Document Title:	HNG-X TO RMG TECHNICAL INTERFACE SPECIFICATION
Document Type:	Technical Interface Specification (TIS)
Release:	Release Independent
Abstract:	Technical interface between TMS and POL LAN infrastructure at CSC Northern Data Centre, Sungard LTC at Hounslow and CSC Maidstone Data Centre
Document Status:	APPROVED
Author & Dept:	Stephen Wisedale, RMGA, Fujitsu Services
Internal Distribution:	See section 0.4
External Distribution:	See section 0.4

Approval Authorities:

Name	Role	Signature	Date
Ian Trundell	Design Authority (Post Office)		
Sridhar Arun Kumar	Professional Services (CSC)		
Mark Jarosz	Design Authority (Fujitsu Services)		

Note: See RMG Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

0 Document Control

0.1 Table of Contents

0.2 Table of Figures

0.3 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	08/04/08	Initial Draft for review	
0.2	24/04/08	Review comments incorporated.	
0.3	20/07/08	Updated diagrams and Approval Authorities	
0.4	04/09/08	Changed NAT Space as requested by POL	
0.5	12/09/08	Minor updates as requested by POL	
0.6	05/10/08	General update including NAT information	
0.7	24/10/08	Maidstone Transit LAN Update	
0.8	24/11/08	Update for Maidstone IP addresses	
0.9	12/03/09	Update for Maidstone IP addresses	
0.10	16/03/09	Minor update to table in section B.1 for Maidstone IP addresses	
1.0	14/04/09	Issued for approval	
1.2	11/06/10	Updated for POLSAP	
1.3	14/06/10	Revised reviewer / approver list	
2.0	27/7/10	Issued for approval	

0.4 Review Details

Review Comments by :	24-Jun-2010
Review Comments to :	stephen.wisedale GRO & PostOfficeAccountDocumentManagement GRO
Mandatory Review	
Role	Name
Solution Design/Development	Andy Williams*
Infrastructure Design	Pat Lywood
SSC	Steve Parker*
Optional Review	
Role	Name
Security Architect	Tom Lilywhite
CTO	Amit Apte
Security risk team	CSPOA.Security GRO
HNG-X R1 Programme Manager	Geoff Butts
POLSAP Infrastructure PM	Dave Paddon
LST Manager	Sheila Bamber

SV&I Manager	Chris Maving
Service Network	Ian Mills
Migration	Alan Flack
Migration	Craig Rogers
Head of Service Operations	Tony Atkinson
Post Office Design Authority	Ian Trundell
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

(*) = Reviewers that returned comments

0.5 Associated Documents (Internal & External)

	Reference	Version	Date	Title	Source
1	TI/IFS/001 PCSTIPIS.DOC	7.0	02/10/03	Pathway to TIP Application Interface Specification	Post Office Ltd
2	BP/IFS/010 RDP/AIS/014	5.2	23/10/02	Application Interface Specification Reference Data to Pathway	Post Office Ltd
3	BP/DES/023 JED/LFS/007	4.0	04/11/03	LFS to SAPADS and SAPADS to LFS Application Interface Specification	Prism Alliance
5	BP/CON/315	1.0	15/01/03	Schedule 15 –Service Levels and Remedies	
6	RDP/OLA/001	1.3	19/07/99	Reference Data – POCL/ICL Pathway Operational Level Agreement	Post Office Ltd
7	TI/IFS/003 RDP/TIS/001	2.2	30/11/98	Pathway to Post Office Ltd Technical Interface Specification	Post Office Ltd
8	BP/IFS/011 RDP/AIS/011	4.3	07/10/99	Application Interface Specification Reference Data to Pathway Type B Data	Post Office Ltd
9	JED/LFS/008 BP/DES/024	1.1	16/07/99	LFS Data Retention	Post Office Ltd
10	CS/OLA/038	4.1	10/10/03	Operational Level Agreement for Logistics Feeder Service	Fujitsu Services
11	CS/SPE/011	5.0	28/03/03	Network Banking End to End Reconciliation Reporting	Fujitsu Services
12	NB/SDS/008	2.0	14/08/02	Network Banking MIS Reports Design	Fujitsu Services
13	NB/IFS/012	3.0	10/11/03	Bureau de Change Transaction Feed for FRTS	Fujitsu Services
14	RD/IFS/033	3.0	10/11/03	Post Office Ltd to Fujitsu Services AIS for Bureau de Change	Fujitsu Services

15	AIS_ADS to POLFS_V1.0	1.0	10/12/03	SAP ADS to POL FS Application Interface Specification	Prism Alliance
16	NB/HLD/023			Network Banking Replacement/TES Reports	Fujitsu Services
17	NB/IFS/036			Transaction Enquiry Service (TES) Post Office Ltd Reports Specification	Fujitsu Services
18	NB/IFS/037			Transaction Enquiry Service (TES) MSU Reports Specification	Fujitsu Services
19	POLFS TIS	2.2	10/3/05	POLFS technical interface specification	Prism Alliance
20	AS/DPR/018			Design Proposal for APOP	Fujitsu Services
21	AP/IFS/065			APOP Host System Reporting to EDG Application Interface Specification	Fujitsu Services
22	AP/IFS/063			Post Office Ltd EDG to Horizon APOP Authorisation Service Application Interface Specification	Fujitsu Services
23	POLFS Portal Infrastructure	1.0		Current Workplace and Future Portal Components	Prism Alliance
24	AS/IFS/002			Horizon to EDG - Technical Interface Specification for Track and Trace	Fujitsu Services
25	AP/AIS/072			FAD code to Agent ID Mapping file AIS	Fujitsu Services
26	AP/AIS/073			MoneyGram Web Server Control Files AIS	Fujitsu Services
26a	CR/TIS/001	1.01		POLFS DR Infrastructure & POLFS DR Infrastructure Diagrams	Post Office Ltd/ CSC
27	DE/LLD/038	In PVCS		Network Design for Horizon to POL Including LTC DR	Fujitsu Services (PVCS)
28	PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office Ltd Account HNG-X Document Template	Dimensions
29	DES/NET/HLD/0015	Current	10 Nov 07	Transit LAN Design	Dimensions
30	REQ/CUS/STG/0001			HNG-X Migration Strategy - Agreed Assumptions and Constraints	
31	DEV/INF/LLD/0041	Current		Data Centre LAN Design	Dimensions
32	POLSAP/DEV/INF/LLD/0121	Current	04/07/09	POLSAP Consolidation Project	Dimensions

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

0.6 Abbreviations

Abbreviation	Definition
ACE	Application Control Engine
ADS	(Post Office) Advanced Distribution System
AIS	Application interface Specification
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
BGP	Border Gateway Protocol
CE	Customer Edge
CSC	Computer Science Corporation
CTS	Client Transaction Summaries
DMZ	De-Militarised Zone
DR	Disaster Recovery
DRS	Data Reconciliation Service
EDG	Electronic Data Gateway
FS	Fujitsu Services
FTMS	File Transfer Managed Service
FTP	File Transport Protocol
FRTS	First Rate Travel Services
HNG-X	Horizon Next Generation
HO	Hand-Off Router
HRSAP	Human Resource SAP
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol security
IRE11	Ireland 11 data centre
IRE19	Ireland 19 data centre
ISO	International Standards Organisation
LAN	Local Area Network
LFS	Logistics Feeder System
LTC	London Technology Centre
LPR	Line Printing Remote Protocol

NAT	Network Address Translation
NBS	Network Banking Systems
NDC	Northern Data Centre
NMS	Network Management Server
MGRM	Money Gram
MIS	Management Information System
MSAD	Microsoft Active Directory
OSPF	Open Shortest Path First
PAT	Port Address Translation
POL FS	Post Office Ltd Financial Systems
POL RDS	Post Office Ltd Reference Data System
POLSAP	Consolidation of POL FS and SAPADS to be hosted in IRE11 and IRE19
QOS	Quality Of Service
RDMC	Reference Data Management Centre
RDS	Reference Data System
RMG	Royal Mail Group
RV	Release Verification
SAPADS	SAP Advanced Distribution System
SAPGUI	SAP Graphic User Interface
T&T	Track and Trace
TES	Transaction Enquiry Service
TIP	Transaction Information Processing
TMS	Transaction Management System
TPS	Transaction Processing System
VLAN	Virtual LAN
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol (RFC3768)
WAN	Wide Area Network

0.7 Glossary

Term	Definition
Carrier	Local Exchange Carrier
CSC	Manage RMG Data Centres at Maidstone, & NDC

DMZ	A DMZ is a subnet between a trusted internal network and an untrusted external network. Typically, the DMZ contains publicly accessible systems (e.g., Web servers, file servers, mail servers and DNS servers). It usually is located at the perimeter of the trusted internal network.
Operation Interface	Demarcation point between the HNG-X and RMG networks, which is implemented with the use of the Transit LAN
Operational Server	Hosted HNG-X Servers are the FTMS servers
Production	When referring to data centre use, indicates the data centre primarily providing service to the customer business. Normally the Primary data centre at IRE11.
Test	When referring to data centre use, indicates the data centre primarily providing a test service. Normally the Secondary data centre in IRE19.
TMS	This refers to all transactional services which Fujitsu services manages on-behalf of POL in relation to RMG

0.8 Changes Expected

Changes
Upgrade of circuits and handoff routers at Huthwaite to provide additional bandwidth and improved throughput underway at time of writing
FTMS remote gateways are currently located remotely in NDC however these may move to IRExx . It has been confirmed that the CSC servers listed in appendix C.1 are incomplete. CSC have confirmed that they shall, in the future, provide an accurate and complete list at which point this document shall be updated

0.9 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.10 Copyright

1 Introduction

1.1 Background

This document defines the technical interface between Transaction Management Systems (TMS) managed by Fujitsu Services and the POL LAN infrastructure at CSC Northern Data Centre, Sungard London Technology Centre (LTC) at Hounslow and CSC Maidstone Data Centre.

These interfaces exist in order to supply RMG with information concerning counter transactions, stock movements at RMG outlets and external payments, the main recipients being RMG TIP, SAP ADS (until POLSAP convergence) and EDG systems respectively. TMS is also required to pass reference data from the Reference Data System (RDS) to RMG outlets via the HNG-X RDMC. This single Technical Interface Specification is defined for all RMG systems at the RMG Data Centres that need to communicate with systems in the HNG-X Data Centres.

The LTC data centre serves as a disaster recovery site for NDC (excluding EDG). The Maidstone Data Centre serves as a disaster recovery site for only the EDG Remote Server.

1.2 Purpose

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

- To specify the technical details of the interface between the Fujitsu-hosted HNG-X and POLSAP systems and the host systems of RMG.

- To provide a consistent communications vehicle amongst the technical teams responsible for providing the various nodes and connections comprising the interface.

- To be regarded as a base document against which project change control should be assessed when implementing changes to the HNG-X – RMG connection.

1.3 Scope

This document describes the boundaries of responsibility between Fujitsu Services and RMG and does not document the service requirements of the Fujitsu Services interface.

The interface is defined at two levels:

1. The Application level, concerned with the application data passed across the interface (Refer to 2, 8, 21, 22)
2. The Technical level, concerned with the mechanisms by which the data is passed across the interface (The TIS – this document).

It does not define the rules for each file transfer. These are documented in the relevant Application Interface Specifications. There are single AIS documents for each application, which could be referenced in section 0.6

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.

