NICC ND 1612 V1.2.2 (2008-05)

NICC Document

Generic IP Connectivity for PSTN / ISDN Services between Next Generation Networks

Network Interoperability Consultative Committee,
Ofcom,
2a Southwark Bridge Road,
London,
SE1 9HA.

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.

Contents

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' [1]**Error! Reference source not found.**.

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 [2] 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 [**Error! Reference source not found.**].

2.1 Normative references

[1] ND1610 "Multi-Service Interconnect of UK NGNs".

[2] ND1611 "Multi-Service Interconnect Common Transport for UK NGNs".

[3] ND1018 "Transmission Control Protocol (TCP)"

[4] ND1007 "ISDN User Part (ISUP)"

[5] ND1012 “Interconnect Stream Control Transmission Protocol (SCTP) and Adaptation Layers”

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

[7] ND1701 ”Recommended Standard for the UK National Transmission Plan for Public Networks”

[8] IETF RFC 3261: “IETF SIP: “ Session Initiation Protocol.”

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

[10] IETF RFC 2327: “SDP: “ Session Description Protocol.” M. Handley, V. Jacobson.”

[11] IETF RFC 0768: “User Datagram Protocol, J. Postel”

[12] IETF RFC 3550: “RTP: A Transport Protocol for Real-Time Applications, Internet Engineering Task Force”

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

[14] ITU-T Recommendation T.38: “Procedures for real-time Group 3 facsimile communication over IP networks”

[15] IETF RFC 2833: “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”

[16] ITU-T Recommendation G.826: “End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections”

[17] ITU-T Recommendation G.811: “Timing characteristics of primary reference clocks”

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

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

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

[21] STD0013 IETF RFC1034: “Domain names - concepts and facilities”

[22] IETF RFC1035: “Domain names -implementation and specification. Nov 1987.”

[23] IETF RFC3490, section 2: “IETF, Internationalizing Domain Names in Applications (IDNA)”

[24] ETSI TS 133 210: “Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security”

[25] IETF RFC3491: “Nameprep: A Stringprep Profile for Internationalized”

[26] IETF RFC3492: “Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)”

2.2 Informative references

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

2.3 Compatability

To allow the compatility of document revisions, for a set of purposes, to be derived from an external table which, for convenience, is contained in the release documents

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 [27].

3.2 Abbreviations

3GPP..... 3rd Generation Partnership Project

A/V ..... Audio/Visual

B2BUA..... Back to Back User Agent

CP ..... Communications Provider

DNS ..... Domain Name Service

DSCP ..... Differentiated Service Code Point

DTMF..... Dual Tone Multi-Frequency

ESR..... Errored Second Ratio

ETSI ..... European Telecommunication Standards Institute

Func. ..... Function

Gbps ..... Gigabit per second

Hz ..... Hertz

IAM ..... Initial Address Message in ISUP

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

ITU-T ..... International Telecommunication Union - Telecoms

kbps ..... Kilobits per second

kHz ..... Kilohertz

Mbps..... Megabits per second

MF4 ..... Multi-Frequency signalling No. 4

ms ..... milliseconds

MSI..... Multi-Service Interconnect

NAT..... Network Address Translation

NGN ..... Next Generation Network

NNI ..... Network Network Interface

POS..... Packet Over SDH

PPP ..... Point-to-Point Protocol

PSTN ..... Public Switched Telephone Network*

PT ..... Payload Type

RIPE ..... Regional Internet Registry (RIR) for Europe, the Middle East, and Central Asia

RIR ..... Regional Internet Registry

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

TDM ..... Time Division Multiplex

UDP..... User Datagram Protocol

UNI..... User Network Interface

URI ..... Uniform Resource Indicator

VBD ..... Voice Band Data

* 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.

