MINISTRY OF HEALTH
MANATŪ HAUORA

hiso Health Information Standards Organisation
PAEREWA PĀRONGO HAUORA

Connected Health Network to Network Interface Specifications

HISO 10037.2

To be used in conjunction with:
HISO 10037.1 Connected Health Architectural Framework
HISO 10037.3:2015 Connected Health User to Network Interface Specifications

Copyright

Keeping standards up-to-date

HISO standards are regularly updated to reflect advances in health information science and technology. Always be sure to use the latest edition of these living documents. We welcome your ideas for improving this standard and will correct any errors you report. Contact us at standards@health.govt.nz or write to Health Information Standards, Ministry of Health, PO Box 5013, Wellington 6145. See the HISO website for information about our standards development processes.

First published September 2010
by the Ministry of Health
PO Box 5013, Wellington, New Zealand

978-0-478-44497-1 (online)
This document is available on the HISO website:
http://ithealthboard.health.nz/standards

Updates

Date	Changes
September 2010	Published
December 2011	Change status from ‘Interim’ Standard to ‘Full’ Standard
April 2014	Removal of historic organisation from document contributors to support legal requirement
July 2016	Move to Creative Commons Attribution 4.0 International licence

Table of Contents

Table of Figures

Table of Tables

Document Contributors

The following contributed to the drafting of this document:

Name	Organisation
Mikel Huth	Ministry of Health
Murray Milner	Milner Consulting Ltd
Steve Martin	Ministry of Health
Steve Miller	Formerly Gen-i
Jamie Baddelley	FX Networks
Health IT Cluster Standards Working Group	A group from the NZ health service provider community, including Datacraft, Smartlinx3, Kordia, Gen-i, Telecom, FX Networks, Microsoft, HealthLink, VividSolutions.

The terms ‘normative’ and ‘informative’ are used in Standards to define the application of an appendix. A ‘normative’ appendix is an integral part of a Standard, whereas an ‘informative’ appendix is only for information and guidance and does not form part of the mandatory requirements of the Standard.

Related Documents

HISO Standards
HISO 10029:2015 Health Information Security Framework
HISO 10037.1 Connected Health Architectural Framework
HISO 10037.2 Connected Health Network to Network Interface Specifications
HISO 10037.3:2015 Connected Health User to Network Interface Specifications

New Zealand Legislation
Telecommunications Act 2001

New Zealand Standards
SNZ HB 8169:2002 Health Network Code of Practice

Other Standards
Health Level Seven Inc., HL7 Standard version 2.4 - An Application Protocol For Electronic Data Exchange in Healthcare Environments.

Other Connected Health Documents
Connected Health: An Overview
Connected Health Principles
Connected Health Operational Policy for Telecommunications Service Providers
Service Management Guide

Other Publications/Websites
Commerce Commission 13 December 2007 (incorporates clarifications up to 8 July 2010). *Standard Terms Determination for Telecom's Unbundled Bitstream Access Service* URL: http://www.comcom.govt.nz/assets/Telecommunications/STD/UBA/UBA-STD-as-at-8-July-2010/UBA-STD-General-Terms-8-July-2010.pdf Accessed 17 August 2010.
International Telecommunication Union – Telecommunication Standardisation Sector 2006. Recommendation Y.1541 *Network performance objectives for IP-based services* URL: http://www.itu.int/rec/T-REC-Y.1541-200602-I Accessed 17 August 2010.
InternetNZ, NZ Marketing Association, Telecommunications Carriers' Forum 2007. *Internet Service Provider Spam Code of Practice* URL: http://www.tcf.org.nz/library/45a3afab-3e1d-4d43-b8d4-b6d73cfbd201.cmr Accessed 17 August 2010.
IT Health Board 2010. *National Health IT Plan* URL: http://www.ithealthboard.health.nz/our-plan Accessed 17 August 2010.
MIT Communications Futures Program 2006. *Interprovider Quality of Service whitepaper* version 1.1URL: http://cfp.mit.edu/docs/interprovider-qos-nov2006.pdf Accessed 17 August 2010.
Telecom Wholesale 2010. *Product Profile: High Speed Network Service* URL: http://www.telecomwholesale.co.nz/f73,1460/1460_25751_HSNS_3-0.pdf Accessed 17 August 2010.
Telecom Wholesale 2008. *Product Profile: Unbundled Network Service* URL: http://www.telecomwholesale.co.nz/f77,5705/5705_22570_UNS_A3_2-0.pdf Accessed 17 August 2010.
Telecommunication Carriers' Forum 2009. *Guidelines for Undertaking Community Engagement for Wireless Telecommunications Facilities* URL: http://www.tcf.org.nz/library/2f5239c7-446e-4171-8ff3-387d01b1f85a.cmr Accessed 17 August 2010.

Telecommunication Carriers' Forum 2007. *Co-siting Code* URL: http://www.tcf.org.nz/library/c4efc274-8252-4482-9e2c-0c679dc8f899.cmr Accessed 17 August 2010.
Telecommunication Carriers' Forum 2008. *Customer Complaints Code* URL: http://www.tcf.org.nz/library/b6808eed-f840-4d29-bb52-9693e610eaff.cmr Accessed 17 August 2010.
Telecommunication Carriers' Forum 2006. *Code for the Transfer of Non Regulated Telecommunications Services* URL: http://www.tcf.org.nz/library/c96a3a73-ebb3-4ec3-a48b-68afe0d17eb7.cmr
Telecommunication Carriers' Forum 2006. *Code for the Transfer of Telecommunications Services* URL: http://www.tcf.org.nz/library/d72c3ecf-8f4e-4871-9deb-f1b9e566ac3f.cmr Accessed 17 August 2010.
Telecommunication Carriers' Forum 2008. *Disconnection Code* URL: http://www.tcf.org.nz/library/2c5f7197-fca9-4763-a7dc-e4464755f978.cmr Accessed 17 August 2010.
Telecommunication Carriers' Forum 2009. *Emergency Calling Code* URL: http://www.tcf.org.nz/library/a4a3ad46-2e90-42f3-8733-a66f7bd1065c.cmr Accessed 17 August 2010.
Telecommunication Carriers' Forum 2009. *Guidelines for Interception Capability* URL: http://www.tcf.org.nz/library/cc58568d-2100-46a8-9cfc-982c3d0679d8.cmr Accessed 17 August 2010.
Telecommunication Carriers' Forum 2008. *Code of Practice for Provision of Content via Mobile Phones* URL: http://www.tcf.org.nz/library/90423ff2-0e52-4eeb-985e-0b00e9d2a854.cmr Accessed 17 August 2010.
Telecommunication Carriers' Forum 2008. *Mobile Premium Messaging Services Code* URL: http://www.tcf.org.nz/library/163a6fd5-abd8-4774-9497-391afa6c1c9c.cmr Accessed 17 August 2010.
Telecommunication Carriers' Forum 2010. *Code for Residential and SOHO Premises Wiring* URL: http://www.tcf.org.nz/library/e72d1374-8040-4022-ba79-428d56eb4a9b.cmr Accessed 17 August 2010.
Telecommunication Carriers' Forum 2008. *Code for the Control of Unauthorised Use of Mobile Phones in Prisons* URL: http://www.tcf.org.nz/library/e7b0100d-e056-4ef7-9d12-c18e5b4fb103.cmr Accessed 17 August 2010.

