Document Title:	HNG-X SUPPORT NETWORK LLD
Document Reference:	DEV/INF/LLD/0054
Document Type:	Low Level Design (LLD)
Release:	1.8
Abstract:	Provides a Low level description of the Support access network infrastructure.
Document Status:	APPROVED
Author & Dept:	Jon Dawes
Internal Distribution:	Dean Parsons Gill Jackson
External Distribution:	

Approval Authorities:

Name	Role	Signature	Date
Solution Design / Infrastructure Design	Dave Haywood		
Infrastructure	Mark Jarosz		

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

0 Document Control

0.1 Table of Contents

0.2 List of Tables

0.3 List of Figures

0.4 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	15-Oct-2007	Initial for review	Internal Peer Review
0.2	10/11/07	Made changes in line with peer review	TBD
0.3	13/01/08	Made changes in line with formal review	TBD
0.3A	11/02/08	Made changes inline with design changes as agreed with implementation team	
0.3A v002	12/02/08	Made changes inline with DAB comments.	
0.3A v003	22/02/08	Added BRA01 NAT and Firewall tables	
0.3A v004	05/05/08	Updated BRA01 NAT and Firewall tables for additional SSN server access.	
0.3A v005	13/05/08	Updated BRA01 NAT and Firewall tables in line with re-DAB comments on SSN IP addresses.	
0.4	27/05/08	Final LLD subject to DC LAN LLD changes and firewalls addition. DC LAN LLD impacts the firewall rules.	
0.4	05/06/08	Updated with DAB review comments and SSC firewall rules.	Kept version inline with DAB process.
0.4	09/06/08	Updated with remote sites firewall rules	Kept version inline with DAB process.
1.0	06/07/08	Updated with regards review comments. Now for Approval	For Approval
1.1	10/02/09	SSN Access Updates & Removal of ST RIG	
1.2	06/03/09	Updated with SSN IP address changes following CP0295. It should be noted that if these changes are implemented before the DC LAN and servers have been changed things will no longer work.	
1.3	02/06/09	Updates following DAB review. STE04 layout revised to reflect C&W connection via spare FastEthernet interface. Added flow for rvacc KSN to ACD in IRE19	
1.4	08/06/09	Amended flow for RVACC KSN following testing. Added a range of ports from 49152 – 50151 to cater for dynamic allocation of RPC service ports. The ACD server will need to be patched to restrict RPC services to this range.	

1.5	10/06/09 14/07/09	Added access for RVACC KSN to KMN on TCP 33031 for CAPO volume testing and end-to-end counter transactions. Updated IP subnet for the LEW02 transit network VLAN 914 due to address conflicts with the BRA01 migration routers 172.20.0.240/28 has been allocated. Winrtr001 & bonrtr001 lo100 interface IPs changed to resolve conflict with IRE11 aggregation router.	
1.6	21/09/09	Added BRA01 SSC→ IRE SSN on RDP (TCP3389) to BRA01 Firewall rules Added LEW02 SSC → IRE lprpssc001 on RDP, SSH, FTP to LEW02 Firewall rules.	
1.7	21-07-10	New requirement Table 11 - top 3 rows new Table 12 - top 2 rows new tabvle 15 - top row new	
1.8	01-08-10	New requirement Table 11 – added bsysinv02 Table 15 – added bsysinv02 Underlined text in sect 2.2 following service Incident	

0.5 Review Details

Review Comments by :	n/a
Review Comments to :	steve.freke GRO & RMGADocumentManagemen GRO

Mandatory Review	
Role	Name
IA&D (peer reviewer)	Dave Haywood
SSC	Steve Parker
System Test	John Rogers
SV&I Manager	Chris Maving
Optional Review	
Role	Name
System Qualities Architecture	Dave Chapman
Chief Information Security Officer	Tom Lillywhite

Security and Risk Team	CSPOA.security GRO
Architect	Jason Clark
Business Continuity	Adam Parker
Service support	Tony Atkinson
HNG-X Service Transition	Graham Welsh
Service Network	Ian Mills
Data Centre Migration	Geoff Butts
Data Centre Migration	Vince Cochrane
SV&I Manager	Sheila Bamber
RV Manager	James Brett (POL)
VI / TE Manager	Mark Ascott
Integrity Testing	Michael Welch
Networks Architect (Data Centre)	Mark Jarosz
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

0.6 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
ARC/SOL/ARC/0001			HNG-X Overall Solution Architecture	Dimensions
DES/PPS/HLD/0006			Naming Standard	Dimensions
ARC/SYS/ARC/0001			Support Services Architecture	Dimensions
ARC/SOL/ARC/0001			HNG-X Solutions Architecture Outline	Dimensions
ARC/SEC/ARC/0003			Security Architecture	Dimensions
ARC/NET/ARC/0001			HNG-X Technical Network Architecture	Dimensions
DES/NET/HLD/0012			HNG-x Network Management HLD	Dimensions
DES/NET/HLD/0014			Branch Access Network HLD	Dimensions
DES/NET/HLD/009			Wide Area Network HLD	Dimensions
DES/NET/HLD/008			Data Centre LAN Design	Dimensions
DES/NET/HLD/0015			Transit LAN HLD	Dimensions

DES/SYM/HLD/0017			Remote Support Secure Access Server High Level Design	Dimensions

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
AAA	Authentication, Authorisation and Accounting
ACE	Application Control Engine
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ASDM	Adaptive Security Device Manager
ASA	Adaptive Security Algorithm
AUX	Auxillary
BCP	Best Current Practice
BGP	Border Gateway Protocol
BT	British Telecommunications PLC
BTL01	IRE19 data centre
CE	Customer Edge
CEF	Cisco Express Forwarding
CoPP	Control Pane Policing control
CoS	Class Of Service (IEEE802.1p) (layer 2 QoS)
DAI	Dynamic ARP Inspection
dCEF	Distributed Cisco Express Forwarding
CSM	Content Switching Module
DMS	Degrees, Minutes, Seconds
DWDM	Dense Wave Division Multiplexing
DMZ	De-Militarised Zone
DRS	Data Reconciliation Service
DTP	Dynamic Trunking Protocol
DWH	Data WareHouse
FWSM	Firewall Services Module
GMT	Greenwich Mean Time
HP	Hewlett Packard
ICMP	Internet Control Message Protocol

IPMP	Internet Protocol Multi Pathing
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPSec	Internet Protocol security
IRE11	Ireland 11 data centre
IRE19	Ireland 19 data centre
ITU	Infrastructure Test Unit
LAN	Local Area Network
MDS	Multilayer Data Centre Switch, Multilayer Fabric Switch used for Storage
MSFC	Multi-layer Switch Feature Card
MTBF	Mean Time Between Failures
MTBR	Mean Time Between Repairs
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NNM	Network Node Manager
NMS	Network Management Server
NPS	Network Persistence Store
NTP	Network Time Protocol
OEE	Overall Equipment Effectiveness
OS	Operating System
OSPF	Open Shortest Path First
OVO	OpenView Operations
PDU	Power Distribution Unit
PFC	Policy Feature Card
POA	Post Office Account
PVST+	Per-VLAN Spanning Tree +
QoS	Quality Of Service
RFC	Request For Comments
RMGA	Royal Mail Group Account
ROSS	The Router Operational Support System
SAN	Storage Area Network
SAS	Secure Access Server
STD	Standard
SYSMAN	The Horizon Systems Management product

TES	Transaction Enquiry Service
TPS	Transaction Processing System
TTY	Teletype
UDLD	Uni-Directional Link Detection
UPS	Uninterruptible Power Supply
UTC	Coordinated Universal Time
VLAN	Virtual LAN
VLSM	Variable Length Subnet Mask
VRF	Virtual Routing & Forwarding
VRRP	Virtual Router Redundancy Protocol (RFC3768)
VTP	VLAN Trunking Protocol (IEEE802.1q)
VTY	Virtual Teletype
WAN	Wide Area Network
WGN01	IRE11 data centre
HO	Handoff Router

0.8 Glossary

Term	Definition
AAA	AAA is Cisco's framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).
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.
DWDM	Dense Wave Division Multiplexing. A technique for multiplexing many data streams (usually 32) over a single fibre optic cable by using different frequency laser optics.
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.
mrEth	BladeFrame Mega Redundant Ethernet. Allows a vSwitch interface to failover between chassis.
pServer	BladeFrame Processing Server. A virtual processing server composed of physical and virtual hardware resources. I.e., consists of a number of pBlades.

rEths	BladeFrame redundant Ethernets. Two or more physical NICs from different cBlades providing resilience to failure. A vSwitch rEth is similar to a traditional switch uplink port.
LPANs	BladeFrame Logical PAN. A collection of physical and virtual resources allocated to provide resource for a set of applications. I.e. a number of pServers.
PAN	BladeFrame Processing Area Network.
cBlade	BladeFrame Control Blade. Physical component used to interface IO between the BladeFrame internal network and the external network. The PAN Manager software runs on the cBlade. Load balancing and fail-over policies are configured in the cBlade. Each cBlade has a 100Mb management interface and eight 1000Mb external network interfaces. Redundant cBlades provide resilience.
pBlade	BladeFrame Processor Blade. Physical component used to provide pServers
sBlade	BladeFrame Switch Blade. Physical component used to provide communication between external networks and the pBlade and cBlade components in conjunction with the bladePlane.
vEths	BladeFrame virtual Ethernet interfaces connected to pServers. The PAN Manager software is used to connect vEths to vSwitches.
vSwitch	BladeFrame virtual instance of a layer 2 Ethernet switch that spans pBlades and cBlades. Used to connect pServers together in an LPAN, LPANs together and pServers and LPANs to external network equipment. vSwitches may not be connected to other vSwitches. Routing between vSwitches is performed at layer 3 by a dedicated pServer or an external router.

0.9 Changes Expected

Changes
Changes to IP addressing at Bracknell will require changes to this document

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

1 Introduction

1.1 Purpose

The purpose of this document is to provide a low level design of the HNG-X Support/Business workstations network Access. There are two types of workstations (LAN); RMGA LAN and corporate LAN. The workstations on the corporate LAN are out of scope in this design and are described in the corporate networks LLD (DEVINFLLD0055).

The HNG-X target solution is described for IRE11 / IRE19 and the associated support sites as described in the WAN HLD - DESNETHLD0009 and the provision of infrastructure for the migration of services from the existing data centres in WGN01 and BTL01.

The design document is intended for Systems Integration and Network Services engineers. It provides the details and enumeration for the network required for the new support access into the support DMZs in IRE 11 & 19.

The design will enumerate an integrated HNG-X/Horizon support network at all RMGA remote sites for HNG-X support connectivity.

The Support DMZs will host SAS and SSN (HNGx SAS Server), these servers will act as a gateway for support activities into the rest of the HNG-X estate. They will be used for terminal services and remote desktop type activity to the servers in IRE11 and 19.

1.2 Readership

This document is intended to be reviewed by the Support, Operations and Architect communities. A low level design of the solution is provided, although parts of the content are technical.

1.3 Scope

Workstations at support Sites including;

1. BRA01
2. STE04
3. LEW02
4. CRE02
5. WAR13
6. IRE11 (Local support)
7. IRE19 (Local support)
8. WGN01 (migration phase)
9. BTL01 (migration phase)

Support DMZ in IRE 11 & 19 as depicted in the Data Centre LLD.

The associated transport between the support sites and the support DMZ in IRE 11 & 19.

1.4 Assumptions

HNG-X build workstations will be connecting to this network,.

No live IP addressing will be redone.

1.5 Risks

Horizon and HNG-X build support workstations will co-exist on the same LAN at various remote sites.

The support traffic will transverse an existing Horizon C&W MPLS VPN …..

1.6 Dependencies

The new data centres IRE 11 & 19 already exist.

The underlining transport infrastructure already exists.

The HNG-x infrastructure cannot be managed without the physical environments, hardware, software, physical links and services are available.

The Network management LLD already exist and addresses the various management workstations like the Tivoli, HP Openview, and Cisco Works e.t.c.

1.7 Constraints (Standards, Policies, Guidelines)

The design must conform to:

- ARC/NET/ARC/0001
- ARC/SEC/ARC/0003
- DES/NET/HLD/0015
- DES/SYM/HLD/0017
- DESNETHLD0009

This design will integrate HNG-X with the existing legacy Horizon infrastructure at the remote support sites.

2 Overview

2.1 Design Proposal - “RED LAN” Support Network

2.1.1 Target design high level diagram,

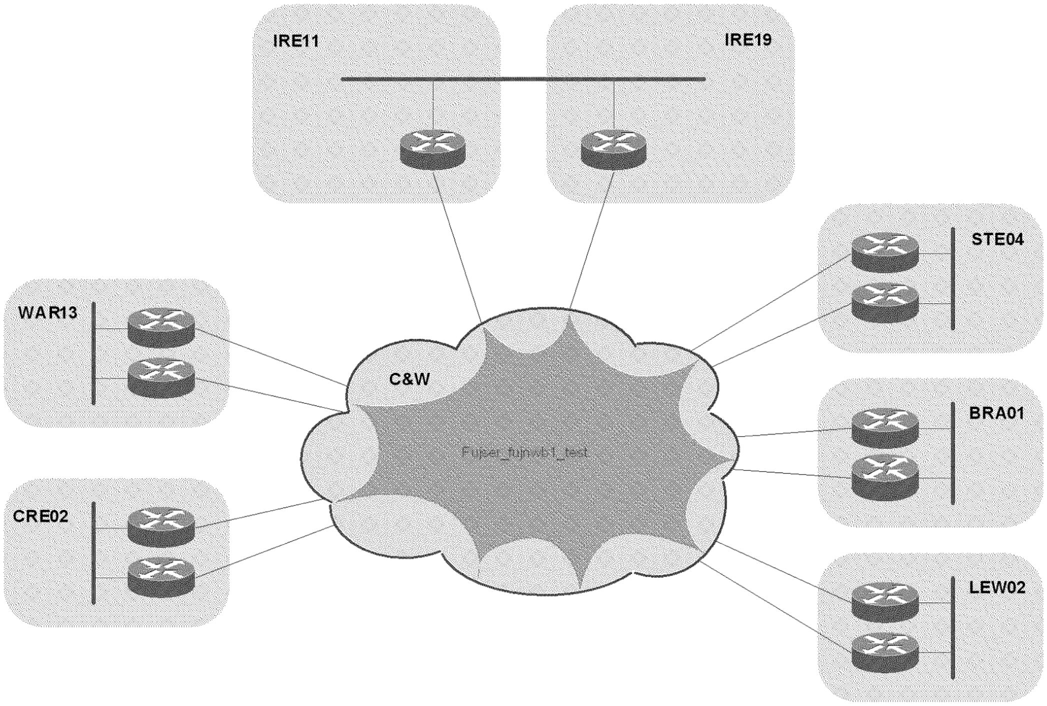


Figure 1 Support sites target design High level diagram.

Migration phase design high level diagram:

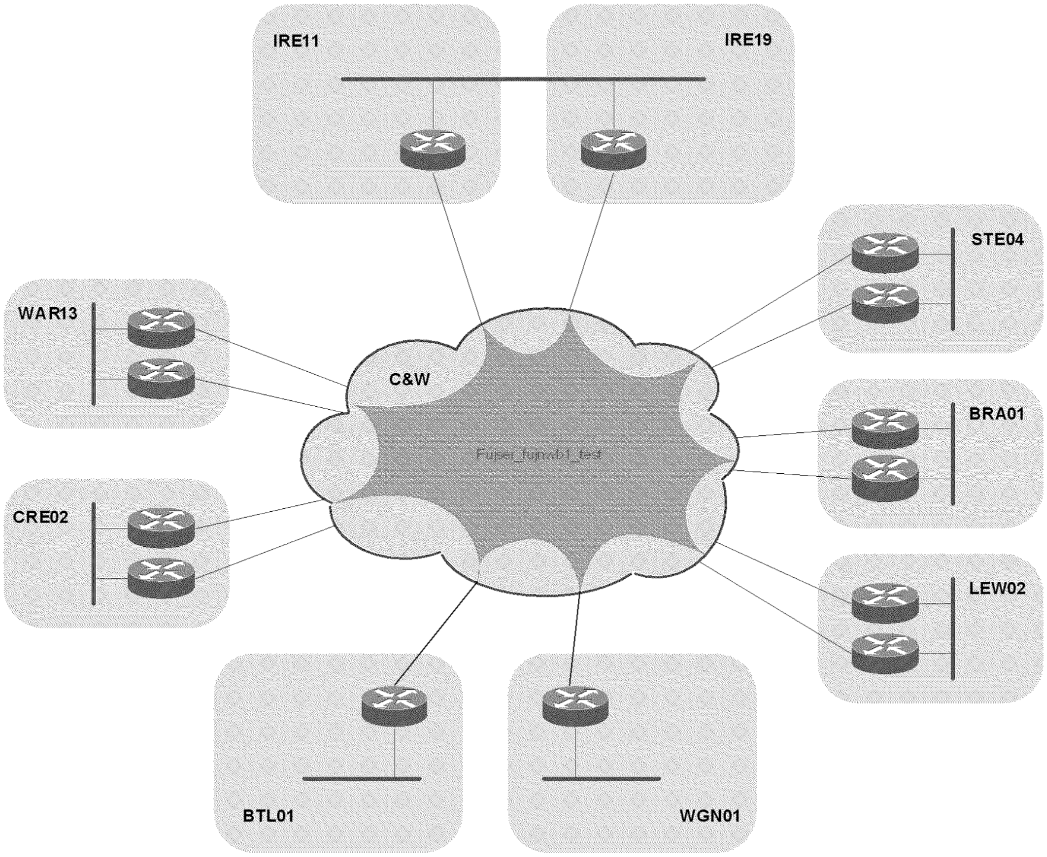


Figure 2 Support Networks (Migration phase) Four DC sites High level diagram.

