BAHRAIN POLYTECHNIC بوليتكنك البحرين

Assessment Cover Sheet

Assessment Title	Thesis Document		
Assessment Type	Uncontrolled	Individual	Not must-pass
Due Date	28th December 2025	**Course Code**	IT7099
Course Title	IT Project		
Internal Moderator's Name	Bahruz Mashrequi		
External Examiner's Name			

Instructions:

1. This cover sheet must be completed (section in red below) and attached to your assessment before submission in hard copy/soft copy.
2. The time allowed for this assessment is 8 weeks
3. This assessment carries 30 marks assessing CILO 1, CILO 2 and CILO 4.
4. The materials allowed for use in this assessment are Thesis (Design + Technical) document.
5. The **use of generative AI tools is strictly prohibited**.
6. References consulted (if any) must be properly acknowledged and cited.
7. The assessment has a total of XXX pages.

Learner ID	202202674	**Date Submitted**	28/12/2025
Learner Name	Husain Ali		
Programme Code	IT8030		
Programme Title	Networking		
Lecturer's Name			

By submitting this assessment for marking, I affirm that this assessment is my own work.

Learner Signature	**Husain Ali**

Do not write beyond this line. For assessor use only.

Assessor's Name			
Marking Date		**Maks Obtained**	

Comments:

CCNP Route For A Global Health Network

A Thesis Submitted in

(Partial) Fulfillment of the

Requirements for the Degree of

Bachelor of Science

in Information & Communication Technology

at

Bahrain Polytechnic

December 2025

Title

CCNP Route For A Global Health Network

Copyright

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Signature Husain Ali Name Husain Ali Date 28/12/2025

Approval Signatures

APPROVED FOR THE ICT PROGRAMME

_____

(thesis supervisor), Thesis Supervisor Date

_____

(writing tutor), Technical Writing Tutor Date

Abstract

The creation, installation, and assessment of an enterprise-grade Wide Area Network (WAN) for the Global Health Network (GHN), a global healthcare organization with operations in Bahrain, England, Luxembourg, and China, is explained in this project. By providing a secure, scalable, and resilient routing architecture that can support high-definition medical communication and essential healthcare services while adhering to legal requirements like Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and Bahrain's Personal Data Protection Law (PDPL), the main goal is to address shortcomings in the current network.

Requirements analysis, architectural design, simulation-based implementation, and thorough testing are all part of the procedure's structured engineering approach. Using Enhanced Interior Gateway Routing Protocol (EIGRP), Named EIGRP, Open Shortest Path First version two (OSPFv2), OSPFv3, and Multiprotocol Border Gateway Protocol (MP-BGP), several routing protocols are implemented across several autonomous systems. Dynamic Multipoint VPN (DMVPN) Phase 3 with Internet Protocol Security (IPsec) encryption provides secure inter-site connectivity, allowing for high availability and dynamic spoke-to-spoke communication. To satisfy operational requirements, enterprise services including Domain name system (DNS), Dynamic Host Configuration Protocol (DHCP), web, File transfer protocol (FTP), Email, and Authentication, Authorization, and Accounting (AAA) are integrated.

Complete end-to-end reachability, consistent routing convergence, encrypted WAN communication, and efficient delivery of services across all sites are all demonstrated by the deployed solution. The findings verify that the suggested architecture satisfies GHN's operational, technological, and legal criteria, offering a strong basis for further growth and improved digital healthcare services.

Acknowledgements

I would like to express my sincere gratitude to Mr. Mohamed Elkanzi for his guidance, support, and constructive feedback throughout the development of this thesis and in my study. His insights and encouragement played a key role in shaping both the technical depth and overall quality of this work.

I would also like to thank my instructors and academic supervisors Dr. Ayman Al Ani for providing the knowledge, resources, and academic foundation necessary to complete this project. Their expertise and direction were essential in navigating the technical and theoretical challenges encountered during the research and implementation phases.

Special appreciation goes to my colleagues and peers who offered support, discussion, and valuable perspectives during this work. Their collaboration and shared problem solving contributed significantly to the learning experience.

Finally, I am deeply grateful to my family for their continuous support, patience, and motivation throughout my academic journey. Their encouragement made it possible to stay focused and committed to completing this thesis.

Table of Contents

List of Figures

List of Tables

List of Symbols

No table of Symbols entries found.

GHN project does not have symbols in it.

