NICC ND 1614 V 1.2.2 (2008-10)

NICC Document

NGN Interconnect:

PSTN/ISDN Service;
General Connectivity Management

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 the NICC TSG Management Working Group.

1 Scope

The scope of this specification is restricted to the management aspects of Purple Release PSTN/ISDN interconnect; the architecture and specification of generic connectivity for PSTN/ISDN service sessions are specified in [3], and the protocol and procedures for establishment of such sessions are defined in [5].

This document specifies management activities that require co-ordination between the two CPs operating the interconnect. Only processes that change significantly in the evolution from TDM interconnect to NGN interconnect are included. Only management activities relating to the operation of the PSTN/ISDN service are specified in this document; for management activities relating to the Transport Connectivity layer see [4].

2 References

For the particular version of a document applicable to this release see ND1610 [1].

2.1 Normative references

[1] ND1610 Multi-Service Interconnect of UK Next Generation Networks

[2] ND1611 Multi-Service NGN Interconnect: Common Transport

[3] ND1612 Generic IP Connectivity for PSTN/ISDN Service between UK Next Generation Networks

[4] ND1613 NGN Interconnect; Transport Service Layer Management

[5] ND1017 Interworking between Session Initiation Protocol (SIP) and UK ISDN User Part (UK-ISUP)

2.2 Informative references

[6] ND1628 Signalling Security

[7] ND1701 Recommended Standard for the UK National Transmission Plan, NICC

3 Abbreviations

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

ACC	Automatic Congestion Control
ATM	Asynchronous Transfer Mode
CDR	Call Details Record
CP	Communications Provider
CPS	Carrier Pre-Selection
DTMF	Dual Tone Multi-Frequency
ETSI	European Telecommunication Standards Institute
GNP	Geographic Number Portability
IA	Indirect Access
IP	Internet Protocol
ISDN	Integrated Services Digital Network*
ISUP	ISDN User Part of C7 signalling
ND	NICC Documentation
NGN	Next Generation Network
NGNP	Non-Geographic Number Portability
NICC	Network Interoperability Consultative Committee
PSTN	Public Switched Telephone Network*

QoS	Quality of Service
RTP	Real-time Transport Protocol
SDH	Synchronous Digital Hierarchy
SIP	Session Initiation Protocol
SIP-I	SIP with encapsulated ISUP
TDM	Time Division Multiplex
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
UK	United Kingdom
URI	Uniform Resource Identifier
VLAN	Virtual Local Area Network

* 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 Introduction

NGN interconnect management processes are those processes that are required to plan, establish and operate an NGN interconnect, and account for its usage. They are additional to the processes and procedures for actually using the interconnect.

This document identifies the processes, and associated data, needed to maintain operability of a generic connectivity for PSTN/ISDN service across a Next Generation Network, Multi-Service Interconnect.

5 Document Structure

The Purple Release NGN interconnect work [1] has only been scoped for the PSTN/ISDN emulation service, but the need to provide underlying transport functions that generically supported a range of services is recognised. This is represented in a number of functional layers as shown in figure 1. The transport layer provides physical connectivity based on various transmission technologies, e.g. SDH and Ethernet Physical. The transport capability layer offers a number of transport types with various characteristics, e.g. TDM, ATM, and IP to the services they support.

Although the scope of this Purple Release NICC work is confined to IP interconnect for the PSTN/ISDN emulation service, there is not one but many PSTN/ISDN interconnect products at the service level, e.g. Standard calls, CPS, Number Portability, Number Translation Services. To avoid redefining these products for the NGN environment, a PSTN Service Connectivity layer is defined that can serve these interconnect products and to connect them to the underlying transport capability. This layering is shown in Figure 1.

Product Layer	Geographic Calls, Non-Geographic Calls, GNP, NGNP, CPS, IA, etc
Generic Connectivity Layer	PSTN/ISDN, or Voice Line Access Connectivity. Controls Bearer Routes, Signalling Associations etc
Transport Capability Layer	IP over Ethernet VLAN, TDM, ATM Etc
Transmission Layer	SDH / Ethernet Physical

Figure 1:- Layering of functions for PSTN over a Multi-service Interconnect

Figure 2 shows interconnect functional layers overlaid with the broad areas of management activity. This document is concerned with the management activities at the PSTN/ISDN Connectivity Layer. For management areas related to the Transport Capability Layer see [4].

The section of this document where the management area is addressed is indicated in figure 2.

