FUJ00088557

Document Title:	HNG-X Wide Area Network HLD
Document Type:	High Level Design (HLD)
Release:	Not Applicable
Abstract:	HNG-X Wide Area Network high level design. Provides WAN connectivity for support services and external companies. Excludes branch access connectivity.
Document Status:	APPROVED
Author & Dept:	Stephen Wisedale
Internal Distribution:	As per review details
External Distribution:	As per review details

Approval Authorities:

Name	Role	Signature	Date
Mark Jarosz	Systems Architect		
Pat Lywood	Infrastructure Design		

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

FUJ00088557

0 Document Control

0.1 Table of Contents

FUJ00088557

FUJ00088557

FUJ00088557

0.2 Figures

0.3 Tables

FUJ00088557

0.4 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	18/05/07	First draft	
0.2	05/06/07	Changes identified at team group review	
0.3	07/06/07	Draft for review	
0.4	12/07/07	Complete revision – to use C&W network instead of FSBN	
1.0	09/08/07	For approval	
1.1	16/11/09	Revised to reflect changes during implementation	

0.5 Review Details

Review Comments by :	30/11/09
Review Comments to :	Stephen Wisedale & PostOfficeAccountDocumentManagement GRO

Mandatory Review	
Role	Name
Infrastructure Design	Pat Lywood
Infrastructure Design	Dave Tanner
Infrastructure Design	Dave Haywood
Architect	Mark Jarosz
SSC	Tony Little
Security	Tom Lillywhite
Business Continuity	Adam Parker
SV&I	John Rogers
RVMig	Graham Jennings

Optional Review	
Role	Name
Security & Risk Team	CSPOA.Security GRO
Programme Manager	Alan D'Alvarez
Applications Architecture	David Johns
System Qualities Architecture	Dave Chapman
Architect	Jason Clark
Security Architect	Jim Sweeting
Test Design	George Zolkiewka
Head of Service Management	Gaetan van Achte
Head of Service Change & Transition	Graham Welsh

FUJ00088557

Service Support	Kirsty Gallacher
Service Network	Ian Mills
Data Centre Migration	Geoff Butts
Integration Team Manager	Peter Okely
Testing Manager	Debbie Richardson
SV&I Manager	Sheila Bamber
Tester	Hamish Munro
RV Manager	James Brett (POL, JTT)
POL Design Authority	Ian Trundell (POL, via Document Control)
VI & TE Manager	Mark Ascott
Integrity Testing	Alan Child
Integrity Testing	Michael Welch
Core Services	Ed Ashford
Core Services	Andrew Gibson
Business Architect	Gareth Jenkins
Development	Graham Allen
Solution Design Architect	Sarah Selwyn
Software & Solution Design Developer	Stuart Honey
Service Manager - Retail and RMGA	Claire Drake
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

(*) = Reviewers that returned comments

0.6 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	1.0	13/6/06	Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
ARC/NET/ARC/0001	V0.7	04/10/07	HNG-X Technical Network Architecture	Dimensions
ARC/SEC/ARC/0003	V2.0	08/01/09	HNG-X Technical Security Architecture	Dimensions
DES/NET/HLD/0008	V1.2	13/11/08	Data Centre LAN Design	Dimensions
DES/NET/HLD/0010	V0.11	12/06/09	Branch Router Network High Level Design	Dimensions
DES/NET/HLD/0014	V2.0	28/07/08	Branch Access HLD	Dimensions

FUJ00088557

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

0.7 Abbreviations

Abbreviation	Definition
A&L	Alliance and Leicester plc
AAQ	Advanced Application QoS
AES	Advanced Encryption Standard
AF	Assured Forwarding
AS	Autonomous System (BGP)
ASA	Adaptive Security Appliances™ (Cisco Systems inc)
BGP	Border Gateway Protocol (routing protocol)
BRA01	Fujitsu site: Bracknell 01
BTL01	Fujitsu site: Bootle 01
C&W	Cable and Wireless plc
CAPO	Card Account at Post Office
CE	Customer Edge [router] (MPLS)
CIS	Corporate Information Services
CPE	Customer Premises Equipment
DC	Data Centre
DMZ	Demilitarised Zone
DN	Design Note
DR	Disaster Recovery
DSCP	Diff(erentiated) Services Code Point
DVLA	Driver and Vehicle Licensing Agency
DWDM	Dense Wave Division Multiplexing
EBGP	Exterior Border Gateway Protocol
EF	Expedited Forwarding
FSBN	Fujitsu Services Backbone Network
GRE	Generic Routing Encapsulation
HLD	High Level Design
HSD	Horizon System Helpdesk
HSRP	Hot Standby Routing Protocol (proprietary protocol - Cisco Systems inc)

FUJ00088557

IBGP	Interior Border Gateway Protocol
IGP	Interior Gateway Protocol (e.g. OSPF)
IMS	Management Information Services
IP	Internet Protocol
IP/MPLS	Internet Protocol/Multi Protocol Label Switching
IPsec	IP Secure
IRE11 / IRE19	Fujitsu site: Ireland 11 and Ireland 19
ISDN	Integrated Services Digital Network
L2VPN	Layer 2 Virtual Private Network (includes Pseudowire, PWE3, draft Martini & VPLS)
L3VPN	Layer 3 Virtual Private Network (RFC2547bis)
LAN	Local Area Network
LLD	Low Level Design
MED	Multi Exit Discriminator (BGP)
MIS	Management Information Services
MPLS	Multi Protocol Label Switching
MSFC	Multi-layer Switch Feature Card™ (Cisco Systems inc)
NAT	Network Address Translation
NTP	Network Timing Protocol
OCMS	Operational Change Management System
OSPF	Open Shortest Path First (routing protocol)
PE	Provider Edge [router] (MPLS)
POP	Point of presence
QoS	Quality of Service
RDT	Reference Data Team
RMG	Royal Mail Group
RMGA	Royal Mail Group Account
SAN	Storage Area Network
SAS	Secure Access Server
SDC01	Fujitsu site: Southern Data Centre 01
SNMPv3	Simple Network Management Protocol version 3
SSC	System Support Centre
SSHv2	Secure Shell version 2
SSL	Secure Sockets Layer
STE04 / STE09	Fujitsu site: Stevenage 04 and Stevenage 09
TCY01 / TCY02	Fujitsu site: Telecity 01 and Telecity 02 (TelecityRedbus group – collocation sites)
VLAN	Virtual Local Area Network
VPLS	Virtual Private LAN service

FUJ00088557

VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WGN01	Fujitsu site: Wigan 01
WWW	World Wide Web (Internet)

0.8 Glossary

Term	Definition
802.1q	IEEE standard for VLAN encapsulation (VLAN trunking)

0.9 Changes Expected

Changes

0.10 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.

0.11 Copyright

FUJ00088557

1 Introduction

1.1 Purpose of document

This document describes the Wide Area Network for HNG-X. The document describes the target design with connectivity to two new data centres in Northern Ireland, and considers parallel operation and inter-connection with the existing Horizon network. The document covers access for support locations and for external connections but specifically excludes the branch access network.

1.2 Readership

This document is intended for design and operational staff involved with low-level design, implementation and operation of WAN platforms or the development of service-specific solutions across the WAN. The document may also prove useful for anyone that requires a high-level appreciation of the WAN for HNG-X.

1.3 Scope

- WAN HLD will include wide area network capability in support of:
  - External client connections
  - Fujitsu support networks
  - Test environment
  - Inter-DC WAN (WGN01/BTL01 – IRE11/19 via C&W IP Select)
  - Migration

- WAN HLD will specifically EXCLUDE:
  - Branch Access Network HLD (WAN) – documented separately
  - Inter-DC LAN and SAN interlinks (IRE11 – IRE19 via dedicated DWDM) – documented separately
  - Data Centre LANs
  - Support centre LANs
  - External client LANs

1.4 Assumptions

VLANs provide adequate separation for differing traffic types and services.

The geographic extent of support access within Fujitsu Services is limited to the following sites:

- Bracknell BRA01
- Lewes LEW02
- Stevenage STE04
- Crewe CRE02

FUJ00088557

- Wigan WGN01
- Warrington WAR13
- Ireland IRE11
- Ireland IRE19
- Solihull SOL02

1.5 Risks

Resilience at IRE11 and IRE19 is provided through triangulation between sites. Diverse fibre routes will be used for the DWDM service between the sites. There is a risk of a dual failure impacting the active site if minimum spatial separation requirements are not adhered to.

1.6 Dependencies

FUJ00088557

2 Overview

The purpose of the Wide Area Network (WAN) is to provide connectivity for external clients, test rigs and support access, along with inter-data centre connectivity for four data centre operation. This document specifically excludes branch access which is the subject of a dedicated HLD (DES/NET/HLD/0014). Also excluded is inter-data centre connectivity between the two Northern Ireland data centres as this is included in the LAN HLD (DES/NET/HLD/0008).

The following diagram, taken from the Technical Network Architecture document (ARC/NET/ARC/0001), provides a high-level view of the relationship of the WAN to other network areas.

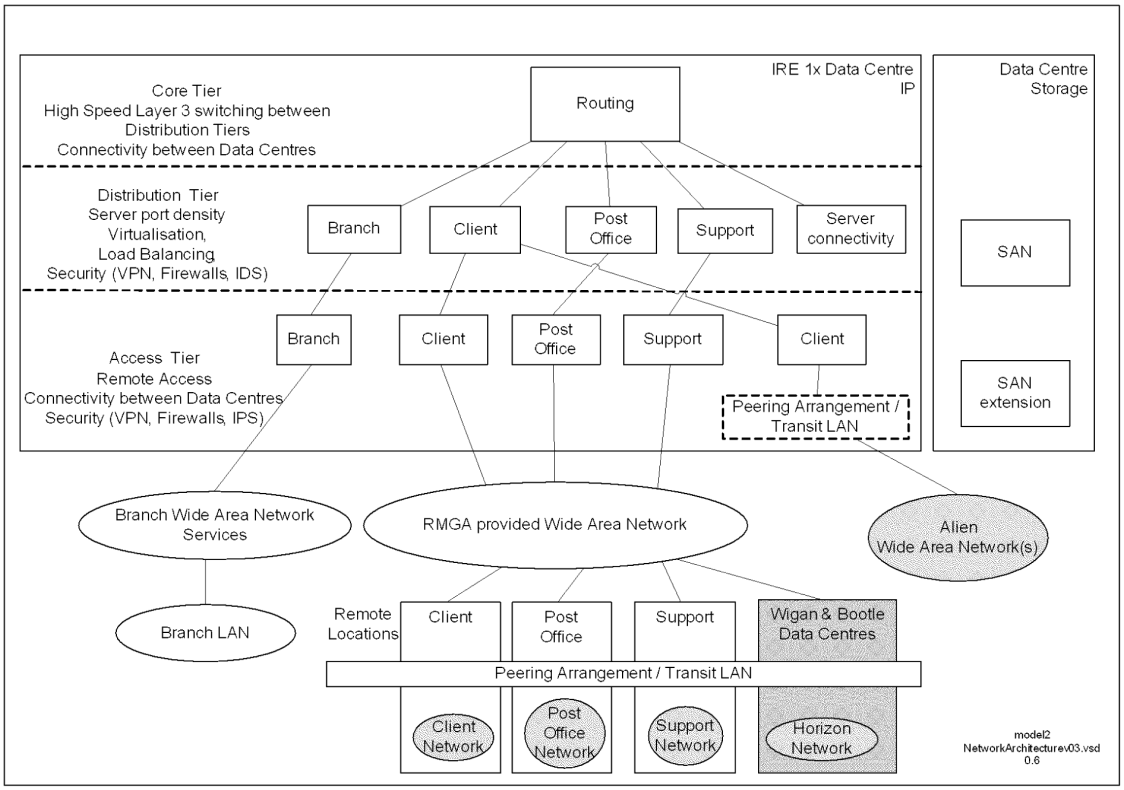

Figure 1 Network Architecture

The existing Wide Area Network serving the Wigan and Bootle data centres makes extensive use of layer 3 VPNs (L3VPNs) from Cable and Wireless. These VPNs will be extended to include the new data centres for HNG-X. The two new data centres in Northern Ireland, IRE11 and IRE19, operate in an active/DR relationship, although the network, particularly the WAN access tier, operates in an active/active manner. In addition to operating in a four data centre configuration for the period of migration, the network will need to support the dual running of Horizon with HNG-X as branches are migrated across.