1 Introduction

1.1 Background

Currently health information is accessed from and transferred over many different types of computers, telecommunications networks and information systems in the New Zealand health sector. Often these have been implemented in isolation of one another making it difficult and costly to share information between providers and systems in a secure way.

In a person-centred health system the ability to connect services, applications and systems is essential for allowing patients to be cared for by the right clinician, at the right time and place, providing access to their records electronically with the confidence that information is kept secure at all stages.

The Connected Health (CH) programme is a key step in achieving this aim. Its purpose is to establish the secure environment needed for the safe sharing of health information between all the participating health providers. To achieve this, the programme is delivering the following foundation components:

- a common connectivity framework
- connectivity standards
- core network components
    - three managed points of interconnection
    - a uniform addressing scheme
- an accreditation and certification process for telecommunication service providers
- governance and management oversight.

To date, the connectivity standards delivered include:

- HISO 10037.1 Connected Health Architectural Framework
- HISO 10037.2 Network to Network Interface Specifications (this document)
- HISO 10037.3:2015 User to Network Interface Specifications

Further specifications and standards will be developed over time.

Further background information about CH, product certification and supplier accreditation can be found in Connected Health: An Overview.

1.2 Document purpose

The CH Architectural Framework describes the role of and the need for Network to Network Interfaces (NNIs).

This document expands on the design principles listed in the Framework and details the technical specifications for NNI-1, NNI-1a, and NNI-2. It defines a set of minimum characteristics for each network to network interface in the Framework and forms the baseline requirements for the definition of standardised CH certified interconnection products.

1.3 Target Audience

This technical specification is intended for organisations looking to provide certified telecommunications services in the CH environment. It is also intended for CH management to inform policy and procedure development around accreditation of Telecommunication Service Provider (TSP) organisations, and certification of products and solutions.

2 Points of Interconnect

The CH network will initially deliver three Points of Interconnect (POI). The POIs provide 'meet me' functionality for TSPs. The POIs will be installed in Auckland, Wellington and Christchurch, in locations providing practical access to the widest selection of potential providers. They will enable the implementation of the NNI-1 performance requirements.

The POIs will be owned by CH and will consist of at least:

- a dedicated and secure cabinet
- fibre and cable management
- a gigabit ethernet switch
- a router or route server supporting Boarder Gateway Protocol (BGP)
- quality of Service (QoS) measurement equipment.

Due to the size of the network, switching and routing functionality may be combined into one device.

3 Interface Specifications

CH network services could be provided by multiple TSPs. To supply seamless Internet Protocol (IP) connectivity for CH consumers and providers, some level of TSP network interconnectivity domains, or interconnection points are required for public internet network traffic, and CH private IP traffic.

Establishing CH accredited interconnection points will ensure that equal access is provided for all potential CH TSPs. This will enable wide access to telecommunications products for CH service providers and members. Some IP domains are interconnected and this interconnection could be achieved with links that traverse interconnection points.

3.1 Requirements

Table 1 below lists the minimum requirements for these interconnectivity domains or peering points.

Table 1: Basic NNI definition

Definition	Properties
Private IP Interconnection (NNI-1)	• 1Gbps, Layer 2 (Layer 3 aware) or Layer 3 connectivity. • TSPs must support BGP peering for Internet Protocol version 4 (IPv4)[1] unicast and multicast. • Support Institute of Electrical and Electronic Engineers (IEEE) 802.1p and Differentiated Services Code Point (DSCP) markings. • TSPs must connect, or arrange transport to connect to each of the POIs. There are three initial locations: Auckland, Wellington and Christchurch. Further locations may be added as demand requires. • Transport between interconnects must not be delivered using a public IP network. • TSPs must advertise only CH registered addresses into the CH network over the NNI-1. • TSPs must accept all CH registered addresses exposed over the NNI-1.

[1] The IPv4 is an interface reserved for the interconnection of private TSP IP domains. The NNI should ensure integrity of transfer for traffic and management functions across the interface, from a performance, security and quality perspective.

Definition	Properties
Private IP Interconnection (NNI-1a)	• ≥100Mbps, Layer 2 (Layer 3 aware) or Layer 3 connectivity. • Supports regional or limited reach TSPs, who are unable or unwilling to connect to all POIs. • Redundant Layer 3 connectivity must support BGP peering for IPv4 unicast and multicast. • Single or redundant layer 2 connectivity may support static routing. • Transport between interconnects must not be delivered using a public IP network. • TSPs must advertise only CH registered addresses into the CH network over the NNI-1a. • TSPs must accept all CH registered exposed over the NNI-1a.
Public IP Interconnection (NNI-2)	• ≥100Mbps, Layer 2 (Layer 3 aware) or Layer 3 connectivity. • Supports networks where CH traffic is not logically separated from other traffic. • CH traffic is secured through the use of tunnelling and encryption as per the HISO 10029 Health Information Security Framework (HISF). • TSPs must advertise only CH registered addresses into the CH network over the NNI-2. • TSPs must accept all CH registered addresses exposed over the NNI-2.

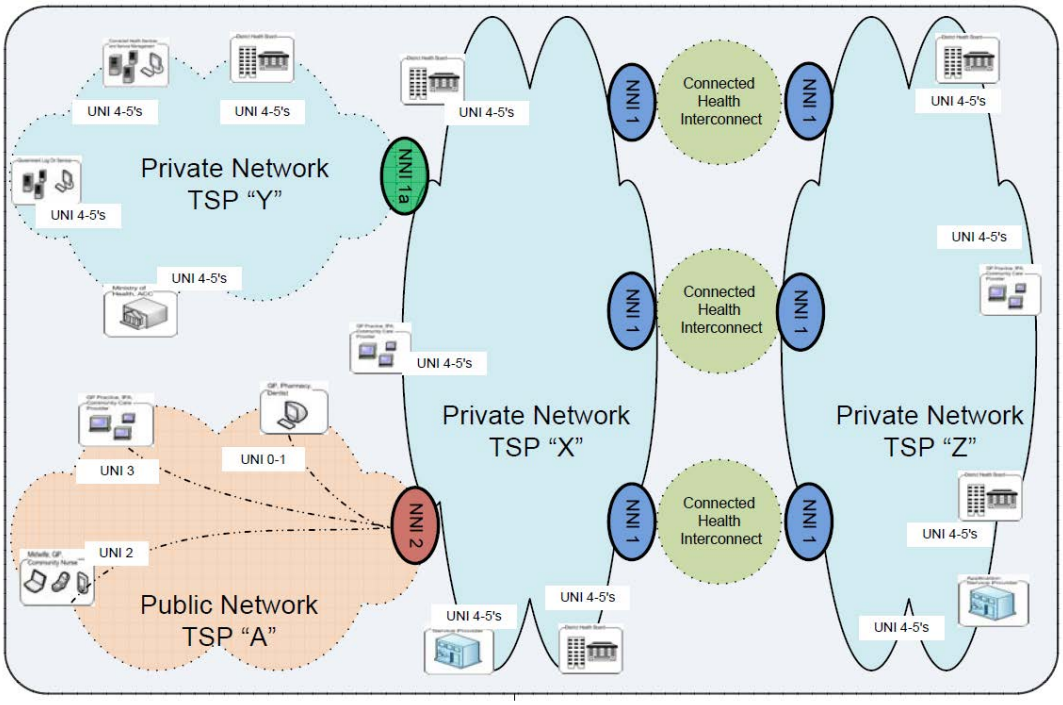
The NNI-1 is an interface reserved for the interconnection of private TSP IP networks.

