FUJ00001890

EMV – Banking and Retail

NBX - LINK Technical Interface Specification (TIS)

Changes in version 0.6 like this

Changes in version 0.7 like this

Changes in version 0.8 like this

Changes in version 0.9 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		
LINK Sign-off	Phil Hanson			
Fujitsu Services Sign-off	Tony Drahota	**RASD Director**		
DA Sign-off (Peer Reviewer)	David Gray	**Design Authority**		
Programme Director	Beverley Dunn	**Project Delivery**		

FUJ00001890

1 Document Control

1.1 Document Information

Horizon Release No:	S75
Document Title:	EMV Banking and Retail: NBX – LINK Technical Interface Specification
Document Type:	Technical Interface Specification
Abstract:	This document defines the technical interface between the Horizon domain and LINK
Document Status:	Approved
Originator & Department:	David Gray Design Authority
Contributors:	
Post Office Distribution:	Design Authority – David Gray POST OFFICE LTD. Document Control – Post Office Programme Office
Supplier Distribution:	LINK: Phil Hanson 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 Nov 2003	First working draft. Based on document produced by IBM entitled "LINK / Post Office Limited Connection: Schedule 2 – Technical Design Specification" (Version 1.4)	
0.2	1st Feb 2004	Second working draft based on discussion / decisions reached at workshop between LINK, Post Office Ltd. and Fujitsu services on Jan 22nd 2004	
0.3	17th Feb 2004	Third working draft updated during workshop between LINK, Post Office Ltd. and Fujitsu Services on 5th Feb 2004. Additional changes made following workshop.	
0.4	2nd March 2004	Fourth working draft updated during workshop between LINK, Post Office Ltd. and Fujitsu services on 19th Feb 2004. Further changes made following workshop	

© Post Office™ 2003

FUJ00001890

0.5	16th March 2004	Accepted all changes in version 0.4 and earlier in order to make the document easier to read and maintain. Minor changes requested by Link	
0.6	16th May 2004	Change in Wide Area Network Design with LINK providing circuit for Inter Campus traffic between Bootle and Wigan.	
0.7	13th July 2004	Major update on specification of TCP level application behaviour This version is a candidate for sign off subject to remaining Drafting notes, identified by "DN:" being removed.	
0.8	9th August 2004		
0.9	3rd September 2004	Version for signoff containing minor updates	
1.0	7th September 2004	Version for signoff	

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

© Post Office™ 2003-2004

FUJ00001890

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
LINK	Chas Wilcockson
Optional Review / Issued for Information	
Post Office Ltd	Bob Booth, Paul Warbrick, Jason Crellin
LINK	Ian Murphy
Fujitsu Services	Mark Jarosz

1.5 Changes in this Version

Version	Changes
1.0	1. IP addresses and ports documented in Appendix A 2. Updated Figure 2: Post Office Ltd. to LINK Communications Infrastructure 3. Table summarising routing information exchanges across the interface has been added in section 6.4.9.

Table 3: Changes in this Version

1.6 Changes expected

Number	Change
1	Completion of IP address and Port information in Appendix A

© Post Office™ 2003-2004

FUJ00001890

2	Completion of missing document references in 1.8
3	Removal of "DNs"

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 - LINK Application Interface Specification	PVCS
2.	OSI			OSI/ISO Reference Model	ISO
3.	RFC1918			RFC 1818 Address Allocation for Private Internets	www.faqs.org/rfcs/rfc1918.html
4.	SLA			LINK / Post Office Ltd. Service Level Agreement (Schedule 6a)	Tbs
5.	OLA			Operational level agreement between Fujitsu, Post Office Ltd. and LINK	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.

© Post Office™ 2003-2004

FUJ00001890

Table of Contents

© Post Office™ 2003-2004

FUJ00001890

© Post Office™ 2003-2004

FUJ00001890

List of Tables

List of Figures

© Post Office™ 2003-2004

FUJ00001890

2 Introduction

2.1 Purpose

The objective of this document is to describe the technical features of the LINK to Post Office Ltd. connection in sufficient detail to enable the system to be implemented. It should be viewed as the base technical specification against which any project change control should be assessed.

2.2 Scope

This TIS describes the interface for exchange of information between the NBX and LINK 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 LINK 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].

This documents includes a specification of the TARDIS service (see section 4.6). Whilst not directly concerned with this interface, this section is retained in this document for historic reasons.

2.3 Structure

The following table summarises the structure of this document.

Section	Overview
2.5	Identifies Data Centre locations and summarises the application flows across the interface.
2.6	Summarise outstanding Design questions
2.6	Provides an Overview of the Online Interface.
4	Provides an overview of the Batch Interface
5	Specifies Security across the interface.

© Post Office™ 2003-2004

FUJ00001890

6	Specifies Communication (Physical, Link, Network, and Transport) across the interface.
7	Specifies application level properties across the interface.
8	Documents Disaster recovery invocation for the interface.
9	Documents identifiers associated with the Interface.
Appendix A	Documents configuration information, such as IP addresses and ports used across the interface.
Appendix B	Specifies provision for Testing

2.4 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
BBA	Basic Bank Account
DES	Data Encryption Standard
DR	Disaster Recovery
FI	Financial Institution
HDLC	High-level Data Link Control
HSRP	Cisco Hot Standby Router Protocol
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 {QoS / Separation tool used in WAN}
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.
OSI	Open Systems Interconnection
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
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP MSS	The TCP maximum segment size is the maximum number of TCP bytes that can be carried in a single IP datagram.
TIS	Technical Interface Specification
VIP	Virtual IP Address
VPN	Virtual Private Network
WAN	Wide Area Network
ZMK	Zone Master Key

© Post Office™ 2003-2004

FUJ00001890

2.5 Interface Context

The following diagram provides an overview of the Interface location, the application level flows across the interface and the roles of NBX and LINK data centres.

