New Zealand Telecommunications Forum

IP Interconnection for Voice
Technical Standards
("Technical Standards")

DOCUMENT VERSION:	
Number and Status:	**1.0 Approved**
Date:	**14 September 2012**
Prepared by:	TCF IP Interconnection Working Party (the working party, IPIWP)
Note	Items contained in this document in quote marks " " have been included verbatim from the CRTC Interconnection Steering Committee Network Working Group IP Interconnection Guidelines Version 1.0 document for the purposes of this draft.

© 2012 The New Zealand Telecommunications Forum Inc. All rights reserved. Copyright in the material contained in this document belongs to the New Zealand Telecommunications Forum Inc. No part of the material may be reproduced, distributed or published for any purpose and by any means, including electronic, photocopying, recording or otherwise, without the New Zealand Telecommunications Forum Inc. written consent.

CONTENTS

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 DSCP replaces the outdated IP precedence, a 3-bit field in the Type of Service byte of the IP header originally used to classify and prioritize types of traffic.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
Media	Packet	3. Network[5]	Path determination and logical addressing

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

5 Sometimes referred to as the IP layer.

	layers	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 pr 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]			
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.			

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

© 2012 New Zealand Telecommunications Forum

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; and

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

2.2.3 The Technical Standards:

i. "could be used to provide guidance on technical discussions and facilitate a more standard interconnection deployment between two carriers wishing to interconnect in native IP if they so choose,

ii. would address inter-carrier NNI issues for the interchange of voice traffic,

iii. would not address and/or resolve telecommunication policy issues,

iv. would not address and/or resolve cost and cost recovery issues,

v. would 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, and"

vi. seek to address testing requirements for interoperability.

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

3. Principles to guide the technical design

3.1 #1: Support for Commercial Constructs

3.1.1 The IP Interconnect NNI design should not unduly limit the commercial models and ICAs that can be enacted over that NNI. The NNI design should be able to support current commercial models, future commercial models to support initially agreed Call Types, and as much as possible, be open to supporting future commercial models for new services.

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 The immediate goal for the working party is to define an NNI that is able to support voice calls. The NNI design should have an eye to future enhanced services that may run over the same NNI, and should try not to make design choices that preclude expansion to enhanced services. Given the uncertainty around the details of future services, the initial NNI design can only try to be open to enhancement, rather than trying to solve future design questions today.

3.3 #3: Call Types Supported Will Be Specified

3.3.1 Some existing PSTN call types and services are difficult to replicate in an IP environment. The NNI design should include a list of call types that are supported, and explicitly list call types that are not supported. (E.g. low speed data) Call types may be defined on technical or commercial criteria.

3.3.2 It will be necessary to define call types for clear discussion. Different call types may be treated differently at the NNI.

3.4 #4: Freedom to choose POIs

3.4.1 Each Carrier should 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 Different services or network types may involve different interconnect topologies. The interconnection topology should allow efficient network design principles to be applied in interconnecting networks.

3.6 #6: Transport and Transit Services will be supported

3.6.1 Carriers 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 must allow for the concept of transport charges, either by a third party carrier, or by one of the interconnecting parties. The NNI design must support the concept of transit networks.

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 should address 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 must specify a default list of supported CODECs. This list may depend on network type. E.g. Mobile, PSTN, NGN. Use of additional CODECs may be negotiated bilaterally by carriers. Transcoding should be minimized.

3.9 #9: The NNI Design should not be unduly optimized

3.9.1 The NNI design should strive to be non-restrictive regarding end subscriber type. It should support call types and commercial models between mobile, VoIP, and PSTN subscribers.

3.9.2 The NNI should attempt to support foreseen developments in IP voice telephony. For example, VoIP calling may include Best Effort and Premium call quality grades.

3.10 #10: NNI Design should not dictate Transition Plans

3.10.1 The transition of interconnection (NGN to PSTN) is a separate topic from the NNI design. The NNI design should try to support a decoupled physical and commercial transition from the current interconnection model to a future, all IP-world. Any aspect of the NNI design that may constrain transition approaches will be tabled to the TCF for consideration.

3.11 #11: Location Information should be preserved across the NNI

3.11.1 The design should include an approach to maintaining the signaling of geographic information, as appropriate to the network (mobile, land) and call type.

3.12 #12: A Default SIP Message Set will be defined

3.12.1 The design should include a baseline SIP messaging set. Although SIP is an evolving group of standards, the working party should try to define a SIP message set that will not be unduly unique to New Zealand or specific vendors.

3.13 #13: Some problems are beyond the scope of the NNI Design

3.13.1 The NNI design must support basic voice calling, but aspects of the calling applications are beyond the control of the NNI itself. For example, Resource Access Control may involve the NNI, or may reside entirely within the calling application. Any assumptions regarding the scope of the NNI design should be listed explicitly in the design document.

3.13.2 The preliminary NNI design will raise thorny problems regarding technical, commercial, and transition choices for the industry and individual carriers. To allow progress on the near term goal of defining an NNI for NGN voice interconnection, the working party will embrace an iterative approach to the design. Difficult, complex, and unwieldy problems will be listed in a “Parking Lot” appended to the Draft Design. These problems can then be discussed with the appropriate TCF member’s representatives for clarification and guidance. The technical working party will then use this wider guidance to make final design choices.

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. Layer 1 and 2

5.1 The External Network to Network Interface (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	1000BASE-LX, 10GBASE-LR
Fibre Type	Single Mode, 1310nm centre frequency
Speed	1Gbps, or 10Gbit/s
Mode	Auto-negotiate
MAC Layer	IEEE 802.3 - 2005
MTU	9100 bytes
Service Muliplexing	Yes
Bundling	Yes
All to One Bundling	No
CE-VLAN ID for untagged and priority tagged Service Frames	NA

5.2 Attribute Notes:

i. Ingress profile per OVC is defined by the specific OVCs.

ii. ∑OVC_CIRi is the sum of the access CIR bandwidths purchased by the Service Provider for their End-users associated with the E-NNI

iii. Both QinQ and 802.1ad will be supported on the E-NNI.

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

v. 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					

© 2012 New Zealand Telecommunications Forum

6. Layer 3

6.1 IPv4 & IPv6 Support

6.1.1 IPv4 must be supported.

6.1.2 IPv6 traffic exchange between networks is not precluded by these Standards.

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

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

6.1.5 It is agreed that where IPv6 is agreed and implemented between network operators, the Service Class markings defined in the Standard will be populated in the DSCP field in the IPv6 header.

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

6.2 Service Classes

6.2.1 The TCF IP Interconnection Working Party (IPIWP) has not yet reached agreement on how many Classes may need to be defined on an industry wide basis to support the most common applications anticipated over an IP Interconnect.

6.2.2 The IPIWP is currently proposing at least one Service Class be mandated in the minimum standards suitable for the transport of low latency, delay variation and loss sensitive applications, such as Voice over IP. (Refer to the table in clause 6.4.3 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 Service Class Markings

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

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

6.3.3 Parties can also bi-laterally negotiate an alternate to DSCP for indicating the Service Class across the NNI.

6.3.4 To maintain backward compatibility with legacy equipment that does not support the use of DSCP, the first three bits of this field will be used to define the various Service Classes. This will allow the use of the legacy IP precedence bits to define the same Service Class.