The NNI-1a is used where the TSPs supply service over a private network, but rely on other TSPs to provide connectivity to the POI. The specific requirements for the NNI-1a would be negotiated between TSPs (TSP Y and TSP X in Figure 1) to ensure the end to end performance criteria can be achieved.

The NNI-2 is an interface reserved for Virtual Private Network (VPN) termination. The NNI provides termination of VPN sessions and tunnels from public IP end-points to the CH network, for routing of traffic to other NNIs or User to Network Interfaces (UNIs). NNI-2 must be connected to all POIs via a private TSP.

Figure 1 shows a typical CH network of networks topology, with UNI to UNI service achieved via multiple IP networks interconnected by multiple NNI links.

Figure 1: Typical CH network of networks topology



Connected Health – a "network of networks"

The CH 'network of networks' is made up of an integrated network of interconnected IP networks provided by the TSPs (refer to Figure 1).

Each network has a number of certified CH UNIs connected to it. Public networks support UNI-0, UNI-1, UNI-2 and UNI-3 while UNI-4 and UNI-5 are supported by the TSPs private IP network, typically in the form of MultiProtocol Label Switching (MPLS) based Virtual Private Networks (VPNs). The UNIs can be physically located anywhere within New Zealand.

Two or more interconnection links provide connectivity between each network domain. The interconnection links are defined as NNI-1. The specification for NNI-1 is that any traffic sent from one UNI to another UNI will meet all requirements of the involved UNIs. Therefore, the integrity of end to end traffic will be maintained as the traffic traverses from one UNI to another UNI including any traffic transfer across network boundaries.

In Figure 1:

- TSP X offers UNI, NNI-1a and NNI-2 connections to downstream customers/TSPs.
- TSP Y only offers UNI connections and is connected to the CH network via an upstream private TSP (X) which acts as a transit TSP for TSP Y.
- TSP Z only offers UNI connections and has a presence at each POI.
- TSP A only offers UNI-0, UNI-1, UNI-2 and UNI-3 and transports traffic via VPNs into NNI-2 which is connected to TSP X for routing over CH.

Table 2 specifies the requirements of the three types of NNIs. In accordance with the CH architectural principle of Openness (refer to HISO 10037.1 Connected Health Architectural Framework*)* access to applications and services connected by a UNI must be available to all participating suppliers and sector organisations.

Table 2: Detailed NNI specifications

NNI-1		
Description	**Minimum Requirements**	**Preferred Requirements**
Private IP NNI. The boundary between TSPs and POI provide interconnection for CH private IP traffic moving between TSPs that are providing private IP services to CH members. Therefore any UNI connected participants must be able to access all services and users as authorised by the user's access profile.	1Gbps, Layer 2 (Layer 3 aware) or Layer 3 connectivity. Each provider IP carrier network interconnecting at a NNI must use a unique Autonomous System Number (ASN). Must only advertise CH registered routes. Each NNI connection must exchange CH route table information with all other partner NNI(s) using a common interconnection point. NNI-1 will be implemented by the TSP at all the CH private IP interconnection points. Interconnect traffic will be handled in a non discriminatory manner as it traverses NNI-1. It is up to the originating network provider to ensure that traffic flows are marked correctly, in accordance with the Class of Service (CoS) tags as defined for the respective UNIs. QoS markings shall not be changed at the NNI boundary. No trans-coding shall be undertaken at the NNI-1 boundary. Each NNI-1 link must be dimensioned to accommodate the aggregate traffic flowing across the link from all UNIs using the given link, including the breakdown of traffic into aggregate CoS streams. Abides by the Telecommunication Carriers Forum (TCF) codes of practice.	Meet or exceed minimum requirements

Table continued on the following page.

Table 2: Detailed NNI specifications continued

NNI-1a		
Description	**Minimum Requirements**	**Preferred Requirements**
Private IP NNI. The boundary between regional and transit TSPs, provides interconnection for CH private IP traffic moving between TSPs that are providing private IP services to CH members. Therefore any UNI connected participants must be able to access all services and users as authorised by the user's access profile.	≥100Mbps, Layer 2 (Layer 3 aware) or Layer 3 connectivity. Each provider IP carrier network interconnecting at a NNI must use a unique ASN. Must only advertise CH registered routes. Must provide universal connectivity to CH network. It is up to the originating network provider to ensure that traffic flows are marked correctly, in accordance with the CoS tags as defined for the respective UNIs. QoS markings shall not be changed at the NNI boundary. No trans-coding shall be undertaken at the NNI boundary. Each NNI-1a link must be dimensioned to support the end to end QoS budgets of all traffic streams flowing across the NNI. Abides by the TCF codes of practice.	Preferred requirements to be agreed between interconnecting parties
NNI-2		
Description	**Minimum Requirements**	**Preferred Requirements**
VPN termination to NNI provides termination of VPN sessions and tunnels from end-points to the CH network, for routing of traffic to other NNIs or UNIs. Provides a boundary between public networks and the CH environment. Therefore any UNI connected participants must be able to access all services and users as authorised by the user's access profile.	>100 Mbps tunnelled Layer 2 or 3 connectivity. Only 'encryption domain' routes can be advertised into the CH network and must be CH registered. NNI-2 providers must ensure that these interconnection points comply with minimum CH performance, security and throughput requirements. NNI-2 providers are responsible for providing all encryption equipment and credentials. Abides by the TCF codes of practice.	Meet or exceed minimum requirements

3.2 Routing Policy

3.2.1 NNI-1

When peering with the POI route servers (NNI-1) the following policies apply:

- Providers must only originate their assigned CH routes.
- Providers must advertise their CH assigned summary route at all POIs.
- Providers must advertise summary routes with consistent metrics at all POIs.
- Providers must accept all CH routes advertised to them from the CH route servers.
- Providers may use public or private ASNs (ASN 32-bit). Private ASNs will be assigned by the CH network if required.
- Providers are free to advertise routes which are a subset of their CH assigned routes to any of the POIs.
- Transit TSPs must advertise their client TSP summary routes at all POIs.

3.2.2 NNI-1a and NNI-2

When peering between providers (NNI-1a and NNI-2), the following policies apply:

- Providers must only originate their assigned CH routes.
- Providers must accept all routes advertised to them.
- Providers may use public or private ASNs. Private ASNs will be assigned by the CH network.
- Providers are free to advertise routes which are a subset of their CH assigned routes at any of the NNIs.
- Downstream providers must advertise their CH assigned summary route at all NNIs.
- Upstream (transit) providers must advertise either a default route, the CH network summary route, or all discrete CH network routes (or a combination) to their downstream TSPs.
- Providers may negotiate between themselves the metrics used to determine path selection.

3.2.3 CH routing

The CH network is initially expected to utilise ’Hot Potato’ routing and the CH route servers may manipulate metrics in an effort to enforce this.