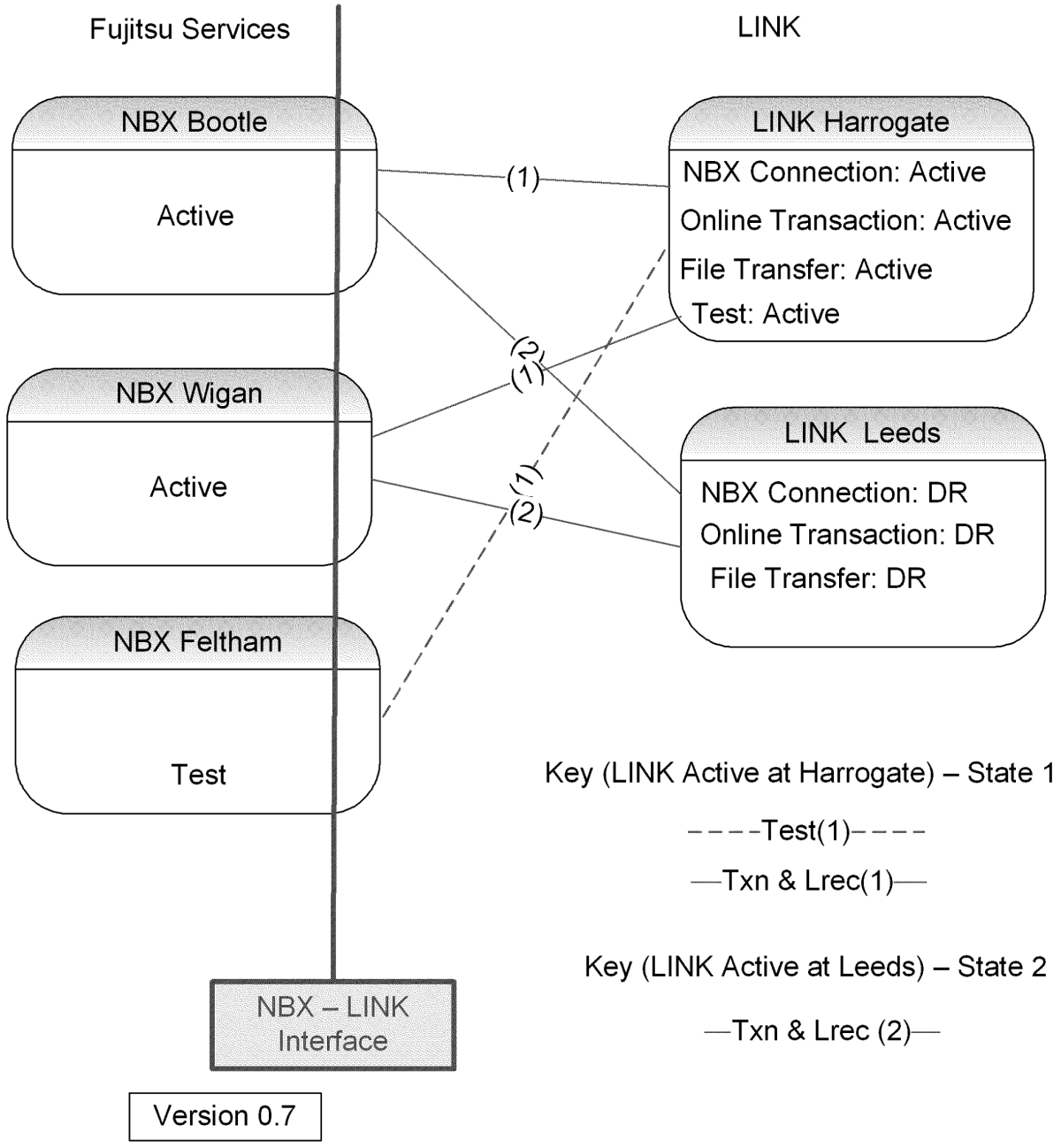


Figure 1 Interface Context

2.6 Outstanding Design questions

There are no outstanding Design questions.

© Post Office™ 2003-2004

FUJ00001890

3 Online Interface Overview

3.1 Supported Message Set

Please refer to [AIS] for details of online messages supported across the interface.

3.2 Transacting day

NBX will be able to acquire transactions and forward to LINK for routing on a 24 x 7 basis. Planned maintenance or DR testing does not count towards service level calculation.

NBX will have a reserved daily maintenance slot, at a time and duration specified in the [OLA].

Full details of the service levels to be met by LINK and Post Office Ltd are defined in the LINK / Post Office Ltd Service Level Agreement [SLA]..

© Post Office™ 2003-2004

FUJ00001890

4 Settlement and Reconciliation Processing

4.1 Settlement

Settlement will follow LINK's normal standards. The LINK business day runs from 20:00 hrs to 20:00 hrs seven days a week with net settlement effected between LINK and Post Office Ltd. on the following banking business day (England).

4.2 Business day

Each transaction request response message will contain the field (015) Date, Settlement. The content of this field indicates which settlement day the LINK system considers that individual transaction to be in. Post Office Ltd. use this field to reconcile the LINK LREC report to their own transaction logs.

0800 network management, end of day messages will be exchanged when the LINK system cuts from one business day to the next.

4.3 Central Settlement

Settlement is based on LINK produced net settlement figures showing the amount owing/due between Post Office Ltd. and LINK central settlement.

Settlement will take place each English banking day although there will be a separate settlement figure produced for each LINK business day.

Settlement will be between specially designated accounts at the Bank of England.

4.4 Reconciliation

Reconciliation of the Post Office Ltd./LINK settlement positions will be the responsibility of NBX, using a data file (LREC) of transactions supplied by LINK.

4.5 Reconciliation File Transfer

The LREC file will be transferred from the LINK Tandem system to the NBX system using Connect: Direct file transfer software from Sterling Commerce, over a TCP/IP socket connection.

The version of Connect: Direct used by LINK and NBX is specified in [OLA].

The Connect: Direct file transfer will be made between the LINK Production data centre and an NBX Production data centre.

LINK creates the file, and to comply with their usual operating procedure, they will initiate sending the file. This also means that they will initiate the TCP connection.

NBX will provide 2 IP addresses for LINK to use for Connect: Direct, - Primary IP address and Secondary IP address.

LINK will use these two IP addresses in the following manner:

- Attempt transfer to Primary IP address, if okay then done
- Else try Secondary IP address (subject to [OLA] procedure)

The following table provides further details on how LINK used these IP address endpoints for File Transfer.

© Post Office™ 2003-2004

FUJ00001890

Condition	Overview
TCP Connection failure retry	A number of TCP connection attempts (at least 3), separated by at least 2 minutes will be attempted. This is to allow for any network convergence within and across IP Routing protocols.
Failure during transfer	Should a failure occur during file transfer, at least one retry will be attempted.
Switch from Primary IP address	In the event that a TCP connection cannot be established to the Primary IP address or the File transfer does not succeed (having been retried as stated above) on the Primary IP address, LINK will follow the procedure defined in [OLA]. This may result in switching to the Secondary IP address and repeating the transfer attempt.

The following table summarises properties for the file transfer

Property	Details
Authentication details	Username / password obtained as specified in [OLA].
Filename	NBXP.XFER.LINK.LRECddmmyyyy (note in test, NBXP is replaced with NBXT)
Directory	NBXP (note in test, NBXP is replaced with NBXT)

Note that unlike the Transactional application interface, NBX does not provide a virtual IP address for the Service.

When DR is invoked, LINK will send the LREC file using Connect: Direct from its contingency site.

A CD-Rom (ISO 9960, Mode 2/XA, Single Session) will provide the standby in the event of a prolonged Connect:Direct file transfer failure. The CD-Rom will be sent to the NBX representative nominated in [OLA]. The Directory name will be NBXP and the file name will be the same as production but with the full stops "." replaced by underscores (_) in order to comply with the ISO 9960 file name format.

(DN: Need to state how capacity of this CD will be managed, is the following okay?
LINK will capacity manage the size of the LREC file and propose an alternative scheme (compression or media) when the LREC file is predicted to no longer fit on the CD-Rom.)

Refer to [OLA] for further details including the delivery schedule for the LREC file.,

4.6 TARDIS

(DN: Chas to review and provide replacement if necessary)
TARDIS is LINK's transaction history database. TARDIS holds online the LINK view of every transaction that has passed across the LINK switch in the past 12 months. Historical data will be maintained for 7 years and is accessible by special request. Transaction details are applied to the TARDIS system by 09:00hrs on the LINK business day after the LINK Business day on which they were performed.

