FUJ00001883

EMV – Banking and Retail

NBX – A&L Technical Interface Specification (TIS)

Changes in version 0.8 like this

Changes in version 1.0 like this

ROLE	NAME	AREA OF RESPONSIBILITY	SIGNATURE	DATE
Authors	Mark Jarosz on behalf of Post Office Ltd	**Business Architecture**		
		Product Deployment		
		Technical Architecture		
Fujitsu Services Sign-off	Tony Drahota	**RASD Director**		
DA Sign-off (Peer Reviewer)	David Gray	**Design Authority**		
Programme Director	Beverley Dunn	**Project Delivery**		

FUJ00001883

1 Document Control

1.1 Document Information

Horizon Release No:	S75
Document Title:	EMV Banking and Retail: NBX – A&L Technical Interface Specification
Document Type:	Technical Interface Specification
Abstract:	This document defines the technical interface between the Horizon domain and Alliance and Leicester
Document Status:	Approved
Originator & Department:	David Gray Design Authority
Contributors:	
Post Office Distribution:	Design Authority – David Gray POL Document Control – Post Office Programme Office
Supplier Distribution:	A&L: Tony Douglas, Andy Irvine, Richard Yarwood, Ian Willams, Ian Antrobus, Mark Clarke, Avtar Dhanjal, Steve Wells, Steve Green, Neil Scott Fujitsu Services: Mark Jarosz, Steve Probert
Client Distribution:	N/A

Table 1: Document Information

1.2 Document History

Version	Date	Reason for Issue	Associated WP / CT
0.1	10 Dec 2003	First working draft. Based on document produced by IBM entitled "Network Banking Engine: A&L Technical Interface Specification" (Version 2.0)	
0.2	18th Jan 2004	Second working draft based on discussion / decisions reached at workshop between A&L, POL and Fujitsu services on Jan 7th 2004	
0.3a	4th March 2004	Third working draft updated during the workshop between A&L, POL and Fujitsu services on Jan 21st 2004. Additional changes agreed during the workshop have also been applied.	
0.4	22nd April 2004	Fourth working draft based on discussion between A&L, POL and Fujitsu services on 1st April 2004 and subsequent update	

FUJ00001883

0.5	28th May 2004	Fifth working draft based on discussion between A&L, POL and Fujitsu services on 28th April 2004	
0.6	6th July 2004	Version issued as "ready for approval" subject to remaining DN's being removed.	
0.7	15th July 2004	Update to remove all (but one) outstanding DN's and update Test network to use ISDN2e	
0.8	6th August 2004	Update to remove use of IPSEC for Test Network	
1.0	2nd September	Version for sign off	

Table 2: Document History

1.3 Change Process

Any changes to this issued version of this document will be made, controlled and distributed by: -

Bob.Booth GRO

FUJ00001883

1.4 Review Details

Review Comments by :	
Review Comments to :	

Mandatory Review Authority	Name
Post Office Ltd	Beverley Dunn, David Gray, Post Office Ltd
Fujitsu Services Ltd	Tony Drahota
A&L	Tony Douglas, Andy Irvine, Ian Williams
Optional Review / Issued for Information	
Post Office Ltd	Bob Booth, Paul Warbrick, Jason Crellin
A&L	A&L: Tony Douglas, Andy Irvine, Richard Yarwood, Ian Willams, Ian Antrobus, Mark Clarke, Avtar Dhanjal, Steve Wells, Steve Green, Neil Scott
Fujitsu Services Ltd	Mark Jarosz, Steve Probert

1.5 Changes in this Version

Version	Changes
1.0	1. Date in Footer changed to “saved date” 2. Updated version of Figure 6 Test Network Interface to correct error in illustration of boundaries between IP address spaces 3. Updated section 2.4 to include abbreviation for VLAN 4. Updated sections 4.3.1.1 and 4.3.3 to clarify use of Virtual addresses 5. Updated IP addresses information in Appendix A and deleted entries not required 6. Added new section 1.6 to document planned changes 7. Updated Figure 3 Application Endpoints to show single IP address per data centre for NBX platform 8. Inconsistencies between log on and sign on (and off) have been removed by replacing log on (and off) with sign on (and off). 9. Section 5.3 updated to avoid repeating information already in section 4.7.5 and remove reference to AIS since AIS references the TIS. 10. Deleted last sentence in section 4.7.5 since it stated that normally NBX would initiate “sign on” and this is not the case.

FUJ00001883

	11. Updated section 4.7.10.1 to clarify when NBX can send Reversals. 12. Included NBX local names for A&L PIs in Appendix A

Table 3: Changes in this Version

1.6 Changes Forecast

Number	Change
1	To update Appendix A with Connect: Direct information which currently this "tbs" against the entry.
2	To complete references in Table 5: Associated Documents. Currently these have entry's "Tbs".

1.7 Key Contacts

Name	Position	Phone Number
Jason Crellin	Solutions Architect	GRO

Table 4: Key Contacts

1.8 Associated Documents

	Reference	Version	Date	Title	Source
1.	AIS			NBX-A&L Application Interface Specification	Tbs
2.	OSI			OSI/ISO Reference Model, ISO Standard 7498	ISO
3.	BC			Business Continuity Framework Between Post Office and Alliance & Leicester	Post Office
4.	OLA			Operational Level Agreement	Tbs
5.	DRTEST			A&L DR Test Plan	A&L
6.	DRPLAN			A&L DR Plan	A&L
7.	BPD			NBX Business Parameters Document	Tbs

Table 5: Associated Documents

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

FUJ00001883

Table of Contents

1 DOCUMENT CONTROL 2

1.1 Document Information 2

1.2 Document History 2

1.3 Change Process 3

1.4 Review Details 4

1.5 Changes in this Version 4

1.6 Changes Forecast 5

1.7 Key Contacts 5

1.8 Associated Documents 5

2 INTRODUCTION 9

2.1 Purpose 9

2.2 Scope 9

2.3 Structure 9
2.3.1 Introduction 9

2.4 Abbreviations 10
2.4.1 Abbreviations 10

3 ENVIRONMENT 12

3.1 Introduction 12

3.2 Context 13
3.2.1 Design Principles 14
3.2.2 Location of NBX – A&L Physical Interface 15

3.3 Components 16
3.3.1 Wide area Network Links 16
3.3.2 NBX Servers 17
3.3.3 NBX File Transfer Server 17
3.3.4 A&L Servers 17
3.3.5 Security Hardware 17
3.3.6 Network Equipment 17

4 MEDIUM OF TRANSFER 18

4.1 Interface Overview 18

4.2 Layers 1 and 2 - Physical and Link 18

FUJ00001883

4.3 Layer 3 – Network 18
4.3.1 Control Plane 19
4.3.2 Data Plane 19
4.3.3 Virtual IP Addressing 19
4.3.4 IP Address spaces 20

4.4 Layer 4 Transport 21
4.4.1 Transport Level interface 21
4.4.2 TCP Keep Alive 21
4.4.3 TCP Data Flow 21
4.4.4 Application Endpoints 22
4.4.5 Migration of IP Address to another Computer System 24
4.4.6 TCP Connection Management 24
4.4.7 Load Sharing 25

4.5 Layer 5 – Session Layer 26
4.5.1 Sign on / Sign off 26
4.5.2 PI identification 26
4.5.3 Sessions 26

4.6 Layer 6 – Presentation Layer 26
4.6.1 Character Sets 26
4.6.2 Base 64 Encoding Rules 26

4.7 Layer 7 – Application Layer 26
4.7.1 Interface to Transport Layer 26
4.7.2 Message delineation 27
4.7.3 Reconciliation File Transfer 27
4.7.4 Communications Handling 28
4.7.5 Handshakes 28
4.7.6 Acquirer Working Key (AWK) Exchange 30
4.7.7 Network Management Messages (Network Management Codes) 30
4.7.8 Delay (“Stand In”) Processing 30
4.7.9 Time-outs 30
4.7.10 Message Exchange patterns 30

5 OPERATIONAL CONSIDERATIONS 33

5.1 Systems Management 33

5.2 Network Management 33

5.3 Restarts 33

5.4 Resilience and Fail Over 33

5.5 Performance 34
5.5.1 A&L and NBX Platforms 34
5.5.2 Wide Area Network 35

6 SECURITY 36

6.1 End-to-End Identification 36

6.2 Encryption and Decryption Methods 36
6.2.1 Network data privacy and authentication 36

FUJ00001883

6.3 Application Key Management 36
6.4 Protection 37
6.5 PIN Encryption 37
6.6 Key Changes 37
6.7 Key Ownership 37
6.8 Line Encryption 37
6.9 Firewalls 38
6.10 Authorised Engineering access to A&L locations 38

7 RECOVERY FACILITIES AND PROCEDURES 39

7.1 Fault Detection 39
7.2 Disaster Recovery Environment 39
7.3 Disaster Recovery Testing 39
7.4 Disaster Recovery Invocation 39
7.5 A&L Move to DR Processing 39
7.6 NBX Move to DR processing 39

APPENDIX A DETAILED CONFIGURATION 40

A.1 Production System Addresses and Ports 40
A.2 DR System Addresses and Ports 41
A.3 Test System Addresses and Ports 42
A.4 Connect Direct details 43

APPENDIX B – TESTING 44

Table of Figures

Figure 1 – NBX and A&L Context..... 13
Figure 2 – NBX – A&L Physical Interface..... 15
Figure 3 Application Endpoints..... 23
Figure 4 – Acquirer Working Key Exchange..... 30
Figure 5 IPSEC Tunnels..... 38
Figure 6 Test Network Interface..... 44

FUJ00001883

2 Introduction

2.1 Purpose

The purpose of this Technical Interface Specification (TIS) is:

- To specify the technical details of the interface between the Post Office Network Banking Switch (NBX) system and the host systems of Alliance and Leicester (A&L).
- To provide Network Architects with sufficient detail to implement the NBX – A&L connection.
- To provide a consistent communications vehicle amongst the technical teams responsible for providing the various nodes and connections comprising the interface.
- It should be regarded as a base document against which project change control should be assessed when implementing changes to the NBX – A&L connection.

2.2 Scope

This TIS describes an interface for exchange of information between the NBX and A&L computer systems.

The interface is defined at two levels:

1. The Application level, concerned with the application data passed across the interface (The AIS)
2. The Technical level, concerned with the mechanisms by which the data is passed across the interface (The TIS – this document).