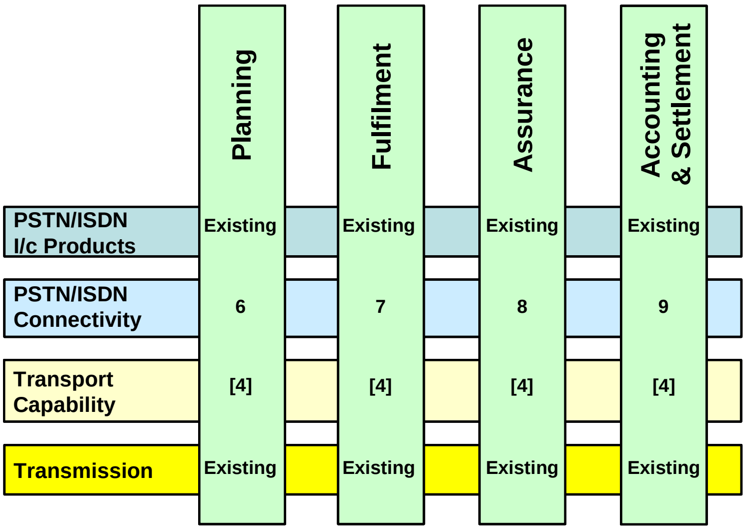

Figure 2:- Structure of NGN Interconnect Management areas

Note for clarity; [4] in figure 2 is a reference, not a section in this document. The numbers 6, 7, 8 and 9 refer to sections in this document.

6. Planning

6.1 Supported VLAN Sizes

The following two sets of VLAN bandwidth sizes **should** be supported for PSTN/ISDN Media and Signalling, where the numbers signify Mbps. Other VLAN sizes **may** be supported by bi-lateral agreement.

Supported PSTN/ISDN Signalling VLAN sizes (Mbps):

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
22	24	26	28	30					
32	34	36	38	40					
42	44	46	48	50					

Supported PSTN/ISDN Media VLAN sizes (Mbps):

	10	15	20	25	30	35	40	45	50
55	60	65	70	75	80	85	90	95	100
105	110	115	120	125	130	135	140	145	150
155	160	165	170	175	180	185	190	195	200
205	210	215	220	225	230	235	240	245	250
255	260	265	270	275	280	285	290	295	300
305	310	315	320	325	330	335	340	345	350
355	360	365	370	375	380	385	390	395	400
405	410	415	420	425	430	435	440	445	450
455	460	465	470	475	480	485	490	495	500
510	520	530	540	550	560	570	580	590	600
610	620	630	640	650	660	670	680	690	700
710	720	730	740	750	760	770	780	790	800

6.2 Sizing of PSTN/ISDN VLANs

6.2.1 Signalling VLANs

Signalling VLANs are provided between Signalling Border Functions, a Signalling VLAN can carry signalling between several combinations of Session Control Functions located behind the SBFs. A signalling VLAN shall therefore be dimensioned to carry all of the signalling between the combinations of SCFs that it is supporting.

There will usually be multiple pairs of SBFs used to carry signalling between two networks in order to provide the necessary signalling capacity between the networks, including in the event of failure. The VLANs interconnecting the SBFs must therefore be dimensioned appropriately for the signalling relationships that they are supporting. For example if an SBF-SBF Signalling VLAN fails then the affected signalling could be re-routed via other SBFs and the VLAN sizing will have to take into account the policies for re-routing the signalling in the event of failures e.g. is the load from 1 failed Signalling VLAN distributed across n remaining Signalling VLANs or is it all carried by 1 alternative Signalling VLAN.

Two scenarios where signalling load will be re-distributed are:

6.2.1.1 Failure of one path of a Multi-Homed SCTP Association

If one path of an association fails (with no failure the media path(s) that it is supporting) then its signalling load will transfer to the alternative SCTP path. Hence VLANs must be dimensioned assuming that the SCTP paths that they are supporting are carrying the total signalling load of the SCTP association.

6.2.1.2 Failure of media path(s)

If a media path, or paths, fail then re-routing at the application layer could take place. Hence a new SCF-SCF relationship could be used to support the media traffic from the failed path and hence there could be an increase in signalling between the SCFs involved, and consequently the Signalling VLAN(s) supporting this SCF-SCF relationship **shall** be dimensioned accordingly.

Significant co-operation between CPs will be required to achieve dimensioning of the signalling VLANs.

6.2.2 Media VLANs

6.2.2.1 Single Media VLAN between CPs

Where this is the only connection between CPs, this VLAN **shall** be dimensioned to carry all the traffic flowing between the CPs. In this scenario, the lack of media resilience **shall** be given consideration.

6.2.2.2 Multiple Media VLANs to Media Border Functions

Where a VLAN is one of two or many VLANs all terminating on different combinations of Media Border Functions, each VLAN **shall** be dimensioned according to planning rules to carry the traffic flowing between these Border Functions. E.g. one media VLAN should be dimensioned to carry its own traffic and, potentially, some or all of the traffic from a failed VLAN, according to the resilience agreements between CPs.

Significant co-operation between CPs will be required to achieve dimensioning of the media VLANs.

6.2.3 Detailed VLAN SIZING

6.2.3.1 Detailed Signalling VLAN Bandwidth Sizing

To calculate the bandwidth required to sustain a signalling VLAN between Communication Providers, a number of characteristics relating to interconnect must be analysed. The more important items are: Carried (agreed) Calling Rates, Number of media sessions in supported route(s), Call Hold Times, Signalling protocols to be used, e.g. SCTP, SIP-(I), IPSec, and interrelated messages conveyed for each of the transport and control layer parts of the protocols. Where SCTP is deployed as the transport mechanism, an association is established between two signalling end points. Each association may consist of more than one physical routed path for transporting the signalling messages and this is termed multi-homing. To ensure resilience, each path must be able to support all the traffic between the end points and it is a requirement that each path be sent via a separate VLAN.

