CCNP Route For A Global Health Network Network Design Document

Version 3.0

1/4/2026

Document Details

Approvals

The Supervisor and the Client shall approve this document.

Document Change Control

Initial Release:	14/11/2025
Current Release:	14/11/2025
Date of Last Review:	
Date of Next Review:	
Target Date for Next Update:	

Distribution List

This following list of people shall receive a copy of this document every time a new version of this document becomes available:

Customer: Ayman Alani

Team Members:

Husain Ali

Ayman Alani

Change Summary

The following table details changes made between versions of this document

Version	Date	Modifier	Description
1.0	14/11/2025	Husain Ali	Adding the introduction
2.0	15/11/2025	Husain Ali	Updated the sections
3.0	16/11/2025	Husain Ali	Adding the Deployment diagram

Table of Contents

Introduction

The design document describes the proposed wide area network (WAN) and local area network (LAN) design for the Global Health Network (GHN), interconnecting the main site in Bahrain with international branches in England, Luxembourg and China through an internet service provider (ISP) core. The design uses a mix of internal gateway protocols (IGPs) EIGRP, Name Eigrp, OSPF and OSPFv3, BGP for inter AS routing, and DMVPN with IPsec for secure redundant hubs and spokes connectivity. Each country keeps its own addressing and routing domain while still providing end to end IP reachability for users and servers.

Network Design

The network design section focuses on the infrastructure of the network and gives the guidance on the configuration and the topology. This part of the document serves as the blueprint for the Network Designer who will be designing the physical and the topology for the project.

Context

The GHN is a multinational healthcare organisation that requires secure, reliable connectivity between four main locations:

- **Bahrain** primary regional hub and main data centre, hosting core services and internal users.
- **England** large branch with multiple access switches and local users.
- **Luxembourg** European branch hosting central AAA services and internal servers.
- **China** Asia branch with local users and access to GHN applications.

These sites are interconnected through an ISP backbone using public network 90.0.0.0/26. Each country site runs its own IGP and BGP AS, and it has redundant links towards the ISP. A DMVPN with IPsec overlay is built between the main hub in Bahrain and the remote branches to provide scalable, encrypted communication between sites. The design must support future growth in users and services, provide redundant routing, and allowing centralised security policies with minimal disturbance to the network in each site.

Location Floor Plans

Each site is abstracted as:

Core and Distribution layer: aggregating local subnets and providing connectivity thru IGP.

Access layer: Layer 2 switches connecting end user PCs, servers and local devices.

Server and Service area: dedicated subnets for servers, such as Bahrain Server VLANs, Luxembourg AAA server, and local services at each branch.

Addressing Scheme

Network Adders Table	
Area	**Network Address**
Bahrain	172.16.0.0/16
England	172.17.0.0/16
Luxembourg	172.18.0.0/16
China	172.19.0.0/16
ISP	90.0.0.0/26
Tunnel1	100.100.100.100/28
Tunnel2	100.100.100.200/28

Bahrain				
Device	**Interface**	**IP Address**	**Subnet Mask**	**Default Gateway**
BH-R1	S1/0 (BH-R2)	172.20.1.1	255.255.255.252	N/A
	S1/1 (BH-R3)	172.20.1.5	255.255.255.252	N/A
	S1/2 (ISP-R2)	90.0.0.42	255.255.255.252	N/A

