COMMUNICATIONS
ALLIANCE LTD

INDUSTRY GUIDELINE

MOBILE NUMBER PORTABILITY- IT SPECIFICATION PART 3: COMMON NETWORK

G573.3:2020

G573.3:2020 Mobile Number Portability - IT Specification Part 3: Common Network

First published as ACIF G573.3:2001
Second edition as ACIF G573.3:2003
Third edition as ACIF G573.3:2004 Sept
Fourth edition as ACIF G573.3:2004
Fifth edition as G573.3:2009
Sixth edition as G573.3:2020

Communications Alliance Ltd (formerly Australian Communications Industry Forum Ltd) was formed in 2006 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

TABLE OF CONTENTS

1 GENERAL

1.1 Purpose

The purpose of this document is to define technical specifications and other requirements associated with interfacing between Participants and the PIPN provider.

1.2 Scope

This document specifies the requirements of the Private IP Network (PIPN) to provide interconnectivity which facilitates Mobile Number Portability.

The PIPN will be used to support Mobile Number Portability and other uses as approved by the Electronic Information Exchange Management Committee (EIEMC).

NOTE: For EIEnet purposes please refer to ***EIE Infrastructure Common Network Specification*** *(G608:2004).*

1.3 2009 Revision

In 2009, the Mobile Number Portability Code was revised. At that time all associated Mobile Number Portability documents were republished as Communications Alliance documents to reflect the change of organisational name from ACIF. Where relevant any references to other documents have also been updated.

1.4 2010 Revision

In 2010, a minor revision was conducted to enhance current guidance on fault management processes and diagnostics in order to better address MNP fault scenarios arising from connectivity issues.

1.5 2020 Revision

In 2020, a minor revision was conducted to provide an alternative to the ATM Frame Relay access services. This was required due to the retirement of the ATM Frame Relay networks. This revision outlines the replacement service based on the private Fibre Ethernet Point-to-Point service.

2 REVIEW PERIOD

This Guideline will be reviewed in conjunction with ***Mobile Number Portability*** Industry Code (C570:2009), or when either the current PIPN provider changes, or additional IP network providers want to connect to the PIPN.

3 ACRONYMS AND DEFINITIONS

3.1 Acronyms

For the purposes of this Guideline, the following acronyms apply:

ATM

Asynchronous Transfer Mode

BGP

Border Gateway Protocol

CSP

Carriage Service Provider

DNS

Domain Name Server

EIERP

Electronic Information Exchange (Inter-Operator) Reference Panel

FlexENet

Product name describing an Ethernet access service

IP

Internet Protocol

IPSec

IP Security

MC

Management Centre

MNP

Mobile Number Portability

NMC

Network Management Centre

OSPF

Open Shortest Path First

PIPN

Private IP Network

PSD

Prime Service Deliver

PSS

Portability Service Provider

VC

Virtual Connector

RIP

Routing Internet Protocol

SLA

Service Level Agreement

WAN

Wide Area Network

3.2 Definitions

For the purposes of this Guideline, the following definitions apply:

Act

means the *Telecommunications Act 1997*.

Bilateral Agreements

means any agreement between two parties.

Carrier

has the same meaning as in the *Act*.

Participant

means those parties involved in MNP including any Carrier, CSP or PSS that interconnects with the PIPN to either send or receive MNP transactions, or who use the PIPN for a purpose authorised by the EIEMC.

Private IP Network

means a transmission network that interconnects all Participants and provides a common network layer service.

Portability Service Supplier

means a Carrier or CSP or their agent or a contractor who provides supporting services to Carriers and/or CSPs in the provision and operation of MNP. For example, Port administration services, Ported number reference databases and network services for call.

4 MNP COMMON NETWORK

The common network infrastructure is an electronic messaging platform that allows Participants to exchange information electronically with each other, in order to perform business functions associated with MNP and other uses approved by the EIEMC.

Currently there is only one provider offering a single PIPN. The PIPN may be provided using one or more network providers. Should a multiple provider PIPN model be adopted in the future, the PIPN must provide seamless and transparent interconnection between any and every Participant.