This document considers the target design, and an interim design to allow for four data centre operation, along with migration towards the target design.

FUJ00088557

2.1 Cable and Wireless WAN

The WAN solution is based on the continued use of C&W for the WAN. C&W provide the RMGA account with multiple MPLS layer 3 VPNs over which RMGA will build secure connectivity using IPSec encrypted GRE tunnels as described later in this document.

2.2 Live branch access

Live branch access will continue to use the current live VPN which will be extended to include the new data centres; IRE11 and IRE19. Branch access is described in the Branch Access HLD (DES/NET/HLD/0014).

2.3 Support connectivity

Regional connectivity to the new IRE11 an IRE19 data centres is required from the following sites. These are Fujitsu Services sites and the access is provided for Fujitsu Services staff to fulfil operational and support roles. Access to IRE11 and IRE19 for all of these sites will be provided via a common 'RMGA' VPN on the C&W network.

- Bracknell BRA01
- Lewes LEW02 – backup for BRA01 (test facilities and SSC DR)
- Stevenage STE04
- Crewe CRE02
- Wigan WGN01
- Warrington WAR13 – new site for Support teams moving from WGN01 and BTL01
- Ireland IRE11
- Ireland IRE19

[1] Current practice is that all firewall connectivity is managed by RMGA. Where corporate firewalls are used then a set of SLA/OLA's need to be put in place to ensure RMGA meet their ISO 27001 contractual obligations.

FUJ00088557

2.4 Test connectivity

New test rigs will be constructed in IRE19 (LST, ST, RV Mig, SV&I and RV Acc.), Unlike Horizon, where dedicated C&W VPNs are provided per rig, HNG-X test counter WAN connectivity will comprise a single new 'test' VPN presented at BRA01, SDC01, TCY02, IRE11 and IRE19 sites. Inter data centre connectivity for test rigs will be provided using dedicated IPSec/GRE tunnels over the Support VPN as used in section 2.3.

2.5 External connectivity

The following external companies have WAN connectivity to Wigan and Bootle extended to include IRE11 and IRE19.

- Post Office Limited (RMG)
- DVLA
- Alliance and Leicester
- CAPO (provided by EDS)
- E-pay
- VocaLink
- Streamline
- MoneyGram International.

The following table summarises the services and connectivity requirements for external organisations:

FUJ00088557

Client	Service	Location	Primary/ Secondary (DR) site	WAN provision	WAN link ownership/ management	CPE ownership/ management	WAN HLD: in/out of scope ?
Post Office Limited	Multiple applications (run by CSC)	Huthwaite	Dual primary	C&W IP Connect Direct	RMGA	RMGA	IN
Post Office Limited	Multiple applications (run by CSC)	Hounslow (Sungard)	DR	C&W IP Connect Direct	RMGA	RMGA	IN
Post Office Limited	EDG (DR) (run by CSC)	Maidstone	DR	C&W IP Connect Direct	RMGA	RMGA	IN
DVLA	n/a	Morriston, Swansea	Dual primary	C&W IP Connect Direct	RMGA	RMGA	IN
DVLA	n/a	Swansea Vale	Dual primary	C&W IP Connect Direct	RMGA	RMGA	IN
Alliance & Leicester	Network Banking	Carlton Park, Leicester	Primary	C&W IP Connect Direct	RMGA	RMGA	IN
Alliance & Leicester	Network Banking	Bootle	Secondary (DR)	C&W IP Connect Direct	RMGA	RMGA	IN
CAPO	Network Banking	Doxford	Primary	C&W IP Connect Direct	EDS	EDS	OUT[2]
CAPO	Network Banking	Washington	Secondary (DR)	C&W IP Connect Direct	EDS	EDS	OUT
E-pay	Electronic Top-up (mobile phones)	Kelting House, Basildon	Primary	C&W IP Connect Direct	RMGA	RMGA	IN
E-pay	Electronic Top-up (mobile phones)	Hornsby Sq, Basildon	Secondary (DR)	C&W IP Connect Direct	RMGA	RMGA	IN
VocaLink	Network	Harrogate	Primary	MPLS	VocaLink	VocaLink	OUT

[2] The WAN connectivity is out-of-scope as it is owned by EDS.

FUJ00088557

	Banking						
VocaLink	Network Banking	Leeds	Secondary (DR)	MPLS	VocaLink	VocaLink	OUT
Streamline	Debit card (online transactions)			X.25	RMGA	Streamline	IN
Streamline	Debit card (file transfer)			ISDN2e	RMGA	Streamline	IN
MoneyGram Intl.	Money transfer	Minneapolis, USA		Frame relay	MoneyGram	MoneyGram	OUT
MoneyGram Intl.	Money transfer (backup)	Minneapolis, USA		ISDN2e	RMGA (local end only – not encryption)	RMGA	IN
MoneyGram Intl.	Money transfer (test access)	Minneapolis, USA		Internet access (from BRA01[3]	RMGA (local access only – not encryption)	RMGA	IN

Table 1 External connections

Those sites shown as out-of-scope for this document will be subject to client specific LLD and TIS documents developed with the individual organisations.

In addition to the principal external connections above, there may be a requirement for miscellaneous dial access and/or Internet access for the following:

- EMC – dial access for remote diagnostics
- Fujitsu-Siemens – dial access for remote diagnostics (Bladeframes)
- Alarmpoint - PSTN dial-out from data centres to SMC
- Outlet file feed to STE14 – requirement TBD

2.6 Inter-DC connectivity

Inter-DC connectivity (WGN01/BTL01 to IRE11/19) will be achieved using IPSec/GRE tunnels over the Support VPN.

[3] Internet access for MoneyGram Intl. will migrate to the proposed RMGA Internet Access solution when available (for test rig access only).

FUJ00088557

3 Requirements

This document is based on requirements as described in the Technical Network Architecture and Technical Security Architecture documents, along with support and test access requirements as provided by individual support and test teams as described in the relevant sections.

All traffic is required to be encrypted across the WAN. Encryption will be provided by either the network, using IPSec encrypted GRE tunnels, or at a session level using SSL[4]. RMGA are only responsible for the encryption of traffic across devices under its control, and therefore excludes encryption of traffic for MoneyGram Intl., CAPO, and other clients that provide their own WAN connectivity.

[4] SSL encryption will only be used for HNG-X counter application encryption as described in the Branch Access HLD (DES/NET/HLD/0014).

FUJ00088557

4 Design

The general approach for the Wide Area Network is to extend the current Cable and Wireless WAN to include the new data centres in Northern Ireland. The network makes use of L3VPNs (RFC2547bis) between all sites (C&W IP Connect service). Access to the data centres will follow one of two basic approaches:

- VPNs will present to a directly connected handoff routers managed by RMGA within each site. IPSec encrypted GRE tunnels will be used to carry encrypted traffic across the C&W provided VPNs. This approach will be used for support users and external clients that use C&W VPNs.
- VPNs will redistribute into OSPF at the CE router for routing to the access platforms. Traffic will be encrypted within the application and do not require tunnels across the C&W VPNs. This approach will be used for branch access which is outside of the scope of this document (see DES/NET/HLD/0014) but covered here for Test access.

The handoff routers, where used, will be low-end Cisco devices and will be deployed on a router per VPN basis (VRFs may be used in some circumstances such as support for test LANs). Encryption will be AES256 unless otherwise defined.

Note that C&W impose a limitation of 30 VPNs maximum on each of the CE routers at IRE11 and IRE19.

There are several external clients that require connectivity but do not use C&W VPNs and will be described separately, where the connectivity is owned and managed by RMGA.

4.1 Target Design

The target design has all services that are currently provided by the C&W IP Select network extended to include the two new data centres in Northern Ireland.

The Horizon data centres at Wigan and Bootle operate in an active/active configuration. For HNG-X however, the two new data centres in Northern Ireland will operate in an active/DR manner, with IRE11 as the normally active site. IRE19 will be used as a test facility under non-DR conditions. Although applications and services from the data centres will operate as active/DR, the network will operate active/active at all times.

Live traffic will be steered towards IRE11 under normal circumstances using BGP attributes. The local CE router (and handoff router) will be preferred, and the path will be deterministic. Traffic will not be load balanced across parallel paths. Test traffic will be steered towards IRE19 in a similar manner. Traffic shaping will be provided to ensure that high volume test traffic does not adversely impact live traffic. This is particularly important for VPNs terminating in SDC01/TCY01. Support staff will have connectivity to either site.

Failure of data centre WAN equipment on the preferred path (local CE and/or local Handoff router) will result in traffic re-routing via the equivalent router in IRE19 and the intercampus LAN. Failover will be dynamic with convergence dependent on the routing protocol in use.

Invocation of DR is a manual process that will take up to two hours to conclude. Network failover to DR does not need to be dynamic and will use scripting wherever possible to manage the changeover.

Note that the WAN design is based on Layer 3 connectivity in all cases. Layer 2 connectivity, including Pseudowire (draft Martini L2VPN) and VPLS, is NOT supported by this network.

Connectivity to the new data centres is covered in the following sub-sections:

FUJ00088557

4.1.1 Support access

Support access has two forms:

- Access from RMGA workstations on dedicated RMGA LANs (also known as Red LAN).
- Access from Corporate LAN connected workstations.

Both access requirements will be met using a single C&W VPN. The Support VPN will be extended to include the IRE11 and IRE19 data centres, along with any new sites introduced for HNG-X, over which connectivity will be provided using dedicated IPSec encrypted GRE tunnels. Corporate LAN access will traverse back-to-back firewalls at each end and all addresses between RMGA and Corporate will be NAT translated.

4.1.2 Test counter access

Test counter access is the only requirement within the scope of this document to follow the branch access model and does not require handoff routers. A single new C&W VPN will be used for test counter connectivity.