2.1.2 Design overview

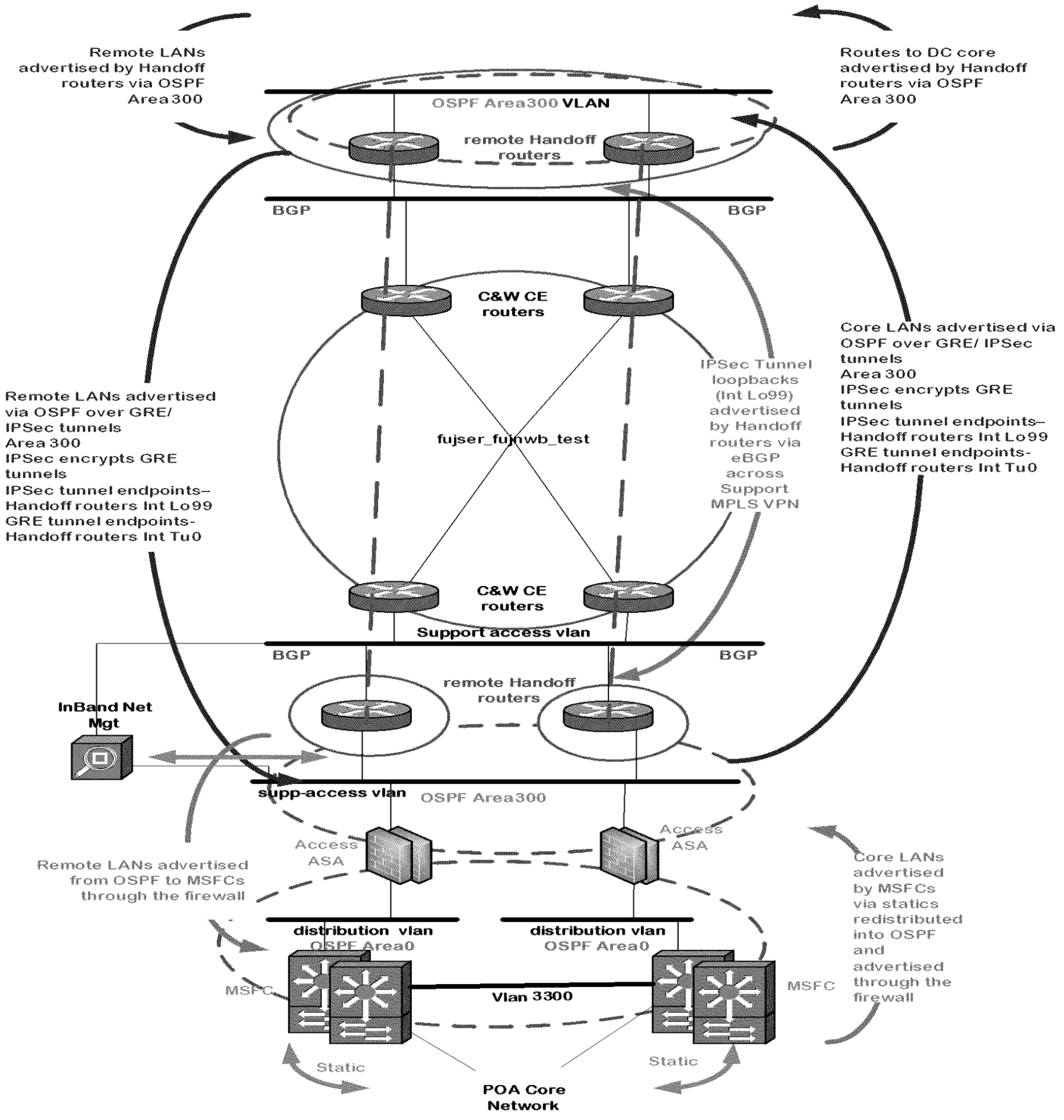

Remote LANs advertised by Handoff routers via OSPF Area 300
Routes to DC core advertised by Handoff routers via OSPF Area 300
OSPF Area300 VLAN
remote Handoff routers
BGP
BGP
C&W CE routers
Core LANs advertised via OSPF over GRE/ IPSec tunnels Area 300 IPSec encrypts GRE tunnels IPSec tunnel endpoints– Handoff routers Int Lo99 GRE tunnel endpoints- Handoff routers Int Tu0
IPSec Tunnel loopbacks (Int Lo99) advertised by Handoff routers via eBGP across Support MPLS VPN
Remote LANs advertised via OSPF over GRE/ IPSec tunnels Area 300 IPSec encrypts GRE tunnels IPSec tunnel endpoints– Handoff routers Int Lo99 GRE tunnel endpoints- Handoff routers Int Tu0
fujser_fujnwb_test
C&W CE routers
Support access vlan
BGP
BGP
remote Handoff routers
InBand Net Mgt
supp-access vlan
OSPF Area300
Access ASA
Access ASA
Remote LANs advertised from OSPF to MSFCs through the firewall
Core LANs advertised by MSFCs via statics redistributed into OSPF and advertised through the firewall
distribution vlan OSPF Area0
distribution vlan OSPF Area0
MSFC
Vlan 3300
MSFC
Static
Static
POA Core Network

Figure 3 Traffic flow diagram TBC when the next version of the DC LAN LLD is issued.

Remote HNG-x Support workstation on Horizon LAN – The generic connectivity between HNG-x workstations and Horizon LAN with respect to IRE11 & 19 bound traffic is thus; there will be no re-addressing on the existing remote support sites presently using the Horizon IP range IRRELEVANT The new HNG-X build support workstation will be assigned a Horizon IP address in the IRRELEVANT range if the Horizon LAN for the platform already exists at the remote site. The allocated IP address will then be statically NAT on the local Horizon firewalls to a HNG-X IP address in the IRRELEVANT range. The local Horizon firewalls are the demarcation between the HNG-X and the existing Horizon based networks, as shown in figure 3 above.

Traffic coming from each remote site will be source NATed to a HNG-X IRRELEVANT IP address.

Destination networks in IRE11 and 19 will not be NATed, as HNG-X IRRELEVANT range will be visible to Horizon remote networks.

Remote HNG-x Support workstation on HNG-x LAN – If an Horizon LAN does not exist, a new HNG-x LAN will be created on the new HNG-x IRRELEVANT remote support IP range. This will be subject to switch port allocation and accessibility to the HNG-x switch platforms

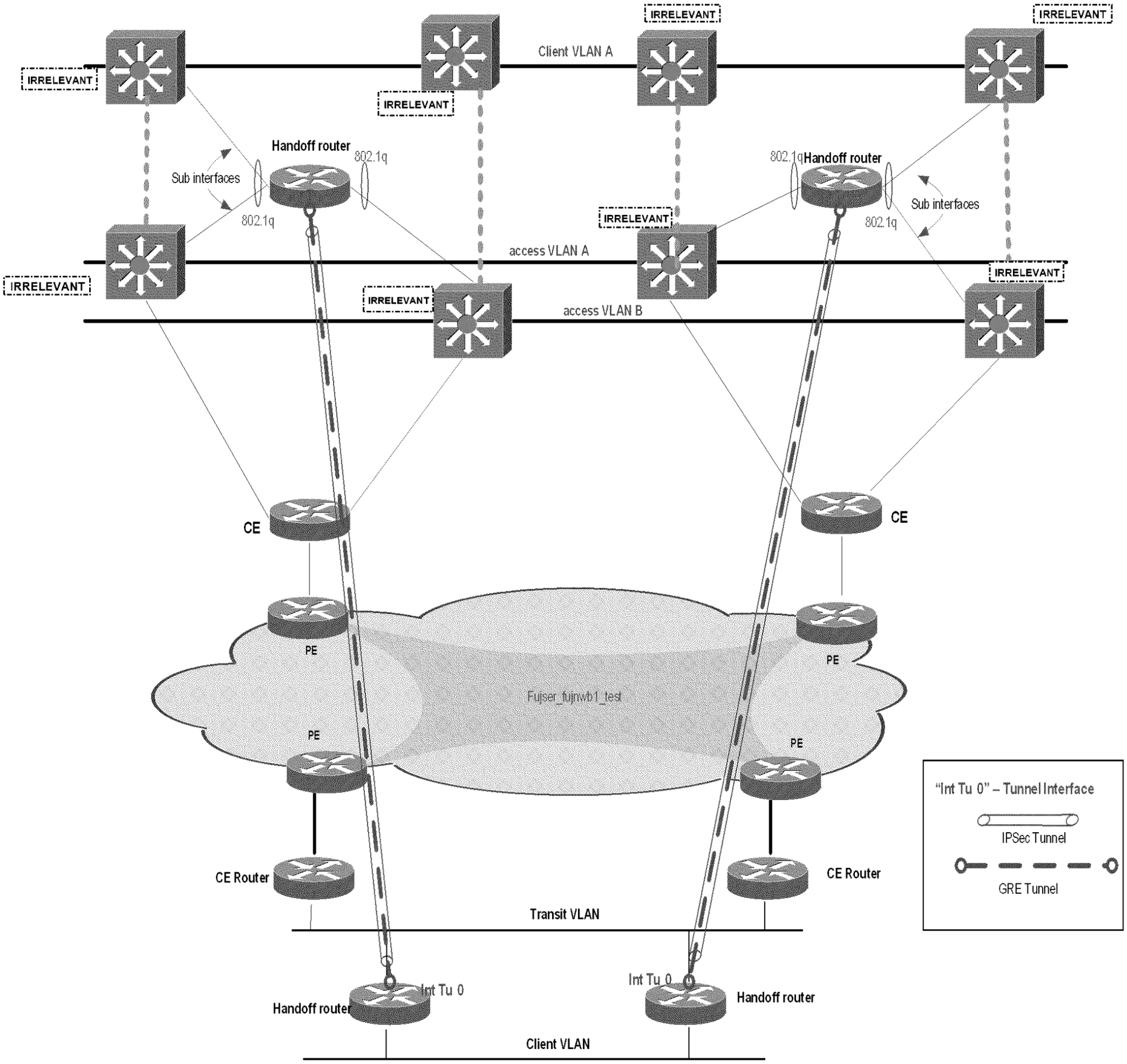


Figure 4 Generic GRE tunnel diagram

The Support network will follow the "Handoff router" model as enumerated in the WAN networks LLD (DESNETHLD0009). The "Handoff" router model will run GRE tunnelling from "Handoff" routers in the DC to "Handoff" routers at the remote client LAN and the GRE tunnels will be further secured using IPSec tunnelling as shown above in figure 4.

There will be no mesh tunnels; the primary remote handoff router will terminate its tunnels on pi11nrtr006 in IRE11. The secondary remote handoff router will terminate its tunnels on pi19nrtr006 in IRE19. The tunnels will back up each other and the failover will be invoked via IP SLA tracking and VRRP configured on the remote handoff routers to monitor the DC access VLAN in its routing table.

IRRELEVANT

Figure 5 Logical network diagram

Figure 5 depicts the logical routing topology for the support networks as seen in OSPF for each remote site.

2.1.3 IRE11 and IRE19

Issued in line with DC LAN LLD (DEVINFLLD0041 v0.3 draft).

The data centres will operate in an Active and DR state, while the network component will operate in an "Active" "Active" state. IRE11 will be the Active DC while IRE19 is the DR. Network traffic path does not determine the state of the data centres as failure of IRE11 access network does not necessarily invoke IRE19 as the DR.

The access layer of the network is primarily concerned with:

- WAN termination
- Network edge security enforcement and DMZ provision
- Inter-data centre connectivity at layer 2 and layer 3

Access layer network components within each Ireland Data Centre include 1 x C&W CE Router, 2 x Cisco catalyst 6513 series switches with integrated ACE module and MSFC, multiple Cisco ASA 5540's and multiple Cisco 2811 handoff routers two of which are used in this design proposal to cater for support access IPSEC termination/handoff. The handoff router Cisco 2811 devices provide routing between the FJ and C&W domain for HNG-X support traffic.

The access layer physical switches will provide high availability and resiliency across the access layer domain whilst the ASA devices operate as an active/standby pair and provide security against unauthorized or malicious threats towards the distribution and core layers of the network.

All traffic will be encrypted via IPSec tunnels across the MPLS VPN between sites and terminated on the handoff routers. The handoff routers will be the demarcation between clear and encrypted traffic. The encrypted tunnels will carry all live and test support traffic from BRA01, LEW02 and from the rest of the remote support site both for user data and network management.

The distribution layer of the network is primarily concerned with:

- Inter Access layer DMZ connectivity
- Distribution security enforcement with IPS/IDS

Distribution layer network components within each Ireland Data Centre include multiple ASA 5540's, 2 x McAfee Intrashield IPS 3000's and 2 x MSFC routers. The ASA devices within this layer are the same ASA devices as those residing in the access layer. The ASA firewalls provide a security policy enforcement point between the access and distribution layers. The IPS components operate inline as transparent layer 2 devices and provide further security against malicious/suspect traffic through pattern matching against known signatures.

The core layer of the network is primarily concerned with:

- High speed routing (or layer 3 switching)
- Inter-data centre connectivity at layer 2 and layer 3
- Core security enforcement and DMZ provision with IPS

Core layer network components within each Ireland Data Centre include 2 x Cisco catalyst 6513 series switches with integrated ACE module, MSFC module and FWSM. The MSFC devices provide routing between the core and distribution layers of the network. The ACE modules in either switch operate as an active/standby pair and provide a virtualized service for backend servers residing on core layer LANs. There is no requirement for server IP addressing virtualization in the support environment.

Two core layer physical switches (Cisco 6513's), provide high availability and resiliency across the core layer domain, the FWSM's operate as an active/standby pair and provide a final security policy enforcement point to critical systems residing on core LANs in the network.

In line with the Data Centre LAN Design – DEVINFLLD0041 the ASA devices are to be configured with interface security levels set to 0. Used in conjunction with "same-security-traffic permit inter-interface" this sets all interfaces as untrustworthy requiring an ACL to be applied to the interface to allow traffic to pass through an interface.

The below table defines the preferred ASA Firewall interface security configuration model.

INTERFACE TYPE	SECURITY LEVEL
Inside	0
Outside	0
DMZ	0
State	Default

Table 1 ASA Interface Security

DC Support Networks ACCESS/DMZ: Physical Diagram.

The following are installed in IRE11 and 19;

Ire11

2 x Cisco catalyst 6513 with integrated ACE and MSFC

2 x Cisco catalyst 6513 with integrated ACE, MSFC and FWSM

Multiple Cisco ASA 5540

Multiple Cisco 2811

2 x McAfee IPS

Ire19

2 x Cisco catalyst 6513 with integrated ACE and MSFC

2 x Cisco catalyst 6513 with integrated ACE, MSFC and FWSM

Multiple Cisco ASA 5540

Multiple Cisco 2811

2 x McAfee IPS

IRRELEVANT

Figure 6 Data Centre Support Access physical

All LAN devices will be connected as shown in the physical diagram inline with DC LAN LLD (DEVINFLLD0041).

KIT Name	Int. Loopback 99	Int. Loopback 100	Management Int.
IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT
IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT

Table 2 DC Handoff routers

DC Support Networks ACCESS/DMZ: Logical Diagram.

Interface Loopback 100 will be used to manage the handoff routers.

Interface Loopback 99 will be used as IPSec/GRE endpoints. This will be further explained in the

IPSec/GRE sections.

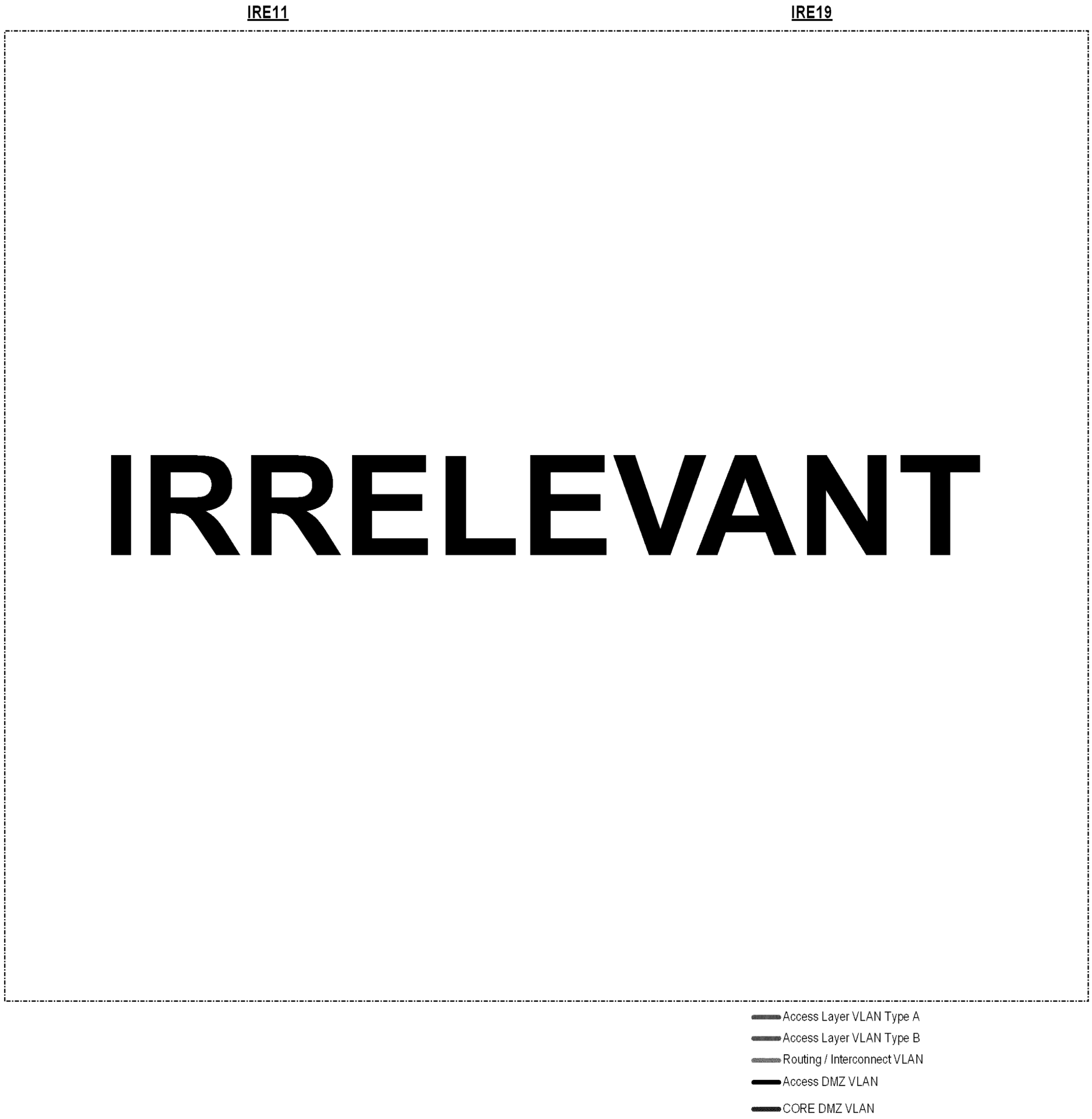

IRE11
IRE19
IRRELEVANT
▬ Access Layer VLAN Type A
▬ Access Layer VLAN Type B
▬ Routing / Interconnect VLAN
▬ Access DMZ VLAN
▬ CORE DMZ VLAN

Figure 7 Data Centre Support Access logical

Layer 2 will be configured as shown in figure 7 above and inline with DC LAN LLD (DEVINFLLD0041).

The Network Management/support servers in IRE11 and IRE19 data centre are connected to the core and access switches in a DMZ; the Network Management servers to the core and the SAS/SSM/RSA servers to the access. The management tools and servers will be used for secure support access into the Data centres, Post Office branches and other remote network equipment. As depicted in the network management LLD (DEVINFLLD0045), HP OpenView and CiscoWorks will have access to all network equipment and application servers within the data centres and to the Client access routers.

At each data centre, two Catalyst switches are installed in the Access Layer and two at the Core Layer for resilience as header and footer switches. HP Openview, Cisco Works and all other support servers will use two NIC's; primary NIC connects to header switch and the other to footer switch in IRE11 and 19.

In the Header/Footer switch connection; the Header switch is
is the preferred switch for

- Spanning tree, Footer switch backs it up.
- Data over bonded links on dual eth attached devices Blade / individual servers
- In the case of HO routers the header would normally take the traffic in the active standby model

The Footer switch backs up the Header switch for all of the above functions.

IRE11 IRE19

IRRELEVANT

Figure 8 Data Centre Support Access routing

2.1.3.1 External Routing:

eBGP will be used as the preferred routing protocol between the CE (in Ire11 and 19) and the handoff routers. eBGP peering will be between CE's and the handoff routers' interface IP addressing on VLAN IRRELEVANT and IRRELEVANT. There will be two eBGP peer commands on the handoff router "IRRELEVANT" and Ire11's CE, the same applies to between the handoff and the CE in Ire19. There will be no need for bgp multihop as eBGP peering across sites is not needed.

BGP will only be required to advertise IPSec tunnel endpoints interface loopback 99, as specified in the figure 8 above.

2.1.3.2 Internal Routing:

Inline with the DC LAN LLD (DEVINFLLD0041), OSPF is the preferred routing protocol for internal routing. OSPF area 300 has been designated as the support client access OSPF area id. The core of the network at the date centre will be configured as Area 0 with the client ASA firewalls serving as the OSPF Area Border routers (ABR) into Area 0. Only routes specifically allowed through the firewalls will be allowed into area0.

OSPF area 300 will be used to advertise all subnets as shown in figure 8, in addition it will advertise the management interface (loopback 100) and the GRE tunnel endpoints (interface tunnel 0).

There will be no redistribution between eBGP and OSPF locally in IRE11 and 19.

The ASA's will be configured with a higher OSPF priority so that they will always become the designated router (OSPF DR) and the backup designated router (OSPF BDR) on the support client access VLANs.

Note: OSPF traffic engineering will be included in the next update of the document.

2.1.3.3 GRE:

GRE tunnelling will be used to extend OSPF Area 300 from the Data centre support access into all remote support sites. GRE Tunnel interfaces will be configured as depicted in the various remote support BGP/OSPF/GRE diagrams below. Tunnel source will be interface loopback 99 on the local handoff router while the Tunnel destination will be the IP address of interface loopback 99 of the corresponding handoff router.