3.3 Performance requirements for NNI

Table 3: Performance requirements for NNI

Business Requirements	Service Level
Industry Best Practice	The network must incorporate design and configuration characteristics in line with industry best practice.
Auditing	As part of maintaining CH certification, TSPs may be subject to audit of the implementation of NNI against this specification by CH (or its assigned agent).
Fit for Purpose	The provider warrants that the network, including Customer Located Network Equipment (CLNE), is suitable for the business objectives outlined in the CH architecture.
Scalability	The deliverables are to incorporate a flexible architecture with scalable capacity to support changing requirements and new applications, or services that CH may choose to deploy to the network. The network has been scoped to allow for those applications detailed under the 'fit for purpose' business requirement above, to function at the sites within the network performance as detailed below.
Reporting	The provider will provide to CH (or its assigned agent) on request: • Live reports – online reports based on actual data that is typically refreshed every 5-15 minutes (i.e. 'real time' reports). Live reports include: ◦ Utilisation (measured at interfaces, CoS queues and CLNE) ◦ Traffic (throughput, average packet size, packet discards) ◦ CoS/QoS performance (Latency, Jitter and Packet Loss) ◦ CLNE health (Port up/down status, traffic level, utilisation and error rate). • Static reports – paper reports based on actual data that has been accumulated over a defined period of time (i.e. 'historical' reports). These reports compare actual data with service targets (i.e. one means by which CH can measure service level targets). Static reports include: ◦ Faults (fault restoration times vs. service targets) ◦ Availability (overall availability vs. service targets).

Table continued on the following page

Table 3: Performance requirements for NNI Continued

Business Requirements	Service Level
Security and Privacy	The provider warrants that any data passed over any network boundary: • will not be modified in any way except by written agreement with CH • will not be passed to or become accessible to any non CH third party without express written permission from CH.
Monitoring Access	The provider will provide to CH (or its assigned agent) Simple Network Management Protocol (SNMP) (SNMP v.2c or higher) read/write access to CLNE devices for network management system(s) and to assist in problem resolution as required.
Network Service Desk	A network service desk will answer telephone calls from CH (or its assigned agent), or the providers' customers on a 24 hour – 7 day a week basis and will log information relevant to a fault or other details relevant to the service required by CH.

Availability, Monitoring and Restoration		
Service Delivery **- all sites**	**Monitoring Hours:** 24 hours x 7 days	The hours during which infrastructure monitoring systems are operational.
	Alarm Notification: Within 45 minutes of alarm occurrence.	The elapsed time between a service impacting alarm or an event occurs and CH being notified that it has occurred and is being investigated.
	Response Time: 30 minutes for severity 1 faults, otherwise 60 minutes.	The elapsed time during agreed service hours between the provider receiving a call from CH or alarm occurrence and the provider commencing restoration work. An estimated restore time is to be provided if known.
	Initial Restoration Update: 30 minutes for severity 1 faults, otherwise 60 minutes.	The elapsed time during agreed service hours between the provider receiving a call from CH or alarm occurrence and CH being notified that initial diagnosis is completed. An estimated restore time is to be provided.
	Progress Updates: Hourly or as agreed.	Progress updated on the status of service restoration activity.

Table continued on the following page

Table 3: Performance requirements for NNI Continued

Availability, Monitoring and Restoration		
Service Delivery **- all sites**	**Remote Service Restoration:** 80% within 2 hours, otherwise 4 hours.	The elapsed time during agreed service hours between the provider receiving a call from CH or alarm occurrence and CH being notified that service is restored to the defined levels without a site visit.
	Planned Outage Notification: 5 business days.	Prior notice of planned maintenance that could cause service outage. If the provider notifies CH that such planned maintenance is scheduled outside CH's normal maintenance window then CH may withhold consent (acting reasonably) for such planned maintenance to proceed at those times. If the provider undertakes the planned maintenance irrespective of CH's failure to consent, any such planned maintenance will be measured against the provider's availability service levels.
	Exception Reports: Within 7 business days of the end of each month.	The provider will provide exception reports to CH (or its arranged agent). Exception reports will be defined in Service Level Agreements (SLAs)[2] or Operating Level Agreements (OLAs).
	Incident Reports: Draft Report – Within 24 business hours of incident logging. Final Report – Within 24 business hours of incident closure.	The provider will provide incident reports to CH (or its arranged agent). Incident reports will be defined in SLAs or OLAs.
Availability (per Link)	The service is available for CH use and functioning in accordance with the product definition against the following performance targets: **Metro:** 99.9% **Rural:** 99.8%	

Table continued on the following page

[2] This document defines what is required for SLA measurements but not how SLA measurements will be carried out.

Table 3: Performance requirements for NNI Continued

Time Period	Cumulative service unavailability (based on total outage minutes per month)	
	Metro sites (99.9%)	**Rural Sites (99.8%)**
Calendar month	≤ 43 minutes per site.	≤ 86 minutes per site.

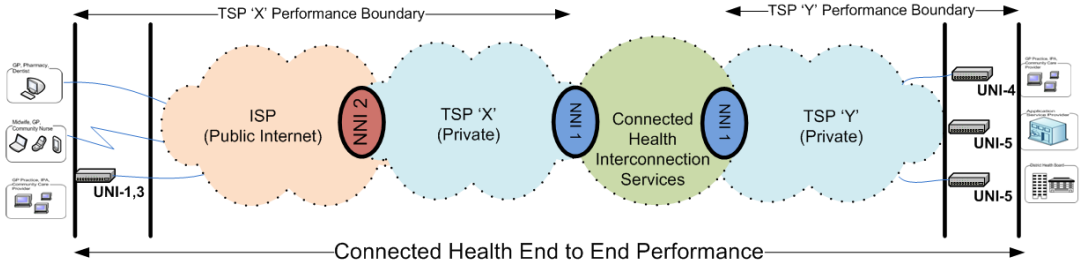
Geographic Areas: New Zealand locations	
Metro	Within 30 kilometres of central Auckland, Hamilton, Rotorua, Tauranga, New Plymouth, Napier, Wellington, Palmerston North, Nelson, Christchurch and Dunedin
Rural	All other New Zealand locations

3.4 Performance Measurement

All CH certified NNI SLAs are measured between the CH UNI and the Service Provider NNI-1.

Where a TSP (either public or private) obtains transit to an NNI, the transit network is included in the TSP's performance boundary. This is illustrated in Figure 2 below.

Figure 2: CH end to end performance

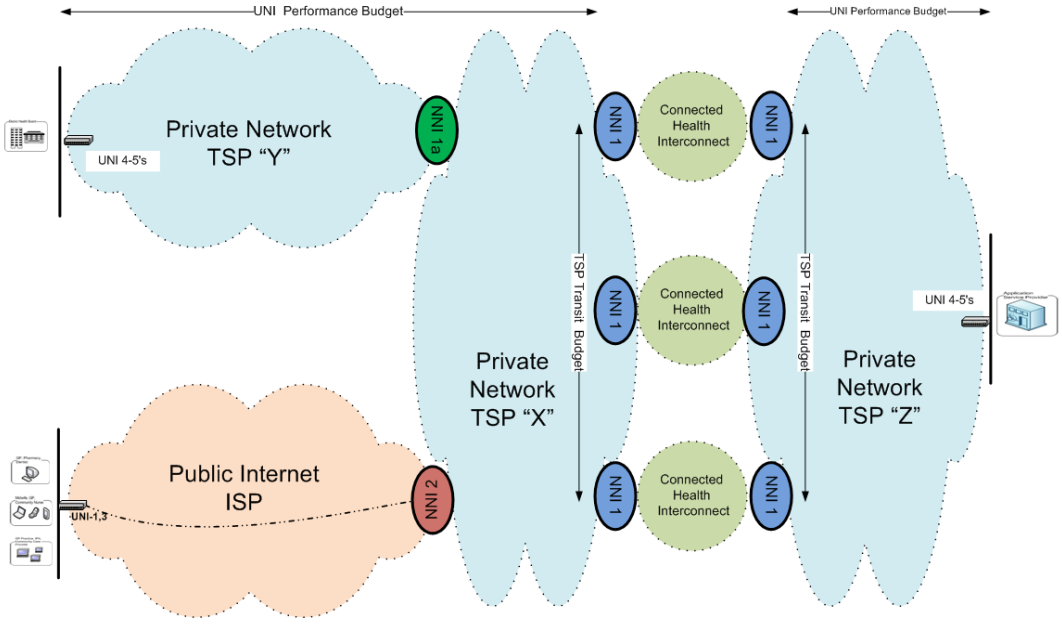


3.5 QoS Budgets

The end to end performance budget of a circuit can be broken down into three parts. As well as each end of the circuit (UNI) having its own budget (which is separately defined in the UNI specification), the interconnection points themselves will be assigned a budget. The interconnect budget is an allowance for transport between any of the interconnect points.