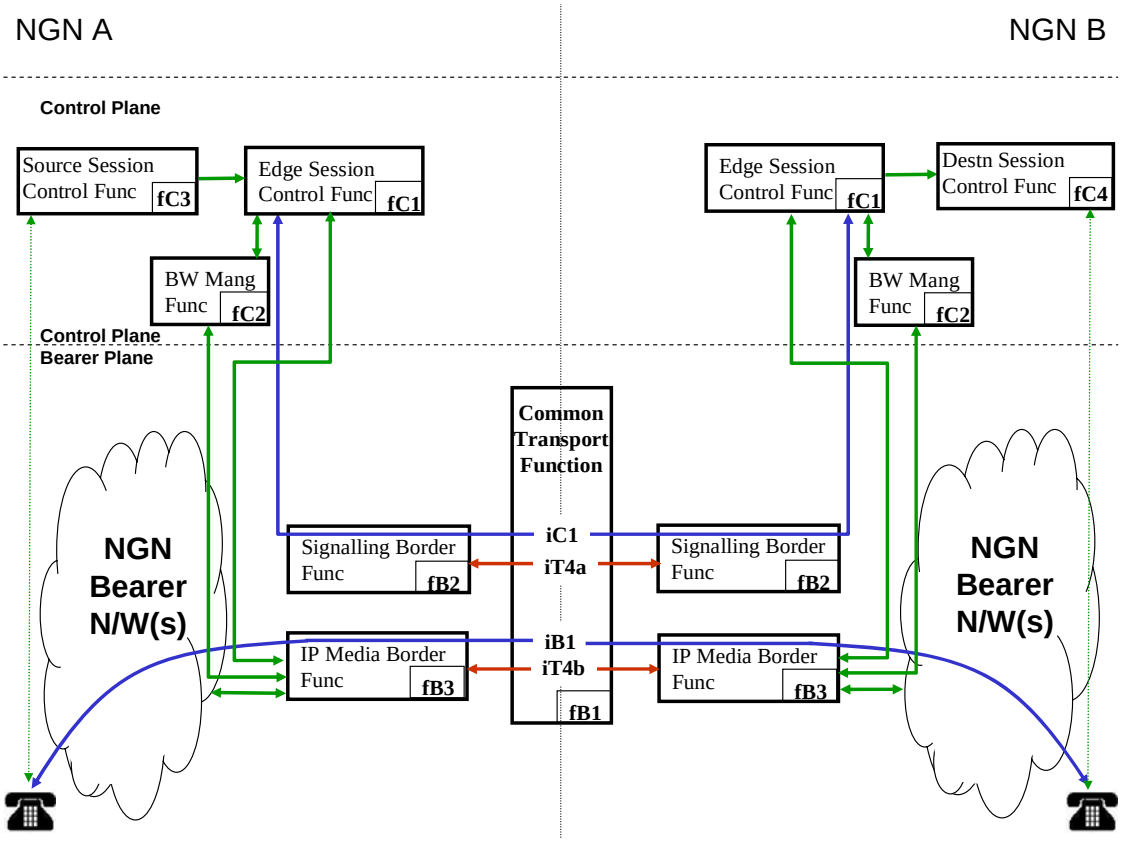


Figure 1: Functional Architecture for PSTN / ISDN Generic Connectivity

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 routeing 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 [10]), 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 Recommended Standard for the UK National Transmission Plan, NICC [7] and the ETSI NGN Service & Capabilities Requirements [19].

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 ([8] Section 16.3 step 3). To enable this mechanism to be used, the edge session controller **shall** support the Max-Forwards header field ([8] 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 [6]
   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 routeing 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) [6].

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 [2] 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 [24] 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 [24] 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 [24] **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 [24] 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 CPs 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 [24] 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 [6].

4.4.2.2 Signalling Transport Protocols

The signalling interface (iC1)

- **should** use SCTP as defined in ND1012 [5]
- **may** use TCP as defined in ND1018 [3]

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.

4.4.2.3.1 URI Format

This naming scheme defines the <*domainname*> part of the SIP URI format as shown below:

sip: <*userinfo*>@<*domainname*>

The standard "Inter-working between Session Initiation Protocol (SIP) and UK ISDN User Part (UK ISUP) [6] defines the <*userinfo*> of the SIP URI.

The <*domainname*> part of the SIP URI **shall** consist of 3 component parts, as follows:

<*network element identifier*>**.**<*provider*>**.**<*NGN root domain*>

where:

- <*NGN root domain*> **shall** be "*uktel.org.uk*" for all NICC compliant NGN IP interconnects.

  Note that this may be subject to change following agreement of a standardised NGN root domain name by ETSI.

  The <*NGN root domain*> name **shall** appear in the public DNS but public internet originated queries related to that domain name **need not** return a valid address for an NGN network element (i.e. Edge Session Control function) that is providing PSTN interconnect service.

- <*provider*> **shall** uniquely identify the NGN CP.
  Valid <*provider*> names **shall** be those registered with the owner of the <*NGN root domain*>. Names chosen for the <*provider*> component **should**, where possible, reflect the CP's company name. The <*provider*> **shall** contain a single label.

- <*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 <*provider*> name. The owner of the registered <*network element identifier*> **shall** ensure that <*network element*

identifier> is unique to each of the Edge Session Control functions within their NGN. The <*network element identifier*> **may** contain a series of labels, separated by dots.

4.4.2.3.2 Naming Standards

Labels **shall** be compliant with STD0013 [21]. Characters used in names shall be from the "LDH code points" set defined in RFC3490 section 2 [23]. This consists of the 26 ASCII letters, the 10 ASCII digits, and the hyphen-minus.

Other characters **should not** be used. Where it is essential to use characters outside this repertoire, they **shall** be encoded in accordance with the IDNA scheme defined in RFCs 3490 [23], 3491 [25] & 3492 [26].

4.4.2.3.3 Name Length

The <*network element identifier*> **shall** consist of a maximum of 38 characters. Note that this excludes the dot between the <*network element identifier*> and the <*provider*> components.