	Lo0	1.1.16.1	255.255.255.255	N/A
	Lo1	1.1.16.100	255.255.255.255	N/A
	Tunnel1	100.100.100.1	255.255.255.240	N/A
BH-R2	S1/0 (BH-R1)	172.20.1.2	255.255.255.252	N/A
	S1/1 (BH-R4)	172.20.1.9	255.255.255.252	N/A
	S1/2(ISP-R1)	90.0.0.18	255.255.255.252	N/A
	Lo0	1.1.16.2	255.255.255.255	N/A
	Tunnel2	100.100.200.1	255.255.255.240	N/A
BH-R3	S1/0 (BH-R4)	172.20.1.13	255.255.255.252	N/A
	S1/1 (BH-R1)	172.20.1.6	255.255.255.252	N/A
	E0/2.10	172.16.10.1	255.255.255.0	N/A
	E0/2.20	172.16.20.1	255.255.255.0	N/A
	E0/2.30	172.16.30.1	255.255.255.0	N/A
	E0/2.100	172.16.100.1	255.255.255.0	N/A
	Lo0	1.1.16.3	255.255.255.255	N/A
BH-R4	S1/0 (BH-R3)	172.20.1.14	255.255.255.252	N/A
	S1/1 (BH-R2)	172.20.1.10	255.255.255.252	N/A
	E0/1.10	172.16.10.2	255.255.255.0	N/A
	E0/1.20	172.16.20.2	255.255.255.0	N/A
	E0/1.30	172.16.30.2	255.255.255.0	N/A
	E0/1.100	172.16.100.2	255.255.255.0	N/A
	Lo0	1.1.16.4	255.255.255.255	N/A
BH-SW1	VLAN 100	172.16.100.101	255.255.255.0	172.16.100.254
BH-SW2	VLAN 100	172.16.100.102	255.255.255.0	172.16.100.254
BH-SW3	VLAN 100	172.16.100.103	255.255.255.0	172.16.100.254
BH-SW4	VLAN 100	172.16.100.104	255.255.255.0	172.16.100.254
BH-SW5	VLAN 100	172.16.100.105	255.255.255.0	172.16.100.254
BH-PC1	Eth0	172.16.10.10	255.255.255.0	172.16.10.254
BH-PC2	Eth0	172.16.20.20	255.255.255.0	172.16.20.254
BH-Server	Eth0	172.16.30.31	255.255.255.0	172.16.30.254
BH-Server-Backup	Eth0	172.16.30.32	255.255.255.0	172.16.30.254

England				
Device	**Interface**	**IP Address**	**Subnet Mask**	**Default Gateway**
EN-R1	S1/0 (EN-R1)	172.20.1.17	255.255.255.252	N/A
	S1/1 (ISP-R2)	90.0.0.38	255.255.255.252	N/A
	S1/2 (EN-R3)	172.20.1.21	255.255.255.252	N/A
	Lo0	1.1.17.1	255.255.255.255	N/A
	Lo1	1.1.17.100	255.255.255.255	N/A
	Tunnel1	100.100.100.2	255.255.255.240	N/A
	Tunnel2	100.100.200.2	255.255.255.240	N/A
EN-R2	S1/0 (EN-R1)	172.20.1.18	255.255.255.252	N/A
	S1/1 (EN-R3)	172.20.1.25	255.255.255.252	N/A
	S1/2 (ISP-R5)	90.0.0.46	255.255.255.252	N/A
	Lo0	1.1.17.2	255.255.255.255	N/A
	Lo1	1.1.17.200	255.255.255.255	N/A
	Tunnel1	100.100.100.5	255.255.255.240	N/A

	Tunnel2	100.100.200.5	255.255.255.240	N/A
EN-R3	S1/1 (EN-R1)	172.20.1.22	255.255.255.252	N/A
	S1/2 (EN-R2)	172.20.1.26	255.255.255.252	N/A
	E0/0.10	172.17.10.1	255.255.255.0	N/A
	E0/0.20	172.17.20.1	255.255.255.0	N/A
	E0/0.30	172.17.30.1	255.255.255.0	N/A
	E0/0.100	172.100.1	255.255.255.0	N/A
	Lo0	1.1.17.3	255.255.255.255	N/A
EN-SW1	VLAN 100	172.17.100.101	255.255.255.0	172.17.100.254
EN-SW2	VLAN 100	172.17.100.102	255.255.255.0	172.17.100.254
EN-SW3	VLAN 100	172.17.100.103	255.255.255.0	172.17.100.254
EN-PC1	Eth0	172.17.10.10	255.255.255.0	172.17.10.254
EN-PC2	Eth0	172.17.20.20	255.255.255.0	172.17.20.254