This is illustrated in Figure 3 as the TSP transit budget.

Figure 3: Performance budgets



Note: Budgets are always defined in a uni-directional manner i.e. they are specified between the sender UNI and the nearest NNI-1. In some cases, the measured metrics in one direction will differ greatly from the return path. This may be because of asymmetric circuit rates or asymmetric routing. All paths in any direction must comply with the QoS performance budget.

3.5.1 TSP transit budget

The interconnect, or TSP transit budget is measured between each of the interconnect points, using SLA monitors placed within each interconnection point, and is the responsibility of the TSP providing the transit.

Table 4 describes the QoS budgets allowed within and between the interconnection points (sender to receiver) and shall be measured over each calendar month in accordance with the recommendations found in International Telecommunication Union– Telecommunication Standardisation Sector 2006. (ITU-T) Recommendation Y.1541 (refer to Related Documents). The CH POIs themselves are not factored in these budgets as they will have a negligible impact on performance.

Table 4: Network performance under normal operating conditions (99.9% of calendar month)

	Real Time	**Interactive**	**Best Effort**
IPTD (Latency)	15ms	20ms	20ms
IPDV (Jitter)	2ms	5ms	5ms
IPLR (Loss)	0.1%	0.1%	0.5%*****

*Best Effort must meet or exceed 0.1% Internet Packet Loss Ratio (IPLR) for 90% of each calendar month.

Although the Interactive and Best Effort classes have the same performance metrics, this is a reflection of high performance IP networks, rather than a specific requirement.

3.5.2 UNI budget

The UNI budget is measured to the closest interconnect point as nominated by the providing TSP. This can be measured using the UNI Customer Premises Equipment (CPE) as responders to a SLA monitor. However, 'hardware' time stamping and clock synchronisation would be required to get accurate one way metrics.

UNI and interconnect budgets are subject to review as required. The provider will be notified if a review is necessary. For example, a review may be required if additional interconnect points are added.

Where a public or private network is connected to the CH network via a private network, the budget allowance for the UNI is still measured to the closest interconnect.

3.6 QoS Classification

Table 5: QoS Classification

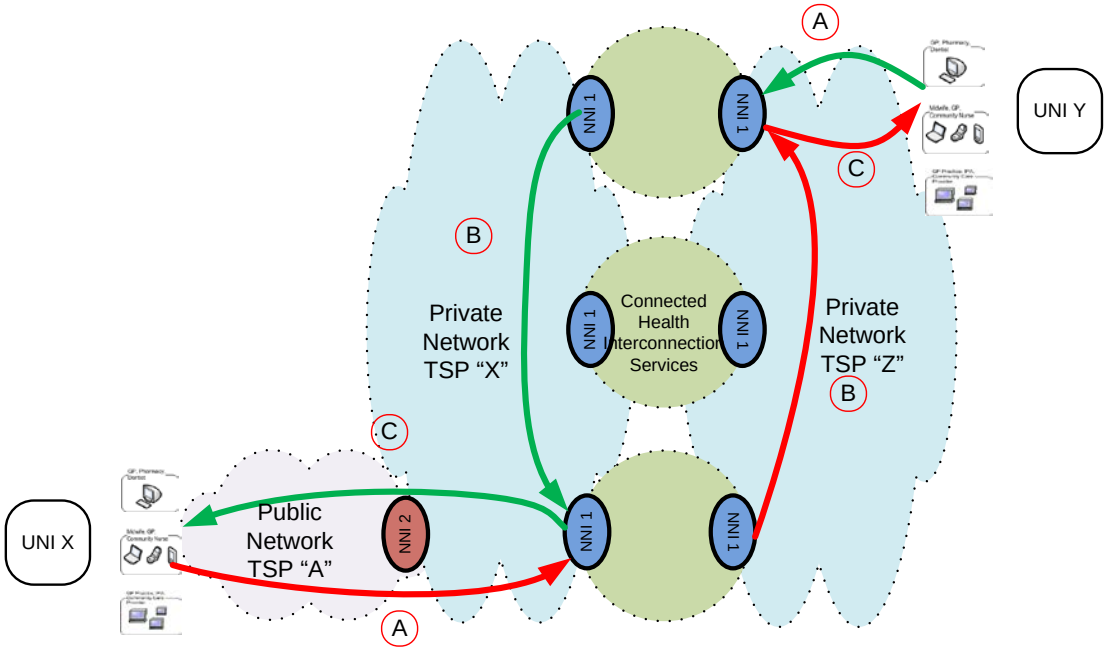
CoS Queue	Usage Type	DSCP	Binary	Decimal	Preferred/ Supported		
	Reserved	Nc2/cs7	111000	56			
		Nc1/cs6	110000	48			
Realtime	IP Voice	Ef	101110	46	Preferred		
		Cs5	101000	40	Preferred	NNI-1	
	Interactive Video	Af41	100010	34	Preferred		
		Af42	100100	36	Supported		
		Af43	100110	38	Supported		
		Cs4	100000	32	Preferred		
Interactive	Interactive data	Cs3	011000	24	Preferred		
		Af31	011010	26	Preferred	NNI-1	
		Af32	011100	28	Supported		
		Af33	011110	30	Supported		
		Cs2	010000	16	Supported		
		Af21	010010	18	Supported		
		Af22	010100	20	Supported		NNI-2
		Af23	010110	22	Supported		
Best Effort	Data	Af11	001010	10	Supported		
		Af12	001100	12	Supported		
		Af13	001110	14	Supported		
		Cs1	001000	8	Supported		
		Be	000000	0	Preferred		

3.7 Performance Diagram for Differentiated QoS: Real time, Interactive and Best Efforts

Figure 4 illustrates the various components in the end to end budget, and where they are measured. The diagram assumes 'Hot Potato' routing, i.e. TSPs will tend to deliver traffic to the closest interconnection point.

Budgets used in the examples may not reflect the actual budgets for a service but are used for illustration purposes only.

Figure 4: End to end performance budget allocations by best efforts QoS category and UNIs



The above diagram illustrates a UNI 0-3 to UNI 4-5 customer connection, and Table 6 below shows how the latency budget for best effort (for example) are assigned.

3.7.1 Best Effort examples

Table 6: Best Effort examples

UNI X	UNI Y	"A" budget	"B" budget	"C" budget
0,1	4	400ms	20ms	100ms
0,1	5	400ms	20ms	100ms
2	4	400ms	20ms	100ms

This is an example based on the NNI-2 UNI 0-3 provider connecting to an NNI-1 via UNI 4-5 to access CH services or other UNI connected consumers. It is expected that the budget allocations for device to carrier, across TSP, will reflect the physical delivery used.