The transaction details in TARDIS provide LINK customer' settlement departments with the LINK transaction view. This view is provided to aid in settlement disputes or customer queries.

Access to TARDIS is achieved using standard windows Dial Up Networking services and standard web browser technology. TARDIS is available to LINK customers between 09:00 and 17:00 each English banking day.

© Post Office™ 2003-2004

FUJ00001890

Post Office Ltd. access TARDIS to enquire on any transactions acquired at its counter positions. Post Office Ltd. are provided with dial-up access via a shared, dual paired, Cisco 2509 routers to the TARDIS system. This arrangement will be mirrored at the LINK DR facility.

Post Office Ltd. operate a Single concurrent connection license to the TARDIS system.

© Post Office™ 2003-2004

FUJ00001890

5 Security Requirements

5.1 PIN Encryption

The security requirements with respect to PIN concealment and message confidentiality between LINK and Post Office Ltd. are as specified in the LIS5 Security standard. Dynamic Key Management will be adopted, with keys being exchanged and verified at least once every 24 hours.

5.2 PIN Block Format

The PIN information is held in a 16-digit HEX string PIN block.

RACAL/ZAXUS Format 01 is used within the LINK network. This is the format adopted by the American National Standards Institute (ANSI X9.8) and is one also known by the International Standards Organisation (ISO 95641 – format 0).

This format combines the customer PIN and account number as follows:

- A 16-digit block is made from the digit 0, the length of the PIN, the PIN and a pad character (hexadecimal F).
- Another 16-digit block is made from four zeroes and the 12 right most digits of the account number, excluding the check digit.

The 2 blocks are then exclusive-OR added giving the final PIN block, which is then encrypted.

5.3 Key Changes

Acquirer Zone Master Key (AZMK) changes will take place every 6 months. Such a change requires a service outage during a planned maintenance slot, refer to [OLA] for further details.

NBX will use the same AZMK for all Agent PIs. LINK will transmit Triple DES (3DES) Acquirer Working Keys (AWK) to NBX systems encrypted under the AZMK.

All encryption keys used between LINK and NBX systems will be double length keys, 32 HEX Characters. The PIN block is encrypted using triple DES (3DES) encrypt-decrypt-encrypt (EDE2) techniques.

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

Acquirer Working Keys (AWK)
These Keys apply at the Agent / Processor Interface (PI) level, i.e. there will a unique Acquirer Working Key (AWK) for each PI. NBX will need to use the correct current AWK for the PI that they will send the acquired transaction to.

5.4 Key Ownership

NBX will own the AZMK to be used between LINK and NBX.

NBX will generate and distribute the 3 AZMK components to LINK in a secure manner as described in the LIS5 Security Standard document.

© Post Office™ 2003-2004

FUJ00001890

The 3 components will then be combined and stored in the LINK Advantage database encrypted under the LINK Local Master Key (LMK)

No person will ever be allowed to see all 3 clear components of the AZMK.

5.5 Line Encryption

LINK will provide Line Encryption Units (LEU's) to protect the data being transported over the Wide Area Network circuits in place between NBX and LINK.

These LEU's are Thales DC2K bulk encryptor – 3DES level.

The Session key lifetime is *(DN: TBS by LINK)*

The Key change frequency is annually, subject to compromise.

*On site access is required for LINK authorised Engineers. This is covered in [*OLA*].*

Two units will implemented at each LINK datacentre (one per Leased Line) and 2 units will be implemented at each NBX datacentre..

Each WAN Circuit will be protected by a pair of LEU's.

Where ISDN is used, as in test, no bulk encryption over the ISDN circuit will be applied.

All management and monitoring of the line encryption units is the responsibility of LINK.

5.6 Firewalls

LINK will install a firewall security system in front of each of the Ethernet ports on the LINK mainframe.

NBX will install a firewall security system between the NBX servers and the LINK Routers.

The use of firewalls to protect NBX systems are highly recommended by LINK, but will remain the responsibility of NBX.

For further details regarding firewalls refer to section 6 of this document.

5.7 LINK Authorised Engineering access to Post Office Ltd. locations

Refer to [OLA] for further details.

© Post Office™ 2003-2004

FUJ00001890

6 Communications Requirements

6.1 Background

LINK will operate 2 systems, one production and one contingency. Only one LINK site will be running the production service at any time.

There is no requirement for NBX to provide a contingency capability, since both Data Centres are active.

6.2 Design Principals

LINK adheres to key principles of system design that are applied to all connections and ongoing application configuration.

LINK systems are built around the principle that no single failure will affect the service offered to customers.

6.2.1 Physical Communications:

LINK will provide a Leased line circuit to each NBX data centre at Wigan and Bootle and a Leased Line circuit between Wigan and Bootle. The Test Connection from Feltham to LINK will be achieved via ISDN dialup owned and maintained by Post Office Ltd..

Following a failure of a component on one physical line, remaining leased line circuits will be capable of handling peak transaction volume on its own.

Each physical communication line entering LINK and customer datacentres is routed via a different Telco exchange enters the building at a different point and approaches the building from a different direction subject to confirmation by Telco provider.

6.2.2 Tandem Hardware

LINK selected the Tandem hardware due to its fault tolerant features and functionality.

All hard disk drives are mirrored

There are 2 I/O paths to each hard disk drive or I/O device on the system.

6.2.3 Logical Application Configuration

The Advantage PROCCTL process runs as a non-stop process pair, spread across 2 CPU's on the LINK Tandem.

Each LINK site will run 4 PI's, and full customer transaction volume is sustainable with up to two PI's down.

All PI's can be dynamically routed across the network.

6.3 Communications Infrastructure

The connection will use the TCP/IP communications protocol. An overview of the communications infrastructure provided by LINK is given in Figure 2: Post Office Ltd. to LINK Communications Infrastructure below. The physical interface between LINK and Post Office Ltd. will be achieved using BT Leased Lines and Cisco Routers, which will be owned and managed by LINK.