6.3.5 Similarly, these first three bits will map directly to both the MPLS EXP bits and also the Ethernet, 802.1p bits, giving network providers a large degree of flexibility in how they apply the defined Service Classes.

6.3.6 This approach will give up to six possible available industry Service Classes (the highest two values (110 and 111) are proposed to be reserved for network control). Through the use of the next three bits in the DSCP field, the six Service Classes can be further split into sub-Service Classes.

6.4 Service Class Performance Parameters

6.4.1 The performance parameters detailed in clause 6.4.3 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.

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

6.4.3 Proposed markings for Service Classes

Service	DSCP	TOS	802.1p	MPLS	Quality of Service	Drop

Class	Marking (Decimal)	(IP Precedence)	CoS bits	EXP bits	(QoS) Performance Parameters	Behaviour
Class 0 (Low Latency)	EF 101110 (46) Expedited Forwarding	101 (5)	101 (5)	101 (5)	ITU Y.1541 - Class 0 IPTD (latency): < 100ms IPDV (delay variation): < 50ms IPLR (loss) : $1*10^{-3}$	
Class 2 (Low Loss)	AF 31 011010 (DSCP 26) ***OR***[11] AF 21 010010 (DSCP 18)	010 (2)	010 (2)	010 (2)	ITU Y.1541 - Class 2 IPTD (latency): < 100ms IPDV (delay variation): Undefined IPLR (loss) : $1*10^{-3}$	Tail Drop (Discard all excess traffic)
Class 5 (Best Efforts)	BE 000000 (0) Best Efforts	000 (0)	000 (0)	000 (0)	N/A	

6.5 General Traffic Handling

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

6.5.2 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.

6.5.3 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.

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

6.5.5 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.

6.5.6 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.

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

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

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

11 Further discussion required by Tech Group to reach agreement on which DSCP marking to use for Class 2 – AF31 or AF21.

6.5.10 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.

6.5.11 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.

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

6.5.13 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.

6.5.14 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.

6.5.15 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.

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

6.5.17 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.

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

6.6 UNI to UNI Performance (End-To-End)

6.6.1 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.

6.7 Impairment Budget

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

6.7.2 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.

6.7.3 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.

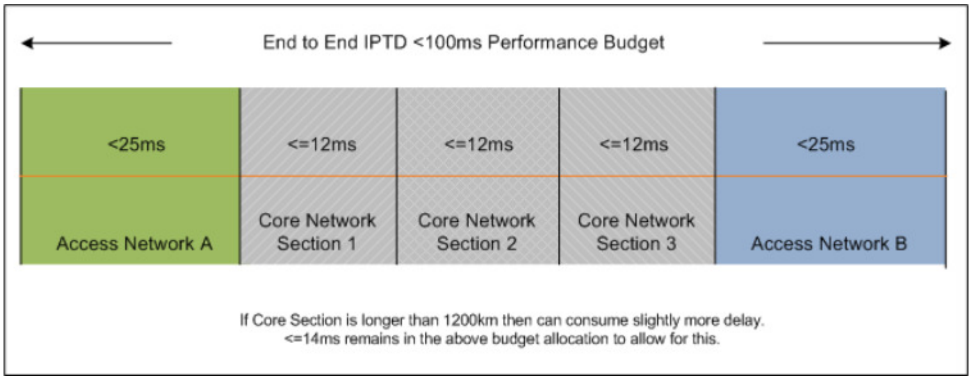
6.8 IP Transfer Delay

6.8.1 The diagram 6.8 and 6.8.3 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.

6.8.2 Although the MIT white paper12 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. This is the same as what is proposed by the ITU recommendation.

6.8.3 End to end IP Transfer Delay performance budget

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



6.9 IP Packet Delay Variation (IPDV) (Jitter)

6.9.1 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.]

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

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

6.9.4 Findings from the MIT white paper25 and the draft paper E.841 also suggest that the proposed delay variation budget for Core network segments be that shown in Table B below.

6.9.5 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%

6.9.6 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%

6.10 IP Packet Loss Ratio (IPpacketLR)

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

6.10.2 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%).

6.10.3 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[13] recommends a minimum of 1500 samples be used in any measurement interval to enable IPLR of better than 0.1% to be observed.

6.10.4 Because access networks are typically more susceptible to transmission errors, it is possible that a higher portion of the end to end loss budget may be allocated to access networks. Allocation of budgets for IPLR has not yet been discussed by the working party.

6.10.5 Findings from the MIT white paper26 and the draft ITU recommendation E.841 suggest the IPLR budget allocations shown in Table C below.

6.10.6 Table C: IP Packet Loss Ratio Budget Allocations

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

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

D. VOICE SERVICE DESCRIPTION

7. Interconnection Architecture

7.1 Functional Architecture

7.1.1 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.

7.1.2 The Functional architecture does not define physical implementation within a NGN.

7.1.3 Functional architecture diagram:

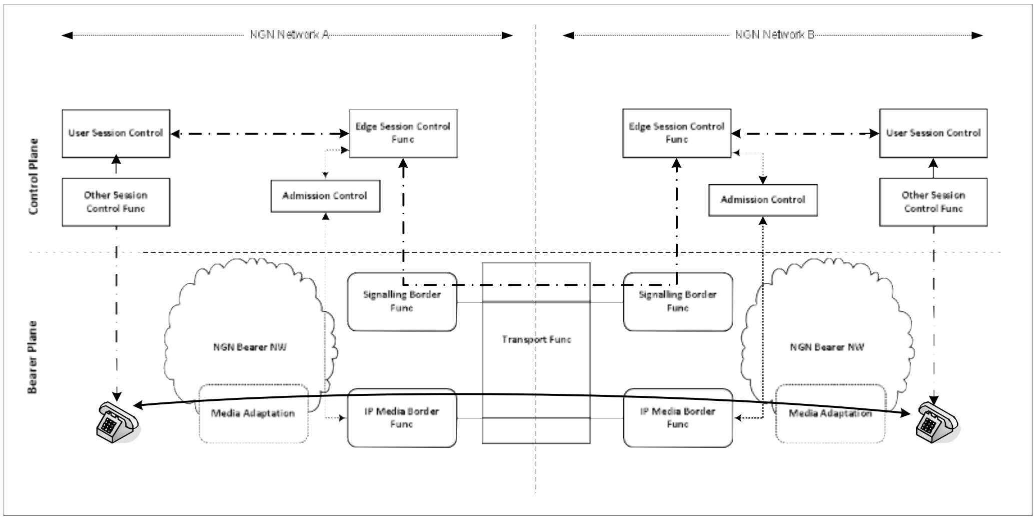


Figure 2: Interconnection for IP Voice Functional Architecture

7.2 Functional Components Description

7.2.1 Transport Function

i. 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.

ii. Transport Function provides the framing of the transmission bit streams to provide separate VLANs with associated fixed bandwidth.