FUJ00088557

4.1.3 External Client access

The following diagram describes access for external clients via the C&W network. In all four cases, RMGA managed CPE routers are installed, and RMGA are responsible for WAN connectivity. Each client will have its own dedicated C&W VPN that will be presented as a VRF on the IRE11 and IRE19 CE routers. In turn, this will be presented to dedicated handoff routers within the Access LAN via a dedicated VLAN.

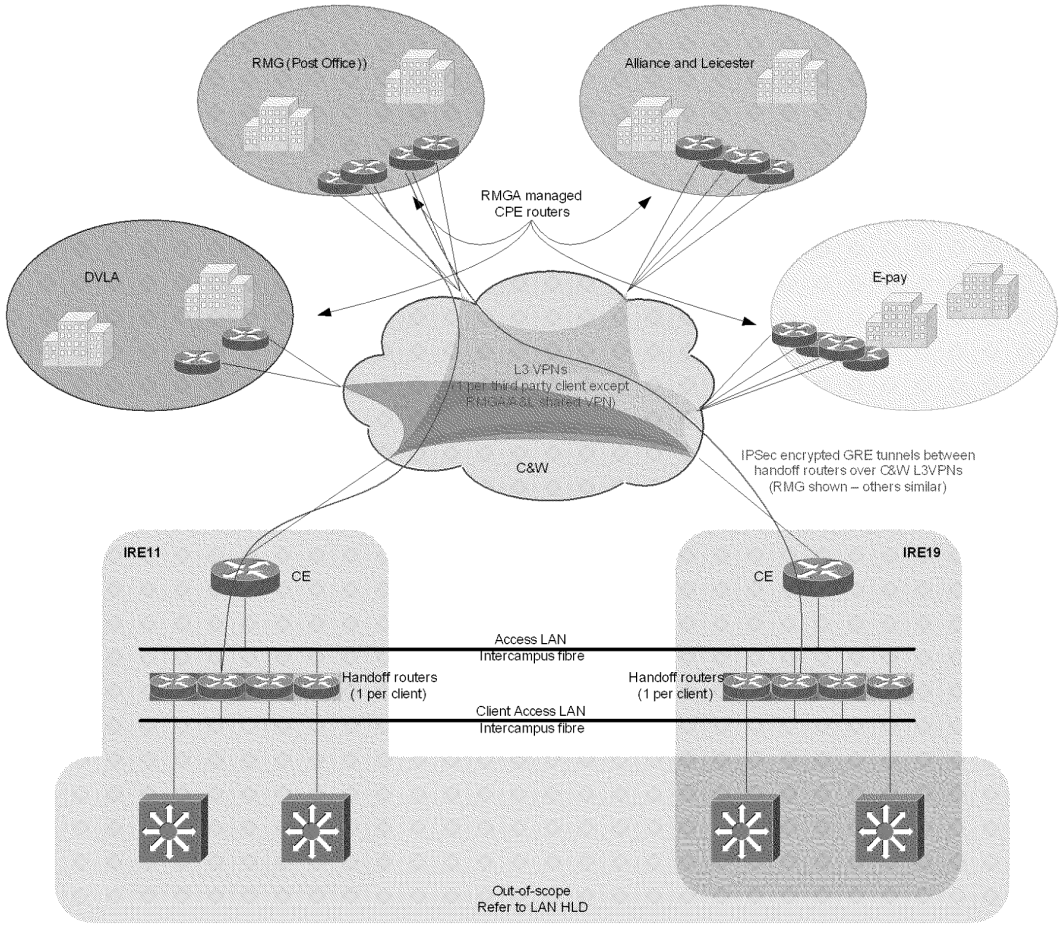

Figure 4 Target design – External access via C&W

FUJ00088557

4.1.4 Non-C&W connectivity

The following diagram shows WAN connectivity for those third parties that do not use C&W VPNs for access. Of these companies, Streamline is the only client for which RMGA is responsible for WAN connectivity, requiring X.25 and ISDN access. All of the others are out-of-scope for this HLD.

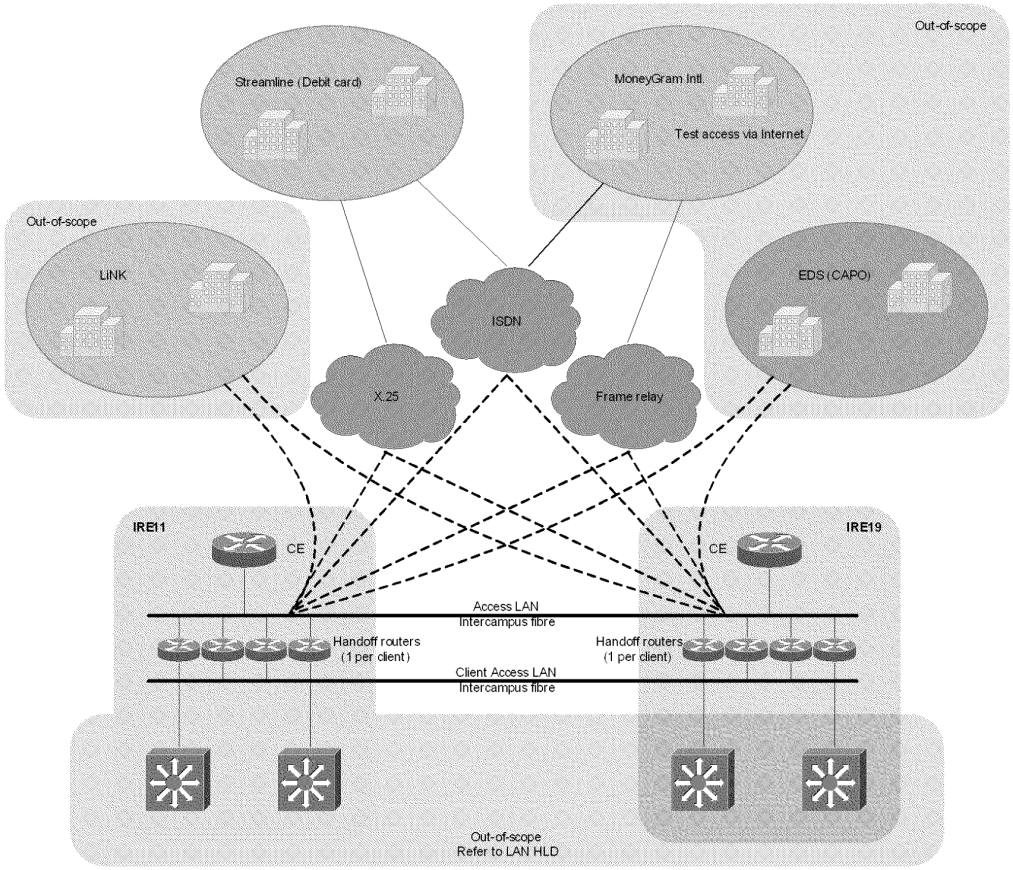

Figure 5 Target design – Non-C&W external clients

4.1.5 Clarification of handoff router LLD design responsibility

The WAN LLD will identify all handoff router requirements in the IRE11/19 data centres and provides a template configuration to enable deployment to a state where the device can be managed. The WAN LLD does not include VPN termination and IPSec/GRE tunnel configuration for handoff routers.

The individual component LLDs will arrange deployment of remote handoff routers (along with C&W CE routers where necessary), and will determine the configuration for VPN termination along with IPSec/GRE tunnels at each end. The component LLD will also define the creation or extension of the associated C&W VPN to include IRE11 and IRE19 data centres, and will include management connectivity to the remote site.

FUJ00088557

4.2 Access classes

There are four access classes:

Model	Service
Handoff router	RMG, E-pay, Alliance & Leicester, DVLA, RMGA-Horizon, RMGA LAN, CIS, IMS and Remote access via firewalls
Non-handoff router	Branch Access (out-of-scope for WAN HLD), Test rig connectivity
Special	Debit card (Streamline) and MoneyGram Intl.
Out-of-scope	CAPO, VocaLink, MoneyGram Intl.

Table 2 Access classes

4.3 Data Centre WAN presentation

The data centre WAN presentation utilises a single C&W CE router at each site. The CE router is owned and managed by C&W. Each CE router has two LAN interfaces, one to each of the two Cisco 6513 WAN access switches at each site. Each VPN is presented as a VRF on the CE router, and sub-interfaces/VLANs on both LAN interfaces are present within each VRF. Resilience will be achieved through triangulation with the CE router at the other data centre via common VLANs between the sites.

For support access and external connections, dedicated Cisco 2811 'handoff' routers will be used. Individual routers for each service (one per external connection) will be installed at each data centre (RMGA Red LAN and Corporate access will share the same handoff routers and C&W VPN). Resilience will be achieved through triangulation with the equivalent service-specific handoff router at the other data centre via common VLANs. The handoff routers will be used for IPSec/GRE tunnel termination, and OSPF will be used for client traffic towards the ASA firewalls. In most cases, traffic will be encrypted within tunnels.

The following diagram shows the data centre physical connectivity for WAN devices within the Access LAN. Note that a single interface is used on the client VLAN side; this is necessary as the ASA firewalls operate in an active/failover configuration that requires the same subnet to be presented. It is not possible to configure the same subnet on two interfaces of the same router.

FUJ00088557

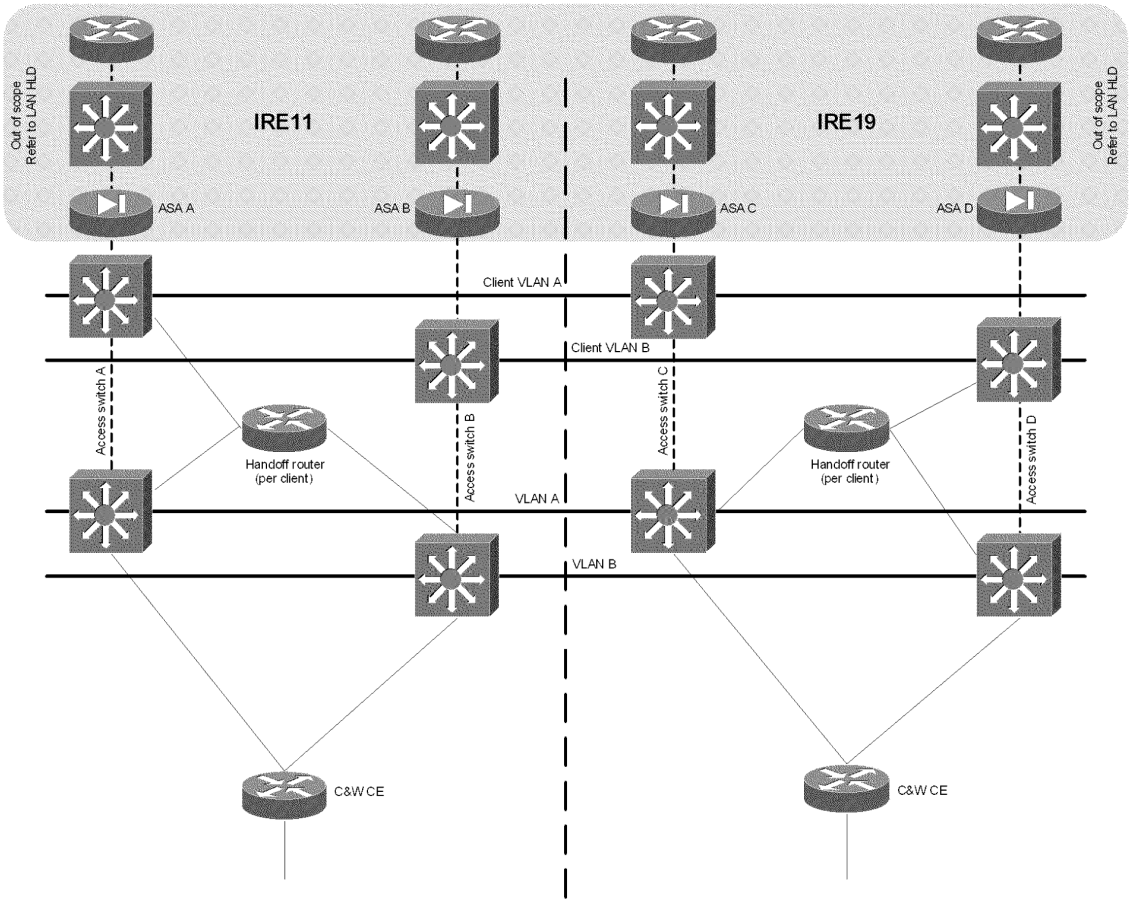

Figure 6 Data Centre Access LAN physical

The handoff routers require a minimum of two LAN interfaces, using sub-interfaces and VLAN separation between the CE side VLAN and the ASA side VLAN.

