New Zealand Telecommunications Forum

IP Interconnection for Voice Technical Standards

("Technical Standards")

Guideline Status:	**V2 Approved**
Classification:	Industry Standard
Date:	August 2026

A. DEFINED TERMS

In these Technical Standards, unless the context otherwise requires the following defined terms apply.

AF (Assured Forwarding)	Assured Forwarding consists of Service Classes within the Diffserv (DSCP) architecture. AF comprises Classes 1 through 4, and within each class, there are three drop precedence's. Assured Forwarding PHB is suggested for applications that require a better reliability than the best-effort service.
Asymmetric Traffic Flow or Asymmetry	Means traffic forwarded from the first device to the second device may travel a different route than traffic forwarded in a second direction from the second device to the first device.
Best Efforts	Service Class 0 under the Diffserv architecture. DSCP value = 0
Differentiated Services Code Point (DSCP)	A value used under the Diffserv architecture to specify different service classes. It is a 6-bit field in the header of IP packets for packet classification purposes. DSCP replaces the outdated IP precedence, a 3-bit field in the Type of Service byte of the IP header originally used to classify and prioritize types of traffic.
End User Migration	Means the migration of a carrier's own customers from one technology to another.
Expedited Forwarding (EF)	Is a Service Class that has DSCP markings set to decimal 46 or binary 101110.
IP Packet Delay Variation (IPDV) (Jitter)	Means the difference in end-to-end delay between selected packets in a flow with any lost packets being ignored.[1] Sometimes referred to as 'jitter'.
IP Packet Loss (IPpacketLR) (IPLR)	Means the ratio of total lost IP packet outcomes to total transmitted IP packets in a population of interest.[2]
IP Transfer Delay (IPTD) (Latency)	Means the average time a network takes to transfer packets between two Measurement Points.[3]
Layer	Means the layer (1 of 7) referred to in the Open Systems Interconnection basic reference model (the OSI Model)[4] where each layer in the model performs a specific function as shown in the table below. The IPWP proposes the IP Interconnection Technical Standards deals with Layers 1, 2 and 3.

OSI Model			
	Data unit	**Layer**	**Function**
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation and encryption
		5. Session	Interhost communication
	Segment	4. Transport	End-to-end connections and reliability

1 Source: http://en.wikipedia.org/wiki/Packet_delay_variation

2 Source: http:// portal.etsi.org/docbox/workshop/2008/2008_06_stqworkshop/cini_salvatore_dantonio.pdf –slide 14

3 Source: www.mcs.vuw.ac.nz/courses/COMP414/2007T1/assignments/ass3/Precise-QoSIPbasedNetworks-seby.doc

4 Source: http://www.itu.int/rec/T-REC-X.200-199407-I/en

	Media layers	Packet	3. Network[5]	Path determination and logical addressing
		Frame	2. Data Link	Physical addressing (MAC & LLC)
		Bit	1. Physical	Media, signal and binary transmission

Table source: Wikipedia

NNI (Network to Network Interface)	Means the boundary or point of interaction between network service providers. The NNI is both a physical and logical point of demarcation. The NNI serves the technical boundary where protocol issues are resolved and as the point of division between the responsibilities of the individual service providers. NNIs are defined for asynchronous transfer mode (ATM) and frame relay, as examples[6].
QoS (Quality of Service)	Means the resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.[7]
Service Migration	Means the migration of the various call types and services from TDM to VoIP.
Symmetric Traffic Flow or Symmetry	Means the relationship of information flow between two (or more) access points or reference points involved in a communication. It characterizes the structure associated with a telecommunication service or a connection. Values associated with this attribute are unidirectional, bidirectional symmetric, and bidirectional asymmetric.[8]
TDM (Time Division Multiplexing)	Is a scheme in which numerous signals are combined for transmission on a single communications line or channel. Each signal is broken up into many segments, each having very short duration.
Trans-coding	Means the direct digital-to-digital conversion of one encoding to another. This is usually done to incompatible or obsolete data in order to convert it into a more suitable format. When trans-coding one lossy file to another, the process almost always introduces generation loss.[9]
Transport provider	Means any network operator that transports IP service traffic between another provider(s) network without providing the IP service itself. This includes bi-lateral interconnection between two service providers as well as interconnection of sites for a single service provider. A 'Transport' situation is where two parties at each end of the transport are in control of the impairments. No requirement for flow awareness to exist.
Transit provider	Means any network operator that provides IP service application(s) for more than two service providers to interconnect with each other. A 'Transit' situation is where two parties at each end may not be in control and a (third party) transit provider may be. No single party has admission control and flow awareness may be more likely to be required.
Transition	Means the transition of a carrier's interconnect network from TDM to IP Interconnect.
UNI (User to Network Interface)	Is a demarcation point between the responsibility of the service provider and the responsibility of the subscriber.[10]

5 Sometimes referred to as the IP layer.

6 Source: http://www.yourdictionary.com/nni

7 Source: http://en.wikipedia.org/wiki/Quality_of_service

8 Source: http://www.its.bldrdoc.gov/projects/devglossary/_symmetry.html

9 Source: http://en.wikipedia.org/wiki/Transcode

10 http://en.wikipedia.org/wiki/User-Network_Interface

URI (Uniform Resource Identifier)	Is a generic term for all kinds of object-identifiers used on the Internet, including web page addresses (URLs) and email addresses.

B. INTRODUCTION

1. Purpose

1.1 As operators deploy IP networks, the need arises to interconnect those networks to enable end to end service delivery across multiple networks.

1.2 The purpose of this document is to provide Technical Standards for VoIP that work for most call types; minimise the requirement for customisation between New Zealand telecommunications providers and reduce the potential cost of interconnecting.

1.3 These guidelines are intended as a minimum set of standards. Interconnecting carriers are free to build additional requirements upon these Technical Standards.

2. Scope and Objectives

2.1 SCOPE

2.1.1 These Technical Standards provide:

- i. Principles to guide the technical design of an IP Interconnect NNI
- ii. Recommended minimum technical requirements for IP interconnect for VoIP; and
- iii. Information for operators who deploy or plan to deploy an IP network on issues relating to low speed data modem services.

2.2 OBJECTIVES

2.2.1 To define a generic, service agnostic, interconnection framework capable of supporting multiple service classes.

2.2.2 To define minimum national standards for IP voice interconnection (VoIP).

2.2.3 To provide a prescriptive standard such that a single implementation following this standard should be sufficient for successful interconnection with all other carriers.

2.3 SCOPE EXCLUSIONS

2.3.1 These IP Interconnect Standards do not apply to:

- i. Lawful interception
- ii. ‘A’ number manipulation
- iii. Any commercial aspects of IP Interconnection
- iv. End User Migration within a carrier’s own network
- v. The Technical Standards:
  - a. Shall not address and/or resolve telecommunication policy issues,
  - b. Shall not address and/or resolve cost and cost recovery issues, and
  - c. Shall not address and/or resolve network technology issues that are entirely within the domain of an individual carrier, (i.e. intra-carrier network technology issues are not within the scope of the guidelines).

2.4 COMPLIANCE

2.4.1 The Code Compliance Framework specifically lists TCF Standards and TCF Guidelines as out of scope of the CCF, as per the below excerpt:

> *7. Exclusions from Scope*
> *7.1. This CCF does not apply to:*

7.1.1 TCF Standards or TCF Guidelines, which are a set of general recommendations that are non-binding;

2.5 TRANSITION PLANS

2.5.1 This standard is intended be adopted in whole by all carriers to avoid the additional effort of specific interworking variations which are different for each carrier. However, it is recognised that there may need to be a transitional period required to bring the interconnection implementation up to the standard in all areas. Please see Principle 3.10.

2.5.2 Where a transitional period is required then a Transition Plan is agreed between the two interconnect parties providing the technical details of any variation required from the standard and the length of time it will apply.

2.5.3 The Transition Plan:

- 2.5.3.1 Is agreed between two parties only.
- 2.5.3.2 Provides the technical details of each variation required.
- 2.5.3.3 Provides the timeframe for which each variation will apply.
- 2.5.3.4 Provides the transitional activities and plan to be undertaken to meet the standard.
- 2.5.3.5 Is valid for a maximum of 12 months. Any additional transition activities beyond 12 months are reagreed in a new Transition Plan.

3. Principles Guiding the Technical Design

3.1 #1: SUPPORT FOR COMMERCIAL CONSTRUCTS

3.1.1 The IP Interconnect NNI design does not unduly limit the commercial models and ICAs that can be enacted over that NNI.

3.1.2 The NNI technical design is distinct from Interconnect Agreement (ICA) commercial models.

3.2 #2: VOICE IS THE IMMEDIATE GOAL

3.2.1 This standard defines an NNI that is able to support VoIP calls. The NNI design does not preclude future enhanced services that may run over the same NNI.

3.3 #3: CALL TYPES SUPPORTED WILL BE SPECIFIED

3.3.1 The supported call types are specified in the standard.

3.4 #4: FREEDOM TO CHOOSE POIS

3.4.1 The standard supports Carriers to be free to determine their own points of interconnection and associated free traffic zones.

3.5 #5: INTERCONNECTION POINTS MAY DIFFER DEPENDING ON SERVICE TYPES OR NETWORK TYPES

3.5.1 Only voice services are determined in this standard

3.6 #6: TRANSPORT AND TRANSIT SERVICES WILL BE SUPPORTED

3.6.1 Carriers will have the freedom to offer fewer interconnection points than Local IP Catchment Zones. Carriers also have the freedom to build to all, some or none of another carrier's advertised interconnection points. The NNI design supports the concept of transit networks.

3.6.2 It is a requirement that all number ranges allocated by the NAD to a carrier intended for public customer use are reachable across the interconnect domain. While 3.6.1 allows the ability to choose interconnect points with commercial freedom it does not remove the responsibility of the carrier who owns a public number range to ensure that the number range is reachable from all other interconnect points either directly or via a proxy transit routing function by another carrier agreement. This routing check should be triggered as part of the PNCA process.

3.6.3 Note: some number ranges are exclusively allocated to a carrier for internal use only and are not exposed as routable destinations. These number ranges are allocated such that they cannot be used or routed across other carrier networks. A PNCA is not issued for these exclusive internal number ranges.

3.7 #7: CALL QUALITY BUDGET WILL BE ALLOCATED AMONG CARRIERS

3.7.1 There is a finite budget of latency available to be consumed by carriers' networks while maintaining voice quality. The NNI design addresses the assignment of this budget for calls between different network types, including transit networks.

3.8 #8: MINIMUM CODECS SUPPORTED WILL BE SPECIFIED

3.8.1 The NNI design allows CODECs to be negotiated bilaterally by carriers. Transcoding should be minimized.

3.8.2 G.711a is the only mandatory codec to be supported over the IP Interconnect. This supports a good quality voice call as well as simple dial up data and fax while they remain required services.

3.9 #9: THE NNI DESIGN SHOULD NOT BE UNDULY OPTIMIZED

3.9.1 The NNI design is non-restrictive regarding end subscriber type. It supports call types and commercial models between mobile, VoIP, and PSTN subscribers.

3.10 #10: NNI DESIGN SHOULD NOT DICTATE TRANSITION PLANS

3.10.1 The NNI design does not define transition plans. It specifies an IP interconnect standard for VoIP between two carriers. The interconnect parties will need to agree between themselves as to how they will migrate traffic from existing interconnect mechanisms to the new IP interconnect while also avoiding any outages to calling traffic and maintaining reachability to public number ranges.

3.11 #11: LOCATION INFORMATION SHOULD BE PRESERVED ACROSS THE NNI

3.11.1 The design allows the passing of location information within SIP messages. No other mechanism is provided.

3.12 #12: A DEFAULT SIP MESSAGE SET WILL BE DEFINED

3.12.1 The design includes a baseline SIP messaging set that is as open as possible.

3.13 #13: SOME PROBLEMS ARE BEYOND THE SCOPE OF THE NNI DESIGN

3.13.1 The NNI design supports basic voice calling. Other aspects of voice operations within or across carries is not included.

4. References

4.1 Other TCF Codes and Standards of relevance to those deploying IP Networks include:

i. Emergency Services Calling Code

ii. Terms for Local and Mobile Number Portability in New Zealand (“LMNP Terms”)

C. TECHNICAL STANDARDS - LAYERS 1, 2 & 3

5. Layers 1 and 2

This section defines the IP connectivity requirement.

5.1 LAYER 1 – PHYSICAL CONNECTIVITY

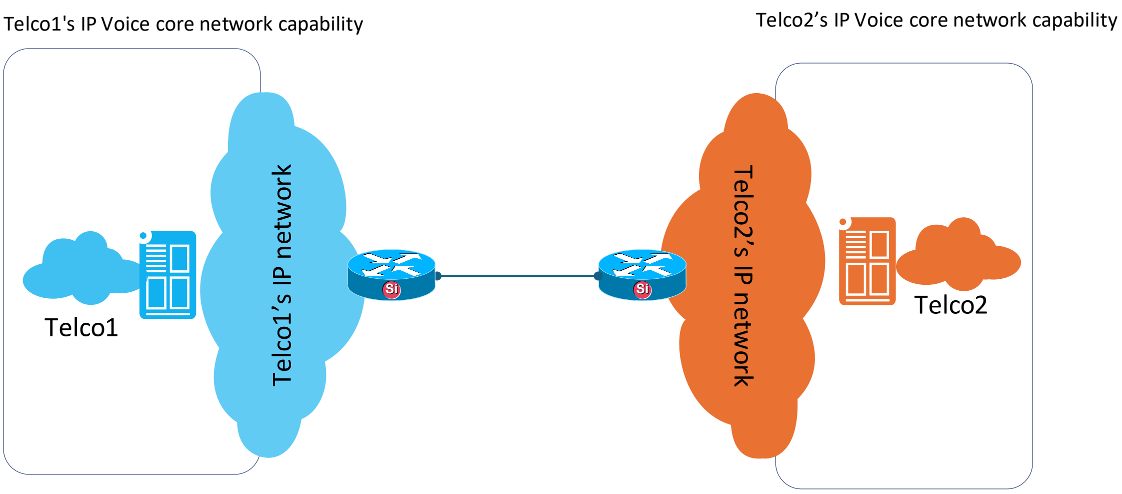
There are two instances of network interconnection required. These are:

1. Model/Lab Environment Network
2. Production Environment Network

5.1.1 Model

The model/lab network shall be implemented with a single connection via a 10Gbps fibre optic link rate limited to 1Gbps. This may be implemented on the production equipment but must be independent of production call flow before acceptance. The model connection may share the same physical path as a Production link but must be separated by VLAN ID or a similar construct at the transport layer or interface.