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

7.2.2 Signaling Border Function

i. Signaling Border Function supports signaling across interconnect between two networks. The Signaling Border Function includes:
   - Signaling Firewall between NGN and the interconnection space
   - Signaling IP Address Translation for the signaling stream between the two NGN's address spaces across interconnection
   - Security Gateway as defined in ETSI TS 133 210
   - Ability to detect the loss and reestablishment of communications with its peer Signaling Border Function and support monitoring requests from its peer

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:

© 2012 New Zealand Telecommunications Forum

- RTP streams connection between the two NGN.
- Policing of Media Streams in accordance with the signaling message info.
- Pinhole Firewall between the NGN and the interconnect space for RTP media.
- IP Address Translation (NAT) for media streams between the two NGN's address spaces and set of UDP ports numbers across interconnection.
- Detect the loss and reestablishment of communications with its peer Signaling Border Media Border Function across interconnect.
- QoS marking and metering to support multiple traffic types with different QoS requirements providing differentiation at packet-level across the interconnect by reference to 802.1p or PCP markings.
- Media Encryption to provide confidentiality of RTP payload and integrity protection of the RTP packets.

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 of this Standard.

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 signaling 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 ensures signaling protection by providing encryption of the signaling transmission.

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).

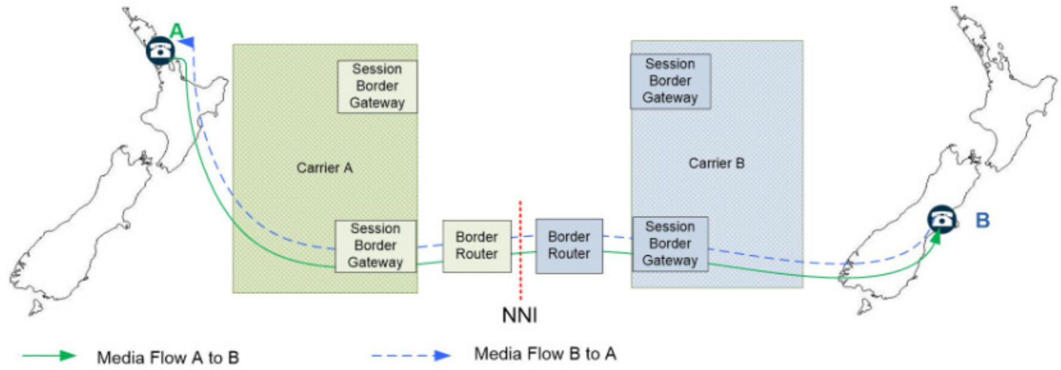
7.6 User Session Control/Other User Session Functions

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

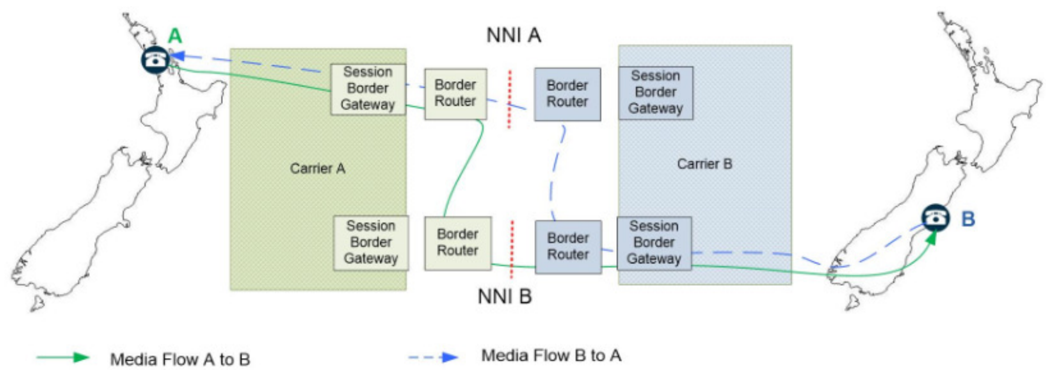
8.1 Single Call – Symmetric Media Flow Supported



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.
iii. The same NNI is used for both media flow directions
iv. Commercials are determined by 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.

8.2 Single Call – Asymmetric Media Flow

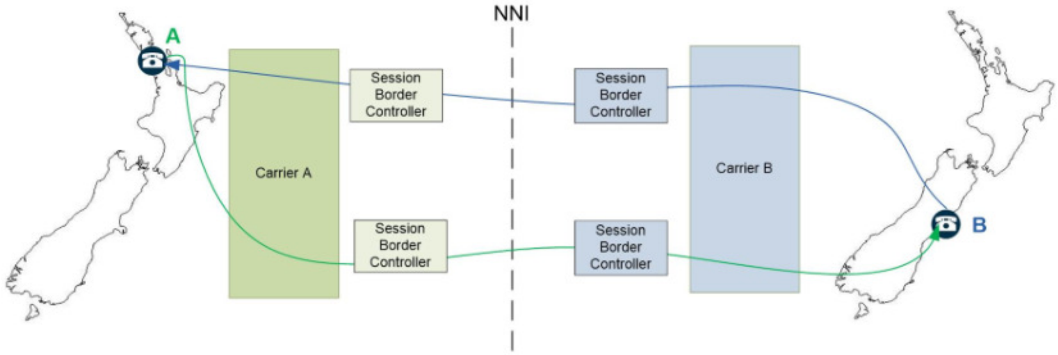


8.2.1 Notes

ii. It is currently proposed by the Working Party that asymmetric media flow for a single call as shown in the above diagram **NOT** be supported in the Technical Standards.
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 based on where 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 Call Path Available



Originating Call from Carrier A to recipient on Carrier B network

A separate call originating on Carrier B to recipient on Carrier A network may traverse a different path to the path (for the same two callers) that Carrier A would choose to use.

In either situation the network on which the call originates receives the revenue and the path chosen by the carrier may be based on lowest cost/free handover or the specific service being delivered.

9. Signalling

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 either the UDP or TCP protocol over the IP NNI. The use of SCTP, TLS or any other IP transport protocol for SIP signalling transport is to be based on a bilateral agreement."

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.

© 2012 New Zealand Telecommunications Forum

(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 and Calling Name 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, calling names and CLIDs 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."

9.2.6 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 should be sent back over the IP NNI."

9.2.7 Call Forward Indicator

i. 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

ii. 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)

9.2.8 Number Portability & Toll Free

i. 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)

9.2.9 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. Either UDP or TCP could be used for transport of the SIP signalling messages."

9.2.10 Routable End Points

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."

9.2.11 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."

9.2.12 Support for Trunk Groups (including Virtual)

i. "When two carriers require multiple trunk groups 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)"

9.2.13 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 End to End DTMF Signalling

9.3.1 "In an IP NNI, it may be necessary to allow for the passing of end point to end point DTMF signalling information transmitted 'out of band' to avoid the potential corruption of 'in band' DTMF tones due to codec and packet transport mechanisms. RFC 4733 provides an 'out of band' DTMF transmission process, however, some CPE associated with voice mail and IVR applications have been known to be susceptible to "leakage" caused inherently by VoIP Gateways (GWs).

9.3.2 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."

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 RTP

11.1.1 "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."