© Post Office™ 2003-2004

FUJ00001890

POL NETWORK DIAGRAM

Created by:- C Wilcockson
Last Updated by:- C Wilcockson
Date of last Update:- 16/04/2004
NB Not accurate in printed form

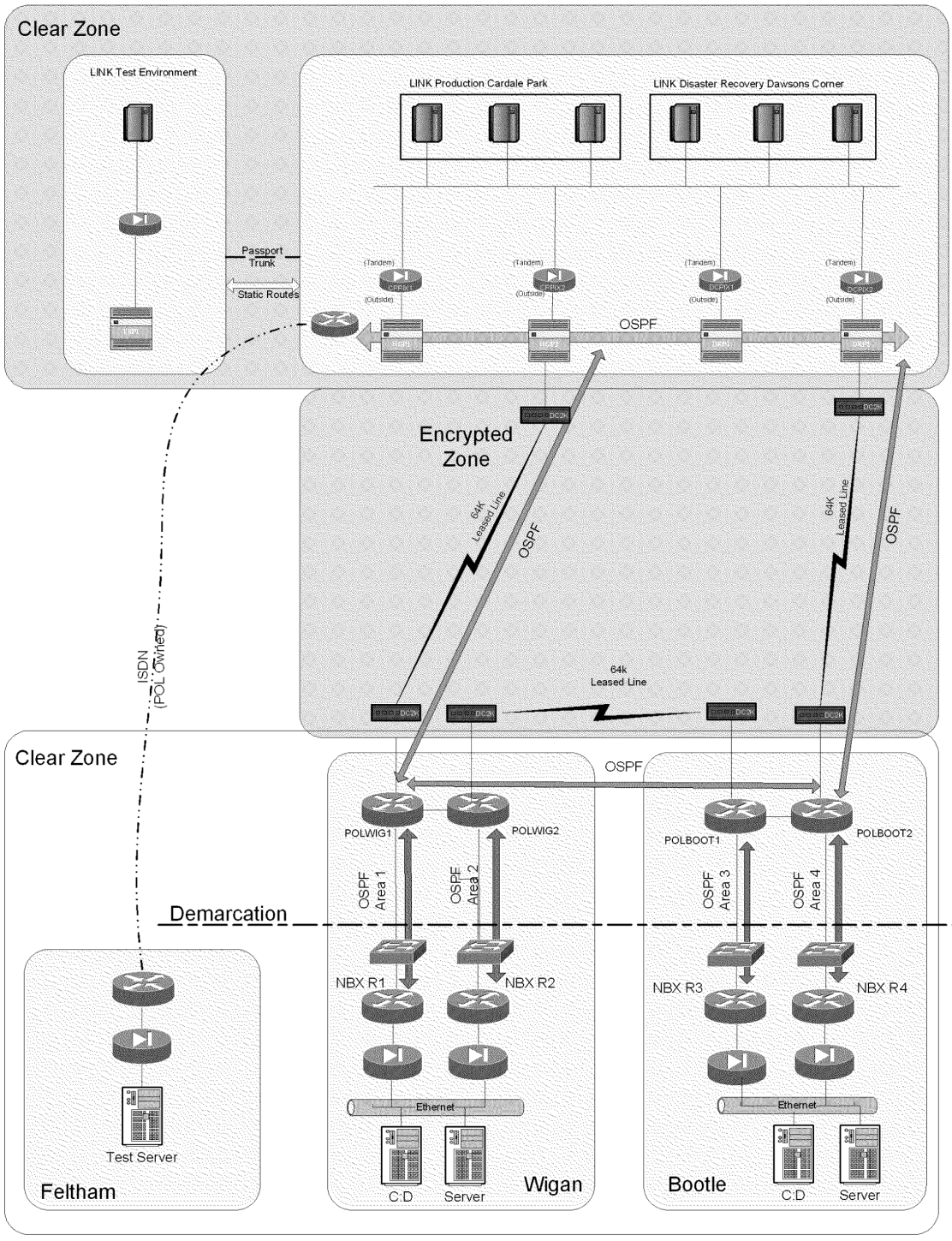


Figure 2: Post Office Ltd. to LINK Communications Infrastructure

© Post Office™ 2003-2004

FUJ00001890

6.4 Physical Connections

6.4.1 Physical Connections for Production and Test

As illustrated in, Figure 2, one Kilostream circuit from LINK, will terminate at each NBX Datacentre. An additional Kilostream will be provided between Wigan and Bootle for Resilience purposes.
LINK will manage the bandwidth requirements of the LINK managed circuits.

LINK will ensure the onward routing of the connection between its production and contingency (DR) sites.

Both of the physical NBX locations will operate a production service at any one time. Testing will be supported from a separate location (Feltham).

The Network has been designed with no single points of failure (refer to Figure 2: Post Office Ltd. to LINK Communications Infrastructure and Figure 3 Connection endpoints for further details).

LINK will, at a time and frequency defined in [OLA], provide (initiate) additional TCP/IP socket connections to facilitate the Connect:Direct transfer of the LREC file.

Further connections for testing will be required – refer to Section Appendix B.

6.4.2 Data and Systems Security

LINK will implement a “firewall” including intrusion detection systems to ensure the security of LINK’s own systems and network.

NBX are responsible for ensuring the security and integrity of transactions whilst within their networks and systems.
LINK requires connection to either;

- A dedicated Router Interface
- Firewall Interface (or Router running Firewall software)
- Access through a private VLAN (i.e. only LINK device plus 1 NBX device on this VLAN)

NBX will provide a dedicated Router Interface per LINK Router at each Data Centre (configured as 100 Mbps, Full Duplex)..

6.4.3 TCP Connection Management

At the TCP/IP communications level, connection establishment and re-establishment will be managed from the LINK end of the interface for all TCP/IP socket connections.

The following table summarises the main properties of TCP Connection Management and TCP Connection maintenance.

© Post Office™ 2003-2004

FUJ00001890

Property	Overview
Connection Initiation	LINK initiates TCP Connections, NBX acts as a TCP server. LINK initiates TCP Connections under the following conditions; 1. Manually by LINK Operations 2. Automatically in certain error scenarios. Please refer to 6.4.4 for further details.
Number of Connections	LINK supports more than one TCP connection per PI but note that Key changes and Logons are per PI. Note that the TIS document specifies one active* TCP connection between each LINK PI and the NBX Application. * Since LINK initiates TCP connections there may be occasions when LINK has TCP connection state indicating a TCP connection whilst NBX has no TCP connection (stale connection). This condition will persist until either TCP KEEP Alives initiated by LINK terminate the TCP connection or the TCP application traffic from LINK results in the TCP connection being aborted.
Connection Maintenance	When a TCP Connection is terminated in a Graceful* manner then LINK will not attempt to automatically establish another similar connection (same NBX destination port). *Note the term Graceful is defined in the section 6.4.4.3.
Ports	LINK use dynamic ports in range [1024..64*1024-1], NBX is listening on one distinct port per LINK PI
Data retransmission	Both NBX and LINK implement standard TCP behaviour with respect to exponential back off and retransmission.

© Post Office™ 2003-2004

FUJ00001890

Keep Alive behaviour	TCP Keep Alive Behaviour The following 3 parameters are defined in order to explain the behaviour of the TCP Keep Alive process: Keep Alive Idle • Seconds between each TCP keep alive segment if no data has been sent on the connection. Keep Alive Retransmit Interval • Seconds between successive retransmissions of the keep alive segment when a response to an initial keep alive is not received. Keep Alive Retry Count • After sending (Keep Alive Retry Count) retransmissions the connection is abandoned. For LINK the following values apply: • Keep Alive Idle = 45 seconds • Keep Alive Retransmit Interval = 45 seconds • Keep Alive Retry Count = 8 For NBX the following values apply: • Keep Alive Idle = 30 seconds • Keep Alive Retransmit Interval = 30 seconds • Keep Alive Retry Count = 5
Multiple connections	Since there is one TCP/IP connection per PI, an NBX Agent has to handle the case when a LINK PI attempts to open a connection and the NBX Agent already has an existing connection from that PI. In this case the NBX Agent will accept the new connection and will abort the existing connection. This approach means that if LINK and the NBX Agent have different views as to whether the original connection actually exists – then those views will be brought back into alignment. It also covers the case where a LINK operator opens a new connection to overcome a stale connection without first aborting the stale one.