The <*network element identifier*> component plus the <*provider*> component **shall** consist of a maximum of 43 characters including the dot between them but excluding the dot between the <*provider*> component and the <*NGN root domain*> name.

To accommodate any future changes, a maximum <*domainname*> length of 63 characters **shall** be capable of being accommodated.

Note: These constraints have been chosen to allow for a potential future information privacy requirement to mask the <*provider*> identity to something less meaningful, and to facilitate a migration to an <*NGN Root Domain*> aligned with ETSI standards.

4.4.2.3.4 Example

A typical <*domainname*> example based on this scheme could be:-

pstn-23.cs.example-telco.uktel.org.uk

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) [6] 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 [10]), 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 [4] and as carried within the SIP-I signalling.

4.4.3 Media Stream Transport Interfaces

4.4.3.1 Media Stream use of the Common Transport Capability (iT4b)

The media stream interface **shall** be carried over the IP capability of the transport function (iT4b) on a trail of fixed bandwidth reserved for media streams only.

4.4.3.2 Media Stream IP Address Allocation

An IP subnet **shall** be allocated, in accordance with section 6, for each media trail connection (VLAN) between the media border functions in each CP's network. Each media border function **shall** be allocated a specific IP address within this subnet.

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 [6].

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) described in IETF RFC 0768 [11], and **shall** use the Real-Time Transport Protocol (RTP) described in IETF RFC 3550 [12].

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 [13]. 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 [6].

Modified Tables 6 and 26 in ND1017 [6] 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, if the “a=ptime” attribute is not used, is given in the RTP A/V Profile defined in RFC 3551 [13] as 20 ms. This default of 20ms **shall not** be used for this service type. A 10 ms packet size is required to meet the delay requirements in Recommended Standard for the UK National Transmission Plan, NICC. [7] and ETSI NGN Service & Capabilities Requirements [19].

The media stream **shall** only support symmetric RTP (i.e. originating and terminating media flows use the same IP address and port number).

4.4.4.1 Voice-Band Data

The media stream **shall** natively support voice-band data (VBD).

The media stream interface **shall not** support fax modem bypass standard T.38 [14].

The media stream interface **shall not** support DTMF (MF4) bypass standard [15].

4.4.4.2 Voice Activity Detection

The media stream **shall not** support silence suppression / voice activity detection.

4.4.4.3 Error performance and Packet Loss

In order to emulate current ISDN services with the same error performance, interconnecting networks **shall** meet the national end-to-end error allocation and packet loss that are given in ITU-T Recommendation G.826 [16] and Recommended Standard for the UK National Transmission Plan, NICC. [7].

4.4.4.4 Delay and Packet Delay Variation

Refer to Recommended Standard for the UK National Transmission Plan, NICC [7] for information on delay and packet delay variation.

4.4.4.5 Echo control

Refer to Recommended Standard for the UK National Transmission Plan, NICC [7] for information on echo control.

4.4.4.6 Media Stream Synchronisation

The multi service interconnect is not a reliable source for the provision of a clock synchronisation service.

In order to meet the required media slip rate for PSTN and ISDN service types, each interconnecting network **shall** be synchronised to a clock source in accordance with ITU-T recommendation G.811 [17] by an independent means. Further guidance is available in Recommended Standard for the UK National Transmission Plan, NICC. [7].

4.4.4.7 Monitoring of IP Media Streams

The interface (iB1) **shall** carry RTCP packets between packetisation end points, which **shall** enable the following parameters to be monitored:-

- Delay
- Packet loss
- Jitter

This **may** be achieved using the ***Sender Reports*** described in the Real Time Control Protocol (RTCP) specified in IETF RFC 3550 [12].

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 repectively by that used for the call.

5.3 Priority Call Detection

Priority calls **shall** be detected in accordance with ND1017 [6].

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) [9] or Ethernet frame marking [20] 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 [2]. Therefore, these packet marking fields **should** be ignored**.**

7. IP Addressing

7.1 Version of Internet Protocol

IPv4 **shall** be used across interconnects [See interfaces iT4a & iT4b].

7.2 IP Address Ranges

Public IP addresses (assigned by a relevant RIR such as RIPE, and not used for any other purpose or link) **shall** be used for IP interconnect unless the interconnecting CPs mutually elect to use some other arrangement (e.g. private IP addresses). In the latter case, they will be responsible for resolving any incompatibilities which arise.

Each CP **shall** be responsible for obtaining addresses for use within its own network and for informing the other CP of the addresses used to reach interconnection functions (e.g. see 4.4.1.2).

Addresses for the shared network segment between CP network edges (i.e. between media or signalling border functions) **should** be provided by one of the two parties. In the absence of any other agreement, the requesting CP **shall** provide the addresses.