At the points of interconnect, an MSIL is configured and connected between the respective providers. A number of Signalling VLANs could exist between the SBFs in each network. Each VLAN could be supporting a number of SCTP signalling association paths from a variety of source/destination pairs. Where multiple associations exist, the total Signalling VLAN bandwidth required must be derived by a summation of each of the individual paths between respective end points. (Note that although there could be more than one Signalling VLAN between any two signalling border functions, it is imperative that these are planned to ensure no single point of failure exists. Two, or more, paths of the same association must not be routed over the same Signalling VLAN or MSIL.) Finally, the Signalling Border Function in each respective network is responsible for grooming the appropriate signalling paths into the Signalling VLAN and implementing IPSec encryption between the providers.

When deploying a network interconnect that is likely to support a mixed calling pattern, perhaps based upon time of day, the most onerous mix and hold time must be applied to calculations to ensure that no congestion is encountered. As an example the following schematic illustrates possible interconnects between two providers:

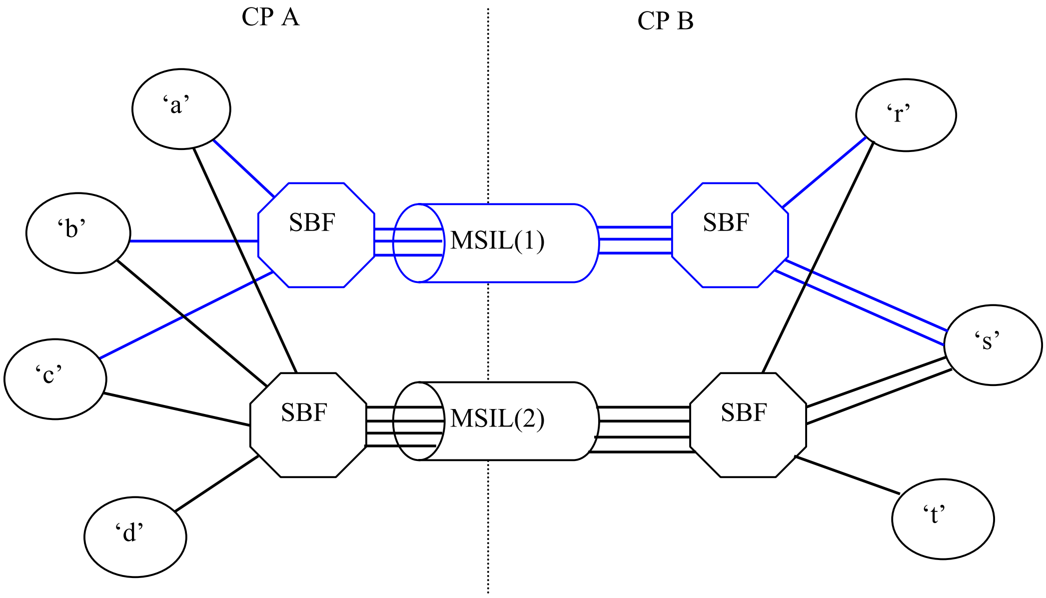

Figure 3. Schematic example of an interconnect

Where relationship:

"a:r" is a dual homed association between call servers at nodes 'a' and 'r'.

"b:s" and "c:s" are dual homed between call servers at 'b', 'c' and 's'.

"d:t" is a single homed association between call server at 'd' and 't'.

Bandwidth on an MSIL / SVLAN is the summation of individual element bandwidths supported on each association path that traverses the MSIL / SVLAN.

To calculate bandwidth required on MSIL (1).

$$\text{Total b/w on MSIL (1)} = \sum \left\{\text{b/w(a:r)} + \text{b/w(b:s)} + \text{b/w(c:s)}\right\}$$

To calculate bandwidth on MSIL (2), (that is provided to support 2nd path in the associations from 'a', 'b', and 'c' and the single path from 'd') utilises the same formula.

$$\text{Total b/w on MSIL (2)} = \sum \left\{\text{b/w(a:r)} + \text{b/w(b:s)} + \text{b/w(c:s)} + \text{b/w(d:t)}\right\}$$

To determine the bandwidth required for each path element, the following formula is used:

$$\text{Bandwidth per route} = \text{b/w (n:m)} = \frac{\text{Route size * Signalling per call * scaling}}{\text{Call hold time}}$$

Where:

Route size =	max concurrent calls on the media VLANs controlled over this path element (an integer value).
Signalling per call =	signalling bits per call in maximum direction (normally reverse direction unless overlap sending), including 72 octets per message overhead due to IPsec.
Scaling factor =	number
Call hold time =	average call holding time on the media VLAN in seconds, including failed calls.

Note with SIP-(I) there is no concept of a maximum route size, (although there may be a limit imposed by the underlying transport infrastructure), so this size is to be determined with a bi-lateral agreement between CPs.