FUJ00088557

4.4 Routing

Routing within the WAN is dynamic using BGP. Static routes will be used where necessary to resolve indirect next-hops. OSPF will be used within the data centre, and (where necessary) for routing across tunnels to remote sites regardless of whether the remotes sites are internal or external organisations.

The target solution provides common VLANs between IRE11 and IRE19 at the Access LAN layer as described in the LAN HLD. A single C&W CE router is installed at each data centre and resilience will be achieved via the intercampus LAN and CE at the other site. Although handoff router to CE connections at both sites use the same AS number, IBGP is not be used to establish a neighbour relationship between the sites. All traffic is carried within IPSec encrypted GRE tunnels that terminate on dedicated handoff routers. OSPF metrics will be used to ensure that traffic is forwarded in a deterministic manner, with preference via the local CE router.

Note that the use of MSFCs to provide a layer 3 capability within the Access network is not proposed. This is because the handoff routers are managed and configured by RMGA and provides sufficient layer 3 routing capability for the Access network. Further, the use of MSFCs in this role would result in the mixing of traffic classes at layer 3 that could only be overcome through use of VRF-lite, which would unnecessarily complicate the design.

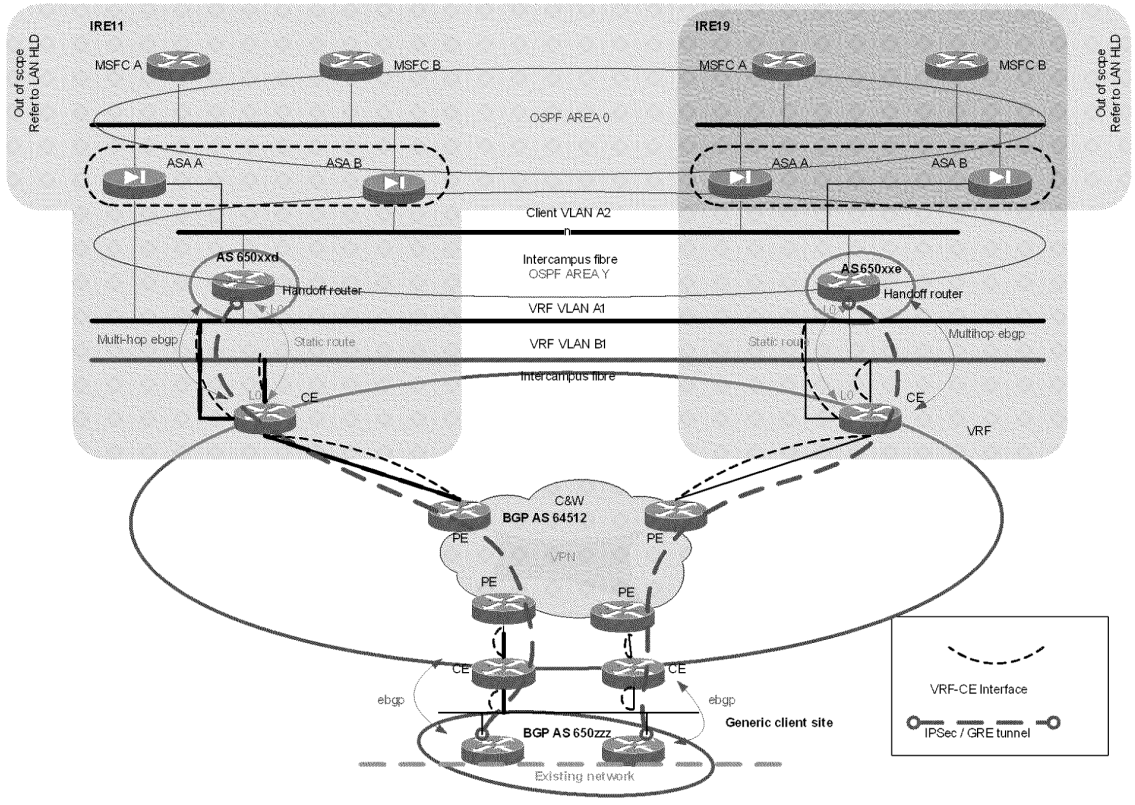

Figure 7 Generic WAN to data centre connectivity

FUJ00088557

Note that for the example above, multi-hop EBGP should be configured between loopback interfaces on the CE and handoff routers, as this allows for the peering to use both local Cisco 6513 switches. If the peering is provided between physical interfaces, loss of the configured interface could lead to an unacceptable requirement for DR invocation. The static route required for multi-hop EBGP should be configured between the local CE and handoff routers only, as shown in the previous diagram.

Metrics will be used to steer traffic towards the appropriate site; IRE11 for live traffic and IRE19 for test. OSPF metrics will be used to steer egress traffic and the BGP attribute, AS-Path pre-pend, is proposed between the CE and handoff router to steer ingress traffic. There is no distinction between active and DR for the BGP peering in this design.

4.4.1 WAN access methods

WAN access across the C&W VPNs can be divided into two distinct methods:

- Support and external access – where traffic is encapsulated within an IPSec or GRE tunnel terminating on dedicated handoff routers within the data centres or on the RMGA managed CPE routers at regional or client sites. This approach will be used for all support access, third party access and inter-DC connectivity.
- Branch access – where native IP traffic enters the Access LAN at the CE router. The C&W CE router will redistribute into OSPF within the VRF serving this traffic. The traffic will be encrypted using SSL. Although this access method is outside of the scope of this document, this approach will be used for test counter access and will be covered here at a high-level.

FUJ00088557

4.5 Internet Access

Connectivity to the Internet is required for the Broadband Web Server. The BWS supports three services: Broadband Checker (the Post Office is to resell consumer broadband through their branches), Postcode Anywhere and Neopost/Kahala. Internet access is also required for software updates, anti-virus updates and for Post Office access to the web server.

Initial Internet access is provided using a single ADSL line at each data centre presented on a Cisco 1801 router at each site. The Cisco 1801 router provides a basic firewall with a second tier of firewalls provided using dedicated Cisco ASA firewalls. This initial solution is non-resilient in operation but provides a Horizon equivalent service.

Within the data centres, all interactive Internet access sessions traverse a Webwasher proxy server.

4.6 C&W CE router consolidation

At BRA01 and LEW02 sites, multiple C&W CE routers were deployed each serving one or more VPNs. It was planned to consolidate the VPNs on to two larger routers providing greater aggregate WAN access bandwidth. In the event, larger routers were installed and the access capacity upgraded to 100Mb/s per router for the support VPN (fujser_fujnwb_test), but no consolidation has taken place; the remaining CE routers will be retained until their associated rig is decommissioned in BRA01.

C&W CE name (VPN_name/s)	Router type	Circuit number	B/wdth	Location
He11-r73-001 (fujser_fujnwb_test)	7301	ISFE2909855	100Mb/s	LG33 Live A rack
He11-r73-002 (fujser_fujnwb_test)	7301	ISFE2910105	100Mb/s	LG33 Live B rack
U064-r28-001 (fujser_fujnwb1 & fujser_fujnwb_bracknell1)	2620	ISA53223	2Mb/s	LAB3 lower ground - FRIACO
U064-r26-002 (fujser_fujnwb1 & fujser_fujnwb_bracknell2)	2620	ISA53743	2Mb/s	6th floor rack 10 – LST
U064-r22-001 (fujser_relrig & fujser_fujnwb1)	2610	ISA2533720	2Mb/s	LG33 - Release rig
U064-r22-002 (fujser_brac_btc)	2610	ISA2533724	2Mb/s	LG33 – BTC rig
U064-r22-003 (fujser_rel_rig & fujser_fujnwb1)	2621	ISA2533725	2Mb/s	LG33 – Backup release rig
U064-r22-004 (fujser_brac-btc)	2621	ISA2533726	2Mb/s	LG33 – Backup BTC rig
Gr33-r16-001 (fujser_lst_btlr)	1721	ISJ2611923	64kb/s	6th floor – LST bootloader

Table 3 C&W BRA01 consolidation

FUJ00088557

4.7 Support networks

4.7.1 Support connectivity

There are two access classes for support staff:

- RMGA LAN model (i.e. RMGA dedicated 'Red' LAN)
- Corporate model (includes Corporate LAN users, remote access via the Corporate LAN and all other non-RMGA LAN internal networks)

In both cases, access to platforms should be via the SAS servers in IRE11 and IRE19. The SAS servers will authenticate users and log activity. There will however, remain cases where certain support staff will require direct access to platforms.

4.7.1.1 RMGA 'Red LAN' access

Regional site access: For access via the RMGA LAN model, support staff will have workstations on a dedicated Post Office LAN known locally as the 'Red' LAN. This will have direct access via the VPN extended to IRE11 and IRE19. Note that all traffic using the RMGA VPN will be carried within IPsec encrypted GRE tunnels. Encryption will be AES256. Tunnels will terminate on RMGA managed handoff routers at the data centres and regional sites. A full mesh of tunnels is not necessary, however sufficient tunnels to provide resilience and to allow inter-site connectivity will be provided.