The known applications which traverse this interface include:-

- MIS (Management Information System) - An Oracle based system to provide Management information reporting to Post Office on POL counter transactions etc. TPS takes transactions from the counter and nearly all transactions are sent to POL MIS (some – e.g. balancing transactions) are suppressed. [ref 1]
- RDS (Post Office Reference Data System) - Reference data is provided by Post Office to control the Horizon / HNG-X systems, and this data is held and managed from the database application RDMC (Reference Data Management Centre).[ref 2,8].
- Distribution - ADS (receipt and distribution of transaction stock information) [ref 3] ADS interfaces to the HNG-X system LFS (Logistics Feeder System). ADS also interface to the Post Office Ltd Financial System (POL FS) Hosted within the HNG-X Data Centres [ref 15]. At the introduction of S80 release additional SAP hosts were employed both in the production and development environments with different access requirements.

  Please Note: The POLSAP project will merge the SAP ADS and POL-FS systems to form a single SAP instance hosted in the HNG-X Data Centres.
- TP (DRS reconciliation reports [ref 11] and MIS reports [ref 12]. Network Banking – transfer of NBS reports from the Horizon System NBS and Network Banking Replacement reports [refs 16, 17]). It should be noted that TP is an organisation, rather than a system. A mechanism needs to be defined by the Post Office for extraction of the NBS, NBX and DRS reports from the remote gateway.
- Track & Trace - Application data flows (message exchanges) across the Track & Trace interface between HNG-X and the EDG domain. It requires a SOAP exchange that originates from the HNG-X client SOAP and is used to push a message to the EDG system. [ref 24].
- Online access to POL FS (and subsequently POLSAP) within POL via the CSC Data Centre in Huthwaite.

  Please Note: Although there are business data flows between POL-FS (and subsequently POLSAP) and the CSC Data Centre in Huthwaite, the physical interfaces employ the HNG-X FTMS service and there is no direct batch interfacing. The only direct connections between RMG and POL-FS/POLSAP are for online access.

1.4 Structure

1.1.1 Introduction

This section describes the structure of the information contained within this document.

Section	Overview
1 Introduction	This Introduction.
2 Environment	This section describes the context and major components of the HNG-X and RMG environment.
3 Medium of Transfer	This section describes the interface in terms of the various ISO OSI Reference Model layers.
4 Application ports and services summary between HNG-X and RMG	This section describes Application ports and services summary between HNG-X and RMG
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 Resilience, Recovery	This section deals with disaster recovery design, facilities and procedures.
8 Migration	This section covers the migration strategies, interfaces and post migration
9 Testing	This section covers end-to-end testing for application platforms between RMG and HNG-X
A Detailed Configuration Information	This section details IP Address and other configuration details.

2 Environment

2.1 Introduction

This section presents an overview of the context in which RMG and HNG-X 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 Transport protocol, 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.

2.2 Context

The following diagram provides an overview of the interface location, the application level flows across the interface and the roles of the HNG-X and RMG data centres:

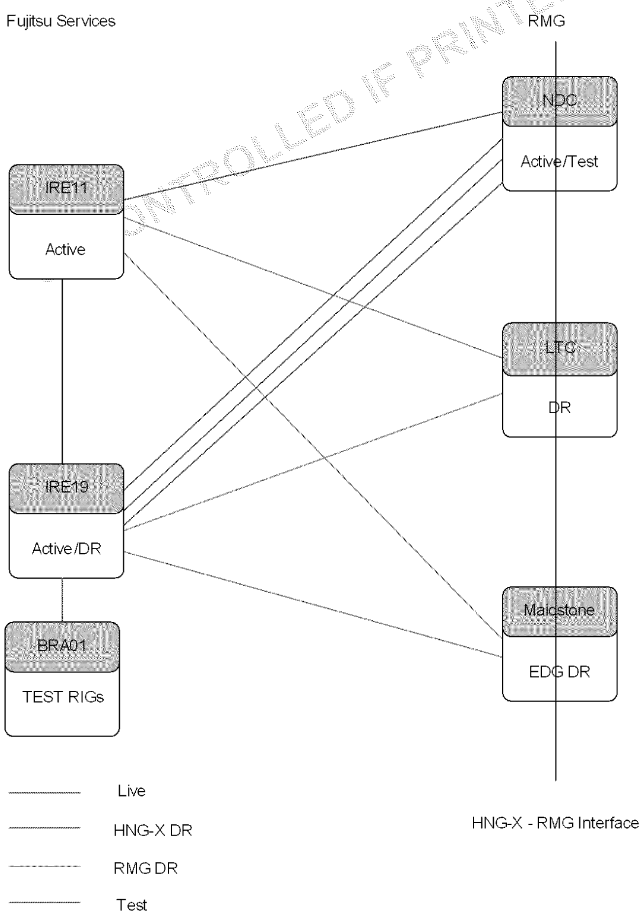

Figure 1 HNG-X – RMG Interface Context

Notes:

1. Network connectivity is always maintained between both the Fujitsu Data Centres and the RMG sites.
2. Functional testing capabilities will be provided by HNG-X IRE19 site, BRA01 and NDC. 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.

2.2.1 Design Principles

The following principles are assumed to govern the design and implementation of the interface. [Refer to 29]:

- 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.

- Each physical communication line is routed via a different Carrier exchange, 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 Carrier network will be specified if the Carrier does not provide for dynamic rerouting when failures occur.

- Encryption of data over the Wide Area Network (for production and test traffic) will be provided via the IPSEC protocol (Hand-Off router to Hand-Off router). Note that FS provide the Wide Area Network and the encryption / decryption takes place fully within the FS domain.

- The Applications requiring resiliency, should be logically configured to use multiple threads so that loss of a thread does not impact the service to customers. Note that not all applications have resiliency requirements (Refer to AIS [2, 8, 21 & 22]).

- HNG-X 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 RMG Data Centres. (RMG Data Centre sites operate a cold standby Disaster recovery model)

If either the RMG or HNG-X Production systems fail, suitable contingency systems will be provided to maintain service in accordance with the SLA (Refer to AIS [2, 8, 21 & 22]).