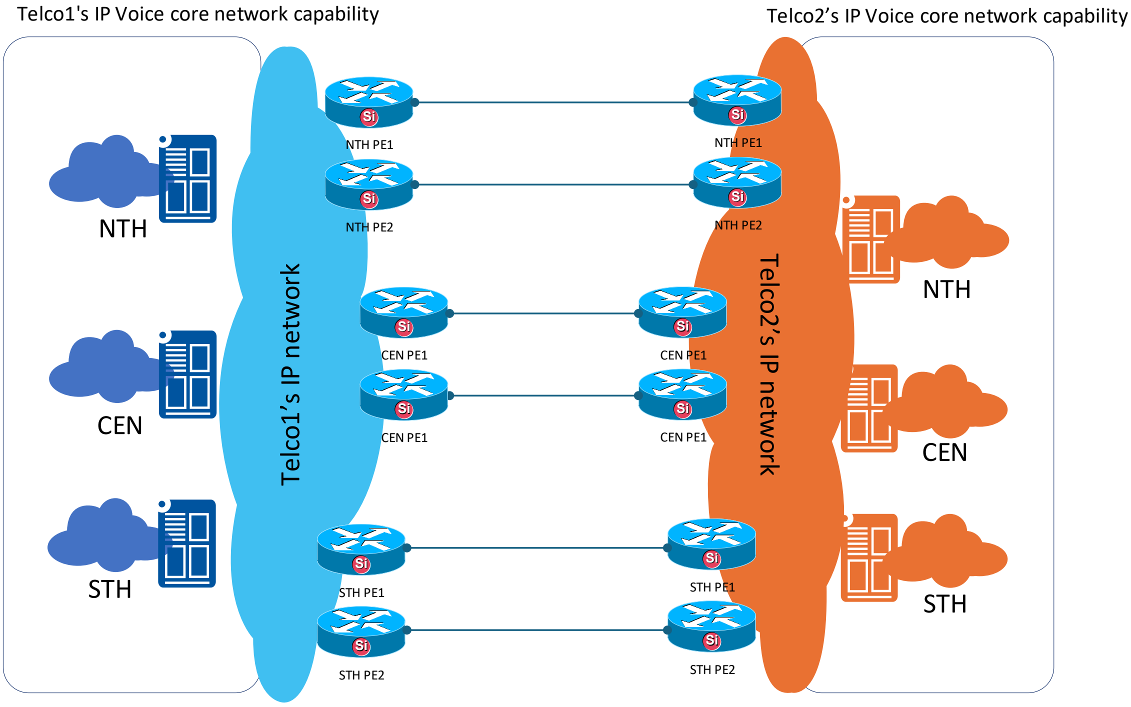
Example Model Diagram



5.1.2 Production

The Production network shall be implemented with ideally redundant links at each interconnect centre and preferably with no less than three interconnect centres spread across the geography of New Zealand. An example is using Auckland, Wellington and Christchurch as interconnect centres with dual 10 Gbps links at each centre.

Example Production Diagram



This design provides the continuation of robust communications in the event of a significant geographical event (e.g. earthquakes or volcanoes, weather events) and also provides significant capacity to allow successful bursting of call volumes in the event of significant national events (eg Covid lockdown announcements).

The interconnect design agreement between the parties shall list the interconnect device names and ports and physical locations for each side of a link for each party.

Example Table diagram – Hostnames and port allocations to be defined in the Interconnect Agreement between the parties

(One table for each Telco)

Telco Production Device Location

Telco1 PE Router	Hostname	Port Allocation	Physical Location
Telco1 NTH PE1	TBA	TBA	Upper North Island 1
Telco1 NTH PE2	TBA	TBA	Upper North Island 2
Telco1 CEN PE1	TBA	TBA	Central 1
Telco1 CEN PE1	TBA	TBA	Central 2
Telco1 STH PE1	TBA	TBA	South Island 1
Telco1 STH PE2	TBA	TBA	South Island 2

5.2 THE EXTERNAL NETWORK TO NETWORK INTERFACE (E-NNI)

5.2.1 The E-NNI is a generic component for all End-user segments. The table below shows the Service attributes for the E-NNI with all valid attribute value ranges:

Service Attribute	**Valid Attributes Requirements**
UNI Identifier	OSS/BSS
Physical Medium	10GBASE-LR
Fibre Type	Single Mode, 1310nm centre frequency
Speed	10Gbit/s
Mode	Auto-negotiate
MAC Layer	IEEE 802.3
MTU Size	9100 bytes

5.3 LAYER 2

5.3.1 The Layer 2 connectivity requirement is 802.1Q (tagged)

5.3.2 It is possible to initially configure single 10GigE links for each major site. However, increasing reliability and future capacity expansion may be obtained by adding additional 10GigE links as required. If dark fibre is not used, then use BFD to improve failover timing.

5.3.3 10G fibre interfaces are reasonably ubiquitous now and should be the foundation for physical connectivity. Although the physical layer should remain at 10G this can be rate limited on the interfaces to 1G if there is a concern over managing traffic flooding. Capacity increases are very straightforward if interfaces can be uprated at times of extreme demand without physical interface changes.

5.3.4 Attribute Notes:

i. 802.1ad (QinQ) will be supported on the E-NNI.

802.1ad, commonly referred to as QinQ or Double VLAN tagging, extends the capabilities of 802.1Q. It allows the nesting of VLAN tags within another VLAN tag. QinQ effectively creates a 'VLAN within a VLAN', allowing for more extensive network segmentation. Supports a large number of VLANs due to nesting.

ii. The outer VLAN tag and inner VLAN tag each have their VLAN IDs.

iii. The Ethernet MTU includes: MAC header, the Ethertype or Length field, any VLAN tags, the payload and FCS.

iv. The Ethernet MTU excludes: Preamble and Inter-Frame-Gap.

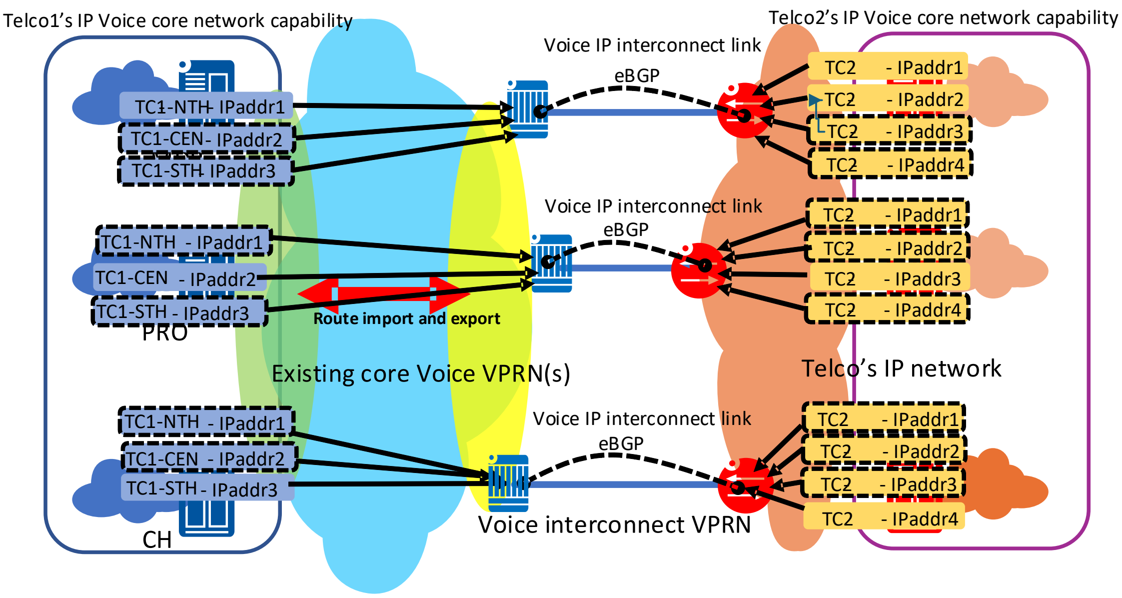
Preamble	**Flag**	**Destination Address**	**Source Address**	**T/L**	**Data**	**FCS**	**Postamble**
56 bits	8 bits	48 bits	48 bits	16 bits	46 to 9,082 bytes	32 bits	96 bits
		MTU					

6. Layer 3

6.1 IPV4 SUPPORT

6.1.1 IPv4 must be supported.

6.1.2 Example Routing Architecture diagram



BGP routing protocol shall be used to exchange IP route information between interconnect parties' networks (i.e. exchanging NLRI for Voice border gateways). The parties shall advertise all IP addresses across all of IP interconnect links, i.e. not constrained via geographical location. Links will be numbered, e.g. /30 from the public IPv4 address space.

Public IPv4 address space is required to ensure that all addresses are unique. As there is no central coordinating body controlling addressing, exposing private addressing on the interconnect may lead to conflicts and loss of service.

The following applies with this IPv4 connectivity requirement:

- The IP network will reroute traffic via alternate routes if the primary routes are unavailable. For example, if an event which causes routes to be withdrawn at a single location (port/card/link/node failure or can be a planned outage), then the same IP routes shall be available via other IP interconnect links. That is, for example, if the NTH IP routes from one party are lost but still available via other IP interconnect links, then the other party is still able to route traffic to either CEN or STH, and the destination IP address stays the same for the traffic.

- The parties should employ Hub and Spoke designs to enforce correct traffic handling using Local Preference routing.

6.2 IPV6 SUPPORT

6.2.1 IPV6 is not currently supported by this standard. Only IPV4 shall be required.

6.2.2 However, IPv6 traffic exchange between networks is not precluded in the future by these Standards and may be optionally supported by mutual agreement of the connecting parties.

6.2.3 If IPV6 is agreed to be supported, then:

6.2.3.1 The exchange of IPv6 routes and traffic will be made available at the NNI boundary where both parties offer IPv6 services.

6.2.3.2 How a provider transits IPv6 traffic across their network will be at their own discretion.

6.2.3.3 Service Class markings defined in the Standard will be populated in the DSCP field in the IPv6 header.

6.2.3.4 The defined Service Class behaviour will apply to IPv6 traffic in the same manner as they are applied to IPv4 traffic.

6.3 SERVICE CLASSES

6.3.1 Two Service Classes shall be mandated as the minimum standards suitable for the transport of low latency, delay variation and loss sensitive applications, such as Voice over IP media and signalling (refer to the table in clause 6.5.3 for more details). It is expected that a maximum of six Service Classes would be sufficient for the industry, with the further definition of sub-Service Classes being for providers' own use and subject to bilateral agreement between providers, where necessary.

6.3.2 The mandatory service classes are:

- DSCP 46 for Voice Media traffic (RTP)
- DSCP 24 for Voice Signalling traffic (SIP)

6.4 SERVICE CLASS MARKINGS

6.4.1 The Differentiated Services Code Point (DSCP) field in the Layer 3 IP Header shall be used to distinguish between the defined Service Classes.

6.4.2 All parties have an obligation to receive packets with DSCP markings as defined in these Technical Standards.

6.4.3 Quality of Service (QoS) markings should be applied at the network edge (closest to the source) and preserved throughout the network. Best practice recommendations are to use Layer 3 DSCP for end-to-end traffic prioritization and Layer 2 p-bit (CoS) for local priority on trunked Ethernet frames.

6.5 SERVICE CLASS PERFORMANCE PARAMETERS

6.5.1 The performance parameters detailed in clause 6.5.3 define minimum performance criteria for each defined Service Class between each UNI. In the case where the traffic flow may originate or terminate internationally (an international voice call for example), the nature of their measurement and allocation is to be further discussed and agreed bilaterally between the interconnect parties.

6.5.2 These parameters apply to end-to-end IP voice sessions. Hybrid situations (mixture of TDM and VoIP technologies in a given connection) have not been considered although the same parameters should be adhered to where possible.

6.5.3 Proposed markings for mandatory Service Classes:

Service Class	**DSCP Marking**	**Traffic Type**	**Associated Layer 2 CoS Marking**	**QOS Performance Parameter**	**Drop Behaviour**
Class 0 (Low Latency)	EF 101110 (DSCP 46) Expedited Forwarding	Voice Media (RTP)	802.1p = 6	ITU Y.1541 Class 0 IPTD (latency): <100ms IPDV (delay variation): < 50ms IPLR (loss) : 1*103	Tail Drop (Discard all excess traffic)
Class 2 (Low Loss)	CS 3 011000 (DSCP 24) Class Selector 3	Voice Signalling (SIP)	802.1p = 3	ITU Y.1541 Class 2 IPTD (latency): <100ms IPDV (delay variation): Undefined IPLR (loss) : 1*103	
Class 5 (Best Efforts)	BE 000000 (DSCP 0) Best Efforts	Data	802.1p = 0	N/A	

6.6 GENERAL TRAFFIC HANDLING

6.6.1 Where traffic crosses an NNI boundary, DSCP markings should not be altered.

6.6.2 This means that when a network operator receives a packet at an NNI boundary with a Service Class marking set in accordance with the Technical standard, that packet will egress their network with the same marking.