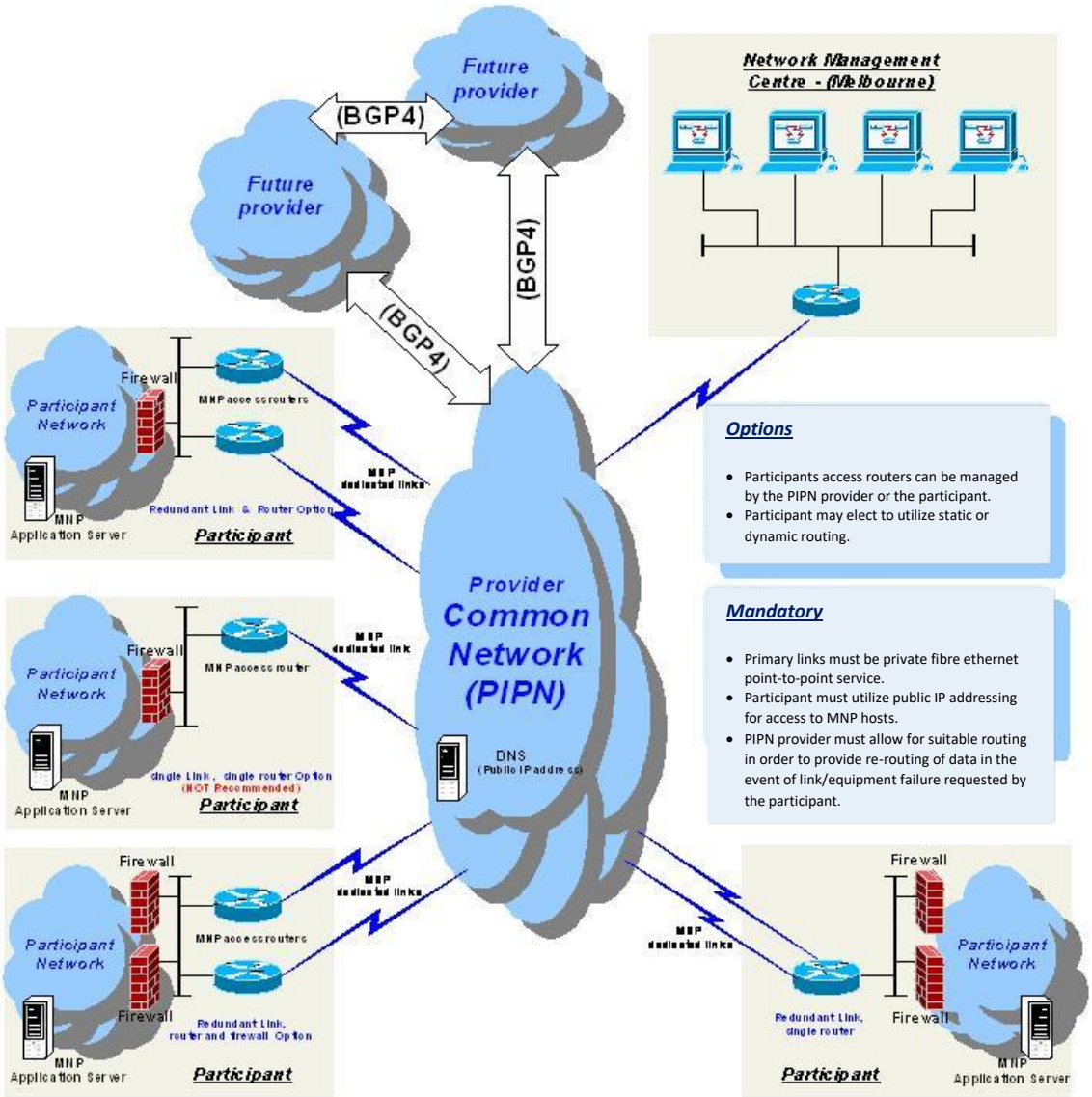

FIGURE 1
Private IP network diagram – Phase 1

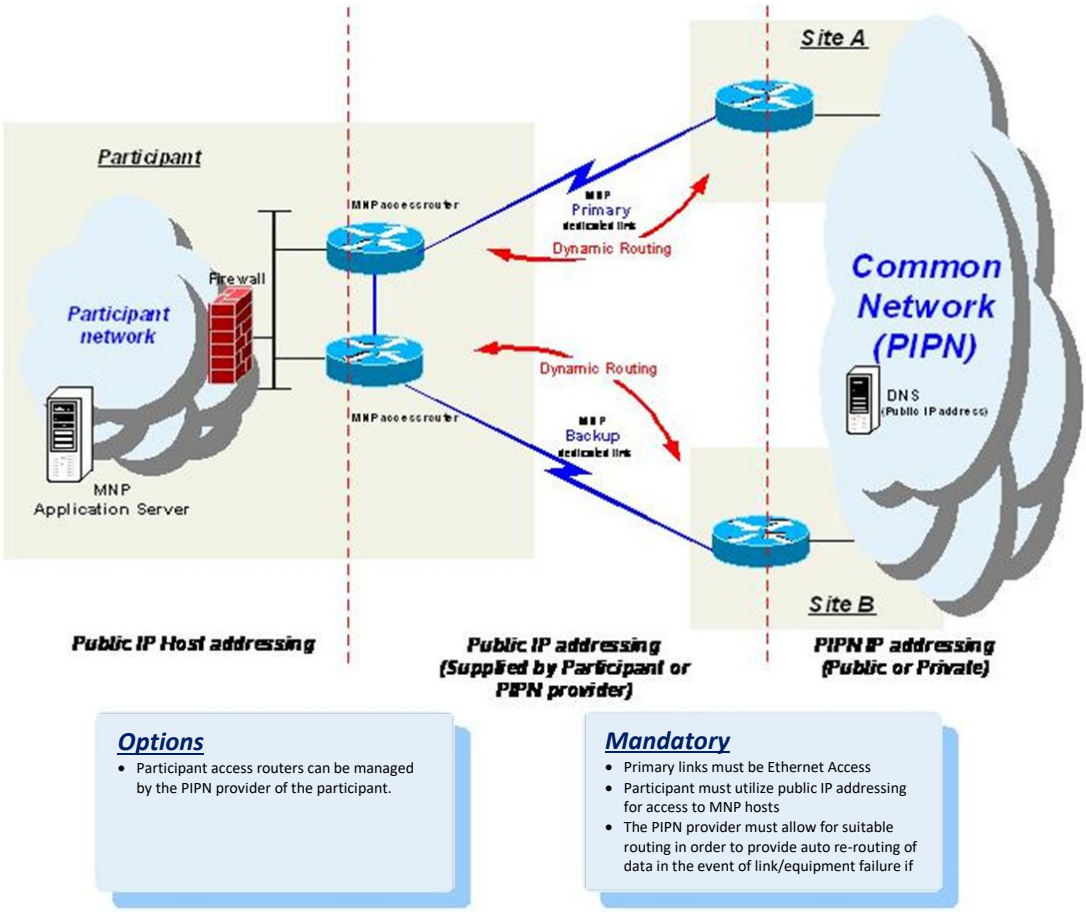

FIGURE 2

Recommended Participant interface to PIPN with dynamic routing

4.1 Access

The PIPN is a communications medium that is only available to those parties approved by the MNP Administration Group, for MNP purposes; or by the Electronic Information Exchange Management Committee, for EIEnet purposes.

The PIPN provider must not provide access to the PIPN to a potential Participant without the written consent of the:

(a) MNP Administration Group, for MNP purposes; or

(b) Electronic Information Exchange Management Committee, for EIEnet purposes.

4.2 Types of Transmission Link

The primary links between the PIPN provider's routers and the Participant's access routers must support Ethernet. Diverse Ethernet service may be used as the backup link.

The primary links must be dedicated to meet the service levels as defined in the ***Mobile Number Portability*** Industry Code (C570:2009). This will be determined by agreements between the Participant and the PIPN Provider.

Participants will make arrangements with a PIPN Provider for network and routing dimensioning needs (for example bandwidth, number of PVCs).

4.3 Interconnection

4.3.1 **Network Provider to Network Provider:** Border Gateway Protocol (BGP4) must be used as the base routing protocol for interconnection of PIPNs.

4.3.2 **Participant to Network Provider:** Each Participant will access the PIPN through the access router located on the Participant's premises. The Participant's access router(s) can be managed either by the PIPN provider or by the Participant themselves.

A Participant may elect to use static or dynamic routing between themselves and the PIPN.

For maximum compatibility, proprietary network routing protocols (for example, IGRP, EIGRP) must not be used.

4.3.3 **Channels and associated MNP priority scheme:** For MNP the PIPN provider's network and the Participant's router must provide for three priority schemes. The three priority schemes include the Production, Testing and Administration channels.

A priority scheme must be implemented in the PIPN provider's network for handling of the queues associated with these MNP Channels with the Production channel having the highest priority.

The implementation of the MNP priority scheme must be negotiated between the Participant and their PIPN provider.

Where other applications associated with the EIEnet are authorised (subject to Clause 5.1) for use on the PIPN, they must be on separate channels to those used for MNP and must not have any impact on any MNP channel or priority scheme.

4.3.4 **Common network equipment and associated protocols:** Participants (that manage their own routers) must choose a router protocol that is compatible with that of the PIPN.