Luxembourg				
Device	**Interface**	**IP Address**	**Subnet Mask**	**Default Gateway**
LU-R1	S1/0 (LU-R2)	172.20.1.30	255.255.255.252	N/A
	S1/2 (ISP-R2)	90.0.0.30	255.255.255.252	N/A
	E0/1.10	172.18.10.1	255.255.255.0	N/A
	E0/1.20	172.18.20.1	255.255.255.0	N/A
	E0.0/30	172.18.30.1	255.255.255.0	N/A
	E0/1.100	172.18.100.1	255.255.255.0	N/A
	Lo0	1.1.18.1	255.255.255.255	N/A
	Lo1	1.1.18.100	255.255.255.255	N/A
	Tunnel1	100.100.100.3	255.255.255.240	N/A
	Tunnel2	100.100.200.3	255.255.255.240	N/A
LU-R2	S1/0 (LU-R1)	172.20.1.29	255.255.255.252	N/A
	S1/1 (ISP-R1)	90.0.0.22	255.255.255.252	N/A
	E0/0.10	172.18.10.2	255.255.255.0	N/A
	E0/0.20	172.18.20.2	255.255.255.0	N/A
	E0/0.30	172.18.30.2	255.255.255.0	N/A
	E0/0.100	172.18.100.2	255.255.255.0	N/A
	Lo0	1.1.18.2	255.255.255.255	N/A
	Lo1	1.1.18.200	255.255.255.255	N/A
	Tunnel1	100.100.100.6	255.255.255.240	N/A
	Tunnel2	100.100.200.6	255.255.255.240	N/A
LU-SW1	VLAN 100	172.18.100.101	255.255.255.0	172.18.100.254
LU-PC1	Eth0	172.18.10.10	255.255.255.0	172.18.10.254
LU-PC2	Eth0	172.18.20.20	255.255.255.0	172.18.20.254
LU-AAA_Server	Eth0	172.18.30.30	255.255.255.0	172.18.30.254

China				
Device	**Interface**	**IP Address**	**Subnet Mask**	**Default Gateway**
CH-R1	S1/0 (CH-R1)	172.20.1.34	255.255.255.252	N/A
	S1/1 (ISP-R1)	90.0.0.26	255.255.255.252	N/A
	E0/1.10	172.19.10.1	255.255.255.0	N/A
	E0/1.20	172.19.20.1	255.255.255.0	N/A

	E0/1.30	172.19.30.1	255.255.255.0	N/A
	E0/1.100	172.19.100.1	255.255.255.0	N/A
	Lo0	1.1.19.1	255.255.255.255	N/A
	Lo1	1.1.19.100	255.255.255.255	N/A
	Tunnel1	100.100.100.4	255.255.255.240	N/A
	Tunnel2	100.100.200.4	255.255.255.240	N/A
CH-R2	S1/0 (CH-R1)	172.20.1.33	255.255.255.252	N/A
	S1/1 (ISP-R2)	90.0.0.34	255.255.255.252	N/A
	E0/0.10	172.19.10.2	255.255.255.0	N/A
	E0/0.20	172.19.20.2	255.255.255.0	N/A
	E0/0.30	172.19.30.2	255.255.255.0	N/A
	E0/0.100	172.18.100.2	255.255.255.0	N/A
	Lo0	1.1.19.2	255.255.255.255	N/A
	Lo1	1.1.19.200	255.255.255.255	N/A
	Tunnel1	100.100.100.7	255.255.255.240	N/A
	Tunnel2	100.100.200.7	255.255.255.240	N/A
CH-SW1	VLAN 100	172.19.100.101	255.255.255.0	172.19.100.254
CH-PC1	Eth0	172.19.10.10	255.255.255.0	172.19.10.254
CH-PC2	Eth0	172.19.20.20	255.255.255.0	172.19.20.254