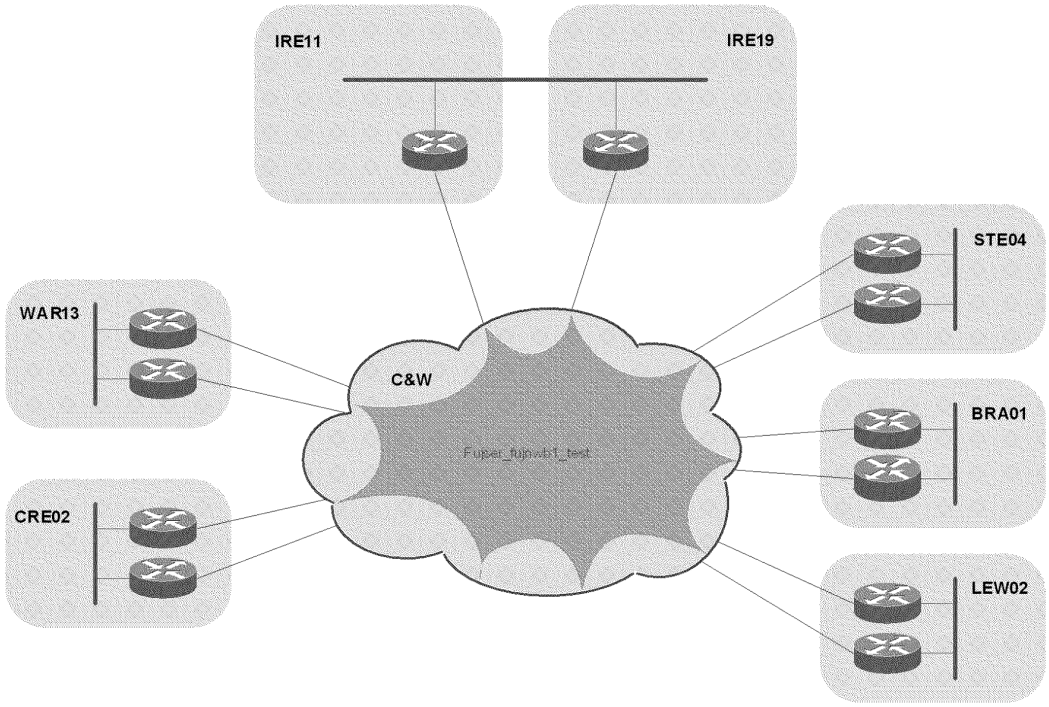

Figure 10 RMGA LAN VPN access

FUJ00088557

4.7.1.2 Corporate LAN access

WAN connectivity for Corporate LAN access is provided over the same 'Support VPN' used for Red LAN access. Interconnection with the corporate network is provided via RMGA-owned/Corporate-managed Checkpoint firewalls at large sites (Bracknell Stevenage and Lewes). Smaller sites will use the corporate WAN to IRE11/19 with Checkpoint firewalls at these sites.

Using the Support VPN for WAN access between BRA01 and IRE11/19 overcomes issues with WAN capacity and performance issues for software distribution from Bracknell.

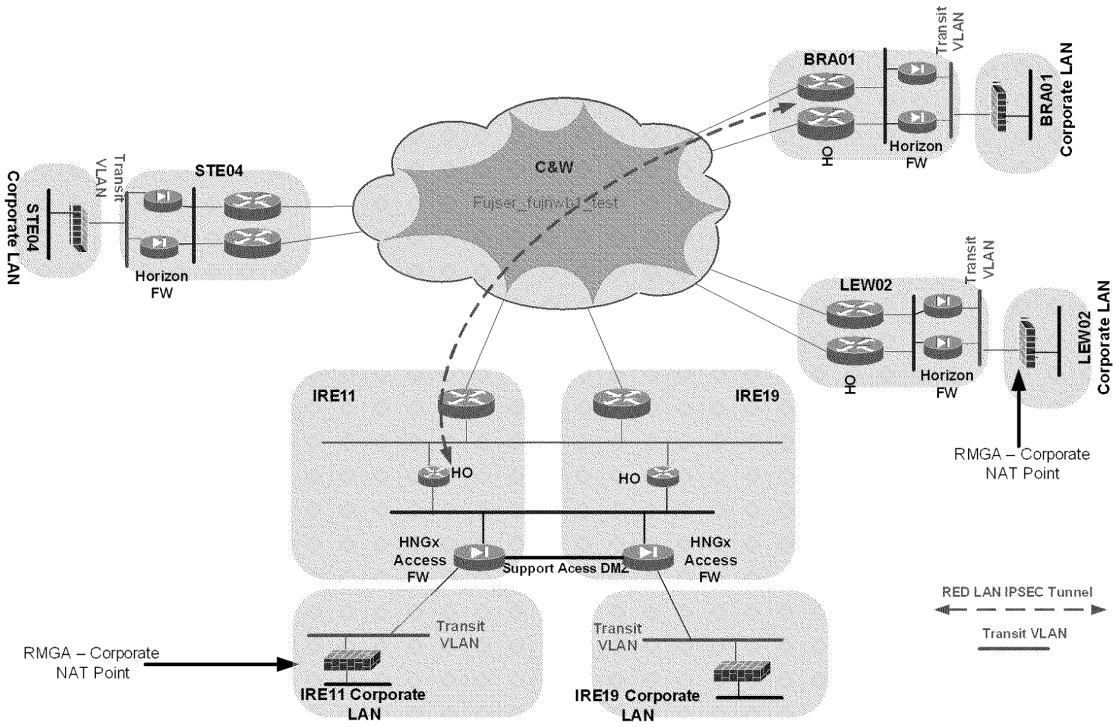

Figure 7 Corporate LAN access

FUJ00088557

4.7.2 Bracknell BRA01

4.7.2.1 SSC

All SSC workstations reside on the RMGA LAN and use hardware encryption. Continued use of the RMGA LAN is required along with provision to access platforms directly as well as via the SAS (SSN) servers.

For out-of-hours access, remote workstation access via Corporate LAN VPN access with a fixed IP address allows routing to the RMGA firewall where RADIUS authentication provides access to the SAS (SSN) servers only. Direct access to platforms not permitted via this method.

4.7.2.2 MIS (Service Delivery team)

MIS at Bracknell have workstations on the corporate LAN that will require access to IRE11 and IRE19. Remote VPN access is also required.

In addition, there are dedicated NT clients for Data warehouse/TES/DRS and Tivoli that reside on the RMGA LAN that will require connectivity.

4.7.2.3 RDT

RDMC workstations in BRA01 are connected to the RMGA LAN and require access to the live platforms in IRE11/19 along with continued connectivity to other RDT platforms at other sites (LEW02, STE04/09, WGN01 and BTL01)

4.7.2.4 DR facilities

BRA01 is also used to provide a DR site for SMC, OBC (CRE02, but may move to WAR13) and soon to include HSD DR.

4.7.3 Stevenage STE04

The SMC currently have 3 workstations, connected to the Corporate LAN that can access the rigs in IRE 11 and IRE19. These are standard builds with fixed IP addresses with firewall access to the test rigs. The workstations access via the SAS (SSN) servers for all services. The number of devices is expected to increase closer to go-live.

4.7.3.1 Reference Data Teams

RDMC workstations in STE09 are currently connected to the RDT LAN and require access to the live platforms in IRE11/19 along with continued connectivity to other RDT platforms at other sites (BRA01, LEW02, WGN01 and BTL01).

FUJ00088557

4.7.4 Crewe CRE02

There are two teams within Crewe that are involved with the RMG account. The IDS team is still being developed and their requirements are unknown at the time of writing, but are expected to comprise a small number of workstations on the RMGA LAN. The OBC team currently have four of five staff with two workstations each; an OCMS workstation on the RMGA LAN and a corporate desktop on the corporate LAN.

4.7.5 Wigan WGN01

MSS requirements at Wigan are similar to the Stevenage SMC requirements. There are currently three workstations on the Corporate LAN with fixed IP addresses accessing services via the SAS (SSN) servers. Access for these devices will be via the Checkpoint firewalls in IRE11/19.

4.7.6 Belfast IRE11/IRE19

The local support team in IRE11 have workstations on the corporate LAN that require access via the SAS (SSN) servers to individual platforms. Local access is provided via a CIS/RMGA firewall within IRE11 and IRE19.

Out-of-hours access is required via the corporate VPN. The KMA key management platform is not available via remote access for security reasons.

4.7.7 Lewes LEW02

RDMC workstations for RDT in LEW02 are connected to the RDT LAN and require access to the live platforms in IRE11/19 along with continued connectivity to other RDT platforms at other sites

4.7.8 Warrington WAR13

New site for Network Support and Firewall Support teams moving from WGN01 and BTL01.

4.7.9 Solihull SOL10

4.7.9.1 NOSS

NOSS users follow the corporate model with access via the Corporate firewalls in IRE11/19, terminating on the SAS (SSN) platforms for authentication. There are no RMGA dedicated workstations within this building.

FUJ00088557

4.7.10 Out-of-hours access

Support access is provided through continued use of the corporate Internet VPN access from the corporate network, via the Checkpoint firewalls in IRE11/19 and terminating on the SAS (SSN) platforms for authentication.

4.8 Test counter access

Test rigs for HNG-X are available within IRE19 (unless DR is invoked). Test counter access follows the live access approach using Utimaco VPN encryption across the WAN. The WAN for test rig connectivity is the same as that for the branch access network that is outside of the scope of this document; further detail is provided in the Branch Access Network HLD (DES/NET/HLD/0014).

Test counter traffic is steered towards the IRE19 CE router through use of BGP attributes; this is achieved through extending the AS-Path attribute on the VPN Crypt router to CE BGP peering in IRE11 (AS-path pre-pending).

4.8.1 Test rig connectivity

Up to five test rigs have been built in IRE19; LST, ST, SV&I, RV Mig and RV Acc. Of these, only the LST rig will remain post-live. Unlike Horizon test counter access, where dedicated C&W VPNs have been deployed per rig, a single VPN will be used for all HNG-X test counter access between SDC01/TCY02 and IRE11/19 (fujser_hngx_test).

A further Volume and Integration (V&I) rig was built on the live network at both IRE11 and IRE19. Essentially, this is a pre-live proving and integrity testing of the live platforms. Connectivity will be as for live services and the requirement will cease when IRE11 goes live. A dedicated V&I VLAN will be required in BRA01 for the duration of V&I testing; this LAN will be ceased when HNG-X goes live.

4.8.2 Lewes LEW02 test rig networks

Lewes acts as a backup site to BRA01 for testing. There is a single LST test rig with access to the HNG-X Test VPN (fujser_hngx_test).

4.8.3 RDT rig in BRA01 and LEW02

The RDT rig comprises a number of Solaris and Windows systems located on the RDT LAN in LEW02.

The equipment currently in LEW02 is scheduled to move to one of IRE11/IRE19 to become the RDT Live operational kit at the time of data centre migration but be available for proving RDT migration to Solaris 10/Oracle 10 and HNG-X platforms alongside the main testing this autumn.

When this equipment moves it will require a separate LAN segment of its own in IRE19 which has full and unrestricted two-way connectivity to the BRA01 (42), LEW02 (95) and STE09 (46) LANs. There will also need to be the same access for the Primary Solaris system to the Live Host for both the read access and the mounted share. At some point after the RDT operational system moves to IRE19 a DR

FUJ00088557

set of equipment will need to be commissioned in the other data centre. This will need the same level of connectivity as the main system with interconnectivity between the two data centres.