IP MTU size and TCP maximum segment size will be adjusted accordingly after tests have been carried out to determine what values will work best.

2.1.3.4 IPSec:

IPSec will be used to secure the GRE tunnels across the C&W MPLS VPN. IPSec will provide secure tunnels between two peers namely the handoff routers in the DC and the handoff routers at each remote site.

IPSec tunnels are formed when an IPSec peer recognizes a sensitive packet; the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. With IPSec you define what traffic is “sensitive” between the two IPSec peers by configuring access lists and applying these access lists to interfaces by way of crypto map sets. The access lists used for IPSec (crypto access list) are used only to determine which traffic should be protected by IPSec, not which traffic should be blocked or permitted through the interface. The crypto access lists will only permit traffic with GRE tunnel endpoints as sensitive traffic between sites.

The steps for IPSec configuration are as follows

1. Create Crypto Access List.

   Since we are securing GRE Tunnels;

   - IRE 11 & 19; “interface loopback 99” will be the source networks and the corresponding handoff router’s “interface loopback 99” at the client site will be the destination.
   - Client Site; “interface loopback 99” will be the source networks and IRE 11 & 19’s “interface loopback 99” will be the destination.

2. Define **IKE** to handle negotiation of protocols and algorithms based on local policy.
   - For encryption use “**aes 256”**
   - For authentication, a **pre-shared key** will be defined.

3. Defining Transform Sets: A Combination of Security Protocols and Algorithms.
   - For Encryption (ESP Encryption Transform), **esp-aes 256** (ESP with the 256-bit AES encryption algorithm) will be used
   - For Header Authentication (AH Transform), **ah-sha-hmac** { AH with the SHA (an HMAC variant) authentication algorithm} will be used

4. Create Crypto Map Sets.
   - This will be **ipsec-isakmp** based.

5. Apply Crypto Map Sets to handoff router Interfaces on VLAN IRRELEVANT and VLAN IRRELEVANT
6. Apply Crypto Map Sets to corresponding handoff router’s Interface FE0/0 at remote site.

2.1.3.5 DC Local Support Network

RMGA (RED) LAN: Physical

IRE11 **IRE19**

IRRELEVANT

IRE11 **IRE19**

Figure 9 IRE11/19 RMGA LAN physical

The local RMGA LAN in IRE 11 and 19 will be connected as shown in figure 9. New cabinets are being installed to accommodate each switch and handoff router.

KIT Name	Int. Loopback 99	Int. Loopback 100	Management Int.
IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT
IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT

Table 3 DC Local Support Handoff router

Layer 2:

The switches will be configured as VTP transparent mode and all trunks will be IEEE802.1q. VTP domain name will be determined by the RMGA support team.

VLAN IRRELEVANT and VLAN IRRELEVANT will be used as an access VLAN connecting the local site support handoff routers to the access LAN in the Data centres.

VLAN IRRELEVANT (IRE11) will be the local RMGA LAN and it will serve as the management VLAN for the access switches IRRELEVANT

VLAN IRRELEVANT (IRE19) will be the local RMGA LAN and it will serve as the management VLAN for the access switches IRRELEVANT

IRE11 IRE19

IRRELEVANT

Figure 10 IRE11/19 RMGA LAN Logical

OSPF area 300 will be used to advertise all subnets as shown in figure 10.

2.1.3.6 IRE11 & IRE19 Acceptance into Service Criteria

This section provides some criteria for Acceptance into Service tests to be performed. The AIS tests will show conformance of the implementation to the design but are not exhaustive and need to be performed in conjunction with other tests which are within the remit of the implementation teams.

The local Hand-Off routers at IRE11 and IRE19, respectively IRRELEVANT and IRRELEVANT are directly attached to the HNG-X infrastructure so the AIS criteria for IRE11 and IRE19 will be different from other support sites.

- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OSPF Area 300 for the following support LANs
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
- IRRELEVANT and IRRELEVANT will learn routes via OPSF Area 300 for the following support LANs
    - IRRELEVANT
    - IRRELEVANT

2.1.4 BRA01

The following will be installed at BRA01;

2x Cisco 2811 – Handoff routers

2x Catalyst 2960 – Access switch.

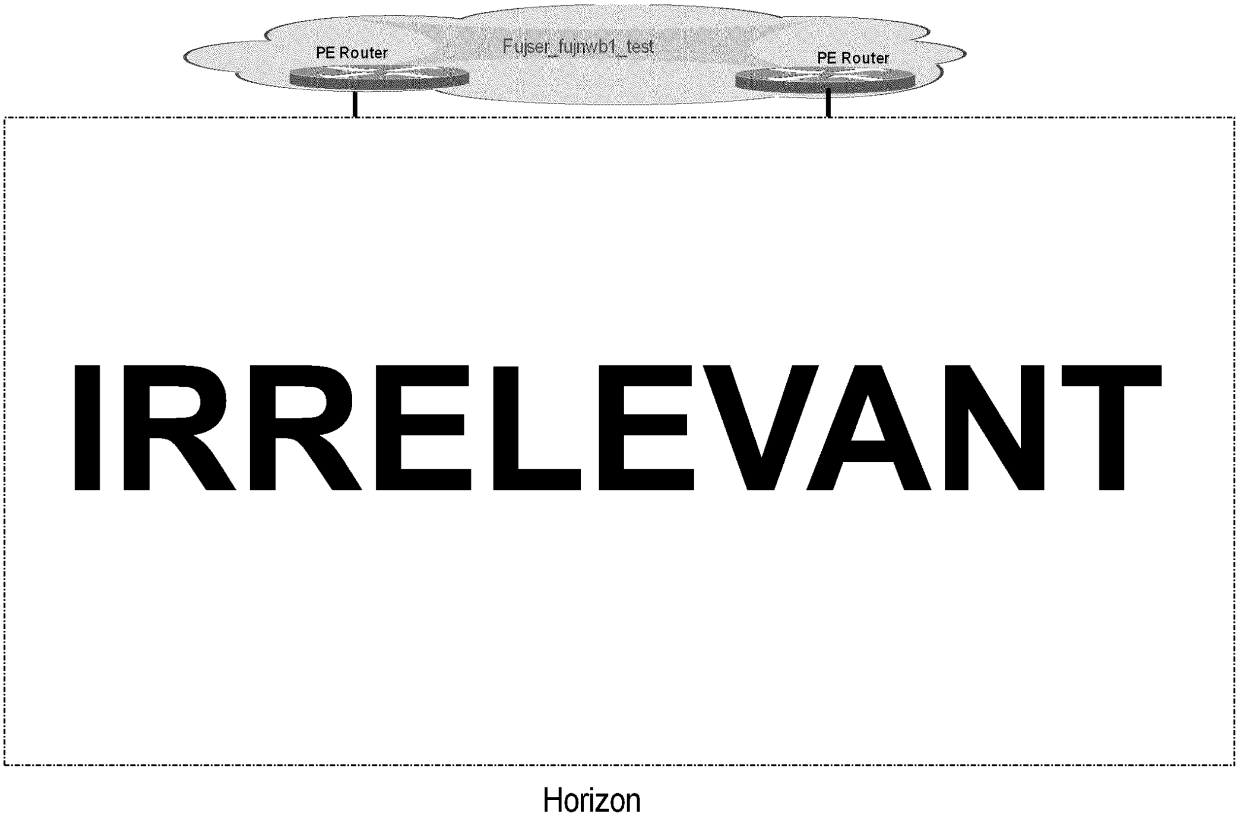


Figure 11 BRA01 Support transit Network Physical

All LAN devices will be connected as shown in the physical diagram for resiliency. There will be no single point of failure on the LAN.

The support team will determine where to install the kits.

Interface Ethernet 0 is configured as a trunk port on IRRELEVANT to carry the new HNGx to Horizon transit DMZ.

To interconnect the Horizon – HNG switches, fa0/19 has been allocated on switches IRRELEVANT These will be cabled up with cross over cables.

KIT Name	Int. Loopback 99	Int. Loopback 100	Int. VLAN 915	Management Int.
IRRELEVANT				
IRRELEVANT				
IRRELEVANT				
IRRELEVANT				

Table 4 BRA01 LAN info

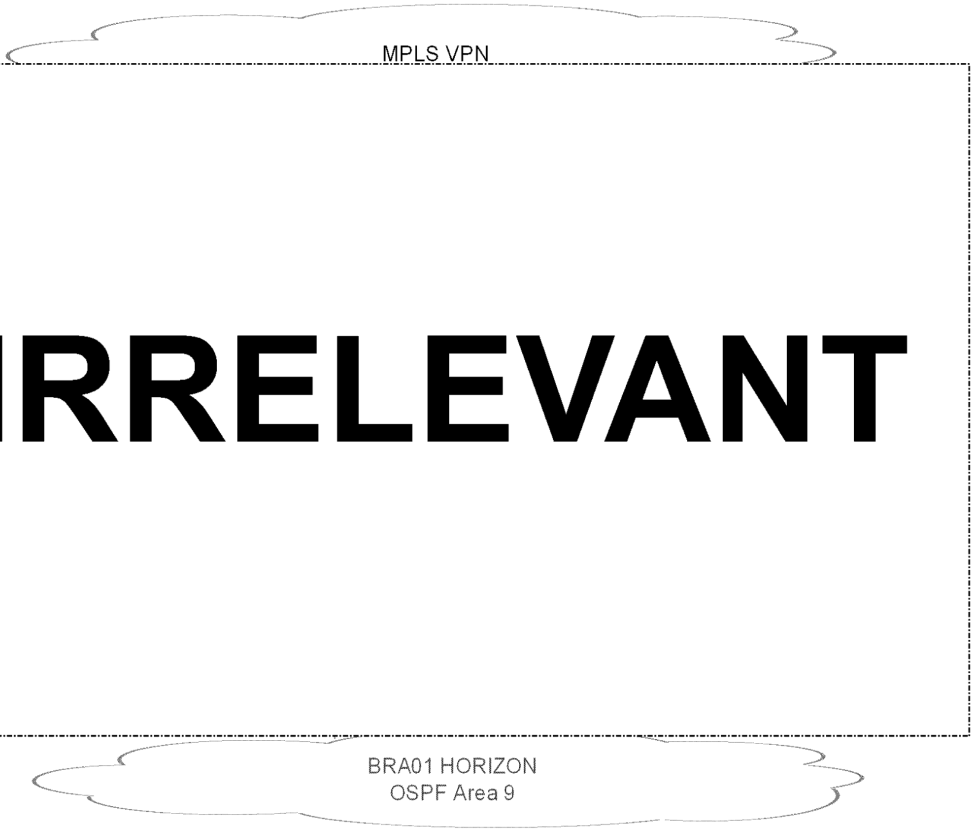


Figure 12 BRA01 Support transit network Layer 3 diagram

Layer 2:

The switches will be configured as VTP transparent mode and all trunks will be IEEE802.1q. VTP domain name will be determined by the RMGA support team.

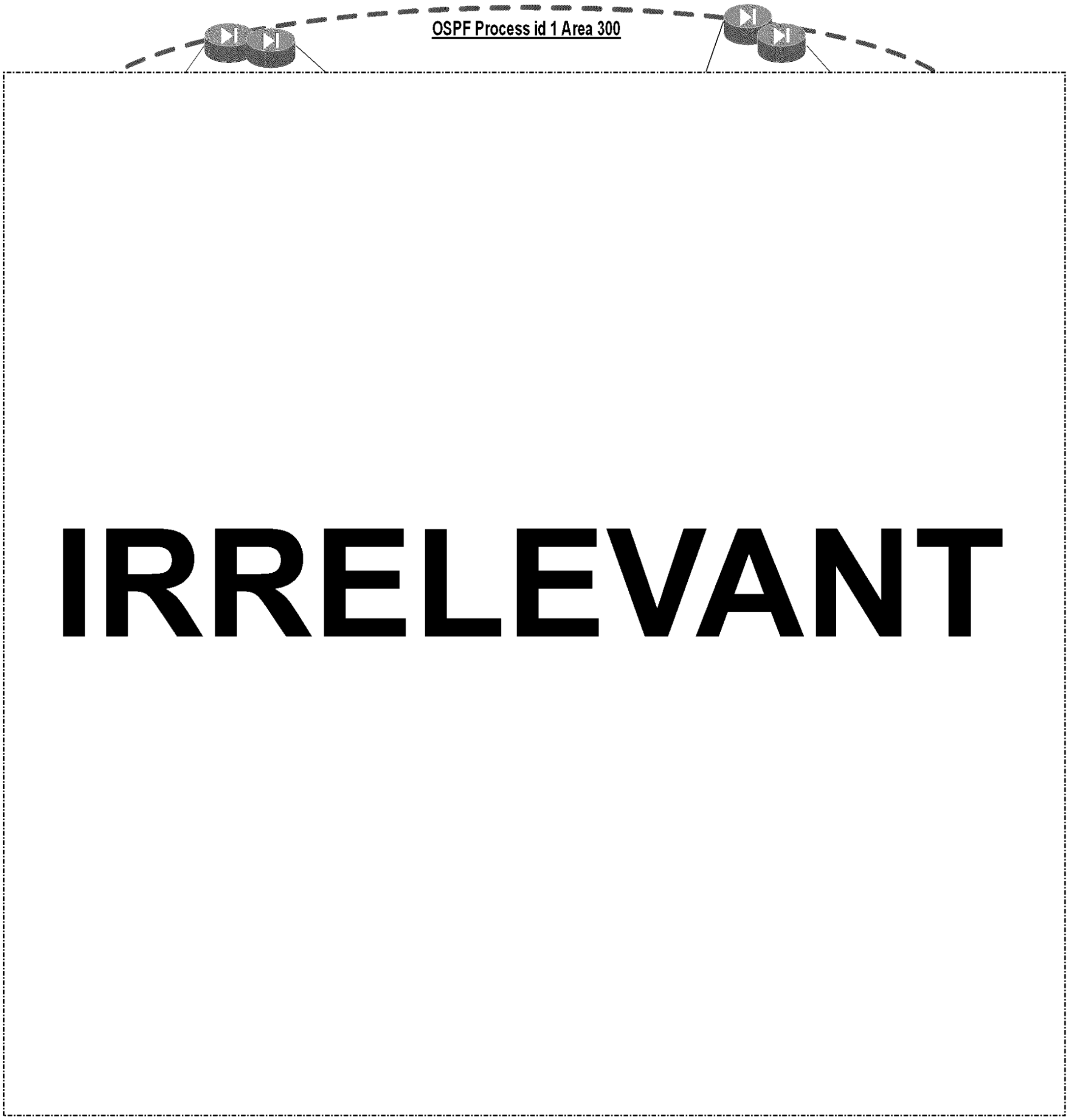
VLAN IRRELEVANT will be used as an access VLAN connecting the support VRF interface on the CE with interface FE0/0 on the handoff routers. It will also serve as the management VLAN for the access switches IRRELEVANT and IRRELEVANT

VLAN IRRELEVANT will be the local transit LAN connecting HNG-X handoff routers to Horizon firewalls and will have the handoff router's VRRP address as the default gateway.

High availability:

VRRP group 1 will be configured on interface FE0/1 on IRRELEVANT and IRRELEVANT The virtual router master for the group will be IRRELEVANT, configured with a priority 110. The virtual router backup fro group 1 will be IRRELEVANT with a priority of 100. VRRP tracking will be used to dynamically failover between the master and the backup. The IP address to be tracked will be IRRELEVANT, the IP address configured on interface IRRELEVANT on IRRELEVANT

IRRELEVANT and IRRELEVANT will operate as a failover High availability (HA) pair so will have the same IP address on IRRELEVANT.



IRRELEVANT

Figure 13.BRA01 BGP/OSPF/IPSEC/GRE diagram

External Routing:

eBGP will be used as the preferred routing protocol between the CE (in BRA01) and the handoff routers as depicted in figure 13. eBGP peering will be between CE's and the handoff routers' interface IP addressing on VLAN IRRELEVANT as shown. There will be one eBGP peer commands on the primary handoff router IRRELEVANT and its BRA01's corresponding CE, the same applies to between the secondary handoff and it corresponding CE. There will be no need for bgp multihop as eBGP.

BGP will only be required to advertise IPSec tunnel endpoints interface loopback 99, as specified in the figure 13 above.

GRE :

GRE tunnelling will be used to extend OSPF Area 300 from the Data centre support access into all remote support sites. GRE Tunnel interfaces will be configured as depicted in figure 13. Tunnel source will be interface loopback 99 on the BAR01 handoff router while the Tunnel destination will be the IP address of interface loopback 99 of the corresponding IRE11/19 handoff router.

GRE Interface Tunnel 0 will be configured between handoff routers in IRE11/19 and handoff routers in BRA01.

IP MTU size and TCP maximum segment size will be adjusted accordingly after tests have been carried out to determine what values will work best.

IPSec:

The steps for IPSec configuration are as follows

1. Create Crypto Access List - To secure the GRE Tunnel;

   IRE 11 & 19; "interface loopback 99" will be the source networks and the corresponding handoff routers "interface loopback 99" at the client site will be the destination.

   BRA01; "interface loopback 99" will be the source networks and IRE 11 & 19's "interface loopback 99" will be the destination.

2. Define IKE to handle negotiation of protocols and algorithms based on local policy.

   For encryption use "aes 256"

   For authentication, a pre-shared key will be defined.

3. Defining Transform Sets: A Combination of Security Protocols and Algorithms.

   For Encryption (ESP Encryption Transform), esp-aes 256 (ESP with the 256-bit AES encryption algorithm) will be used

   For Header Authentication (AH Transform), ah-sha-hmac { AH with the SHA (an HMAC variant) authentication algorithm} will be used

4. Create Crypto Map Sets.

   This will be ipsec-isakmp based.

5. Apply Crypto Map Sets to handoff router Interfaces on IRRELEVANT and IRRELEVANT.

6. Apply Crypto Map Sets to corresponding handoff router IRRELEVANT and IRRELEVANT VLAN IRRELEVANT Interfaces

Internal Routing: HNG-X and Horizon -

OSPF is the preferred routing protocol for internal routing. OSPF area 300 has been designated as the support client access OSPF area id. Area 300 in the data centres will be extended to the BRA01 handoff routers over a GRE tunnel, which is encrypted in IPSec tunnel over C&W's MPLS VPN as shown in figures 13 and 14.

OSPF area 300 will advertise the LAN subnet IRRELEVANT, in addition it will advertise the management interface (loopback 100) and the GRE tunnel endpoints (interface tunnel 0).

There will be no OSPF neighbours formed on VLAN IRRELEVANT and there will be no OSPF routing between HNG-X (area 300) and Horizon (area 9).

The Handoff routers will point (via static routing) the NAT IP addresses IRRELEVANT, IRRELEVANT, IRRELEVANT to firewalls IRRELEVANT High availability (HA) IP address IRRELEVANT. To dynamically failover the static routing, each handoff router will be configured to track interface FE0/1's IP routing (track xx interface FE0/1 ip routing). Each static route will be configured to reference the tracking ID (xx) as configured and then redistributed into area 300. This will allow the static routes configured on the Primary/secondary HO routers dynamically failover.

All OSPF routing and static routes (redistributed into Area 300) on the secondary HO router will be configured with a higher metric cost for LIVE traffic so that the primary handoff router will always be preferred for outgoing/incoming traffic.

Static routes will be configured on the pair IRRELEVANT pointing the HNG-X IRRELEVANT IP address to the Handoff routers VRRP IP address IRRELEVANT. The static route will be redistributed on IRRELEVANT into Horizon's OSPF area 9. The Horizon ABR routers (presumably IRRELEVANT and IRRELEVANT) will be configured with the "area range (no advertise)" to prevent the advertising of the HNG-X IRRELEVANT IP range outside BRA01 into Horizon OSPF backbone area. All other OSPF devices in Horizon OSPF Area 9 will see HNG-x routes advertised to them via IRRELEVANT

Management of the layer 2 access switches will be via static routes configured on the handoff routers IRRELEVANT and IRRELEVANT pointing each switch management interface out the HO router IP address for interface FE0/0. These static routes will be redistributed into Area 300.