6.6.3 Providers may encapsulate packets and mark the encapsulating header with a value for use "locally" on their network, provided the received IP packet header is not modified.

6.6.4 It is up to the originating network to ensure that traffic presented at an NNI boundary is marked appropriately.

6.6.5 In addition to the default rule outlined above, it is expected that providers will enter into bi-lateral agreements with other providers which will define the more commercial aspects of the interconnect arrangements, such as traffic volumes, further Service Classes etc. It is up to the originating network to ensure that traffic presented at an NNI boundary conforms to these agreements for that NNI.

6.6.6 Interconnect traffic will be treated in a non-discriminatory fashion. This means that the traffic of other providers will be treated the same way as your own traffic, within the relevant Service Class.

6.6.7 Each defined Service Class in addition to minimum performance criteria will have an associated "set of agreed behaviours". This is the:

6.6.7.1 Agreed action that will be applied to any received traffic that may exceed agreed NNI SLAs for each Service Class;

6.6.7.2 Agreed action that will be applied to any received traffic that may exceed agreed UNI SLAs for each Service Class; and

6.6.7.3 Generic action that will be applied to any received traffic when the aggregate traffic offered to a provider network exceeds available capacity, including abnormal network conditions.

6.6.8 If excess traffic in a Service Class were to be re-marked and carried across a network in a lower Service Class, or randomly discarded, there is a high probability that the customers using a service being transported within this Service Class would experience erratic performance. This presents operational issues for the service provider when trying to fault-find the erratic service.

6.6.9 While packet discarding may, on first thoughts, seem a harsh approach, it is the easiest solution to effect and manage.

6.6.10 There are no restrictions on what drop behaviour network operators may bi-laterally agree to for application to agreed Service Classes in addition to those defined in the Technical Standard.

6.6.11 When the DSCP value in a received packet does not conform to a Service Class value defined in the Technical Standard, then onward transmission behaviours (including any remarking) are to be bilaterally agreed between the networks interconnecting at that NNI. The default behaviour for an incorrectly marked packet is for it to be treated as best efforts.

6.6.12 If the volume of traffic for a single Service Class defined in the code exceeds the receiving network's SLA for that Service Class providers are not to discard traffic from other Service Classes as a response.

6.6.13 Specifying an SLA for an individual Service Class is not mandatory.

6.6.14 If the traffic profile sent on the NNI does not exceed any individual Service Class SLA for that NNI (or where no individual service class SLA has been agreed), but exceeds the aggregate volume SLA for that NNI, then packets from the lowest priority Service Class supported across that NNI shall be dropped in preference to higher priority Service Classes.

6.6.15 The above is consistent with the idea that a service provider has the right to protect their own network.

6.7 UNI TO UNI PERFORMANCE (END-TO-END)

6.7.1 The NNI Standard will have minimal impact on UNI to UNI performance. UNI to UNI is impacted by individual service provider networks and is outside the scope of these Standards.

6.8 IMPAIRMENT BUDGET

6.8.1 The impairment budget apportionment is proposed on a fixed allocation per network section (provider), rather than on a path by path basis.

6.8.2 This approach means that any network segment does not need to know the performance of any other network segments in the end to end path.

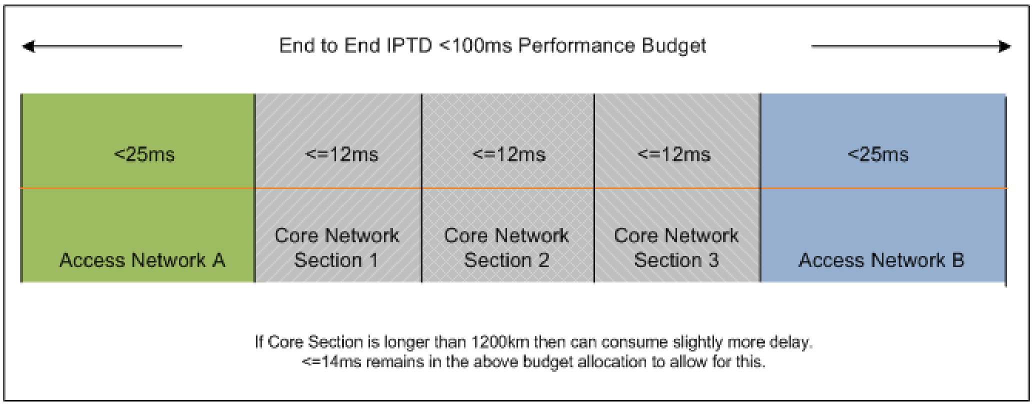
6.8.3 This allows providers to design their networks as they wish, but with a high degree of confidence that the end to end performance targets will be met.

6.9 IP TRANSFER DELAY

6.9.1 The diagram in 6.9.3 below shows the proposed end to end budget for a standard composition which could allow for up to three core network sections and an access network at each end.

6.9.2 The ITU[11] recommends a 10ms budget in core sections, these standards allow for 12ms, as this will allow a core segment path that extends the length of NZ, without adversely impacting on the overall end to end budget.

6.9.3 End to End IP Transfer Delay Performance Budget:



6.10 IP PACKET DELAY VARIATION (IPDV) (JITTER)

6.10.1 These Standards adopt the delay variation definition recommended by the ITU in ITU-T Y1540. [This metric is not additive and further work is required to determine the allocation of this component between network providers.]

6.10.2 The delay variation may be split into Access and Core network functions, and has a statistical element to it.

6.10.3 Refer to Tables A & B below for the Access Network and Core Network Segments budget.

6.10.4 Findings from the MIT draft paper V1.1 also suggest that the proposed delay variation budget for Core network segments be that shown in Table B below.

6.10.5 Table A: Delay Variation Budget for Access Networks:

Budget Region	IPDV Range	Performance Target
Low	<= 16ms	> 99%
High	> 16ms and <= 20ms	< 0.999%
Extreme	> 20ms	< 0.0001%

11 **ITU-T E.800-series Recommendations Supplement 8 (11/2009),** ***Guidelines for inter-provider quality of service***. The ITU-T Supplement appears to incorporate the MIT CFP white paper and provides the later formalised reference for inter-provider QoS guidance.

6.10.6 Table B: Delay Variation Budget for Core Network Segments:

Budget Region	IPDV Range	Performance Target
Low	<= 2ms	> 99%
High	> 2ms and <= 6ms	< 0.999%
Extreme	> 6ms	< 0.0001%

6.11 IP PACKET LOSS RATIO (IPPACKETLR)

6.11.1 These Standards adopt the IP Packet Loss Ratio (IPLR) definition contained in ITU Rec, Y.1540.

6.11.2 For all practical operational purposes, numerically adding the IPLR value for each network in an end-to-end connection is adequate to estimate the end to end IPLR, provided the IPLR values are small (i.e. better than 0.1%).

6.11.3 The total IPLR budget for Class 0 in ITU Rec. Y.1541 is 0.1%. Any measurement of IPLR must ensure a large enough measurement sample is used to enable the IPLR to be observed. The MIT white paper[12] recommends a minimum of 1500 samples be used in any measurement interval to enable IPLR of better than 0.1% to be observed.

6.11.4 Findings from the MIT white paper V1.1 suggest the IPLR budget allocations shown in Table C below.

6.11.5 Note that allowed packet loss may be higher depending on the codec used. For example, enablement of PLC on G.711 can allow operation with as high as 5% packet loss. However as supported codecs are only agreed between the connecting parties allowing higher packet loss by use of a particular codec is only allowed by mutual agreement of the two parties for a particular interconnect and is not appropriate for any generic capability.

6.11.6 Table C: IP Packet Loss Ratio Budget Allocations

Network Section	IPpacketLR Budget
Access Network	> 4x10-4 (0.04%)
Core Network	> 1x10-5 (0.001%)

12 MIT white paper URL: http://cfp.mit.edu/docs/interprovider-qos-nov2006.pdf

D. VOICE SERVICE DESCRIPTION

7. Interconnection Architecture

7.1 FUNCTIONAL ARCHITECTURE

The Interconnect functional architecture defines the NGN's logical network functions in the context of interconnection for IP Voice between two Next Generation Networks, NGN A and NGN B. The functions are split into two parts and presented as control plane functions and bearer plane functions.

7.1.1 The Functional architecture does not define physical implementation within an NGN.

7.1.2 Functional architecture diagram:

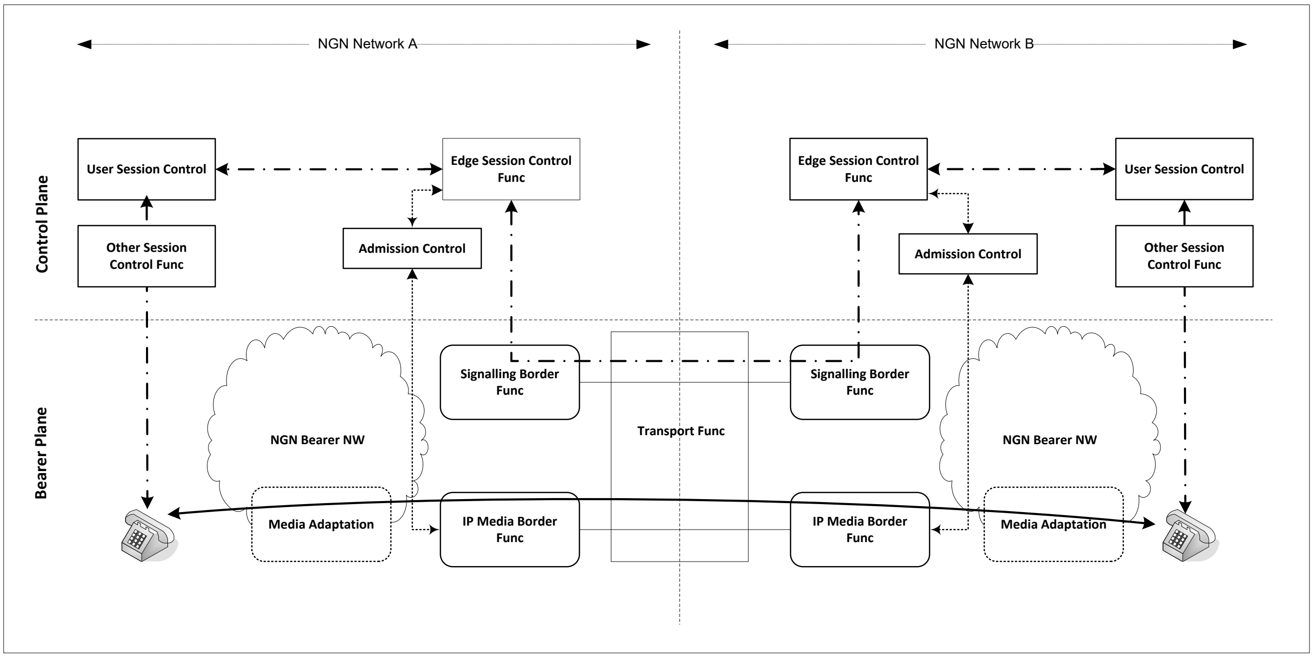


Figure 2: Interconnection for IP Voice Functional Architecture

7.2 FUNCTIONAL COMPONENTS DESCRIPTION

7.2.1 Transport Function

i. Transport Function provides the framing of the transmission bit streams to provide separate VLANs with associated fixed bandwidth (note may be set to 10Gbps or 1Gbps).

ii. Transport Function controls access across the interconnect by implementing of IP Access lists security.

7.2.2 Signalling Border Function

i. Signalling Border Function supports signalling across interconnect between two networks. The Signalling Border Function includes:

- Signalling Firewall between NGN and the interconnection space (mandatory)
- Signalling IP Address Translation for the signalling stream between the two NGN's address spaces across interconnection (optional)
- Security Gateway as defined in ETSI TS 133 210 (mandatory)
- Ability to detect the loss and reestablishment of communications with its peer Signalling Border Function and support monitoring requests from its peer (mandatory)

7.2.3 IP Media Border Functions

i. Media Border Function ensures the appropriate handling of voice traffic at the edges of NGNs It provides the following:

- RTP streams connection between the two NGN (mandatory).

- Support for RTP events (mandatory).
- Policing of Media Streams in accordance with the signalling message info (optional).
- Pinhole Firewall between the NGN and the interconnect space for RTP media (optional).
- IP Address Translation (NAT) for media streams (optional). NAT should not be used for IP interconnect – direct routing is required.
- Detect the loss and reestablishment of communications with its peer Media Border Function across interconnect (mandatory).
- QoS marking and metering to support multiple traffic types with different QoS requirements providing differentiation at packet-level across the interconnect (mandatory).
- Media Encryption to provide confidentiality of RTP payload and integrity protection of the RTP packets (optional).

7.3 MEDIA ADAPTATION FUNCTION

7.3.1 Media adaptation function provides CODEC transcoding e.g. G711a to G.729 if required. It also provides T38 Gateway functionality to ensure fax service across interconnect.

7.3.2 RTP to TDM conversion can also be part of Media Adaptation Function, but it is out of scope as it not a part of IP Interconnect.

