** be allocated, in accordance with section 7, for each signalling connection between the signalling border functions in each CP’s network. Each device, IP interface, or other network element on the connection **shall** be allocated an agreed IP address from within this subnet.
Each CP shall inform the other of the IP addresses to be used to communicate with each relevant edge session control function.

4.4.1.3 Signalling VLAN Bandwidth

The bandwidth required for each signalling VLAN should be determined by taking account of:

- the number of signalling paths carried on the signalling VLAN
- the peak signalling rate of each of the signalling paths carried on the VLAN
- the failure modes and required resilience of the signalling VLANs

4.4.1.4 Signalling Security

Signalling trails shall be protected from unauthorised access from inside or outside a communication provider’s network.

As the signalling between NGNs controls the opening and closing of media streams in the Media Border Functions (fB3), the signalling transport between NGNs shall be secured by an IPSec tunnel that provides authentication and encryption as defined in Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security [33] but with the following modifications and clarifications:

4.4.1.4.1 References to the Security Gateway or SEG should be considered analogous to the Signalling Border Function (fB2) defined in this document.

4.4.1.4.2 References to securing internal interfaces within ‘Service Provider Security Domains’ should be ignored as this is internal to CPs network and therefore outside the scope of this document.

4.4.1.4.3 Reference to the 'Za' interface between CPs in Section 5.6.2 of Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security [33] shall be considered equivalent to the CP signalling interconnect interface (iT4a) in this document.

4.4.1.4.4 Clause 5.2.1 of Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security [33] describes an element of the IPSec security architecture - the Security Policy Database and considers the possibility of connections not protected by IPSec by policy. For the purposes of this document, all signalling communication between Service Providers shall be protected by IPSec, and the entries in each CP’s Security Policy Database shall reflect this.

4.4.1.4.5 For the purpose of clause 5.2.1 of Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security [33] IPSec Shared Secrets shall be used. This Shared Secret shall be changed only by mutual management agreement between CPs. The minimum shall be a bilaterally agreed Shared Secret per interconnect agreement. This Shared Secret shall be unique between CPs.

4.4.1.5 Media Security

Media security should be provided by the dynamic pin-hole functions of the Media Border Function (fB3) under the control of the Edge Session Control Function (iC1) which it derives from the internal and interconnect signalling.

Authentication or encryption of the content of a media stream shall not be required between the Media Border Functions (fB3) on an interconnect.
4.4.2 Signalling Control Interface (iC1)

4.4.2.1 Application Layer Protocol

The application signalling protocol for iC1 shall be as defined in ND1017 [14].

4.4.2.2 Signalling Transport Protocols

The signalling interface (iC1)

- should use SCTP as defined in ND1012 [11]
- may use TCP as defined in ND1018 [9]

The use of UDP is not defined.

4.4.2.3 SIP URI Naming Scheme

This SIP URI naming scheme shall be used at the NNI for PSTN service but it should be noted that it is not intended for use at the UNI.

The SIP URI naming scheme shall conform to ND1633 [7], using the format:

\(<\text{network internal part}\.\text{local application ID}\.\text{provider}\.\text{NGN root domain}>\)

Taken together, \(<\text{network internal part}\.\text{local application ID}>\) shall comprise the \(<\text{network element identifier}>\). The \(<\text{network element identifier}>\) shall identify the particular Edge Session Control function within a CP’s NGN and is allocated by the owner of the registered \(<\text{provider}>\) name. The owner of the registered \(<\text{network element identifier}>\) shall ensure that the \(<\text{network element identifier}>\) is unique to each of the Edge Session Control functions within their NGN. The \(<\text{network element identifier}>\) may contain a series of labels, separated by dots.

Typical examples of SIP URI names are depicted in Table 4.4.2.3.a.

<table>
<thead>
<tr>
<th>Network Internal Part</th>
<th>local application ID</th>
<th>Provider</th>
<th>NGN Root Domain</th>
<th>Consequent Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>pstn</td>
<td>cs-23</td>
<td>example-telco</td>
<td>uktel.org.uk</td>
<td>pstn.cs-23.example-telco.uktel.org.uk</td>
</tr>
<tr>
<td>cs-23</td>
<td>pstn</td>
<td>example-telco</td>
<td>uktel.org.uk</td>
<td>cs-23.pstn.example-telco.uktel.org.uk</td>
</tr>
</tbody>
</table>

4.4.2.4 SIP URI to IP Address Binding

The binding of SIP URI to IP address shall be passed as management information at the time of service establishment or as a result of any subsequent modifications.