2.2.2 Transit LAN at RMG

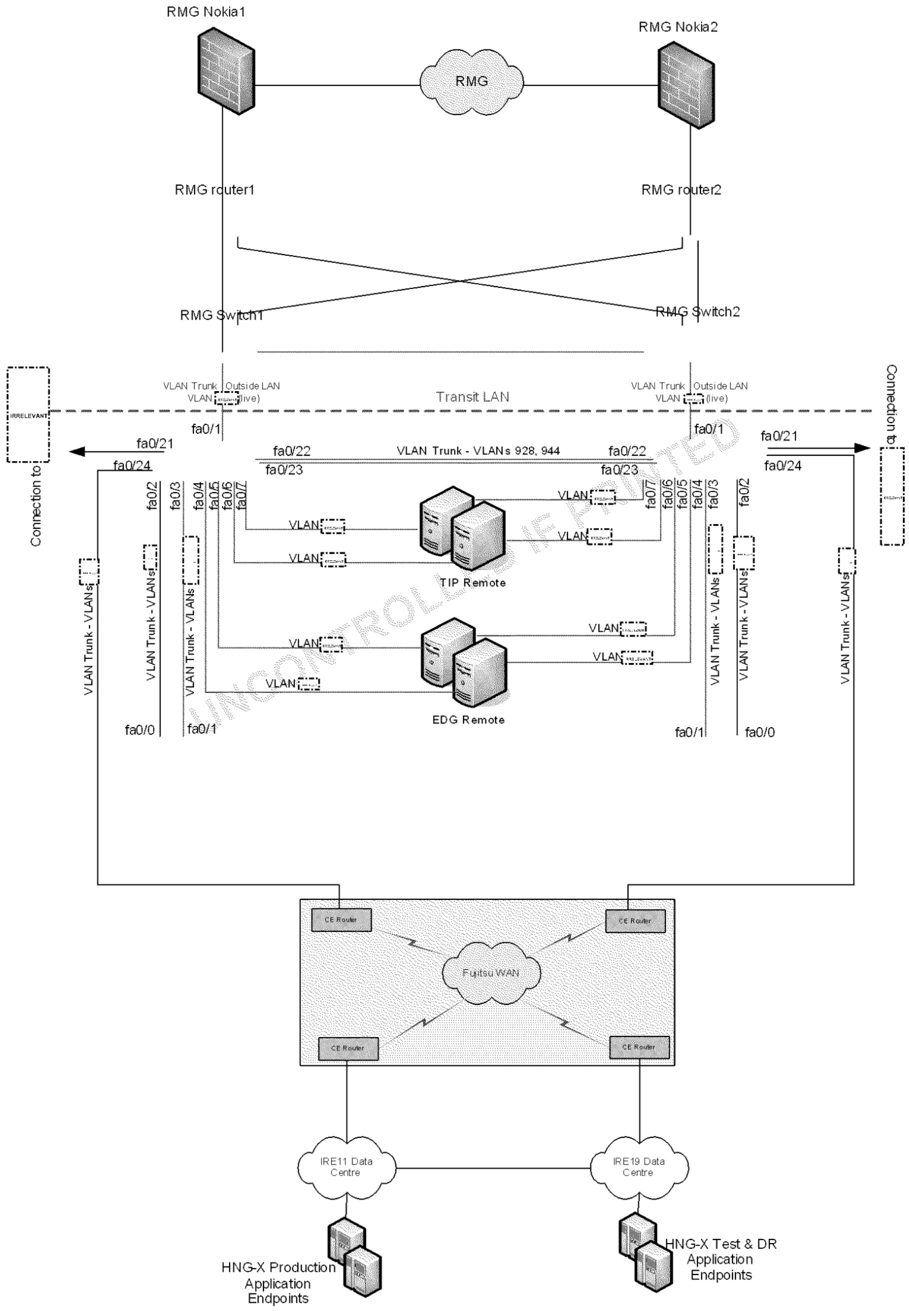

Figure 2: NDC Physical Topology

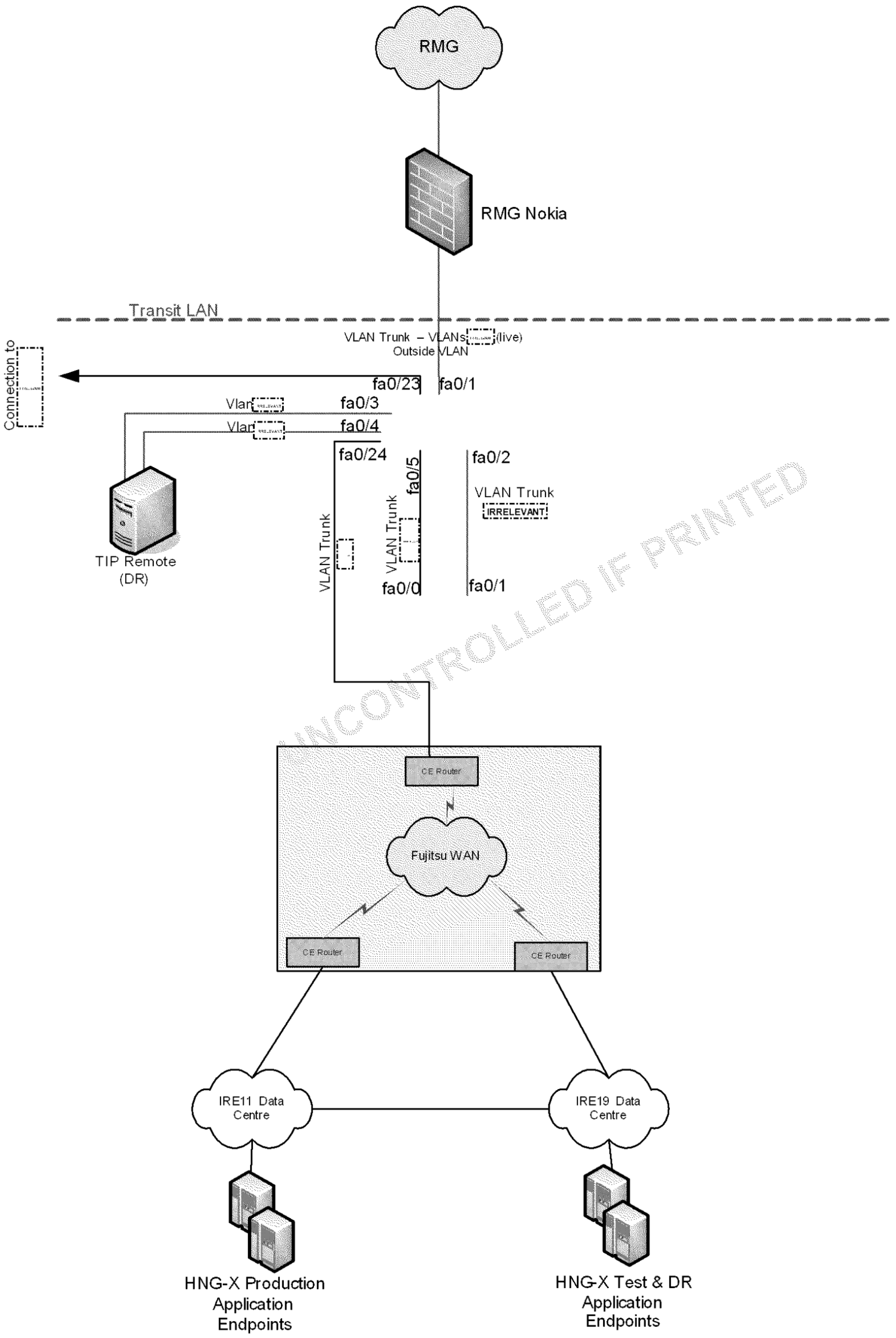

Figure 3: LTC Physical Topology

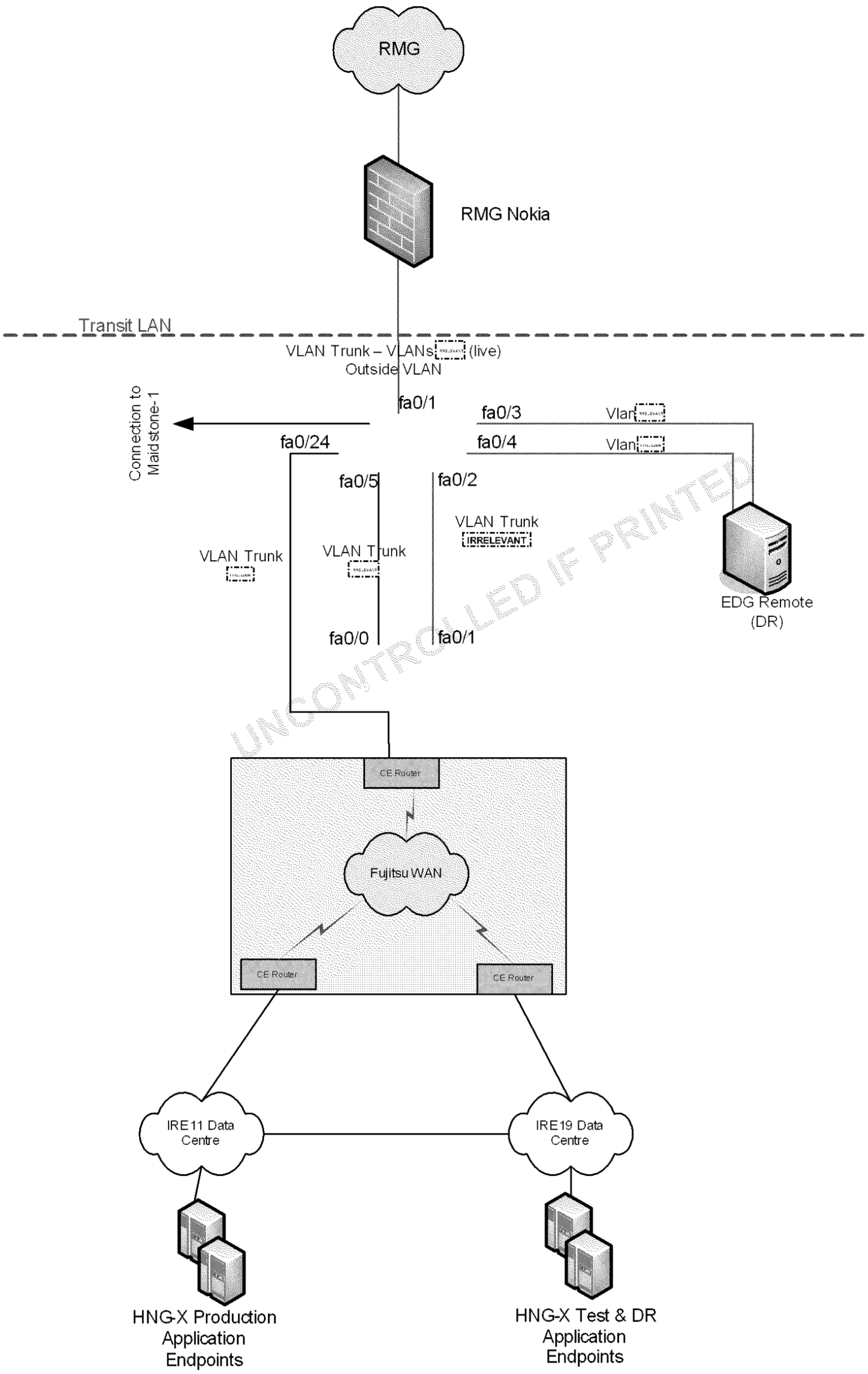

Figure 4: Maidstone Physical Topology

At each remote data centre a transit LAN exists to create a demarcation between the HNG-X network and the RMG network. This exists for security reasons and to provide unambiguous boundaries between the HNG-X network and the RMG network.

This demarcation exists at the physical level for switches or firewalls depending on location, at the logical level for addressing and routing and at the service level for the traffic between application endpoints that traverse it. The Transit LAN should not be confused with the DMZ; the Transit LAN is the exposed and unpopulated perimeter of the HNG-X network, beyond which no further controlled network devices exist.

A clearly defined demarcation is necessary to assist fault and service resolution, to facilitate technical interface specification and to prevent administrative conflicts or inter-penetration between HNG-X and an external organisations network.

At the NDC Data Centre, the Transit LAN model described as the Remote High Availability with Layer 2 provision is implemented, as shown in Figure 2 and Figure 5. In addition to the existing equipment, FS will provide two switches and two Hand-Off routers (requiring [Post Office Ltd/FS] IP addressing). The switch will provide connectivity between the existing FS CE routers and the current Horizon routers, therefore replacing the cross over cabling. The new routers for HNG-X will also connect to this switch.

2.2.2.1 Physical Infrastructure to support HNG-X

HNG-X network at NDC extends from the transit LAN, which is defined on two switches and two routers and made routable to the rest of the HNG-X network at Ireland across the FS WAN to the HNG-X Production Data Centres at IRE11 and IRE19. Traffic between Data Centres is encrypted in IPSec VPN Tunnels. Similar LANs are deployed at LTC and Maidstone but via a single switch and router.

The WAN implementation is fully redundant, ensuring resilient data paths between HNG-X sites and CSC Data Centres. Utilisation, performance of the circuits and router-to-router availability are constantly measured by Fujitsu Services. [Ref 30]

A separate remote LAN hosts the HNG-X Remote FTMS servers for EDG and TIP, (the POL back office applications).

Specific characteristics of the interface are documented in the following table:

Boundary	Overview
Component	Post Office Ltd (through its agent Fujitsu Services) will provide and manage all components (routers, switches & remote servers) on the HNG-X boundary of the Transit LAN. RMG will also supply the cables for the connections to the RMG switches. Within the RMG Data Centres, space will be made available within racks for the HNG-X routers and switch, as well as the TIP and EDG servers.
Network Management	The HNG-X devices are fully within the HNG-X Network Management domain. The RMG devices are fully within the RMG Network Management domain. The Connections between the RMG devices and the HNG-X devices fall into both the RMG and HNG-X Network Management domains as far as monitoring is concerned. ICMP is explicitly permitted for both test and fault diagnostics.

Operational	The HNG-X routers, switches and servers located at the RMG Data Centres are operated remotely. Once these devices have been commissioned, occasional and infrequent physical access may be required.
Environmental	RMG are responsible for providing a suitable environment for the HNG-X Systems physically located at the RMG Data Centres.

Table 1: Interface Characteristics

3 Medium of Transfer

3.1 Interface Overview

This section provides an overview of the Physical and Network interconnection arrangements between HNG-X and RMG. The interface will support the Production and DR network connections:

- Between the HNG-X Domain at IRE11/IRE19 and NDC Domain
- Between the HNG-X Domain at IRE/11IRE19 and LTC Hounslow Domain
- Between the HNG-X Domain at IRE11/IRE19 and Maidstone Domain

Note that in normal operation all of these site connections are active at the same time and function independently. As shown in the Transit LAN diagrams, figures 2, 3 & 4, services and components below the line labelled "Transit LAN" fall within the HNG-X Operational Domain. Similarly all Services and Components above the line fall within the RMG Operational Domain.

3.2 Layers 1 and 2 – Physical and Link

At NDC, there are two FS remote routers and two FS transit switches as shown in Figure 2. The remote routers are each connected to two CE Routers via the transit switches. The two Circuits to NDC are 8Mbps WAN circuits[1]. Over these WAN circuits, a single VPN is deployed across the WAN connecting the NDC to both Ireland sites at IRE11 and IRE19. Each remote router has two Fast Ethernet interfaces and is connected as follows; a single 100BaseTX interface, to the FS switch, over which the Transit LAN exists as well as the LAN connecting back to the HNG-X Data Centre and the second 100BaseTX interface, again to the FS switch to logically connect to its CE WAN router.

At LTC, there is a single FS remote router and a single transit switch as shown in Figure 3. The remote router connects to the CE router via the transit switch. The single Circuit to LTC is a 2Mbps WAN circuit. Over this WAN circuit, a single VPN is deployed across the WAN connecting LTC to both Ireland sites at IRE11 and IRE19. The remote router has two Fast Ethernet interfaces and is connected as follows; a single 100BaseTX interface, to the FS switch, over which the Transit LAN exists as well as the LAN connecting back to the HNG-X Data Centre and the second 100BaseTX interface, again to the FS switch to logically connect to the CE WAN router.

At Maidstone, there is a single FS remote router and a single transit switch as shown in figure 3. The remote router connects to the CE router via the transit switch. The single Circuit to Maidstone is a 2Mbps WAN circuit. Over this WAN circuit, a single VPN is deployed across the WAN connecting Maidstone to both Ireland sites at IRE11 and IRE19. The remote router has two Fast Ethernet interfaces and is connected as follows; a single 100BaseTX interface, to the FS switch, over which the Transit LAN exists as well as the LAN connecting back to the HNG-X Data Centre and the second 100BaseTX interface, again to the FS switch to logically connect to the CE WAN router.

[1] Huthwaite access circuits being upgraded from 2Mb/s to 8Mb/s – due for completion 19/06/2010

3.3 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:

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

3.3.1 Control Plane

3.3.1.1 IP Routing - NDC

Each FS Remote router at the NDC is connected to separate layer 2 switches, the transit switches. To provide redundancy, each remote router provides endpoints to tunnels, one from IRE11 and one from IRE19. The Transit switches which are used to provide demarcation between the two parties hosts several routed VLANs. These include, the outside LAN and the inside LAN

The outside LAN is used to route traffic between HNG-X and RMG. The FS remote routers operate a VRRP group. Its IP address is the default-gateway for the RMG network towards HNG-X, likewise, on the same network, the RMG routers operates its own VRRP group on the same subnet. The VRRP IP address is HNG-X's default-gateway. By running the VRRP groups, it allows for use of the available redundant hardware and routes between the networks without the need for a dynamic routing protocol between the HNG-X and RMG autonomous systems. VRRP groups also operate on the inside VLAN.