7.4 EDGE SESSION CONTROL FUNCTION

7.4.1 The Edge Session Control Function interacts with its peer across the interconnect performing SIP Interworking and network topology-hiding function to prevent from learning details across interconnect, about the NGN network configuration.

7.4.2 It provides SIP session screening to make sure that the signalling messages contain the required parameters

7.4.3 Edge Session Control Function is responsible for Admission Control (rate restriction) to manage overload.

7.4.4 Edge Session Control Function may provide signalling protection by providing encryption of the signalling transmission within a carrier's network (optional).

However, SIP signalling encryption (including TLS) shall not be used across the IP NNI. Any encryption shall terminate at the carrier network boundary before signalling is exchanged across the NNI.

7.5 CALL ADMISSION CONTROL

7.5.1 IP Quality of Service is an effective mechanism for resolving Network congestion for data traffic but is not effective for Real time traffic (sensitive to delay or packet drops). Call Admission Control (CAC) is typically used in conjunction with IP QoS to ensure acceptable call quality can be provided for each new call and is initiated in the call establishment phase. CAC decides whether to accept or reject a new call request based on currently available or predefined resource limits.

7.5.2 Although CAC is primarily used to ensure sufficient network resources are available it may also be used as a mechanism for network security (e.g. authorise the requesting server), attack protection (e.g. limiting the rate of call requests from one or many requesting servers), and network load distribution (e.g. rejecting calls so that they can be established using another link).

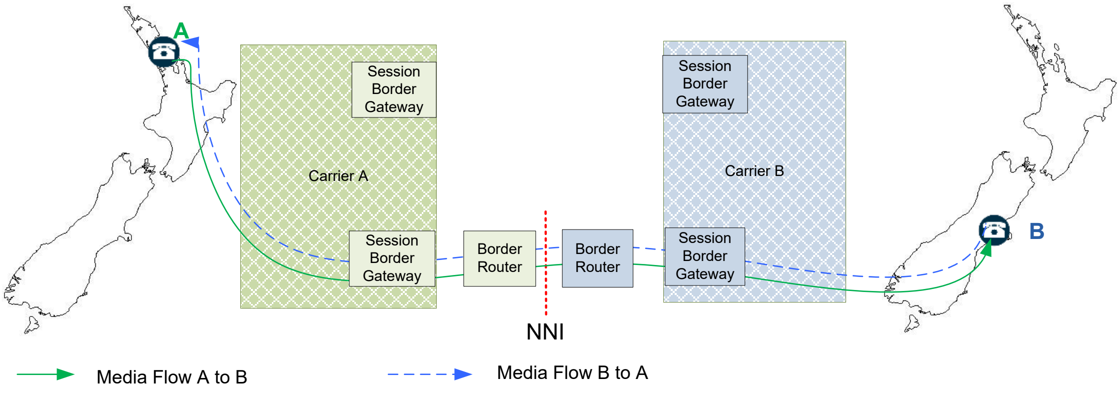
7.6 USER SESSION CONTROL/OTHER USER SESSION FUNCTIONS

7.6.1 The User Session Control Function provides SIP Call Agent functions ensuring the call control and features offered to the end user.

7.6.2 It stores the SIP URIs received during the registration of the end user and provides SIP URI resolution; provides User Authentication and Authorisation, and User Location information.

8. Interconnect Topology

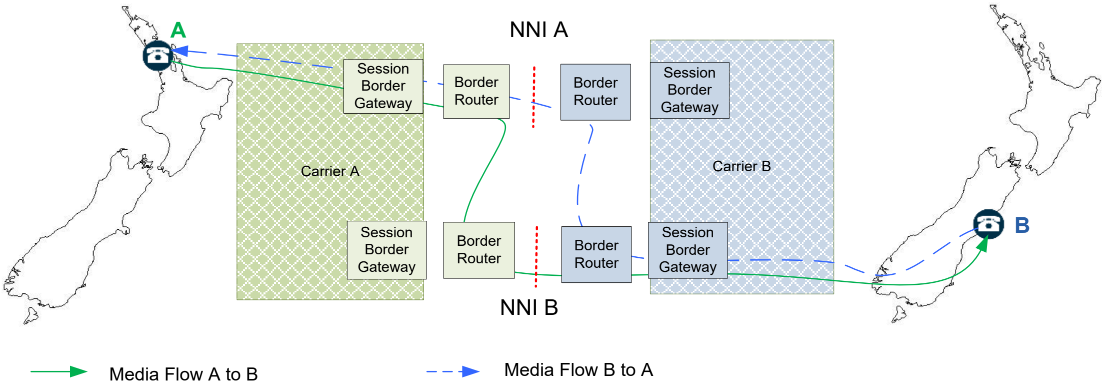
8.1 SINGLE CALL – SYMMETRIC MEDIA FLOW SUPPORTED (NON-FAILOVER SCENARIO)



8.1.1 Notes:

i. The session in this diagram originated by A in Carrier A
ii. Network of Call Originator (A) determines the NNI for the session and the SDP portion of the SIP INVITE shall provide details of where the originating media endpoint is located.
iii. The same NNI is used for both media flow directions
iv. Commercials are determined by the location of the handover of media packets. In this case it is the location of the NNI in relation to the terminating party (B).
v. The dialled number (Terminating party number) will be resolved to the IP address of Carrier B's Session Border Gateway serving the terminating party (B)
vi. The Originating party's IP address will be the Carrier A's Session Border Gateway serving the terminating party's NNI.
vii. Local preference Policy routing should be used for call routing

8.2 SINGLE CALL – ASYMMETRIC MEDIA FLOW (FAILOVER SCENARIO)



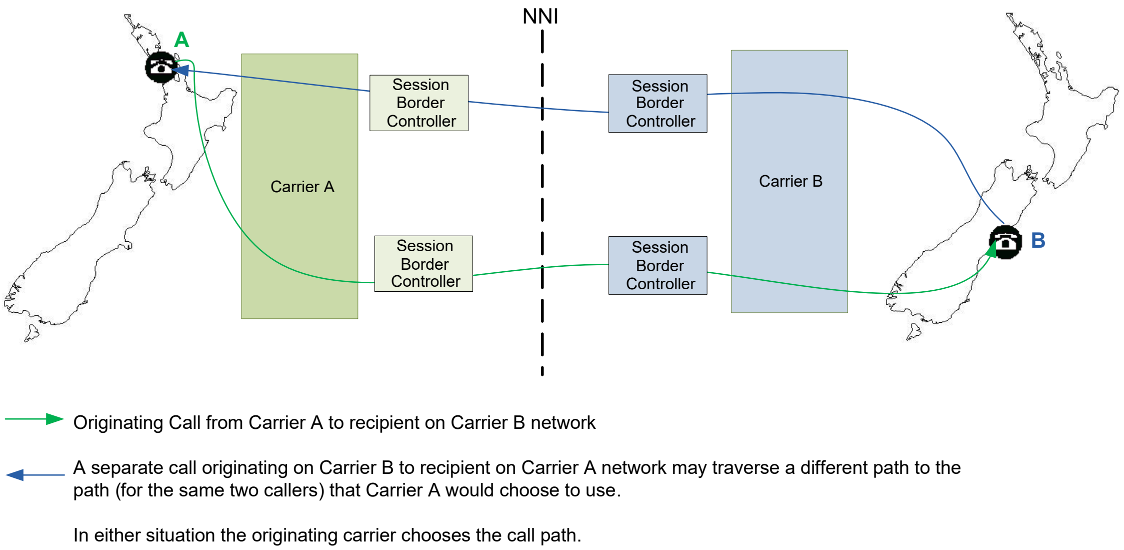
8.2.1 Notes

ii. Asymmetric media flow for a single call as shown in the above diagram shall be supported for failover scenarios.
iii. The session in the above diagram originated by A in Carrier A
iv. NNI used for the packet media flow in each direction is determined by the sending carrier, irrespective of which party originated the session.
v. Media packet flows for a given call may by routed over different paths and different NNI's in each direction.
vi. Commercials are determined by the location of the handover of media packets. In this case media packets are handed over in relation to the packet destination for each direction of a media flow.
vii. Interconnection commercials may be independent of which party "originates" the session

viii. The dialled number (Terminating party number) will be resolved to the IP address of the terminating carrier's Session Border Gateway serving the terminating party (same as for symmetric flow)

ix. Originating party's IP address will be the originating carrier's Session Border Gateway serving the originating party's NNI

8.3 ASYMMETRICAL SIGNALLING CALL PATH AVAILABLE



The network architecture shall be designed to support both symmetric and asymmetric routing scenarios. Symmetric routing shall be the mandatory preferred routing option under normal network conditions. Asymmetric call routing is required for failover call scenarios.

8.4 CALL TYPES ROUTING

The following headings detail the different types of calls.

8.4.1 Interconnect Call Types

- National and Mobile Call – (Fixed, Mobile, Special Services etc.)
- Ported Numbers - Same as above scenario but for ported numbers.

8.4.2 Toll Bypass Non Code Access (TBNCA)

- TBNCA is now withdrawn and is not considered further.

8.4.3 Toll Free

- Standard – Toll free number that terminates to a single national number (e.g. Auckland number only)
- Complex – Toll Free terminating to geographic numbers in multiple areas.

8.4.4 Service Codes

- Emergency (111,911)

- Special Service Codes
- Personal Number Service codes
- Premium rate codes
- Value Add
- International Transit.

9. Signalling

9.1 SIP RFC

9.1.1 With any RFC reference the contents of the actual RFC supersedes this document unless explicitly stated otherwise.

9.1.2 Interconnecting carriers will utilize the Session Initiation Protocol (SIP) at the IP NNI. The IPIWP recommends a selection of IETF RFCS's be adopted.

9.1.3 SIP signalling is to be transported with the TCP protocol over the IP NNI. UDP for SIP signalling should not be used. The use of SCTP, TLS or any other IP transport protocol for SIP signalling transport should not be supported. Encryption of the SIP signalling over the NNI should not be supported as all headers must be available for call processing.

9.2 BASIC CALL CONTROL

9.2.1 For the purpose of voice call setup and take down, the SIP Methods "INVITE", "ACK", "BYE", and "CANCEL" as per RFC 3261 and "UPDATE" as per RFC 3311 are to be used over the IP NNI.

9.2.2 PRACK

i. According to the SIP base specification, RFC 3261, provisional responses (i.e., 1xx level) are not sent reliably, but final responses (i.e. 2xx, 3xx, 4xx, 5xx, and 6xx level) are sent reliably. The fact that provisional responses are not sent reliably could cause issues in IP networks and also on carrier to carrier interfaces based on IP.

ii. One call type where this problem becomes apparent is related to the call scenarios where one way audio path is required to be established to the calling party.

iii. In order to establish a one-way speech path back to the calling party, a SIP 183 response with a SDP is required to be sent. According to RFC 3261, when one network element (e.g., softswitch) on the NNI sends the 183 response, it will never get any acknowledgement that this response was received and acted upon by the network element on the other side. Thus, the network that sends the 183 response has no way of knowing that one-way audio path has been established to the calling party, and consequently the calling party will never hear the in-band audio information.

iv. This problem is solved by the RFC 3262, "Reliability of Provisional Response in the Session Initiation Protocol (SIP)". This specification provides a mechanism, namely the SIP PRACK method, to provide reliability of provisional responses.

v. PRACK is required to be supported over the NNI.

(Pre-requisites: RFC 3261)

9.2.3 Session Description Protocol

i. RFC 4566, "Session Description Protocol (SDP)", details how to describe sessions between end points. Only through the use of SDP can sessions be established when using the SIP protocol.

ii. RFC 3264, "An Offer/Answer Model with the Session Description Protocol (SDP)" details how two entities can come to a common understanding with regard to SDP information in order to exchange media for a voice session.

iii. In particular, RFC 3264 details a protocol for coming to a common agreement on codec(s) and packetization time to be used for a media session between two endpoints. This would be required over an IP NNI interface.

iv. It is recommended that over the NNI, requirements of RFC 4566 and RFC 3264 applicable to unicast voice sessions should be followed.

(Pre-requisites: none)

9.2.4 Privacy Indicators

i. RFC 3323, "A Privacy Mechanism for the Session Initiation Protocol (SIP)" details mechanisms for providing calling party privacy. One mechanism is via the use of the SIP "Privacy" header. This RFC defines the privacy value options (priv-values) of "header", "session", "user", "none" and "critical".

ii. IETF's RFC 3325," Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", builds on RFC 3323, and provides an additional privacy value option of "id".

iii. Over the IP NNI, when a carrier receives a SIP message with a Privacy header containing the priv-values of either "user", "header" and/or "id", the carrier transmits the message towards the called party with the appropriate action to preserve caller privacy. If the call is to be transmitted to another carrier (transit or terminating), the privacy indicators are to be preserved. If the call is to be routed to the called party, then the calling party identify is to be obscured or suppressed.

(Pre-requisites: RFC 3323, 3325 and 3261)

9.2.5 Calling Line and Calling Name Information

i. The Calling Line (mandatory) and Calling Name (optional) information are to be sent using the SIP "P-Asserted-Identity" header for interworking of the Minimum Message Set features of CLID and CNAM when sending SIP signalling over the IP NNI. The header information is generated by the carriers rather than the subscribers and as such is considered to be more reliable than user supplied information. The "P-Asserted-Identity" is identified in RFC 3325.
ii. Further, when the Calling Party contact information is available to the originating carrier, it is to be included in the SIP or TEL URL portion of the P-Asserted Identity header. As well, when the calling party's name information is available, it is to be included in the calling name display portion of the P-Asserted-Identity header.
iii. It is noted that under the current rules, CLIDs (and optionally CNAMs) are transmitted between carriers. As such, within the context of CLID and CNAM, the interconnecting carriers are considered as trusted networks. With respect to referencing RFC 3325 for CLID and CNAM information, this section only deals with the use of the "P-Asserted-Identity" header. No other functions such as authentication are implied.
iv. If a user is served by a network, then that network operator is responsible for its integrity and validation of that user. All calls across the IP interconnect, with the exception of emergency calls, shall include the PAI header and it is up to the originating network to validate the integrity of the calling party in the PAI header. When either party sends the PAI across the interconnect they have undertaken that the calling party is asserted and is responsible for any issues arising out of that (e.g. SPAM, Fraud).
v. Assertion can be established by commercial agreement by both carriers. if the call cannot be asserted, then do not pass the call to the receiving network unless it is an emergency call.