RDT Counters and other systems in BRA01/LEW02:

In addition to the RDMC workstations there are a number of counters and other servers used by RDT on the BRA01 (42) and LEW02 (95) LANs. These must retain full access to all of the RDT equipment, regardless of where it is located and which LAN it is connected to.

Testing access:

There have been suggestions that RDT should have RDMC workstation access to the test rigs once they are operational in IRE19. This would probably mean a further access from the 42/95 LANs on to the relevant test LAN(s).

FUJ00088557

4.9 External connections

For external (third party) connections, RMGA is responsible for the WAN connections (along with CPE routers) for Post Office Ltd (POL), DVLA, E-Pay and Alliance & Leicester. For all other external connections, individual agreement with the third parties will need to be sought to enable them to provide suitable WAN connections, and is out-of-scope for this document.

4.9.1 Managed CPE refresh

For those clients where RMGA is responsible for managed CPEs, the opportunity to refresh and standardise the managed CPE routers at external client sites was undertaken as part of the HNG-X project. The new managed CPE routers are Cisco 2811.

The connectivity for each client is subject to contractual requirements with the individual clients and is documented in a Technical Interface Specification document. However, each is based on a generic approach using IPSec or GRE tunnels across a dedicated C&W VPN. At the IRE11 and IRE19 data centres, a single handoff router is used with resilience provided via the handoff router in the other data centre, accessible via the intercampus LAN.

4.9.2 External client tunnel termination

Termination of the GRE and IPSec tunnels will take place on dedicated handoff routers within IRE11 and IRE19 data centres. At the remote sites, the tunnels will terminate on the managed CPE routers. Using dedicated handoff routers for each client offloads the tunnel and encryption overhead from the WAN access router (MSFC) and helps to reduce the likelihood of routing configuration errors that could lead to advertisement of routes between clients.

The following diagrams show the routing between the data centres and the client site via a C&W VPN, and tunnel connectivity with OSPF redistribution at the data centres. Note that there is no requirement for OSPF across the tunnels.

FUJ00088557

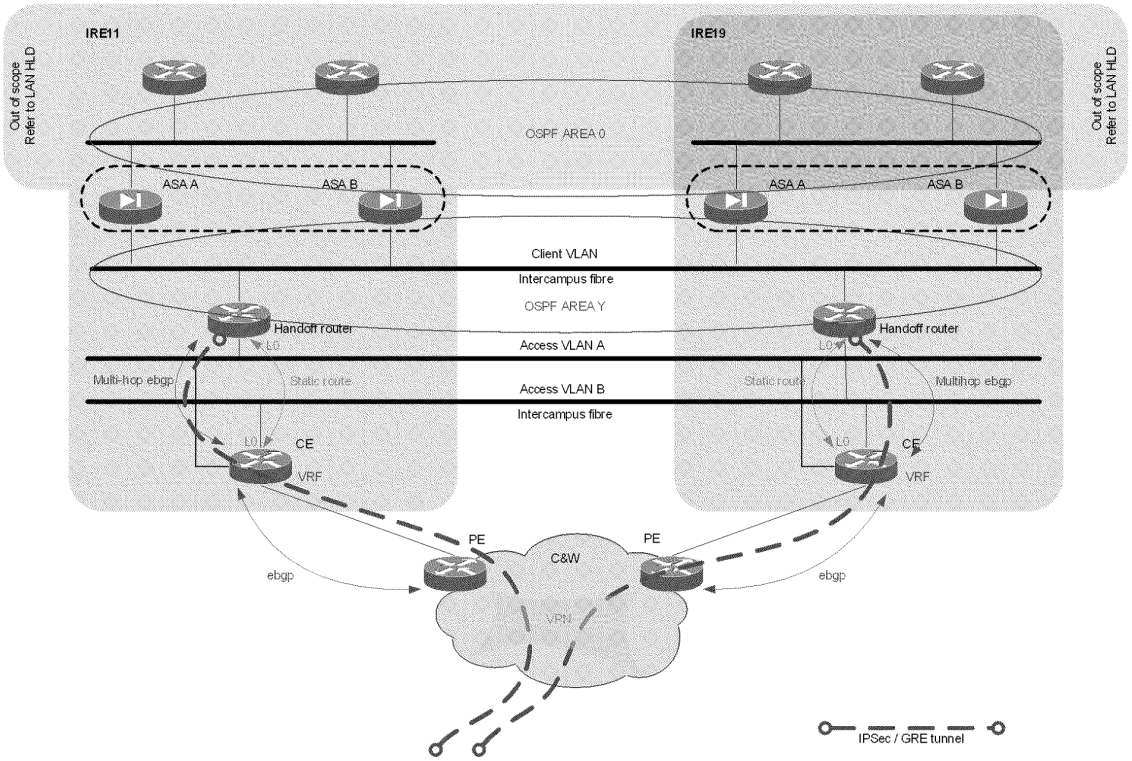

Figure 14 External client handoff - BGP routing

FUJ00088557

4.10 Summary of VPN requirements

The following table summarises the C&W VPNs and identifies which CE routers require access to individual VPNs:

Site VPN	IRE11	IRE19	BRA01	STE04	CRE02	WAR13	LEW02	SDC01/ TCY01	WGN01	BTL01	External sites
Live branch traffic (out-of-scope) (fujser_fujnwb1)	X	X	X			X	X	X	X	X	
Support RMGA LAN (fujser_fujnwb_test) (includes MIS / RDT / Security LAN requirements)	X	X	X	X	X	X	X	X	X	X	
Post Office Ltd. (fujser_fujnwb_aux1)	X	X							X	X	X
DVLA (fujser_fujnwb_dvla)	X	X							X	X	X
A&L (fujser_fujnwb_aux1)	X	X							X	X	X
E-Pay (fujser_fujnwb_aux2)	X	X							X	X	X
HNG-X Test VPN (all HNG-X test rigs)	X	X					X	X			
Test1 (fujser_fujnwb1_test)			X				X	X			
VPN test rig (fujser_fujnwb_bracknell1)							X	X			
Horizon LST rig (fujser_fujnwb_bracknell2)			X	X			X	X			
Horizon REL rig (fujser_rel_rig)			X					X			
Horizon BTC rig (fujser_brac_btc)			X					X			
Live Boot (VPN instantiated by Branch Router HLD)	X	X	X					X			
LST Boot (VPN instantiated by		X	X				X	X	X	X	

FUJ00088557

Branch Router HLD)											
BTC Boot (VPN instantiated by Branch Router HLD)		X	X					X	X	X	

Table 5 Summary of C&W VPN requirements

.

FUJ00088557

5 Migration

5.1 Inter-DC connectivity

The inter-data centre connectivity is a temporary solution until cessation of the Wigan and Bootle data centres, and will make use of IPSec encrypted GRE tunnels to dedicated handoff routers at all four sites.

The solution provides for up to 100Mb/s throughput between data centre campuses with up to six level of QoS

5.2 Support connectivity

Unchanged from the support access model described previously.

5.2.1 Out-of-hours support access

Unchanged from the support access model described previously.

5.3 Test rig access

Unchanged from the test counter access model described previously.

FUJ00088557

5.4 External connections

Migration of external clients will require the existing C&W VPNs to be extended to include the IRE11 and IRE19 PEs where C&W will present as VRFs on their CE routers. Connectivity will be extended to the dedicated handoff routers within IRE11 and IRE19 using EBGP. New tunnels can then be created between the handoff routers in IRE11/19 and the managed CPE routers at the client site. Whether the tunnels terminate on the new or existing CPE routers is independent of this design. By extending the original tunnel mesh to include IRE11 and IRE19, the infrastructure will be in place to accommodate various migration scenarios from full four-centre operation to cease and re-provide.

The number of additional tunnels should be kept to a minimum sufficient provide resilience. For an external client site with dual CPE routers, a single additional tunnel to one of the IRE11 or IRE19 handoff routers from each CPE is sufficient. Dual connecting the CPEs to both handoff routers is unnecessary. If the external client site has a single handoff router (e.g. Sungard site for Post Office Ltd.) then a tunnel to each of the IRE11 and IRE19 handoff routers should be provided. See diagram below. In all cases, the tunnels depicted are in addition to the existing tunnels to the Wigan and Bootle data centres.

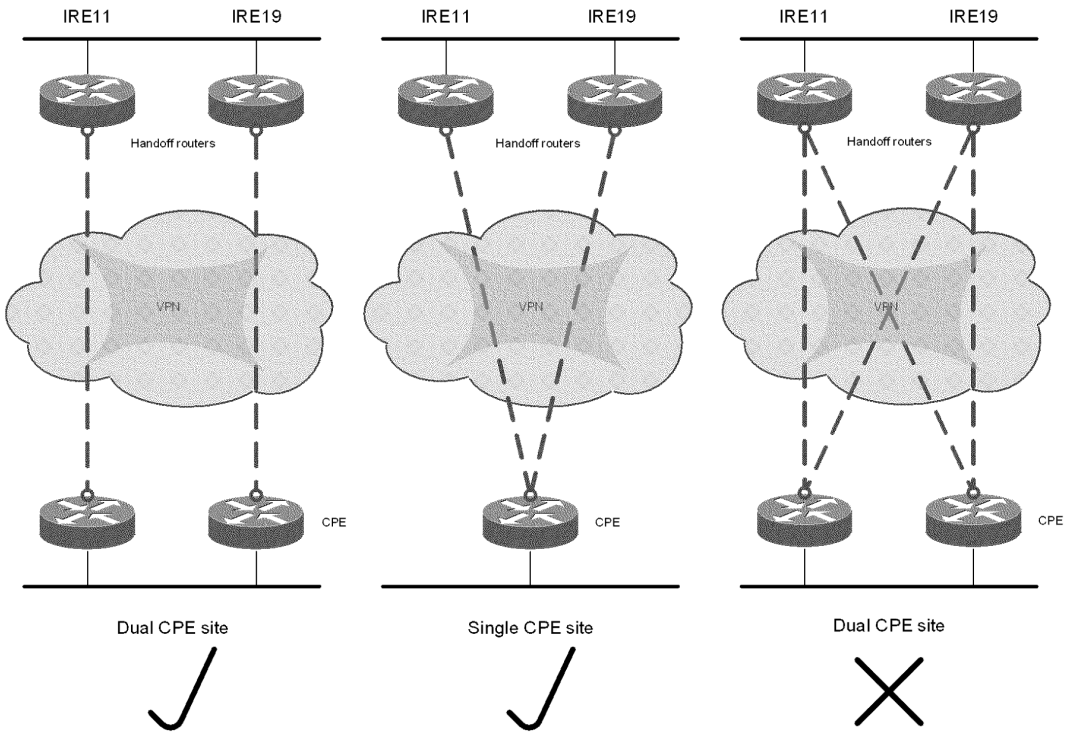

Figure 16 External client tunnel topology

Where a client site has common VLANs between their sites, a variant of the Dual CPE approach can be adapted to represent both client sites, saving in CPE routers and tunnel complexity.

The pre-existing tunnels to Wigan and Bootle can be cessation of Horizon activities in Wigan and Bootle, in addition to the decommissioning of the C&W VPN at these sites.