The CP providing addresses is permitted to allocate a /30 or any larger subnet that they deem suitable.

In the absence of any other agreement, the address space **shall** be divided equally between the two CPs, with the CP providing the addresses using the lower half and the other CP the upper half. It is recommended that addresses be used starting from the outside and working towards the middle. Disregarding the 'any host' (all zeros) and 'every host' (all ones) sub-net addresses, it is recommended that addresses be used starting from the outside and working towards the middle.

7.3 Network Address Translation

Network Address Translation (NAT) **may** be implemented by an interconnecting network. However, neither party **may** require or forbid the other to use NAT.

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 [18]. 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 [18] .

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 [5] path or TCP [3] **may** be used. Otherwise multi-homed SCTP [5] **shall** be used.

8.3.1 Signalling Resilience using SCTP

If signalling resilience features are required when using SCTP [5] 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 [6]. The corresponding Edge Session Control function (fC1) in the

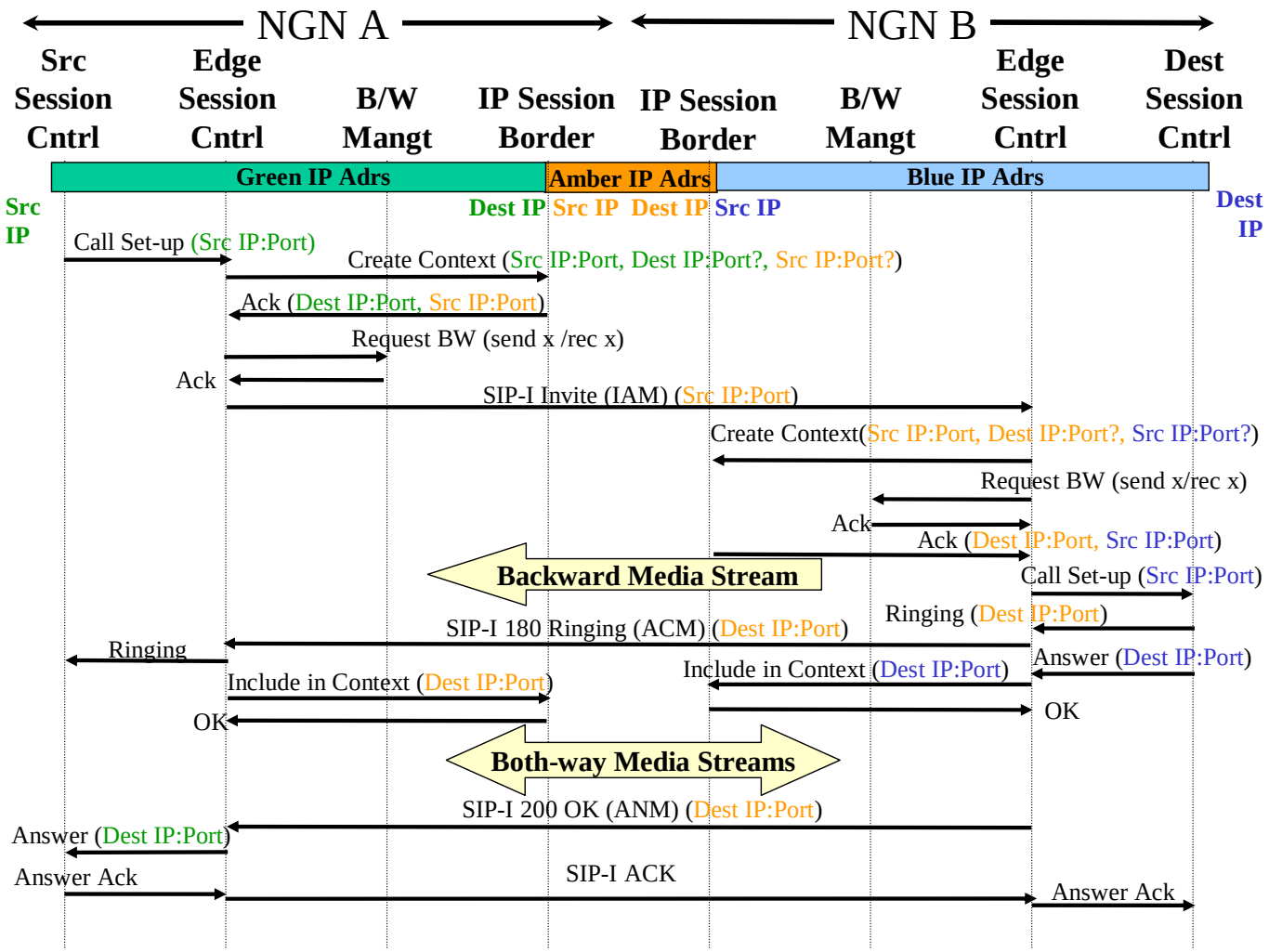
interconnecting network **shall not** send any more invites associated with that Media Route until the 'Retry-After' timer has expired.