Table 6 TCP Connection Management

6.4.4 TCP Failure scenarios

This section provides an overview of the mechanisms used by the LINK TCP Client (named Advantage) to establish TCP connections after various failure conditions result in current TCP connections having closed through Abort or Timeout. These terms are defined in section 6.4.4.3).

6.4.4.1 NBX TCP/IP layer still active but server application is not

This is the scenario where the NBX Agent has failed or aborted the TCP connection resulting in a "TCP reset". For example this would occur during a controlled NBX failover (no platform

© Post Office™ 2003-2004

FUJ00001890

failure) and no network failure. In this case the TCP layer on NBX will realise that the NBX server application is not up and respond to the LINK data packet* with a TCP Reset. This will cause the TCP layer on the Tandem to report an ECONRESET error up to the client application (Advantage). Advantage will deal with this by closing and reopening the socket. If the socket request is not successful (because the server application is not up yet) the TCP layer will report an ECONREFUSED error up to Advantage. This will cause Advantage to close and reopen the socket again. This will keep happening until a configurable number of attempts has been reached (which can be set to infinite) or the socket connects successfully. (*DN: Sufficient attempts will be configured to ensure that retries continue for at least 2 minutes*).

* Note since Link send application heartbeats every 30 seconds it is the case that at least every 30 seconds the TCP stack on Tandem will send data.

6.4.4.2 NBX TCP/IP layer is not active

This can either happen because the NBX server has failed or because the network path from LINK to the NBX server has failed.
When LINK send data and get no response, the TCP layer on the tandem will resend the data at 8, 16, 32 then 64 seconds. However this is immaterial, since after 50 seconds Advantage will time out the socket, close and then reopen the socket. This will cause SYNs to be sent to NBX, which will be repeated at 3,6,12 and 24 seconds (This is hard coded within the Tandem TCP stack). If NBX does not respond to any of these SYNs then LINK will close the socket and operator intervention will be necessary to re-establish communications.

In summary in the case where communication between LINK and NBX is lost completely, there is at 95 seconds [50 + (3+6+12+24)] within which to get the TCP/IP layer back (for example a TCP reset from an NBX platform). Provided this happens within this time** then the situation described in the previous scenario (6.4.4.1) is in effect where Advantage gets an ECONREFUSED back and can keep trying as long as necessary (more or less). If TCP/IP recovery takes longer than 95 seconds then the line will close and require operator intervention.

** Note the above assumes that LINK tried to send data as soon as communications we lost, this is worst case and in practice the time is likely to be longer. Also after sending the last SYN a few seconds will be allowed for the response. This means that the actual value will be greater than 95 seconds + SYN timeout value.

6.4.4.3 Closing TCP Connections

This section documents a classification scheme for all possible ways in which an established TCP connection can be terminated.

Termination Type	Subtype / Overview
Graceful	This represents the mutually agreed closure case. Both TCP peers exchange FIN segments that are acknowledged explicitly.
Abort	Abort initiator The TCP peer forces the connection to be closed by sending a TCP reset. Note that the peer causing the TCP reset could be the platform TCP/IP stack if the application has disappeared. Abort Observer The TCP Peer receives a TCP reset and the connection is

© Post Office™ 2003-2004

FUJ00001890

	aborted.
Timeout (Silent fail)	A TCP peer observes no response at all from the other TCP peer. This is typically the result of a network path failure between the platforms. The TCP peer eventually times out* the connections and send a TCP reset. In general the other peer will not receive this TCP reset. * Either though data transmission or TCP Keep Alives

Table 7 TCP Connection closures

6.4.5 Description of TCP Connections

LINK will configure four LIS5 Processor Interfaces (PI's) and associated TCP/IP Communications Handlers (CH's) on each of their Production and Contingency (DR) Advantage applications (refer to Figure 2: Post Office Ltd. to LINK Communications Infrastructure)..

Each PI will operate a TCP/IP connection; this gives a total of 4 active sessions for production transactions. Each PI process will use its socket connections for production transactions so long as they are available.
The NBX will load balance (as specified in 6.4.6) Post Office Ltd. acquired transactions. The objective being to ensure an approximately even load balance on the LINK PI's, CH's, Ethernet ports and firewalls.

The above environment will be replicated in the Disaster Recovery, Test, Development and Certification application environments at LINK. When testing connections are required additional TCP/IP socket connections will be made to the TCP/IP addresses and ports nominated by Post Office Ltd. for their test systems.

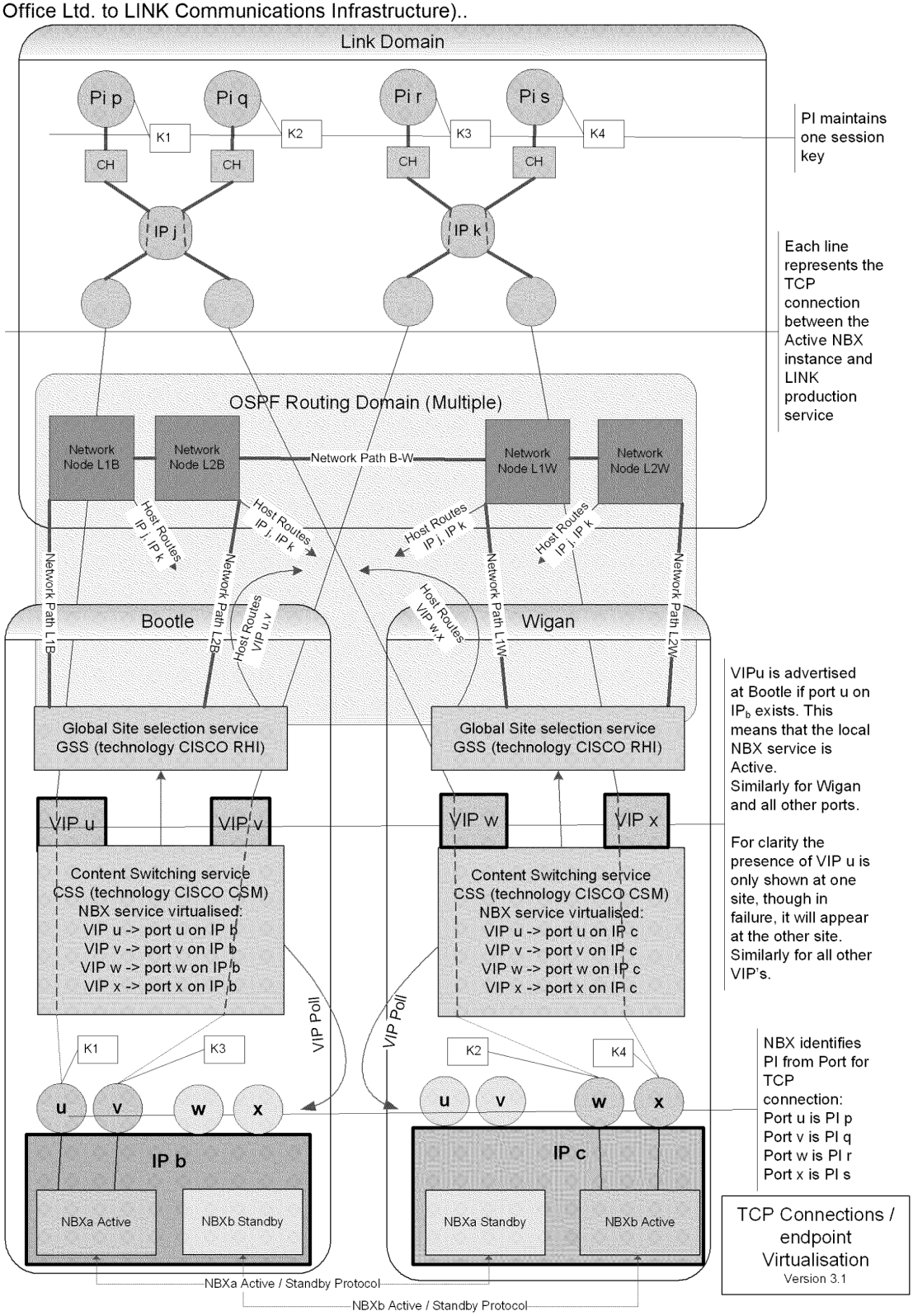
The Connect:Direct and additional testing sockets will be established over the existing communications infrastructure.