This document covers the specification of the technical mechanisms by which information is passed between the NBX and the A&L system.

This document does not cover the description of the information in terms of record/field structure and the meaning ascribed to information by either party. This aspect is addressed in the Application Interface Specification Standard [AIS].

This document does not cover any Application level protocol aspects; these are either covered or referenced in the AIS. The exception is where Application level protocol exchanges impact on elements that are within the scope of the TIS, for example constraints on use of the same TCP connection for message exchange and Application level heart beats causing TCP connections to be dropped.

This document does not describe internal interfaces (between production and DR instances for example). The activity to document and understand the Business impact from recovery in the event of a disaster will be conducted as part of the wider work in the Business Recovery area.

This document is concerned only with the specification of information that is both computer-generated and computer-consumed. Specifically manual procedures, such as Master Key Exchange (for example), are excluded. Details of the procedure for Master key Exchange are documented in [AIS] and [OLA].

2.3 Structure

2.3.1 Introduction

This section describes the structure of the remainder of this specification.

FUJ00001883

Section	Overview
3 ENVIRONMENT	This section describes the context and major components of the NBX and A&L environment.
4 MEDIUM OF TRANSFER	This section describes the interface in terms of the various ISO OSI Reference Model layers [OSI].
5 Operational Considerations	This section considers the operational impact and characteristics of the interface
6 Security	This section covers the security aspects of the interface.
7 RECOVERY FACILITIES AND PROCEDURES	This section deals with disaster recovery design, facilities and procedures.

2.4 Abbreviations

2.4.1 Abbreviations

Abbreviation	Explanation
AIS	Application Interface Specification
ARP	Address Resolution Protocol; this protocol determines which Ethernet Address corresponds to a given IP address
AWK	Acquirer Working Key
CPE	Customer Premises Equipment – the network equipment used by a telecommunications service provider to provide a service interface at the Customer premises
DES	Data Encryption Standard
DR	Disaster Recovery
FI	Financial Institution
FWSM	Firewall Services Module - A module that can be added to a Cisco Catalyst 6500 switch to provide Firewall capability.
HDLC	High-level Data Link Control
HSRP	Cisco Hot Standby Router Protocol
IANA	Internet Assigned Numbers Authority
ICF	Integrated Cryptographic Facility
ICMP	Internet Control Message Protocol
IPSEC	IP Security Protocol provides crypto at the IP layer by encapsulating IP within IP.
MAC	Message Authentication Code
MPLS	Multiprotocol Label Switching – A protocol which enables IP tunnels to be created through a network.
MSS	Maximum Segment Size – This is the maximum number of TCP payload bytes encapsulated within a single IP datagram.
NAT	Network Address Translation
NBX	Network Banking Switch – the system that handles the interface between the Horizon counter systems and the Financial Institutions (FI). The NBX allows Post Office outlets to transact automated banking services.
NIC	Network Interface Card
OSI	Open Systems Interconnection

FUJ00001883

OSPF	Open Shortest Path First, a protocol used by Routers to determine which interface to use for forwarding IP Datagrams
PI	Processor Interface. Interfaces to the NBX modules that handle the communications in order to obtain data from external systems.
PVC	Private Virtual Circuit
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP MSS	The TCP maximum segment size is the maximum number of TCP payload bytes that can be carried in a single IP datagram.
TIS	Technical Interface Specification
VIP	Virtual IP Address
VLAN	Virtual Local Area network
VPN	Virtual Private Network
WAN	Wide Area Network
ZMK	Zone Master Key

FUJ00001883

3 ENVIRONMENT

3.1 Introduction

This section presents an overview of the context in which A&L and NBX operate and provides a lower level description of the components that are concerned directly with the operation of the Interface being described in this document. The approach taken to determine if a component is directly concerned with the interface operation is based on the following:

- The Transport protocol is TCP and this can be visualized as a two-way pipe into which bytes are written and /or read. In general, this 'pipe' terminates on two different computer systems.
- The Components directly concerned with the Interface are taken to be both those that terminate the TCP 'pipe' and all other components through which the IP datagrams that implement the 'pipe' may flow. These may be Servers, Network links and /or Network devices such as routers etc.

3.2 Context

The following diagram provides an overview of the Interface location, the application level flows across the

FUJ00001883

interface and the roles of NBX and A&L data centres..

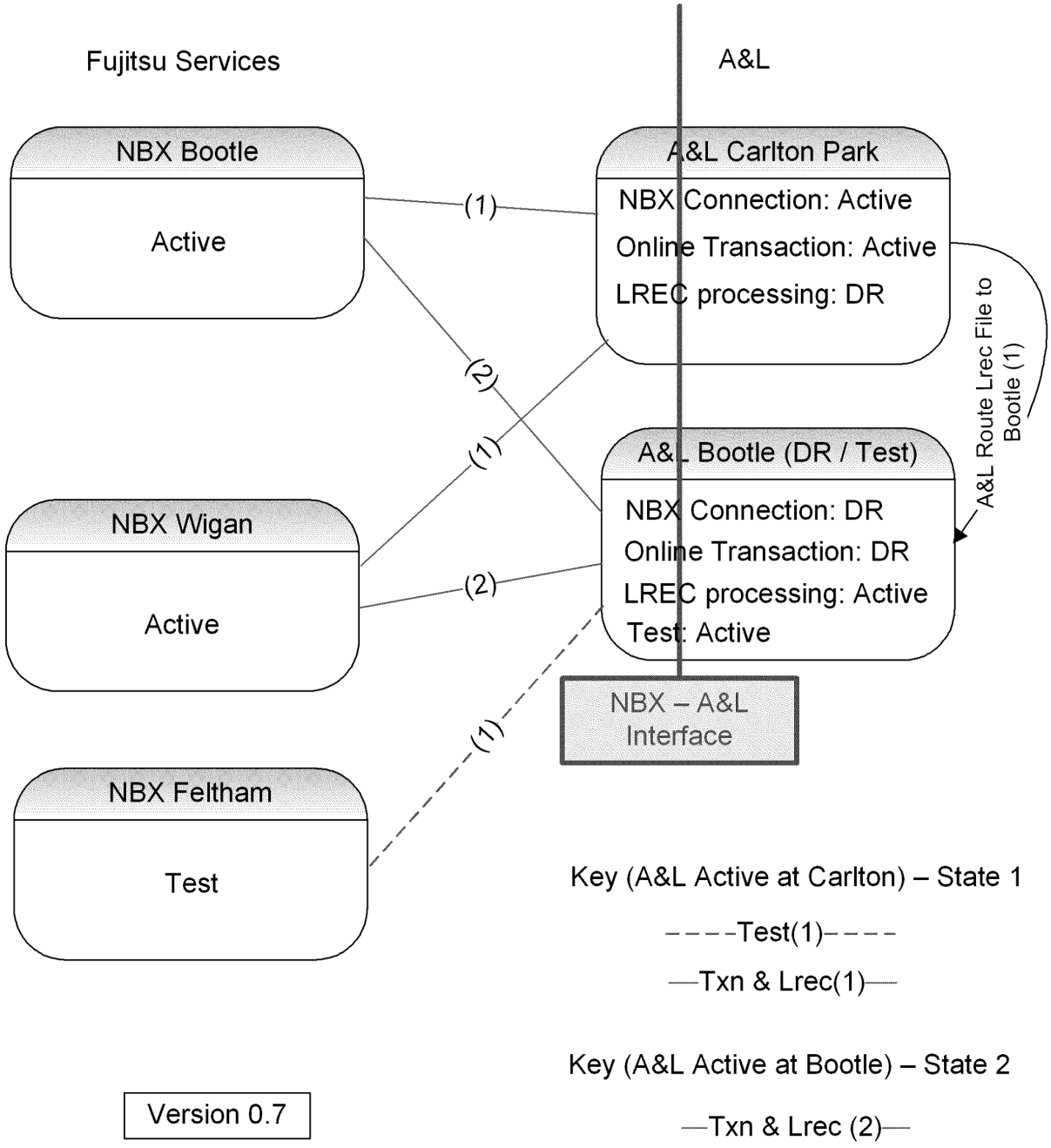

Figure 1 – NBX and A&L Context

Notes.

1. Internal Interfaces between prime and disaster recovery sites of each party (e.g. A&L Prime to A&L DR) are excluded from this specification and so are omitted on the diagram.

FUJ00001883

2. Only one A&L site will be running the production financial transaction processing service at any time.
3. Network connectivity is maintained between both the Fujitsu Data Centres and both A&L sites. Therefore the network equipment terminating the wide area network at the A&L DR site is functioning.
4. A&L onward route the REC file from Carlton Park, Leicester to Bootle in production.
5. The Production server (for LREC file processing) is located at Bootle and the DR server for LREC file processing) is located at Carlton park. In normal operation (Carlton Park not in DR for Online Transactions), the LREC file is physically routed via Carlton Park, and A&L then onward route to Bootle.
6. Functional testing capabilities will be provided by NBX Feltham and A&L DR location. The proposed design for test allows primarily for functional testing to be conducted. Within the constraints of the bandwidth provided (and any applied QoS measures) volume testing may also be carried out.

3.2.1 Design Principles

The following principles are assumed to govern the design and implementation of the interface:

- In the production environment, no Single Points of Failure will be operated by either party. In the DR environment each party will take a risk based approach to assess the need for redundancy / resilience etc.
- No single failure will impact the service offered to customers. In the event of a single failure, the full load will still be supported.
- Multiple physical communication lines are configured. Following the failure of any single communications circuit, a backup will take over automatically (no manual intervention). The resulting network configuration will be capable of handling peak transaction volumes.
- Each physical communication line is routed via a different Telco exchange (subject to survey), enters the building at a different point and approaches the building from a different direction. The option for keeping the individual physical communication lines separate within the Telco network will be specified (subject to survey) if the Telco does not provide for dynamic rerouting when failures occur.
- Encryption of data over the Wide Area Network (for production traffic only) will be provided via the IPSEC protocol (FJ Router to FJ Router). Note that FJ provide the Wide Area network and the encryption / decryption takes place fully within the FJ domain.
- The Applications should be logically configured to use multiple threads so that loss of a thread does not impact the service to customers.
- NBX will Operate an Active / Active data path model, meaning that in the event of a disaster the data connections are already established, requiring only the Application to re-establish TCP connection to A&L. If the A&L Tandem goes into contingency this will not force the NBX to invoke any contingency location due to the Active / Active NBX model described above.
- If either the A&L or NBX live systems fail, suitable contingency systems will be provided to maintain service in accordance with the SLA.