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

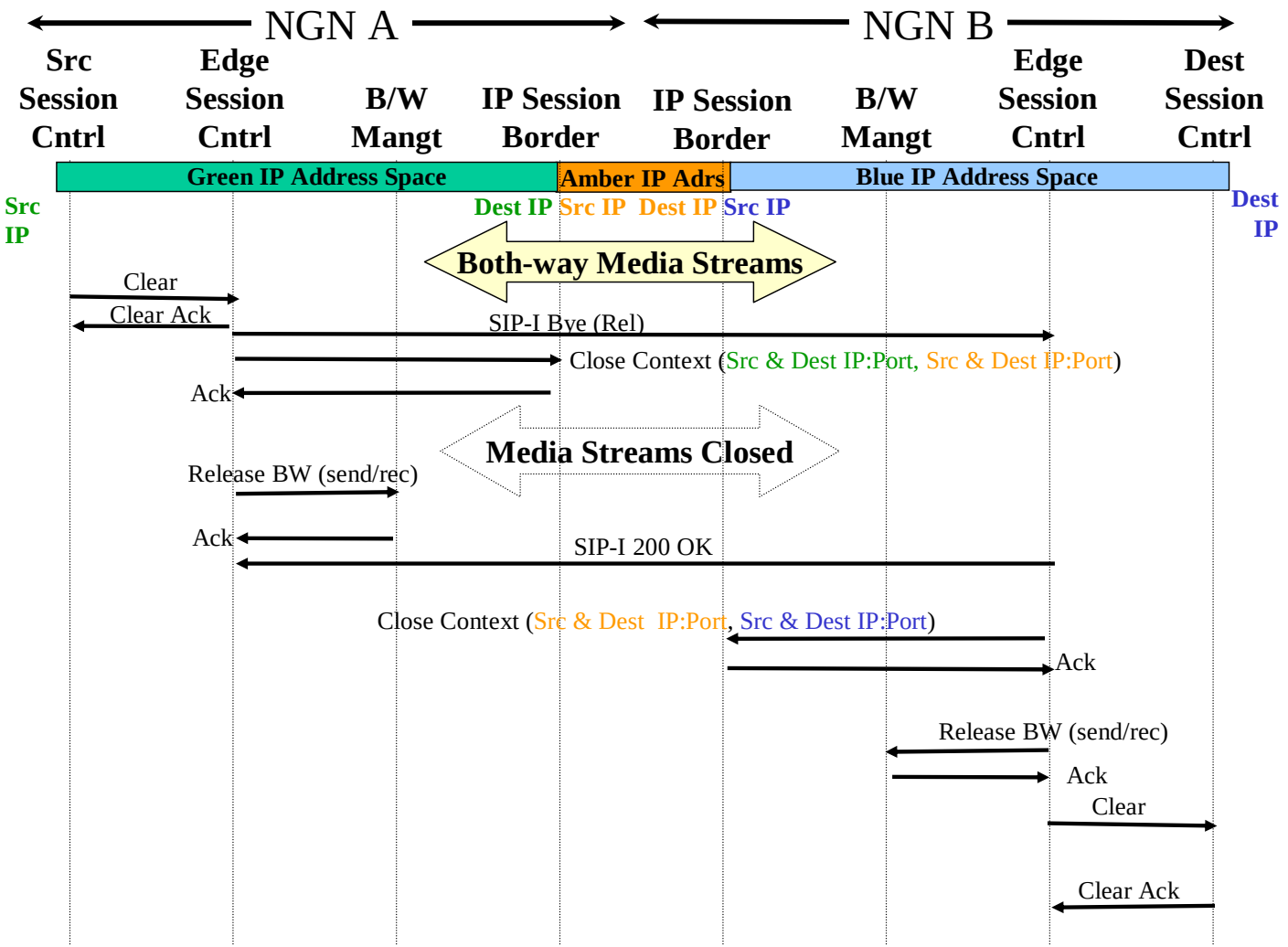
- The Edge Session Control function (fC1) is unable to communicate with the Media Border function (fB3).
- The Bandwidth Management function (fC2) is unable to communicate with the Media Border function (fB3).
- The Edge Session Control function (fC1) is unable to communicate with the Bandwidth Management 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.