4.4.2.5 Circular Routeing Limitation in SIP

Refer to Inter-working between Session Initiation Protocol (SIP) and UK ISDN User Part (UK ISUP) [14] for information to limit circular routeing in SIP.
4.4.2.6 Unsupported Media Types

If the media type and characteristics that are requested in the signalling, (Session Description Protocol RFC 2327 [23]), are not compatible with the PSTN/ISDN service as defined in the media stream definition and announcement section (see section 4.4.4) the SIP request shall be rejected with the SIP message, ‘415 Unsupported media type’ and with an ISUP reject cause value 79, ‘Service or option not implemented, unspecified’.

4.4.2.7 Session Processing Overload Control

SIP has no mechanism for managing processing overloads resulting from high levels of offered session set-up traffic. Therefore, traffic overloads shall be controlled using the Automatic Congestion Control mechanism defined in UK ISUP [10] and as carried within the SIP-I signalling.

4.4.3 Media Stream Transport Interfaces

Shall be conformat to the format defined in ND1635 [4].

4.4.4 Media Stream Definition and Announcement (iB1)

The media stream shall be announced across the signalling interface (iC1) using the Session Description Protocol (SDP) defined in IETF RFC 2327 [8] with parameters set as shown in modified Tables 6 and 26 given in ND1017 [14].

The coding types supported by the NGN for PSTN/ISDN service shall be:-

- G.711 A-law
- 64 kbps Transparent or Clearmode

64 kbps “Clearmode” or “Transparent” calls cover applications such as the transfer of ISDN 64 kbps data, and ISDN 7 kHz wideband voice (possibly using a codec such as G.722) where there is no encoding or decoding in the interconnect gateways and the only function required is packetisation of the data.

The media stream transport shall use the User Datagram Protocol (UDP) as described in ND1635 [25].

The RTP payload type (PT) header field identifies the RTP payload format, and the mapping of payload type codes to payload formats may be static or dynamic (static means that the same code is bound to a particular format for all calls, whereas dynamic means that the code associated with a particular payload format may change from call to call). The number range 96-127 shall be reserved for dynamic assignment of payload type numbers in accordance with RFC 3551 [26]. The payload type codes for PSTN/ISDN call types shall be the same as those given in the fmt-list in modified Tables 6 and 26 in ND1017 [14].

Modified Tables 6 and 26 in ND1017 [14] include the SDP “a=ptime:” attribute. The “a=ptime:” attribute shall be present in all these SDP types in order to specify that a 10 ms encoding packet size shall be used.

Note that the default encoding packet size is defined in ND1635 [4].

The media stream shall only support symmetric RTP as described in ND1635
4.4.4.1 Voice-Band Data
This is defined in ND1635 [4].

4.4.4.2 Voice Activity Detection
This is defined in ND1635 [4].

4.4.4.3 Error performance and Packet Loss
This is defined in ND1635 [4].

4.4.4.4 Delay and Packet Delay Variation
This is defined in ND1635 [4].

4.4.4.5 Echo control
This is defined in ND1635 [4].

4.4.4.6 Media Stream Synchronisation
This is defined in ND1635 [4].

4.4.4.7 Monitoring of IP Media Streams
This is defined in ND1635 [4].

5. Interconnect Routes that Carry Priority Calls

A route carrying ordinary and priority traffic between two NGNs should be configured so that the total bandwidth available on the route shall be equal to the bandwidth configured for ordinary calls plus that configured as reserved for priority calls.

5.1 Ordinary Calls
For ordinary calls, where the bandwidth currently being used on the route plus the bandwidth required for a new call is less than or equal to the bandwidth configured for ordinary calls, the call shall be allowed. However, if this condition is not met (i.e. there is insufficient spare bandwidth available for a new ordinary call), then this call attempt shall be failed and re-routeing may take place.

5.2 Priority Calls
For priority calls, where the bandwidth currently being used on the route plus the bandwidth required for a new call is less than or equal to the total (i.e. ordinary and priority) bandwidth on the route, the call shall be allowed. However, if there is insufficient spare bandwidth on the route, re-routeing and retry functions shall take place.

On ordinary or priority call set up and completion, the bandwidth in use on the route is increased and decreased respectively by that used for the call.
5.3 Priority Call Detection

Priority calls shall be detected in accordance with ND1017 [14].