FUJ00001883

3.2.2 Location of NBX – A&L Physical Interface

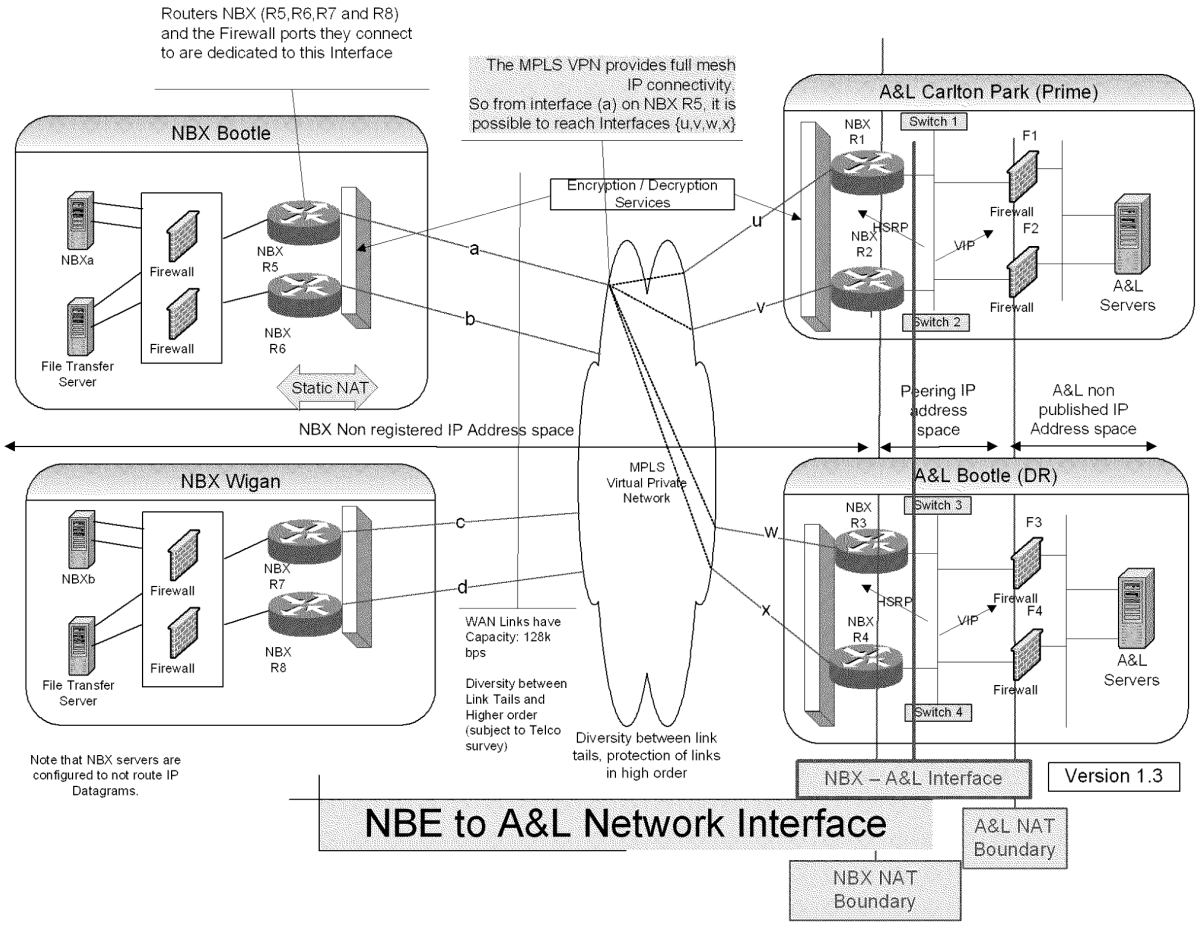

Figure 2 – NBX – A&L Physical Interface

The following table defines how the data paths are normally used;

Data path	Usage
A	Primary data path for NBX Bootle
B	Secondary Network path for NBX Bootle
C	Primary data path for NBX Wigan
D	Secondary Network path for NBX Wigan
U	Primary data path for A&L Carlton park
V	Secondary Network path for A&L Carlton park
W	Primary data path for A&L Bootle
X	Secondary Network path for A&L Bootle

IP Routing will apply costed routes in order to prefer Primary data paths. This will result in deterministic data paths and symmetry when no failures are outstanding. So for example if NBXa is sending an IP datagram to the A&L server at Carlton Park, then the data path will be (a, u).

.

FUJ00001883

Readers should note that the testing configuration can be found in Appendix B – Testing.
Fujitsu will provide a maximum of two A&L Facing routers (requiring A&L IP addressing) per A&L location as shown in figure 2 above. In addition the Telecommunications service provider (ENERGIS) will terminate their service on a pair of CPE Routers at each A&L location.
It is expected that there would be no more than four Fujitsu devices (Routers) per A&L location.

A&L will provide two sets of rack space in each of their Data centres.

The interface is shown on the diagram, 'mid span' between the cables that connect the Fujitsu Routers to the A&L Switches. Fujitsu Services supply two routers at each A&L site. Encryption over these WAN links will be provided using Cisco software encryption (IPSEC).

.Specific characteristics of the Interface are documented in the following table.

Boundary	Overview
Component	POL (through its agent Fujitsu Services) will provide and manage all components to the left of the line labelled A&L – NBX interface in Figure 2 – NBX – A&L Physical Interface. A&L will supply the cables for the connections to the A&L switches. Within the A&L locations, space will be made available within racks for the NBX routers. These routers will have connections to: The WAN circuits from the telecommunications provider The A&L firewalls.
Network Management	The A&L firewalls are fully within the A&L Network Management domain. The NBX routers are fully within the NBX Network Management domain. The Connections between the A&L Firewalls and the NBX Routers fall into both the A&L and NBX Network Management domains as far as monitoring is concerned. ICMP Ping requests received from the NBX Routers and similarly to the NBX Routers will normally be denied. This may under exceptional circumstances be enabled through change control with the explicit consent of both parties.
Operational	The NBX routers located at the A&L locations are operated remotely. Once these routers have been commissioned, occasional and infrequent physical access may be required, for example to replace a faulty component, and on a periodic basis to update the Shared Keys within the A&L located (Fujitsu provided) routers. The Connections between the A&L Firewalls and the NBX Routers are placed within the same Operational domain as the A&L Firewalls. Changes will only be made to the Connections under agreed procedures. Performing these procedures will require agreement from both network change management domains.
Environmental	Responsibility for providing a suitable environment for the NBX Routers physically located at A&L falls to A&L.

3.3 Components

3.3.1 Wide area Network Links

Fujitsu Services will provide an IP backbone service based on an MPLS VPN cloud between the two A&L locations and the two NBX locations (two live, 1 test).

All production links into NBX locations are diverse (subject to Telco survey) with high order separation. Similarly for all the links into both the A&L locations. The term diverse is used to denote physical separation of 'tail circuits' from the Telecommunications provider. The term "high order separation" is used to denote the service provided by Telecommunications providers where the pair of Tail circuits are not multiplexed into the same physical higher bandwidth links. Encryption is provided using Cisco Router (IPSEC) encryption.

FUJ00001883

The WAN implementation is fully meshed, covering all possible data paths for Production traffic.

Utilisation, performance of the circuits and router-to-router availability are constantly measured by Fujitsu Services.

3.1.2 NBX Servers

There are two Computer Platforms that contain the interface endpoints on the Horizon side.

Hardware	Fujitsu Server
Software	Windows 2000
	NBX Agent Application
Security Hardware	Integral HSM.

3.1.3 NBX File Transfer Server

Hardware	Fujitsu Server
Software	Windows 2000
	CONNECT: Direct

3.1.4 A&L Servers

This platform type consists of a Tandem S Series Computer System that supports A&L processes that communicates with NBX. There will be a Computer System at each of the primary and disaster recovery locations (Carlton Park and Bootle respectively). Normally the A&L processes will run on the Computer System at the primary location, with the Computer System at the disaster recovery location. The contingent data held at the DR location is updated in real time. Each Server will run multiple processes.

3.1.5 Security Hardware

The NBX and A&L configurations will include firewalls and routers to implement security policy for specified ports and addresses. The network infrastructure also includes Triple DES cryptographic capability which is implemented within the routers. This is used to create IPSEC tunnels over the Wide area network for protection of production application traffic.

The NBX and A&L configurations include hardware cryptographic features to conform to the requirement for PIN block Encryption. PIN blocks are Triple DES encrypted.

3.1.6 Network Equipment

Cisco routers are used for Fujitsu Services provided routers.

Cisco switches are used for A&L provided switches.

FUJ00001883

4 MEDIUM OF TRANSFER

4.1 Interface Overview

The Interface between NBX and A&L is a telecommunications link. All data passes on this link except the three Zone Master Key components which are passed in securely printed envelopes at intervals between six and twelve months. This Key transfer and its associated procedures are outside the scope of this document.

The online interface between NBX and Generic FI will support a set of messages as described in the AIS [AIS].

The OSI Reference model [OSI] is used as a convenience to structure the documentation of interface components, starting at the Physical level.

4.2 Layers 1 and 2 - Physical and Link

At the A&L prime location, A&L firewalls (F1, F2) will connect (via a LAN segment) to the NBX routers (NBX R1, NBX R2). The router Interfaces will be Fast Ethernet. Each Router and Firewall will be connected to two separate switches.

At the A&L Bootle location two routers and two firewalls will be utilised in order to maintain consistency of approach with the primary location at Carlton Park.

Fujitsu Services will provide IP connectivity between NBX locations and A&L locations.

Resilient termination of network connections is provided across all production sites.

Production Network links will also provide backup routes, which enter the locations at a different point and follow a different route to a second local exchange. These provisions are dependent on physical structures, wayleaves and local exchange location.

Two circuits will terminate at each A&L datacentre. The bandwidth may increase in accordance with the volume requirements of the service.

Both of the physical NBX locations will operate a production service. Conducting of Testing and the hosting of PO Ltd testing servers is supported from a separate PO Ltd location,.. A&L testing is Hosted at and conducted from the A&L DR site (Bootle).