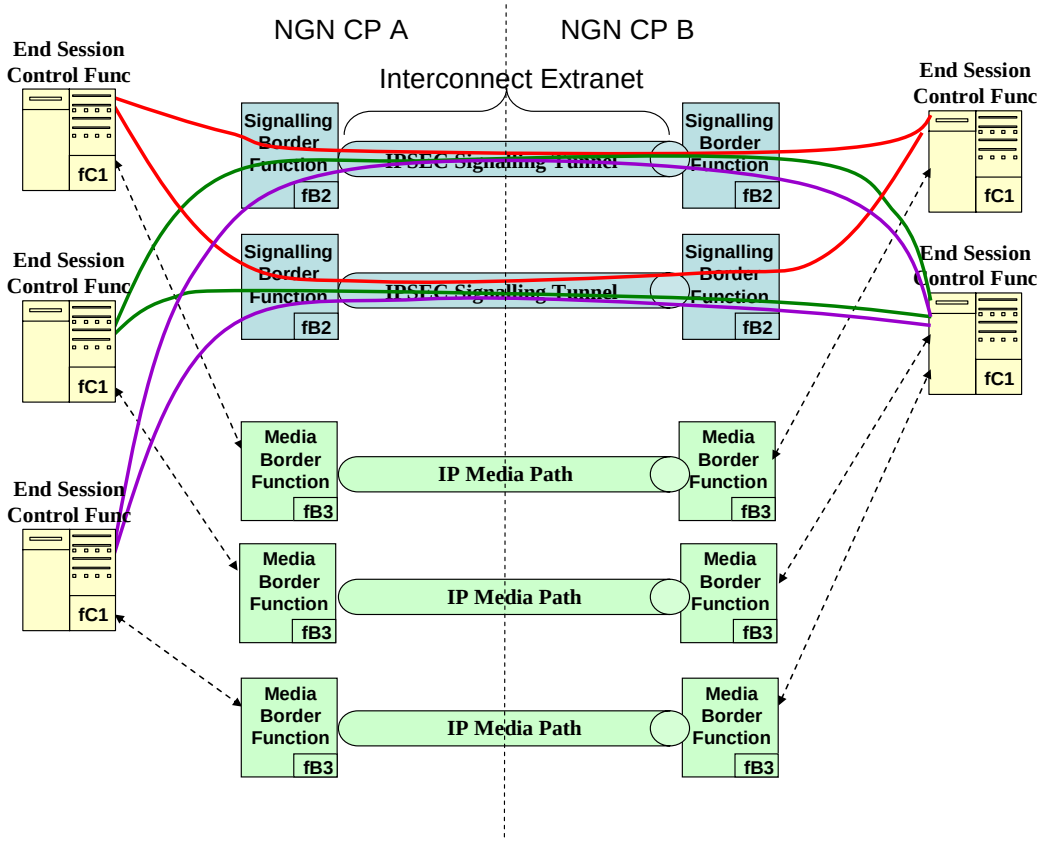
'Session Establishment' for PSTN/ISDN service between NGNs



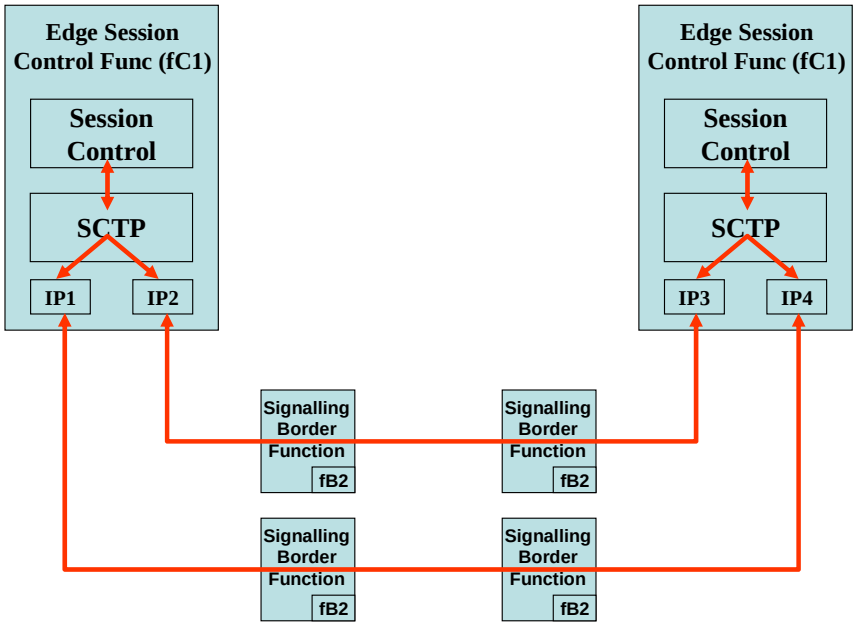
'Session Clearing' for PSTN/ISDN service between NGNs

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.