ISP				
Device	**Interface**	**IP Address**	**Subnet Mask**	**Default Gateway**
ISP-R1	S1/0 (ISP-R2)	90.0.0.1	255.255.255.252	N/A
	S1/1 (ISP-R3)	90.0.0.5	255.255.255.252	N/A
	S1/2 (BH-R2)	90.0.0.17	255.255.255.252	N/A
	S1/3(LU-R2)	90.0.0.21	255.255.255.252	N/A
	S2/0(CH-R1)	90.0.0.25	255.255.255.252	N/A
	Lo0	1.1.1.1	255.255.255.255	N/A
	Lo1	10.10.10.10	255.255.255.255	N/A
ISP-R2	S1/0 (ISP-R1)	90.0.0.2	255.255.255.252	N/A
	S1/1 (ISP-R4)	90.0.0.9	255.255.255.252	N/A
	S1/2 (LU-R1)	90.0.0.29	255.255.255.252	N/A
	S1/3(CH-R2)	90.0.0.33	255.255.255.252	N/A
	S2/0(EN-R1)	90.0.0.37	255.255.255.252	N/A
	Lo0	1.1.1.2	255.255.255.255	N/A
	Lo1	20.20.20.20	255.255.255.255	N/A
ISP-R3	S1/0(ISP-R4)	90.0.0.13	255.255.255.252	N/A
	S1/1(ISP-R1)	90.0.0.6	255.255.255.252	N/A
	S1/2(BH-R1)	90.0.0.41	255.255.255.252	N/A
	Lo0	1.1.1.3	255.255.255.255	N/A
	Lo1	30.30.30.30	255.255.255.255	N/A
ISP-R4	S1/0(ISP-R3)	90.0.0.14	255.255.255.252	N/A
	S1/1(ISP-R2)	90.0.0.10	255.255.255.252	N/A
	S1/2(EN-R2)	90.0.0.45	255.255.255.252	N/A
	Lo0	1.1.1.4	255.255.255.255	N/A
	Lo1	40.40.40.40	255.255.255.255	N/A

Router-ID	
BH-R1	1.1.16.1
BH-R2	1.1.16.2
BH-R3	1.1.16.3
BH-R4	1.1.16.4
EN-R1	1.1.17.1
EN-R2	1.1.17.2
EN-R3	1.1.17.3
LU-R1	1.1.18.1
LU-R2	1.1.18.2
CH-R1	1.1.19.1
CH-R2	1.1.19.2
ISP-R1	1.1.1.1
ISP-R2	1.1.1.2
ISP-R3	1.1.1.3
ISP-R4	1.1.1.4

VTP	
Bahrain	bahrain@vtp
England	england@vtp

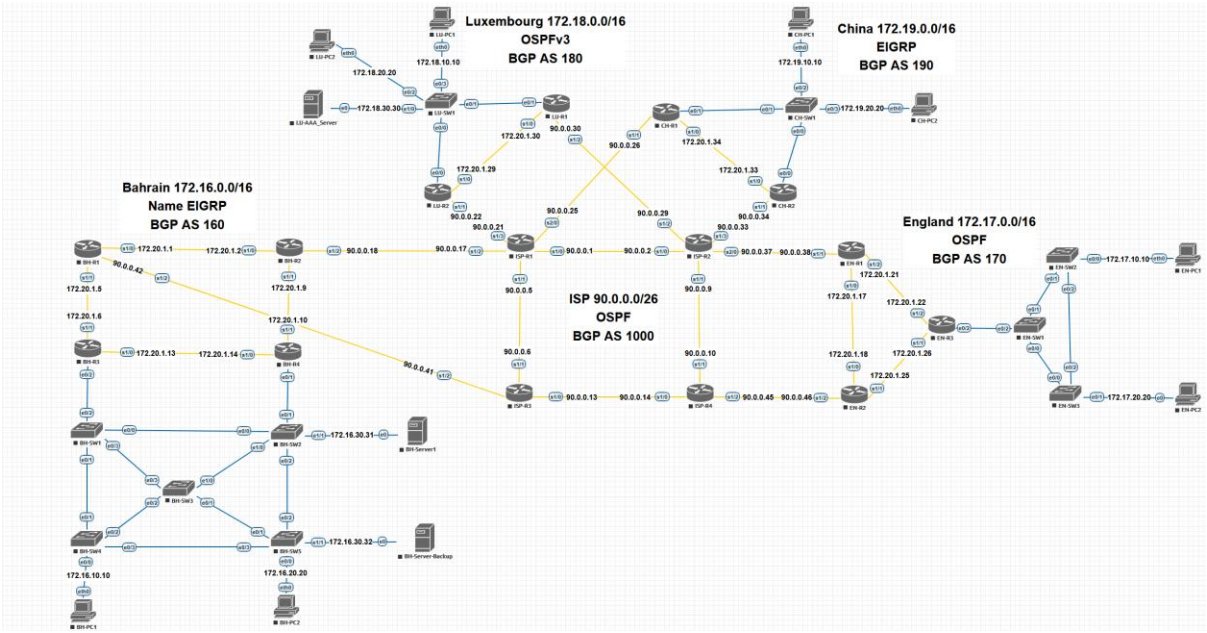
VLANs	
IT	10
Guests	20
Servers	30
Management/Native	100