11.2 Use of RTCP

11.2.1 Technical Teams to provide feedback on whether to include RTCP in the Technical Standards.

11.3 Use of SBCs (Media Proxies)

11.3.1 Refer to Section 9.2.11.

11.4 Supported Codecs

11.4.1 "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."

11.5 Fax Over IP

11.5.1 For facsimile transmission over IP interface, the normal G.711 encoding should be used consistent with voice transmission recommendation over IP NNI. The use of ITU-T T.38 protocol is to be based on bilateral agreement only.

11.6 (Adaptive) Jitter Buffer

11.6.1 "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 ii".

11.7 Media Port Selection

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

11.8 Voice Activity Detection

11.8.1 Voice activity detection causes clipping and is not recommended.

11.9 Packet Size

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

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=46 and voice signalling streams with DSCP=40 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."

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 are yet to be defined.

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	Tbc [is it RFC 2833 also?]	Support of this required. Propose minimum standard be RFC 2833, anything else can be agreed bilaterally.
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 6.6 to 6.10.

© 2012 New Zealand Telecommunications Forum

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 [include SIP terminology for these here as well]	tba
	Display Name	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.

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.	tbc
	Source Location To be defined, however intention is to use this field to provide information on the physical location of the Source user.	tbc
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	Upon receipt of a redirection response (for example, a 301 response status code), clients SHOULD use the URI(s) in the Contact header field to formulate one or more new requests based on the redirected request.	Y/N
	Redirecting counter	SIP URI

	Redirecting number	SIP URI
	Original called number	SIP URI
Calling Party Category	Feature 1295 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. Ordinary, Payphone etc	
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 Section E for 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.	tbc
	Source Location To be defined, however intention is to use this field to provide information on the physical location of the Source user.	tbc
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	IP Address

	device.	
Redirection	Upon receipt of a redirection response (for example, a 301 response status code), clients SHOULD use the URI(s) in the Contact header field to formulate one or more new requests based on the redirected request.	Y/N
	Redirecting counter	SIP URI
	Redirecting number	SIP URI
	Original called number	SIP URI
Calling Party Category	Feature 1295 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. Ordinary, Payphone etc	
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 Call Routing Requests

13.8.1 SIP uses six types (methods) of requests:

a) INVITE—Indicates a user or service is being invited to participate in a call session.

b) ACK—Confirms that the client has received a final response to an INVITE request.

c) BYE—Terminates a call and can be sent by either the caller or the callee.

d) CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.

e) OPTIONS—Queries the capabilities of servers.

f) REGISTER—Registers the address listed in the To header field with a SIP server.

13.9 Call Routing Responses

13.9.1 The following types of responses are used by SIP:

a) SIP 1xx—Informational Responses

b) SIP 2xx—Successful Responses

c) SIP 3xx—Redirection Responses

d) SIP 4xx—Client Failure Responses

e) SIP 5xx—Server Failure Responses

f) SIP 6xx—Global Failure Responses

13.10 Fax Calls

13.10.1 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 or Fax Pass-Through-with-upspeed could be used.

13.11 Low Speed Data Services

13.11.1 The treatment and support for low speed data services is still being researched by the IPIWP and investigated through technical trials by Telecom Retail. Refer to Appendices G and H for further background information on this topic.

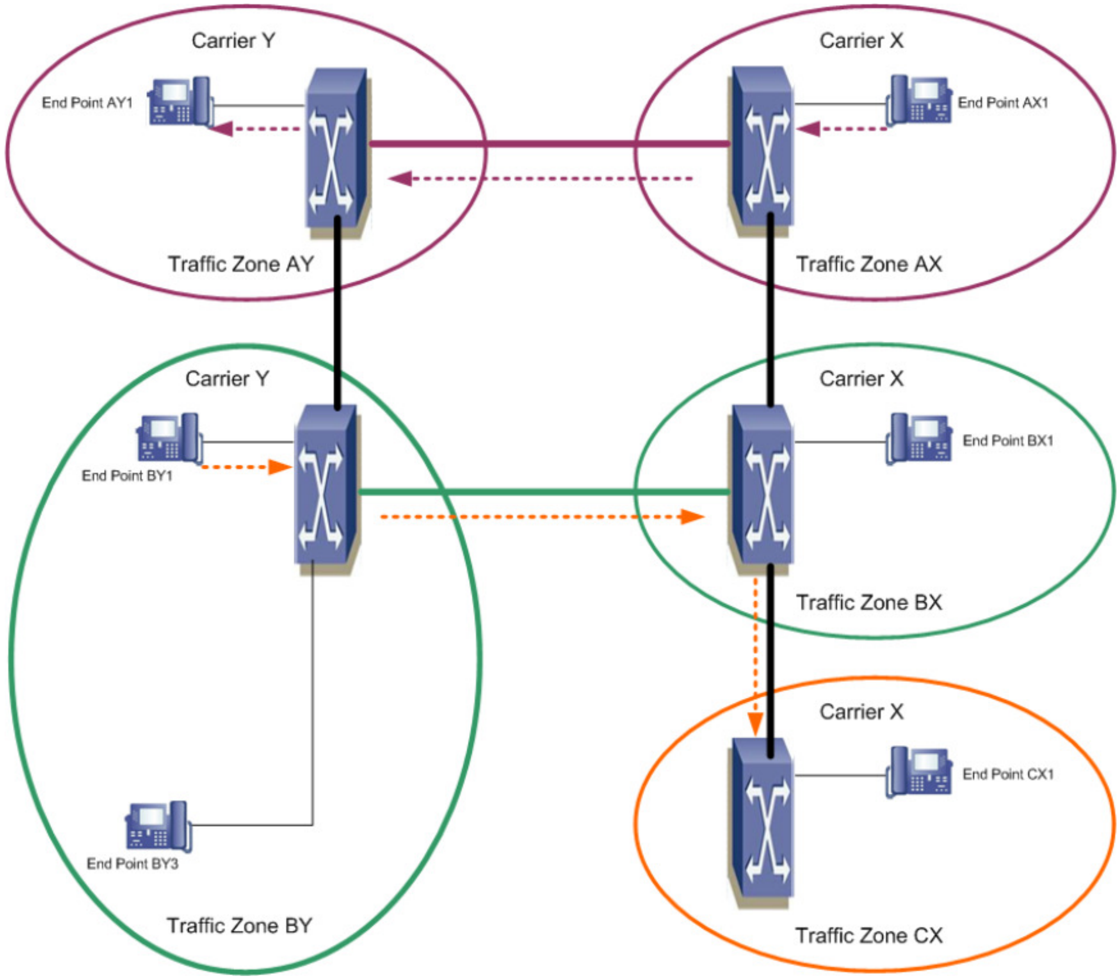
13.12 Nomadicity

13.12.1 There will be optimized routing for national and international roaming; however nomadicity is dependent on geo spatial information sources which are yet to be confirmed.

E. 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

F. APPENDIX: CALL FLOW SCHEMATIC



G. APPENDIX: FAX & LOW SPEED DATA

Discussion Paper prepared by TelstraClear

1.1 Introduction

Fax and low-speed data present some challenges to a VoIP network. There are specific solutions, such as T.38 for fax, but in the absence of these specific solutions and given that fax and modem calls are designed to mimic voice calls, it might be expected that fax and data could just pass transparently through a suitable CODEC such as G.711.