4.4 IP Addressing

MNP application servers and Participant's access routers must be addressable using public IP addresses. Where the Participant does not supply the Public IP addresses then their PIPN provider may supply them.

Within the PIPN, public or private IP addresses may be used.

For IP protocol selection and maintenance, IP v4 is the protocol of choice. Any change of standard (e.g. IP v6) must be coordinated through Communication Alliance.

4.5 Setup of Firewall

A firewall must be used in the Participant's network. The firewall must be capable of passing both way traffic based on the IP addresses of all Mobile Carriers and Mobile CSPs, PSSs and PSDs (estimated to be 37 parties). In the case of multiple IP network providers to the PIPN, the Participant's MNP application server must be able to communicate with MNP application servers of other Participants with different IP network providers.

4.6 Domain Name System (DNS)

The PIPN must provide a central DNS service capability. In the case of multiple IP network providers to the PIPN the provision of the DNS service capability must be determined by the PIPN providers. The DNS service must have a Public IP address.

4.7 Network Security

Security is provided at the application level and the messages will be encrypted when transacting through the common network, as specified in ***Mobile Number Portability IT Specification - Part 2: Architecture and Messaging Requirements*** (G573.2:2009).

4.8 Network Scalability

The network solution must be scalable to be able to carry actual volumes, and agreed forecasts, of Mobile Number Portability transactions.

5 DATA LINK REDUNDANCY

It is highly recommended that Participants subscribe to a back-up link to an alternative physical path. This is to be addressed through commercial agreement between each Participant and a nominated PIPN supplier. The PIPN must be able to provide recovery from single point of failure situations.

In the case of multiple IP network providers, Participants may arrange back-up links in two ways:

- by subscribing to multiple IP network providers; or
- by having fully redundant (and, where possible, diversely routed) links to different locations of a single IP network provider.

It is envisaged the Participant can subscribe to multiple PIPN providers or have fully redundant links to the single provider at different physical locations.

In the event of any single point of failure in one PIPN provider, the Participant access router can be auto configured to pass the IP traffic to the alternative PIPN provider through the back-up link. The back-up link is shown in Figure 1 and Figure 2.

5.1 Availability

The standard availability target for the PIPN Provider is 99.85%.

The following service performance objectives apply to PIPN Providers:

Class of Service	Standard 6COS
Data Delivery Ratio %	99.90%
Network Availability %	99.95%
Network Round Trip Transit Delay (milliseconds maximum)	100
Network Packet Delay Variation (milliseconds maximum)	20

Availability targets are averaged over a one calendar month period. All targets apply within the Private IP network and do not include access services. Planned outages are excepted.

5.2 Planned Outages

In the event that a PIPN Provider needs to carry out maintenance on the PIPN they must notify each Participant and other PIPN providers as per pre-established Bilateral Agreements. Should maintenance be required industry co-ordination and agreement with respect to scheduling the planned outage must be in place before the planned outage is carried out.

6 COMMERICAL OFFERING

The access to the PIPN will be provided to Participants on a commercial basis.

7 FAULT MANAGEMENT

7.1 Fault Management Principles

7.1.1 The PIPN must provide self-diagnostic capability to identify faults in the PIPN network. The self-diagnostic capability includes the ability for Participants to 'ping' and 'trace-route' to other Participants access routers and edge routers.

7.1.2 The results of the 'ping' and 'trace-route' data should be made available to other Participants upon request via the standard operational escalation path following due diligence in assessing any other factors which may be contributing to connectivity issues, including firewall and application server troubleshooting. A connectivity issues checklist is provided as an appendix to this guideline at Appendix A1.

7.1.3 The PIPN provider must provide a contact list for the reporting and escalation of faults. This will be established under Bilateral Agreements.

7.1.4 Restoration times depending on the severity of the fault must be documented.

7.1.5 Fault Management procedures and Service Levels must be agreed between the Participant and the PIPN Provider.

7.2 Participant and PIPN Provider Responsibilities

Participants and PIPN provider(s) are both responsible for ensuring that appropriate arrangements are agreed between themselves for PIPN fault management procedures.