9.2.6 ROUTING NUMBERS, NETWORK ROUTING CODES, HAND OFF CODES

Background

RSPs use network routing codes (NRC) allocated by the NAD according to the LMNP rules to route calls to numbers that have been ported to other service providers, i.e. non-native numbers now hosted in recipient networks.

Traditionally, within the TDM interconnects, these NRC codes have been prefixed to the destination address in the ISUP IAM

E.g.

Called Party Number = 01124792801234
(NRC=11247 for a call to Telco1 native number 92801234 that has been ported to Telco2.

Or

Called Party Number = 011647212345678
(NRC=11647 for a call to Telco3 native number 212345678 that has been ported to Telco4

In IMS (3GPP), the recommended way to carry Network Routing Code information is with the use of the RN parameter to identify the target / recipient network and help with the routing of that call to that network (see RFC4694). If the number portability database is looked up, the NPDI flag will be set to indicate that a number portability dip has been performed and to therefore prevent subsequent number portability database lookups further along the call path towards the destination.

The recommended path forward is to align with the IMS/3GPP and use the RN/NPDI parameters which were designed exactly for this purpose, not to take forward TDM mechanisms where possible. One advantage of this approach is that when a Telco moves its IP Interconnect to an IMS/3GPP based one, the Telco can do this without impacting on connecting Telcos or relying on the connecting Telcos making any changes.

Sending Network:

1. On the NNI interface between the Telcos, for a call to a ported number, the sending network will send the NRC in the RN parameter.
2. If the sending carrier uses NRC steering codes prefixed to the called number destination internally then the sending network must convert the NRC to an RN/NPDI at the NNI SBC/IBCF using HMRs.

Receiving Network:

1. On the NNI interface between the Telcos, the receiving network will receive the NRC in the RN parameter.
2. If the receiving network uses NRC steering codes prefixed to the called number destination internally then they must convert the received RN to a NRC at the NNI edge SBC/IBCF using HMRs.
3. The receiving network may decide to trust the received RN/NPDI or ignore it and perform their own number portability lookup.
    a. A Telco may ignore the received RN/NPDI and perform an ENUM lookup for all received calls from another Telco because that Telco may have internal RNs/NRCs that are not visible for external networks.
    b. A Telco may accept the received RN/NPDI from another Telco and convert it to a NRC Steering code if required.

RN /NPDI Format:

There are several formats that can be used to implement RN/NPDI format, the proposed implementation is;

1. RN is in E.164 international format
2. The receiving network may change the domain to suit their requirements
3. For calls to native numbers in the receiving network, the sending network will include NPDI and will not include an RN
4. Number Portability lookup failure (IN or ENUM). The sending network shall default route the calls as appropriate and having regard to avoidance of recirculation.

Call Scenarios that Use RN:

1. SIP URI with an RN after an ENUM/NPDB lookup (generally speaking these are to ported numbers)

   E.g. Call from Telco1 to an out-ported Telco1 native number now hosted in Telco2.

   Request-URI: sip:+6448029648;**rn=+6411247@telco1.co.nz**; user=phone SIP/2.0

2. SIP URI without RN after an ENUM/NPDB look up (generally speaking these may be native numbers of the receiving network or special codes e.g. emergency numbers.

   E.g. Call from Telco2 to a native Telco1 number (that has not been ported to another carrier, remains on Telco1).

   Request-URI: sip:+6449059648**@telco1.co.nz**; user=phone SIP/2.0

Request-URI: sip:+64105@telco1.co.nz; user=phone SIP/2.0

3. SIP URI without an RN where there has not been an ENUM/NPDB look up (generally speaking these MAY be to native numbers of other networks or special codes e.g. emergency numbers).

   E.g. Call from Telco to a native (non-ported) Telco Number or to special codes

   Request-URI: sip:+64272708343@telco.co.nz; user=phone SIP/2.0

   Request-URI: sip:+64111@telco.co.nz; user=phone SIP/2.0

9.2.7 EMERGENCY CALLS

For mobile-originated emergency calls, the Telco is to replace the 111 called number with an emergency Location Directory Number (LDN) of which there are currently 29. Spark uses this number to send the call to the correct ICAP emergency call centre answering point and onwards to the correct Emergency Service answering point (e.g. 78325100 for a 111 call from a mobile in Whangarei; 78326000 for a 111 call from a mobile in Hamilton).

9.2.8 SUBSCRIBER INITIATED CALL FORWARD FEATURE

i. It is recommended that in the case of subscriber-based call forwarding, a new call leg is established from the point of forwarding to the terminator in order to preserve the current billing methodology. In the scenario where the call is answered at the final destination, a SIP 200 response message must be provided. ***(the use of SIP-REFER is not supported).***

ii. It is recommended that when a call is sent over the IP NNI, and the call has been previously subscriber forwarded, the "History-Info" SIP header field should be added to the SIP message as per RFC 4244. The information conveyed needs to include the following:
   - the call has been previously forwarded by a subscriber;
   - the redirecting or call forwarding party (in case of multiple call forwarding, the last redirecting party shall be used);
   - redirection information (which includes redirection counter and reasons); and
   - the original called party

iii. RFC 4244, "An Extension to the Session Initiation Protocol (SIP) for Request History Information", defines a new SIP header called "History-Info". When a call is sent over the IP NNI, and the call has been previously subscribe- forwarded, the "History-Info" SIP header field can be added to the SIP message. This will capture the fact that the call has been previously forwarded by a subscriber, as well as the original called party, redirecting party, or call forwarding party, address information and redirection information.

(Pre-requisites: RFC 3261, RFC 3323 and RFC 3326)

9.2.9 CALL FORKING

i. Support for call forking is established by the originating carrier in the Request-Disposition tag. Per RFC 3841, the Request-Disposition header field specifies caller preferences for how a server should process incoming requests. Its value is a list of tokens, each of which specifies a particular directive. For call forking, it is defined by the "Fork-Directive" which indicates if a server should or should not fork an incoming SIP invite. The Telco IP NNI shall support the call forking as per RFC3841. Per this directive, calls received across the NNI may invoke multiple SIP dialogs (e.g. Call diversion to voicemail or Sim ring capability). It is the responsibility of the Telco to support multiple SIP dialogs across the IP NNI.

9.2.10 NUMBER PORTABILITY & TOLL FREE

ii. The Working Party agrees that Number Portability and Toll Free need to be supported across the NNI. This requires further discussion on three main points:
   - There may be requirements within Deeds about what level of technical specification is required;

- Some carriers have a desire to maintain the status quo; and
- Other carriers want to take advantage of new techniques for managing this because of new technologies available.

(Pre-requisites: RFC 3261)

9.2.11 SIGNALLING PORT SELECTION

i. The default port to be used for both sending and receiving SIP signalling messages is 5060, unless otherwise agreed to by the interconnecting parties.

ii. With 3GPP and some of the headers becoming larger, the industry direction is heading towards use of TCP for signalling. For IP Interconnect TCP should be used.

9.2.12 ROUTABLE END POINT

i. SIP signalling relies on the Session Description Protocol (SDP), RFC 4566, to identify the destination IP address and port where media streams (e.g., voice sessions) are to be sent. If a destination IP address is behind a NAT device that is not SIP aware, this can cause problems in a SIP & SDP network architecture. Therefore, when a carrier provides a destination IP address for where a voice stream is to be sent, and this is signalled to another carrier over the IP NNI, the IP address in question must be routable.

9.2.13 USE OF SESSION BORDER CONTROLLERS OR EQUIVALENT FUNCTIONS

i. Session Border Controllers (SBC) execute a variety of security functions, including signalling / media firewalls, network topology hiding for downstream devices, authentication, denial-of-service (DoS) prevention, and signal / media encryption termination. The SBC is also a product that improves security directly by hiding real addresses and policing signalling and media connections. Other unique security functions include network address and port translations, flow statistics reporting, bandwidth policing, media replication for lawful intercept, DTMF insertion/extraction and media timers and transcoding. As such, the SBC allows interconnecting parties to be confident they can safely exchange traffic while at the same time hide the topology of their networks and maintain a level of security and quality of service.

ii. As next generation architectures transform and alternative interconnection options become apparent, vendors will undoubtedly have different element names and acronyms describing 'Session Border Controller' functionality.

iii. It is noted that SBCs may be implemented and deployed centrally or in distributed manner. The method of implementation is service provider dependent and beyond the scope of this document. Further, the need for Session Border Controller functionality is not considered to be mandatory.

9.2.14 SUPPORT FOR TRUNK GROUPS (INCLUDING VIRTUAL)

i. When two carriers require multiple trunk groups, as mutually agreed, between each other for the purpose of treating certain traffic differently over the IP NNI, the tel URI trunk group parameters, as defined in RFC 4904 "Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)", is to be used.
(Pre-requisites: RFC 4904, RFC 3261 and RFC 3966)

9.2.15 SECURITY

i. Interconnecting carriers are expected to have mechanisms to prevent security threats but at the same time enable traffic to pass between interconnecting networks.

ii. Network security implementation practice is under the sole control of the network operator. The desired level of protection and implementation should be developed on the basis of bi-lateral agreement between the carriers to ensure proper interworking and" carriage of traffic.

9.3 TRUST TREATMENT AND THE SENDING/STRIPPING OF HEADERS

9.3.1 TRUST TREATMENT

All Telco participating in the IP interconnect NNI will treat each other as trusted networks. This is required for the handling of privacy requests and asserting identities. There is the ability within this to agree to strip or pass headers

- Privacy header
- P-Headers
- UUID
- GUID
- Other

9.3.2 PRIVACY HEADER

- As the IP Interconnect is a trusted interface, the FROM Header is never anonymised by the sending network.
- The privacy header is passed over the IP Interconnect interface, and each operator will honour the privacy request and anonymise the FROM header and other parameters as per the standard Privacy Header highlighted in RFC3323, as it leaves the receiving network Trust domain.
- If a call is anonymised before it arrives into the shared Trust Domain and it cannot be otherwise asserted (e.g. PBX pilot number), then, except for emergency calls, do not pass the call to the receiving network. Emergency calls can be routed but will show the PAI or FROM originating point to the emergency service call centre operator.

  In a trusted interconnect domain, the sending network must be able to assert the authentic identity of the initiating caller while the call is traversing their network or otherwise reject the call and not forward it on through the IP Interconnect. This is enforced to stop spoofed and fraudulent calling from being disseminated to other networks. This must remain the case until a method is agreed whereby the assertion of identify validation can be passed though the interconnect and the receiving network can choose to accept or reject the call based on the identity information provided.
- Telcos will always set the privacy id flag to be “critical” (i.e. Privacy service must perform the specified services or fail the request).

9.4 END TO END DTMF SIGNALLING

9.4.1 DTMF sending between media endpoints is generally to be sent by telephone event method.

9.4.2 Where a compressed codec is negotiated (e.g. AMR, WB-AMR, G.722 etc), the media endpoints must:

9.4.2.1 Support Telephone events sending/reception.

9.4.2.2 Comply with RFC 4733 for Telephone Event sending/reception.

9.4.2.3 Provide backward compatibility for the obsoleted (Dec 2006) RFC2833

9.4.3 When a non-compressed codec is negotiated (e.g. G.711A), the media endpoints must also:

9.4.3.1 Support in-band DTMF sending/receiving where telephone event is not offered from the far end media endpoint.

9.4.4 Telephone event sending is preferred in VoIP to avoid the potential corruption of 'in band' DTMF tones due to codec and packet transport mechanisms. When this occurs, the tones are removed from the audio path and transmitted by telephone RTP events and at the far end inserted back again into the audio path (both governed by RFC 4733/2833). Problems can arise with some VoIP-TDM gateways where the compliance to RFC 4733/2833 is not great (e.g. leakage from the tone removal in the audio path, poor performing DTMF recognition/qualification), in which case in-band DTMF sending should be used. This is accomplished by the profile of the media endpoint in the SDP not offering support for telephone events.

9.4.5 It is recommended that RFC 4733 be the base line standard for the carriage of 'out of band' DTMF tones. With regards to DTMF leakage, it is recommended that adoption of other standards or other methods to address this delay issue could occur via bi-lateral negotiations between carriers.

9.4.6 Note INFO method (RFC6086) is not required to be supported on this technical standard NNI. However, INFO headers may contain information that is useful for call routing investigation or debugging and therefore are allowed within the SIP packets. Nevertheless, any INFO header must be able to be ignored and no call failure shall occur due the presence of the INFO header.

10. User Identifier Formats

10.1 ENUM

10.1.1 Public ENUM is a mapping between E.164 telephone numbers and URI". The IPIWP is to investigate this further before making any recommendation.