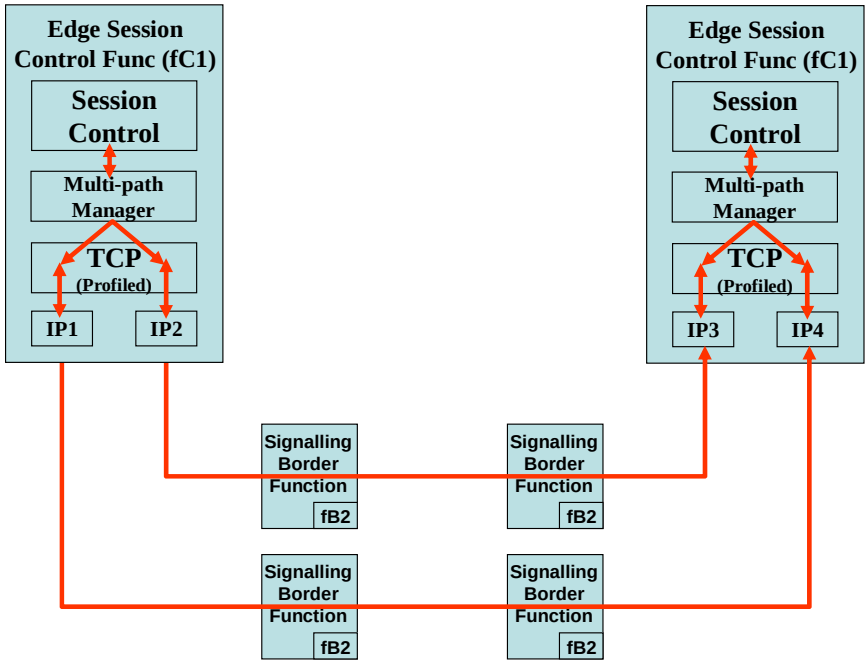
Annex C (informative): Example Schematic of SCTP Multi-PATH signalling Resilience



Annex D (informative):
Example Schematic of TCP Multi-PATH

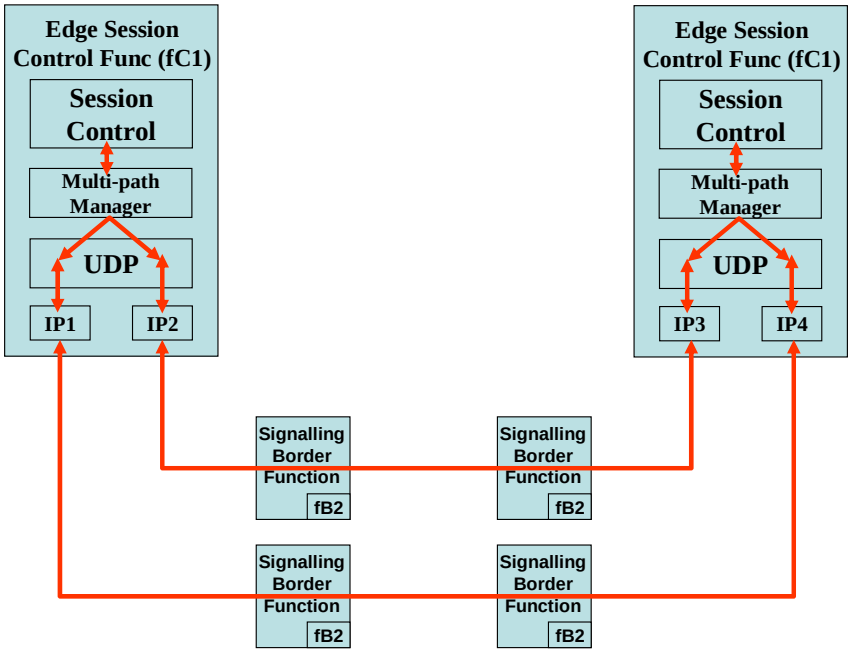
SIGNALLING RESILIENCE

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.