FUJ00088557

5.4.1 Post Office Limited

The Post Office connectivity is used to support a multi application environment. Applications supported are TIP, POLFS, EDG, TES, Track and Trace and APOP. Access to POL applications is via the RMG Northern Data Centre at Huthwaite, Nottinghamshire, with a DR site at Sungard London Technology Centre in Hounslow (supporting TIP, POLFS and EDG only). The network to both sites is considered active/active at all times.

Post Office connectivity currently uses a mesh of GRE tunnels across a C&W IP Select VPN. VPN name is fujser_fujnwb_aux1 and provides a 2Mb/s constrained service.

Traffic is encrypted within the tunnels and OSPF is used for routing across the tunnel mesh. The two Post Office sites of Huthwaite and Sungard each use OSPF area 1 to access the Wigan data centre, and area 2 to access Bootle data centre.

The mesh of IPSec tunnels will be extended to include the new dedicated Post Office handoff routers at IRE11 and IRE19. As per the original design, OSPF will be used as an IGP across the tunnel mesh. The relationship of OSPF area to data centre will be determined by the LLD designer under agreement from the client.

5.4.2 DVLA

Current connectivity for DVLA follows a similar solution to that for the Post Office, with a mesh of GRE tunnels deployed across a L3VPN from C&W. The VPN name is fujser_fujnwb_dvla and is bandwidth constrained to 960kb/s to each site. Routing comprises non-contiguous OSPF areas, with Area 1 serving Swansea/Morriston to Wigan, Area 2 serving Swansea/Morriston to Bootle and Area 3 connecting Swansea with Morriston directly.

Note that DVLA traffic is not encrypted within the tunnels.

The proposed solution for DVLA follows the same practice as that for the Post Office, albeit with unencrypted GRE tunnels.

5.4.3 Alliance and Leicester

Connectivity for Alliance and Leicester follows similar practice as for Post Office and DVLA, using a mesh of encrypted tunnels and similar OSPF configuration.

[DN: awaiting detail of existing A&L connectivity]

5.4.4 E-pay

TBD

FUJ00088557

5.4.5 Streamline (Debit Card)

The Debit Card service provided by Streamline currently terminates on Cisco 2651 routers within Wigan and Bootle. WAN connectivity is provided over X.25 for debit card transaction traffic and over ISDN for file transfers.

The solution for HNG-X is to re-provide this service within IRE11/19. A dedicated handoff router will be installed in each of IRE11 and IRE19 with a common VLAN between them. The handoff routers will each require an ISDN and serial interface. The router will be required to perform X.25 protocol translation. The X.25 service is currently provided by TNSI International.

5.4.6 CAPO (EDS), LiNK and Moneygram

These companies own and manage their CPE equipment along with any WAN links. Design for connectivity to these companies is outside of the scope of this HLD and will be covered by individual transit LAN LLDs.

5.5 Retirement of Zergo hardware encryption devices

Wigan and Bootle inter-DC communications for Horizon make use of obsolete Zergo encryption devices. These will be replaced by IPSec tunnels between handoff routers across a C&W VPN.

Requirements are undetermined at the time of writing.

FUJ00088557

6 Design constraints

6.1 Device naming

Device names will conform to the standard defined in DES/PPS/HLD/0006.

6.2 Traffic engineering

The network design provides for fully resilient connectivity to both data centres. Although C&W connectivity to each of the IRE11 and IRE19 data centres is limited to a single CE router, triangulation is provided via the fibre inter-campus LAN.

Single points of failure are limited to instances where switched media is used for access (e.g. Streamline access).

6.3 Resilience

The WAN, both target and interim is designed to have no single points of failure. Network connectivity to IRE11 and IRE19 will operate in an active/active state (although the applications and services provided by the data centres may operate as active/DR).

Although each of the new data centres in Northern Ireland has a single C&W CE router, resilience through triangulation is provided by intercampus VLANs over DWDM fibre. Handoff routers for third party connections will be similarly provided as single routers triangulated between sites. The intercampus WAN links and provision of VLANs is documented within the LAN HLD.

Network devices are deployed in pairs for resilience (with the exceptions previously mentioned), and will be mounted within separate racks and have separate power feeds from an uninterruptible power supply.

Devices interfacing with equipment that cannot operate dynamic routing protocols will use VRRP to provide a resilient gateway.

6.4 Network cabling

Cabling external to the data centres will be spatially separated by at least ten metres. Within the data centres, cabling will use separate patch frames and/or devices within separate racks.

Network cabling will confirm to the following standards:

- Copper – UTP Category 5e ANSI/EIA/TIA 568B (max. 100m0
- Fibre – multimode 850nm/62.5micron (max. 220m)

6.5 Network Protocols

The network protocol is IPv4 (RFC791) and all application traffic is unicast UDP (RFC768) or TCP (RFC793). The network is optimised for TCP.

FUJ00088557

MPLS VPNs will be L3VPNs to RFC2547bis.

X.25 will be used for connectivity to Streamline.

6.6 IP addressing

IP addressing is taken from RFC1918 private address space only.

6.7 Routing protocols

The following routing protocols will be used. In all cases, MTU sizes will be optimised to avoid packet fragmentation.

6.7.1 BGP

BGP-4 is the preferred routing protocol within the WAN domain. The use of BGP is inherent for RFC2547bis VPNs, and is mandated for all PE to CE links on the C&W network. EBGP will be used for routing between the C&W CE routers and the RMGA managed handoff routers at all sites. Redistribution between BGP and OSPF is not envisaged (the exception being between mBGP and OSPF within the branch access VRF for HNG-X. This will be configured by C&W and will be for SSL terminated traffic only).

6.7.2 OSPF

OSPF is the IGP routing protocol of choice for use on the data centre LANs as defined in the LAN HLD.

6.7.3 VRRP

VRRP will be used for gateway resolution for instances where a routing protocol is unavailable or undesirable. HSRP will be used only if VRRP cannot be used. It is not envisaged that VRRP will be used within the WAN, but likely to be used within the Transit LAN designs.

6.7.4 Static routes

Static routes may be required where EBGP peers are not directly connected in order to resolve next-hop (multi-hop EBGP), or in place of an IGP for next-hop resolution for IBGP neighbours.

FUJ00088557

6.8 Bandwidth requirements

The following bandwidth requirements have been taken directly from the Network Architecture document pending availability of revised data.

#	Description	'A' End	'B' End	Speed	Comment
L1	Intercampus – SAN	DC1	DC2	n G bit/s Fibre Channel	n is 1,2 or 4
L2	Intercampus – SAN	DC1	DC2	n G bit/s Fibre Channel	Needs to be diverse and separate from L1
L3	Intercampus – Network	DC1	DC2	1 G bit/s IP	
L4	Intercampus – Network	DC1	DC2	1 G bit/s IP	Needs to be diverse and separate from L3
L5	3rd line support (SSC)	DC1/DC2	BRA01	4 M bits/s, resilient	Diversity and Separate routing required to provide high resilience
L6	2nd Line Support	DC1/DC2	STE09	2 M bits/s resilient	Diversity and Separate routing required to provide high resilience
L7	OBC	DC1/DC2	CRE02	2 M bit/s resilient	Diversity and Separate routing required to provide high resilience
L8	Ops	DC1/DC2	IRE11	2 M bit/s resilient	Diversity and Separate routing required to provide high resilience
L9	DR – 3rd line (SSC)	DC1/DC2	LEW02	2 M bit/s resilient	Diversity and Separate routing required providing high resilience. Not normally used.
L10	DR – Ops	DC1/DC2	IRE19	2 M bit/s resilient	Diversity and Separate routing required providing high resilience. Not normally used.
L11	3rd line (MSS)	DC1/DC2	???	2 M bit/s resilient	Diversity and Separate routing required to provide high resilience
L12	Branch Traffic	Tele city/ SDC01	DC1/DC2	70 M bit/s resilient	Diversity and Separate routing required to provide high resilience
L13	IP Select via IP gateway	Tele city/ SDC01	DC1/DC2	10 M bit/s resilient	Diversity and Separate routing required to provide high resilience

Table 7 Bandwidth requirements

| # | Description | 'A' End | 'B' End | Speed | Comment |

FUJ00088557

T3	Test Access	DC1/DC2	BRA01	45Mbit/s with 8Mbit/s backup.	Connectivity provided over IPSec/GRE tunnels over support VPN. Access circuits upgraded to 100Mb/s. CAR used to rate limit to 45Mb/s for test.
T4	Test Access – DR	DC1/DC2	LEW02	2Mbit/s no resilience	No resilience required.
	Migration connectivity	DC1/DC2	WGN01/ BTL02	90Mb/s with resilience	Connectivity provided over IPSec/GRE tunnels over support VPN. QoS using CBWFQ and six queues to prioritise flows.

Table 8 Four centre operation - test link bandwidth requirements

6.9 Cable and Wireless VPN constraints

The IP Connect Direct service is productised by C&W that results in supported limitations for their service. These limitations are based on their internal testing, representing the service they are prepared to support, and are not technological constraints:

Tail circuit bandwidth (PE to CE)	Maximum supported VPNs
Up to 100Mb/s	4
100Mb/s	18
155Mb/s	30

Table 10 C&W VPN constraints

6.9.1 C&W IP Connect Direct QoS

C&W can provide bandwidth guarantees between VPNs such that one VPN cannot impact another, however this could also prevent a VPN bursting into unused bandwidth.

Additionally, C&W can provide a QoS capability within a VPN providing Gold, Silver and Bronze service classes within a VPN (known as their Olympic model). Note however, that support for QoS within a VPN is only available for where a maximum of 4 VPNs are configured on a CE, irrespective of the tail circuit bandwidth.

C&W plan to support Advanced Application QoS (AAQ), where DSCP bits are mapped to AF and EF forwarding classes. This service will only be available to new deployments and is therefore not suitable for the RMGA network.

There is no QoS applied to the current (Horizon) C&W VPN network.

6.10 Device deployment

6.10.1 Network Management

Devices are configured to support SSHv2 and SNMPv3.

FUJ00088557

Device configurations are automatically recovered and stored by Cisco Works.

Devices are configured to log SYSLOG to the Cisco Works server. The Cisco Works server should forward SYSLOG to the RSA EnVision logging server, with incidents raised in accordance with the Incident Management Process (SVM/SDM/PRO/0018).

Device interfaces are monitored for availability by HP Network Node Manager. Failures are reported to the Tivoli enterprise manager.

The following protocols / toolsets are used for device management:

Device	Toolset
Router	SSHv2, SNMPv3, CiscoWorks

Table 11 Device Management Toolsets

The C&W network, including layer 3 VPNs and associated CE to PE links is out-of-scope for RMGA network management.

6.10.2 Routers

All routers acting as CE routers will support multiple VRFs. VLAN separation (802.1q trunking) is sufficient to ensure data separation on Ethernet interfaces.

Handoff routers, deployed within the Access LAN environment at IRE11 and IRE19, are dedicated to individual third parties or support access, and are not required to support VRFs.

6.10.3 Switches (core sites and BRA01 interlink)

VLAN separation (802.1q trunking) is sufficient to ensure data separation.