8 MINIMUM PARAMETER VALUES

UNI Attribute	Attribute Description	Attribute Value
Bandwidth	This attribute allows the user to select the interface speed. The user can select the interface speed as per the data consumption.	The standard available range is 20Mbps – 1000Mbps.
Interface Type	This attribute allows the user to select the type of Interface supported on the UNI.	The available interface options are: GE 1000 Base LX / LH (SMOF, 1000Mbps Optical) GE 1000 Base SX (MMOF, 1000Mbps Optical) GE 1000 Base T (100/1000 Mbps Copper)
Availability	This attribute defines the UNI Redundancy options.	Single Access Dual Access
Interface Mode	This attribute allows the customer to select information exchange attributes.	Auto Neg
Frame Size	This attribute defines the size of the Ethernet frame in use.	The maximum MTU is 1546

NTU Interfaces

Copper Interface	**Minimum Cabling Standard**
10/100/1000 – 10BaseT	2-Pair Category-5 UTP – 100m
10/100/1000 – 100BaseTX	2-Pair Category-5 UTP – 100m
10/100/1000 – 1000BaseT	4-Pair Category-5/5e/6 UTP – 100m
Gigabit Fibre-Optics Interface	
1000Base-SX	MMOF – 550m
1000Base-LX/LH	SMOF – 10km

10-Gigabits Fibre-Optics Interface	
10G-SR	FDDI-Grade MMOF – 26m
10G-SR	OM-3 Grade MMOF – 300m1: Preferred option
10G-LR	SMOF – 10km

NOTE 1: This will only be used for the purposes of providing MNP

APPENDIX

A Fault Management Diagnostics

A1 Connectivity Issues Checklist

Checklist Step	Recommended Action
1	Check for any relevant network alarms through alarm browser
2	Perform an end to end test to attempt to replicate the fault (ping/trace/telnet via a specific port
3	Test your own network end to end from demarcation point back to the source/destination and vice versa (via ping/trace/telnet via specific port)
4	If fault can be replicated in own network, check each hop between the source, destination and edge for a fault condition using the following steps: ▪ Start at one end with trace ▪ Check device logs for interface or hardware failures ▪ Ping/trace, telnet via specific port from each device ▪ Interrogate routing on each device being investigated
5	Check logs of any traversed firewalls for dropped packets between source and destination
6	Setup TCP//IP dump/packet snoop and perform end to end testing if needed
7	Look for possible firewall rule problem
8	Check POI between carriers for interface status and/or errors
9	Check and validate routes into and from the other carriers neighboring router
10	Ping/trace into the other carrier's network
11	Check for incoming/outgoing packets between participants via edge router interface

Checklist Step	Recommended Action
1	Check for any relevant network alarms through alarm browser
2	Perform an end to end test to attempt to replicate the fault (ping/trace/telnet via a specific port
3	Test your own network end to end from demarcation point back to the source/destination and vice versa (via ping/trace/telnet via specific port)
4	If fault can be replicated in own network, check each hop between the source, destination and edge for a fault condition using the following steps: ▪ Start at one end with trace ▪ Check device logs for interface or hardware failures ▪ Ping/trace, telnet via specific port from each device

	▪ Interrogate routing on each device being investigated
5	Check logs of any traversed firewalls for dropped packets between source and destination
6	Setup TCP//IP dump/packet snoop and perform end to end testing if needed
7	Look for possible firewall rule problem
8	Check POI between carriers for interface status and/or errors
9	Check and validate routes into and from the other carriers neighboring router
10	Ping/trace into the other carrier's network
11	Check for incoming/outgoing packets between participants via edge router interface

9 REFERENCES

Publication	Title
Industry Codes	
C570:2009	Mobile Number Portability
Industry Guidelines	
G573.1:2009	Mobile Number Portability - IT Specification Part 1: Transaction Analysis
G573.2:2009	Mobile Number Portability - IT Specification Part 2: Architecture and Messaging Requirements
G608:2004	EIE Infrastructure Common Network Specification
G579:2009	Mobile Number Portability Operations Manual
Industry Documents	
Telecommunications Act 1997(Cth)	

PARTICIPANTS

The Working Committee responsible for the revisions made to this Guideline consisted of the following organisations and their representatives:

Organisation	Representative
Vodafone Hutchison Australia	Kiang Chia Allan Standbridge
Telstra	Manoj Antony Bruno Romanin Alistair Toscano
AAPT / TPG	Adam Rogers Stuart Bridge
Optus	Nick Nicolaou Jim Mandalakoudis Anuj Chatrath
Paradigm.One Symbio/ MNF Group	Dev Gupta Martin Cantwell Beau Tran
Lycamobile	Chandramouli Arjunan P Arumuga Siva Sankar

This Working Committee was chaired by Darshan Nair, Telstra. Craig Purdon and Alexander Osborne of Communications Alliance MAG provided guidance.

Communications Alliance was formed in 2006 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 9
32 Walker Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
TTY 61 2 9923 1911
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507