The inside network, hosts both the TIP and EDG remote servers. IP connectivity exists between the remote servers and the backend TIP and EDG local servers hosted at IRE11 and IRE19. See Figure 5.

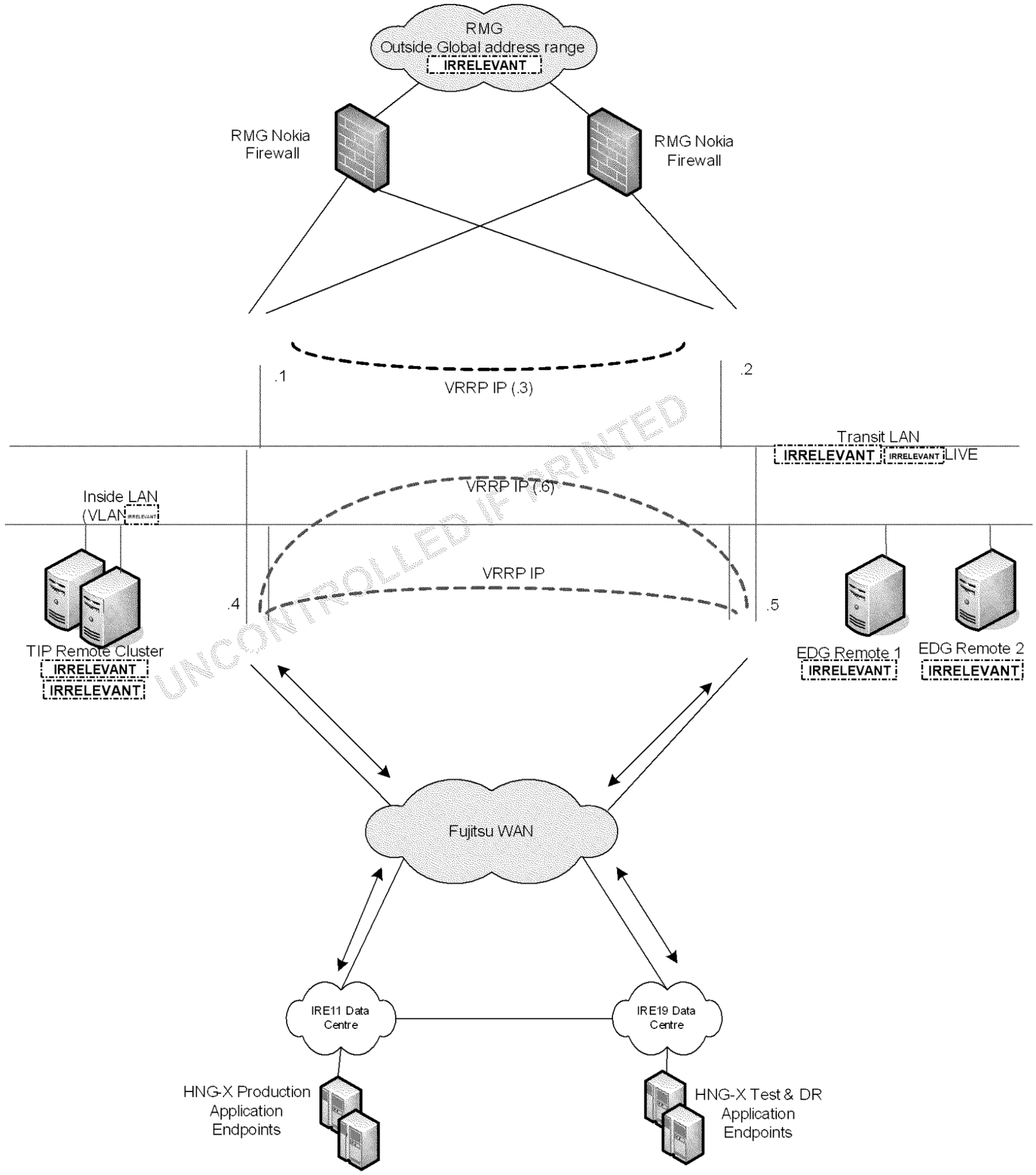

Figure 5: NDC Layer 3 Topology

3.3.1.2 IP Routing – LTC

A single remote router at the LTC is connected to a layer 2 switch, the transit switch. The remote router provides endpoints to the tunnels from IRE11 and IRE19. The transit switch which is used to provide demarcation between the two parties has several routed subnets configured. These include the outside LAN, and the inside LAN.

The outside LAN is used to route traffic between HNG-X and RMG. The IP address on the remote router serves as the default-gateway for the RMG network towards HNG-X, likewise, on the same network, the RMG routing device serves as a default-gateway for the HNG-X network. There is no dynamic routing protocol configured between these devices. There is also no redundant network configuration such as VRRP configured between the networks.

The inside network hosts the TIP remote server. IP connectivity exists between the remote server and the backend TIP local servers hosted at IRE11 and IRE19. See Figure 6

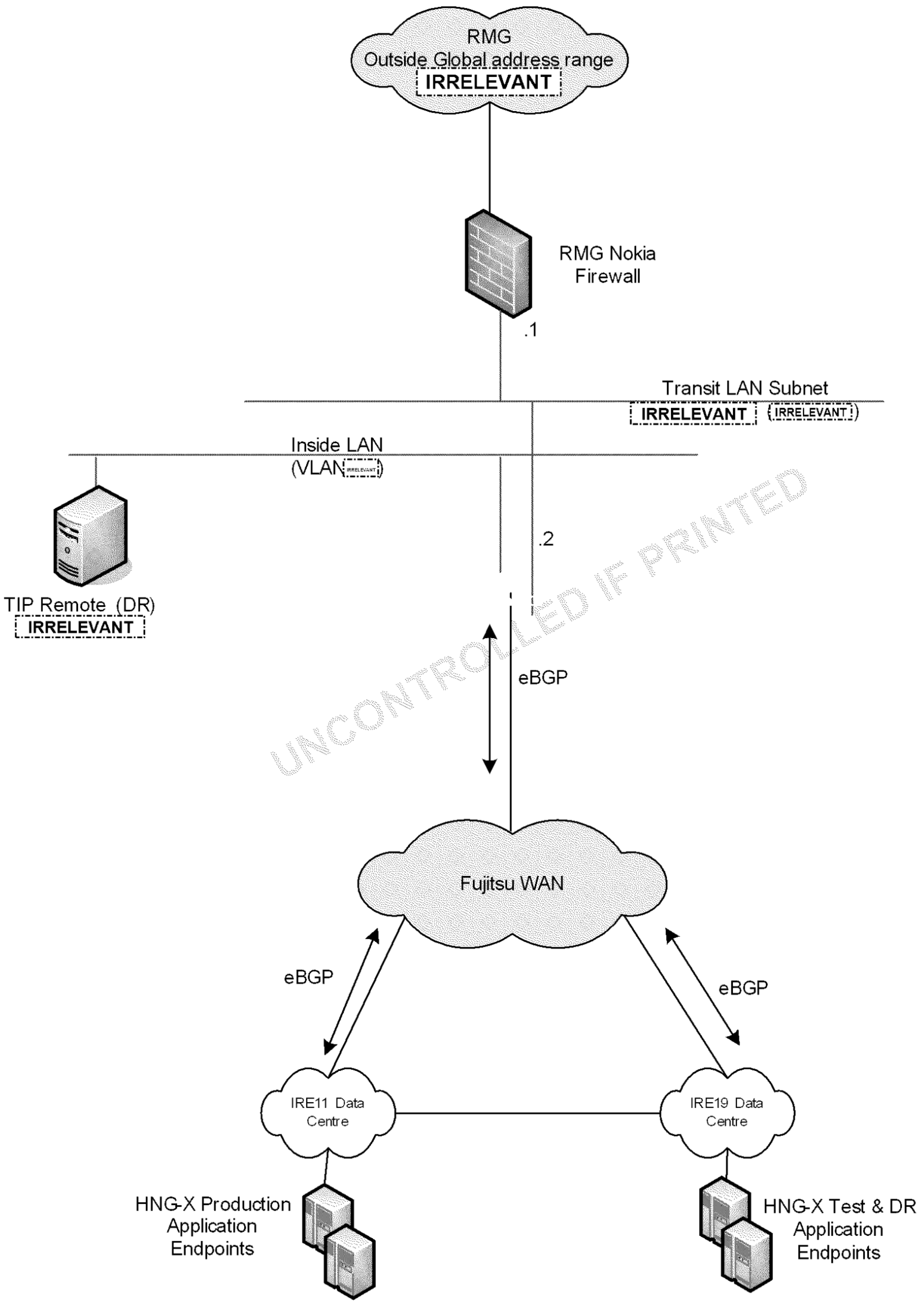

Figure 6: LTC Layer 3 Topology

3.3.1.3 IP Routing – Maidstone DC

This setup is very similar to LTC; however it serves as a disaster recovery site for just the EDG server. The remote router provides endpoints to the tunnels from IRE11 and IRE19. The transit switch which is used to provide demarcation between the two parties has several routed subnets configured on. These include the outside LAN, and the inside LAN.

The outside LAN is used to route traffic between HNG-X and RMG. The IP address on the remote router serves as the default-gateway for the RMG network towards HNG-X, likewise, on the same network, the RMG routing device serves as a default-gateway for the HNG-X network. There is no dynamic routing protocol configured between these devices. There is also no redundant network configuration such as VRRP configured between the networks.

The inside network, hosts the EDG remote servers. IP connectivity exists between the remote server and the backend EDG local server hosted at IRE11 and IRE19. Refer to Figure 7.