There will be no redistribution between eBGP and OSPF locally in BRA01.

IRRELEVANT

Figure 14 BRA01 HNGx - Horizon integrated Layer 3 Support Workstation LAN

Support Workstations:

BRA01 assigned IP NAT range – IRRELEVANT, IRRELEVANT, IRRELEVANT

Presently as shown in figure 13, Horizon – Corporate IP NAT range is (Horizon) IRRELEVANT – (Corporate) IRRELEVANT. This will be expanded as corporate has provided the IRRELEVANT IP NAT range.

BRA01 NAT addresses: The following will be NAT configured on IRRELEVANT to allow for software delivery and SAS server connectivity to IRE11 and 19 from BRA01 corporate sourced traffic.

Node	Source IP Address	HNG-X NAT IP Address	Comment
CMWKS06	IRRELEVANT	IRRELEVANT	CM Workstation 06
CMWKS02			CM Workstation 02
CMWKS05			CM Workstation 05
PRJ000405DT			CM Workstation 07
Support traffic			Support PAT IP address for terminal access to IRE11/19.
IRRELEVANT			IRE19 SAS server
			IRE19 SAS server
			IRE11 SAS server
			IRE11 SAS server
			IRE 19 Corporate proxy
			IRE 19 Corporate proxy
			IRE 11 Corporate proxy
			IRE 11 Corporate proxy
			IRE11 SAS server
			IRE19 SVI SAS server
			IRE19 RV MIG SAS server
			IRE19 RV ACC SAS server
			IRE19 LST SAS server
			IRE19 LST SAS server
			IRE19 LST Corporate Proxy

Table 5 BRA01 NAT table – Corporate to Horizon to HNG-X. - Now moved to corporate workstations LLD.

2.1.4.1 BRA01 Acceptance into Service Criteria

This section provides some criteria for Acceptance into Service tests to be performed. The AIS tests will show conformance of the implementation to the design but are not exhaustive and need to be performed in conjunction with other tests which are within the remit of the implementation teams.

- IRRELEVANT will show C&W CE router IRRELEVANT as a BGP neighbour
- IRRELEVANT will show C&W CE router IRRELEVANT as a BGP neighbour
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- a GRE tunnel can be built between br01nrtr001 and IRRELEVANT
- a GRE tunnel can be built between br01nrtr002 and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OSPF Area 300 for the following support LANs
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OPSF Area 300 for the following remote LANs
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT

- IRRELEVANT

2.1.5 LEW02

The following will be installed;

2x Cisco 2811 – Handoff routers

2x Catalyst 2960 – Access switch.

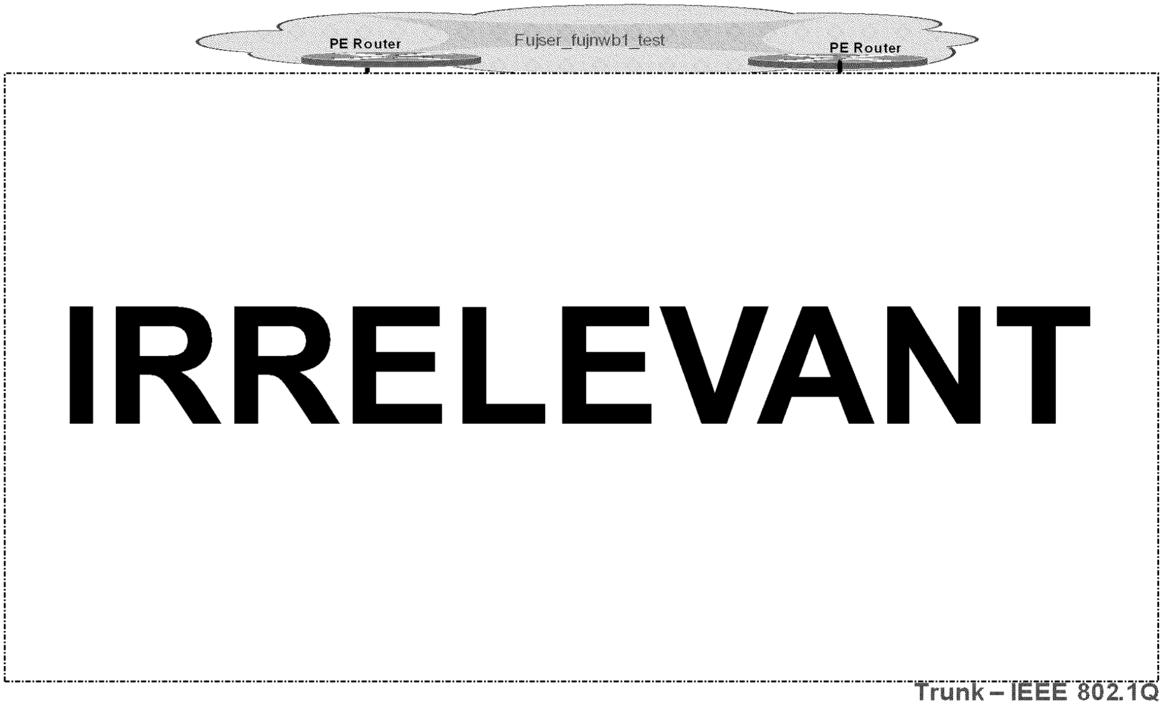


Figure 15 LEW02 Support transit Physical Network

All LAN devices will be connected as shown in the physical diagram for resiliency. There will be no single point of failure on the LAN.

The support team will determine where to install the kits and which switches on the existing infrastructure the catalyst 2960 switch trunk ports will connect to.

To interconnect the horizon – HNG-x switches, fa0/23 has been allocated on switches IRRELEVANT These will be cabled up with cross over cables as shown above.

KIT Name	Int. Loopback 99	Int. Loopback 100	Int. VLAN 914	Management Int.
IRRELEVANT	IRRELEVANT	IRRELEVANT	-	Int. Loopback 100
IRRELEVANT	IRRELEVANT	IRRELEVANT	-	Int. Loopback 100
IRRELEVANT	-	-	IRRELEVANT	Int. VLAN 914
IRRELEVANT	-	-	IRRELEVANT	Int. VLAN 914

Table 6 LEW02 LAN info

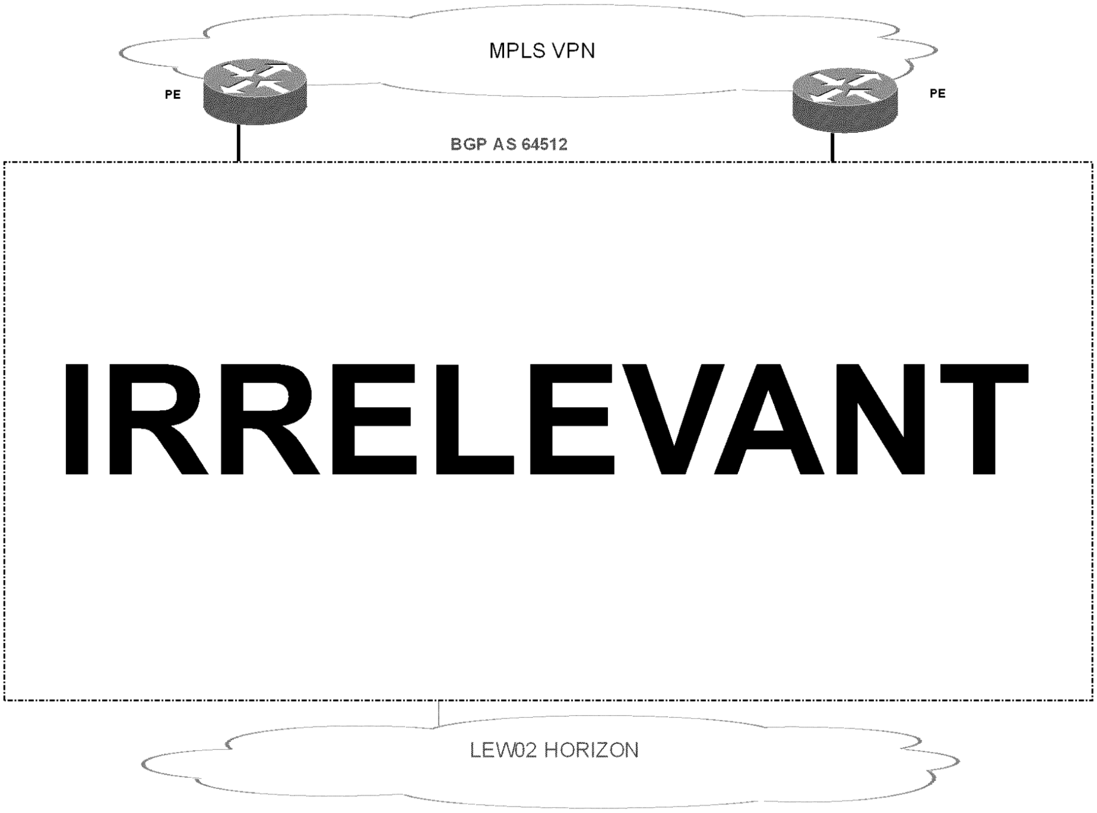


Figure 16 LEW02 Support transit network Layer 3 diagram

Layer 2:

The switches will be configured as VTP transparent mode and all trunks will be IEEE802.1q. VTP domain name will be determined by the RMGA support team.

VLAN IRRELEVANT will be used as an access VLAN connecting the support VRF interface on the CE with interface FE0/0 on the handoff routers. It will also serve as the management VLAN for the access switches IRRELEVANT and IRRELEVANT

Horizon VLAN IRRELEVANT will be the local transit LAN connecting HNG-X handoff routers to Horizon firewalls and will have the handoff router's VRRP address as the default gateway for all HNG-x traffic.

High availability:

VRRP group 1 will be configured on interface FE0/1 on IRRELEVANT and IRRELEVANT as shown above. The virtual router master for the group will be IRRELEVANT, configured with a priority 110. The virtual router backup for group 1 will be IRRELEVANT with a priority of 100. VRRP tracking will be used to dynamically failover between the master and the backup. The IP address to be tracked will be IRRELEVANT, the IP address configured on interface IRRELEVANT

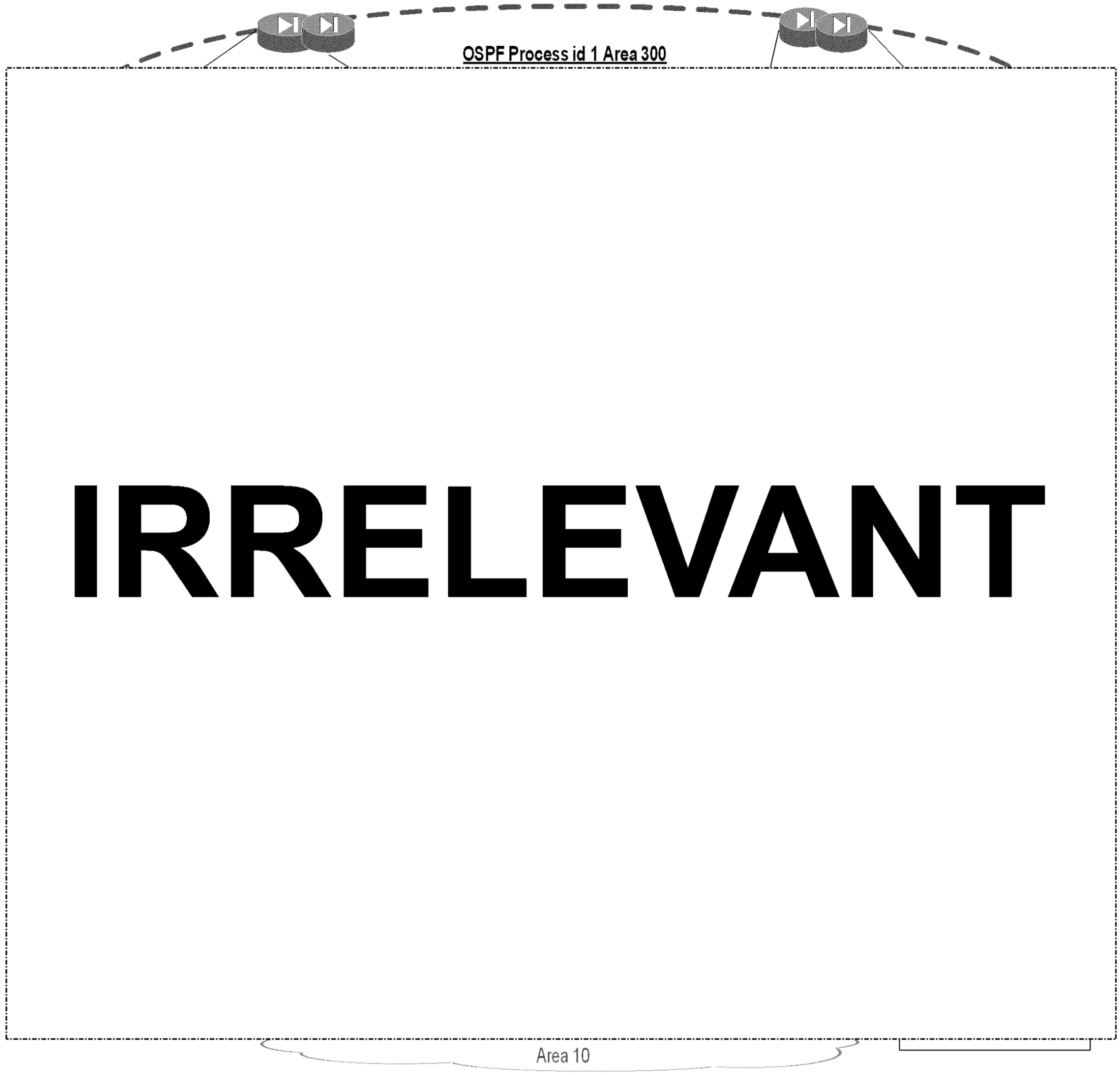


Figure 17 LEW02 BGP/OSPF/IPSEC/GRE diagram

External Routing:

eBGP will be used as the preferred routing protocol between the CE (in LEW02) and the handoff routers as depicted in figure 17. eBGP peering will be between CE's and the handoff routers' interface IP addressing on VLAN IRRELEVANT as shown. There will be one eBGP peer commands on the primary handoff router IRRELEVANT and its LEW02's corresponding CE, the same applies to between the secondary handoff and it corresponding CE. There will be no need for bgp multihop.

BGP will only be required to advertise IPSec tunnel endpoints interface loopback 99, as specified in the figure 17 above.

GRE :

GRE tunnelling will be used to extend OSPF Area 300 from the Data centre support access into all remote support sites. GRE Tunnel interfaces will be configured as depicted in figure 17. Tunnel source will be interface loopback 99 on the LEW02 handoff router while the Tunnel destination will be the IP address of interface loopback 99 of the corresponding IRE11/19 handoff router.

GRE Interface Tunnel 1 will be configured between handoff routers in IRE11/19 and handoff routers in LEW02.

IP MTU size and TCP maximum segment size will be adjusted accordingly after tests have been carried out to determine what values will work best.

IPSec:

Configure as depicted in section 2.1.3.4.

Internal Routing: HNG-X and Horizon -

OSPF is the preferred routing protocol for internal routing. OSPF area 300 has been designated as the support client access OSPF area id. Area 300 in the data centres will be extended to the LEW02 handoff routers over a GRE tunnel, which is encrypted in an IPSec tunnel over C&W's MPLS VPN as shown in figure 17.

There will be no OSPF neighbours formed on VLAN IRRELEVANT and there will be no OSPF routing between HNG-X (area 300) and Horizon (area 10).

OSPF area 300 will be used to advertise (via static routing redistributed into Area 300) the NAT subnets IRRELEVANT and IRRELEVANT. The static route will point to firewalls IRRELEVANT high availability (HA) IP address IRRELEVANT. To dynamically failover the static routing, each handoff router will be configured to track interface FE0/1's IP routing (track xx interface FE0/1 ip routing). Each static route will be configured to reference the tracking ID (xx) as configured and then redistributed into area 300. This will allow the static routes configured on the Primary/secondary HO routers dynamically failover. In addition Area 300 will advertise the management interface (loopback 100) and the GRE tunnel endpoints (interface tunnel 0).

Static routes will be configured on the pair IRRELEVANT pointing the HNG-X IRRELEVANT IP address to the Handoff routers VRRP IP address IRRELEVANT The static route will be redistributed on IRRELEVANT IRRELEVANT into Horizon's OSPF area 10. The Horizon ABR routers (presumably IRRELEVANT and IRRELEVANT) will be configured with the "area range (no advertise)" to prevent the advertising of the HNG-X IRRELEVANT IP range outside LEW02 into Horizon OSPF backbone area. All other OSPF devices in Horizon OSPF Area 10 will see HNG-x routes advertised to them via IRRELEVANT

Management of the layer 2 access switches will be via static routes configured on the handoff routers IRRELEVANT and IRRELEVANT, pointing each switch management interface out the HO router IP address for interface FE0/0. These static routes will be redistributed into Area 300.
There will be no redistribution between eBGP and OSPF locally in LEW02.

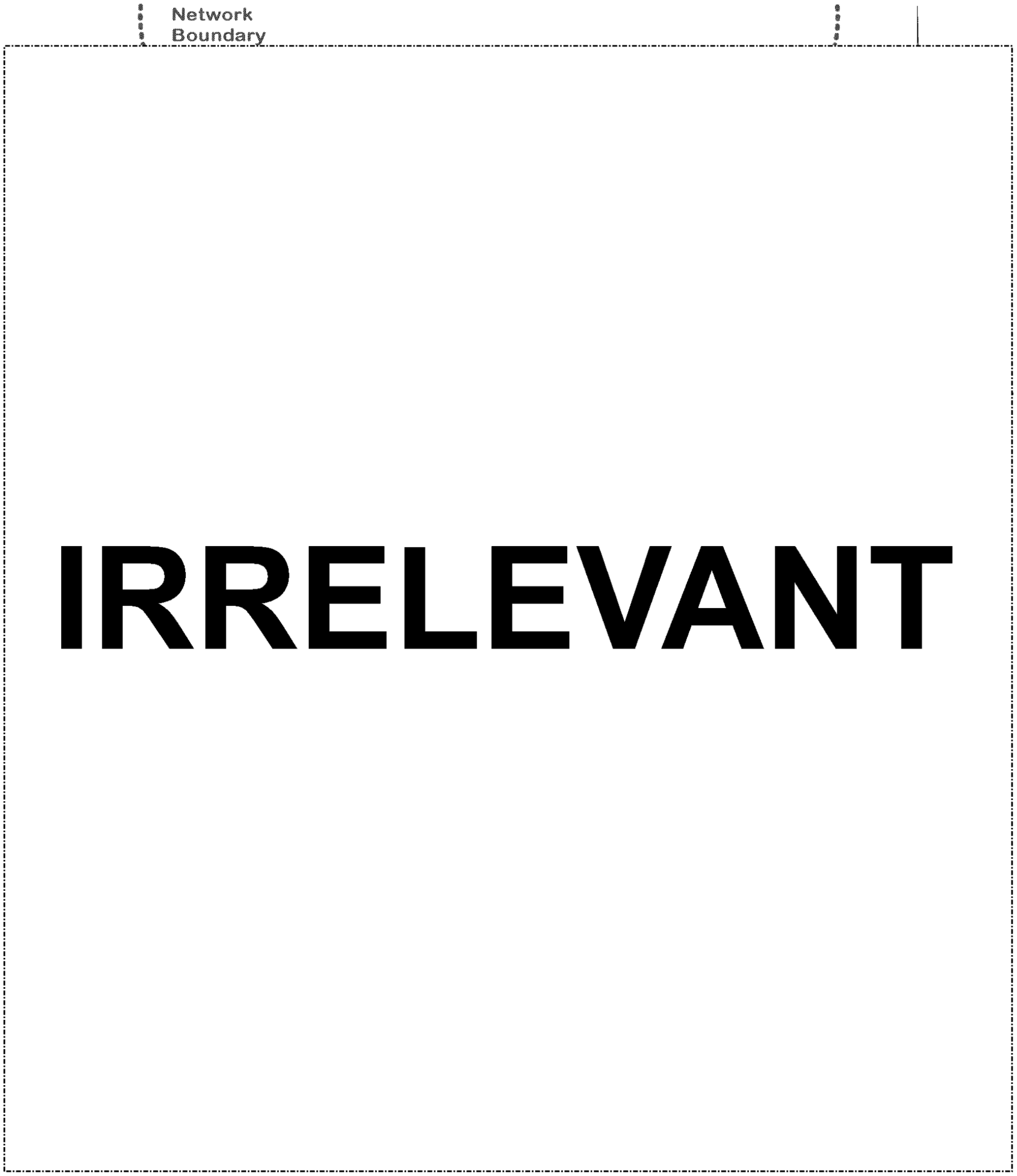


Figure 18 LEW02 HNGx - Horizon integrated Layer 3 Support Workstation LAN

2.1.5.1 LEW02 Acceptance into Service Criteria

This section provides some criteria for Acceptance into Service tests to be performed. The AIS tests will show conformance of the implementation to the design but are not exhaustive and need to be performed in conjunction with other tests which are within the remit of the implementation teams.