Figure 5: End to end performance budget allocations for interactive and real-time QoS categories and UNIs

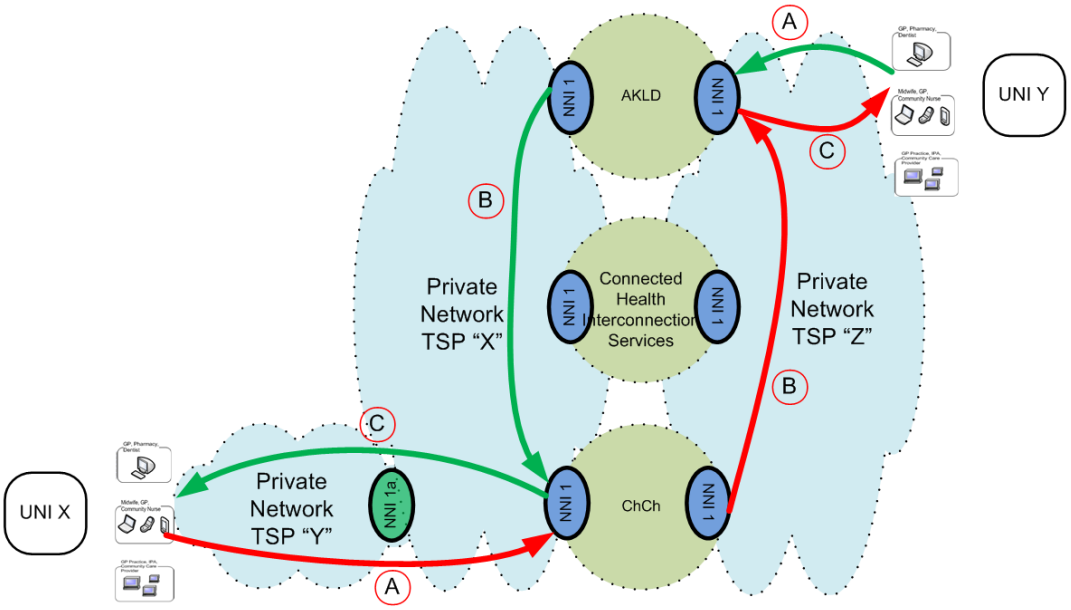


Figure 5 illustrates a UNI 4-5 to UNI 4-5 customer connection. Tables 7 and 8 show how the latency budget for interactive and real time classes (for example) are assigned.

3.7.2 Interactive class examples

Table 7: Interactive class examples

UNI X	UNI Y	"A" budget	"B" budget	"C" budget
4	5	50ms	20ms	25ms
5	5	25ms	20ms	25ms

3.7.3 Real time class examples

Table 8: Real time class examples

UNI X	UNI Y	"A" budget	"B" budget	"C" budget
4	5	20ms	15ms	10ms
5	5	10ms	15ms	10ms

3.7.4 Assumptions

- That there will be no more than two NNI transversals for any CH connection.
- The performance characteristics are based on international standard ITU-T Y.1541 (refer to Related Documents) for end to end QoS. However it is recognised that New Zealand's size allows for tighter budgets.

3.8 Requirements for CH Products to Deliver Agreed QoS

Admission control is a challenging issue for any IP network. Admission control will be the subject of further CH developments.

3.9 Roles and Responsibilities

Table 9 describes the different classes of organisation that exist within the CH community, along with the services that they must provide or use and any rules that govern their operations. Organisations may provide services from more than one organisational category listed below.

Table 9: Roles and responsibilities of CH organisations

Description	Example	Minimum services provided	Services consumed	Mandatory Accreditation Requirements
Consumer				
Consumes applications and services	District Health Board (DHB), Primary Health Organisation, Non-governmental organisation, General Practice	None	UNI 0-5	Comply with the Health Network Code of Practice (HNCOP) and the HISO 10029 Health Information Security Framework (HISF).
Application Service Provider (ASP)				
Provides applications	Ministry of Health, DHB, Vivid Solutions, ASPX	UNI 3-5 connecting to a TSP network. Application appropriate help desk, customer billing, SLA reporting	UNI 3-5 connection	To be a CH accredited ASP the organisation must utilise a UNI 3-5 connection connected to the CH network to expose their service to users of the CH Network. If a product is certified as a national service it must provide appropriate resiliency.

Table continued on the following page.

Table 9: Roles and responsibilities of CH organisations Continued

Description	Example	Minimum services provided	Services consumed	Mandatory Accreditation Requirements
Retail Telecommunications Service Providers				
Provides UNI and NNI	Gen-i, FX Networks, Kordia, Vodafone	UNIs, NNIs. 24/7 tier 1 help desk, customer billing, SLA reporting.	NNI	To be accredited as a CH TSP the organisation must: • Have NNI-1s connected to each POI or obtain transport to each POI. • Support at least one certified UNI and either an NNI-1 or and NNI-2 as appropriate to the UNI types supported. • Be a registered network service provider as defined under the Telecommunications Act 2006. • Not restrict who their users can access or who can access their users within the CH environment. • Any TSP supporting UNI-4 or UNI-5 must support an NNI-1 and either connect to all defined CH POIs, or use the NNI-1 to connect to an accredited Transit TSP, which by definition connects to all defined CH POIs. • To be accredited to provide UNI 1-3 products the service provider must support an NNI-2 connection to CH to ensure termination of the VPN tunnels and the NNI-2 must be connected to at least one CH NNI-1.

4 Examples

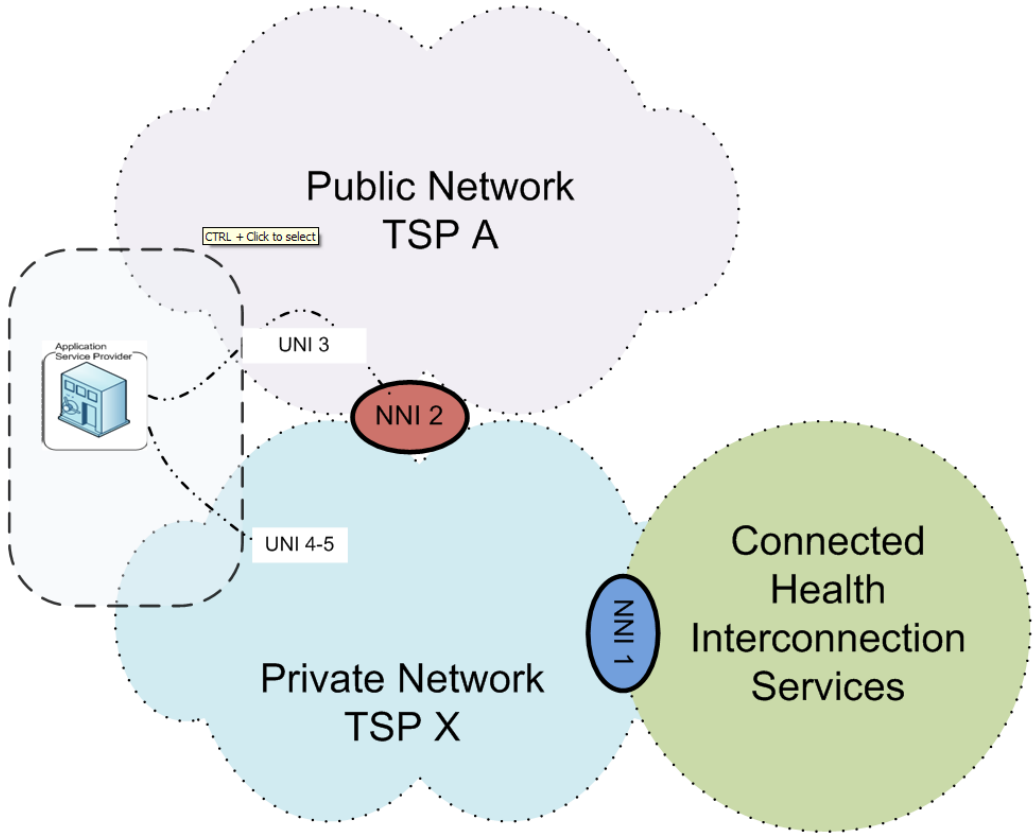
4.1 Examples illustrating the different roles and responsibilities of an ASP and a CH Retail TSP

Organisations can be both an ASP and a TSP. ASP products will be certified separately.