NBX does not provide inter campus PVCs directly between A&L sites and therefore A&L will ensure the onward routing of the LREC file between Leicester & Bootle in production. If A&L invoke DR procedures then all traffic from NBX locations will be routed to Bootle.

Only one of the physical A&L locations should operate a logical production service at any one time (noting the onward routing by A&L above – the system for Production LREC processing is hosted at Bootle).

4.3 Layer 3 – Network

This section is concerned with the interface description at layer 3 that is IP. For purposes of description this section is split into 4 subsections:

FUJ00001883

- Control plane, concerned with Routing and ICMP
- Data plane, concerned with actual flow of IP datagrams
- Virtual IP Addressing
- IP Address spaces, concerned with enumeration of IP address space and translation schemes

4.3.1 Control Plane

4.3.1.1 IP Routing

At each A&L location, in order to provide a fully resilient link between the pair of A&L Firewalls and the pair of NBX Routers, the following method is used:

1. Each NBX Router is connected to a separate layer 2 switch provided by A&L. Note that both Routers are connected to the same VLAN.

2. The layer 2 switches are trunked together in order to provide resilience.

3. The pair of NBX Router's runs HSRP in order to provide a resilient IP Gateway to A&L for reaching the NBX locations. Note that HSRP provides a floating IP address which is assigned to the primary Router. The A&L Firewalls will be configured to use this HSRP address as the "next hop" for all non local IP datagrams destined for NBX platforms.

4. Similarly each A&L Firewall is connected to a separate layer 2 switch provided by A&L. Note that both Firewalls are connected to the same VLAN.

5. The pair of A&L Firewall's operates in an Active / Standby configuration and provides a virtual IP address for the A&L Online Transaction service and the A&L LREC file transfer service. The "Active" firewall will respond to ARP requests for these VIP's and route traffic received for these VIP's to the relevant A&L platforms. In a Firewall failover scenario the Firewall that has recently become active will use "Gratuitous ARP" to cause the Fujitsu Routers to forward traffic to it.

There is no IP Routing protocol running across the interface.

4.3.1.2 ICMP

In an investigative or pre-live testing scenario, the following may apply subject to agreement and on acceptance of an appropriate change control by both parties: NOTE – the default behaviour to all ICMP Echo traffic will be drop the packet and not respond.

1. ICMP Ping traffic is allowed to the directly connected interfaces on the NBX Router pair. Similarly, the A&L Firewall will be configured to accept ICMP Echo Requests and respond on the interface that they have directly connected to the NBX Router Pair. The source IP addresses of these interfaces is documented in the IP Address space section.

2. ICMP Ping traffic is allowed to pass from A&L to the IP addresses (Virtual) associated with the NBX. Also ICMP Ping traffic is allowed to pass from NBX to the IP addresses associated with the A&L servers. This is to allow complete network routes to be confirmed.

4.3.2 Data Plane

All traffic over the interface at level 3 will be IPv4.

4.3.3 Virtual IP Addressing

FUJ00001883

The NBX Routers at the A&L locations use HSRP to provide a resilient IP gateway to A&L.

The A&L Firewalls use a clustering protocol to provide a Virtual IP address (VIP) for the A&L Online Transaction service and the A&L LREC file transfer service.

The A&L platform provides a facility for resilience to Network Interface failure.

The NBX platform provides a facility for resilience to Network Interface failure. This is achieved by use of a "teamed" network Interface cards.

The failure of an Interface will be transparent to level 4 (TCP/IP) and have a negligible impact on agreed service levels – e.g all routes are pre-configured, with session disconnect / reconnect at the TCP level being visible.

4.3.4 IP Address spaces

The purpose of this sub section is to:

- Provide an overview of the various IP address spaces from which components associated with the interface are allocated IP addresses. Note that the criteria for associating a component with the interface are stated in section 3.1.
- State the points at which Network address translation (NAT) is performed and the type of NAT.
- Enumerate the usage of IP addresses in all components associated with the interface.

4.3.4.1 Address Space Overview

There are three separate IP Address domains (please see below for terminology):

- NBX Non Registered and Non Published
- Peering IP address space
- A&L Non Published

These are illustrated in Figure 2 – NBX – A&L Physical Interface. The Boundary between the NBX Non Registered domain and the A&L Published domain is labelled NBX NAT Boundary. Similarly the boundary between the A&L Non Published domain and the A&L Published domain is labelled A&L NAT boundary.

The NAT Boundary represents the location within the Network that Network address translation is implemented.

The Peering IP address space is jointly agreed between A&L and NBX and documented in Appendix A.

IP Address space Terminology

- **Non Registered** IP address space refers to a collection of IP addresses not assigned by IANA.
- **Non Published** IP address space refers to a collection of IP addresses which are associated with components involved in this interface (for example addresses associated with physical interfaces) but whose values are not relevant to IP datagram exchange across the interface,
- **Published** IP address space refers to a collection of IP addresses that are used for any or all IP datagram's that traverse the interface,

4.3.4.2 Network Address Translation

Network Address Translation (static with no port overloading) is performed at the points shown in Figure 2 – NBX – A&L Physical Interface.

FUJ00001883

4.3.4.3 IP Address usage

The values for the IP addresses are provided in Appendix A.

4.4 Layer 4 Transport

The only Transport protocol used across the interface is TCP/IP. The mode of use is Client Server, and NBX is the Client in the relationship initiates all TCP Connections. Either end can initiate Data Transfer (subject to the AIS). Either end can terminate TCP Connections.

4.4.1 Transport Level interface

At this level, there is no single location for the A&L NBX Interface. This is because TCP/IP is essentially a cooperative protocol between two endpoints. For example, a TCP connection exists between a component (A&L Process) located on the A&L Server and a component Agent on the NBX If the flow of bytes from the A&L Server to the NBX is slow then this can be caused by either the NBX reading too slowly, or the A&L process writing too slowly. Whilst these behaviours can be distinguished by observing the TCP communication, they cannot simply be differentiated at the Application interface into TCP (socket level). The consequence of this is that any measurement of service levels at the transport layer and above need to take account of this TCP connection behaviour.

4.4.2 TCP Keep Alive

The purpose of TCP Keep Alive's is to detect disappearing endpoints and inform applications that a connection is broken. For example, in a client server environment, if a client fails then a listening server will not necessarily detect this. Over a period of time 100's of such stale connections may result in the server running out of resource and having to be reloaded. TCP Keep Alive's are only sent when the connection has been idle for a defined time interval and thus pose very little overhead. Section 4.7.5 states that 0800 echo test messages will be used. However TCP Keep Alive's are configured as they prevent the server having to be reloaded as a consequence of too many stale sessions

The following table defines the parameters which define the TCP Keep Alive behaviour over the interface.

TCP Property	Overview	NBX	A&L
Keep Alive Idle	Seconds between each TCP keepalive segment if no data has been sent on the connection.	30	45
Keep Alive Retransmit Interval	Seconds between successive retransmissions of the keepalive segment when a response to an initial keepalive is not received.	5	45
Keep Alive Retry Count	After sending (Keep Alive Retry Count) retransmissions the connection is abandoned.	6	8

The impact of the above is that from the NBX perspective, a failure will be detected and the connection re-establishment process will begin within 1 minute.

4.4.3 TCP Data Flow

This section documents configuration options for TCP Data Flow behaviour and their settings.

FUJ00001883

TCP Property	Overview	NBX	A&L
Delayed Acknowledgements	When a TCP peer receives a segment, the acknowledgement of the segment is not sent immediately.	Enabled (Delay Ack Time) 5 milliseconds	20 milliseconds
Nagle Algorithm	Please refer to RFC 896 for further details.	Enabled	Enabled
MSS Adjustment	Cisco Routers provide the functionality to adjust the MSS on a TCP connection to avoid IP datagrams that are too large to pass through the network without fragmentation and / or discard.	Set to 1300 bytes to avoid IP fragmentation on any Ethernet interfaces that are traversed by the IPSEC tunnels.	NA for A&L (WAN only)

4.4.4 Application Endpoints

This section provides an illustration of Application Endpoints and associated TCP connections concerned with the NBX – A&L Transactional Interface.