Signalling per call is a value determined by measurement and other calculation to estimate the maximum required octets per call based on call type. For example, a typical basic call using en-bloc signalling requires approximately 7688 octets of signalling to set up, control, and clear the call (3338 forward and 4350 backward). A more complex call type i.e. one that uses overlap signalling may require as much as 50% more octets.

NB The signalling size shall include all protocol overheads for IPSEC, Ethernet, IP and SCTP and is not just the SIP(I) message size.

The scaling factor is used to ensure that some headroom exists to ensure that the variable arrival rate of call setup / clear can be supported. If a typical distribution is assumed then experience indicates that this must be a 5 times scaling factor. This would also allow for re-transmission of errored packets. Note that in a 'noisy' environment, due to the fact that the SIP-I packets are considerably longer than TDM, it is expected that they will be effected proportionately more and thus more re-transmission will be encountered on IP signalling routes. Other impact on the scaling factor may have to be determined from characteristics of Call Servers. For example in extremis if a Call Server was running at its maximum BHCA and had only a single destination available, all signalling would be conducted over a restricted number of paths that would necessarily need to be large.

Call Hold time in seconds determines the rapidity of the signalling sequence. An average call hold time of 3 minutes (180 seconds) can be assumed for most voice calls, but routes that support data only may have significantly longer hold times perhaps 20 minutes (1200 seconds) , whereas those that support televotes would be very much shorter, typically 6-10 seconds.

From measurements taken the following bandwidths are required to support a SIP-I interface. Three different call types are illustrated.

Messages, octet aggregation for a typical call.
SIP-I, (plus SCTP, IP, LLC/MAC and IPSec headers) in forward direction, = 3338
SIP-I, (plus SCTP, IP, LLC/MAC, and IPSec headers) in backward direction, = 4350

Messages, octet aggregation for a call utilising max length domain names.
SIP-I, (plus SCTP, IP, LLC/MAC and IPSec headers) in forward direction, = 4573
SIP-I, (plus SCTP, IP, LLC/MAC, and IPSec headers) in backward direction, = 5959

Messages, octet aggregation for a call with branch, tags, Call ID and Call Sequence.
SIP-I, (plus SCTP, IP, LLC/MAC and IPSec headers) in forward direction, = 4773
SIP-I, (plus SCTP, IP, LLC/MAC and IPSec headers) in backward direction, = 6220

Where the route size is an agreed integer figure between the providers; (and for the following examples is assumed to be equal to 3840).

Example simple calculations, based upon Figure 3.

Let route (a:r) be a televote route
Let route size = 3840
Let the calls require = 4350 octets each of signalling
Let the call hold time be typical = 10 seconds

$$\text{Bandwidth required} = \frac{3840 * (4350 * 8)*5}{10} = 66{,}816{,}000 \text{ bits per second}$$

Let route (b:s) be a voice call route
Let route size = 3840
Let the calls require = 5959 octets each of signalling
Let the call hold time be typical = 180 seconds

Bandwidth required = $\frac{3840 * (5959 * 8) * 5}{180}$ = 5,085,013 bits per second

Let route (c:s) be a data route with complete call set
Let route size = 3840
Let the calls require = 6220 octets each of signalling
Let the call hold time be typical = 1200 seconds

Bandwidth required = $\frac{3840 * (5959 * 8) * 5}{1200}$ = 762,752 bits per second

Let route (d:t) be a televote route..
Let route size = 3840
Let the calls require = 4703 octets each of signalling
Let the call hold time be typical = 10 seconds

Bandwidth required = $\frac{3840 * (6220 * 8) * 5}{10}$ = 95,539,200 bits per second

To calculate SVLAN bandwidth required via each MSIL indicated in figure 1.

Total b/w on MSIL (1) $= \Sigma \left\{ b/w(a{:}r) + b/w(b{:}s) + b/w(c{:}s) \right\}$
$= \Sigma \left\{ 66.82+5.09+0.76 \right\}$
$= 72.67$ Mbps

Total b/w on MSIL (2) $= \Sigma \left\{ b/w(a{:}r) + b/w(b{:}s) + b/w(c{:}s) + b/w(d{:}t) \right\}$
$= \Sigma \left\{ 66.82+5.09+0.76+95.54 \right\}$
$= 168.21$ Mbps

In this example above the greatest bandwidth is demanded on MSIL(2). Note in this calculation the call servers (‘d’ to ‘t’) on this SVLAN are single homed and do not have a resilient path via MSIL(1), it is acceptable to have different size MSIL and SVLAN scaling. However, if (‘d’ to ‘t’) was dual homed via both MSILs then each would need to be scaled to support 168.21 Mbps. This example illustrates that a worst case is due to short call hold times, large route sizes and high calling rates, as would be experienced during a typical national media promoted televote.

Caveat: The values of signalling octets used in these examples have been derived from actual measurements taken in good faith from model implementations of a SIP-(i) interconnect interface. The final calculation must use the full call flow information available for each CP implementation of the SIP-I interconnect protocol.

See also section 8.7.

6.2.3.2 Detailed Media VLAN Bandwidth Sizing

Constraints on Media VLAN fill for NGN interconnect of PSTN / ISDN Service.