One barrier to such calls working successfully is echo, or rather echo cancellation, which is discussed here.

The nature of the problem

A voice call is full-duplex. That is, both sides can talk at the same time.

A normal characteristic of a voice call, and of natural conversation, is echo. We hear our voice reflected back off our surroundings. We hear ourselves speaking when we talk into a telephone handset. Complete absence of echo, such as is found in an anechoic chamber, is unnatural and disturbing.

However, if the delay gets too high—greater than about 10 ms—the effect is disruptive. Small amounts of delay cause the sound to be distorted. Larger amounts result in detectable discrete echo, which is immensely disruptive.

Source of echo

Apart from the natural near-surface echo, traditional telephone systems are subject to multiple other sources of echo. Every change in electrical impedance in a circuit results in some echo. In particular, the transition from the 2-wire access line to a 4-wire trunk introduces significant echo. There may be many sources of electrical echo within a telephone network. Finally, when delivered to the handset at the other end there will be acoustic echo at the handset and potentially off the local environment.

2.1 Solutions to the problem

Echo Suppression

Echo suppression is an older technique that essentially turns the call from full-duplex to half-duplex. When the phone detects that you are talking, it partially or totally suppresses the incoming channel. This is not ideal as it makes normal conversation difficult.

Echo suppression is normally done within the carrier network—not at the customer phone—and only when really necessary. For example, at trunk gateways where long distance and resulting high latency is a problem.

I am not sure if echo suppression has ever been employed within New Zealand. The TelstraClear network for instance has never used echo suppression.

Echo Cancellation

Echo Cancellation is a more recent technique that analyses the incoming signal for traces of the delayed outgoing signal, which it then digitally subtracts.

Whereas echo suppression works independently of the amount of delay, echo cancellation must take into account the delay in order to allocate a suitable amount of buffer.

Echo cancellation is rarely perfect and different implementations may produce variable results.

Echo cancellation does not work in the presence of too much distortion, that is, if the received signal is too dissimilar to the sent signal. For similar reasons it fails if the received signal has already been partially echo cancelled elsewhere in the network: partial cancellation prevents further cancellation.

On the other hand, echo cancellation has undesirable effects on things like modem signals, which is highly likely to be mistakenly detected as echo.

Since standard analogue telephones don't have echo cancellation ability, this function has been performed where required by the PSTN.

Owing to the relatively short distance and high quality of the New Zealand telephone networks, echo cancellation has not been widely deployed—usually only on a few, long latency links.

Signal balancing

The best solution to the problem is to avoid it as much as possible. Since a major source of echo is caused by electrical impedance changes, careful management of these can eliminate most echo—and generally provides a better quality line.

The effect of small amounts of echo is multiplied by the amount of latency in the network. The greater the latency, the smaller the amount of echo that can be tolerated. The amount of latency found within New Zealand combined with good signal balancing means that in general echo cancellation has not been necessary. However, were the latency greater (and for some long latency paths such as when calls loop through to a voicemail system) echo cancellation would (and does) become necessary.

3.1 Solutions to the solution

Both echo suppression and echo cancellation introduce problems of their own. In particular, modems—including fax—suffer severe problems in their presence, so there is an ITU standard ‘answer tone’ at 2100Hz, which, when detected, turns echo suppression/cancellation off. However, not all equipment sends this. Because New Zealand telephone networks don’t tend to employ echo suppression/cancellation, partially because they are so well engineered, some manufactures don’t bother with the answer tone. For instance, some EFTPOS terminals omit it in order to reduce the transaction time.

4.1 Echo cancellation and VoIP

Pure VoIP

For a pure VoIP call, there is no possible source of echo between the CODEC stages. Once a call has been converted to packets, there is no way for any electrical or signal level mismatches in the digital network to result in valid media packets being echoed back to the originator.

Thus, the only possible echo in a pure VoIP environment must occur on the analogue sides of the call. Ambient reflection from the speaker’s handset is normal and desirable. The other source of echo can be from the listener’s handset or environment.

Every VoIP handset includes echo cancellation hardware. It might be assumed that this is there to cancel the speaker’s voice when reflected back from the listener. That is not the case. The echo cancellation is there to prevent the far end signal being reflected back.

That is, your echo canceller doesn’t improve your listening experience—it improves the other end’s listening experience. If you hear echo on a VoIP call it is because the other end is not doing its job.

Note that in contrast to the PSTN, the echo cancellation function is performed by the phone, not be the network.

Mixed VoIP/PSTN

In a mixed VoIP/PSTN environment, echo can be a problem.

VoIP is inherently lossless with distance, so volumes can be high (which accentuates echo), combined with high latency.

Whereas the PSTN is equipped to deal with echo, as discussed above it often is not configured to do so, because latency has not been high enough to require it. However, VoIP can incur significantly greater latency. Although this does not affect VoIP-VoIP calls, VoIP-PSTN calls can suffer from debilitating echo owing to the uncancelled echo in the PSTN section.

The solution is to require that there be echo cancellation at each CODEC in any chain of VoIP circuits. In particular, that means that there must be good echo cancellation at the VoIP-PSTN gateway.

Modems and VoIP

As discussed, VoIP requires echo cancellation. Since this interferes with modems, any use of modems on a VoIP circuit will require adherence to answer tone standards, or the modem call will probably fail. This makes the use of non-compliant EFTPOS modems (for example) inherently problematic.

Conclusions

All VoIP handsets should perform echo cancellation. The effect of not doing so will be poor voice quality at the other handset.

There must be echo cancellation at each CODEC in any chain of VoIP circuits. In particular, there must be good echo cancellation at the VoIP-PSTN gateway.

Modems that don't follow standards by transmitting a 2100Hz answer tone and which transit VoIP are likely not to work.

Other things can go wrong. Since modems tend to be tuned to extract the maximum performance out of the available (and limited) bandwidth, they can be extremely intolerant of anything 'different'. Levels of loss, jitter and phase change that would be utterly imperceptible on a real voice call may be enough to prevent a modem or fax call from working at all.

5.1 Conclusions

1. All VoIP handsets should perform echo cancellation. The effect of not doing so will be poor voice quality at the other handset.
2. There must be echo cancellation at each CODEC in any chain of VoIP circuits. In particular, there must be good echo cancellation at the VoIP-PSTN gateway.
3. Modems that don't follow standards by transmitting a 2100Hz answer tone and which transit VoIP are likely not to work.
4. Other things can go wrong. Since modems tend to be tuned to extract the maximum performance out of the available (and limited) bandwidth, they can be extremely intolerant of anything 'different'. Levels of loss, jitter and phase change that would be utterly imperceptible on a real voice call may be enough to prevent a modem or fax call from working at all.

© 2012 New Zealand Telecommunications Forum

H. APPENDIX: LOW SPEED DATA CALLS

Discussion Paper prepared by Telecom NZ Ltd

Date: 6 December 2010

Version: 0.1 draft

6.1 Purpose

The purpose of this discussion paper is to identify the major categories of low speed data calls currently extant in the NZ telephony environment. The paper then analyses these categories in terms of scale, complexity and end user impact. Finally it proposes possible methods for resolution.