FUJ00001883

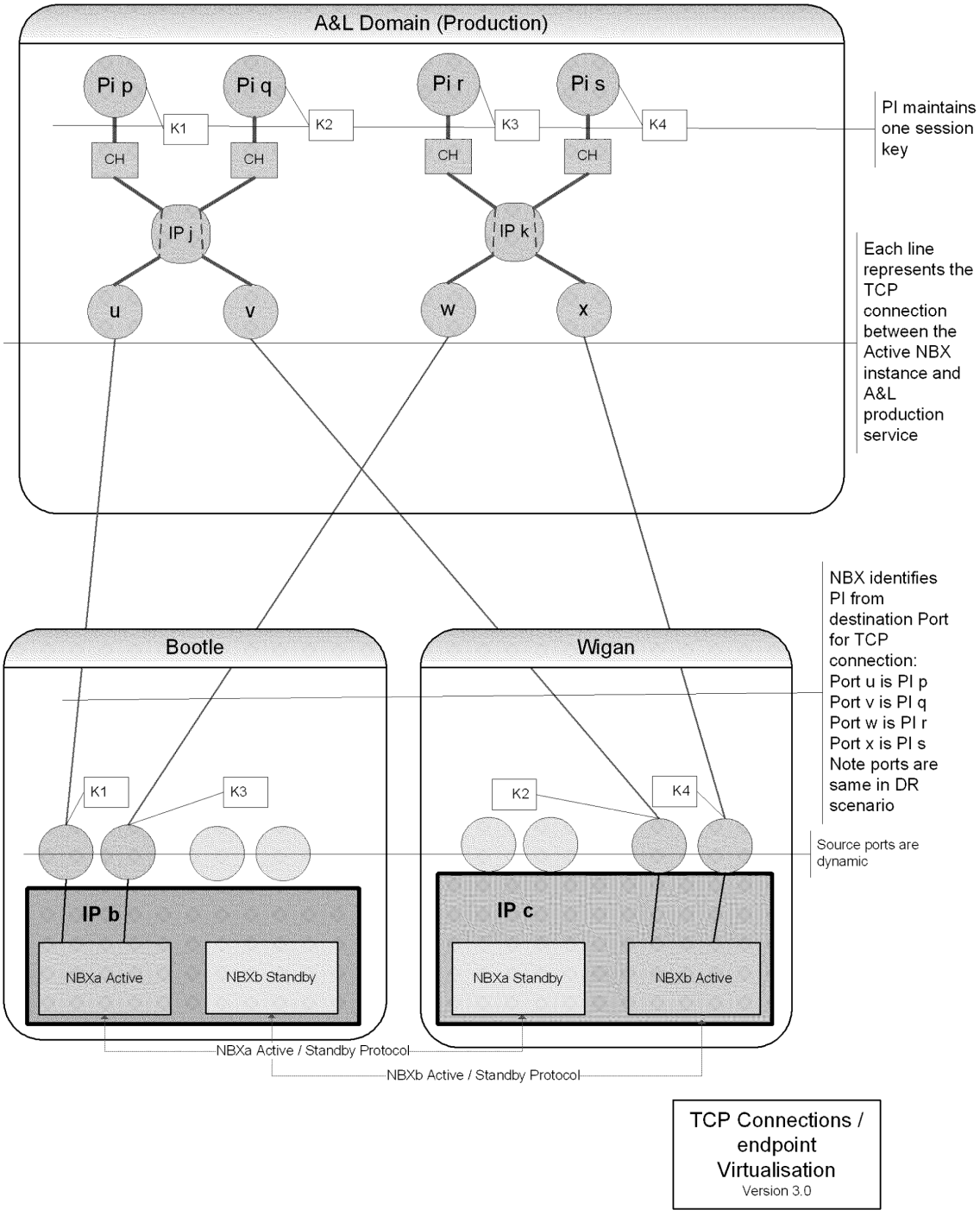

Figure 3 Application Endpoints

FUJ00001883

4.4.5 Migration of IP Address to another Computer System

TCP/IP connections will fail during a machine swap over (for example if the hardware platform is changed). In order to remake these connections the components will:

- For A&L - enter into a listening state, ready to accept connections from NBX
- For NBX - Attempt to initiate connection setup by retry (after a delay reference section with behaviour rule) until the connection is made.

4.4.6 TCP Connection Management

4.4.6.1 Overview

A&L will configure four BASE24 PI's on their Production and Contingency (DR) applications. Also A&L will configure 4 such PI's on their testing system.

Each PI will operate a TCP/IP socket on each Ethernet port used for this connection, giving multiple active sessions for production transactions. Each PI will use all of its socket connections for production transactions so long as they are available.

The NBX will load balance Horizon acquired transactions between the available socket connections to ensure the load is distributed across the PI's. Please refer to 4.4.7 for a description of Load sharing.

The environment described in this section is is replicated in the Disaster Recovery, Test, Development and Certification application environments at A&L, scaled appropriately. When testing connections are required additional TCP/IP socket connections will be made to the TCP/IP addresses and ports nominated by NBX for their test systems. These additional testing and CONNECT: Direct sockets will be established over the existing communications infrastructure.

The scheme for sockets and TCP/IP addresses and ports is as follows. The A&L BASE24 implementation will be configured with four PI's facing the NBX. There will be one port per PI. This configuration will support the full peak transaction load with a single failure to any component. Refer to Figure 3 Application Endpoints for an illustration of the socket connections between NBX and A&L PIs.

In production separate A&L threads will maintain a TCP/IP socket connection down each Ethernet Port at A&L. This configuration allows for the failure of a circuit, the Node, the Switch or one of the firewalls while still maintaining full production service between A&L and NBX.

(DN: Ethernet ports on Tandem –Active / Standby – from A&L, replace above paragraph.)

As and when required, additional TCP/IP socket connections will be established to facilitate the CONNECT: Direct transfer of the Reconciliation file or the establishment of testing connections.

At the TCP/IP communications level, connection establishment and re-establishment will be managed from the NBX end of the interface for all TCP/IP socket connections. The NBX end will use dynamic ports as detailed in "Appendix A" Detailed Configuration.

If NBX fails to establish a connection, or a connection fails it will retry connection establishment (after a delay of at least ten seconds, configurable) until the connection is made.

FUJ00001883

4.4.6.2 NBX failover

Fujitsu have two data Centres, located at Wigan and Bootle. The NBX is mapped to two computer platforms, one at each Data centre.
For example NBXa will be “Active” on a Computer platform at the Wigan Data Centre and in “Standby” on a Computer platform in the Bootle Data Centre. The “Active” and “Standby” roles are agreed and maintained using a protocol between the Two Computer Platforms.

1. The “Active” instance of NBXa (and similarly NBXb) will maintain TCP connections with A&L as already mentioned earlier in this document.
2. When a “Standby” instance takes over as “Active”, a TCP connect followed by an application level sign on will be performed on relevant PI.

4.4.6.3 A&L Move To DR

After DR invocation by A&L [OLA], the published (as visible to NBX) IP addresses at the DR site are different to those in live.. The Ports do not change since these are used by NBX to identify the Pi’s. Correct identification of PI’s is necessary – please refer to 4.7.10.

4.4.6.4 TCP Connection termination

Either end can terminate TCP Connections.

Dynamic source ports are used on the NBX (initiator) hence a connection that has terminated but remains in TIME WAIT state (default RFC 793 is 240 seconds) will not prevent a new TCP connection being established.

4.4.7 Load Sharing

NBX is responsible for the sharing of transaction volumes across its PIs and the established TCP/IP sockets. The population of Post Office Outlets is split across the two NBX instances (NBXa and NBXb) in an approximately even split.

The objectives of this load sharing are twofold:

- To ensure that the A&L software processes are balanced in terms of transaction volumes and hence CPU utilisation on the A&L switch.

If the entire system is well balanced at the communications infrastructure and PI level then the response times across the A&L switch and communications queue times between A&L and NBX will be reduced, resulting in better overall transaction response times.

Each NBX instance will round robin select the PI for each transaction to be sent to A&L. (This needs to be done for correct AWK selection). The NBX will then round robin select one of the usable*TCP/IP sockets associated with the A&L facing PI, for the transaction to be sent to. This is illustrated in .

* The NBX will attempt to maintain TCP connections as defined previously. The NBX instance will consider the TCP connection usable if no errors have been reported for the connection from the Sockets API and the backlog of outstanding (awaiting A or timeout) R messages is less than an agreed threshold (as set in configuration parameters).

A&L will deliver the transaction response message to NBX using the same TCP/IP socket as the original transaction request came to A&L on. In the event of the TCP/IP socket being unavailable for delivery of the response message the transaction response will be reversed by A&L. It is assumed that the Counter position will have timed out and hence denied this transaction.

A NBX initiated reversal will be scheduled to the same PI as the original R message. Please refer to Message Exchange patterns section 4.7.10 for further details.

FUJ00001883

4.5 Layer 5 – Session Layer

4.5.1 Sign on / Sign off

NBX and A&L initiate or close sessions using sign-on and sign-off messages. Sign-on messages are followed by transmission of an acquirer working key, AWK, from A&L to NBX. Message details and flows are provided in the AIS. For an overview of the AWK exchange refer to Figure 4 – Acquirer Working Key Exchange.

4.5.2 PI identification

The NBX Agent application needs to be aware of which A&L PI a TCP connection is associated with. For example, establishing a session with a sign on message is done per PI not per TCP connection.

NBX identifies the PI by use of Configuration items (IP addreses and ports).. Refer to Detailed Configuration for an illustration of this configuration data. Note that each PI has a unique port and this is preserved during DR.

Note that the NBX Agent does not share session keys across computer platforms.

4.5.3 Sessions

A A&L PI can only hold one working key (AWK), since NBX Agent processes do not share AWK's, this means that a A&L PI can only maintain sessions with one NBX Agent process at a time. However an NBX Agent process can maintain sessions with many A&L PI's concurrently. The configuration as show in Figure 3 Application Endpoints meets these constraints.

4.6 Layer 6 – Presentation Layer

4.6.1 Character Sets

The A&L Servers and the NBX use the ASCII English character set (CCSID = 437). This is a 7-bit character set. Note that the parity bit is not used and set to 0.

4.6.2 Base 64 Encoding Rules

All encoding will be carried out according to the scheme defined in [RFC2045] section 5.2.

4.7 Layer 7 – Application Layer

Information regarding transmission of financial transactions and key exchanges at this layer in described in the AIS [AIS].

Transfer of reconciliation information (REC) will be performed using CONNECT: Direct.

4.7.1 Interface to Transport Layer

The NBX - A&L interface is comprised of the following two major interface types:

- The NBX - A&L BASE24 v6 Interface. This is the default Interface, used for all messages defined in the AIS [AIS]..

FUJ00001883

- The Data Reconciliation Interface. This interface is only used for the batch transfer (per day) of data to the Reconciliation service.

Figure 3 Application Endpoints illustrates the TCP Connections and Ports between the A&L Systems and the NBX Systems. Only some of the interface elements are shown in order to provide clarity. This is based on the following key features of the A&L Server design and how this is to be interfaced most effectively with the NBX software.

- The connection relationship must be maintained for certain messages (0200/0210).
- There will be one Port per PI and there will be one TCP/IP socket connections per Port). These Ports will be opened as listeners, that is the NBX will be acting as a client.
- Under normal operational conditions there will be no Application connections made between any NBX servers and the A&L DR site. In the event of a DR scenario then all Application connections from the NBX Active server will be with the A&L DR site.

4.7.2 Message delineation

As the messages defined in the AIS are (or can be) of variable length, a mechanism is required for the applications on either side of the interface to recognise when a complete messages has been read from the socket.

The mechanism used is for a length field to precede each message defined in the AIS. This is a 2-byte binary Big Endian field.

Since TCP is a stream based protocol with no explicit support for message boundaries, the applications on either side of the interface will issue one or more calls to the TCP layer in order to get a complete message. Specifically the applications support the fact that there is no alignment between application message boundaries and the data returned from the TCP layer on a read call.

An application may close a TCP connection if it detects a fundamental inconsistency in the data being received which may not be ultimately recoverable by any other method (for example an invalid message length field).

4.7.3 Reconciliation File Transfer

The Reconciliation file will be transferred from the NBX system to the A&L system using CONNECT: Direct file transfer software from Sterling Commerce, over a TCP/IP socket connection.

The CONNECT: Direct file transfer will be made between any NBX data centre and the A&L Production data centre. NBX is always the initiator of any File Transfer.

When A&L is operating from its DR site the CONNECT: Direct transfer will be made to this site.