5.4 Priority Calls and Overload Management

A priority call shall not be subject to overload control or any inbound or outbound call rate restrictors at the interconnect interface.

6. Packet / Frame Marking

In order to introduce new and as yet undefined services to the MSI without changing this service, IP packet marking (DSCP) [22] or Ethernet frame marking [29] are not used. Media and signalling rely on being carried in independent VLANs, each with its own shaped and policed bandwidth, as a service provided by the Common Transport Function [1]. Therefore, these packet marking fields should be ignored.

7. IP Addressing

Details of IP Addressing issues including Version of Internet Protocol, IP address ranges and Network Address Translation can be found in ND1636 [5].

8. Resilience

8.1 Definitions of Terms in this Section

A Signalling Link is a signalling connection between two edge session controllers.

A Media Route is managed bandwidth between paired, peer Media Border Functions.

There is a one to one relationship between a Signalling Link and a Media Route.

8.2 IP Connectivity Failure Detection

Where a border function uses UDP for signalling or media it shall detect the loss and reestablishment of communications with its peer in an interconnecting network. This shall be achieved by sending ICMP Echo messages [27]. The absence of an ICMP Echo Reply within 25ms to three consecutive Echo messages shall be interpreted as a failure in IP connectivity and should be reported to the NGNs internal fault monitoring functions. Echo messages shall continue to be re-transmitted to detect signalling channel re-establishment. Signalling channel re-establishment shall be deemed to have occurred when the response to three consecutive Echo messages has been received. ICMP Echo messages shall be sent every 25ms.

Where a border function uses UDP for signalling or media it shall respond to an ICMP Echo message from its peer across the interconnect with an ICMP Echo Reply, the response shall be sent such that it will be received within 25ms of the sending of the original message.

Where TCP and SCTP are used, IP connectivity shall be monitored by their in built functionality and meet at least the failure detection time for UDP as above. Where TCP and SCTP are used, IP
connectivity **shall** be monitored by their in built functionality configured to detect failure within 100ms.

If the IP connection between Media Border Functions has failed then the Bandwidth Management Function **shall** be notified of the loss of bandwidth so that the Edge Session Control Function **shall not** establish new sessions across that interconnect until the connection is re-established.

### 8.3 Signalling Path Resilience

Signalling Links **may** have resilience provided at the common transport function layer.

Signalling Links **should** be configured to use multiple physically separate interconnect points between CP’s Edge Session Control Functions (fC1). The signalling path between Edge Session Control Functions **shall** be monitored for failure depending on the transport protocol used and on detection of failure **shall** use an alternative path if configured. The restoration of any failed signalling path in a resilient multi-path configuration **should** be detected and automatically become available for use. (See Annex B)

Where signalling peers, i.e. ESCFs (fC1), are connected by only one logical path which provides performance that is acceptable to CPs concerned, either a single-homed SCTP [11] path or TCP [9] **may** be used. Otherwise multi-homed SCTP [11] **shall** be used.

#### 8.3.1 Signalling Resilience using SCTP

If signalling resilience features are required when using SCTP [11] this **shall** use the multi-stream connectivity of signalling streams through the SCTP ‘multi-homing’ feature and the signalling layer connection continuity monitoring through the inbuilt heartbeat within the protocol. (See Annex C)

#### 8.3.2 Signalling Resilience using TCP

An example of achieving signalling resilience using Interconnect Transmission Control Protocol (TCP) is described in Annex D.

#### 8.3.3 Signalling Resilience using UDP

An example of achieving signalling resilience using UDP is shown in Annex E. Note that UDP in the UK is yet to be defined.

### 8.4 Media Path Resilience

Media Routes **may** have resilience provided at the common transport function layer.

The media stream for all sessions / calls in progress might be lost in the event of a Media Route failure that is not protected by common transport function layer mechanisms.

Resilience **should** be provided at the application layer via alternative routeing mechanisms within an originating NGN’s session control functions. In this case, when a session is being established, if the Edge Session Control Function for a particular interconnecting Media Route detects that the Media Route is unavailable, through Media Route failure, it **should** direct the session setup to an Edge Session Control Function that controls an alternative Media Route. The session **should** then be established through this alternative Media Route as normal. (See Annex F)

If the Edge Session Control Function (fC1) determines that the associated Media Route which is terminated by the media border function (fB3) cannot be used then, when it receives an incoming SIP-I Invite, it **shall** respond with a SIP Response 503 (Service Unavailable) message with a ‘Retry-After’ field set to 60 seconds [14]. The corresponding Edge Session Control function (fC1) in the
interconnecting network shall not send any more invites associated with that Media Route until the ‘Retry-After’ timer has expired.