- IRRELEVANT will show C&W CE router IRRELEVANT as a BGP neighbour
- IRRELEVANT will show C&W CE router IRRELEVANT as a BGP neighbour
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- a GRE tunnel can be built between le02nrtr001 and IRRELEVANT
- a GRE tunnel can be built between le02nrtr002 and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OSPF Area 300 for the following support LANs
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OPSF Area 300 for the following remote LANs
    - IRRELEVANT (need to check this range is correct)
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT

2.1.6 CRE02

The following will be installed;

2x Cisco 2811 – Handoff routers

2x Catalyst 2960 – Access switch.

These will be installed 1st floor comms room racks 1B and 2B by the installed C&W CE's by the existing network – a Cisco 2500 router and a hub.

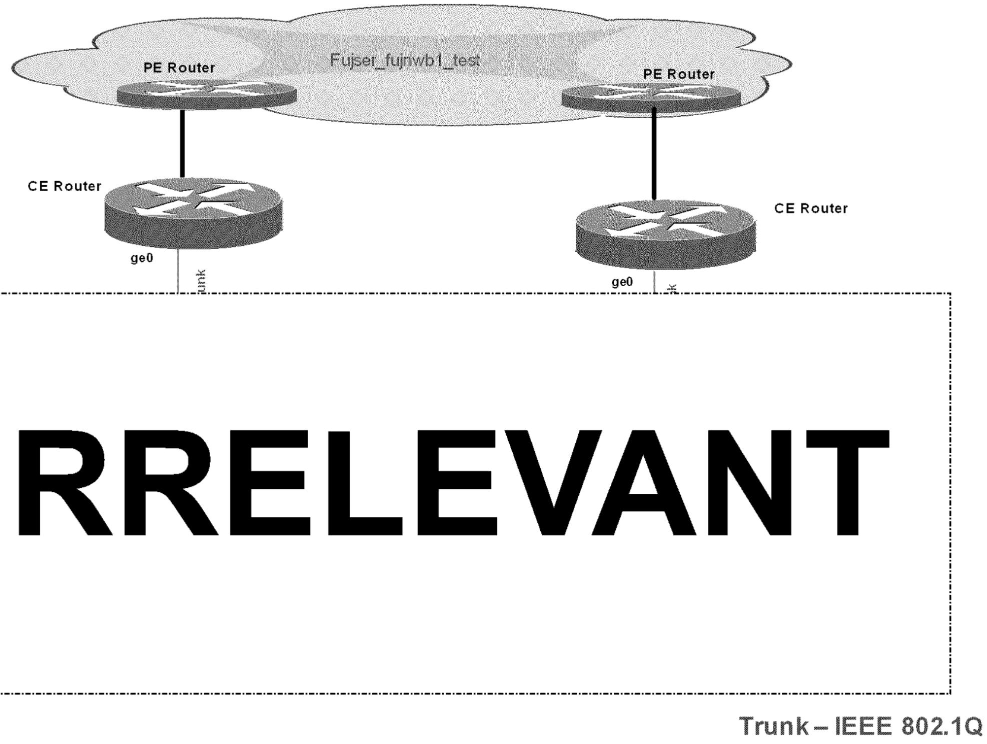
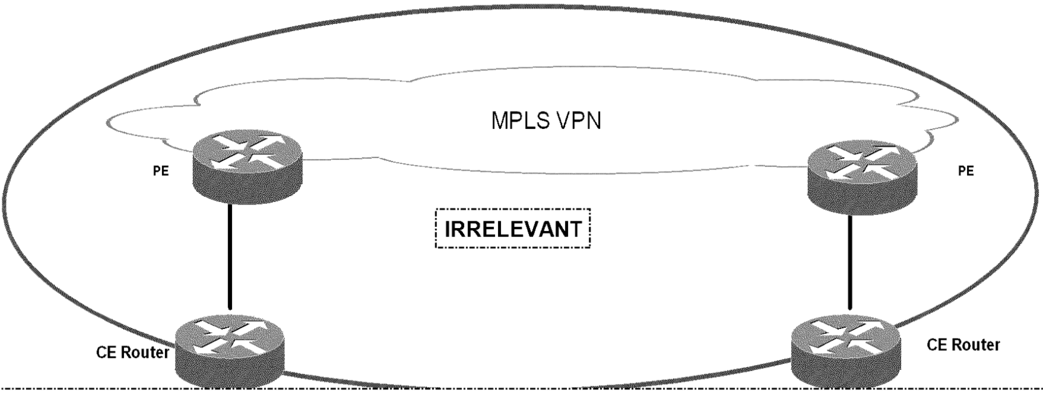


Figure 19 CRE02 Physical

All LAN devices will be connected as shown in the physical diagram for resiliency. There will be no single point of failure on the LAN.

KIT Name	Int. Loopback 99	Int. Loopback 100	Int. VLAN 916	Management Int.
IRRELEVANT				
IRRELEVANT				
IRRELEVANT				
IRRELEVANT				

Table 7 CRE02 LAN info



IRRELEVANT

Figure 20 CRE02 Layer 2/BGP/NAT diagram

Layer 2:

The switches will be configured as VTP transparent mode and all trunks will be IEEE802.1q. VTP domain name will be determined by the RMGA support team.

VLAN IRRELEVANT will be used as an access VLAN connecting the support VRF interface on the CE with interface FE0/0 on the handoff routers. It will also serve as the management VLAN for the access switches IRRELEVANT and IRRELEVANT.

VLAN IRRELEVANT will be configured as the local LAN.

High availability:

VRRP group 1 will be configured on interface FE0/1 on IRRELEVANT and IRRELEVANT. The virtual router master for the group will be IRRELEVANT, configured with a priority 110. The virtual router backup fro group 1 will be IRRELEVANT with a priority of 100. VRRP tracking will be used to dynamically failover between the master and the backup. The IP address to be tracked will be IRRELEVANT, the IP address configured on interface IRRELEVANT.

External Routing:

eBGP will be used as the preferred routing protocol between the CE (in BRA01) and the handoff routers as depicted in figure 20. eBGP peering will be between CE's and the handoff routers' interface IP addressing on VLAN IRRELEVANT as shown. There will be one eBGP peer commands on the primary handoff router IRRELEVANT and its BRA01's corresponding CE, the same applies to between the secondary handoff and it corresponding CE. There will be no need for bgp multihop.

BGP will only be required to advertise IPSec tunnel endpoints interface loopback 99, as specified in the figure 20.

Internal Routing:

OSPF is the preferred routing protocol for internal routing. OSPF area 300 has been designated as the support client access OSPF area id. Area 300 in the data centres will be extended to the CRE02 handoff routers over a GRE tunnel, which is encrypted in an IPSec tunnel over C&W's MPLS VPN as shown in figure 21 below.

OSPF area 300 will be used to advertise the LAN subnet IRRELEVANT shown, in addition it will advertise the management interface (loopback 100) and the GRE tunnel endpoints (interface tunnel 0).

Management of the layer 2 access switches will be via static routes configured on the handoff routers IRRELEVANT and IRRELEVANT, pointing interface VLAN IRRELEVANT IP addresses to CRE02.

There will be no redistribution between eBGP and OSPF locally in CRE02.

GRE :

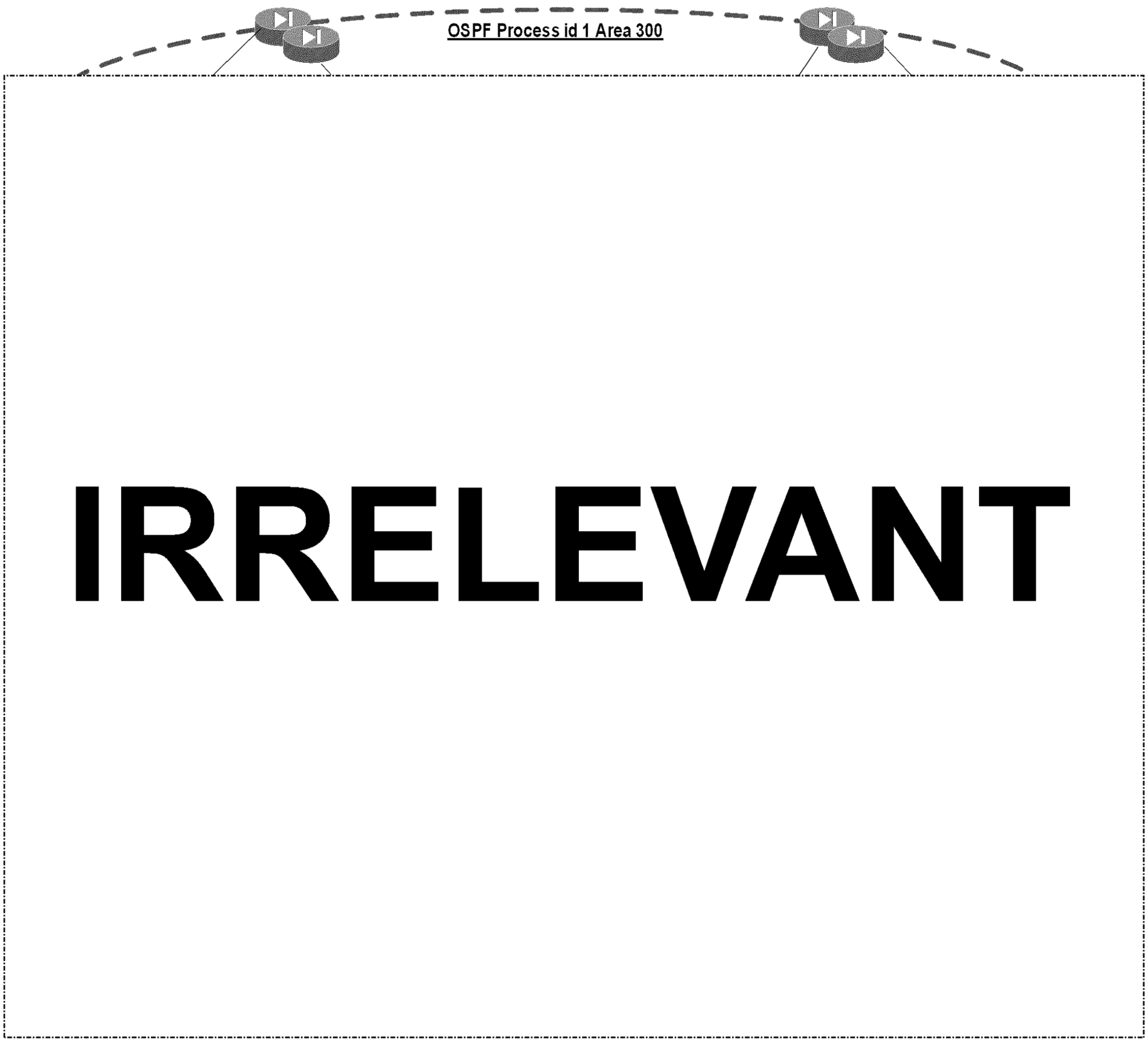
GRE tunnelling will be used to extend OSPF Area 300 from the Data centre support access into all remote support sites. GRE Tunnel interfaces will be configured as depicted. Tunnel source will be interface loopback 99 on the CRE02 handoff router while the Tunnel destination will be the IP address of interface loopback 99 of the corresponding IRE11/19 handoff router.

GRE Interface Tunnel 2 will be configured between handoff routers in IRE11/19 and handoff routers in CRE02.

IP MTU size and TCP maximum segment size will be adjusted accordingly after tests have been carried out to determine what values will work best.

IPSec:

Please refer to section 2.1.3.4.



IRRELEVANT

Figure 21 CRE02 Layer OSPF/GRE diagram

2.1.6.1 CRE02 Acceptance into Service Criteria

This section provides some criteria for Acceptance into Service tests to be performed. The AIS tests will show conformance of the implementation to the design but are not exhaustive and need to be performed in conjunction with other tests which are within the remit of the implementation teams.

- IRRELEVANT will show C&W CE router IRRELEVANT as a BGP neighbour
- IRRELEVANT will show C&W CE router IRRELEVANT as a BGP neighbour
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- a GRE tunnel can be built between IRRELEVANT and IRRELEVANT
- a GRE tunnel can be built between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OSPF Area 300 for the following support LANs
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OPSF Area 300 for the following remote LANs
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT

2.1.7 STE04

The following will be installed;

2x Cisco 2811 – Handoff routers

Access switches – Existing Horizon switches will be used for Handoff router connectivity as shown below.

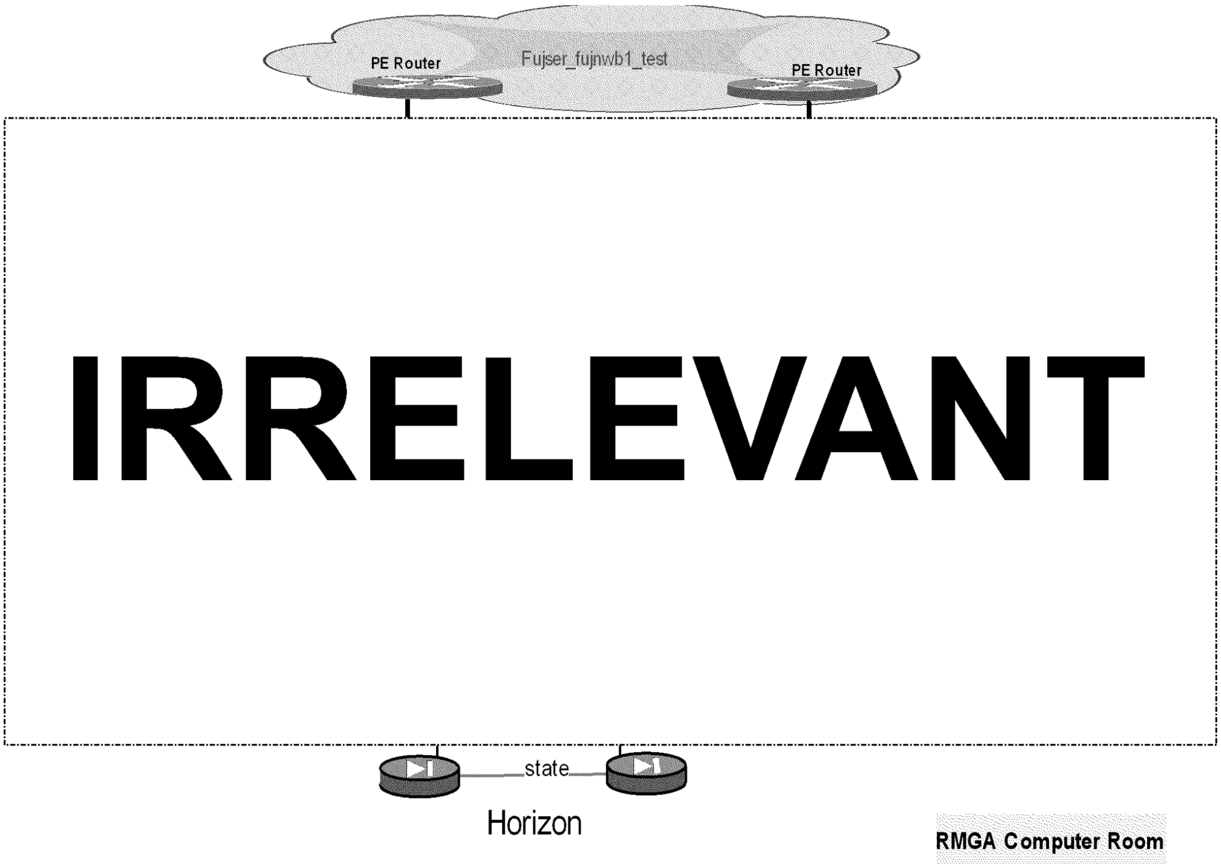


Figure 22 STE04 Physical

All LAN devices will be connected as shown in the physical diagram for resiliency. There will be no single point of failure on the LAN.

The support team will determine where to install the handoff routers.

KIT Name	Int. Loopback 99	Int. Loopback 100	Management Int.
IRRELEVANT			
IRRELEVANT			

Table 8 STE04 LAN info

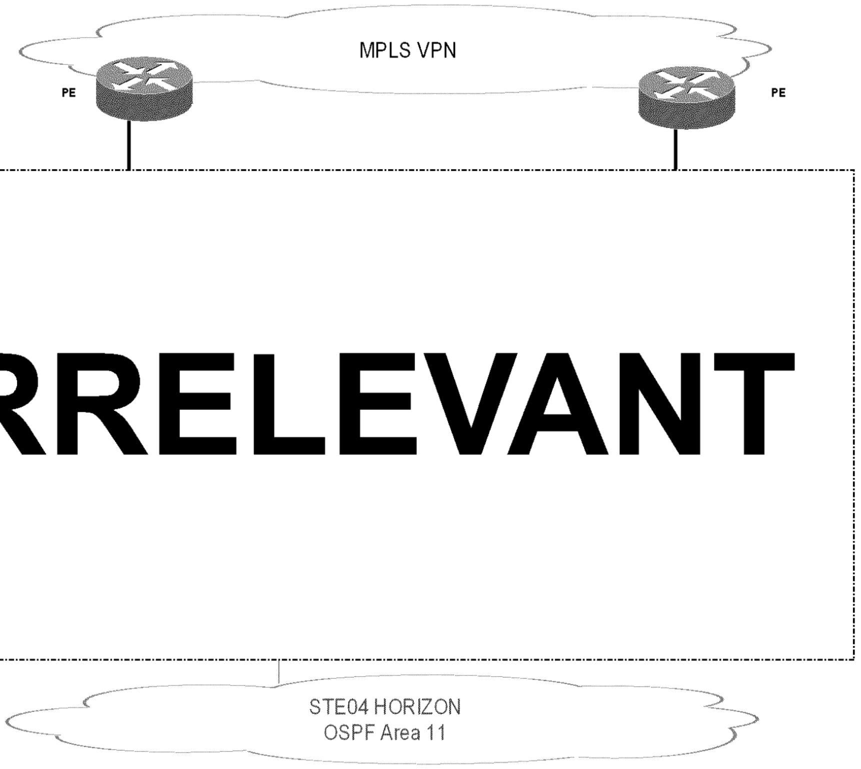


Figure 23 STE04 Layer3 diagram

<u>Layer 2:</u>

The switches will be as configured in Horizon. New HNG-X VLAN will be configured as shown.

VLAN IRRELEVANT will be used as an access VLAN connecting the support VRF interface on the CE with interface FE0/0 on the handoff routers. It will also serve as the management VLAN for the access routers IRRELEVANT and IRRELEVANT

Horizon VLAN IRRELEVANT will be the local transit LAN and will have the handoff router's VRRP address as the default gateway for all HNG-x destined traffic.