4.1.1 ASP

Figure 6 illustrates an organisation acting as an accredited CH application service provider and exposing its service via a TSP UNI 3, 4 or 5 to CH Network users. The ASP boundary of responsibility is indicated by the dashed line.

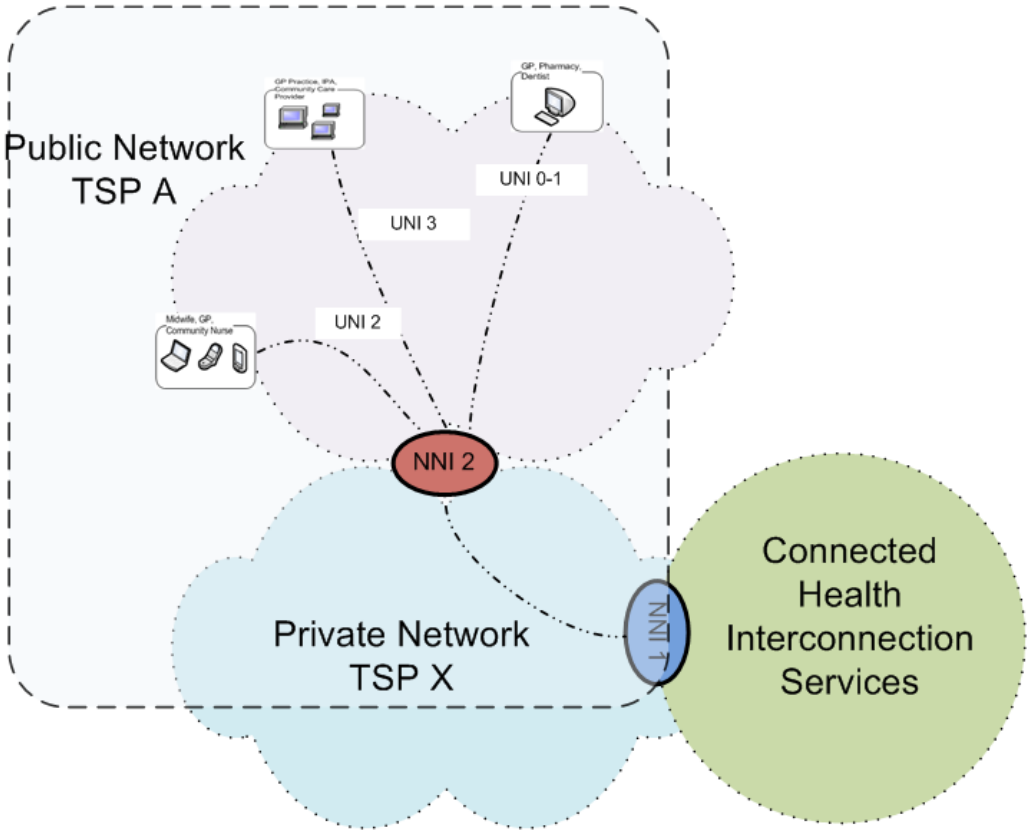
Figure 6: ASP boundary of responsibility



4.1.2 Retail TSP: UNI 0 - 3

Figure 7 illustrates an organisation acting as an accredited CH TSP supplying UNI 0-3s. It indicates the provision of VPN termination by a NNI-2 and the routing of traffic to an NNI-1. The TSP boundary of responsibility is indicated by the dashed line.

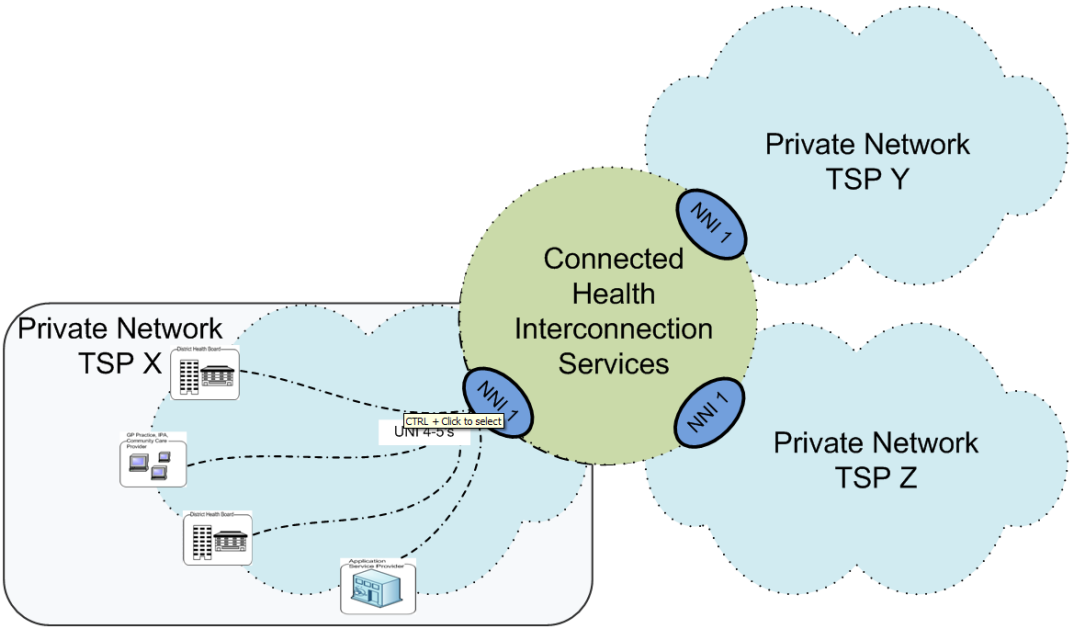
Figure 7: TSP:UNI 0-3 boundary of responsibility



4.1.3 Retail TSP: UNI 4 – 5

Figure 8 illustrates an organisation acting as an accredited CH TSP supplying UNI-4 or UNI-5s and interconnecting to other TSP providers by NNI-1s. The TSP boundary of responsibility is indicated by the solid line.