The Following diagram illustrates the TCP Endpoints for the online application interface. The Connect: Direct application interface uses the same infrastructure as shown in (Figure 2: Post

© Post Office™ 2003-2004

FUJ00001890

Office Ltd. to LINK Communications Infrastructure)..



© Post Office™ 2003-2004

FUJ00001890

Figure 3 Connection endpoints

Note that the default configuration of the NBXa and NBXb agents is for them to be active at alternative data centres.

6.4.6 Load Balancing

As the transaction acquirer NBX are responsible for the balancing of transaction volumes across the PI's and the established TCP/IP sockets.

The objectives of this load balancing are twofold:

- To ensure that the LINK PI processes are balanced in terms of transaction volumes and hence CPU utilisation on the LINK switch.
- To ensure that the TCP/IP processes and Firewalls are balanced in terms of transaction volumes.

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

Each NBX instance will use round robin selection across usable* TCP Connection for each transaction to be sent to LINK. The Round Robin will alternate transactions between PI's. Having chosen a PI the Round Robin will also alternate between the usable TCP connections for that PI.

* The NBX instance will consider a 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 defined threshold (as set in configuration parameters).

The population of Post Office Branches is partitioned across the two NBX instances (NBXa and NBXb) in an approximately even split. Within each partition, all transactions originating at Post Offices will be handled by the NBX instance associated with that partition).

6.4.7 Network Address Translation

There are three separate IP Address domains:

- NBX Non Registered and Non Published
- Non Registered and Published Peering address space
- LINK Non Published

The Boundary between the NBX Non Registered domain and the LINK Published occurs within the NBX Router / Firewall facing LINK. (Refer to Figure 2)

The NAT Boundary represents the location within the Network that Network address translation is implemented. (Refer to Figure 2)

The Peering IP address space is based on RFC1918 [RFC1918]. LINK & NBX jointly agree the Peering address space and this will be documented in the TIS.

© Post Office™ 2003-2004

FUJ00001890

6.4.8 IP Addressing

NBX (online) acts as a TCP server and its IP address is virtualised to provide transparent (from an IP addressing perspective) resilience to platform failure.

No address virtualisation is used for the Connect: Direct File Transfer Server within the NBX domain.

6.4.9 IP Routing

The OSPF routing protocol will be used across the interface. The routers installed by LINK at both Wigan and Bootle will each have two OSPF processes. One process will exchange routing information specific to the NBX host platforms to and from the Fujitsu campus network. The second OSPF process will manage the onward routing into the LINK infrastructure.

NBX will advertise HOST Routes for the four Virtual IP addresses and the two subnet IP addresses for the File Transfer server. These Routes will only be advertised form the NBX Data centre where the platform / service are active. Specifically NBX will not advertise the availability of hosts / service which would require incoming traffic from LINK to be routed Cross Campus.

Direction	Routes	Meaning
NBX to LINK	192.168.26.0 / 24	Subnet at Bootle for File Transfer server. Only advertised from Bootle NBX Routers
NBX to LINK	192.168.25.0 / 24	Subnet at Wigan for File Transfer server. Only advertised from Wigan NBX Routers
NBX to LINK	192.168.24.1	VIP u, advertised from either Wigan or Bootle but not both
NBX to LINK	192.168.24.2	VIP v, advertised from either Wigan or Bootle but not both
NBX to LINK	192.168.24.3	VIP w, advertised from either Wigan or Bootle but not both
NBX to LINK	192.168.24.4	VIP x, advertised from either Wigan or Bootle but not both
LINK to NBX	192.168.17.0 / 24	LINK subnet for PI's, advertised from all LINK Routers
LINK to NBX	192.168.18.0 / 24	LINK subnet for File Transfer client, advertised from all LINK Routers

LINK will advertise Host Routes / subnets for its source IP associated with all TCP/IP connections. Note that the Routing protocol will operate on IP addresses in the peering space – that is the LINK Published IP address space.

In non failure scenarios, IP Traffic between LINK and NBX will use the Network path to the NBX Data centre containing the Active NBX
If a single Network Path between Link and an NBX data centre containing the Active NBX fails then IP traffic will flow using the alternative Network Path (between Link / NBX data centre) and across the Network Path between the NBX Data Centres.

6.4.10 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 a TCP socket.

© Post Office™ 2003-2004

FUJ00001890

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

6.1.11 Message Exchange Patterns

This section summarises properties of the Application message exchange which have direct bearing on the TCP endpoints.

6.1.1.1 Response from LINK

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

6.1.1.2 Response from NBX

NBX will deliver the response message to LINK using the same TCP/IP Connection and hence PI as the original request came to NBX on.

6.1.1.3 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 (as defined in 6.4.6) TCP connection to the PI, NBX will hold the Reversal 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 LINK 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 following section.

6.1.1.4 PI identification

NBX identifies the PI from the Port on which it accepted the incoming TCP connection.
Based on the notation convention used in this document:

- NBX Port u, ↔ PI p
- NBX Port v ↔ PI q
- NBX Port w ↔ PI r
- NBX Port x ↔ PI s

© Post Office™ 2003-2004

FUJ00001890

7 Online Interface Detail

7.1 Overview

The interface between LINK and Post Office Ltd. will conform to the LIS5 standard (refer to AIS for further details of this standard,message types and message flows).

LINK will initially operate 4 LIS5 Processor Interfaces (PI's) on their Advantage switch for Post Office Ltd. acquired transactions in their Production environment. The same number of PI's will be configured in the DR environment.