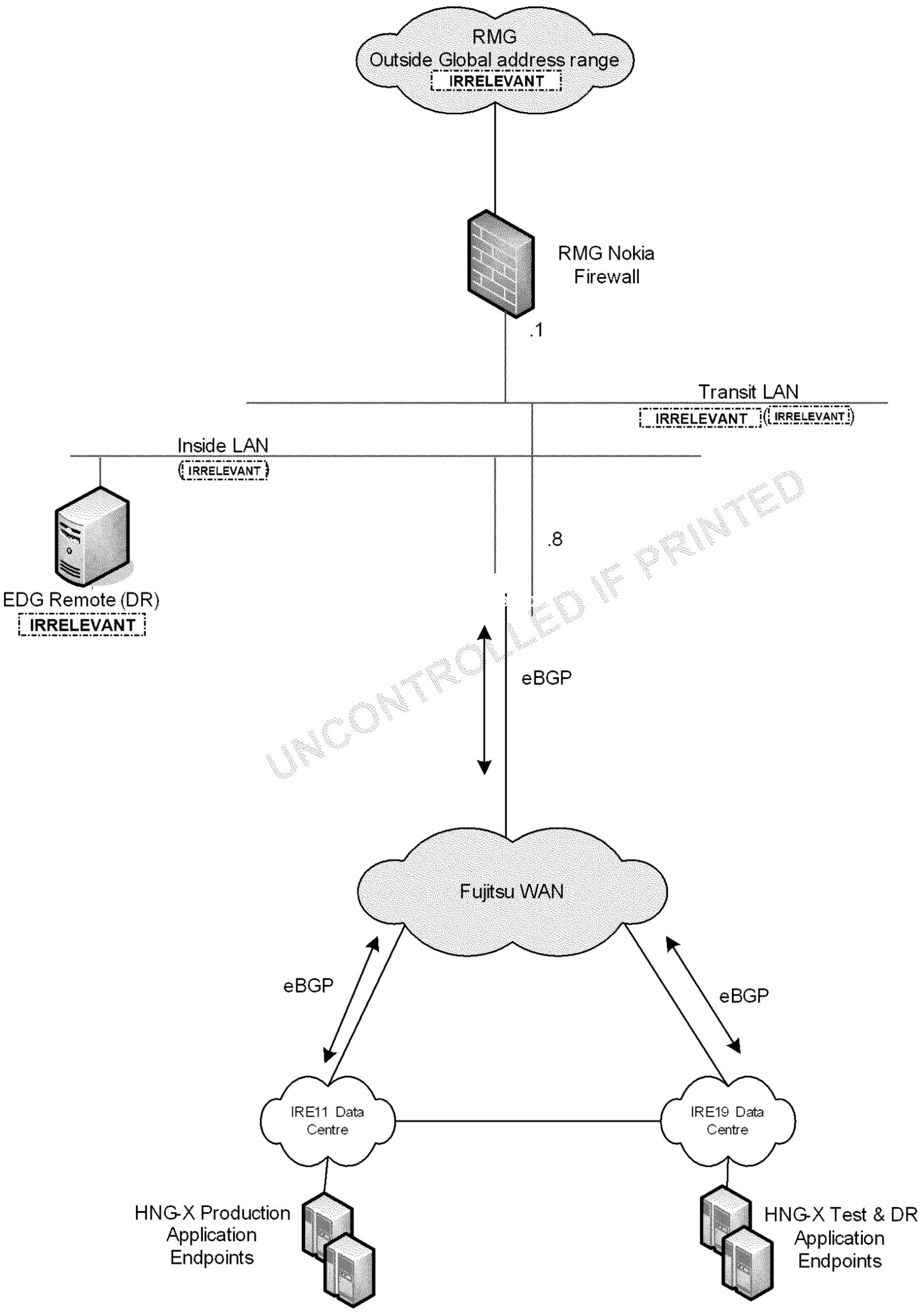

Figure 7: Maidstone Layer 3 Topology

3.3.1.4 ICMP

ICMP is explicitly permitted for test and fault diagnosis.

3.3.2 Data Plane

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

3.3.3 Virtual IP Addressing

The HNG-X Routers at the NDC Data Centre use VRRP to provide a resilient IP gateway to RMG.

RMG routers use VRRP to provide a resilient IP gateway to the HNG-X network. This allows for resilience to Network Interface failure.

3.3.4 IP Address Space

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 2.1.
- 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.

3.3.4.1 Network Address Translation

Network Address Translation mechanism is shown in Figure 8. NAT is used to provide privacy for both the HNG-X and RMG networks; i.e. that for one network, the service source and destination addresses can be described without reference to the other network. This structure maintains address space autonomy. In this network interface, both parties deploy their own ***bidirectional*** NAT via a transit LAN.

Each traffic flow is translated twice; once for HNG-X and once for RMG.

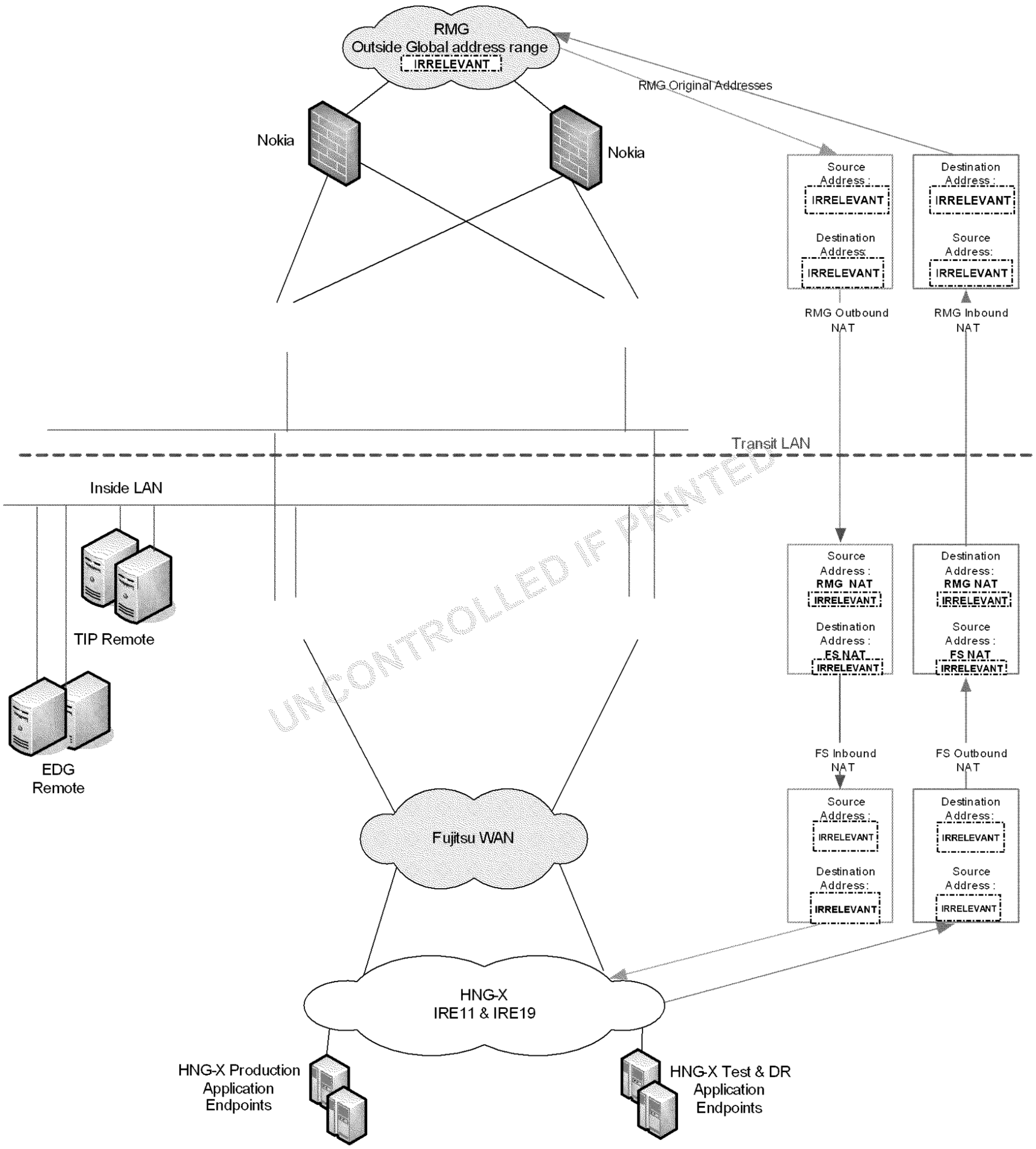

Figure 8: NAT Operation between HNG-X and RMG

3.1.1.1.1 Functionality

For the RMG network in NDC, the local RMG addresses of target services are translated to a peer address space represented single subnet IRRELEVANT. Individual addresses within this transit subnet are available to HNG-X source connections and mask the internal RMG addresses.

The RMG network interface makes use of both Port Address Translation and Static Translations for all source connections. In Port Address Translations a single IRRELEVANT subnet address is overloaded with any number of real connections using separate port numbers to differentiate them. With Static translations, pre-defined IP addresses within the same subnet are used for translation.

The use of an overloaded address both permits simplification of the HNG-X firewall rule base sets and limits the rule base granularity as these inbound RMG connections are regarded as a single source, irrespective of the application or server. However the use of PAT limits FS's fault diagnosis capabilities.

For the HNG-X network, the local HNG-X addresses of target services are translated to a peer address space represented by one or more subnets. Individual addresses within this peer subnet are available to RMG source connections and mask the internal HNG-X addresses. Furthermore, for a number of SAP Services, their HNG-X target addresses further translated with a further layer of translation.

Outbound initiated connections from the HNG-X network do not use Port Address Translation and exist as discrete connection from specific source addresses to specific destination addresses. Therefore the nature of the connection differs, depending on whether the RMG or HNG-X network is the initiator.

The same is NATing mechanism is implemented at both LTC and Maidstone Data Centres to achieve the same network autonomy.

3.1.1.2 IP Addressing

Each RMG data centre will be allocated its own IP Address subnet for dedicated purposes. Allocation of IP Addresses is based on the Data Centre LAN HLD document. [Refer to 31]. Each transit LAN IP subnet is shared between RMG and HNG-X. See appendix A.1 and B.1 for IP addressing.

4 Application ports and services summary between HNG-X and RMG

4.1 SAP Application Specific Requirement

The SAP application makes use of additional configuration to ensure that the end systems are aware of the NAT architecture.

The configuration change requires that the files ***gw/netstat*** and ***gw/alternative_hostnames*** on the FS host systems are edited to include a reference to their local global NAT address. An example is shown below, using the IRRELEVANT server:

Original	gw/netstat =/usr/bin/netstat –in gw/alternative_hostnames =
Final	gw/netstat= gw/alternative_hostnames = IRRELEVANT, IRRELEVANT

In conjunction with the above the ***hosts*** file should contain relevant entries for each host using the local HNG-X address space only. See Appendix C.1 for list of Ports allocated for services

The following table provides a summary of main characteristics of the interface supporting access from RMG to the HNG-X POL FS (and subsequently POLSAP).

Characteristic	Overview
Protocols	FTP / LPR / SAPGUI / SAPRFC / SAP Message Server / SAP Secure Gateway via TCP / IP
RMG Domain Application Endpoint and Connection Management –	Within the RMG domain there are multiple client platforms divided into the following groups; **ePortal** - Production Application Servers used for client access, Production DB Servers, ITS6.20 ePortal Servers, Citrix Server Farm **Other Systems**– SAP Application Servers, Dedicated POLFS/POLSAP Print Server, SAP File Repository, etc. These groups are represented by multiple virtual source addresses created on the RMG network. Appendix C.1 provides the full list of the known RMG servers.

HNG-X Domain Application Endpoint and Connection Management –	Within the HNG-X domain there are multiple host systems and the picture changes between POL-FS migration and POLSAP convergence. For POL-FS SAP POLFS R/3 Production at IRE11 PLP (Development and Quality Assurance remain in Bootle and Wigan). For POLSAP SAP POLSAP R/3 Production at IRE11 PLP SAP POLSAP R/3Development at IRE19 PLD SAP POLSAP R/3 Quality Assurance at IRE19 PLQ and PLE Each of these systems comprises of an R/3 main host with a compliment of application servers.
IP Ports	The specific destination TCP ports within the RMG Peering IP address: LPRINT – IRRELEVANT FTP IRRELEVANT (Build and ongoing SAPGUI Requirement) The specific destination IP ports within the HNG-X Peering IP address with the full range of possible SAP instances: SAPGUI – IRRELEVANT SAPRFC – IRRELEVANT SAP Message Server – IRRELEVANT SAP Secure Gateway – IRRELEVANT FTP – IRRELEVANT Additionally, it has been indicated by RMG that the following ports are required IRRELEVANT, IRRELEVANT, IRRELEVANT, IRRELEVANT The full details for port access are described within DE/LLD/029 POL Perimeter Access.

Table 2: SAP Application Specific Requirement

A full listing of all IP addresses allocated for the RMG servers can be found in Appendix A

4.2 TES Application Specific Requirement

The table below shows the NAT operation only from the RMG network perspective. The interactive traffic for the TES service uses TCP Port 443 between TES servers in IRE11 and IRE19 and user workstations in the RMG corporate network.

Characteristic	Overview
Protocol	HTTPS / TCP / IP

Application Endpoints and Connection Management	TES uses HTTPS within the HNG-X. Network Address Translation is used to allocate a single virtual IP address (VIP). This VIP points to the real IP addresses hosted at IRE11 for normal operation and in case of disaster recovery, the real IP address at IRE19. During disaster recovery, traffic will be automatically re-routed towards IRE19 for the same service under agreed SLA terms. See Appendix A.1 for IP address details

Table 3: TES Application Specific Requirement

4.3 Track and Trace Application Specific Requirement

The following table provides a summary of main characteristics of the Track and Trace online interface supporting interface between RMG and HNG-X. Note for more details please refer to [24].