In the event of a prolonged CONNECT: Direct file transfer failure it is assumed that WAN service can be resumed, the file transferred and the data processed at A&L all within 24 hours of link failure. Therefore there is no need for a magnetic tape standby process. Note that there is a pair of resilient links into each NBX Data centre and each A&L data centre. It is sufficient for just one link to be working in order to provide WAN connectivity for File Transfer. For this reason no standby process has been specified.

The following table summarises properties for the file transfer

FUJ00001883

Property	Details
Authentication details	The local NBX client will have a user ID associated with it - basically the username under which the file copy is performed. A&L map this user name on to an IBM user on A&L's host to give it the appropriate copy permission's both in Connect Direct and to the destination file." This is because the destination file name will be defined in the Connect Direct parameters by NBX. Following data is needed and values are provided in A.4. A&L require from FS: • User ID (one for test, one for prod) • TCP/IP address (x3 - one for prod, one for prod failover, one for test) FS require from A&L: • Node Names (this is the "SNode" Parameter in CONNECT: Direct) - Same Node ID is used for prod & test. • IP address - only one for the CONNECT: Direct Node on S/390.
Filename	Live : "LAB.POCL.FILE(+1)" Test: "DEVAB.POCL.FILE(+1)" Note that filename is as within the quotes. Basically this means that the file created has a generation number one greater than previous file. As soon as the file arrives successfully, the A&L automation will process it. Therefore if NBX needs to resend the file it will require an operator discussion. Note that CONNECT: Direct will resolve the partial loss issues etc and allow for the success of the Transfer to be determined by the return code generated.
Compression	The CONNECT: Direct option to compress the file content during transfer is used and specified by NBX.
Compatibility	In order to maintain compatibility between CONNECT: Direct on NBX and A&L platform the platform Operating system and CONNECT: Direct versions are specified in [OLA]. Prior to making any changes to these items, the proposed change will be checked against the Compatibility Matrix for CONNECT: Direct in order to ensure that as a consequence of the change compatibility is maintained.

4.7.4 Communications Handling

Application level communications handling (i.e. sign-on, sign-off and echo testing) are described in the AIS [AIS].

FUJ00001883

4.7.5 Handshakes

"Handshaking" (Application echo testing) is implemented. The purpose of Application Handshakes is to detect and alert failures in Application to Application communications when no Transactions are flowing. The interval setting for this (per PI) is specified below. Both NBX and A&L may independently initiate these handshakes based on their own timers, and generally, the party whose inactivity timer expires first initiates that handshake.

During a period of low transaction activity, e.g. overnight, the interval between actual transactions may be hours. Should a communications fault occur between transactions then that may not be detected until the next transaction is attempted and failed. Handshaking, testing the existence of a communications connection, can detect and advise of a problem much earlier and have a lesser impact on real transactions. Providing handshakes amd transactions are performed on all TCP connections then any communications problems will not remain undiscovered for any long period of time.

4.7.5.1 NBX behaviour

The NBX application will send ECHO TEST messages when there has been no traffic over a TCP connection for a configurable period of time (set to 60 seconds). NBX sends Handshakes per TCP connection and responds to Handshake requests on the same connection as they were received.

After a configurable number of consecutive non-responses (set to 6),

1. NBX will invoke Application sign on

2. Should there be no response to a number of Application Sign-ons, NBX will terminate (force) the TCP connection and then try to establish another TCP connection, and continue to do so in line with the guidelines in 4.4.6.1..

3. Once the TCP Connection is established, NBX will invoke Application sign on.

4. If NBX is not signed on with respect to a particular PI, it will not send Handshakes to that PI. However it will respond to Handshakes from that PI.

4.7.5.2 A&L behaviour

1. The parameter which specifies the frequency of 0800 handshake messages in the absence of other network traffic is WAIT FOR TRAFFIC and this is set to 60 seconds. A&L sends Handshakes per TCP connection and responds to Handshake requests on the same connection as they were received.

2. There is an additional parameter which specifies how long to wait for a response (NETWORK MANAGEMENT TIMER LIMIT - set to 60 seconds). After a configurable number of attempts, (currently 3 timeouts), a lack of response causes the station to be marked as down.

3. Any message received on the station causes the station to be marked as up.

4. A further parameter (EXTENDED NETWORK TIMER LIMIT - set to 300 seconds) dictates how long to wait if a network management response is not received before sending a further Handshake.

5. If a station is marked as down then this is a logical state that prevents transactions being sent to NBX on that station. However since A&L do not initiate transactions to NBX this has no impact to the operation of the interface.

6. If there are no stations up for NBX, the link is marked down. This is another logical state that causes an EMS message (alert to Operator) to be generated on transition. An extended network management timer is then started.

FUJ00001883

7. When the extended network management timer expires, a new handshake message is sent to NBX. This timer relates to each individual TCP connection. In the case of the current design only 1 TCP connection exists to 1 process (PI).

Note.

All stations down do not cause PI to transition to "signed off" state.

The term station is equivalent to an A&L TCP port and also TCP connection.

If an A&L PI is not "signed on" (refer to 4.7.10.5) then the NBX Handshake will be accepted as normal.

4.7.6 Acquirer Working Key (AWK) Exchange

Figure 4 – Acquirer Working Key Exchange

NBX will generate the Acquirer ZMK (AZMK) that applies to the acquirer zone. It is distributed to A&L using manual procedures. The Acquirer Working Key (AWK) will be generated by A&L and sent to NBX in a 0800 network management message as described in the AIS.

NBX may request the generation of a new Acquirer Working Key at any time as described in [AIS].

4.7.7 Network Management Messages (Network Management Codes)

Within the A&L, Tandem the NBX connection will be configured as Triple DES, Acquirer only.

The Network Management codes that should be used to support the triple DES, Acquirer only configuration are provided in the AIS.

4.7.8 Delay (“Stand In”) Processing

The connection between NBX and A&L will be NBX acquiring only. Delay processing is therefore not strictly applicable to this connection. The design principles state that the service to customers not be affected by single failures, and the sizing and topology of interface components needs to reflect that**.** However, there may still be situations (in multiple failure scenarios) where A&L could be considered by NBX to be “in delay” and therefore the AIS [AIS] needs to document the procedures in this case. In general, the reversal queue will be cleared first before any new transactions will be allowed.

4.7.9 Time-outs

The [OLA] documents the A&L timeout settings within their system design on authorisation requests to the card authorisation system so that other cascading timers can be set accordingly.

4.7.10 Message Exchange patterns

This section documents associations between Application level messages and TCP Connections, PI’s and Ports. It should be noted that Messages may be interleaved and there are no restrictions on the number of outstanding requests without a response.

FUJ00001883

4.7.10.1 Reversal Initiation from NBX

NBX can send Reversals even in the case where a response to the original Request has been received from A&L – there is no possibility of false credits.

4.7.10.2 Response from A&L

A&L will send responses from the same IP address and Port that the associated “Requesting” message was received on.

In the event of a TCP Connection not being available for delivery of the response message, the transaction response will be queued by A&L (up to a configurable buffer size) and forwarded when the TCP Connection becomes available.

4.7.10.3 Response from NBX

NBX will send responses to A&L using the same TCP/IP Connection and hence PI as the original request came to NBX on.

4.7.10.4 Must Deliver Messages (including Reversals)

For “must deliver” messages, the NBX will send these to the same PI as the original request. In the event of there not being a usable TCP connection to the PI, NBX will hold the Reversal Message in a Store and Forward queue and empty this queue once there is a usable connection. The length of time that Reversal messages are held in the queue is configurable.

Note that in the case where A&L has moved to DR, the same set of PI’s is available as in the normal production environment (from the NBX Agent perspective). This is due to the PI identification scheme used – see 4.5.2.

4.7.10.5 Application Sign on

The Application sign on message exchange pattern (MEP) causes side effects at the PI level. Specifically each such MEP results in a new AWK per PI. Note that there will be no sharing of AWK between NBX Agent instances.

For purposes of description:

1. The NBX Application has a local state variable with possible values {"signed on"," signed of", "not sure"} with respect to a particular PI.

2. Similarly for the A&L application.

An NBX Application will transition to a "signed on" state with respect to a particular A&L PI under the following conditions:

- It receives a success response to an associated sign-on request sent to the PI
- It sends a success response to a received sign-on request received from the PI

The following points cover some properties of this "signed on" state and transitions to / from it. Note the term Application applies to both NBX and A&L applications.

1. Application Sign-on / Sign-off apply at the PI level and not the individual TCP connection level.
2. It is not necessary for an Application Sign-on to be performed when a TCP connection is established. This deals with the case where there are multiple TCP connections per PI.
3. An Application Sign-on sequence results in a new AWK for the PI.

FUJ00001883

4. An Application should be in a "signed on" state for a PI before any messages (other than Sign-on request/ handshake request or response) are sent to that PI.

5. An Application leaves the "signed on" state when it receives a successful response to a sign-off message.

6. An Application leaves the "signed on" state when it sends a successful response to a sign-off message.

7. An Application does not have to leave the "signed on" state if all TCP connections between NBX and an A&L PI are terminated.

8. It is valid for an Application to send a sign-on at any time. In this case a new AWK is established. This behaviour is required to handle the condition where the Application is not sure of the state of its peer, for example NBX initiates a new TCP connection to A&L following failure of all TCP connections to that A&L PI. By simply performing an Application Sign-on sequence the NBX application can assert that both it is signed on and the A&L application is signed on.

FUJ00001883

5 Operational Considerations

5.1 Systems Management

There is no centralised Systems Management tool operating across the A&L – NBX Interface. Traffic consists of ICMP data only when agreed, refer to section 4.3.1.2.

5.2 Network Management

All network components and links in the A&L Domain (that is to the right of the line labelled A&L to NBX Interface) in Figure 2 fall fully within the scope of A&L Network Management.

Refer to section 4.3.1.2 concerning use of ICMP Ping.

Utilisation and performance of the circuits and router-to-router availability are monitored by Fujitsu Services.

5.3 Restarts

The NBX and A&L will exchange handshake messages at a regular configurable time interval. Refer to section 4.7.5 for details of the handshake process and action taken upon lock of response to repeated handshakes.,

5.4 Resilience and Fail Over

The following table provides a summary of the resilience mechanism for the components concerned with the A&L – NBX Interface. (The criteria for inclusion of components were stated in section 3.1).

Resilience covers:

- Detecting that a particular component is not providing service.
- Selecting an alternative component that is providing service (termed fail over in the following table).
- Periodic probing of any standby components.