List of Abbreviations

Abbreviations	Definition
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
GHN	Global Health Network
HD	High Definition
DNS	Domain name system
FTP	File transfer protocol
WEB	world wide web
WAN	Wide Area Network
IT	Information Technology
IP	Internet Protocol
EMAIL	Electronic mail
DHCP	Dynamic Host Configuration Protocol
HIPAA	Health Insurance Portability and Accountability Act
GDPR	General Data Protection Regulation
EIGRP	Enhanced Interior Gateway Routing Protocol
OSPFv2	Open Shortest Path First version two
OSPFv3	Open Shortest Path First version three
MP-BGP	Multiprotocol Border Gateway Protocol
IBGP	Internal Border Gateway Protocol
EBGP	External Border Gateway Protocol
VPN	Virtual Private Network
DMVPN	Dynamic Multipoint VPN
IPsec	Internet Protocol Security
AAA	Authentication, Authorization, and Accounting
PDPL	Personal Data Protection Law
ISP	Internet Service provider
VLAN	Virtual Local Area Network
AD DS	Active Directory Domain Services
BPDU	Bridge Protocol Data Unit
EVE-NG	Emulated Virtual Environment Next Generation
OS	Operating System
RBAC	Role-Based Access Control
GRE	Generic Routing Encapsulation
mGRE	Multipoint Generic Routing Encapsulation
AES	Advanced Encryption Standard
SHA	Secure Hash Algorithm
3DES	Triple Data Encryption Standard
RSA	Rivest Shamir Adleman
NHRP	Next Hop Resolution Protocol
LSAs	Link State Advertisements
SPF	Shortest Path First
DUAL	Diffusing Update Algorithm
EGP	Exterior Gateway Protocols
STP	Spanning Tree Protocol

VTP	VLAN Trunking Protocol
SVI	Switched Virtual Interface
HSRP	Hot Standby Router Protocol
EVE-NG	Emulated Virtual Environment – Next Generation
GIU	Graphical User Interface
CLI	Command Line Interface
SFP	Shortest Path First
ESP	Encapsulating Security Payload
EHR	Electronic Health Records
IIS	Internet Information Services
UML	Unified Modeling Language
NHS	Next Hop Server
SRV	Service record

Table 1 List of Abbreviation

Introduction

Project Rationale

GHN operates across multiple countries and depends heavily on reliable, HD communication to deliver medical services. The organization relies on HD video conferencing, internal email, DNS, FTP, and web services for daily operations across Bahrain, England, Luxembourg, and China. The existing WAN infrastructure is unable to meet the demands of modern health care IT, is basic, lacks redundancy, and has limited routing capabilities. Inadequate security measures, single path routing, and inconsistent performance raise the possibility of failures, data exposure, and service degradation problems that have an immediate effect on patient care and organizational effectiveness.

As GHN expands, these weaknesses become more severe. HD medical consultations require predictable bandwidth, low latency, and resilient routing. Sensitive healthcare data must comply with strict legal frameworks, including HIPAA, GDPR, and Bahrain's PDPL Law No. 30 of 2018, making secure inter site communication a nonnegotiable requirement. Without a modern, scalable network, GHN cannot sustain global operations or meet the expected quality of service.

The motivation for this project is to build a WAN architecture that eliminates these limitations by delivering resilience, encryption, intelligent routing, and full operational stability across a multinational network.

Project Objectives

The purpose of this project is designing and implementing an advanced WAN routing solution that enables GHN to operate securely, efficiently, and reliably across its branches. The network must provide encrypted communication channels, scalable network, minimize downtime, and ensure compliance with global and local data protection standards for patient's data.

Project Objectives

1. Build a fully functional enterprise grade WAN interconnecting the four GHN sites.
2. Implement dynamic routing using EIGRP, Name-EIGRP, OSPFv2, OSPFv3, and MP-BGP across different autonomous systems.
3. Deploy DMVPN Phase 3 with IPsec to provide encrypted, scalable, hub and spoke and spoke to spoke communication.
4. Enhance security L2 in all branches.
5. Integrate server services DNS, FTP, Web, and Email across the branches.
6. Ensure that GHN compliance with healthcare data regulations HIPAA, GDPR, PDPL and ISO 27001.
7. Document, test, validate, and evaluate network performance, stability, and security.

Limitations

1) Fixed budget and fixed timeline.
2) Dependence on simulation platforms EVE-NG and limited physical hardware availability.
3) Bandwidth limitations dictated by the ISP infrastructure.

Prior Work

according to the project brief GHN was limited to basic routing. The existing topology lacked route redistribution, advanced BGP features, tunneling technologies, and proper security architecture. Prior work did not address redundancy, multi AS routing, or VPN overlays all essential components for multinational healthcare operations.

Research in enterprise network design commonly highlights the importance of dynamic routing protocols, segmentation, and encrypted overlay networks for distributed organizations. However, these studies remain broad and do not address GHN constraints, such as country specific routing domains, healthcare data regulations, and the requirement for HD telemedicine. The shortcomings in existing work justify the need for a custom design tailored to GHN operational, regulatory, and technical environment. (juniper, 2023)

This project builds a complete, integrated solution that fills these gaps by merging advanced routing, security, scalability, and global healthcare requirements into one cohesive architecture.