Characteristic	Overview
Protocol	SOAP / HTTP/ TCP / IP
Application Endpoints and Connection Management	Track & Trace uses SOAP over HTTP over TCP. RMG host the T&T servers NDC and use uses a single virtual IP address for the HTTP servers. Maidstone serves as a disaster recovery site for T&T. Track & Trace use the existing Network platform between HNG-X and RMG. The T&T http clients (agents) are hosted at IRE11 for normal operation and IRE19 in case of a disaster recovery. One VIP address is used for the T&T agents. During disaster recovery, traffic will be automatically re-routed towards IRE19 for the same service. [ref 24] See Appendix A.1 for IP address details

Table 4: Track and Trace Application Specific Requirement

4.4 Online Interface to APOP Administration Service

The following table provides a summary of main characteristics of the online interface supporting access from RMG to the HNG-X APOP Authorisation service. Note for details of the APOP Administration service and APOP Authorisation application please refer to [20].

Characteristic	Overview
Protocol	HTTP / TCP / IP
Application Endpoints and Connection Management	Within the RMG domain there is a single virtual HTTP client platform created using Network Address Translation. This has a single IP address and can initiate multiple concurrent TCP connections. The HTTP Client can initiate connections to either of the two APOP Administration web services since they are both Active in normal operation.
IP Ports	The source ports for the HTTP clients are as follows; [1024-5000]. The APOP Authorisation web service listens on port IRRELEVANT. See Appendix A.1 for IP address details

Table 5: Online APOP Administration Service

4.5 Reference Data System (RDS)

Characteristic	Overview
Protocol	FTP /FTMS
Application Endpoints and Connection Management	RDS is hosted within the RMG domain at Huthwaite. FTP is used to manually transfer files from RMG TIP to FS remote TIP gateway. FTMS is used to send files to RDMS database hosted within HNG-X.

Table 6 Reference Data System

4.6 First Rate Travel Service (FTRS)

Characteristic	Overview
Protocol	FTP /FTMS
Application Endpoints and Connection Management	First Rate clients transfer two types of files (Spot Rate and Margin files) to the FTMS local gateways:- EDG Local and TIP local servers. . These files are processed and made ready for transfer to the FTMS remote gateways FTMS remote receives the files, logs the delivery, confirms their integrity and delivers them to RMG EDG environment, FRTS pulls the files from the EDG to their environment

Table 7 First Rate Travel Service

4.7 Interfaces to/from POLFS/POLSAP

The interfaces to and from POLFS and POLSAP are documented in appendix H1

4.8 Interfaces from HNG-X to POL Gateway (non POL FS)

Description	Transfer Mechanism 1	Transfer Mechanism 2	Requirements/ Comments
NB101 and NB102 and DRS summary reports for Debit Card transactions	TIP	POL Gateway	
NB101 and NB102 and DRS summary reports for Banking transactions	TIP	POL Gateway	
Various Data warehouse Reports (Banking e.g. Bank Analysis)	TIP	POL Gateway	
Various TES Reports	TIP	POL Gateway	
CTS Report	TIP	POL Gateway	
Desktop Buttons/Account Node data for RDS80	TIP	POL Gateway	

Table 8 Interfaces from HNG-X to POL Gateway (non POL FS)

4.9 Interfaces from HNG-X to EDG (non POL FS)

Description	Transfer Mechanism 1	Transfer Mechanism 2	Transfer Mechanism 3	Requirement/ Comment
AP Client files	TIP	EDG		
Bureau Transaction Data (to FRES)	TIP	EDG		
Bureau Control Total File	TIP	EDG	POL Gateway	
NB101 and NB102 and DRS summary reports for E Top-ups	TIP	EDG	POL Gateway	
EDG Verification File (APOP)	TIP	EDG		

APOP POMM and Generic Reporting	TIP	EDG	PO Admin Server	

Table 9 Interfaces from HNG-X to EDG (non POL FS)

4.10 Interfaces to HNG-X from EDG (non POL FS)

Description	Transfer Mechanism 1	Transfer Mechanism 2	Transfer Mechanism 3	Comment
FRES (Bureau Spot Rate & Margin Files)	EDG	TIP		
EDG Verification File (APOP)	EDG	TIP		

Table 10 Interfaces to HNG-X from EDG (non POL FS)

4.11 Interfaces from HNG-X to POL (non POL FS/POL Gateway/EDG)

Description	Transfer Mechanism 1	Requirements/ Comments
HR SAP file (remuneration data)	TIP	
POL MI file (transaction data)	TIP	
Various SAPADS files (LFS Interface)	TIP	

Table 11 Interfaces from HNG-X to POL (non POL FS/POL Gateway/EDG)

4.12 Interfaces to HNG-X from POL (non POL FS/POL Gateway/EDG)

Description	Transfer Mechanism 1	Transfer Mechanism 2	Requirements/ Comments
RDS80	FTP	TIP	
Various SAPADS files (LFS Interface)	TIP		
POL MI Error files	TIP		

Table 12 Interfaces to HNG-X from POL (non POL FS/POL Gateway/EDG)

5 Operational Considerations

The following sections define the operational considerations of the Production Operational Interface in normal steady state use.

The Test Interface is established to perform application functional testing as determined by the specific requirements of each application test phase.

5.1 Operational Schedule

The HNG-X servers are run continuously 24 hours a day.

For TPS, the frequency and timing of file transfers between the HNG-X Operational Server and the HNG-X Data Centres are determined by the AIS [ref 1].

For LFS, the frequency and timing of file transfers between the HNG-X Operational Server and the HNG-X Data Centres will be recorded in the Operational Level Agreement [ref 10].

Frequency and timing of file transfers between the Reference Data System and HNG-X are defined in the OLA [ref 6].

For the Bureau de Change service introduced at S50, the timing and frequency of file transfers are defined in [ref 1] (TIP), [ref 13] (Bureau de Change Transaction Feed for FRTS) and [ref 14] (Reference Data).

If a RMG system finds a problem in the transfer of files to/from the HNG-X Operational Server this is reported using Help Desk procedures defined in the OLA [ref 6].

In the event of an unrecoverable failure on any component of HNG-X Operational Server to HNG-X Data Centre file transfer link, the link will be automatically re-configured to use an alternate component. This enables file transfers to take place, whilst the failed component on the file transfer link is being restored.

In the event of HNG-X, server, router or switch failure, engineer site access to the hardware is required. Arrangements for engineer server access are covered in the OLA [ref 6].

5.2 Printer Setup

Printers are configured in SAP transaction /nspad. An IP address is configured as the printer server destination host. In the event of DR being invoked a new IP address will be provided for the printer server and it will be necessary to manually change the configuration of each printer to access this new address. See Appendix A for the allocated IP addresses.

5.3 Performance

The interface between HNG-X and NDC over which files are transferred has sufficient bandwidth to cope with the requirements and meet Service Level Agreements [ref 19] prior to the POLSAP convergence (when SAPADS online users will connect to the POLSAP system in the HNG-X Data Centres) . Please see appendix F.1 for current link utilisation. To meet the additional bandwidth requirements of the on-line POLSAP users, upgrades are planned to the HNG-X to NDC link, from 2x2Mbit/Second to 2x8Mbit/Second circuits.

6 Security

6.1 Data Integrity

Data integrity controls across the Operational Interface are implemented at application level as determined by the corresponding AIS [refs 1, 2, 3, 8, 13 & 14].

6.2 Data protection

On the NDC side of the Operational Interface the RMG firewall permits RMG systems to access as far as and not beyond the HNG-X Operational Server.

On the HNG-X side of the Operational Interface the HNG-X routers permit selected HNG-X systems access to the HNG-X Operational Server, and permit the Operational Server to access only the relevant HNG-X systems.

6.3 Data 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 HNG-X and RMG. Cisco router encryption (IPSEC) is used.

7 Resilience, Recovery and High Availability

7.1 Resilience

The HNG-X side of the Operational Interface at NDC is configured to avoid single points of failure.

LTC and Maidstone are disaster recovery sites and therefore are not built with resiliency but serve as backup sites to NDC.

In the Operational Server a resilient pair of processors is provided as protection against server failure. In normal operations the primary server processor is used to run the applications. In the case of failure of the primary processor the backup processor is manually brought into use. The backup processor assumes the IP addresses of the primary processor, so avoiding IP address changes in connecting systems. Raid discs are used to protect against disc failure.

Two links are provided and are diversely routed to separate ducts to protect the file transfer between the HNG-X Data Centres and the remote HNG-X servers against link or router failure. The routers and switches at NDC are cross connected to the server processors to protect against switch or server processor failure.

7.2 Fault Detection

A resilient network management system will manage the FS network infrastructure. This system will monitor the network for abnormal activity at all times. Fault detection is the responsibility of each party in their respective domains.

7.3 Disaster Recovery

Fujitsu Services support for RMG disaster recovery is via replication of the NDC operational environment at LTC and Maidstone Data Centre. In terms of Network connectivity, the NDC network is similarly setup at LTC and the Data Centre at Maidstone, however is not resilient. Figure 9 shows the flow of traffic to the active Data Centre at NDC during normal services:

- Both LTC and Maidstone networks uses a similar but unique address scheme to allow the network to remain operational for access and monitoring purposes outside of this DR deployment. In this context the LTC network infrastructure is operational within the same constraints of the rest of the HNG-X network.
- The failover from NDC to LTC must not exceed 72 hours. While the LTC network is available immediately, some tasks are required on the associated platforms to move the Operational Server between NDC and LTC. The same applies to Maidstone Data Centre for the EDG Server.
- In the case of POLFS (and subsequently POLSAP) there are operational tasks required to activate LTC for Production use in the event of a DR scenario. These do not apply for normal DR testing, where a dummy service is used in its place. The operational tasks are described in the next section.
- In a DR scenario the POLSAP user traffic will come to HNG-X from the LTC site. An upgrade to the LTC network circuit is proposed, from 2Mbit/Sec to 8Mbit/Sec.
- Testing of disaster recovery arrangements will be co-ordinated between POL and Fujitsu Services.

Figure 9 shows the normal flow of traffic and service between the Data Centres. In the event of a DR scenario caused by IRE11 failure, then all Traffic flow will continue between the HNG-X DR Sites and NDC, as shown in Figure 10.