6.2.3.2.1 Assumptions and Definitions

This section describes the set of assumptions and definitions associated with this recommendation on the constraints on VLAN fill for Media streams carried over PSTN/ISDN generic NGN interconnect. It also includes recommendations of the maximum fill for the Ethernet physical connection.

(i) Interconnect type:

This recommendation covers only Ethernet VLAN connections, with different service types in separate VLANs as described in ND1611 [2].

(ii) Ethernet Port-speed

The Ethernet physical connection , which may be shared by multiple VLANs, has a port-speed of 100Mbps or greater. N.B. As latency increases as port-speed is decreased, so more stringent rules would be necessary for lower rates.

(iii) Media traffic characteristics

Each individual Media session consists (at source) of packets of IP-size 120bytes, generated at intervals of 10ms. It is further assumed that packet-timings between packets in separate sessions are essentially uncorrelated at source gateways, i.e. packets from separate sessions are statistically independent in their timings, and not “clumped” together. Furthermore, no significant clumping is introduced by subsequent devices such as gateways or firewalls, beyond what is to be expected by network-layer queuing.

(iv) Use of Prioritisation

Either PSTN/ISDN Media VLANs are the only VLANs carried on the Ethernet port*, or packet queuing prioritisation (or similar) is used to limit the effects of other traffic types on Media VLANs. If relying on prioritisation, then the maximum frame-size of non-Media traffic is assumed to be no greater than 2000bytes, and the NGN interconnect implementation is assumed to be capable of limiting the latency/jitter induced by the total non-Media VLAN on the Media traffic to no more than about two packet-service times at Ethernet port-speed.

* Note: The condition “Media VLANs are the only VLANs carried on the Ethernet port” can be relaxed to include signalling VLANs as well, provided the total bandwidth of these is limited to no more than about 5% of port-speed. Furthermore, as well as Media packets, the Media VLANs themselves may also include RTCP traffic up to an assumed limit of 0.25%.

(v) Definition of VLAN bandwidth

In real-World implementations, policers and shapers are often configured or specified using a definition of bandwidth that accounts for the principal fields of the Ethernet frame, but excludes Preamble, SFD, and IFG. VLAN bandwidth is defined in [4] and follows this approach, accounting for the principal Ethernet fields, including one VLAN tag and FCS, but excludes Preamble, SFD and IFG.

A single G711 Media stream with 10ms framing interval consists of 120byte IP packets transmitted every 10ms, with a corresponding IP bandwidth of 96kbps. According to the definition in [4], with IP packets encapsulated within a single Ethernet VLAN, the frame size is considered to be and additional 22bytes, 142bytes in total, and the stream bandwidth is 113.6kbps. Though not included in the above definition, IFG, SFD, and Preamble are important for Capacity Planning when considering the total available bandwidth that may be assigned to VLANs on a particular Ethernet port. For the same example, the frame-size including these additional fields (of 24bytes) is 162bytes, and the stream bandwidth is 129.6kbps.

6.2.3.2.2 Constraints on VLAN fill

Case 1: No VLAN output shaping

This describes the case where either no shaping is applied on the output, or a shaper is used with a burst-tolerance that is large compared with the expected statistical bursting of the traffic carried, so having no effect on normal traffic.

Here the recommended maximum number of Media sessions **shall** be limited to generate no more than 98% of the VLAN bandwidth, in order to provide sufficient bandwidth for RTCP traffic with some additional margin. Thus:

Max-sessions =INT(0.98 x VLAN-size/113.6kbps)

Case 2: VLAN output shaping is used

Here VLAN shaping is assumed to act strictly, smoothing out bursting in traffic prior to output, so that the VLAN behaves more-or-less as a dedicated leased-line at the VLAN bandwidth.

Statistical variation in the arrival time of packets within individual VLANs is an expected natural occurrence, and leads to variations in the peak bandwidth evident on a fine timescale. The effect of smoothing this out is to introduce a corresponding jitter for individual sessions. The potential amount of jitter incurred is greater for VLANs of smaller bandwidth, with the effect increasing as VLAN fill is increased. Therefore, if it is required to restrict shaper-induced jitter to less than a specified target value, it is necessary to impose a restriction on the maximum fill that can be accommodated for VLANs below a certain size. The recommended target for maximum shaper-induced jitter is 2ms, and combining this objective with the 98% rule applied for Case 1 gives the recommended maximum fill values shown in Table 1.

VLAN size (Mbps)	***Max. permitted no. sessions***		***VLAN size (Mbps)***	***Max. permitted no. sessions***

1	2	30	258
2	4	35	301
3	6	40	345
4	11	45	388
5	18	50	431
6	25	60	517
7	34	70	603
8	43	80	690
9	52	90	776
10	61	100	862
12	81	120	1035
15	110	150	1294
20	161	200	1725
25	213		

Table 1: Max permitted no. sessions with shaper

This Table shows results for VLANs of up to 200Mbps, although for a 2ms limit, the additional constraint due to the shaper affects only VLANs below 30Mbps. For VLANs of 30Mbps or greater, the fomula given for Case 1 **should** be used. The VLAN sizes given in this Table are an example set, and intermediate VLAN values may be obtained through interpolation, though exact values **shall** be agreed between CPs to avoid any possible ambiguity.