NOTE:

1. This paper does not indicate a specific position by Telecom NZ Ltd on any particular issue. It serves as a starting point to aid working group discussions.
2. The recommendations in this discussion paper are options only, for consideration as the technical trial progresses.

7.1 Principles

Low speed data is not an individual Service Provider issue – it impacts the whole industry and involves numerous non industry stakeholders

Low speed data is an issue for both IP interconnection and IP access networks. It cannot be considered in isolation.

Support for low speed data calls varies between services providers and is dependent on individual network configurations including codec choices, access technologies and suchlike.

The industry must engage with other stakeholders sufficiently early enough to ensure a managed change for affected end users.

8.1 Assumptions

The Telecom PSTN and other TDM based voice networks will not remain in place beyond 2020. Transition from TDM to IP will accelerate over the course of the next decade. Therefore leaving IP incompatible services on a TDM network is not a long term option.

Different categories of calls may require different solutions.

Solutions are not the sole domain of Service Providers but may also require participation of associated industry players, interest groups and central government.

Scale, importance and end user preference are all factors to be considered in finding appropriate solutions.

For each category of low speed data call a set of logical steps must be taken to assess the most appropriate method to address support of end user services across interconnect boundaries.

Testing of low speed data services by Telecom NZ will help further understand the keys issues for different call type.

Current understanding indicates that use of a low loss codec at the interconnect boundary is the simplest reliable way in which to maintain support on a best efforts basis for voice band data traffic pending end user access solutions rendering low speed data calls redundant.

Irrespective of current workarounds to support interconnecting calls it must be recognised that an end user's data request may need to be interchanged with an end device connected to another Service Provider's network. This indicates that non-voice call types will need definition in the future if they are to be supported across the IP Interconnection NNI under the proposed TCF framework. Alternatives may be bilateral arrangements between Service Providers.

9.1 Resolution Methods

To address future requirements each low speed data call category must be examined using the following steps:

Determine actual scale of transition

1. Identify existing technology options available on end user terminals and their corresponding host networks.
2. Identify alternative options that are currently available.
3. Determine the scale of deployed base that is capable of a migration without terminal change compared with those requiring a terminal upgrade.

Transition Planning

Once the scale of each category is understood transition plans need to be developed in conjunction with the appropriate stakeholders.

Transition plans should consider management of end user expectations, coordination of stakeholders required to execute transitions and cost allocations to parties involved.

Execution

Dependant on scale, import and cost issues a range of options are available to the industry:

1. Grandfathering of certain categories
2. Discontinuation of services
3. Interim service pending technical resolution

10.1 Categories

The categories of Low Speed Data calls considered are:

1. Dial Up Internet Access
2. EFTPOS
3. Interactive Digital TV Decoders
4. Monitored Burglar Alarms
5. Deaf Relay Service
6. Medical Alarms

11.1 Overview Table

	Scale	Characteristics	Stakeholders	Possible Outcomes
Dial Up Internet Access	Large	Long duration calls, low value, large volume	End users Service Providers (ISPs) MED	Exclude from IP Interconnection. SPs retire service aligned to VoIP access migrations.
EFTPOS	Very large	Short call setup and holding times. Very large volume. High value of transactions.	End users Service Providers Eftpos operators Banking institutions MED	Migrate IP capable terminals with VoIP transition. Non compliant terminal replacement programme.
Interactive Digital TV Decoders	Very large	Short call setup. Moderate holding times. Moderate volume?	End users Service Providers Sky TV Freeview	Migrate IP capable terminals with VoIP transition. Non compliant terminal replacement programme.
Monitored Burglar Alarms	Large	Short call setup and holding times. Moderate volume.	End users Service Providers Alarm monitoring companies	Migrate IP capable terminals with VoIP transition. Non compliant terminal upgrade programme
Deaf Relay Service	Low	Medium call setup and long holding times. Low volume. Very significant importance to end users.	End users Service Providers Deaf Relay Service Provider MoH NZ Relay Advisory Group MED Relevant support groups	New technology options provided to new end users and offered as an option to existing end users. TDM interim options should be explored cover the medium term for other end users. . Strong stakeholder engagement required with particular focus applied to the end user community.
Medical Alarms	Medium	Medium call setup and short holding times. Modest volume. Very significant importance to end users.	End users Service Providers MoH DHBs Ambulance Operators	Identify a technical solution. Grandfather current technology. Deploy new technology as soon as available. Replace technology as part of transition.

This table summarises the relevant factors and recommendations for each of the above categories. Details are provider under each category on the following pages.

12.1 Dial Up Internet Access

Scale

Large ~200k end users. 10mln+ minutes/month of traffic.

Characteristics

Long call setup and holding times. Calls free to caller. Majority of end users are very price sensitive e.g. residential low internet usage.

Stakeholders

End users

Service Providers (ISPs)

Ministry of Economic Development

Impact of IP transition

Due to the broad spread of dial up users there are likely to be users connected to most Telecom exchanges. A significant volume of this traffic is interchanged with other Service Providers. Therefore problems are expected early in transition to IP networks, particularly for Service Providers that elect to transition at an exchange/geographic level rather than on a line by line basis. With the ongoing rollout of IP services over broadband access technology, dial up internet is a redundant technology.

To support dial up internet calls is likely to be costly and would serve a declining market.

Recommendation

It is recommended that dial up internet calling be excluded from IP Interconnection and that Service Providers are free to retire the service as they migrate their access networks from TDM to IP.

13.1 EFTPOS

Scale

Very large ~150k end users. Very large volumes of traffic. Very large value of transactions involved.

Characteristics

Short call setup and holding times. Calls free to caller. Majority of end users (Merchants) are very price sensitive e.g. corner store owners, other small businesses.

Stakeholders

End users

Service Providers

Eftpos operators

Banking institutions

Ministry of Economic Development

Impact of IP transition

Due to the ubiquitous nature of EFTPOS terminals there are likely to be terminals connected to every Telecom exchange and presumably other Service Provider's TDM networks. Therefore problems are expected early in transition to IP networks, particularly for Service Providers that elect to transition at an exchange/geographic level rather than on a line by line basis.

Recommendation

Identify existing technology options available on terminals. IP solutions must also meet financial security standards.

Grandfather out of date terminals.

Determine scale of non IP capable terminals.

Communicate changes to end users.

Migration of end users with IP capable terminals onto VoIP access lines proceeds as per Service Providers' own transition plans.

Non IP capable terminals to be replaced. Investigate potential to align any terminal upgrade plans to network transition plans where possible.

14.1 Interactive Digital TV Decoders

Scale

Very large ~800k end users. Large volumes of traffic. Large value of transactions involved.

Characteristics

Short call setup. Moderate holding times. Calls free to caller. Majority of end users are somewhat price sensitive e.g. residential users.

Stakeholders

End users

Service Providers

Sky TV

Freeview

Impact of IP transition

Due to the ubiquitous nature of digital TV decoders there are likely to be terminals connected to every Telecom exchange and presumably other Service Provider's TDM networks. Therefore problems are expected early in transition to IP networks, particularly for Service Providers that elect to transition at an exchange/geographic level rather than on a line by line basis.