SSH (GHN.com)	
Username/Device	**Password**
BH-R1	bhr1@ssh
BH-R2	bhr2@ssh
BH-R3	bhr3@ssh
BH-R4	bhr4@ssh
BH-SW1	bhsw1@ssh
BH-SW2	bhsw2@ssh
BH-SW3	bhsw3@ssh
BH-SW4	bhsw4@ssh
BH-SW5	bhsw5@ssh
EN-R1	enr1@ssh
EN-R2	enr2@ssh
EN-R3	enr3@ssh
EN-SW1	ensw1@ssh
EN-SW2	ensw2@ssh
EN-SW3	ensw3@ssh
LU-R1	lur1@ssh
LU-R2	lur2@ssh
LU-SW1	lusw1@ssh

CH-R1	chr1@ssh
CH-R2	chr2@ssh
CH-SW1	chsw1@ssh

DMVPN Tunnels				
Router	**Interface**	**EIGRP AS number**	**Hub/Spoken**	**IP Address**
BH-R1	Tunnel 1	100	Hub/ Active	100.100.100.1/28
BH-R2	Tunnel 2	100	Hub/ Backup	100.100.200.1/28
EN-R1	Tunnel 1	100	Spoken	100.100.100.2/28
	Tunnel 2	100	Spoken	100.100.200.2/28
EN-R2	Tunnel 1	100	Spoken	100.100.100.5/28
	Tunnel 2	100	Spoken	100.100.200.5/28
LU-R1	Tunnel 1	100	Spoken	100.100.100.3/28
	Tunnel 2	100	Spoken	100.100.200.3/28
LU-R2	Tunnel 1	100	Spoken	100.100.100.6/28
	Tunnel 2	100	Spoken	100.100.200.6/28
CH-R1	Tunnel 1	100	Spoken	100.100.100.4/28
	Tunnel 2	100	Spoken	100.100.200.4/28
CH-R2	Tunnel 1	100	Spoken	100.100.100.7/28
	Tunnel 2	100	Spoken	100.100.200.7/28

Network Topologies (Logical Design)



Physical Design

rack design

Layer 2 Design and Features

GHN Layer 2 is designed for stability that divided into 3 main categories:

Virtual Local Area Network:

VLANs segment and divide local departments in the network and isolates them to maintain a well structure Local Area Network. This results in enhanced scalability, strengthened network security boundaries, as well as simplifying the overall network and keeping it neater and more organized. Because traffic is secluded to its assigned segment, broadcast domains are minimized to allow each part of the network to be supervised and managed more efficiently and professionally.

Spanning Tree:

Each site has a primary and secondary root bridge to controls the Layer 2 topology. This prevents random switches from taking over, keeps the forwarding path predictable, and stops loops before they even start. The idea is simple: the designated root wins every time, and the backup takes over instantly if the primary fails. This gives you stability, fast convergence, and full control over how the Layer 2 domain behaves.