The method used to derive this Table is as follows: Packet arrival times for Media traffic carried by the VLAN are assumed to follow N*D/D/1 statistics, where the term "N*D/D/1" characterises a well-know statistical process. To produce the Table, a pair of values was chosen, consisting of a target for the maximum shaper-induced delay (2ms) together with the probability by which this **should not** be exceeded (1E-9). Values were then derived for the largest number of sessions that may be accommodated for each VLAN bandwidth while meeting this target.

These results were combined with the "98% fill-rule", using the most binding figure of the two to give the maximum number of sessions.

6.2.3.2.3 Constraint on the sum of VLAN bandwidths

It is a clear aim of ND1611 that per-VLAN bandwidth management should be applied to prevent over-booking of the physical bandwidth resource. To this end it is essential that a rule is applied to limit the maximum single VLAN size for the case where only one VLAN is present, or the maximum sum of VLAN bandwidths for the case where several VLANs share the same Ethernet port. This rule must take account of all layer 2 overheads, including IFG, SFD, and Preamble, in order to derive the true layer2 bandwidth for each VLAN, to then ensure the sum is less than the Ethernet port bandwidth. For Media traffic the true layer 2 bandwidth **shall** be determined using the following:

VLAN-layer2-bandwidth = 1.141 x VLAN-size,

where the value 1.141 corresponds to the ratio 162/142 as discussed in the earlier section, "Definition of VLAN bandwidth". Note that VLANs for other services sharing the same Ethernet port **may** use different average packet-sizes, and may therefore define equivalent conversion formulae using different values of the constant.

To guard against transient interaction effects between VLANs it is recommended that the sum of layer 2 bandwidths across all VLANs **should** be limited to no more than 90% of the Ethernet capacity, unless there are clear reasons for larger values to be tolerated that are agreed between connecting CPs. For example, applying this rule to a 100Mbps Ethernet port would limit the maximum sum of Media VLANs to 78.9Mbps, assuming no other traffic is present. This is value is equal to: 0.9 x 100Mbps/1.141.

Note: This rule is intended as a cautionary measure for general application to guard against transient contention where VLANs are present from multiple services. Because it cannot be assumed that CPs will apply strict shaping to each VLAN, there is potential for transient congestion between VLANs. But it should be recognised that the 90% rule may be unnecessarily restrictive in some cases, for example, when an interconnect is dedicated to a single service. Exact specification of conditions and value for a more relaxed constraint is beyond the scope of a concise recommendation, but it is acknowledged that connecting CPs may agree to use larger values under some circumstances. Each CP should determine the maximum limit for one traffic direction (i.e. traffic egressing from their network), and the combined limit should be the minimum of the limits of two CPs).

7. Fulfillment

7.1 Information exchanged prior to service establishment

This section identifies information which may be exchanged between CPs operating the NGN interconnect prior to service establishment. A subset of this information **may** also be exchanged prior to changing details of the interconnect (for example, bandwidth).

7.1.1 General Background

Item 7.1.1.1 Company name and address

Item 7.1.1.2 Contact (name, address, phone, mobile, email) **details for:**
Commercial,
Technical,
Operational,
Fraud & Security,
Order reference number,
Billing queries.

Item 7.1.1.3 Ready for service target date.

7.1.2 Transmission and Transport

These aspects are covered in ND1613 [4].

7.1.3 PSTN/ISDN Connectivity

Item 7.1.3.1 Interconnect equipment configuration details
Type, model, build and location of the point of handover for the Edge Session Controller
Type, model, build and location of the point of handover for the IP Media Border Function
Type, model, build and location of the point of handover for the Signalling Border Function - Note this information **may** be withheld for security reasons.

Item 7.1.3.2 Interconnect configuration approval test
Has configuration been type approved for interconnection?
Name of Approver
Date of approval
Constraints on approved use

Item 7.1.3.3 Use of Transport layer
Mapping of IP subnet/VLAN(s) to transmission infrastructure identifiers (e.g. fibre numbers) as listed in ND1613 [4].
Mapping of signalling to IP subnet / VLAN(s)
Mapping of media to IP subnet / VLAN(s)
Is IPSec required on the VLAN? Refer to [6] for information to be exchanged for IPSec.

Item 7.1.3.4 Addressing Information
Agreement on who is providing IP addresses (Section 7.2 ND1612 [3]).
IP subnet addresses and allocation
SIP and RTP port ranges
SIP URI to IP mapping
P-Charging-Vector (including Originating Inter-Operator Identifier and icid-gen-addr).

Note on the use of P-Charging Vector: P-Charging-Vector values received across this interconnect might not have been generated by the interconnecting node, or even the interconnecting network. However, on initial interconnect establishment between two CPs, it may be valuable to swap the network identifying component of the P-Charging-Vector, as this information may not otherwise be known to the other party.