Recommendation

Identify existing technology options available on decoders. Determine scale of non IP capable decoders.

Migration of end users with IP capable decoders onto VoIP access lines proceeds as per Service Providers' own transition plans.

Non IP capable decoders to be replaced. Joint industry information campaign to advise end users of need to change out old technology.

15.1 Monitored Burglar Alarms

Scale

Large ~ 100k – 200k end users. Moderate traffic levels.

Characteristics

Short call setup and holding times. Calls free to caller. Majority of end users are not significantly price sensitive e.g. residential home owners, business owners.

Stakeholders

End users

Service Providers

Alarm monitoring companies

Impact of IP transition

Due to the widespread nature of monitored alarms there are likely to be terminals connected to most Telecom exchange and presumably other Service Provider's TDM networks. Therefore problems are expected early in transition to IP networks, particularly for Service Providers that elect to transition at an exchange/geographic level rather than on a line by line basis.

Recommendation

IP based solutions exist today. Some alarm monitoring companies already deploy systems monitored via broadband access lines.

The alarm monitoring industry should be engaged to plan a transition.

Migration of end users with IP capable alarm systems onto VoIP access lines proceeds as per Service Providers' own transition plans.

Upgrades to non IP capable alarm systems proceed as per Service Providers' own transition plans.

16.1 NZ Relay Service/TTY

Scale

Small. ~900 end users. Minimal traffic. Minimal value of transactions involved.

Characteristics

Medium call setup and long holding times. Calls free to caller. End users are technology sensitive. Changing out the user interface is a huge challenge for many end users. Devices use either Baudot or v.18 modems.

Stakeholders

End users

Service Providers

Deaf Relay Service Provider

Ministry of Health

NZ Relay Advisory Group

Ministry of Economic Development

Relevant support groups

Impact of IP transition

Due to the limited volumes involved terminals are not likely to be connected to every Telecom exchange or other Service Provider's TDM networks. Therefore problems may occur later in transition to IP networks.

Recommendation

New technology options should be provided to new end users and offered as an option to existing end users. TDM interim options should be explored such as the use of foreign exchange line type services to cover the medium term. Alternatively local analogue Voice Band Data to IP conversion add on equipment may be required. Strong stakeholder engagement required with particular focus applied to the end user community.

17.1 Medical Alarms

Scale

Moderate. ~50k end users. Call volumes minimal ~500 to 1000 calls per month. Minimal value of transactions involved.

Characteristics

Short call setup and holding times. Calls free to caller. Majority of end users are price sensitive e.g. elderly users, sickness beneficiaries etc.

Stakeholders

End users

Service Providers

Ministry of Health

District Health Boards

Ambulance Operators

Impact of IP transition

Due to the widespread nature of these services there are likely to be terminals connected to numerous Telecom exchange and presumably other Service Provider's TDM networks. Therefore problems are expected early in transition to IP networks, particularly for Service Providers that elect to transition at an exchange/geographic level rather than on a line by line basis.

Recommendation

Identify a technical solution.

Grandfather current technology. Deploy new technology as soon as available to mitigate the scale of the problem. Replace technology as part of transition.

I. APPENDIX: TEST PLANS

General Notes

1. All VoIP handsets should perform echo cancellation. The effect of not doing so will be poor voice quality at the other handset.
2. There must be echo cancellation at each CODEC in any chain of VoIP circuits. In particular, there must be good echo cancellation at the VoIP-PSTN gateway.
3. Modems that don't follow standards by transmitting a 2100Hz answer tone and which transit VoIP are likely not to work.
4. Other things can go wrong. Since modems tend to be tuned to extract the maximum performance out of the available (and limited) bandwidth, they can be extremely intolerant of anything 'different'. Levels of loss, jitter and phase change that would be utterly imperceptible on a real voice call may be enough to prevent a modem or fax call from working at all.

Technical Trial Discussion Paper

18.1 Introduction

This document has been prepared as a straw man for the design of the IP interconnects trial to be conducted between IPWP members once the technical scope has been completed.

Some of the headings are place holders only and may not have much detail under them, this will be fleshed out as required as this document takes form.

19.1 IP Interconnection

It is proposed that as all members of the working party appear to have some network presence in Sky Tower that we use this as the aggregation point for all network connectivity.

Other sites like Mayoral drive may also be possible, but with the rules around connecting between service provider racks this could be an onerous task.

20.1 Network Design

This section provides the basis for network interconnection between the carriers.

NNI

It is proposed to use the NNI model provided by WxC in the draft standards document.

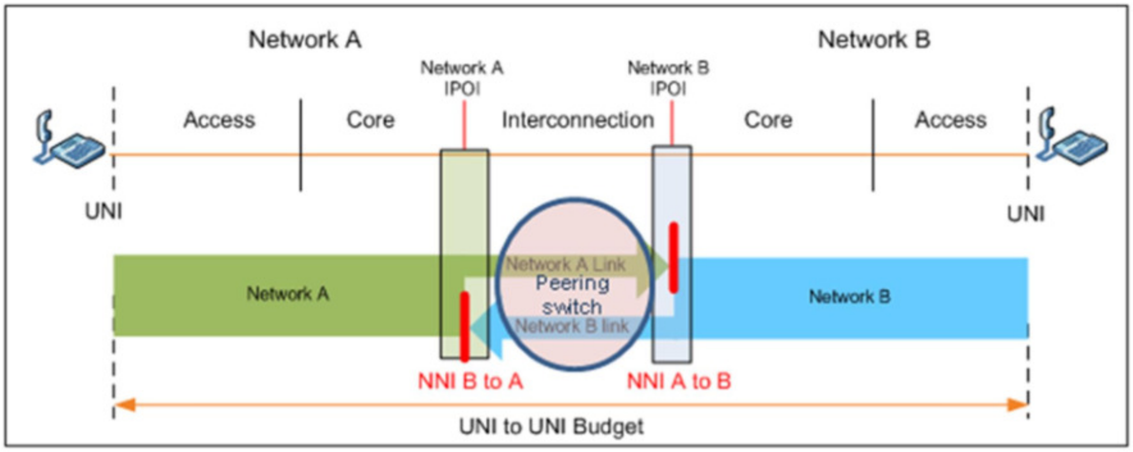
Attribute	Requirements
Physical Medium	1000BASE-LX
Fibre Type	Single Mode, 1310nm centre frequency
Speed	10Mbps, 100Mbps , 1Gbps
Mode	Full Duplex
MAC Layer	IEEE 802.3 - 2005
MTU	1600 bytes Includes: MAC header, Ether type or Length field, any VLAN tags,