6.10.4 Network Time Source

All WAN routers within the scope of this document will derive their timing for NTP from the data centre access LAN devices (6513 switches).

6.11 Hardware requirements

[DN: The following is taken from the Bill of Materials that pre-dates this design and may require amendment.]

The following hardware is required to fulfil both the target and interim designs covered by this HLD:

Role	Platform Component	Per chassis	Per data centre	Total Required

FUJ00088557

Client Access				
A&L Bootle remote	C2811	1	1	2
A&L Leicester remote	C2811	1	1	2
A&L local	C2811	1	2	4
CAPO local	C2811	1	2	4
DCS (Streamline) local	C2811	1	2	4
DVLA local	C2811	1	2	4
DVLA remote	C2811	1	1	2
VocaLink local	C2811	1	2	4
Moneygram local	C2811	1	0	0
RMGA Huthwaite local	C2811	1	2	4
RMGA Huthwaite remote	C2811	1	2	4
RMGA Sungard remote	C2811	1	1	2
STE04 local	C2811	1	2	4
STE04 remote	C2811	1	1	2
Support Access				
BRA01 Support remote	C2811	1	1	2
Warrington remote	C2811	1	1	2
CRE02 remote	C2811	1	1	2
IRE11 remote	C2811	1	1	2
IRE19 remote	C2811	1	1	2
LEW02 remote	C2811	1	1	2

Table 12 WAN hardware requirements

FUJ00088557

7 Non-functional requirements

7.1 Security

From Requirements traceability section of Technical Network Architecture document (ARC/NET/ARC/0001):

ID	Requirements
SEC-3100	Third Party access requirements shall not apply to access by Fujitsu Post Office Account Support Staff that access the system from the operational support centres, or via a network with remote access secured using encryption and 2 factor authentication.
SEC-3167	{CISP 8.5.1g} Data over Wide Area Networks shall be encrypted unless specifically agreed in the relevant Technical Interface Specification or where otherwise specifically agreed by Post Office Limited Information Security. The Fibre Optic link between Data Centres is not considered to be a Wide Area Network. The requirement applies to transaction data between branches and the data centre(s).
SEC-3168	WAN Encryption key management shall be independent of network configuration such that the confidentiality of Post Office traffic is not compromised by a single configuration error of either the WAN or the encryption system.

Table 13 Security requirements

IPSec requirements taken from Technical Network Architecture document (ARC/NET/ARC/0001):

Summary	Description
Encryption	Traffic classes will be encrypted over the Wide Area network if specified by the relevant TIS or HNG-X Security Architecture. The IPSEC tunnel will terminate on devices within the HNG-X service boundary. For example this is the case with A&L where HNG-X Router are at A&L Data Centres. The encryption algorithm will be AES 256.
Authentication	Based on Certificates (except for branch Router) Branch Router will use PSK. The rationale for this is resuse of the Branch Router CHAP solution for key management. The IPSEC keys will be 15 characters in length from alphabet {A-Z, a-z, 0-9}. Entropy with be as for CHAP - Crypto quality.

FUJ00088557

Protection against single configuration error	IPSEC devices are deployed in the following topology. IPSEC Router -> Downstream Router - > WAN The downstream Router will apply an ACL to ensure that the traffic from the IPSEC router is IPSEC traffic only. Also the IPSEC Routers will be configured not to be able to negotiate an NULL encrypted stream. Therefore a single configuration error will not compromise WAN encryption.

Table 14 IPSec security requirements

Remote access and Network Management requirements taken from Technical Security Architecture document (ARC/SEC/ARC/0003):

7.1.1.1 Remote Access

Remote access to the HNG-X network will be provisioned using IPSEC VPN technology, support build laptops and two factor authentication.

Access for remote users will utilise the corporate VPN system and the FSBN. This will require support users to have a two factor authentication token for the corporate VPN and one for the HNG-X network.

Remote support access to the Counter will be provided through the implementation of an SSH service running on the Counter which can then be accessed from the Secure Access Servers, (SAS), in the Data Centre. The SSH server on the Counter is configured with the SAS Server SSH public keys so that connections to the Counter are restricted to only those originating from the SAS servers. This will allow access to a command prompt on the Counter for the retrieval of logs and other data using secure copy, (SCP).

SSH access to the HNG-X servers will also be provided. This will be configured as for the Counter SSH access.

All support user access will be audited at a command line level to ensure an audit trail of administrator activity is available. This auditing will take place at the SSH server, not at the client. SSH will be configured to use a single shell, (sudosh), and to prevent the spawning of additional, non-logging, shell processes.

Firewall rules will be configured to ensure that the SSH and SCP traffic can only be initiated from the SAS servers.

Access control for the SAS servers is provided by the Identity and Access Management service.

7.1.1.2 Management Network Access

A method of obtaining system patches and anti-virus signatures is required for HNG-X as well as a means of providing management support access. It is anticipated that this will be through the provision of a link to the RMG network.

This link will allow management access to the IDS/IPS and Network Intelligence appliances from Crewe and Bracknell. It will also allow anti-virus signatures and system patches to be obtained, via a proxied route, from the Internet.

FUJ00088557

This connection will provide access through the implementation of a DMZ network containing the relevant proxy and access control systems. It is anticipated that console access will be provisioned through the implementation of a Windows Terminal Server system.

7.2 Availability and QoS

7.2.1 C&W IP Connect class of service

The C&W IP Connect service in operation for the RMG account is described as their Bronze service with the following service level characteristics:

- QoS: Default
- Average Round-Trip Delay: 30ms
- Average Packet Delivery: 99.80%
- Jitter: N/A

7.3 Service Level Agreements

The only service covered by this HLD that has a defined SLA is for Alliance and Leicester where the Service Level Target is 99.95%

Services to RMG data centres at Huthwaite and Sungard, along with services from DVLA are subject to independent calculations agreed with the Post Office for each event.

Network Banking allows for a maximum of one outage in excess of two minutes per bank per month, and a maximum of outages to two banks in any one month.

FUJ00088557

A Sites

This section identifies locations used in this design

A.1 Data centres

Two new data centres will be introduced for HNG-X, both of which are in Northern Ireland. The existing data centres in Wigan and Bootle are not included as no changes are envisaged to the current design.

IRE11 – Trident House, 301 Airport Road West, Belfast, BT3 9AE

IRE19 – Unit 4B Bridgeview, Glenville Industrial Estate, Glenville Road, Whiteabbey, County Antrim, BT37 0TU

A.2 Core sites

These sites represent the aggregation point between the access networks and the core network for branch access.

SDC01 – Units 2-5 Weston Avenue, Grays, Essex, RM20 3WZ

TCY02 – Telecity, 8/9 Harbour Exchange, Isle of Dogs, London, E14 9GE

A.3 Support sites

These are Fujitsu Services sites from which access is required to support operational teams and testing of the HNG-X solution:

BRA01 – Lovelace Road, Bracknell, Berkshire, RG12 8SN

LEW02 – Sackville House, Brooks Close, Lewes, East Sussex, BN7 2FZ

STE04 – 14 Cavendish Road, Stevenage, Hertfordshire, SG1 2DY

CRE02 – Infinity House, Mallard Way, off Electra Way, Crewe Bus. Park, Crewe, Cheshire, CW1 6ZQ

WGN01 – c/o Alliance and Leicester, Quayside Centre, Westward Park, Wigan, WN3 5GB

WAR13 – Trafalgar House, Temple Court, Risley, Warrington, WA3 6GD

IRE11 – Trident House, 301 Airport Road West, Belfast, BT3 9AE

FUJ00088557

A.4 External client sites

This section lists only those sites where RMGA has managed CPE equipment deployed at the external location, or where RMGA provide the WAN connectivity (E-pay)

- **Post Office (RMG)**

Huthwaite: The County Estate, Nunn Brook Rise, Sutton-in-Ashfield, Nottinghamshire, NG17 1TD

Sungard: POL Huthwaite DR site, Green Lane, Hounslow, Middlesex, TW4 6ER

- **DVLA**

Swansea Vale: ROSB Building, Sandringham Park, Llansamlet, Swansea, West Glamorgan, SA6 8QL

Morriston: C Block, Longview Road, Clase, Swansea, West Glamorgan, SA6 7JL

- **Alliance and Leicester**

Carlton Park, Narborough, Leicester, LE19 0AL

Bridle Road, Bootle, L30 4GB

- **E-pay**

Kelting House, Southernhay, Basildon, Essex, SS14 1EL

12 Hornsby Square, Southfields industrial Park, Laindon, Basildon, Essex, SS15 6SD

FUJ00088557

B Circuit requirements

The following section identifies new circuits required for the proposed design.

B.1 IRE11 and IRE19

New C&W IP Connect circuits at 155Mb/s to each of IRE11 and IRE19. Each circuit is required to be diversely routed from the other.

In addition, the following circuits will be required:

- ISDN2e circuit in each data centre for MoneyGram International (MoneyGram will provide their own Frame Relay service into each data centre)
- PSTN circuit in each data centre for EMC dial access (requires verification)
- PSTN circuit in each data centre for Fujitsu Siemens dial access (Bladeframe support) (requires verification)
- PSTN circuit in each data centre for Alarmpoint dial-out.

B.2 Regional support sites

New 2Mb/s C&W IP Connect circuits required at:

- STE04 – 2 circuits each with CE router, diversely routed
- CRE02– 2 circuits each with CE router, diversely routed
- WAR13 – 2 circuits each with CE router, diversely routed

Alternatively, connectivity for these sites could be provided via FSBN VPNs direct to IRE11/19 subject to suitable CIS firewalls being deployed at IRE11 and IRE19.

B.3 Post Office Limited

New C&W IP Connect circuit at Maidstone required for EDG DR Service

- 1 circuit (unprotected) at 2Mb/s with 1:1 contention

B.4 Streamline

New X.25 service from TNSI International required at IRE11 and IRE19

Dedicated ISDN line required in each of IRE11 and IRE19

FUJ00088557

B.5 Circuits for cessation on completion

The following table lists the circuits that can be ceased on completion of all Horizon and HNG-X migration activities.

Circuit reference (CE router)	Vendor	Bandwidth	A-end	B-end
NXUK262233	BT	64kb/s	IRE11	WGN01
NXUK262208	BT	64kb/s	IRE19	WGN01
NXUK262200	BT	64kb/s	IRE11	WGN01
NXUK263257	BT	2Mb/s	IRE11	BTL01
NXGB232821	BT	192kb/s	BTL01	CRE02
NXGB232822	BT	192kb/s	WGN01	CRE02
ISA53223 (u064-r28-001)	C&W	2Mb/s	BRA01	n/a
ISA53743 (u064-r26-002	C&W	2Mb/s	BRA01	n/a
ISA2533720 (u064-r22-001)	C&W	2Mb/s	BRA01	n/a
ISA2533724 (u064-r22-002)	C&W	2Mb/s	BRA01	n/a
ISA2533725 (u064-r22-003)	C&W	2Mb/s	BRA01	n/a
ISA2533726 (u064-r22-004)	C&W	2Mb/s	BRA01	n/a
ISJ2611923 (gr33-r16-001)	C&W		BRA01	n/a