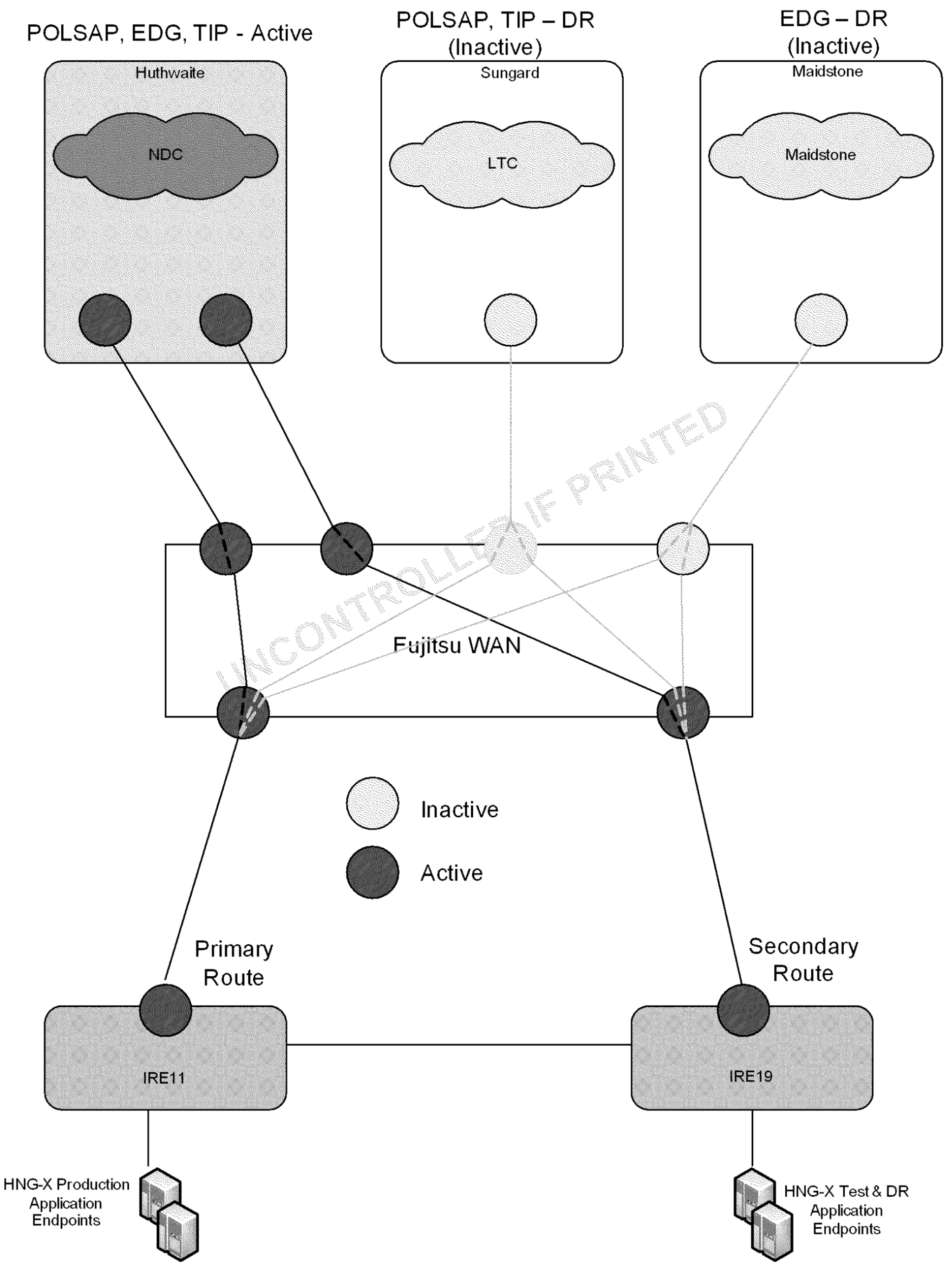

Figure 9: Normal Operation between HNG-X and the RMG

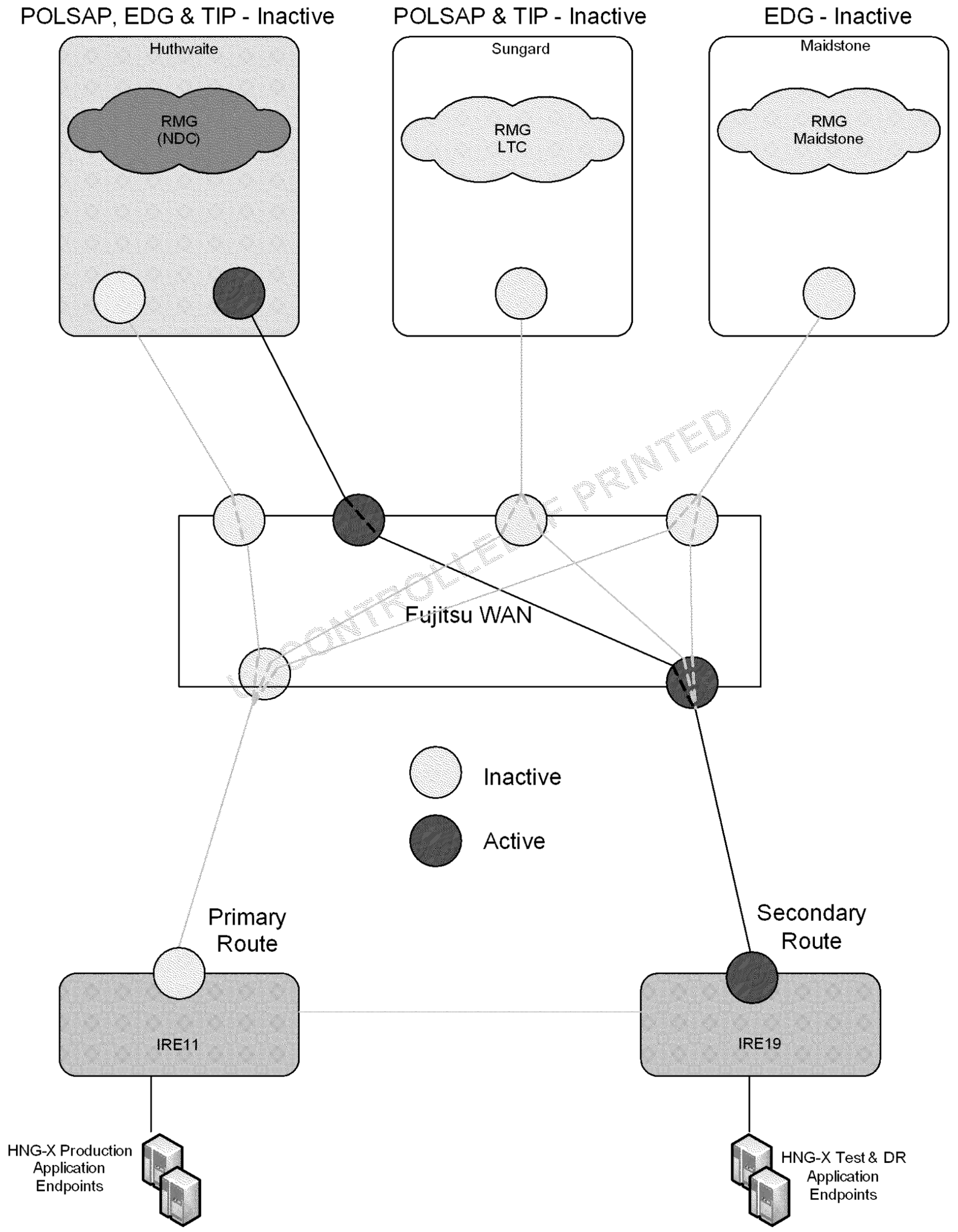

Figure 10: Failure at IRE11 instigating a Disaster Recovery Scenario

In the event that NDC undergoes a Disaster Recovery Scenario, then RMG DR Sites, LTC and Maidstone become active. All traffic flows would be directed to both IRE11 and IRE19

7.3.1 POLFS/POLSAP Specific Disaster Recovery Tasks

In the event of DR being invoked, FS SAP BASIS activities will be to verify the configuration detailed below and make any necessary IP address changes:

7.3.1.1 RFC Connection

RFC connections are maintained in SAP transaction /nsm59.

Existing connections UMP_400 and CSP_400 are configured to enable connectivity between POLFS and other RMG SAP systems. In the event of DR being invoked, these entries will require a manual IP address change.

RFC Connection	IP address configured in sm59	IP address for DR only
UMP_400	TBC	TBC
CSP_400	TBC	TBC

For testing connectivity only, the connections UMP_DR and CSP_DR will also exist.

RFC Connection	IP address configured in sm59
UMP_DR	TBC
CSP_DR	TBC

Note: These connections are for testing only and will not affect the existing environment.

7.4 High Availability

HNG-X provides a High Availability transit LAN with active/standby firewalls in each of IRE11 and IRE19.

8 Migration

8.1 Strategy

Over a period of time, both the HNG-X infrastructure for IRE11 and IRE19 will co-exist in parallel with the Horizon infrastructure at Wigan and Bootle. At this time, the Horizon infrastructure at all the RMG data centres will also co-exist sharing the same FS WAN infrastructure. Therefore the full content of TI/IFS/008 is applicable in the period of dual operation.

8.1.1 RMG Services Migration

RMG links will be considered live as part of weekend B and will operate in a Parallel configuration with both Wigan/Bootle and IRE11/19 active at that point.

All configuration activities will be complete in advance of the migration weekend and left in an admin down status. Minimal activity will be required to bring the RMG interface online, RMG will continue to target the Horizon address space for services provided in Horizon.

HNG-X Migration is split up into 4 weekends.

- Weekend A: POL FS (weekend A follows weekend D)
- Weekend B: Batch Services
- Weekend C: Online Service "There is no impact on CSC"
- Weekend D: Branch Services "There is no impact on CSC"

There is a subsequent migration step for SAP, when SAPADS is converged onto the POL-FS platform to form POLSAP.

- POLSAP Convergence

8.1.2 Weekend B Migration

This starts the service for the following services in IRE11/19

- FTMS TIP and EDG
- Track and Trace
- TESQA Web Service
- APOP Admin Web Service

Changes will be required by RMG to redirect traffic towards the HNG-X address space for the services moving during weekend B

8.1.3 Weekend A Migration

The POL-FS production system will migrate to IRE11 over a single weekend. At that point the development and QA testing environments for POL-FS will continue to use the server infrastructure in Bootle (PLD) and Wigan (PLQ and PLE).

The POLFS landscape becomes active in IRE11 in this phase. In the event of a DR scenario for POL-FS, the production system will be hosted in the IRE19 data centre.

Changes will be required by RMG to redirect traffic towards the HNGX NAT address space specifically for the services moving during Weekend A. POLFS will be running on new servers, with new IP addresses assigned as part of the migration activity when they receive their "HNG-X personality".

8.1.4 POLSAP Convergence

A programme of Fujitsu development work is taking place to transition SAPADS functionality from the existing CSC hosted system to the new Fujitsu hosted SAP system in the HNG-X Data Centres. As well as rationalising the hosting of Post Office SAP systems, this development will rationalise existing interfaces between POL-FS and SAPADS.

Development and testing is taking place on new POLSAP servers in the IRE19 Data Centre. To facilitate Post Office access to these environments, CSC are configuring ePortals for the Development and QA Testing.

At POLSAP Convergence the SAPADS functionality is merged into POL-FS to form the POLSAP Service. Certain reference data and opening balances are migrated, and the user credentials for SAPADS users are migrated to the new system. SAPADS printer definitions will be transferred.

At POLSAP convergence Fujitsu assumes responsibility for all application development and maintenance for the SAP solution. CSC retains management of the ePortal and RMG Wide Area Network used by Post Office users to connect out to the POLSAP environment. The Bootle and Wigan development and QA testing environments are decommissioned and IRE19 hosts the new development and test environments for the converged POLSAP service.

The ePortal will be rationalised by CSC to give a single production portal, pointing at the POLSAP service. Effectively this portal can be based on the POL-FS live system created at Weekend A. The ePortals established during the development and testing phase of POLSAP will be retained after convergence.

8.2 Interface Characteristics

The following interface characteristics are explicitly declared:

1. Physical: The provision by POL of additional rack space, power and environment for HNG-X hardware at NDC, LTC and Maidstone.

2. Network: The allocation of new LAN and subnet details outside of the Horizon addressing. FS will provide new WAN infrastructure paths separate from Horizon. As the Horizon infrastructure and HNG-X are separate from a deployment perspective, traffic for one system cannot be passed across the other system interface.

8.3 Post-Migration

Once migration has successfully concluded, decommissioning of obsolete infrastructure will be scheduled jointly.