Vlan Trunking protocol:

Each site using VTP is crucial because of the important functionality the vtp do is to keep VLAN information consistent across the site switches. It centralizes VLAN creation and updates, making the whole domain easier to manage and reducing configuration drift. With

a single source of truth, new switches fall in line automatically, and the network stays clean, synchronized, and predictable.

Layer 3 Design and Features

Layer 3 is responsible for routing and policy between all GHN sites

IGP per site:

Each site runs the IGP that best fits its role in the GHN. Bahrain and China use EIGRP because it provides fast convergence and straightforward route summarization. England runs OSPFv2 and Luxembourg runs OSPFv3 to support their current design and prepare for future IPv6 deployment. All internal router links use point to point addressing to keep routing simple and make troubleshooting easier. The variation in IGPs reflects the operational needs and responsibilities of each site within the global health network.

BGP edge design

Each country is its own BGP autonomous system: Bahrain AS 160, England AS 170, Luxembourg AS 180 and China AS 190. External border gateway protocol (EBGP) peering is configured between each edge router and the ISP routers over 90.0.0.0/26 links. Route filtering and summarisation are used so that each site only advertises its own aggregate blocks 172.16.0.0/16, 172.17.0.0/16, 172.18.0.0/16, 172.19.0.0/16 into the ISP and each site advertise the loopback 0 for the DMVPN reachability. This keeps the global routing table clean, stable, and tightly controlled.

Redundant protocol with inter vlan and native vlan

Inter VLAN routing is provided through sub interfaces, giving each VLAN its own gateway and IP subnet. Traffic stays segmented, and routing decisions stay clean and predictable. To add resilience, HSRP runs across the gateway routers so that each VLAN has a virtual default gateway. If the active router fails, the standby takes over instantly without interrupting user traffic. This keeps the core services reachable, avoids single points of failure, and maintains stable routing across all VLANs even during device outages. The trunk links use a dedicated native VLAN to carry untagged control traffic and keep management frames separate from user data. This avoids mis tagging issues,

keeps the Layer 2 domain clean, and ensures the Hot Standby Router Protocol (HSRP) hello messages and other control protocols move reliably across the trunk.

This Layer 3 design supports scalability, clear policy separation between AS, and fast convergence in the event of link or router failure.

Internet/Virtual Layer Decisions

To be continue….

Presentation Layer

The presentation layer is where end-user applications live and how they experience the network:

HD video conferencing

video conferencing between sites to help meet the HD video with acceptable latency requirement and quality matrix.

Enterprise applications

Internal web, DNS, FTP, email and file services hosted in HQ with redundancy where possible and reachable via the routed WAN.

Telnet is available but SSH is preferred and mandated for administrative access in the security design.

User access

Users access services using DNS names, with DHCP handing out IP, Email For sending and receiving Emails, FTP to send and receive Files between Branches extremely Fast, gateway and DNS information per site.

Centralised AAA can be extended later to control user access to specific services if needed.

Security Services Layer Decisions

Security is integrated at every layer to satisfy ISO27001 aligned requirements

Authentication Authorization Accounting (AAA) and Role Based Access Control (RBAC)

Central AAA server in Luxembourg 172.18.30.30 authenticates administrative access for routers and switches using RADIUS.

Role based access control is used to limit privilege level 15 access to authorised administrators only.

Dynamic Multipoint Virtual Private Network and Internet Protocol Security

DMVPN Phase 3 gives the GHN a scalable and flexible overlay network. The design uses redundant hubs and redundant spokes, ensuring high availability across all sites. The hubs manage the control plane, while spokes dynamically form direct tunnels whenever traffic demands it. NHRP redirects allow spokes to bypass the hub after the first packet, reducing latency and offloading the core.

All tunnels are secured with IPsec using IKEv1, guaranteeing that inter-site traffic is always encrypted as it moves across the WAN. This satisfies the requirement that communication between Bahrain, England, Luxembourg, and China never travels in clear text. The result is a secure, robust, and efficient site to site mesh without the burden of maintaining static VPN tunnels.