ISO Layers	Components	Resilience Mechanisms
1,2 and 3	**A&L domain and Interface Span** Network devices and links from A&L Server (Interfaces facing towards NBX) to Routers 1, 2, 3, 4 in NBX domain.	• No Single point of failure in the production environment. • Failure detection and fail over takes place mainly at level 2 • A&L Server recovery. This covers failure of the platform, and associated A&L services. Note that an A&L Service can be deemed to have failed if onward connections to other A&L components have failed.

FUJ00001883

1,2 and 3	**NBX Domain** Routers 1,2,3,4 to A&L Cluster	• Failure detection over WAN takes place mainly at level 3 using routing protocols. • NBX comprises two Agent processes NBXa and NBXb. These processes are scheduled to a pair of computer platforms one at each NBX data centre with the result that the Active instance of NBXa is on a separate platform from the standby instance of NBXa and similarly for NBXb. In the event of the Active instance failing the standby is designed to take over as Active. • Layer 2 resilience between NBX Routers and A&K Firewalls – HSRP, VRRP and Spanning tree.
4	All Components	• Most classes of component failure are 'almost transparent' at the TCP level. However, it is important to note that because TCP treats IP datagram loss as congestion, then the TCP connections are likely to shrink their Transmit / Receive Windows. A robust TCP stack is required which will correctly manage its window, especially if the number of TCP connections is low resulting in each connection having to do more work.
5 and above	Application Connection retries.	• When a network outage occurs, whether planned or unplanned the NBX will automatically detect this (usually as a result of an error code following a send or receive) and go into a "Retry" state. This means at a specified interval an attempt is made to re-establish the session. The interval will be no more frequent than 10 seconds. • This document specifies an application level Echo-Test which detects lack of application level connectivity. Please refer to section 4.7.5 for more information.

5.5 Performance

This section states the Performance targets for components concerned with the Interface.

5.5.1 A&L and NBX Platforms

The performance requirements are drawn from figures supplied by POL on the expected hourly transaction rates over the working week for each year of service. The working assumption is that the system be sized for an instantaneous peak of three times the peak hourly average volume of transactions.

This target design point for the interface is 12 counter transactions per second and this is interpreted as a sustained 5 minute peak rate. To convert this to into a rate per second for sizing purposes a multiplier of 1.5 is used giving a target of 18 transactions per second.

The impact of a single component or software thread failure will not materially affect the End User service given the level of duplication of components listed here, so that in the worst case there will still be 100% of over capacity.

FUJ00001883

This resilient & redundant model has been chosen on the grounds of best practice.

5.1.2 Wide Area Network

Based on the target design point stated above, a sizing model predicts that 128 k bps links are required from the NBX location(s) to the A&L locations for the production service. Note that the required bandwidth is predicted as about 90k bps, however taking into account resilience properties –namely a single network link failing does not impact ability to provide service and the fact that network links are procured in the following increments [64k,12k,256k,512k….] results in a pair of 128k bps links being required for the production service.

The test link will be a single ISDN channel of 64,000 bps.

The reconciliation file traffic travels out of hours and its size is proportional to the volume of daily on line transactions.

The predicted transfer time for transmission of the REC file is about 30 minutes without Connect: Direct compression taken into account. Note that Connect: Direct compression will be used however the compression ratios are currently not available.

FUJ00001883

6 Security

This section provides a very brief overview of the security aspects of this Interface.

This is a financial application. IP addresses and ports will not be published to the public. Knowledge of Security Key material/parts is restricted to nominated key holders.

6.1 End-to-End Identification

NBX and A&L open communication to an IP address and send a sign-on message followed by an exchange of working keys transmitted in encrypted form under the shared zone key of the two parties. This provides confirmation of the identities of the two parties.

Messages will be sent to or received from known IP addresses. A message from an unrecognised address will be rejected. Working keys exchanged daily under the ZMK (sent from A&L to NBX) provide positive authentication of the other party.

6.2 Encryption and Decryption Methods

ANSI standard X9.52 (1998) describes the Triple DES encryption process.

When data is Triple DES encrypted, the first half of the encrypting key will be used to encrypt, the second half to decrypt, and the first half to re-encrypt. This is the Encrypt-Decrypt-Encrypt (EDE2) method. To decrypt data the process inverted; Decrypt-Encrypt-Decrypt.

The IPSEC implementation over the WAN will use 3DES. IPSEC is used to protect production application traffic; test application traffic is not protected by IPSEC.

Please refer to [AIS] for details of encryption / decryption applied to the contents of messages. PIN block fields are Triple DES encrypted using double length keys (112 bit keys plus 16 parity bits). Other fields are not encrypted.

6.2.1 Network data privacy and authentication

The protection described here is in addition to application-level authentication and encryption, which is described elsewhere.

Operational procedures are needed for handling keys at both production and disaster recovery sites

Encryption (IPSEC tunnel mode, Triple DES) applied within the routers provided by NBX assure privacy of production data in transit across the Wide Area Network virtual private network. (See Section 6.8 for further detail).

No filtering of production application traffic is applied, all production application data is protected by IPSEC.

6.3 Application Key Management

Procedures for distribution and management of Master Keys are documented in [AIS]. Working keys are used to provide integrity of transmitted data and to encrypt certain fields within the application messages. The use of working keys is also described in [AIS].

FUJ00001883

The Acquirer Working Keys used for PIN block encryption are transmitted under the protection of a shared key encryption key, the Zone Master Key (ZMK). The ZMK is exchanged at an agreed interval. This period is normally between six and twelve months. The Acquirer Working Keys, AWKs, for PIN block encryption translation, are changed daily and exchanged under the protection of the ZMK.

The ZMK is exchanged in component form. Three components will be securely printed by the NBX, and sent to nominated key holders in A&L. These ZMK components are entered separately and securely into A&L's key management system and verified.

6.4 Protection

Defensive coding practices should be employed to check for parameters that are out of specified range, fields or records that exceed expected lengths, and unexpected message sequences.

6.5 PIN Encryption

The security requirements with respect to PIN concealment and message confidentiality between NBX and A&L are to follow Banking industry standards. PINS must be translated in hardware and be encrypted at all times, and must not stored in network nodes. Dynamic key management will be adopted, with keys being exchanged at least once every 24 hours.

6.6 Key Changes

Zone Master Key (ZMK) changes will take place every 6 months.

NBX will use the same ZMK for all PI's. A&L will transmit Triple DES (3DES) Acquirer Working Keys (AWK) to NBX systems encrypted under the ZMK.

All encryption keys used between NBX and A&L systems will be double length keys, 32 HEX Characters. The PIN block is encrypted under the AWK 3DES Double Length Key. The whole message (including the encrypted PIN block) is then encrypted at the Network layer whilst traversing the WAN.

NBX may request a new AWK, key change request at their discretion.

6.6.1.1 Acquirer Working Keys (AWK)

These keys apply at the A&L process level, i.e. there will a unique Acquirer Working Key (AWK) for each of the PI's.

6.7 Key Ownership

NBX will own the ZMK to be used between NBX and A&L.

NBX will generate and distribute the 3 ZMK components to A&L in a secure manner.

The 3 components will then be combined and stored in the A&L database encrypted under a Local Master Key (LMK). No person should ever be allowed to see all 3 clear components of the ZMK.

6.8 Line Encryption

Data encryption (using IPSEC tunnels) will be deployed to protect all the production application data being transported over the Wide Area Network circuits in place between NBX and A&L.

FUJ00001883

Cisco router encryption (IPSEC) is used.

The following diagram illustrates the location of IPSEC Tunnel terminations and number of Tunnels. Figure 2 (NBX to A&L Physical interface shows the overall physical context).

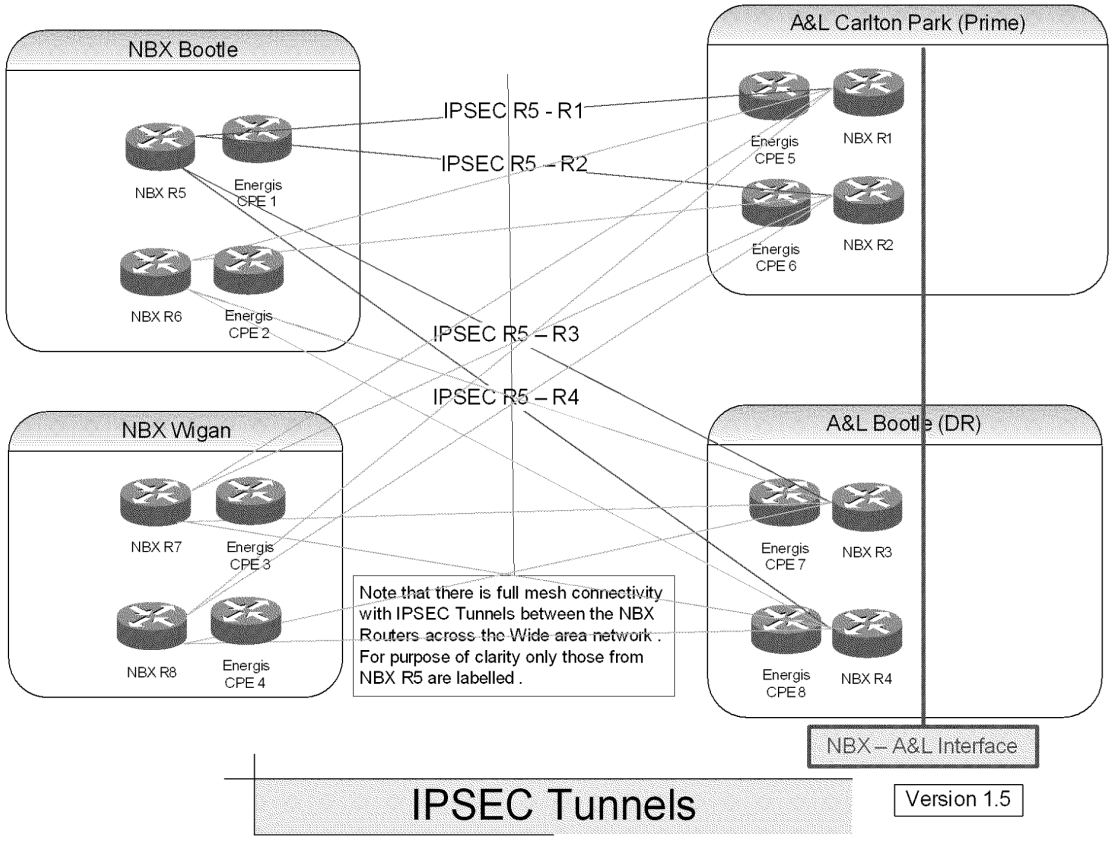

Figure 5 IPSEC Tunnels

Session key exchange is normally once per day. Master key change frequency is specified in [OLA].)