9 Testing

Testing of Production application services and platforms is "Business As Usual" and requires a permanently built infrastructure to support testing. Several Testing Rigs exist and reside at IRE19. These platforms will be utilised continuously to carry out application testing. However, only the Release Verification Accreditation Rig requires end-to-end network connectivity between the RMG and HNG-X Networks. The following applications would be tested end-to-end between the RMG network and the HNG-X network:

- POLFS and subsequently POLSAP
- SAPADS (until POLSAP convergence)
- EDG
- TIP
- APOP
- TES
- E-Portal/ Citrix
- Track and Trace via SOAP

All test traffic will share the tunnel between IRE19 and the secondary remote router at NDC. A dedicated NAT Space and IP address range will be used to isolate the test traffic from the Production traffic. Even though the traffic flows traverse the same IP network, on each side of the network, their destinations are separate platforms. The RMG network supports a dedicated test server platform and at IRE19, the RV Accreditation Rig is isolated from the production platform. The test POLFS platform is discrete and resides on Pathfinder. The table below is a list of required test interfaces between RMG and HNG-X:

From	To	Transfer Mechanism 1	Requirements/Comments
SAPADS	POL FS	TIP	RMG to run job to create POL FS file and transfer file to HNG-X test Gateway (TIP Remote) for onward transfer to POL FS Requirement ends with POLSAP Convergence
POL FS	SAPADS	TIP	FS to transfer file to HNG-X test gateway, ready for processing by SAPADS, for onward pick up by RMG Requirement ends with POLSAP Convergence
E-Portal	POL FS	Online	Continued access to test instances of POL FS in Wigan and Bootle through E-Portal and run user transactions Requirement ends with POLSAP Convergence
E-Portal	POLSAP	Online	Access to test instances of POLSAP in IRE19
TES Reports	TIP	POL Gateway	Files transferred automatically from HNG-X test gateway to POL Gateway (CS ID)
APOP	TIP	EDG	Files transferred automatically from HNG-X test gateway to POL Gateway
SAPADS	LFS	TIP	Files transferred automatically from HNG-X test

			gateway to POL Gateway Requirement ends with POLSAP Convergence
LFS	SAPADS	TIP	Files transferred automatically from POL Gateway to HNG-X test gateway Requirement ends with POLSAP Convergence
Track and Trace Messages to Royal Mail/Parcel force	SOAP over TCP	EDG	Files transferred automatically from HNG-X test gateway to RMG test EDG

Table 13: Equipment Environmental Requirements

As shown in the table above, several of the transfer mechanisms use FTMS gateways. For the testing platform, the FTMS remote gateways will be located at IRE19, instead of placing them at the remote RMG data centres.

A Detailed Configuration

A.1 Production System NAT Address Allocation

Servers	NDC	LTC	Maidstone
IRRELEVANT			

B.1 System Addresses and Ports

HNGX Logical						
Description	Network address	Mask address	VLAN ID - Access or Trunking	Routing protocols	Host address	HSRP/VRRP/ VIP
NDC Subnet Information						
IRRELEVANT						
LTC Subnet Information						
IRRELEVANT						
Maidstone Subnet Information						
IRRELEVANT						
Production – NDC						
IRRELEVANT						
Production – LTC						
IRRELEVANT						
Production – Maidstone						
IRRELEVANT						

C.1 RMG Hosts and IP Addresses for NDC, LTC & Maidstone

RMG Host Names - NDC	RMG IP Addresses
IRRELEVANT	

FUJ00002230

IRRELEVANT

IRRELEVANT

IRRELEVANT

FUJ00002230

IRRELEVANT

RMG Host Names - LTC	RMG IP Addresses
IRRELEVANT	

Host Names	RMG IP Addresses

IRRELEVANT

D.1 POLFS/POLSAP Ports

The ports listed below are ports via which e-portal clients (sap-users) talk to the SAP Applications Servers hosted at IRE11 & IRE19. They will be allowed through the FS Firewall and defined on all the SAP Servers (Production, Development & Test Platforms)

IRRELEVANT

Enterprise Portal Development (UMD and IPD)

Enterprise Portal Production (UMP and IPP)

IRRELEVANT

Enterprise Portal Development 2 (UMC and IPC)

IRRELEVANT

IRRELEVANT

Enterprise Portal QA 2 (UMA and IPA)

IRRELEVANT

Sections D.1 and E.1 list the hardware and environment specification at all RMG data centre sites.

E.1 Hardware

Owner	Part No	Description	Qty
Fujitsu Services	Cisco 2851	Integrated services router with AC power, 2GE, 1 NME, 4 HWICs, 2 3VDM slots, 2 AIMs, and Cisco IOS IP Base Software	2
Fujitsu Services	WS-C2960-24TT-L	24 Ethernet 10/100 ports and 2 fixed Ethernet 10/100/1000 uplink ports	2
Fujitsu Services	RX300	Rack mountable server 19" (2U), Power Supply Module 600W (hot plug)	4

Table 14: Component List at NDC

Owner	Part No	Description	Qty
Fujitsu Services	Cisco2811	Integrated services router with AC power, 2FE, 1 NME, 4 HWICs, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software	1
Fujitsu Services	WS-C2960-24TT-L	24 Ethernet 10/100 ports and 2 fixed Ethernet 10/100/1000 uplink ports	1
Fujitsu Services	RX300	Rack mountable server 19" (2U), Power Supply Module 600W (hot plug)	1

Table 15: Component List at LTC

Owner	Part No	Description	Qty
Fujitsu Services	Cisco2811	Integrated services router with AC power, 2FE, 1 NME, 4 HWICs, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software	1
Fujitsu Services	WS-C2960-24TT-L	24 Ethernet 10/100 ports and 2 fixed Ethernet 10/100/1000 uplink ports	1
Fujitsu Services	RX300	Rack mountable server 19" (2U), Power Supply Module 600W (hot plug)	1

Table 16: Component List at Maidstone

Owner	Model	Interfaces	Function	Supported Media
Fujitsu Services	Cisco 2811	2 x Ethernet 10/100	Transit Router	10/100BaseT
Fujitsu Services	Cisco Catalyst WS-C2960-24TT-L	24 x Ethernet 10/100 2 x Ethernet 10/100/1000	Transit Switch	10/100BaseT 10/100/1000BaseT
Fujitsu Services	RX300	2 x Ethernet LAN (onboard)	Remote TIP & EDG Servers	10/100/1000BaseT

Table 17: Equipment Capabilities

F.1 Environmental Specification

Owner	Platform	Power (Watts)	BTU/Hr	Weight (KG)	Rack Unit	Dimensions H x W x D in CM
Fujitsu Services	Cisco 2811	170	580	6.4	1	4.45 x 43.8 x 41.66
Fujitsu Services	Cisco 2851	280	955	11.5	2	88.9 x 438.2 x 416.6
Fujitsu Services	Cisco Catalyst WS-C2960-24TT-L	30	103	3.6	1	4.4 x 44.5 x 23.6
Fujitsu Services	RX300	600	2324	25	2	8.6 x 48.3 x 78.5

Table 18: Equipment Environmental Requirements

G.1 WAN Interface Utilisation and Availability

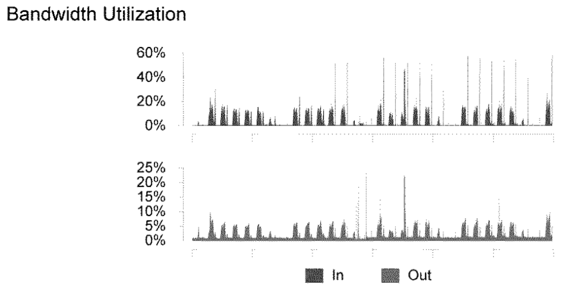

Figure 11: Bandwidth Utilization for Fujer-Huthwaite-a646-r22-001-wan0

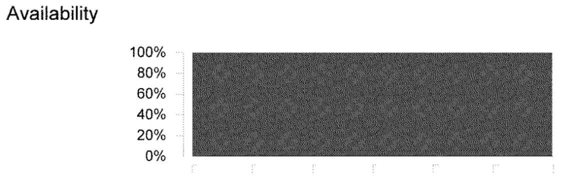

Figure 12: Bandwidth Availability for Fujer-Huthwaite-a646-r22-001-wan0

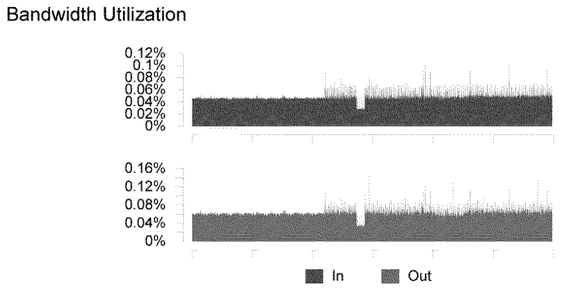

Figure 13: Bandwidth Utilization for Fujer-Huthwaite-a646-r22-002-wan0

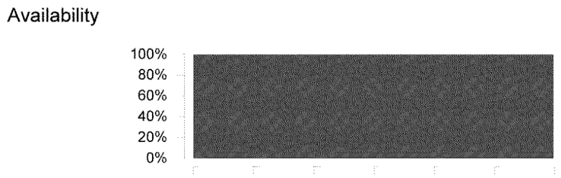

Figure 14: Bandwidth Availability for Fujer-Huthwaite-a646-r22-002-wan0

H.1 POLFS/POLSAP Interfaces

FROM	TO	INTERFACE NAME	MECHANISM
SAPADS	POL-FS	Cash Ledger Entry (CLE)	FTMS
POLFS	SAPADS	Cash-in-Pouch (CIP)	FTMS
SAPADS	TransTrack	Master/Transaction Data	SAP Business Connector
SAPADS	TransTrack	Pouch and Coin Data	SAP Business Connector
SAPADS	TransTrack	Routes Performed	SAP Business Connector
Notes Counting Machine	SAPADS	Notes Counting Results	XI from POLSAP
WCS	POL-FS	Secure Stock Movements	FTMS
RDS	POL-FS	Product Data (Articles)	FTMS
RDS	POL-FS	Branch Data	FTMS
RDS	POL-FS	Customer Data	FTMS
RDS	POL-FS	Vendor Data (Suppliers)	FTMS

POL-FS		GL Accounts	FTMS
Camelot	POL-FS	Client Actuals	FTMS
EDS Cheques	POL-FS	Client Actuals (Cheques Inbound)	FTMS
EDS Personal Banking	POL-FS	Client Actuals (Personal Banking)	FTMS
Moneygram	POL-FS	Client Actuals (Moneygram)	FTMS
Sodexho	POL-FS	Client Actuals (Sodexho)	FTMS
POL-FS	Alliance & Leicester	Transaction Summary (Alliance & Leicester)	FTMS
POL-FS	Horizon	Transaction Corrections	NFS share
Horizon	POL-FS	Branch Level Entry Data (BLE)	NFS share
POL-FS	BACS	Outbound Processing (BACS)	FTMS
FRTS	POL-FS	Pre-orders and Travellers Cheques (First Rate Travel Service)	FTMS
Bank Machines ATM	POL-FS	Client Actuals (Bank Machines ATM)	FTMS
TRM ATM	POL-FS	Client Actuals (TRM ATM)	FTMS
Hanco ATM	POL-FS	Client Actuals (Hanco ATM)	FTMS
Alliance & Leicester ATM	POL-FS	Client Actuals (Alliance & Leicester ATM)	FTMS
POL-FS	NS&I	Transaction Data (National Savings & Investments)	FTMS
Shopping Basket	POL-FS	Shopping Basket sales of Travel Money Cards	FTMS
ETL	POL-FS	POL ETL system sales/ financial postings (via SDI)	NFS share
FRES Spot Rates	POL-FS	Exchange rates used to revalue all currency stock by branch	TBC
POL-FS	Coop	Transaction Data (Co-Op)	TBC