	the payload and the FCS

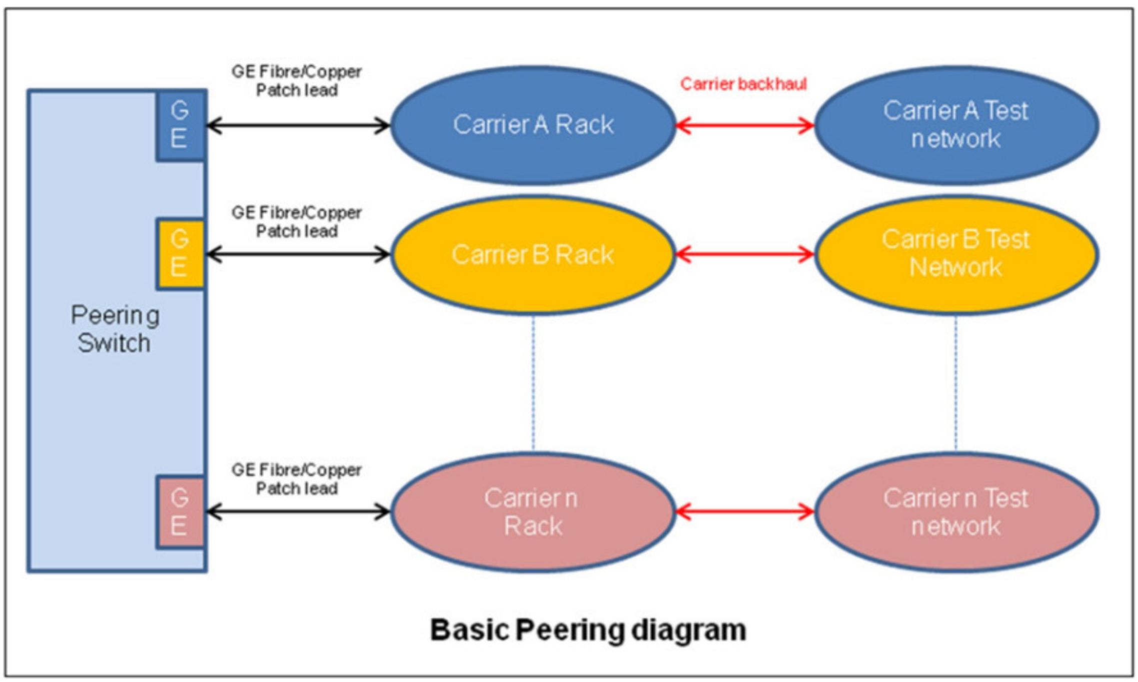
Aggregation (Peering Switch)
It is suggested a switch provided by one of the carriers with a minimum of 100/1000 copper ports is used for the trial as a means of connecting all the test networks together. We could use fibre if desired, but copper at a min would suffice.

A carrier cabinet with spare space or a communal rack could be used to house this switch.

Network Diagram
Network to Network connectivity



Basic peering connectivity



Network Interconnection Template

Carrier	Sky Tower Details		Switch Port	Interface type	Peering switch Port
	Level	Cabinet #			
Peering Switch			N/A	N/A	N/A
Callplus					
Compass	48	4	ge0/?	Copper/Fibre	
Orcon					
Telecom					
TelstraClear					
Vodafone					
WorldxChange					

Routing

Whilst BGP was highlighted as the routing protocol of choice, for the sake of a trial this may be overkill. The peering point would require a router to run BGP routing reflectors (and filters) on as well as a switch.

The easiest choice would be a flat layer 2 network sharing the same IP subnet, private addressing could be used and if each carrier uses VLANS for the test network we should avoid any address clashes with private networks.

21.1 Interworking (SBC to SBC)

Each carrier would be responsible for ensuring their test network is secure and that their Session Border Controllers are setup to allow test traffic to pass between each carrier.

The table below could be used to track which carriers have connectivity

Carrier	Interworking						
	Callplus	Compass	Orcon	TNZ	TCL	VFN	WxC
Callplus	N/A	Y					
Compass		N/A					
Orcon		Y	N/A				
Telecom				N/A			
TelstraClear					N/A		
Vodafone						N/A	
WorldxChange		Y					N/A

The next table could be used to document specific SBC interworking information:

SBC IP settings	Carrier A	Carrier B	Comments
Switch Type			
Switch location			
No of Circuits (CAC)			Per trunk group?
Traffic Type (B/W, O/G, I/C)		B/W	
SBC type			
SBC Location			
SIP version.		2	
SIP Signaling IP address			
RTP IP address 's			
SIP Port		5060	
RTP Port Ranges		40-60K	
Order of Codec selection		G.729, G.711	
SIP option (Keep alive) Yes/No		Yes	
DTMF (RFC 2833) Yes/No		Yes	

Fax		T.38, G.711	Specify G.711 U or A law
Prefix Carrier A to Carrier B			
Prefix Carrier B to Carrier A			

22.1 Interconnection framework

This relates to how the carriers could provision capacity between their networks:

Single Interconnection
This method is used by the tier 2 carriers where a single connection is used for all traffic types. The carriers use the A party and B party numbers to determine the traffic type (e.g. B&K, Transit, National etc)

Multiple Trunk Groups
This may be preferred by the Tier 1 carriers to closely emulate the existing TDM network where traffic types are routed over specific trunk group's and billing etc is based on this.

Failover
This is a Bi Lateral arrangement but could be looked at in the context of multiple interconnect points and how traffic is routed or treated should one fail.

23.1 Call Types

The following headings detail the different types of call to be tested. Test's would have 2 aspects, firstly functional to ensure the call type works and secondly that the calls are treated correctly (CDR information is sufficient to bill on etc)

Also note that the call types listed below are a guide and many of them may not be applicable between carriers. So it is advised test sheets relevant between the carriers should be customised.

Interconnect

Intra Lica
Call between Carrier A and Carrier B in the same LICA (e.g. Auckland to Auckland)

Local Call
Call between Carrier A major LICA and Carrier B minor LICA (in the same LICA, e.g. Auckland to Pukekohe)

National Call
Call terminating in the receiving carriers network outside the originating LICA (Fixed, mobile, special service etc)

Ported numbers
Above scenarios but for ported numbers

TBNCA

National
Carrier A NCA call to national destination via Carrier B network (Fixed and Mobile)

International
Carrier A NCA call to international destination via Carrier B network (Fixed and Mobile)

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.

Transit

Some of these examples can be tested to a third carrier in the working party as well as to other carriers outside of the working party.

National

Calls transiting a carriers network for termination in another national network (fixed, mobile, special service etc)

International

Calls transiting a carriers network for termination in another international network (fixed, mobile, etc)

Service Codes

- Emergency (111)
- Special service codes
- Personal Number Service codes
- Premium Rate codes
- Value Add

24.1 Functional tests

The following functions could be applied to any of the above call types.

Basic functions

- Busy number
- A party release
- B party release
- Disconnected number

IVR

- Bank IVR
- Voice mail service
- Calling card
- International IVR

Call Diversion

- Call transfer
- Call forward

CLIP/CLIR

- All call types

Fax

- All call types

Eftpos

Voicemail

Alarm (not mandatory)

Modem (not mandatory)

25.1 Network performance

Capacity

Capacity testing would be required as a method to determine if network QOS settings are working as expected along with and Call Admission Control.

- Call failure handling (capacity reached, ensure correct cause value mappings to allow originating carrier to re route call)
- Prioritising traffic (e.g. 111 calls)

Network Quality (SLA measures)

- Link stats
- MOS scores
- QOS settings
- Alarm thresholds
- Reporting

© 2012 New Zealand Telecommunications Forum

J. 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