High availability:

VRRP group 1 will be configured on interface FE0/1 on IRRELEVANT and IRRELEVANT. The virtual router master for the group will be IRRELEVANT, configured with a priority 110. The virtual router backup for group 1 will be IRRELEVANT with a priority of 100. VRRP tracking will be used to dynamically failover between the master and the backup. The IP address to be tracked will be IRRELEVANT the IP address configured on interface IRRELEVANT

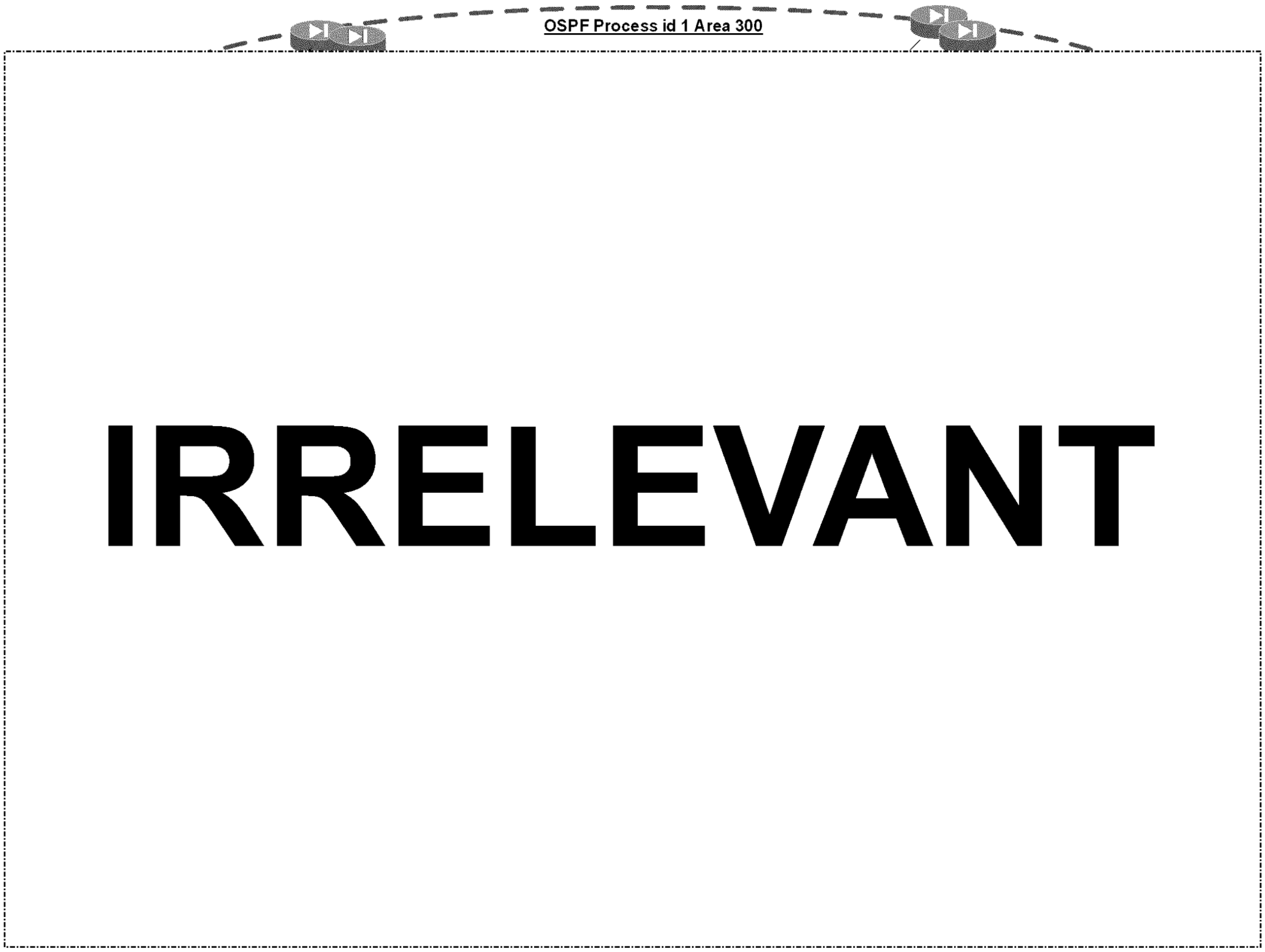


Figure 24 STE04 Layer 3 BGP/OSPF/GRE/IPSec diagram

External Routing:

eBGP will be used as the preferred routing protocol between the CE (in STE04) and the handoff routers as depicted in figure 24. eBGP peering will be between CE's and the handoff routers' interface IP addressing on VLAN IRRELEVANT as shown. There will be one eBGP peer commands on the primary handoff router IRRELEVANT and its STE04's corresponding CE, the same applies to between the secondary handoff and it corresponding CE. There will be no need for bgp multihop.

BGP will only be required to advertise IPSec tunnel endpoints interface loopback 99, as specified in the figure above.

GRE :

GRE tunnelling will be used to extend OSPF Area 300 from the Data centre support access into all remote support sites. GRE Tunnel interfaces will be configured as depicted in figure 10 BGP/OSPF/GRE diagram". Tunnel source will be interface loopback 99 on the STE04 handoff router while the Tunnel destination will be the IP address of interface loopback 99 of the corresponding IRE11/19 handoff router.

GRE Interface Tunnel 3 will be configured between handoff routers in IRE11/19 and handoff routers in STE04.

IP MTU size and TCP maximum segment size will be adjusted accordingly after tests have been carried out to determine what values will work best.

IPSec:

Configure as depicted in section 2.1.3.4.

Internal Routing: HNG-X and Horizon -

Area 300 in the data centres will be extended to the STE04 handoff routers over a GRE tunnel, which is encrypted in an IPSec tunnel over C&W's MPLS VPN as shown in figure 24.

There will be no OSPF neighbours formed on VLAN IRRELEVANT and there will be no OSPF routing between HNG-X (area 300) and Horizon (area 11).

OSPF area 300 will advertise (via static routing redistributed into Area 300) the NAT subnets IRRELEVANT and IRRELEVANT (corporate). The static route will point to firewalls IRRELEVANT high availability (HA) IP address IRRELEVANT. To dynamically failover the static routing, each handoff router will be configured to track interface FE0/1's IP routing (track xx interface FE0/1 ip routing). Each static route will be configured to reference the tracking ID (xx) as configured and then redistributed into area 300. This will allow the static routes configured on the Primary/secondary HO routers dynamically failover. In addition Area 300 will advertise the management interface (loopback 100) and the GRE tunnel endpoints (interface tunnel 0).

Static routes will be configured on the pair IRRELEVANT pointing the HNG-X IRRELEVANT IP address to the Handoff routers VRRP IP address IRRELEVANT. The static route will be redistributed on IRRELEVANT into Horizon's OSPF area 11. The Horizon ABR routers will be configured with the "area range (no advertise)" to prevent the advertising of the HNG-X IRRELEVANT IP range outside STE04 into Horizon OSPF backbone area. All other OSPF devices in Horizon OSPF Area 11 will see HNG-x routes advertised to them via IRRELEVANT.

Management of the layer 2 access switches will be via static routes configured on the handoff routers IRRELEVANT and IRRELEVANT, pointing each switch management interface out the HO router IP address for interface FE0/0. These static routes will be redistributed into Area 300.

There will be no redistribution between eBGP and OSPF locally in STE04.

IRRELEVANT

Figure 25 STE04 HNGx - Horizon integrated Layer 3 Support Workstation LAN

2.1.7.1 STE04 Acceptance into Service Criteria

This section provides some criteria for Acceptance into Service tests to be performed. The AIS tests will show conformance of the implementation to the design but are not exhaustive and need to be performed in conjunction with other tests which are within the remit of the implementation teams.

- IRRELEVANT will show C&W CE router IRRELEVANT as a BGP neighbour
- IRRELEVANT will show C&W CE router IRRELEVANT as a BGP neighbour
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- a GRE tunnel can be built between IRRELEVANT and IRRELEVANT
- a GRE tunnel can be built between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OSPF Area 300 for the following support LANs
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OPSF Area 300 for the following remote LANs
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT

2.1.8 WAR13

The following will be installed;

2x Cisco 2811 – Handoff routers

2x Catalyst 2960 – Access switch.

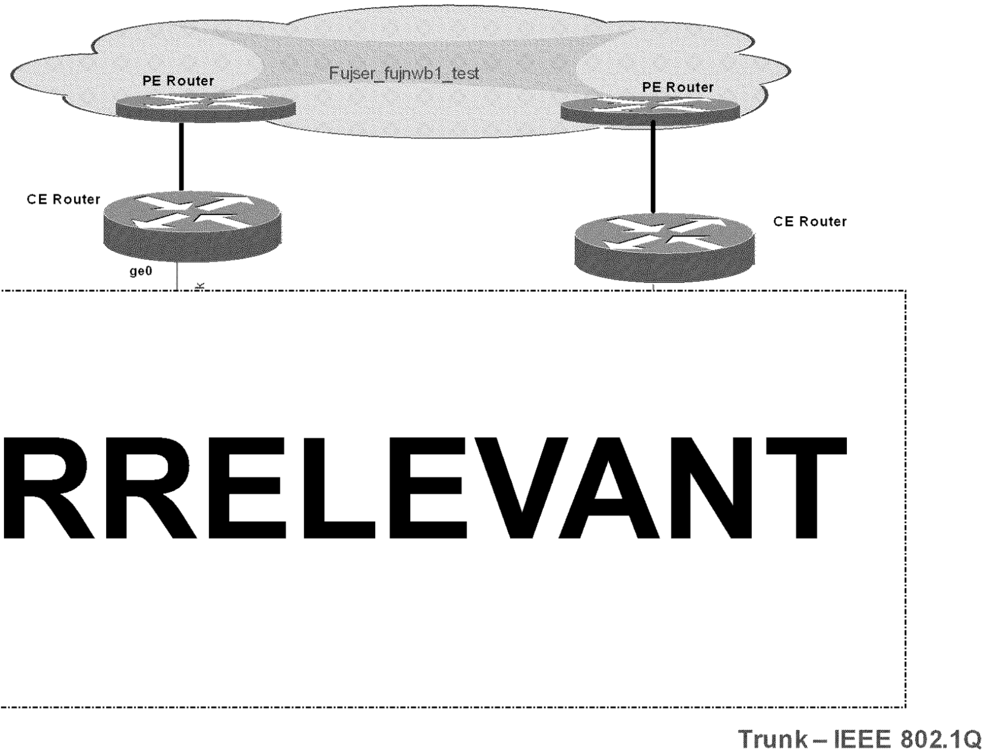


Figure 26 WAR13 Physical

All LAN devices will be connected as shown in the physical diagram for resiliency. There will be no single point of failure on the LAN.

The support team will determine where to install the kits and which switches on the existing infrastructure the catalyst 2960 switch trunk ports will connect to.

KIT Name	Int. Loopback 99	Int. Loopback 100	Int. VLAN 917	Management Int.
IRRELEVANT	IRRELEVANT	IRRELEVANT	-	IRRELEVANT
IRRELEVANT	IRRELEVANT	IRRELEVANT	-	IRRELEVANT
IRRELEVANT	-	-	IRRELEVANT	IRRELEVANT

wa13nsw002	-	-	172.20.0.54/28	Int. VLAN 917

Table 9 WAR13 LAN info

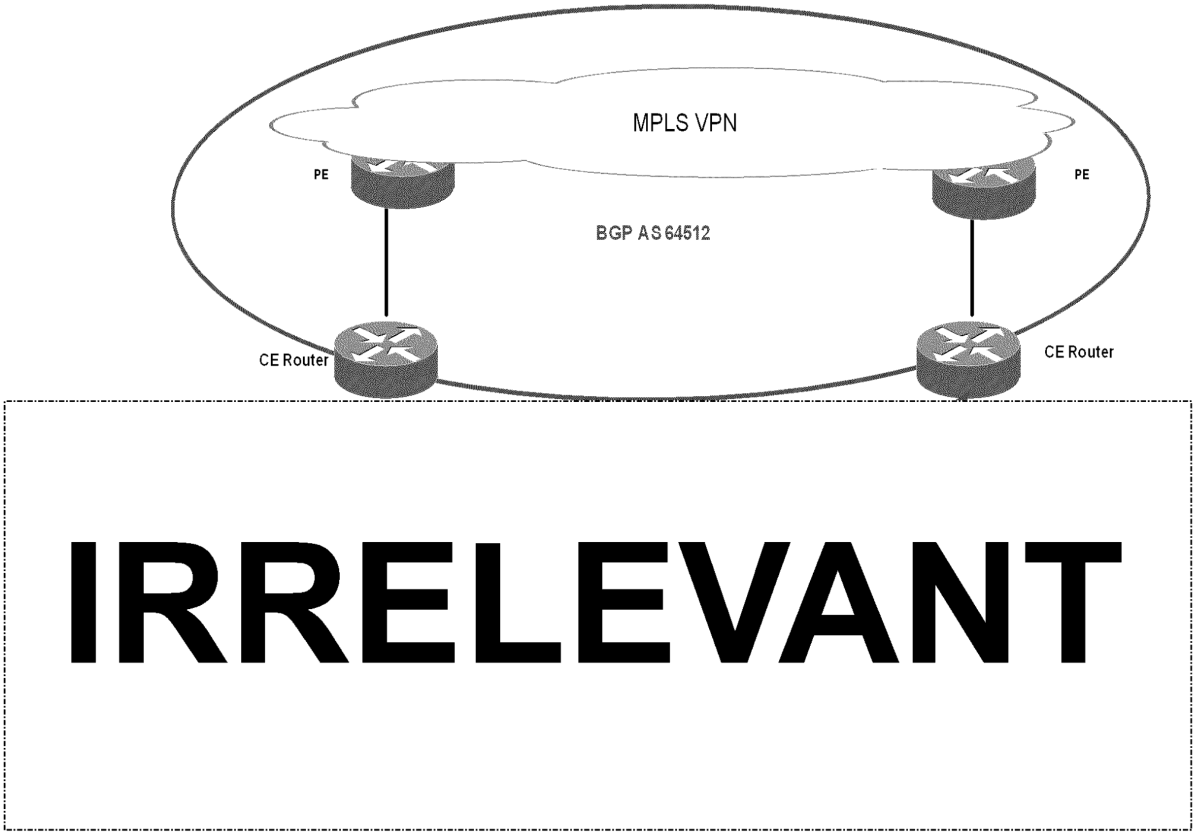


Figure 27 WAR13 Layer 3 diagram

Layer 2:

The switches will be configured as VTP transparent mode and all trunks will be IEEE802.1q. VTP domain name will be determined by the RMGA support team.

VLAN IRRELEVANT will be used as an access VLAN connecting the support VRF interface on the CE with interface FE0/0 on the handoff routers. It will also serve as the management VLAN for the access switches IRRELEVANT and IRRELEVANT

VLAN IRRELEVANT will be configured as the local LAN.

High availability:

VRRP group 1 will be configured on interface FE0/1 on IRRELEVANT and IRRELEVANT. The virtual router master for the group will be IRRELEVANT, configured with a priority 110. The virtual router backup fro group 1 will be IRRELEVANT with a priority of 100. VRRP tracking will be used to dynamically failover between the master and the backup. The IP address to be tracked will be IRRELEVANT, the IP address configured on interface IRRELEVANT on IRRELEVANT.

External Routing:

eBGP will be used as the preferred routing protocol between the CE (in WAR13) and the handoff routers as depicted in figure 20. eBGP peering will be between CE's and the handoff routers' interface IP addressing on VLAN 917 as shown. There will be one eBGP peer commands on the primary handoff router IRRELEVANT and its BRA01's corresponding CE, the same applies to between the secondary handoff and it corresponding CE. There will be no need for bgp multihop as eBGP.

BGP will only be required to advertise IPSec tunnel endpoints interface loopback 99, as specified in the figure 27 above.

Internal Routing:

OSPF is the preferred routing protocol for internal routing. OSPF area 300 has been designated as the support client access OSPF area id. Area 300 in the data centres will be extended to the WAR13 handoff routers over a GRE tunnel, which is encrypted in an IPSec tunnel over C&W's MPLS VPN as shown in figure 28 below.

OSPF area 300 will be used to advertise the LAN subnet IRRELEVANT shown, in addition it will advertise the management interface (loopback 100) and the GRE tunnel endpoints (interface tunnel 0).

Management of the layer 2 access switches will be via static routes configured on the handoff routers IRRELEVANT and IRRELEVANT.

There will be no redistribution between eBGP and OSPF locally in WAR13.

GRE :

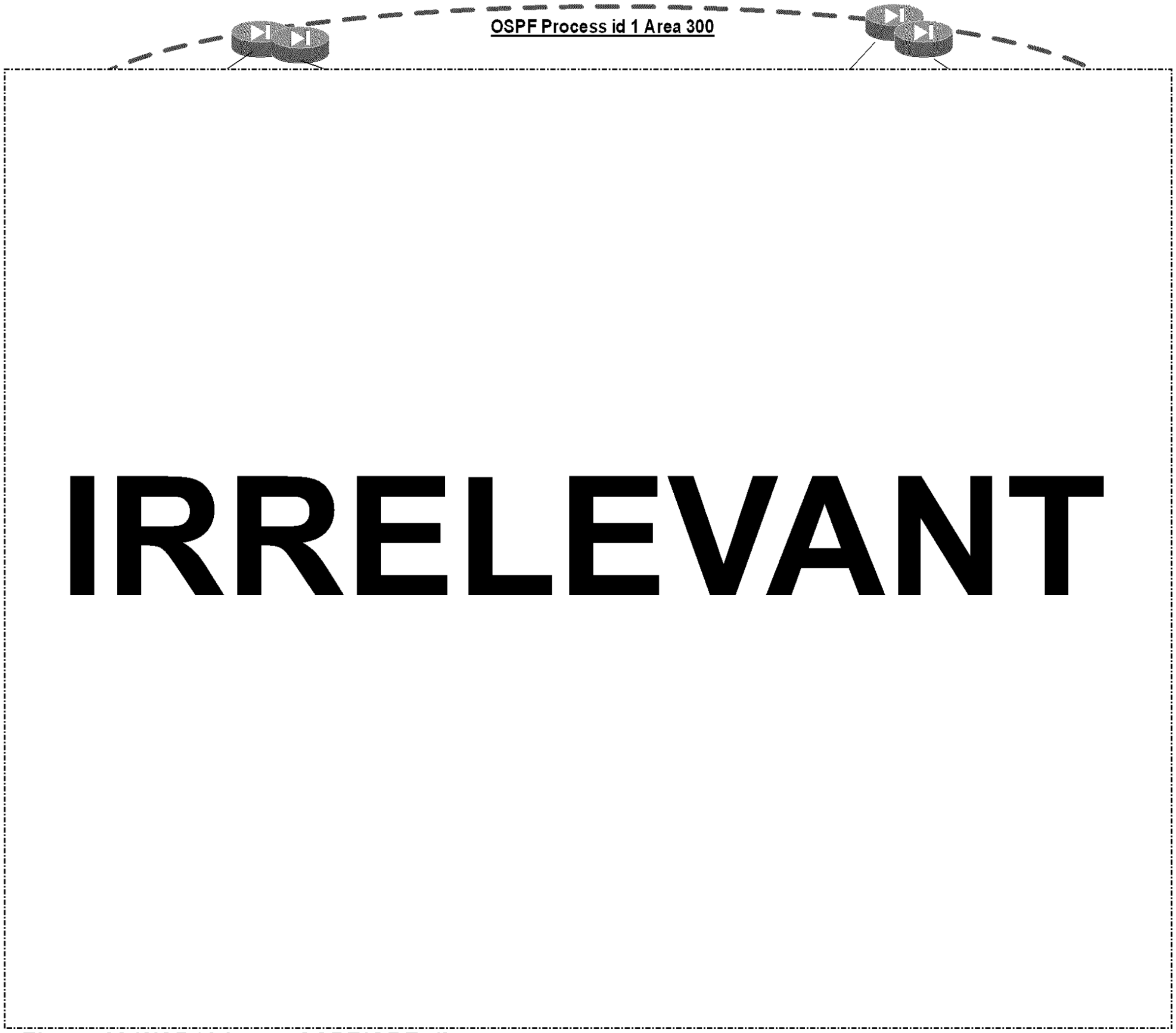
GRE tunnelling will be used to extend OSPF Area 300 from the Data centre support access into all remote support sites. GRE Tunnel interfaces will be configured as depicted in figure 10 BGP/OSPF/GRE diagram". Tunnel source will be interface loopback 99 on the WAR13 handoff router while the Tunnel destination will be the IP address of interface loopback 99 of the corresponding IRE11/19 handoff router.