10.2 GLOBAL UNIQUE IDENTIFIER

10.2.1 The IP to IP Interconnection is to adopt SIP URI with embedded E.164.

11. Media Plane Interconnect Specification

(Section 11 Source: CRTC Interconnection Steering Committee IP Interconnection Guidelines version 1.0, section 2)

11.1 TRANSPORT

UDP is used for RTP Media Transport

11.2 RTP

11.2.1 IETF's RFC 3550, "RTP: A Transport Protocol for Real-Time Applications" provides details related to the transport of real-time applications. It is recommended that the use of RFC 3550 for the purpose of voice transport is mandatory over the IP NNI. Carriers may optionally secure RTP streams by way of mutual agreement.

11.3 USE OF RTCP

11.3.1 RTCP should be supported for monitoring and performance purposes and where RTCP is used then it must comply with RFC3550 and RFC3611 for RTCP handling

11.4 USE OF SBCS (MEDIA PROXIES)

11.4.1 Refer to Section 9.2.13.

11.5 SUPPORTED CODECS

11.5.1 For IP NNI, the interface must support "G.711 a-law "at a minimum. All other types of codec are optional; based upon bilateral codec negotiation.

11.6 FAX OVER IP

11.6.1 For facsimile transmission over IP interface, the normal G.711 pass-through encoding should be supported as consistent with voice transmission recommendation over IP NNI. The use of ITU-T T.38 protocol should also be supported. T.38 is supported by E2E negotiation if required and if negotiation fails then otherwise fall back to G.711 pass-through.

11.7 (ADAPTIVE) JITTER BUFFER

11.7.1 The deployment of adaptive jitter buffer or any type of de-jitter buffer is the responsibility of the individual carrier to implement in order to meet the guidelines outlined in Section 6.10. The general recommendation is to keep jitter buffers as small as possible to reduce packet latency. Ideally maximum jitter buffer size should only be 1.5 to 2 times the packetisation time.

11.8 MEDIA PORT SELECTION

11.8.1 The port range used for the media session is detailed in clause 13.3.1.

11.9 VOICE ACTIVITY DETECTION

11.9.1 Voice activity detection causes clipping and is not recommended.

11.10 PACKET SIZE

11.10.1 The IP NNI's default packetization interval is specified in clause 13.3.1.

11.11 EARLY MEDIA

11.11.1 Early media is to be supported with the 18x Responses. General rules are

- Earlier media can be requested by 18x responses
- 18x responses do not necessarily provide early media
- 18x responses do not necessarily provide provisional acknowledgment or reliability (PRACK)

11.12 SESSION REFRESH

11.12.1 Session Refresh is supported via the UPDATE or RE-INVITE methods. The Session Refresh (excluding the Target Refresh) must contain the SDP and its version number must be updated/incremented in compliance with RFC 4028.

11.13 SESSION AUDIT

11.13.1 Session Audit is supported via the UPDATE or RE-INVITE methods. When it is sent the version number may or may not contain the SDP, if it does, the SDP version number must not be updated.

11.14 TRANSCODING (CODEC OF LAST RESORT)

11.14.1 Negotiated codec/transcoding will depend on the originating and terminating domain. Therefore, the codec selection depends on the offered codec list in the preferential order in the SDP. If a compatible codec cannot be agreed on end to end, then transcoding should be provided to allow the call to succeed. G.711a should always be available as a directly offered codec or as a transcoded codec of last resort.

12. Quality of Service and Performance

(Section 11 Source: CRTC Interconnection Steering Committee IP Interconnection Guidelines version 1.0, section 5)

12.1 ECHO TREATMENT

12.1.1 The degree of end user annoyance due to talker echo depends both on the amount of delay and on the signal level difference between the voice and echo. In TDM networks, echo is usually controlled adequately if ITU-T Recommendation G.131 “Control of Talker Echo” is applied. Connections requiring echo cancellers should use devices that at least meet the requirements of either ITU-T Recommendation G.165 or ITU-T Recommendation G.168.

12.1.2 As this NNI connection utilizes packet transmission and hence is a non-linear facility (non-linear facilities should not exist in the tail path of an echo canceller), and echo cancellation, if required, shall be applied to signals prior to their crossing the NNI. If digital telephone sets are used, they shall comply with ANSI/TIA/EIA-810-A or TIA-920.

12.2 DIFFSERV CODE POINTS

12.2.1 In general, voice communication requires higher priority processing in order to achieve an acceptable Quality of Service (QoS). To ensure voice packets and associated signalling are properly treated by the receiving network of a NNI, the voice media streams are to be marked with DSCP(as per Section 6.5) by the sending network. However, where two carriers use a dedicated connection between themselves for the purpose of IP NNI, the QoS is guaranteed by the transport facility which would be engineered properly to the anticipated traffic the two carriers wish to inter-change. This would include both the signalling messages as well as the voice media streams.

12.2.2 Hence, where two carriers deploy dedicated connections between themselves for the purpose of IP NNI, DiffServ packet marking would not be required. However, packet marking is considered good practice and even for dedicated connections it is recommended to continue to use packet marking to always ensure an acceptable Quality of Service in the event of unintended packet congestion.

13. Technical Call Definitions

13.1 INTRODUCTION

13.1.1 Calls are defined by a suite of parameters which can be grouped into functional categories. These categories are:

i. Technical Call Parameters
ii. Customer Information Parameters
iii. Call Routing Parameters
iv. Accounting Parameters

13.1.2 Under each category a subset is defined by means of components and sub-components, against which a defined data format is ascribed.

13.2 CALL TYPES NOT SUPPORTED

13.2.1 Currently only voice calls have been defined. Low Speed Data and Fax Call Types should also be supported.

13.2.2 Non-voice Call Types e.g. video are not currently supported.

13.3 VOICE CALLS

13.3.1 Voice calls are those calls intended to support human to human audio communications. They are also intended to support human to machine communications by way of speech recognition or DTMF tone interaction.

13.4 TECHNICAL CALL PARAMETERS

13.4.1 This table describes parameters that impact the calling party’s and called party’s call experience with respect to call success i.e. completion ratios and suchlike as well as quality of speech.

Customer Experience	Component	NNI Spec Value	End to End Service Guideline
	GoS	<=0.01	<=0.01

	MoS	n/a	<=1% of calls have MoS score of <=3
	DTMF	RFC 4733 (with backward support for RFC 2833)	Support of RFC 4733 is required.
Media Plane Specification	Codec	G.711a law	n/a
	Packetisation Rate	20 mS default 10mS optional	n/a
	SIP Port	5060	
	RTP Port Ranges	40,000-60,000 OR 16,384 to 53,999 as per WxC checklist Appendix A	
Class	Class 0 (Low Latency)	ITU Y.1541 - Class 0	

13.4.2 Note that transport parameters are common to all call types across the NNI and are defined separately under Section 6.7 to 6.11.

13.5 CUSTOMER INFORMATION PARAMETERS

13.5.1 This table describes parameters that impact the calling party's and called party's call experience with respect to information provided on call progress, supplementary information such as caller display etc.

Component	Sub Component	Format
Caller Information	CLIP/CLIR Presentation Indicator	CLIP – RFC 3325 CLIR – RFC 3323
	Username	RFC3325 (P-Asserted Identity)
Treatments e.g. busy tone etc.	Source	Terminating Network
	Tone Standards	NZ Tones Standard where the network operator is providing the tones (see TNA102).

13.6 CALL ROUTING INFORMATION

13.6.1 This table describes parameters that enable interconnected parties to make logical system call routing choices. It enables the receiving party to provide carriage of a call from handover by the originating or transit network to the designated destination or other treatment as appropriate.

Component	Sub Component	Format
Address	Destination Address This is the address of the called party (traditionally called the B party), the format supported could be E.164 (e.g. +6499652210) or URI (e.g. +6499652210@carrier.co.nz)	SIP URI
	Source Address This is the address of the calling party (traditionally the A party), the format supported could be E.164 (e.g. +6499652210) or URI (e.g. +6499652210@carrier.co.nz)	SIP URI
Location	Destination Location To be defined, however intention is to use this field to provide information on the physical location of the Destination user.	GLN
	Source Location To be defined, however intention is to use this field to provide information on the physical location of the Source user.	GLN
Handoff	Destination SBC IP address or domain name of Destination carrier SBC device.	IP Address
	Source SBC IP address or domain name of Origination carrier SBC device.	IP Address
Redirection	Redirection address	Y/N
	Redirecting counter	SIP URI
	Redirecting number	SIP URI
	Original called number	SIP URI

Calling Party Category	Annex ZA 3GPP TS 29.427- SIP Support for ISUP Calling Party's Category - interworks the Calling Party's Category in the SS7 ISUP message to the SIP network. Interworking of CPC values is supported from the SS7 network to the SIP Network only. The Calling Party Category is a parameter that distinguishes the station used to originate a call. The CPC carries other important information that describes the originating party. Example CPC types are Operator, Payphone, Ordinary Subscriber.	CPC
Priority/Class of Service	The Priority request-header field indicates the urgency of the request as perceived by the client. E.g. Ordinary/Premium/Emergency	
Cause Value	These are the values given to a call to show how a call terminated or failed. This information is required to allow a carrier to re-route if a call cannot be delivered by a transit carrier. E.g. Congestion, Busy etc	

13.6.2 Refer to Appendix Afor a list showing the Call Routing SIP event, PSTN Cause Code and Descriptions.

13.7 ACCOUNTING

13.7.1 This table describes parameters that enable interconnected parties to determine the nature of a call in commercial terms and thus invoke charging mechanisms where agreed between the parties. These parameters do not in their own right define any commercial terms.

Component	Sub Component	Format
Address	Destination Address This is the address of the called party (traditionally called the B party), the format supported could be E.164 (e.g. +6499652210) or URI (e.g. +6499652210@carrier.co.nz)	SIP URI
	Source Address This is the address of the calling party (traditionally the A party), the format supported could be E.164 (e.g. +6499652210) or URI (e.g. +6499652210@carrier.co.nz)	SIP URI
Location	Destination Location To be defined, however intention is to use this field to provide information on the physical location of the Destination user.	GLN
	Source Location To be defined, however intention is to use this field to provide information on the physical location of the Source user.	GLN
Handoff	Destination SBC IP address or domain name of Destination carrier SBC device.	IP Address
	Source SBC	IP Address

	IP address or domain name of Origination carrier SBC device.	
Redirection	Redirection address	Y/N
	Redirecting counter	SIP URI
	Redirecting number	SIP URI
	Original called number	SIP URI
Calling Party Category	Annex ZA 3GPP TS 29.427 - SIP Support for ISUP Calling Party's Category - interworks the Calling Party's Category in the SS7 ISUP message to the SIP network. Interworking of CPC values is supported from the SS7 network to the SIP Network only. The Calling Party Category is a parameter that distinguishes the station used to originate a call. The CPC carries other important information that describes the originating party. Example CPC types are Operator, Payphone, Ordinary Subscriber.	CPC
Priority/Class of Service	The Priority request-header field indicates the urgency of the request as perceived by the client. E.g. Ordinary/Premium/Emergency	
Cause Value	These are the values given to a call to show how a call terminated or failed. This information is required to allow a carrier to re-route if a call cannot be delivered by a transit carrier. E.g. Congestion, Busy etc	

13.8 NUMBER NORMALISATION

Below are the normalisation rules for ISUP to/from SIP.

<table>
<tr><th colspan="5">Conversion of ISUP (Called Party Number) to SIP ADDRESS DIGIT FORMATS</th><th></th><th colspan="2">Examples</th></tr>
<tr><th colspan="4">ISUP</th><th>SIP</th><th></th><th>ISUP</th><th>SIP</th></tr>
<tr><td rowspan="6">abc(n…n)</td><td colspan="3">a=1</td><td>+64abc(n…n)</td><td></td><td>105
111
124
1700</td><td>+64105
+64111
+64124
+641700</td></tr>
<tr><td rowspan="4">a=0</td><td rowspan="2">b=0</td><td>c=0</td><td>+64bc(n…n)</td><td></td><td>000901234</td><td>+6400901234</td></tr>
<tr><td>c≠0</td><td>+c(n…n)</td><td></td><td>0013059876543
0066851559000</td><td>+13059876543
+66851559000</td></tr>
<tr><td colspan="2">b=1</td><td>+64abc(n…n)</td><td></td><td>010
0124
0140</td><td>+64010
+640124
+640140</td></tr>
<tr><td colspan="2">b=2 to 9</td><td>+64bc(n…n)</td><td></td><td>048029274
0273504761
0800666666</td><td>+6448029274
+64273504761
+64800666666</td></tr>
<tr><td colspan="3">Other</td><td>invalid</td><td></td><td></td><td></td></tr>
</table>

13.9 CALL ROUTING REQUESTS

Below are the supported types (methods) of requests across the NNI:

Methods	Descriptions
INVITE	Indicates a user or service is being invited to participate in a call session
ACK	Confirms that the client has received a final response to an INVITE request
BYE	Terminates a call and can be sent by either the caller or the callee
CANCEL	Cancels any pending searches but does not terminate a call that has already been accepted
OPTIONS	Queries the capabilities of servers
UPDATE	Bearer related information update/session refreshment
REFER	Not Supported
PRACK	For reliable provisional responses
INFO	Sending information that does not affect call state. INFO Is optional and may be ignored by the receiving party. Calls must not fail due to the presence of INFO header.