Routing and control plane security

Authentication on OSPFv3 and EIGRP adjacencies key chains to prevent spoofed routing updates.

L2 security

The Layer 2 security posture is built on strict control of switch behaviour and predictable handling of edge ports. PortFast is enabled on access interfaces, so user devices come online quickly without participating in Spanning Tree calculations. Loop Guard is applied on non edge links to stop unidirectional link failures from creating loops. Root Guard is used on interfaces that should never receive superior BPDUs, locking down the root bridge and preventing accidental or malicious STP manipulation.

Negotiation is disabled with nonegotiate on trunk ports to stop unwanted DTP behaviour and keep trunking under strict control. Port Security is enforced on access ports to limit the number of MAC addresses to five and shut down ports that show suspicious activity. BPDU Guard and BPDU Filter are used to make sure access ports stay access only any unexpected BPDU causes an immediate shutdown, protecting the STP domain from rogue switches.

All unused ports are administratively shutdown and moved to an isolated VLAN 999, cutting off any open entry point into the network. The combined effect is a hardened Layer 2 environment that is far less vulnerable to loops, spoofing, or unauthorized devices.

Access controlled list

infrastructure ACLs to protect router control plane, management ACLs limiting SSH/Telnet to trusted management subnets.

Together, these controls support the project’s goals of a secure, reliable and efficient WAN for GHN.

Deployment Diagram

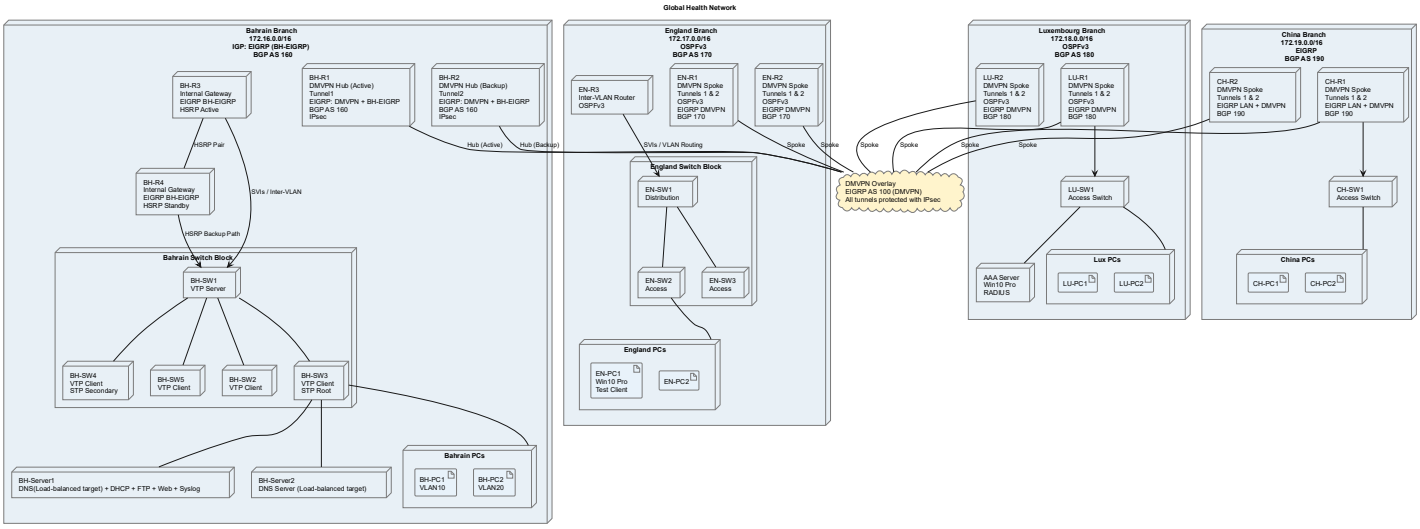


Figure 1 Deployment Diagram