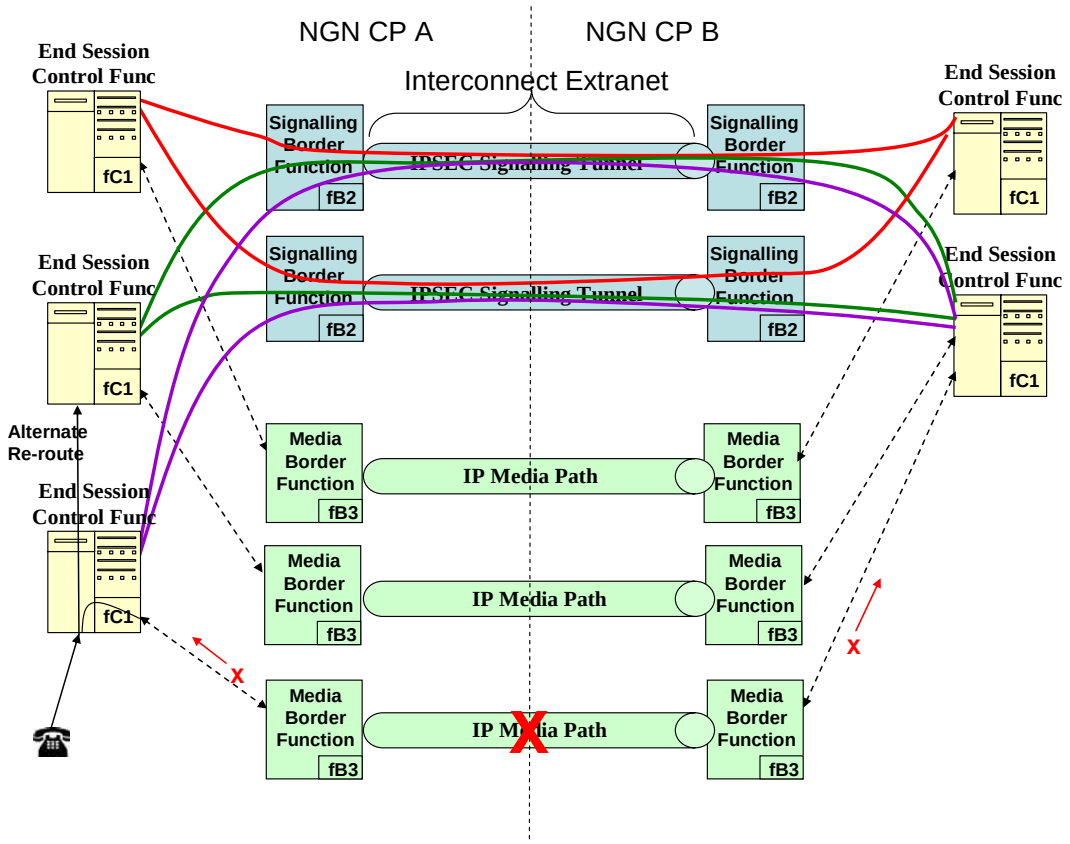
Annex E (informative):
Example Schematic of UDP Multi-Path signalling Resilience

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.



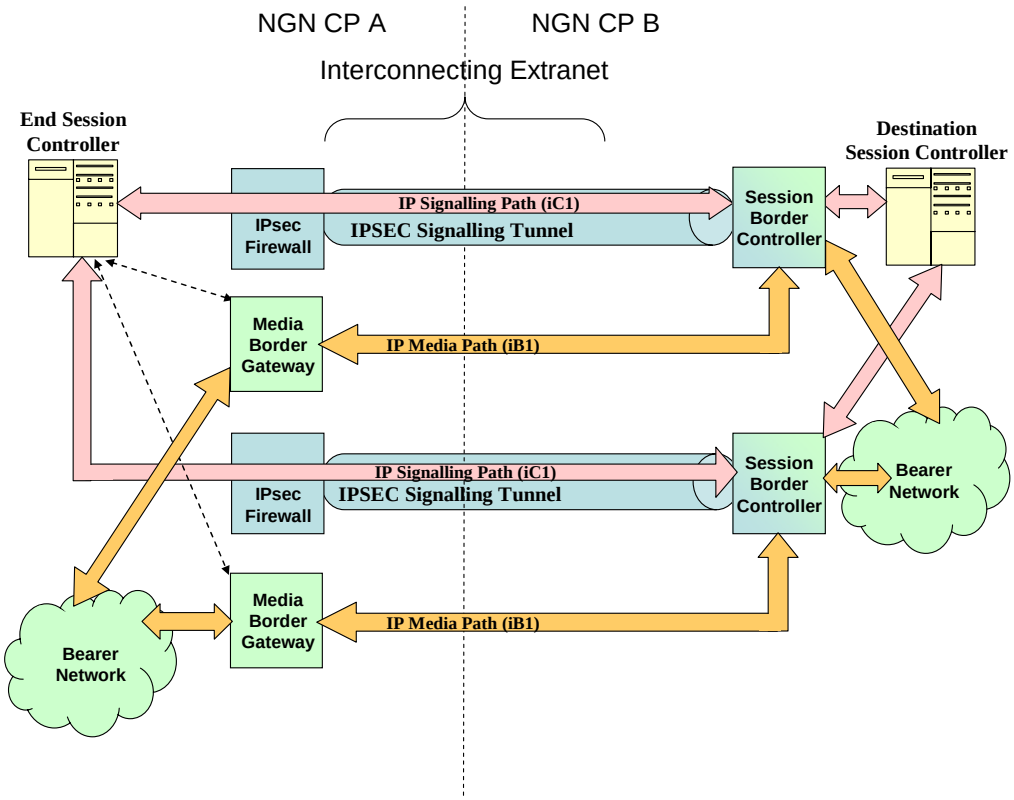
Annex G (informative): Example of Inter-working of Distributed and Integrated Interconnection Solutions

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

Document history		
Issue 1	02/05/2006	First issue
Issue 2	12/06/06	Updated to include new section 5, Interconnect Routes that Carry Priority Calls.
V1.2.1	May 08	Converted to NICC Version numbering scheme
V1.2.2	May 08	Converted to revised NICC ND template. Change to Section 4.4.2.2 on signalling transport protocols to be used.