GRE Interface Tunnel 4 will be configured between handoff routers in IRE11/19 and handoff routers in WAR13.

IP MTU size and TCP maximum segment size will be adjusted accordingly after tests have been carried out to determine what values will work best.

IPSec:

Configure as depicted in section 2.1.3.4.



IRRELEVANT

Figure 28 WAR13 Layer OSPF/GRE diagram

2.1.8.1 WAR13 Acceptance into Service Criteria

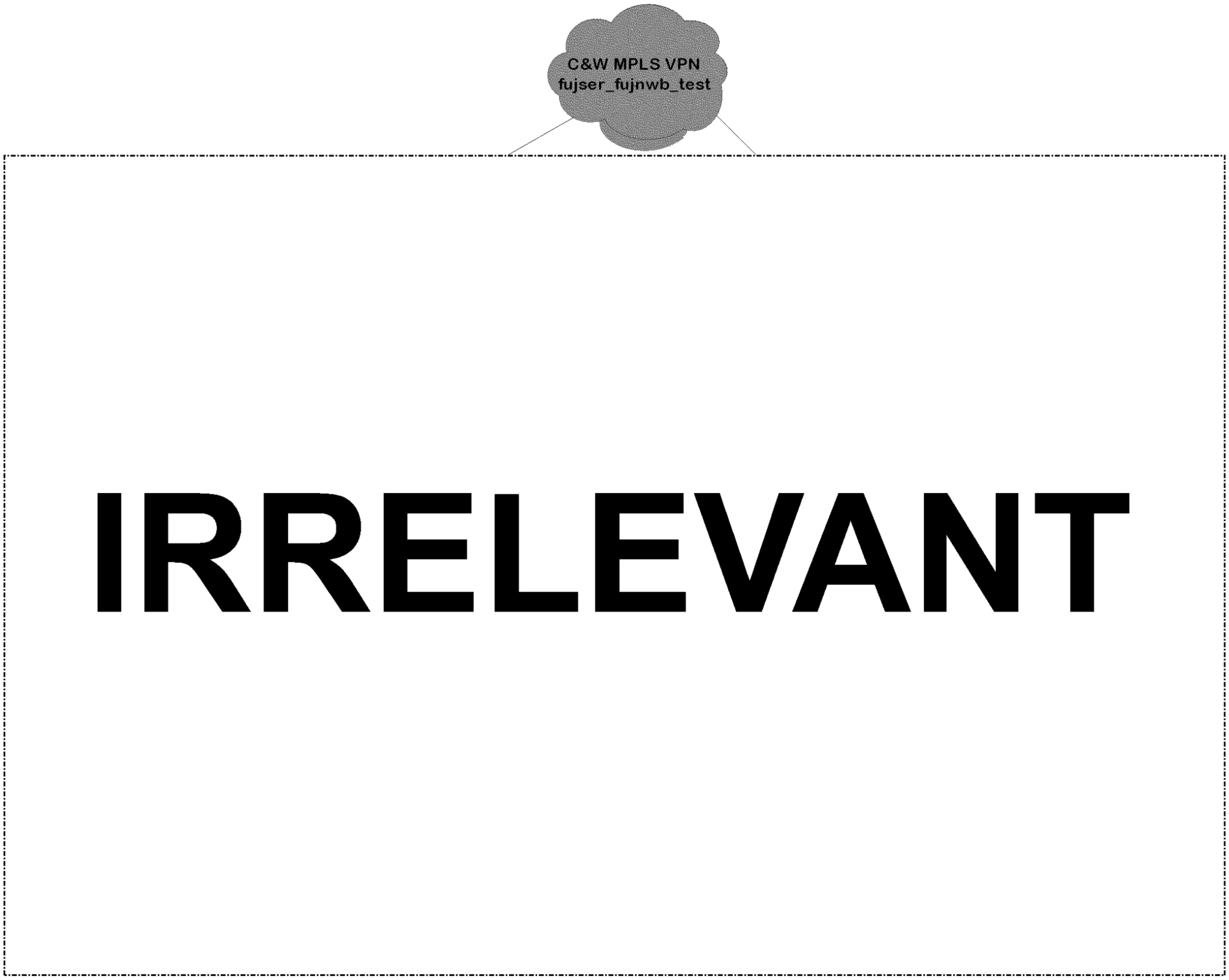
This section provides some criteria for Acceptance into Service tests to be performed. The AIS tests will show conformance of the implementation to the design but are not exhaustive and need to be performed in conjunction with other tests which are within the remit of the implementation teams.

- IRRELEVANT will show the new C&W CE router xxxx-rxx-001 as a BGP neighbour
- IRRELEVANT will show the new C&W CE router xxxx-rxx-002 as a BGP neighbour
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- a GRE tunnel can be built between IRRELEVANT
- a GRE tunnel can be built between IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT
- IRRELEVANT should learn routes via OSPF Area 300 for the following support LANs
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OPSF Area 300 for the following remote LANs
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT
    - IRRELEVANT

2.1.9 WNG01 and BTL01

The following will be installed;

2x Cisco 2811 – Handoff routers



IRRELEVANT

Figure 29 WGN01/BTL01 Data Centre Layer 3 diagram

The support team will determine where to install the kits and which switches on the existing infrastructure the handoff routers will connect to as discussed with Neil P..

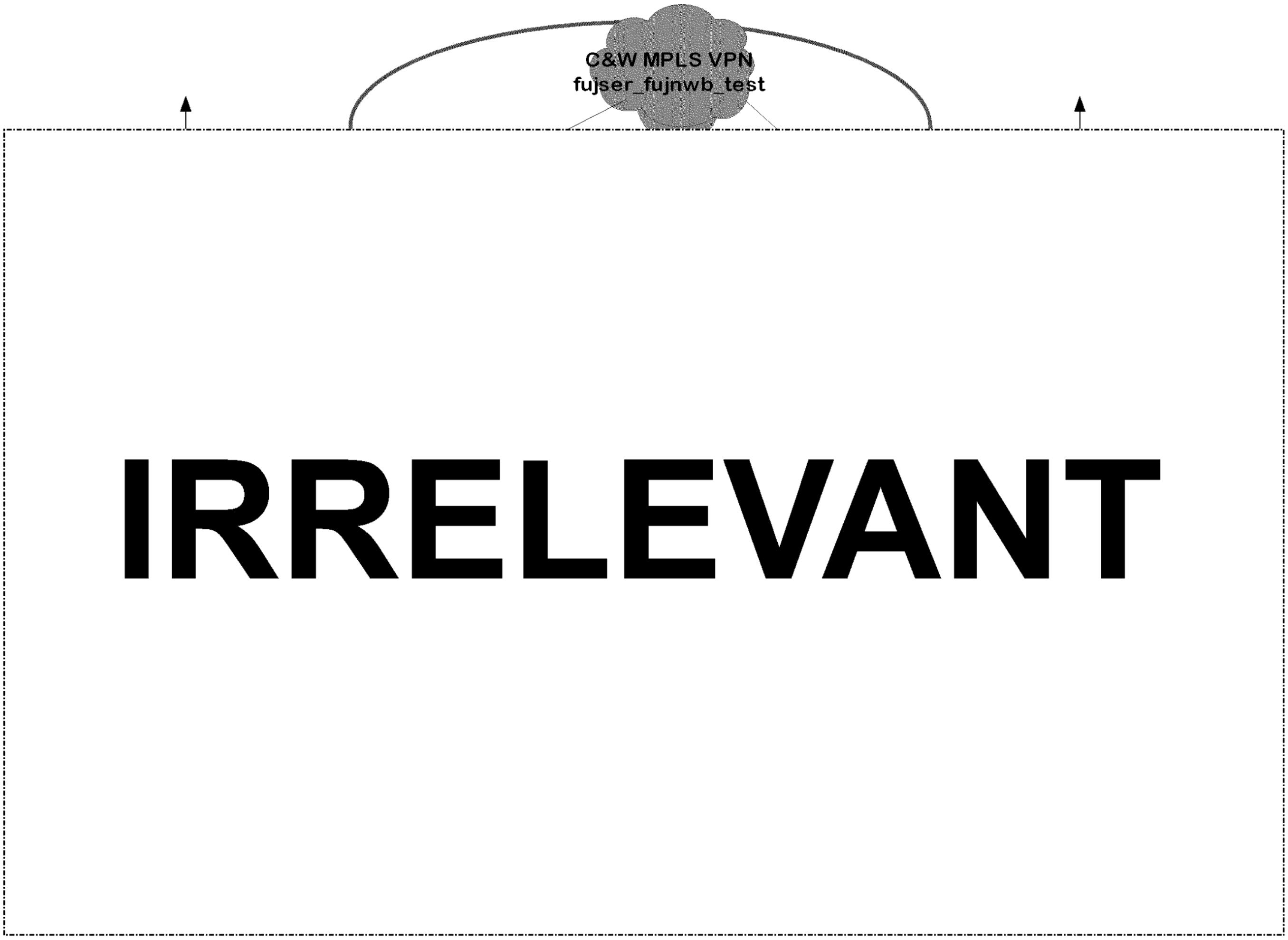


Figure 30 WGN01/BTL01 Data Centre BGP/NAT diagram

KIT Name	Int. Loopback 99	Int. Loopback 100	Management Int.
IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT
IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT

Table 10 WGN01/BTL01 Loopback addresses

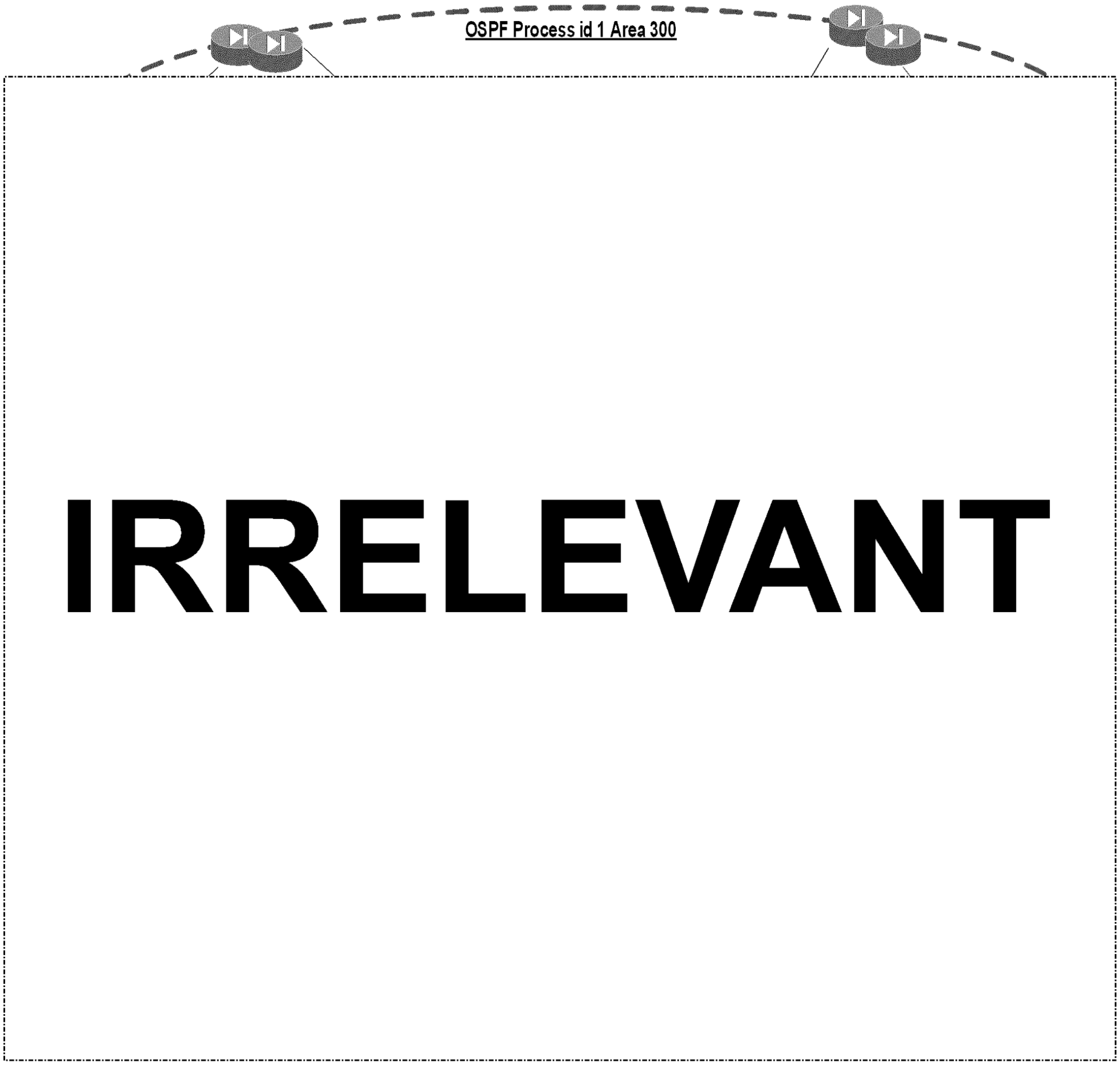


Figure 31 WGN01/BTL01 Data Centre IP Routing/IPSEC/GRE diagram

Layer 2:

VLAN IRRELEVANT (WGN01) and IRRELEVANT (BTL01) will be used as an access VLAN connecting the support VRF interface on the CE with interface FE0/0 on the handoff routers.

VLAN IRRELEVANT (WGN01) and VLAN IRRELEVANT (BTL01) will be configured for HNG-X Support workstations.

External Routing:

eBGP will be used as the preferred routing protocol between the CE and the handoff routers as depicted in figure 29. eBGP peering will be between CE's and the handoff routers' interface IP addressing on VLAN IRRELEVANT (WGN01) and IRRELEVANT (BTL01) as shown. There will be no need for bgp multihop.

BGP will only be required to advertise IPSec tunnel endpoints interface loopback 99.

GRE :

GRE tunnelling will be used to extend OSPF Area 300 from the Data centre support access into all remote support sites. GRE Tunnel interfaces will be configured as depicted in figure 29. Tunnel source will be interface loopback 99 on the WGN01/BTL01 handoff router while the Tunnel destination will be the IP address of interface loopback 99 of the corresponding IRE11/19 handoff router.

GRE Interface Tunnel 5 will be configured between handoff routers in IRE11/19 and handoff routers in WGN01/BTL01.

IP MTU size and TCP maximum segment size will be adjusted accordingly after tests have been carried out to determine what values will work best.

IPSec:

The steps for IPSec configuration are as follows

1. Create Crypto Access List - To secure the GRE Tunnel;

   IRE 11 & 19; "interface loopback 99" will be the source networks and the corresponding handoff router's "interface loopback 99" at the client site will be the destination.

   WNG01/BTL01; "interface loopback 99" will be the source networks and IRE 11 & 19's "interface loopback 99" will be the destination.

2. Define IKE to handle negotiation of protocols and algorithms based on local policy.

   For encryption use "aes 256"

   For authentication, a pre-shared key will be defined.

3. Defining Transform Sets: A Combination of Security Protocols and Algorithms.

   For Encryption (ESP Encryption Transform), esp-aes 256 (ESP with the 256-bit AES encryption algorithm) will be used

   For Header Authentication (AH Transform), ah-sha-hmac { AH with the SHA (an HMAC variant) authentication algorithm} will be used

4. Create Crypto Map Sets.

   This will be ipsec-isakmp based.

5. Apply Crypto Map Sets to handoff router Interfaces on VLAN IRRELEVANT and VLAN IRRELEVANT (IRE11/19).

6. Apply Crypto Map Sets to corresponding handoff router IRRELEVANT VLAN IRRELEVANT (WNG01) and IRRELEVANT VLAN IRRELEVANT (BTL01) Interfaces.

Internal Routing:

Area 300 in the data centres will be extended to WGN01 and BTL01 handoff routers over a GRE tunnel, which is encrypted in an IPSec tunnel over C&W's MPLS VPN as shown in figure 29.

OSPF area 300 will advertise the HNG-X subnets VLAN IRRELEVANT and IRRELEVANT it will also advertise the NAT subnets IRRELEVANT, IRRELEVANT, IRRELEVANT (Wigan NAT ranges) and NAT subnets IRRELEVANT, IRRELEVANT, IRRELEVANT (Bootle NAT ranges) as seen in figure 28 and 29, in addition it will advertise the management interface (loopback 100) and the GRE tunnel endpoints (interface tunnel 5).

There will be no redistribution between eBGP and OSPF locally in WGN01 and BTL01.

NAT:

There will be no re-addressing on the existing support sites presently using the IP range IRRELEVANT, the Horizon IRRELEVANT will NAT to the new HNG-X IP range of IRRELEVANT. All NAT in Wigan and Bootle will be configured on the Handoff routers and they will be the demarcation between the HNG-X and the existing Horizon based networks, as shown in figure 28. Static and Dynamic NAT will be configured on the handoff routers.

Wigan NAT range - IRRELEVANT, IRRELEVANT and IRRELEVANT (Horizon SAS NAT range).

Bootle NAT range - IRRELEVANT, IRRELEVANT and IRRELEVANT (Horizon SAS NAT range).

Static NAT will be configured to the SAS servers as follows;

Horizon SAS Servers Static NAT:

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

HNG-x SSN (SAS) servers Static NAT: TBD, presently access to HNG-x SSN servers is over FJS corporate.

For resilience to work with NAT on the handoff routers, static routing with IP SLA monitoring will be configure on the HO routers locally pointing to the NAT inside interface on VLAN IRRELEVANT - – interface Fe0/1 (WGN01) and to VLAN IRRELEVANT - – interface Fe0/1 (BTL01). These will then be redistributed into OSPF area 300. IP SLA monitoring will be monitoring the handoff router's NAT inside interface – interface Fe0/1 which if it fails causes the NAT to failover between WGN01 and BTL01.

Interface FE0/0 will be configured as NAT outside and FE0/1 as NAT inside interfaces.

2.1.9.1 Wigan/Bootle Acceptance into Service Criteria

This section provides some criteria for Acceptance into Service tests to be performed. The AIS tests will show conformance of the implementation to the design but are not exhaustive and need to be performed in conjunction with other tests which are within the remit of the implementation teams.

- IRRELEVANT will show the new C&W CE router IRRELEVANT as a BGP neighbour
- IRRELEVANT will show the new C&W CE router IRRELEVANT as a BGP neighbour
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the DC HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- IRRELEVANT will learn routes to the remote HO router IRRELEVANT loopback addresses via eBGP
- a GRE tunnel can be built between IRRELEVANT and IRRELEVANT
- a GRE tunnel can be built between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- an OSPF adjacency can be established between IRRELEVANT and IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OSPF Area 300 for the following support LANs
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
- IRRELEVANT and IRRELEVANT should learn routes via OPSF Area 300 for the following remote LANs
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT
  - IRRELEVANT

- IRRELEVANT

2.2 Remote Support Workstations

<u>SSW (SSC Support Workstation)</u> – All SSC workstations will be virtualized on the existing Horizon hardware with three Horizon IP addresses as follows –

- One for the host operating system,

- One for the Windows 2000 VM which is being use to support Horizon, and which will continue during Hydra.