13.10 CALL ROUTING RESPONSES

Below are the supported types (methods) of response across the NNI:

Response Code	Description	RFC Reference	Supported across NNI
100	Trying	[RFC3261]	Yes
180	Ringing	[RFC3261]	Yes
181	Call Is Being Forwarded	[RFC3261]	Yes
182	Queued	[RFC3261]	Yes
183	Session Progress	[RFC3261]	Yes
199	Early Dialog Terminated	[RFC6228]	Yes
200	OK	[RFC3261]	Yes
202	Accepted (Deprecated)	[RFC6665]	Yes
204	No Notification	[RFC5839]	Yes
3xx	Redirection	[RFC3261]	NO
400	Bad Request	[RFC3261]	Yes
401	Unauthorized	[RFC3261]	Yes
402	Payment Required	[RFC3261]	Yes
403	Forbidden	[RFC3261]	Yes
404	Not Found	[RFC3261]	Yes
405	Method Not Allowed	[RFC3261]	Yes

406	Not Acceptable	[RFC3261]	Yes
407	Proxy Authentication Required	[RFC3261]	Yes
408	Request Timeout	[RFC3261]	Yes
410	Gone	[RFC3261]	Yes
412	Conditional Request Failed	[RFC3903]	Yes
413	Request Entity Too Large	[RFC3261]	Yes
414	Request-URI Too Long	[RFC3261]	Yes
415	Unsupported Media Type	[RFC3261]	Yes
416	Unsupported URI Scheme	[RFC3261]	Yes
417	Unknown Resource-Priority	[RFC4412]	Yes
420	Bad Extension	[RFC3261]	Yes
421	Extension Required	[RFC3261]	Yes
422	Session Interval Too Small	[RFC4028]	Yes
423	Interval Too Brief	[RFC3261]	Yes
424	Bad Location Information	[RFC6442]	Yes
428	Use Identity Header	[RFC4474]	Yes
429	Provide Referrer Identity	[RFC3892]	Yes
430	Flow Failed	[RFC5626]	Yes
433	Anonymity Disallowed	[RFC5079]	Yes
436	Bad Identity-Info	[RFC4474]	Yes
437	Unsupported Certificate	[RFC4474]	Yes
438	Invalid Identity Header	[RFC4474]	Yes
439	First Hop Lacks Outbound Support	[RFC5626]	Yes
440	Max-Breadth Exceeded	[RFC5393]	Yes
469	Bad Info Package	[RFC6086]	Yes
470	Consent Needed	[RFC5360]	Yes
480	Temporarily Unavailable	[RFC3261]	Yes
481	Call/Transaction Does Not Exist	[RFC3261]	Yes
482	Loop Detected	[RFC3261]	Yes
483	Too Many Hops	[RFC3261]	Yes
484	Address Incomplete	[RFC3261]	Yes
485	Ambiguous	[RFC3261]	Yes
486	Busy Here	[RFC3261]	Yes
487	Request Terminated	[RFC3261]	Yes
488	Not Acceptable Here	[RFC3261]	Yes
489	Bad Event	[RFC6665]	Yes
491	Request Pending	[RFC3261]	Yes

493	Undecipherable	[RFC3261]	Yes
494	Security Agreement Required	[RFC3329]	Yes
500	Server Internal Error	[RFC3261]	Yes
501	Not Implemented	[RFC3261]	Yes
502	Bad Gateway	[RFC3261]	Yes
503	Service Unavailable	[RFC3261]	Yes
504	Server Time-out	[RFC3261]	Yes
505	Version Not Supported	[RFC3261]	Yes
513	Message Too Large	[RFC3261]	Yes
580	Precondition Failure	[RFC3312]	Yes
600	Busy Everywhere	[RFC3261]	Yes
603	Decline	[RFC3261]	Yes
604	Does Not Exist Anywhere	[RFC3261]	Yes
606	Not Acceptable	[RFC3261]	Yes

13.11 SIP TIMERS

Below are the recommended SIP Timers to be agreed between the Telcos:

Timer	Description	Recommended Value
T1	Round-trip time (RTT) estimate	500 ms (default)
T2	Maximum retransmission interval for nonINVITE requests and INVITE responses	4 sec
T4	Maximum duration that a message can remain in the network	5 sec
Timer A	INVITE request retransmission interval	initially T1
Timer B	INVITE transaction timeout timer	64*T1
Timer C	Proxy INVITE transaction timeout timer	> 3 min
Timer D	Wait time for response retransmissions	> 32 sec for UDP 0 sec for TCP/SCTP
Timer E	Non-INVITE request retransmission interval	initially T1
Timer F	Non-INVITE transaction timeout timer	64*T1
Timer G	INVITE response retransmission interval	initially T1
Timer H	Wait time for ACK receipt	64*T1
Timer I	Wait time for ACK retransmissions	T4 for UDP 0 sec for TCP/SCTP
Timer J	Wait time for retransmissions of nonINVITE requests	64*T1 for UDP 0 sec for TCP/SCTP

Timer K	Wait time for response retransmissions	T4 for UDP 0 sec for TCP/SCTP
Timer L	Wait time for accepted INVITE request retransmissions	64*T1
Timer M	Wait time for retransmissions of 2xx to INVITE or additional 2xx from other branches of a forked INVITE	64*T1

13.12 FAX CALLS

The use of T.38 relay is recommended for improved fax reliability. However support of T.38 is optional within these Standards. For those providers who chose not to support T.38 then simple Fax Pass-Through using G.711a or Fax Pass-Through-with-upspeed can be used.

13.13 LOW SPEED DATA SERVICES

Low speed data services are required to be supported across the IP Interconnect. This will be via a G.711a codec with echo suppression and cancellation automatically disabled for the call. The modem must support the 2100Hz answer tone to trigger disabling of echo suppression and cancellation in accordance with ITU-T recommendation G.164 or G.165.

A. APPENDIX: ROUTING SIP EVENT INFORMATION

SIP Event	PSTN Cause Code	Description
400 Bad request	127	Interworking, unspecified
401 Unauthorized	57	Bearer capability not authorized
402 Payment required	21	Call rejected
403 Forbidden	57	Bearer capability not authorized
404 Not found	1	Unallocated number
405 Method not allowed	127	Interworking, unspecified
406 Not acceptable		
407 Proxy authentication required	21	Call rejected
408 Request timeout	102	Recover on Expires timeout
409 Conflict	41	Temporary failure
410 Gone	1	Unallocated number
411 Length required	127	Interworking, unspecified
413 Request entity too long		
414 Request URI (URL) too long		
415 Unsupported media type	79	Service or option not implemented
420 Bad extension	127	Interworking, unspecified
480 Temporarily unavailable	18	No user response
481 Call leg does not exist	127	Interworking, unspecified
482 Loop detected		
483 Too many hops		
484 Address incomplete	28	Address incomplete
485 Address ambiguous	1	Unallocated number
486 Busy here	17	User busy
487 Request cancelled	127	Interworking, unspecified
488 Not acceptable here	127	Interworking, unspecified
500 Internal server error	41	Temporary failure
501 Not implemented	79	Service or option not implemented
502 Bad gateway	38	Network out of order
503 Service unavailable	63	Service or option unavailable
504 Gateway timeout	102	Recover on Expires timeout
505 Version not implemented	127	Interworking, unspecified
580 Precondition Failed	47	Resource unavailable, unspecified
600 Busy everywhere	17	User busy
603 Decline	21	Call rejected
604 Does not exist anywhere	1	Unallocated number
606 Not acceptable	58	Bearer capability not presently available

B. APPENDIX: TEST CASES

These set of test cases represents a comprehensive coverage of interconnection scenarios. Where either CSP1 or CSP2 do not offer the services referenced in the test cases then these test cases should be removed from the schedule.

CSP1 IMS Outgoing Call

Test	Call Type
CSP1 IMS-FWV	
TC-1	IMS-FWV Call CSP2-IMS 9D dialling
TC-2	IMS-FWV Call CSP2-PSTN 7D dialling
TC-3	IMS-FWV Call CSP2-Mobile
TC-4	IMS-FWV Call Fixed Line ported out to CSP2
TC-5	IMS-FWV Call Mobile ported out to CSP2
TC-6	IMS-FWV Call CSP2 0800 number
TC-7	IMS-FWV Make Emergency Call 105
CSP1 IMS-FWV	
TC-8	IMS-VOF Call CSP2-IMS 7D dialling
TC-9	IMS-VOF Call CSP2-PSTN 9D dialling
TC-10	IMS-VOF Call CSP2-Mobile
TC-11	IMS-VOF Call Fixed Line ported out to CSP2
TC-12	IMS-VOF Call Mobile ported out to CSP2
TC-13	IMS-VOF Make Emergency Call 105
CSP1 IMS-BBIP	
TC-14	IMS-BBIP Call CSP2-IMS 7D dialling
TC-15	IMS-BBIP Call CSP2-PSTN 9D dialling
TC-16	IMS-BBIP Call CSP2-Mobile
TC-17	IMS-BBIP Call Fixed Line ported out to CSP2
TC-18	IMS-BBIP Call Mobile ported out to CSP2
TC-19	IMS-BBIP Call CSP2 0800 number
TC-20	IMS-BBIP Make Emergency Call 105

CSP1 IPC Outgoing Call

Test	Call Type
CSP1 IPC Fixed SIP Phone	
TC-1	IPC Fixed Call CSP2-IMS 7D dialling
TC-2	IPC Fixed Call CSP2-PSTN 9D dialling
TC-3	IPC Fixed Call CSP2-Mobile
TC-4	IPC Fixed Call Fixed Line ported out to CSP2
TC-5	IPC Fixed Call Mobile ported out to CSP2
TC-7	IPC Fixed Call CSP2 0800 number

CSP1 IPC Cisco 8000	
TC-8	IPC 8000 Call CSP2-IMS 7D dialling
TC-9	IPC 8000 Call CSP2-PSTN 9D dialling
TC-10	IPC 8000 Call CSP2-Mobile
TC-11	IPC 8000 Call Fixed Line ported out to CSP2
TC-12	IPC 8000 Call Mobile ported out to CSP2
TC-13	IPC 8000 Call CSP2 0508 number
CSP1 IPC Mobile	
TC-14	IPC Mobile Call CSP2-IMS 7D dialling
TC-15	IPC Mobile Call CSP2-PSTN 9D dialling
TC-16	IPC Mobile Call CSP2-Mobile
TC-17	IPC Mobile Call Fixed Line ported out to CSP2
TC-18	IPC Mobile Call Mobile ported out to CSP2
TC-19	IPC Mobile Call CSP2 0800 number
CSP1 SIP Trunk	
TC-20	SIPT Call CSP2-IMS 9D dialling
TC-21	SIPT Call CSP2-PSTN 9D dialling
TC-22	SIPT Call CSP2-Mobile
TC-23	SIPT Call Mobile ported out to CSP2
TC-24	SIPT Call CSP2 0800 number

CSP1 IPC Outgoing Call

Test	Call Type
CSP1 IPC Fixed SIP Phone	
TC-1	IPC Fixed Call CSP2-IMS 7D dialling
TC-2	IPC Fixed Call CSP2-PSTN 9D dialling
TC-3	IPC Fixed Call CSP2-Mobile
TC-4	IPC Fixed Call Fixed Line ported out to CSP2
TC-5	IPC Fixed Call Mobile ported out to CSP2
TC-6	IPC Fixed Call CSP2 0800 number
CSP1 IPC Cisco 8000	
TC-7	IPC 8000 Call CSP2-IMS 7D dialling
TC-8	IPC 8000 Call CSP2-PSTN 9D dialling
TC-9	IPC 8000 Call CSP2-Mobile
TC-10	IPC 8000 Call Fixed Line ported out to CSP2
TC-11	IPC 8000 Call Mobile ported out to CSP2
TC-12	IPC 8000 Call CSP2 0508 number
CSP1 IPC Mobile	
TC-13	IPC Mobile Call CSP2-IMS 7D dialling
TC-14	IPC Mobile Call CSP2-PSTN 9D dialling
TC-15	IPC Mobile Call CSP2-Mobile

TC-16	IPC Mobile Call Fixed Line ported out to CSP2
TC-17	IPC Mobile Call Mobile ported out to CSP2
TC-18	IPC Mobile Call CSP2 0800 number
CSP1 SIP Trunk	
TC-19	SIPT Call CSP2-IMS 9D dialling
TC-20	SIPT Call CSP2-PSTN 9D dialling
TC-21	SIPT Call CSP2-Mobile
TC-22	SIPT Call Mobile ported out to CSP2
TC-23	SIPT Call CSP2 0800 number

CSP1 Mobile Outgoing Call

Test	Call Type
CSP1 Mobile	
TC-1	Mobile Call CSP2-IMS
TC-2	Mobile Call CSP2-PSTN
TC-3	Mobile Call CSP2-Mobile
TC-4	Mobile Call Fixed Line ported out to CSP2
TC-5	Mobile Call Mobile ported out to CSP2
TC-6	Mobile Call CSP2-ISDN
TC-7	Mobile Call CSP2 0508 number
CSP1 Ported-in Mobile	
TC-8	Ported-in Mobile Call CSP2-IMS
TC-9	Ported-in Mobile Call CSP2-Mobile
TC-10	Ported-in Mobile Call CSP2 0800 number

CSP1 PSTN Outgoing Call

Test	Call Type
CSP1 PSTN	
TC-1	PSTN Call CSP2-IMS full number dialling
TC-2	PSTN Call CSP2-PSTN 7D dialling
TC-3	PSTN Call CSP2-Mobile
TC-4	PSTN Call Fixed Line ported out to CSP2
TC-5	PSTN Call Mobile ported out to CSP2
TC-6	PSTN Call CSP2 0800 number
CSP1 ISDN	
TC-7	ISDN Call CSP2-IMS 7D dialling
TC-8	ISDN Call CSP2-PSTN 9D dialling
TC-9	ISDN Call CSP2-Mobile
TC-10	ISDN Call CSP2 0800 number