7.2 Logical Connections

7.2.1 Application Level Communications

Application level communications handling (i.e. sign-on, sign-off and echo testing) will be handled using 0800/0810 network management messages, as specified in the LIS5 standard

7.2.2 Application Level Handshakes

"Handshaking" (echo testing) will be implemented, with a maximum interval of 3 minutes between exchanges of 0800 echo test messages. These handshakes will be initiated by both LINK and NBX based on their own timers. These timers in the NBX and LINK domains are not synchronised.

The purpose of Application Handshakes is to detect and alert failures in Application to Application communications when no Transactions are flowing. For example overnight the interval between transactions may be hours. Rather than wait for transactions after such a quite period to detect problems and alert, Application Handshakes may be used to detect this sooner. Note that any problems with the underlying TCP connection will be made visible to the application by using that TCP connection for Application traffic. The following table summarises the main properties of Application Level Handshakes.

Property	Overview

Interaction with "Logged on" state	If the LINK PI is not "Logged on" then
	• It will not send Handshakes
	• It will respond to Handshakes
	
	If the NBX Application is not "logged on" with respect to a particular LINK PI then
	• It will not send Handshakes to that PI
	• It will respond to Handshakes from that PI
	
	Refer to "Application Logon / Logoff" for an explanation of the term logged on.

© Post Office™ 2003-2004

FUJ00001890

Interaction with AWK	An application (NBX and LINK) can send and respond to Handshakes without the application needing a valid AWK. The term valid covers all cases where the current AWK is not identical at the NBX and LINK peer. For example it could be stale (i.e. different) or Null.
Handshake Response	NBX and LINK will send the Handshake response on the same TCP connection as the received Handshake request.
NBX Behaviour	NBX will send Handshakes (per TCP Connection) when the connection has been idle for a period and not when the line is busy. NBX will also send Handshakes when it suspects a problem. There are two configurable periods: (a) how frequently NBX sends a Handshake when idle (b) the interval used to realise there is no response NBX has a further configurable period, the minimum period between Handshakes when several suspected problems are detected in quick succession. (example values to be included) NBX behaviour when no responses After N (configurable) consecutive non-responses, NBX will raise an event and stop sending transactions to that PI. Note that NBX will recommence sending transactions to the PI after 1 successful Handshake response or a transaction response is received form the PI.

© Post Office™ 2003-2004

FUJ00001890

LINK Behaviour	LINK will send Handshakes (per TCP Connection) only when the connection has been idle for a period and not when the line is busy. Each time a Handshake response is Timed out an error message is output to the Network Management Interface (NMI). The time between handshakes is configurable (Initial values specified as 30 seconds TIS but subject to change). Therefore LINK will continue sending Handshakes whilst the TCP connection is open. I.e. for ever it does not stop Note that the above behaviour of no automatic action to lack of Handshake response is a consequence of NBX being an Acquirer only, which basically means that, LINK does not initiate Transactions to NBX. If it were the case the NBX were and Issuer and hence Initiated Transactions to NBX then lack of response to consecutive Handshakes would result in LINK not sending Transactions to NBX. This state is termed “in Delay”.

Table 8 Application Handshakes properties

7.2.3 Application Level Acquirer Working Key (AWK) Exchange

NBX will generate the Acquirer ZMK (AZMK) that applies to the acquirer zone.

The Acquirer Working Key (AWK) will be generated by LINK and sent to NBX in a 0800 network management message. NBX should respond to LINK with a 0810 message once the new AWK has been decrypted and applied to the NBX successfully.

NBX may request the generation of a new Acquirer Working Key at any time.

7.2.4 Time-outs

If an authorisation request is sent to the Card Issuer by LINK and not responded to within 15 seconds, the LINK switch will time the request out. All other timers should be set accordingly.

7.2.5 Sessions

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

7.2.6 Application Logon / Logoff

For purposes of description:

© Post Office™ 2003-2004

FUJ00001890

- The NBX Application has a local state variable with possible values {“logged on”,” logged of”, “not sure”} with respect to a particular PI.
- Similarly for the LINK application.

The following table summarises the main properties of Application Level Handshakes.

Property	Overview
NBX Transition to “Logged on” state	An NBX Application will transition to a “logged on” state with respect to a particular 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
LINK Transition to “Logged on” state	The LINK PI will behave as NBX
NBX Transition to “Logged off” state	An NBX Application will transition to a “logged off” state with respect to a particular PI under the following conditions: • An Application leaves the “logged on” state when it receives a successful response to a sign-off message. • An Application leaves the “logged on” state when it sends a successful response to a sign-off message.
LINK Transition to “Logged off” state	The LINK PI will behave as NBX

© Post Office™ 2003-2004

FUJ00001890

Interaction with TCP Connection establishment	Application Logons / Logoffs apply at the PI level and not the individual TCP connection level. It is not necessary for an Application Logon to be performed when a TCP connection is established. This deals with the following cases: • Where there are multiple TCP connections per PI • A TCP connection is re-established Notes; Once the communications links are re-established LINK can start accepting requests with no other messages (logons, key changes) However LINK will typically perform an Application Logon when establishing a TCP connection. So for example after a short term intermittent network failure (say 30 seconds) which causes the TCP connection to fail, then LINK will establish a new TCP connection and perform an Application Logon. When NBX receives the first or only TCP/IP connection for a PI, it delays sending a Sign On message for a few seconds (configured to 3 secs) in the expectation that LINK will immediately Sign On to NBX. This is to avoid unnecessary collisions of Sign On requests.
Interaction with TCP Connection termination	**Case: Non application initiated TCP Connection Termination** The LINK PI remains in a Logged on state (DN: Note I think this behaviour as well as what NBX does is irrelevant. Refer to previous row regarding LINK behaviour when TCP connection is re-established. **Case: Application initiated TCP Connection Termination** An application should always initiate a logoff sequence* and before closing the TCP connection. * the term sequence is used to possible retries after time out waiting for response
Interaction with AWK	An Application Logon sequence results in a new AWK for the PI. This is because LINK has configured NBX to receive a new AWK automatically. NBX receives a new AWK when there is an Application logon sequence plus at set intervals thereafter.

© Post Office™ 2003-2004

FUJ00001890

Interaction with Messages	A “logged off” PI will respond to requests. For acquirer only members being “logged off” does not seem to mean that much, most members both issue and acquire, if a PI is logged off LINK will not forward any issued traffic to it. However because LINK like to present a homogenous view of the world to Operators they require that all PIs are logged on.
Application signoff	Good behaviour e.g. Maintenance period
Application signon	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 detects a new TCP connection initiated from LINK. By simply performing an Application Logon sequence the NBX application can assert that both it is logged on and the LINK application is logged on.

Table 9 Logon and Logoff

© Post Office™ 2003-2004

FUJ00001890

8 Disaster Recovery

8.1 Disaster Recovery Environment

The entire processing environment put in place by LINK to facilitate the connection of NBX will be replicated within the LINK contingency environment.

This contingency environment will be maintained by LINK support staff and will be maintained in parallel with the production environment,

In the event of total failure of the primary LINK systems, DR will be invoked and production service restored to NBX using the LINK contingency systems.

8.2 Disaster Recovery Testing

The LINK contingency systems are normally tested up to twice annually. The entire processing environment is transferred from the LINK production environment to the LINK contingency environment in Pudsey, LEEDS. Notice of this invocation will be provided to NBX at least 7 days in advance of the test.