- One for the XP VM which will support HNG-x, and which will be used during Hydra.

Attached connectivity requirements for SSC workstations in HNG-x and HYDRA -

IRRELEVANT

- <u>BRA01 -</u> Attached is a list of <u>SSC workstation</u> on IRRELEVANT and these will NAT to IRRELEVANT on BRA01 firewalls IRRELEVANT. <u>Only the Windows XP "VM" IP address will be configured for NAT.</u>

IRRELEVANT

- <u>LEW02</u> - <u>SSC workstation on Horizon subnet</u> IRRELEVANT will NAT to IRRELEVANT on LEW02 firewalls IRRELEVANT. These are as follows: Only the Windows XP "VM" IP address will be configured for NAT.

Serial No	**Machine ID**	**IP**				
Host	**Win2K VM**	**XP VM**	**Host**	**Win2K VM**	**XP VM**	**XP VM NAT**
IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT
Gateway	IRRELEVANT					

NMW (Network Management Workstation) – Traffic types/endpoints in HNG-x will be RDP to SSN servers.

- WGN01/BTL01 - HNG-x network management workstations will sit on the HNG-x LAN VLAN IRRELEVANT (Wigan) and VLAN IRRELEVANT (Bootle). Horizon workstations will NAT to IRRELEVANT (Wigan) and to IRRELEVANT (Bootle).
- WAR13 – The HNG-x network management workstations will sit on the HNG-x VLAN IRRELEVANT There will be no need to NAT.

MSS/SMG/MAN (SYSMAN2 Tivoli Workstation) – MSS/SMG workstations will target all Rig SSN servers both for Live and Test

- WGN01/BTL01 - All workstations (HNG-x Horizon) will sit on the Horizon LAN and NAT to HNG-x NAT range IRRELEVANT (Wigan) and to IRRELEVANT (Bootle). Other NAT ranges have been allocated for expansion. SYSMAN2 will in time upgraded to SYSMAN3 and the target endpoint is the Estsysman platform.

  Attached is the port requirements and list of workstations for SYSMAN2.

  IRRELEVANT

- STE04 – SMG sits on the IRRELEVANT LAN and will NAT to IRRELEVANT on IRRELEVANT
- BRA01 – SMG sits on the IRRELEVANT LAN and will NAT to IRRELEVANT on IRRELEVANT.

KAW/KSA/KSN/ACE/CAW : These will target the Keyman domain in IRE11/19.

CAW - Certificate Authority Workstation (Horizon)

KAW - KMA workstation (Horizon)

KSA - KMA Admin Workstation (Horizon)

KSN - KMNG Workstation

ACE Workstation (Horizon)

- BRA01 – These platforms sit on the RMGA security LAN, IP subnet IRRELEVANT and will NAT to HNG-x subnet IRRELEVANT on IRRELEVANT
- LEW02 - These platforms sit on the RMGA security LAN, IP subnet IRRELEVANT and will NAT to HNG-x subnet IRRELEVANT or IRRELEVANT

RVACC KSN for use with ikey USB tokens the RVACC KSN workstation IRRELEVANT (IRRELEVANT) needs to access the active directory on RVACC ACD server IRRELEVANT (IRRELEVANT). Additionally access is required to an HTTPS server on the SSN server IRRELEVANT (IRRELEVANT) for enrolment. The required traffic flows are described in the IRE11/19 firewall rules table 11 and the attached spreadsheet.

These rules contain a range of ports for Dynamic allocation of TCP ports to RPC services. The current version of the firewall software deployed (7.0) does not include the ability to open dynamic ports for RPC service calls. This is addressed in version 7.2 of the software. To allow the KSN servers to communicate with the ACD a range of ports has been specified. The ACD server will need to be patched to restrict the range of ports which can be allocated to services. This range has initially been set at 1000 but will need reviewing to minimise the number of ports open on the firewalls. If the firewall software is upgraded at a later date this range can be removed.

The RVACC KSN also needs access to the KMN on TCP port IRRELEVANT for CAPO volume testing and end-to-end counter transactions.

IRRELEVANT

AUD/AUW: Will target the Keyman domain in IRE11/19.

AUD - Audit Workstation (Horizon)

AUW - Audit Workstation

- BRA01 – These platforms sit on the RMGA security LAN, IP subnet IRRELEVANT and will NAT to HNG-x subne IRRELEVANT on IRRELEVANT.
- LEW02 - These platforms sit on the RMGA security LAN, IP subnet IRRELEVANT and will NAT to HNG-x subnet IRRELEVANT on IRRELEVANT

3 Firewall Rules.

3.1.1 Firewall Rule

Firewall rules TBC, in line with the DC LAN LLD which is presently unavailable.

Updated with BRA01/IRE SSC firewall rules, others to follow.

The RMGA Network team will manage the network equipment in IRE11 and IRE19. The monitoring and management platforms used in the network will be the HP Open View and CiscoWorks platforms. Protocols required for support will be SNMP, SFTP, SSH, SCP.

General firewall policy: deny all inbound traffic unless explicitly authorised and traffic from internal VLAN users is unrestricted. All deny rules are logged.

- Firewall rules coloured Orange are believed to be unnecessary as they define return traffic flows for conversations initiated by client devices outside the data centre rather than initiated by the data centre servers back to the clients. The firewall appliances employed should be capable of handling these implied return rules. These rules tend to be from a single device or cluster of devices to a network or PAT address.
- Entries coloured Blue are new in this version of the document.

Source	Destination	Service	Port	Protocol	Action	Comments
IRE19 IRRELEVANT	IRRELEVANT	Sql	1521	Tcp	allow	Live SSN SQL Connectivity for MSS Team
IRRELEVANT	IRRELEVANT	Sql	1521	Tcp	allow	LST SSN SQL Connectivity for MSS Team
IRRELEVANT	IRRELEVANT	Sql	1521	Tcp	allow	RvMig SSN SQL Connectivity for MSS Team
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	Allow	SSN server connectivity

IRRELEVANT	IRRELEVANT					
IRRELEVANT	IRRELEVANT	OpenSSH	22	TCP	Allow	SAS server LAN to the rest of the Estate.
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	ALLOW	For Steve Glasgow's team (IRE11 NT/UNIX Support) access to the SAS servers in Horizon (WGN01/BTL01)
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	Allow	BRA01 Corporate PAT IP address to SAS server connectivity

	IRRELEVANT					
IRRELEVANT	IRRELEVANT	RDP SSH FTP	3389 22 20,21	TCP	ALLOW	SSC Workstation to IRE11/19 SSC Server
IRRELEVANT	IRRELEVANT	RDP SSH FTP	3389 22 20,21	TCP	ALLOW	IRE11/19 SSC Server to SSC workstation
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	Allow	SSC server to IRE11/19 SSN (SAS) server terminal access
IRRELEVANT	IRRELEVANT	SSH FTP SQL Server/ Client HTTPS EVENTS PerfMon RPC JDBC	22 20,21 1433 1434 443 31111 – 31119 31111 – 31119	TCP/ UDP	ALLOW	IRE11/19 SSC Server to IRE11/19 SSN servers

	IRRELEVANT		135 1433/1434			
IRRELEVANT	IRRELEVANT	SSH FTP SQL Server/ Client HTTPS EVENTS PerfMon RPC JDBC	22 20,21 1433 1434 443 31111 – 31119 31111 – 31119 135 1433/1434	TCP/UDP	ALLOW	IRE11/19 SSN Server to IRE11/19 SSC servers
IRRELEVANT	IRRELEVANT	RPC JDBC Copy file	135 1433/1434 139	TCP/UDP	ALLOW	IRE11/19 SSC Server to IRE11/19 WIN servers
IRRELEVANT	IRRELEVANT	RPC JDBC Copy file	135 1433/1434 139	TCP/UDP	ALLOW	IRE11/19 SSC Server to IRE11/19 NIX servers
IRRELEVANT	IRRELEVANT	SSH FTP EVENTS PerfMon	22 20,21 31111 – 31119 31111 – 31119	TCP/UDP	ALLOW	IRE11/19 SSN Server to IRE11/19 WIN servers
IRRELEVANT	IRRELEVANT	SSH FTP	22 20,21	TCP/UDP	ALLOW	IRE11/19 SSN Server to IRE11/19 NIX servers

IRRELEVANT						
IRRELEVANT	IRRELEVANT	HTTPS jcifs	443 445	TCP/UDP	ALLOW	IRE11/19 SSN Server to IRE11/19 WEB servers
IRRELEVANT	IRRELEVANT	TWS	31111 – 31119	TCP	ALLOW	IRE11/19 SSN Server to IRE11/19 TWS
IRRELEVANT	IRRELEVANT	HTTPS	443	TCP	ALLOW	IRE11/19 SSN Server to IRE11/19 SYSMAN3(RAD & TPM)
IRRELEVANT	IRRELEVANT	SSH	22	TCP	ALLOW	IRE11/19 SSN Server to IRE11/19 Oracles servers

IRRELEVANT	IRRELEVANT	HTTP	80	TCP	ALLOW	IRE11/19 SSN Server to IRE11/19 PAN manager
IRRELEVANT	IRRELEVANT	HTTPS	443	TCP	ALLOW	IRE11/19 SSN Server to Third party Access Servers
IRRELEVANT	IRRELEVANT	all	all	tcp	allow	Key management workstations to Key management domain access.
IRRELEVANT	IRRELEVANT	all	all	tcp	allow	Key management workstations to Key management domain access.
IRRELEVANT	IRRELEVANT	all	all	tcp	allow	Key management workstations to Key management domain access.
IRRELEVANT	IRRELEVANT	all	all	tcp	allow	Key management workstations to Key management domain access.
IRRELEVANT	IRRELEVANT	Postgres Sftp Jscape secure file server HTTPS HTTP	5432 21 10880 443 80	TCP	Allow	CM Workstation access to DXC
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	Allow	STE04 Support PAT IP address to SAS server connectivity

	IRRELEVANT					
IRRELEVANT	IRRELEVANT	LDAP Global Catalogue LDAP Kerberos kpassword cifs RPC Dynamic ports[1]	3268 389 88 464 445 41952-50151	TCP TCP UDP/TCP UDP/TCP TCP TCP	Allow	BRA01 KSN to IRE19 RVACC ACD server for ikey USB token
IRRELEVANT	IRRELEVANT	HTTPS	443	TCP	Allow	BRA01 KSN to IRE19 RVACC SSN for ikey USB token
IRRELEVANT	IRRELEVANT		33031	TCP	Allow	BRA01 KSN to KMN for CAPO

Table 11 IRE11 and IRE 19 ASA Firewall Rule base

[1] Please see note regarding dynamic RPC ports for KSN access in section 2.2 above.

Source	Destination	Service	Port	Protocol	Action	Comments
IRRELEVANT	IRRELEVANT	Sql	1521	Tcp	allow	LST SSN SQL Connectivity for MSS Team
IRRELEVANT	IRRELEVANT	Sql	1521	Tcp	allow	RvMig SSN SQL Connectivity for MSS Team
IRRELEVANT	IRRELEVANT	Postgres Database Ftps Jscape secure file	5432 21 10880 443	TCP TCP TCP TCP	ALLOW	CM workstation to Data Exchange Proxy (DXC) platform for software delivery from BRA01 Corporate LAN to IRE11/19.

	IRRELEVANT	server https http	80	TCP		
IRRELEVANT	IRRELEVANT	Postgres Database Ftps Jscape secure file server https http	5432 21 10880 443 80	TCP TCP TCP TCP TCP	ALLOW	CM workstation to Data Exchange Proxy (DXC) platform for software delivery from BRA01 Corporate LAN to IRE11/19.
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	ALLOW	IRE11/19 SSN (SAS) server terminal access
IRRELEVANT	IRRELEVANT	RDP SSH FTP	3389 22 20,21	TCP	ALLOW	IRE11/19 SSC Server
IRRELEVANT	IRRELEVANT	RDP SSH FTP	3389 22 20,21	TCP	ALLOW	IRE11/19 SSC Server
IRRELEVANT IRRELEVANT	IRRELEVANT	RDP	3389	TCP	Allow	SMG to IRE11/19 SSN (SAS) server terminal access

	IRRELEVANT					
IRRELEVANT	IRRELEVANT	all	all	tcp	allow	Key management workstations to Key management domain access.
IRRELEVANT	IRRELEVANT	all	all	tcp	allow	Key management workstations to Key management domain access.

Table 12 BRA01 Firewall Rule base

Source	Destination	Service	Port	Protocol	Action	Comments
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	Allow	SMG to IRE11/19 SSN (SAS) server terminal access
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	Allow	STE04 Support PAT IP address to SAS server connectivity

Table 13 STE04 Firewall Rule base

Source	Destination	Service	Port	Protocol	Action	Comments
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	Allow	SSC to IRE11/19 SSN (SAS) server terminal access
IRRELEVANT	IRRELEVANT	RDP SSH FTP	3389 22 20,21	TCP	ALLOW	IRE11/19 SSC Server
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	Allow	STE04 support traffic to IRE11/19
IRRELEVANT	IRRELEVANT	all	all	tcp	allow	Key management workstations to Key management domain access.
IRRELEVANT	IRRELEVANT	all	all	tcp	allow	Key management workstations to Key management domain access.

Table 14 LEW02 Firewall Rule base

Source	Destination	Service	Port	Protocol	Action	Comments
IRRELEVANT	IRRELEVANT	Sql	1521	Tcp	allow	Live SSN SQL Connectivity for MSS Team
IRRELEVANT	IRRELEVANT	RDP	3389	TCP	Allow	SSC to IRE11/19 SSN (SAS) server terminal access

Table 15 Wigan and Bottle Firewall Rule base

4 Platform Requirements

4.1.1 Availability & Resilience

As discussed in each remote site section.

4.1.2 SAS Servers

SAS Server Requirements:

The high level requirements for the Secure Access Servers are to provide support teams with:

- Controlled and audited access to the operational platforms
- Multiple sessions for support users
- OpenSSH access from the SAS to the managed operational platforms.
- Secure web based access to campus servers
- Access to the System Management.

This High Level Design sets out the design for the Secure Access Servers described in the Remote Support and Diagnostics architecture (ARC/SYS/ARC/0004). This will provide remote support access to IRE11 and IRE19 for the following user communities:

- SSC
- SMG
- ISD (Unix, NT and Network support)
- Test

Support workstations will access the SAS using RDP and will also have the ability to access BSDB (SSC database) and the SSC server (RDP) directly.

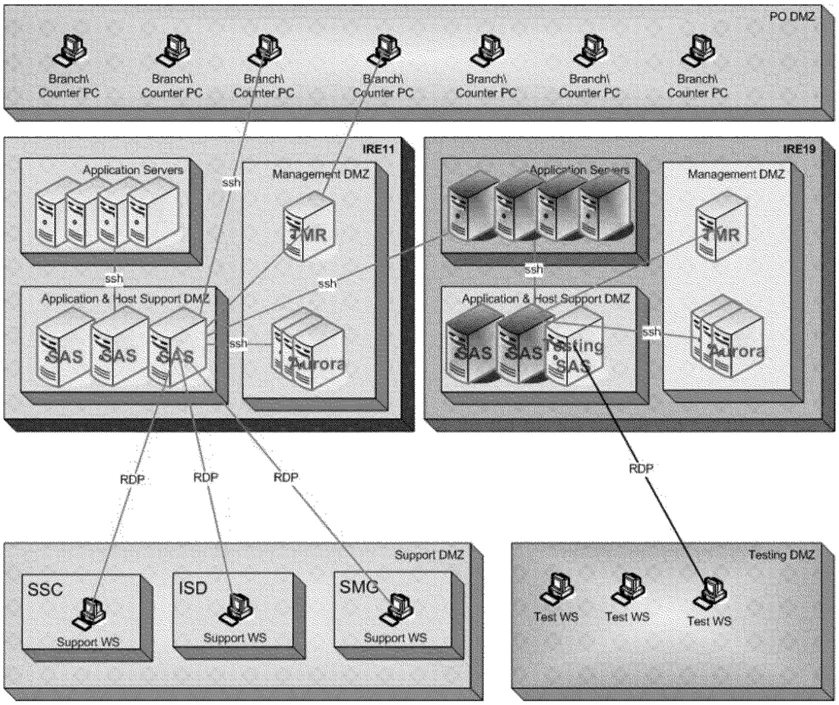


Figure 32 SAS Connectivity diagram

Source	Destination	Description	Protocol	Ports
WGN01, STE09, IRE11, BRA01 workstations.	SAS	Server Support Teams, Application Support Teams and Testing Teams access SAS and Test SAS.	RDP	IRRELEVANT
WGN01, STE09, IRE11, BRA01 workstations.	Application & Host Support MPLS VPN	Testing Teams file transfer to /from Infrastructure.	SFTP	
SAS	Application Servers & Counters	Secure channel between SAS ssh client and target SSH Server.	ssh	
SAS	Application servers	Server Support Teams, Application Support Teams and Testing Teams access to Infrastructure.	RDP*	

** Only in exceptional circumstances and only to DC hosted servers*

Table 16 SAS connectivity requirements

SAS Authentication:

SAS servers will support authentication via Windows Active Directory.

For non Microsoft AD based users, authentication to the SAS servers will be local.

4.1.3 Software delivery

Software delivery flow diagram

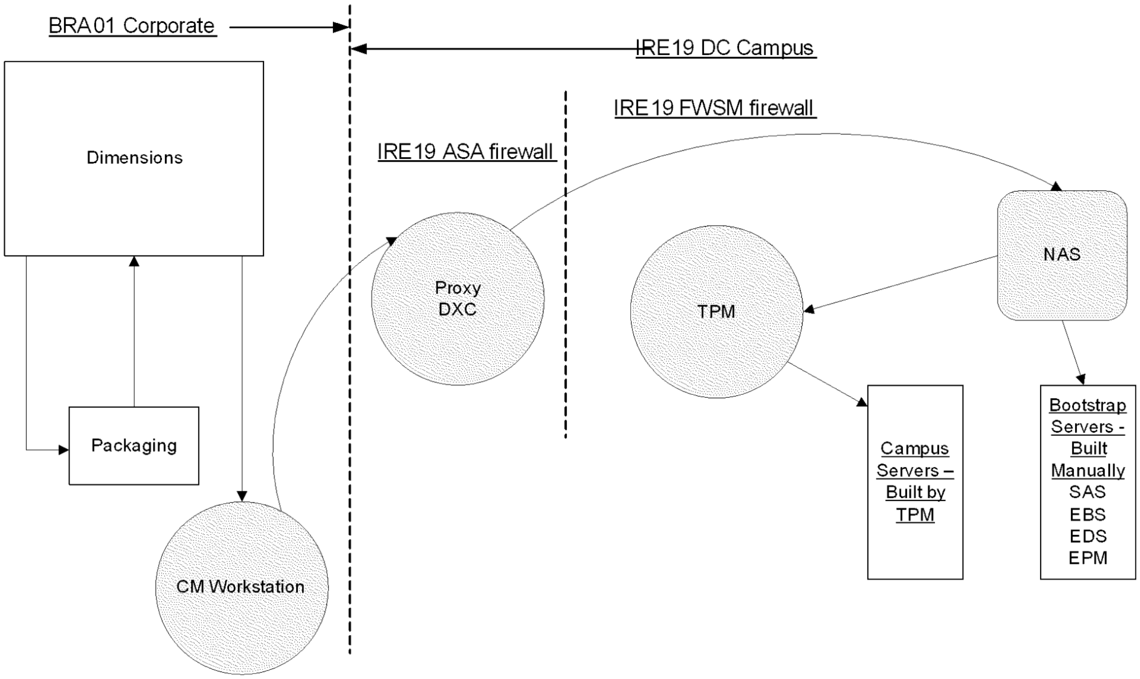


Figure 33 Software delivery diagram (TBC).

Connectivity requirements is as shown

Source	Destination	Description	Method
CM Workstation	Generic Proxy	Software Repository (NAS)	Secure File Transfer

Table 17