Incoming Call to CSP1 from CSP2

Test	Call CSP1 Type
CSP2-IMS	
TC-1	CSP2-IMS Call CSP1 IMS-FWV 9D dialling
TC-2	CSP2-IMS Call CSP1 IMS-VOF 7D dialling
TC-3	CSP2-IMS Call CSP1 IMS-BBIP full number dialling
TC-4	CSP2-IMS Call CSP1 IPC fixed full number dialling
TC-5	CSP2-IMS Call CSP1 IPC Mobile full number dialling
TC-6	CSP2-IMS Call CSP1 SIPT full number dialling
TC-7	CSP2-IMS Call CSP1 Mobile full number dialling
TC-8	CSP2-IMS Call CSP1 CSP1 mobile ported out to CSP2 by full number dialling
TC-9	CSP2-IMS Call CSP1 PSTN by full number dialling
TC-10	CSP2-IMS Call CSP1 CSP1 fixed number ported out to PSTN.
TC-11	CSP2-IMS Call CSP1 0800 number
TC-12	CSP2-IMS Call CSP1 0900 number
TC-13	CSP2-IMS Make Emergency Call CSP1 111
TC-14	CSP2-IMS Make Emergency Call CSP1 999
CSP2-PSTN	
TC-15	CSP2-PSTN Call CSP1 IMS-FWV 9D dialling
TC-16	CSP2-PSTN Call CSP1 IMS-VOF 7D dialling
TC-17	CSP2-PSTN Call CSP1 IMS-BBIP full number dialling
TC-18	CSP2-PSTN Call CSP1 IPC fixed full number dialling
TC-19	CSP2-PSTN Call CSP1 IPC Mobile full number dialling
TC-20	CSP2-PSTN Call CSP1 SIPT full number dialling
TC-21	CSP2-PSTN Call CSP1 FWV full number dialling
TC-22	CSP2-PSTN Call CSP1 Mobile full number dialling
TC-23	CSP2-PSTN Call CSP1 CSP2 mobile ported out to by full number dialling
TC-24	CSP2-PSTN Call CSP1 CSP2 fixed number ported out to CSP1 by full number dialling
TC-25	CSP2-PSTN Call CSP1 PSTN by full number dialling
TC-26	CSP2-PSTN Call CSP1 ISDN by full number dialling
TC-27	CSP2-PSTN Call CSP1 0800 number
TC-28	CSP2-PSTN Make Emergency Call CSP1 111
Mobile in Ported to CSP2	
TC-29	Mobile in ported to CSP2 Call CSP1 IMS-FWV
TC-30	Mobile in ported to CSP2 Call CSP1 IPC fixed
TC-31	Mobile in ported to CSP2 Call CSP1 IPC Mobile
TC-32	Mobile in ported to CSP2 Call CSP1 Mobile
TC-33	Mobile in ported to CSP2 Call mobile ported in to CSP1
TC-34	Mobile in ported to CSP2 Call CSP1 PSTN
CSP2-Mobile	
TC-39	CSP2-Mobile Call CSP1 IMS-FWV

TC-40	CSP2-Mobile Call CSP1 IMS-VOF
TC-41	CSP2-Mobile Call CSP1 IMS-BBIP
TC-42	CSP2-Mobile Call CSP1 IPC fixed
TC-43	CSP2-Mobile Call CSP1 IPC Mobile
TC-44	CSP2-Mobile Call CSP1 SIPT
TC-45	CSP2-Mobile Call CSP1 Mobile
TC-47	CSP2-Mobile Call Mobile ported out to CSP1
TC-48	CSP2-Mobile Call fixed number ported out to CSP1
TC-49	CSP2-Mobile Call CSP1 PSTN
TC-50	CSP2-Mobile Call CSP1 0800 number
TC-51	CSP2-Mobile Make Emergency Call CSP1 111
TC-52	CSP2-Mobile Make Emergency Call CSP1 999

CSP1 Call Failure Treatment

Test	Call Type
CSP1 IMS	
TC-1	IMS-FWV to CSP2-IMS--IMS hang up before CSP2 answer
TC-2	IMS-VOF to CSP2 Mobile--IMS hang up before CSP2 answer
TC-3	IMS-BBIP to CSP2 PSTN--IMS hang up before CSP2 answer
TC-4	IMS-VOF to CSP2 Mobile-- CSP2 Mobile Power off
TC-5	IMS-BBIP to CSP2 Mobile --Unallocated Number
TC-6	IMS-FWV to CSP2-IMS--Busy
TC-7	IMS-VOF to CSP2-PSTN --Ringing Timeout
CSP1 BW	
TC-8	BW-IPC Fixed to CSP2-IMS--BW hang up before CSP2 answer
TC-9	BW-IPC Mobile to CSP2-PSTN--BW hang up before CSP2 answer
TC-10	BW-VC to CSP2 Mobile-- CSP2 Mobile Power off
TC-11	BW-IPC Mobile to CSP2-IMS--Busy
TC-12	BW-IPC Mobile to CSP2-Mobile--Busy
TC-13	BW-IPC Fixed to CSP2-Mobile Ringing Timeout
CSP1 PSTN	
TC-14	CSP1-PSTN to CSP2-PSTN-- CSP1 PSTN hang up before CSP2 answer
TC-15	CSP1-ISDN to CSP2-IMS--CSP1 ISDN hang up before CSP2 answer
TC-16	NEAX-BBIP to CSP2-Mobile--NEAX-BBIP hang up before CSP2 answer
TC-17	CSP1-PSTN to CSP2 Mobile-- CSP2 Mobile Power off
TC-18	CSP1-BBIP to CSP2-Mobile Unallocated Number
TC-19	CSP1-PSTN to CSP2-IMS--Busy
TC-20	CSP1-BBIP to CSP2-Mobile Ringing Timeout
CSP1 Mobile	
TC-21	CSP1-Mobile to CSP2-Mobile—CSP1 Mobile hang up before CSP2 answer
TC-22	CSP1-Mobile to CSP2-IMS--CSP1-Mobile hang up before CSP2 answer

TC-23	CSP1-Mobile to CSP2 Mobile --CSP2 Mobile Power off
TC-24	CSP1-Mobile to CSP2 Unallocated Number
TC-25	CSP1-Mobile to CSP2-IMS --Busy
TC-26	CSP1-Mobile to CSP2-Mobile --Ringing Timeout

CSP1 Supplementary Services

Test	Call Type
CLI Block on	
TC-1	CSP1 Mobile Call CSP2-IMS with CLI Block on
TC-2	CSP1 IMS-VOF Call CSP2-Mobile with CLI Block on
TC-3	CSP1 IPC Fixed Call CSP2-PSTN with CLI Block on
TC-4	CSP1 IPC Mobile Call CSP2-Mobile with CLI Block on
TC-5	CSP1 PSTN Call CSP2-IMS with CLI Block on
Call Forwarding Unconditional	
TC-6	CSP2-Mobile Call CSP1 Mobile CFU to CSP2-IMS
TC-7	CSP2-PSTN Call CSP1 PSTN CFU to CSP1 IPC Fixed
Call Forwarding Busy	
TC-8	CSP1 IMS-BBIP Call CSP1 IPC Fixed CFB to CSP2-Mobile
TC-9	CSP1 SIPT Call CSP1 IMS-BBIP CFB to CSP2-IMS
TC-10	CSP2-PSTN Call CSP1 Mobile CFB to CSP2-IMS
TC-11	CSP1 IPC Mobile Call CSP1 Mobile CFB to CSP2-Mobile
TC-12	CSP2-VOIP Call CSP1 Mobile CFB to CSP2-Mobile
TC-13	CSP2-Mobile Call NEAX-BBIP CFB to CSP1 IMS-BBIP
Call Forwarding No Answer	
TC-14	CSP1 NEAX-BBIP Call IMS-FWV CFNA to CSP2-Mobile
TC-15	CSP1 IMS-VOF Call SIPT CFNA to CSP2-IMS
TC-16	CSP2-PSTN Call CSP1 Mobile CFNA to CSP2-IMS
TC-17	CSP2-Mobile Call CSP1 PSTN CFNA to CSP1 SIPT
Call Forwarding Not Reachable	
TC-18	CSP1 NEAX-BBIP Call IMS-FWV CFNR to CSP2-Mobile
TC-19	CSP1 IMS-VOF Call IPC Fixed CFNR to CSP2-IMS
TC-20	IPC Fixed Call CSP1-Mobile CFNR to CSP1 Mobile
TC-21	CSP2-PSTN Call CSP1Mobile CFNR to CSP2-Mobile
Call Forwarding to Voicemail	
TC-22	CSP2-Mobile Call IPC Fixed CFB to VM
TC-23	CSP2-IMS Call CSP1 Mobile CFNR to VM
TC-24	CSP2-PSTN Call CSP1 PSTN CFNA to VM
TC-25	CSP2-Mobile Call CSP1 IPC fixed CFNA to VM
TC-26	CSP2-Mobile Call CSP1 Mobile CFNA to VM
TC-27	CSP2-Mobile Call CSP1 IMS-VOF CFU to VM
Multiple Stages Call Forwarding	

TC-28	CSP2-Mobile Call IPC Fixed CFU to IMS-VOF CFB to CSP1 PSTN CFNA to CSP2-IMS
TC-29	CSP2-IMS Call CSP1-PSTN CFU to IMS-VOF CFNA to IPC CFB to CSP1 Mobile
TC-30	CSP2-Mobile Call CSP1-Mobile CFB to IMS-VOF CFNA to IPC
TC-31	CSP2-Mobile Call IMS-VOF CFB to IMS-BBIP CFU to IPC CFU to CSP2-VOIP
TC-32	CSP2-IMS Call CSP1-PSTN CFU to IMS-VOF CFU to SIPT
Call Waiting	
TC33	CSP1 IMS-VOF Call Waiting Call with CSP2-Mobile and CSP2-IMS
TC34	CSP1 IPC Fixed Call Waiting Call with CSP2-Mobile and CSP1-Mobile
TC35	CSP1 Mobile Call Waiting Call with CSP2-PSTN and CSP2-Mobile
TC36	CSP1 PSTN Call Waiting Call with CSP2-IMS and CSP2-PSTN
TC37	CSP1 Mobile Call Waiting Call with CSP2-Mobile and CSP2-Mobile
TC38	CSP1 IMS-BBIP Call Waiting Call with CSP2-IMS and CSP2-PSTN
3 Way Calling	
TC39	CSP1 IMS-VOF 3 Way Call with CSP2-Mobile and CSP2-PSTN
TC40	CSP1 IPC Fixed 3 Way Call with CSP2-Mobile and CSP1 Mobile
TC41	CSP1 PSTN 3 Way Call with CSP2-PSTN and CSP2-IMS
TC42	CSP1 Mobile 3 Way Call with IMS-VOF and CSP2-Mobile
TC43	CSP1 Mobile 3 Way Call with CSP2-Mobile and CSP2-PSTN
Call Return	
TC44	CSP1 IMS-VOF Call Return with CSP2-IMS
TC45	CSP1 IPC Call Return with CSP2-Mobile
Last Number Redial	
TC46	CSP1 IMS-BBIP Last Number redial with CSP2-Mobile
TC47	CSP1 IPC Last Number redial with CSP2-IMS
Call Transfer	
TC48	CSP1 IPC transfer CSP1-PSTN Call to CSP2-IMS
TC49	CSP1 PSTN transfer CSP2-PSTN Call to CSP2-Mobile
TC50	CSP1 IPC transfer CSP2-PSTN to CSP2-Mobile
TC51	CSP1 IPC transfer CSP2-Mobile to CSP1-Mobile
Call Hold	
TC52	CSP1 IPC Music on Hold CSP2 Mobile
TC53	CSP1 Mobile Call Hold CSP2 Mobile
Do Not Disturb	
TC54	CSP1 IPC Do not Disturb

C. APPENDIX: TEST CHECKLIST

SIP Detail	Mandatory Requirement	Optional	Description
SIP RFC Compliance	RFC's 3261, 3262, 3264, 3265, 2976		Collection of RFC's commonly referred to as SIP Version 2. Note: Interpretation and implementation of these RFC's by different vendors will require joint interop testing to ensure correct service operation.
DNS Support	RFC 3263		DNS SRV support
SIP Signalling Port			Port used for SIP Signalling (typically 5060)
SIP Media Port Range			Port range used for media sessions (between 16384 to 53999)
Session Description Protocol	RFC 4566 & RFC 3264		
ISUP Support	RFC 3398		ISUP to SIP Mapping
Media Plane – RTP	RFC 3550		
CN Support	RFC3389		RTP Payload for Comfort Noise
DTMF Relay Support	RFC 2833		RTP Payload for DTMF Digits
DTMF 'out of band' tones	RFC 4733		
Fax Support	ITU-T T.38		Real-time Group 3 fax over IP networks
rport extension Support	RFC3581		Symmetric Response Routing
Privacy Options	RFC 3323		Privacy Mechanism for SIP
	RFC 3325		P-Asserted Identity
	IETF Privacy Draft 01		Use of Remote Party ID header
Call Forward Indicator	RFC 4244 (pre-req includes RFC 3326)		
Keep-alive mechanism	RFC 4028		Session Timers in SIP
	SIP OPTIONS or NOTIFY		periodic sending of message to query state of SIP neighbours
Trunk group support	RFC 4904 (pre-req includes RFC 3966)		

Codec Support	**Payload Size**		
G.711a-law	default = 20ms		
[others as agreed]			
Number Format			
Calling Party (A-Number)	NSN		National significant number without National Prefix (0) eg: 09 950 1300 = 99501300
Called Party (B-Number)	E.164		Country Code + NSN eg: +6499501300