Reasons why the Media Route cannot be used include, but are not limited to:-

- The Edge Session Control function (fC1) is unable to communicate with the Media Border function (fB3).
- The Bandwidth Management function (fC2) is unable to communicate with the Media Border function (fB3).
- The Edge Session Control function (fC1) is unable to communicate with the Bandwidth Management function (fC2).
- The Media Border function (fB3) is isolated from its own internal network (i.e. facing into its own NGN) and therefore end-to-end media flows (iB1) cannot be established.
- The Media Route on interface iT4b (i.e. connection between Media Border functions) has failed.
Annex A (informative):
Dynamic Behaviour of Architecture

The dynamic behaviour of the signalling and media interfaces between NGNs for PSTN/ISDN is highlighted by the following typical event flows between internal NGN functions, (which describes the behaviour of the NGN) and its mapping onto the external interconnect interfaces between the NGNs via the two message sequence diagrams below. Note that at the top of these figures the IP address spaces have been colour coded for that internal to NGN A (Green), NGN B (Blue) and the interconnect space (Amber). This colour coding is carried through into the corresponding text for the various messages on the message sequence diagrams.
‘Session Establishment’ for PSTN/ISDN service between NGNs
‘Session Clearing’ for PSTN/ISDN service between NGNs
Annex B (informative):
Example of multi-path Signalling Resilience

In this example, two independent and preferably geographically separate signalling paths (using two signalling VLANs on two different physical transmission systems) are used to carry the signalling associated with three separate and independent media paths.
Annex C (informative):
Example Schematic of SCTP Multi-PATH signalling Resilience
Annex D (informative):
Example Schematic of TCP Multi-PATH

SIGNALLING RESILIENCE

In this example a multi-path manager is used to establish two TCP paths to different IP addresses and to detect when a TCP socket failure occurs, redirecting signalling messages to the alternate TCP path. The TCP timers are profiled to detect socket failure within an appropriate time.
Annex E (informative):
Example Schematic of UDP Multi-Path signalling Resilience

In this example a multi-path manager is used to monitor the ability to communicate with two different IP addresses through a heartbeat message / response. Signalling messages are only sent to available IP addresses.
Annex F (informative):
Example of Media Route Resilience

This example shows that, on detect of a Media Route failure, new session setup attempts are routed to another Edge Session Control Function for connection over a different Media Route.
Annex G (informative):
Example of Inter-working of Distributed and Integrated Interconnection Solutions

There are two main implementation options. These are:-

- Distributed Border Control with separate Signalling Border Function and IP Media Border Function
- Integrated Session Border Controller

The inter-working or these two interconnect scenarios is shown below.

On the left hand side of the figure below is a distributed border control implementation with a physically separate Signalling Border Function and IP Media Border Function, on the right is the Session Border Controller (SBC) implementation. The diagram in this annex shows that the fundamental traffic flows remains the same i.e. signalling streams [iC1] and media [iB1] maintain a point to point relationship.
## History

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue 1</td>
<td>02/05/06</td>
<td>First issue</td>
</tr>
<tr>
<td>Issue 2</td>
<td>12/06/06</td>
<td>Updated to include new section 5, Interconnect Routes that Carry Priority Calls.</td>
</tr>
<tr>
<td>V1.2.1</td>
<td>May 08</td>
<td>Converted to NICC Version numbering scheme</td>
</tr>
<tr>
<td>V1.2.2</td>
<td>May 08</td>
<td>Converted to revised NICC ND template. Change to Section 4.4.2.2 on signalling transport protocols to be used.</td>
</tr>
<tr>
<td>V2.1.1</td>
<td>July 08</td>
<td>Created from V1.2.2. Changed to take account of publication of ND1635, ND1636 and ND1704. Updated to remove spurious abbreviations. Section 4.2.3.3 updated to align with ND1633. Text tidied in Sections 4.4.3 &amp; 7. Diagram re-attached to Annex E.</td>
</tr>
<tr>
<td>V2.1.2</td>
<td>August 08</td>
<td>Reference to ND1610 made normative (was informative) with consequent change to reference numbering. Removal of informative reference to ND1625 as this was not actually mentioned in the document.</td>
</tr>
</tbody>
</table>