It is recommended that CPs additionally exchange the icid-gen-addr of the interconnected nodes. This could assist future fault resolution, and could potentially assist interconnect testing.

Item 7.1.3.5 Media characteristics
Voice codec and packet size (for supported values see [3])
DTMF digit transport mechanism (currently only in-band)
Support of T.38 or V.150 required (currently not supported)
Silence suppression used (currently not supported)

Item 7.1.3.6 Protocol support
SIP transport protocol and version
SIP profile supported.
IPsec profile supported

Item 7.1.3.7 Other technical information
Confirm support for ISUP ACC or Adaptive ACC congestion control.
Is Overlap signalling required? Note – en-bloc signalling is the default.
Call Identity information.

7.1.4 PSTN/ISDN Product

Please refer to the Interconnect Contract that exists between CPs for information on the following aspects –

- Product and Service types
- PSTN and ISDN routeing level information
- Bearer services
- Capacity forecasts

7.2 Security arrangements

The document "Signalling Security across NGN Interconnect" [6] requires the use of IPSec on signalling VLANs across NGN MSILs, except in certain circumstances, as defined in [6].

The document "Signalling Security across NGN Interconnect" [6] defines:

- The characteristics of the IPSec security used on the signalling VLAN.
- The IPSec parameters to be exchanged on establishing NGN interconnect.
- The frequency of key renegotiation.

8. Assurance

8.1 IP Media Border Function isolation

ND1612 [3] contains a full detailed explanation of the management procedures in this section.

Where a failure affects an interconnect-controlling functional node on the sending side of a call, then the sending network **should** detect this failure and **should** avoid routeing calls across the interconnect. If a failure affects signalling or media paths across the interconnect, the sending side **may** detect this situation (by the mechanisms defined in [3]) and the sending end will avoid the failed interconnect. Where a failure affects a functional node on the remote side of an interconnect, the sending side **may** detect this by the consequent failure of either the signalling or the media path, and will avoid routeing calls across the interconnect.

Where communication has been lost between the receiving IP Media Border function and its Edge Session Control Function, the sending side may not be able to detect this before routeing a call across an interconnect. The mechanism for rejecting such calls is defined in [3], and uses SIP 503 responses.

From an interconnect management perspective, the receipt of a 503 response **should** be reported via an alarm. If a subsequent SIP Invite, sent after the 'Retry-After' timer defined in [3] has expired, is successful, the alarm **should** be cleared. Persistence of 503 responses **should** raise the severity of the alarm, and operational intervention **may** be needed to correct the fault.

Once the fault has been rectified in the receiving network, operational staff should be aware that traffic **cannot** flow again until the current 'Retry-After' timer has expired.

8.2 Overload Protection Mechanism

ND1612 [3] contains a full detailed explanation of the management aspects in this section.

The Media Stream (iT4b) [3] is protected from overload by the Bandwidth Management Function, and hence the IP Media Border Function is also protected from overload (assuming correct dimensioning).

Although Bandwidth Managers **may** protect Edge Session Controllers from having to control too many simultaneous sessions, the limiting factor for an Edge Session Controller is not normally the number of simultaneous sessions, but rather the rate at which sessions are set up, i.e. the rate at which Invites are received. The Signalling Border Function **may** provide some protection against such signalling overload, but this is not one of its intended functions, and most Signalling Border Elements will transport more traffic than the Edge Session Controller can handle; further a single Edge session Controller may receive traffic from several Signalling Border Functions.

In the absence of overload control mechanism native to SIP, the ISUP ACC or Adaptive ACC mechanism **should** be used to allow an Edge Session Control Function to request a reduction in the rate it receives traffic from across an interconnect. See reference [3] section 4.4.2.7, use of UK-ISUP ACC, and reference [5].

In initial service establishment CPs **should** verify that the interconnecting network supports the reduction of traffic on receiving ACC. If the ACC procedure is not supported sufficiently to protect the receiving Edge Session Controller, it **may** be necessary to restrict the traffic across the interconnect by imposing a low bandwidth on the media across the interconnect.

8.3 Emergency Calls that Require Priority Treatment

The identification of these calls is covered in ND1612 [3].

8.3.1 Identification of Priority Calls

Examples of priority destination numbers are:

- 999
- 112
- 18000 (Text Phone)
- others agreed bilaterally by the CPs.

Calls to other numbers **may** be identified as priority calls by setting the priority indication in the signalling as defined in reference [5].

8.3.2 Treatment of Priority Calls

On detecting that a call is a priority call, the originating Session Control Function **shall** set the priority indication in the signalling as defined in reference [5].

A priority call **shall not** be discarded due to Call Gapping or other overload protection mechanisms, as specified in [3], unless the overload is caused by the volume of priority calls.

8.3.3 Reservation of Capacity for Priority Calls

This is detailed in ND1612 [3], however the following information **may** be used.

CPs **shall** agree a mechanism to avoid discarding priority calls across Next Generation Network interconnects due to congestion of media paths.

Such a mechanism **may** be:

- reserving bandwidth for priority calls, the specified default in reference [3];
- allocating separate routes for priority calls;
- some other bilaterally agreed means.