8.3 Disaster Recovery Invocation

The decision to invoke the move to the contingency system from production by LINK may be taken by persons in the positions listed below:

- LINK Operations Shift Manager
- LINK Computer Operations Manager
- LINK Data Centre Manager
- LINK Head of System Support
- LINK Operations Director

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.

A decision to move to DR processing may be made by the Post Office Ltd. representatives nominated in schedule 7.

8.4 LINK Move to DR Processing

The move by LINK to DR operation (and back) does not require NBX to change their systems. This is due to NAT and the fact that NBX allows 4 source IP addresses (which are Firewalls) in the Peering Address space..

NBX systems will accept TCP connection requests from the LINK production or DR facility. The LINK production and DR IP addresses are specified in Section Appendix A.

© Post Office™ 2003-2004

FUJ00001890

The NBX firewalls have both production and DR IP addresses configured but not concurrently enabled.

If LINK invokes DR the Post Office Ltd. (NBX) Operations department will be contacted by LINK Operations and informed of the switch to DR processing.

8.5 NBX Move to DR processing

NBX does not move to DR.

8.6 DR Invocation Contacts

The LINK and NBX Operational contact points mentioned above are specified in [OLA].

© Post Office™ 2003-2004

FUJ00001890

9 Identifiers

9.1 Post Office Ltd. Identifiers

The following identifiers will be used for Post Office Ltd. in the LINK network:

Acquirer ID Number:	**2200040000** (This id was allocated by LINK)
Post Office Long Name:	**POST OFFICE LIMITED**
Post Office Short Name:	**Post Office Ltd.**
Post Office PI's:	**PI's x 4 Identifiers to be assigned**
Post Office CH's:	**CH's x 4 Identifiers to be assigned**
Post Office Line Names:	**One Line per PI. Identifers to be assigned.**

Table 10: Post Office Ltd. Identifiers

9.2 ATM ID

9.2.1 ATM ID Reference Data Required by LINK

Post Office Ltd. will provide LINK with reference data describing their Counter Terminal Positions. It has been agreed that Post Office Ltd. will provide LINK with enough information to identify the Post Office Outlet from the online ATM id field.

- At least one-month prior to live operation of a new Outlet Post Office Ltd. must provide address and online identification details of the Outlet.
- At least one-month prior to the closure of an existing Post Office Ltd. Outlet Post Office Ltd. must inform LINK of the impending closure.

A full description of the reference data to be provided to LINK is found in the document:

LINK / Post Office (Post Office Ltd.) RDS to LINK ATM Database Specification. (DN Need reference)

© Post Office™ 2003-2004

FUJ00001890

Appendix A Detailed Configuration Information

All IP addresses documented in this section are from the collection LINK Published IP address space.

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

A.1 Production / DR System

NBX		
System	**IP**	**Port**
NBX	VIP u :192.168.24.1 / 24	5186
NBX	VIP v : 192.168.24.2 / 24	5286
NBX	VIP w : 192.168.24.3 / 24	5386
NBX	VIP x : 192.168.24.4 / 24	5486

LINK Production		
IP	**Port**	**PI**
192.168.17.1 / 24	[1025..2^{16}-1]	p
192.168.17.2 / 24	[1025.. 2^{16}-1]	p
192.168.17.3 / 24	[1025.. 2^{16}-1]	r
192.168.17.4 / 24	[1025.. 2^{16}-1]	s

As stated in 8.4, there is no change in IP addresses or Ports when LINK move to DR.

The following tables defines the TCP/IP socket used between NBX production system and LINK Production / DR system for file transfer using Connect:Direct. Note that LINK initiate sending the File.

File Transfer	NBX IP& Port		LINK Production IP & Port	
LINK ➔ NBX	Bootle: 192.168.26.1 /24 Wigan: 192.168.25.1 /24	Tbs	192.168.18.1 /24	TBS

© Post Office™ 2003-2004

FUJ00001890

The labelling of Routers is as shown in Figure 2: Post Office Ltd. to LINK Communications Infrastructure.

Pint to Point connection	Subnet	IP for interface	Locati
NBXR1 to POLWIG1	192.168.23.0 / 30	NBXR1: 192.168.23.1 POLWIG1: 192.168.23.2	Wigan
NBXR2 to POLWIG2	192.168.23.4 / 30	NBXR2: 192.168.23.5 POLWIG2: 192.168.23.6	Wigan
NBXR3 to POLBOOT1	192.168.23.8 / 30	NBXR3: 192.168.23.9 POLBOOT1: 192.168.23.10	Bootle
NBXR4 to POLBOOT2	192.168.23.12 / 30	NBXR4: 192.168.23.13 POLBOOT2: 192.168.23.14	Bootle

A.2 Testing

NBX		
System	**IP**	**Port**
NBX	VIP u :192.168.9.9 / 29	5186
NBX	VIP v :192.168.9.10 / 29	5286
NBX	VIP w :192.168.9.11 / 29	5386
NBX	VIP x : 192.168.9.12 / 29	5486

LINK Testing		
IP	**Port**	**PI**
192.168.9.17 / 29	[1025.. 2^{16}-1]	p
192.168.9.18 / 29	[1025.. 2^{16}-1]	p
192.168.9.19 / 29	[1025.. 2^{16}-1]	r
192.168.9.20 / 29	[1025.. 2^{16}-1]	s

© Post Office™ 2003-2004

FUJ00001890

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

File Transfer	NBX IP& Port		LINK Production IP & Port	
LINK ➔ NBX	192.168.9.13 / 29	tbs	192.168.9.21 / 29	TBS

Routers

Pint to Point connection	Subnet	IP for interface
NBX to LINK	192.168.8.0 / 24	NBX: 192.168.8.25 LINK: 192.168.8.1

© Post Office™ 2003-2004

FUJ00001890

Appendix B Testing

This section provides a summary of the Test environment. It should be noted that the main purpose of the Test environment is functional testing.

a) LINK will provide the same number of PI's as the Production Environment.

b) Wide area connectivity will be over an ISDN2e service - single 64,000 bps B channel.

c) CHAP (MD5) and Calling Line Identity (CLI) will be used by the NBX Test ISDN Router to authenticate the LINK Router when the LINK Router initiates the connection. Similarly the LINK ISDN Router will authenticate the NBX ISDN Router using CHAP (MD5) and CLI when the NBX Router initiates the connection. The procedure for CHAP secret handling is defined in [OLA].

d) LINK will "open the line" to establish the ISDN call for an agreed testing window. At the end of this testing window LINK will "close the line" to close the ISDN call.

e) Either LINK or NBX can cause the ISDN call to be established. It is expected that normally LINK will establish the ISDN call as stated above. However if the ISDN call gets dropped for whatever reason then traffic from NBX to LINK may cause an ISDN call attempt.

f) The ISDN idle timers will be set to avoid the call dropping during the testing window. Therefore the ISDN idle timer will be set to less than the max of (TCP KeepAlives Interval, Application Heartbeats interval).

© Post Office™ 2003-2004