Figure 8: TSP: UNI 4-5 boundary of responsibility



Appendix 1: Glossary of Terms

(Informative)

Term	Description
Accreditation	The business process through which suppliers are approved to be Connected Health certified suppliers of products and services to the NZ health sector. Suppliers agree to the Connected Health Principles and Operating Policy to become accredited.
Application Service Provider (ASP)	A CH Accredited Supplier that provides certified application products or services to the NZ health sector.
Autonomous System Number (ASN or AS(N))	Within the Internet, an ASN is a collection of connected IP routing prefixes under the control of one or more network operators that presents a common, clearly-defined routing policy to the Internet.
Binary	Something that can be represented as being in one of two available states, and commonly used in data storage in digital systems. In digital systems, the data packet used to define bandwidth or throughput is the binary bit or byte (a byte being 8 bits). Bandwidth is typically defined as bits per second (Bit/s) or bytes per second.
Border Gateway Protocol (BGP)	The core network routing protocol of the Internet.
Certification	The process that confirms that a product meets the Connected Health standards.
CH community	The group of health sector organisations and individuals who are users of Connected Health certified products and services.
Class of Service (CoS)	A method of grouping network traffic into classes for the purpose of prioritisation. Commonly used in relation to Quality of Service (QoS) services.
Communication Lag, Latency or Transfer Delay	The time taken for a packet of data to be sent by an application, travel and be received by another application. The absolute time (in milliseconds) from the time the first bit of an IP packet enters the customer side of the ingress (source) terminating equipment to the time the first bit of the same packet exits from the customer side of the egress (destination) terminating equipment.
Connected Health (CH) / Connected Health Team	The Ministry of Health programme or business entity that implements and supports improved network inter-connectivity for the health sector, facilitating the delivery of improved network resources to health providers.
Customer Located Network Equipment (CLNE)	Equipment from a TSP that supports connection to a customer's network, and is placed on a customer's site.
Customer Premises Equipment (CPE)	Equipment from a TSP that supports connection to a customer's network, and is placed on a customer's site.

Term	Description
Differentiated Services Code Point (DSCP)	A 6-bit field in the header of IP packets for packet classification purposes.
District Health Board (DHB)	An entity responsible for the delivery of health care in a geographical district.
Health Network Code of Practice (HNCOP)	Developed by Standards New Zealand in 2002 as the code of practice for all Health Network members, including telecommunication providers.
HISO 10029 Health Information Security Framework (HISF)	The HISF is based on AS/NZS ISO/IEC 27002:2006. It specifies minimum policy standards and technical requirements to support organisations and practitioners holding personally identifiable health information to improve the security of that information, so it can be produced, stored, disposed of and shared in a way that ensures confidentiality, integrity and availability.
Hot Potato routing	The practice of forwarding packets destined for another ASN via the closest POI. Return packets are treated in the same way, often leading to asymmetric routing.
Institute of Electrical and Electronics Engineers (IEEE) 802.1p	A specification detailing how priority values are mapped into the header of tagged ethernet frames. Untagged ethernet frames do not support priority tagging.
Internet Protocol (IP)	A widely adopted and standardised computer communications protocol used to enable computers to be networked and to communicate by transferring information between them.
IP Packet Delay Variation (IPDV)	A measurement of Jitter as described in the International Telecommunication Union -Telecommunication Standardisation Sector Recommendation ITU-T Y.1541.
IP Packet Loss Ratio (IPLR)	A measurement of packet loss as described in the International Telecommunication Union - Telecommunication Standardisation Sector Recommendation ITU-T Y.1541.
IP Packet Transfer Delay (IPTD)	A measurement of network latency as described in the International Telecommunication Union - Telecommunication Standardisation Sector Recommendation ITU-T Y.1541.
IPv4 address	The fourth revision in the development of the IP and the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based Internetworking methods of the Internet. IPv4 has a smaller address space than IPv6. IPv4 uses a 32-bit address compared to 128 bits for IPv6.
IPv6 address	The next-generation IP version designated as the successor to IPv4. It is an Internet layer protocol for packet-switched networks. IPv6 has a vastly larger address space using a 128-bit address, compared to 32 bits for IPv4.

Term	Description
Jitter	An unwanted variation of one or more characteristics of a periodic signal in telecommunications, also known as Delay Variation. The difference (in milliseconds) between the minimum and maximum Latency. This is calculated one-way over a one minute interval for 99% of equal-sized IP packets in a stream with randomly varying arrival times.
Layer 2	Layer 2 is the 'data' level in Open Systems Interconnection (OSI) 7-layer model. In very basic terms, Layer 1 is the physical cable connection; Layer 2 adds transmission error detection, while Layer 3 adds packet routing/error correction/congestion control. Layer 2 is a non-managed service.
Layer 3	Layer 3 is the network layer is the third layer of the OSI model. Layer 3 is responsible for end-to-end (source to destination) packet delivery, whereas Layer 2 is responsible for node to node delivery. Layer 3 is typically associated with routing. Layer 3 services are often referred to as 'managed services'.
Link layer	Layer two of the five-layer TCP/IP reference model. It provides the functional and procedural means to transfer data between adjacent network nodes in a wide area network or between nodes on the same local area network segment.
Link Layer Discovery Protocol (LLDP)	A vendor-neutral Link Layer protocol used by network devices for advertising of their identity, capabilities, and interconnections on an Institute of Electrical and Electronics Engineers (IEEE) 802 LAN network.
Local Area Network (LAN)	A group of computers and associated devices that share a common communications line or wireless, link within a single physical location.
Metro	Geographic area within 30 kilometres of the centres of Auckland, Hamilton, Rotorua, Tauranga, New Plymouth, Napier, Palmerston North, Wellington, Nelson, Christchurch and Dunedin.
MultiProtocol Label Switching (MPLS)	A mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next. It can encapsulate packets of various network protocols.
Network of Networks	The group of TSP networks interconnected by NNI connection points which make up the Connected Health network.
Network to Network Interface (NNI)	An interconnection point between IP carrier networks. NNI1 is an interconnection between private networks and NNI2 is an interconnection between private and public networks.
Openness	Openness is an architectural principle referring to equal availability of products and services to participating suppliers and organisations.

Term	Description
Operating Level Agreement (OLA)	Agreement which defines the interdependent relationships among the internal support groups working to support a Service Level Agreement. The agreement describes the responsibilities of each internal support group toward other support groups, including the process and timeframe for delivery of their services.
Packet	A formatted unit of data carried by a packet mode computer network.
Packet Loss	Occurs when one or more packets of data travelling across a computer network fail to reach their destination.
Point of Interconnection (POI)	A peering point for national TSP private health networks.
Quality of Service (QoS)	The application of different priorities to different applications, users, or data flows, in order to guarantee a certain level of performance to data transmission.
Retail TSP	A TSP that provides network connectivity services directly to consumers.
Router	A device that interconnects two or more computer networks, and selectively interchanges packets of data between them.
Service Level Agreement (SLA)	A formal agreement between two parties where one party agrees to deliver a defined and measurable level of service to the other party.
Simple Network Management Protocol (SNMP)	A protocol for governing network management and the monitoring of network devices and their functions.
Telecommunications Carriers' Forum (TCF)	Plays a role in the New Zealand telecommunications industry by working collaboratively on the development of key industry standards and codes of practice that underpin the digital economy.
Telecommunications Service Provider (TSP)	A provider of telecommunications services (telephone, network, internet services etc.) to the New Zealand public, private, commercial and government sectors, and which has a network licence as defined under the Telecommunications Act 2006.
Throughput	The maximum average data rate for a given packet size that a network connection can sustain while conforming to the specified functional performance targets. Also known as Sustained Data Rate.
Transit TSP	A TSP that carries network data between POIs.
User to Network Interface (UNI)	The connectivity product/service that connects a subscriber to the Connected Health network. This is the physical and logical IP connectivity to the network from one of the end points, such as a single PC or large private network.

Term	Description
Virtual Private Network (VPN)	A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network.