8.4 Graceful Removal of Traffic

8.4.1 Overview

For operational reasons it may be necessary to remove traffic from a media path, e.g. before deactivating an IP Media Function. To achieve this, traffic **shall** be allowed to decay over the connection for a time Tdecay, after which traffic still using the connection **may** be cleared. Following expiry of timer Tdecay remaining calls **should** be examined to check they are not life-line calls. This **may** be done manually. The remaining calls **may** be cleared by using the procedures for call release defined in [3] and [5].

During the traffic decay period the Edge Session Control Function **shall** avoid originating new sessions using the specified media path, and **shall** reject received session invites using the procedure defined in [3]. Existing PSTN/ISDN connections using the media path **shall not** be affected before expiry of timer Tdecay, and may complete normally before that time.

8.5 Information passed for fault reporting

Management processes between CPs need to exist to allow the CPs to inform one another about faults impacting the interconnect, to react to the faults, minimise the fault impact and correct the underlying problem.

8.5.1 Fault Categorisation

Faults at the PSTN/ISDN Service Connectivity layer can be categorised as being related to the:

- Signalling interface (iT4a) [3];
- Media transport (iT4b) [3];
- Signalling Control (iC1) [3]; or
- Media stream (iB1) [3].

8.5.2 Examples of Faults

Examples of faults in each category are given below:

Signalling interface (iT4a):

- Failure of signalling transport.

Media stream transport (iT4b):

- Failure of media transport.
- Congestion of media transport.
- Isolation of IP media border function.

Signalling Control (iC1):

- Circular routeing.

- Unsupported media type requested.
- Invalid traffic/product type received (e.g. emergency call received when not supported across the interconnect).
- Routeing errors.

Media stream (iB1):

- Deterioration of call quality.
- One-way speech path.

8.5.3 Information to report per fault category

Table 1 shows a typical information report. Further details and information can be found in the relevant O&M manual.

Item		**iT4a**	**iT4b**	**iC1**	**iB1**
Item 6.1.1.1	Company name and address	Y	Y	Y	Y
Item 7.1.1.2	Contact (name, address, phone, mobile, email) details	Y	Y	Y	Y
Item 7.1.1.3	Ready for service target date.				
Item 7.1.3.1	Interconnect equipment configuration details				
Item 7.1.3.2	Interconnect configuration approval test				
Item 7.1.3.3	Use of Transport layer	Y	Y	Y	Y
Item 7.1.3.4	Addressing Information	Y	Y	Y	Y
Item 7.1.3.5	Media characteristics			Y	Y
Item 7.1.3.6	Protocol support			Y	
Item 7.1.3.7	Other technical information			Y	
Item 7.1.4.1	Product and Service types			Y	
Item 7.1.4.2	PSTN and ISDN routeing level information			Y	
Item 7.1.4.3	Bearer services			Y	
Item 7.1.4.4	Capacity forecasts		Y	Y	Y
Item 7.5.3.1	Details of the actual problem, including which service(s) are affected.				
Item 7.5.3.2	When did the problem start?				
Item 7.5.3.3	Is it intermittent or affecting every call, time of day, high or Item 6.5 low traffic volumes?				
Item 7.5.3.4	If a routing problem, are the calls failing or being routed incorrectly?				
Item 7.5.3.5	Exchange of fault references.				
Item 7.5.3.6	Where appropriate, calling and called number details.				

Table 1. This table contains examples of fields that may be completed.

8.6 Monitoring and reporting of Call Quality

CPs **should** track call quality within their networks, and (as far as possible) on calls to and from interconnected networks. End-to-end call quality **may** also be measured. Activities which CPs could undertake to track QoS levels could be: automatic periodic QoS test calls across various portions of the network and across NGN interconnects; RTP signalling monitoring; QoS level recording in CDRs, maintaining a method for customers to report call quality problems.

Where call quality falls below the expected quality, and particularly where National Transmission Plan [7] criteria are not met, the condition **shall** be treated as a fault and investigated, including reporting the fault to interconnect partners.

8.7 Monitoring of VLAN Capacity Usage

This aspect is subject to ongoing modelling and is still under consideration with Consult21.

See also section 6.2.3.

9. Accounting and Settlement

9.1 Start of Charging

No change is proposed to the current arrangements for the start of charging.

However it should be noted that SIP provides two signals which could be used in conjunction with the call charging function:

i) The 200 OK message to the INVITE, which is analogous to the ISUP Answer message and in SIP-I carries the encapsulated ISUP Answer message, and

ii) The Acknowledgement message to the 200 OK message, which has no equivalent in ISUP.

CPs **should** note the presence or absence of a 200 OK Ack on answered calls. While the absence of a 200 OK Ack is a condition which can occur, for example if the calling party clears down before the answer signal reaches the originating Call Server, persistent or high volumes of answered calls missing 200 OK Acks could indicate misuse, and CPs **should** treat such conditions appropriately, and inform affected interconnect partners.

History.

Document history		
Issue 1	December 2006	Initial issue
v1.2.1	October 2008	Clarifications and alignment with Green release
V1.2.2	December 2008	Update to correct references.