6.9 Firewalls

A&L will provide a firewall cluster on their side of the Interface..

NBX Production systems will also be protected by the use of resilient firewall functionality, which will exist at the NBX boundary facing the external wide area network connections.

NBX Test systems will be protected by the use of firewall functionality.

6.10 Authorised Engineering access to A&L locations

In the event of an NBX equipment failure at one of the A&L locations, POL (through its agent Fujitsu Services) will arrange for an authorised engineer to attend the A&L site to diagnose and repair or replace the equipment.

FUJ00001883

This process is documented in [OLA].

FUJ00001883

7 RECOVERY FACILITIES AND PROCEDURES

7.1 Fault Detection

Dual network management centres will manage the WAN. These centres will monitor the network for abnormal activity at all times. Fault detection is the responsibility of each party in their respective domains.

7.2 Disaster Recovery Environment

NBX does not provide a DR capability, since both Data Centres are active.

A&L will create a DR capability at their contingency location, a replica of the production environment.

In the event of total failure of the primary A&L systems, DR will be invoked and production service restored to NBX.

7.3 Disaster Recovery Testing

The A&L contingency systems will be tested (details are provided in DRTEST]).. Should the entire processing environment be transferred from the production environment to the contingency environment for testing purposes, notice must be provided to NBX at least 30 days in advance. Where the need to perform a scheduled DR test is identified, the process to arrange it will conform to the Business Continuity Interface Document [**Error! Reference source not found.**BC] agreed between PO Ltd & A&L.

7.4 Disaster Recovery Invocation

The decision to invoke the move to the contingency system from production by A&L may be taken by persons in the positions listed in the DR Plan [DRPLAN].

This decision will be taken following an incident of sufficient severity to justify the invocation.

The decision may also be taken as a safeguard measure to reduce the impact of an impending systems or environmental failure.

The steps to be taken and the approximate timings will be contained within the DR Plan [DRPLAN].

7.5 A&L Move to DR Processing

At the technical level, the move by A&L to DR operation. will require NBX to change the IP addresses it targets.

It should be noted that NBX systems are able to issue socket connection requests to the A&L production or DR facility. A&L will provide NBX with both its production and DR IP addresses. These will be used when configuring the NBX firewall and host systems.

The process for A&L invoking DR is documented in [OLA].

FUJ00001883

7.6 NBX Move to DR processing

NBX does not move to DR processing.

FUJ00001883

Appendix A Detailed Configuration

A.1 Production System Addresses and Ports

The following tables define the TCP/IP socket used between NB production system and A&L production system for message exchange.

All IP addresses in this section are from the Peering IP address space.

The Labelling of PI's and NBX Systems is as shown in Figure 3 Application Endpoints.

The Labelling of Routers is as shown in Figure 2 – NBX – A&L Physical Interface.

A&L			
A&L IP	**A&L Port**	**PI name (TIS)**	**NBX PI Name**
155.202.231.7	8881	P	PIa1
155.202.231.7	8882	Q	PIb1
155.202.231.7	8883	R	Pia2
155.202.231.7	8884	S	Pib2

NBX		
Name	**NBX IP**	**NBX Ports**
NBXa Wigan	192.168.1.17	[1024..5000] + ICMP Echo request / response (subject to PO Change Control approval)
NBXb Bootle	192.168.1.1	[1024..5000] + ICMP Echo request / response (subject to PO Change Control approval)
Network Management Server Wigan (for commissioning / fault investigation subject to Change Control approval)	192.168.1.19	ICMP echo request ICMP Echo request / response (subject to PO Change Control approval)

FUJ00001883

Network Management Server Bootle (for commissioning / fault investigation subject to PO Change Control approval)	192.168.1.3	ICMP echo request ICMP Echo request / response (subject to PO Change Control approval)

The following table defines the TCP/IP socket used between NBX production system and A&L production system for file transfer using Connect:Direct.

File Transfer	NBX IP& Port		A&L IP & Port	
NBX ➔ A&L	Bootle: 192.168.1.2 Wigan: 192.168.1.18	TBS	155.202.231.8	TBS

Routers / Firewalls	
NBX R1 Interface	155.202.231.5
NBX R2 Interface	155.202.231.6
NBX R1/R2 HSRP	155.202.231.4
NBX R3 Interface	155.202.241.5
NBX R4 Interface	155.202.241.6
NBX R3/R4 HSRP	155.202.241.4
F1/F2 VIP	155.202.231.1
F3/F4 VIP	155.202.241.1

A.2 DR System Addresses and Ports

The following table defines the TCP/IP socket used by NBX DR system or A&L DR system for message exchange.

A&L		
A&L IP	**A&L Port**	**PI**
155.202.241.13	8881	P
155.202.241.13	8882	Q
155.202.241.13	8883	R

FUJ00001883

155.202.241.13	8884	S

The following table defines the TCP/IP socket used by A&L DR system for file transfer using Connect:Direct.

File Transfer	NBX IP& Port		A&L IP & Port	
NBX➔ A&L	Bootle: (IP and Port are same as production) Wigan: (IP and port are same as production)		155.202.241.14	tbs

A.3 Test System Addresses and Ports

The following table defines the TCP/IP sockets used between NBX test system and A&L test system for message exchange.

NBX Test		
Name	**NBX IP**	**NBX Ports**
NBXa Feltham	192.168.1.33	[1025..5000]
NBXb Feltham	192.168.1.34	[1025..5000]

A&L		
A&L IP	**A&L Port**	**PI**
155.202.241.7	8881	P
155.202.241.7	8882	Q
155.202.241.7	8883	R
155.202.241.7	8884	S

The following table defines the TCP/IP socket used between NBX test system and A&L test system for file transfer using Connect:Direct.

File Transfer	NBX IP& Port		A&L IP & Port	
NBE ➔ A&L	192.168.1.35	tbs	155.202.241.8	tbs

FUJ00001883

A.4 Connect Direct details

NBX	
Test User Id	Tbs
Production user Id	Tbs

A&L	
Node Names (this is "SNode" Parameter in C:D) - Same Node ID is used for prod & test	Tbs

FUJ00001883

Appendix B – Testing

The following diagram illustrates the Testing Environment based on use of ISDN2e. The Test IP address assignments are documented in Appendix A.

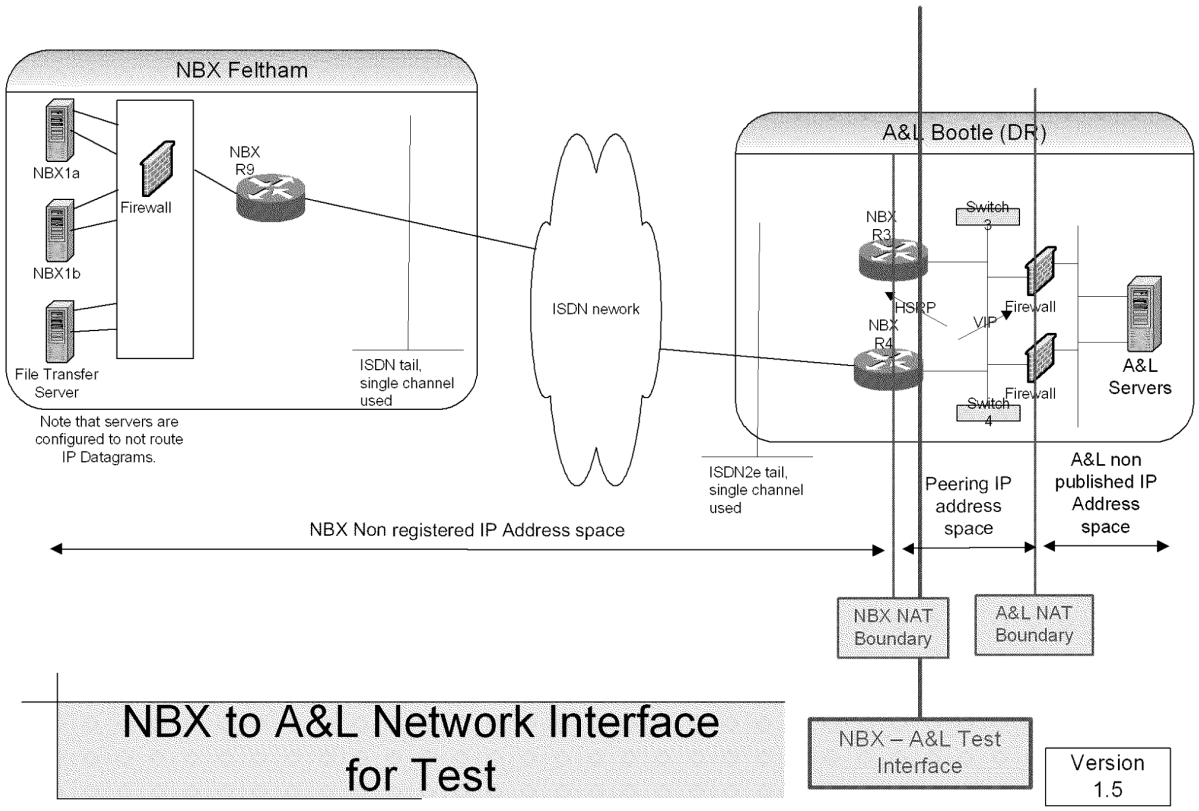

Figure 6 Test Network Interface

Note that NBX Routers R3 and R4 are used for either test application traffic or live application traffic but not both traffic types concurrently. In addition the IP addresses spaces used for Peering in the live and test environments have no “overlap” and therefore can be used concurrently on the NBX R3 and R4 Routers.

Also note that there are no IPSEC tunnels between the NBX test location and the A&L Bootle site,

The test line (ISDN2e) is for test traffic use only. As A&L provide the cards used for testing A&L retain control of the data passed across the interface. As A&L will only ever provide test cards for testing purposes, POL can confirm that no live customer data or passwords will pass through this line.