Hypothesis

If GHN adopts modern WAN architecture that uses dynamic routing, encrypted DMVPN overlays, redundant ISP paths, and a structured addressing scheme, then the organization will achieve secure, stable, and efficient communication across all sites. This will directly improve service quality, reduce downtime, ensure data confidentiality, and enhance operational performance.

The hypothesis assumes that correct implementation of routing protocols, redundancy, and security controls will eliminate the limitations of the current network and meet the organization's technical and compliance requirements.

If GHN adopts modern WAN architecture that uses dynamic routing, encrypted VPN, redundant ISP paths and scalable structured addressing scheme, then GHN will achieve secure, stable, and efficient communication across all sites. This will directly improve service quality, reduce downtime, ensure data confidentiality, and enhance operational performance.

The hypothesis assumes that correct implementation of routing protocols, redundancy, and VPN will eliminate the limitations of the current network and meet the GHN organization technical and compliance requirements.

Success is defined by:

- Full end to end reachability between all GHN sites.
- Stable routing with fast convergence.
- Encrypted communication over all WAN links.
- Zero single points of failure.

- Compliance with healthcare security standards.
- Easy to expand branches

Proposed Solution

The proposed solution is a fully engineered WAN design that interconnects Bahrain, England, Luxembourg, and China. Each country maintains its own IGP and autonomous system while still achieving complete inter site reachability through MP-BGP and route reflection. DMVPN Phase 3 with IPsec provides encrypted tunnels, redundant hubs, and dynamic spoke to spoke communication to reduce latency and improve performance.

The network implements server services, VLAN segmentation, Layer 2 security, and a scalable and structured IPv4 addressing plan that matches GHN operational structure. Security measures align with ISO 27001 and healthcare legislation locally and globally, ensuring the confidentiality and integrity of patient data.

This solution delivers scalability, resilience, high availability, and secure communications, all essential for a modern healthcare organization operating internationally with less down time or disturbance.

Report overview

The complete development of the GHN WAN solution will be split down in the following chapters of this thesis document. A significant amount of the work is covered in each chapter, which explains the decisions, steps, and results involved in creating a secure, scalable, multi branch healthcare network.

The **Background chapter** provides an overview of the networking concepts used in this project, including routing protocols, DMVPN over IPsec, and secure WAN design. It also reviews technologies and research related to building a multinational healthcare network.

This chapter gives an overview of how the **project requirements** were gathered and translated into the final GHN architecture. It addresses the addressing scheme, routing structure, redundancy model, and security controls in use on the network.

The **Implementation chapter** introduces how to build the network of GHN. Configuration within routing protocols, DMVPN tunnels, encryption, VLANs, and server services is also described, which shows a step-by-step explanation of how this was executed.

The **Testing chapter** assesses the performance and reliability of the network. It verifies routing behavior, failover, encryption, service reachability, and overall stability to confirm that the system meets GHN operational demands.

The **Discussion and Conclusion chapter** outlines the summary of achieved results, challenges, and limitations. It further highlights LESPI considerations and personal reflections on the technical and professional experience gained.

In **Bahraini perspective** has been included to relate the project to the country's national direction. This work is considered to go hand in hand with Bahrain's push for better digital healthcare systems, secure communication, and compliance with regulations such as the PDPL, which supports the country broader goal of improving healthcare technology.

Background

Introduction

This chapter establishes the technical and theoretical foundation required for designing and implementing a secure, scalable, and multi country wide area network for the Global Health Network. The GHN environment requires high availability inter branch connectivity, encrypted data transmission, dynamic routing, and interoperability across four autonomous systems deployed in Bahrain, England, Luxembourg, and China. The design relies on industry standard routing protocols, VPN tunneling technologies, and security frameworks.

This section introduces the underlying networking theories, routing protocol mechanisms, tunneling concepts such as DMVPN Phase 3, and encryption standards such as IPsec. It also discusses the technologies selected for the project, the alternatives considered, relevant academic literature, and market research on existing WAN and VPN solutions.

Related Theory

1) Wide Area Network Architecture

A wide area network connects geographically dispersed sites through ISP infrastructure and supports routing, redundancy, and inter domain interoperability. Traditional WANs rely on leased lines or MPLS circuits, while modern enterprise WANs use IP routed connections secured by VPN overlay technologies (Cisco , 2007). WAN architecture depends heavily on routing protocols, convergence algorithms, link state databases, and tunnel based overlays to achieve scalability and resiliency. WAN design principles are described extensively in Internet architecture studies (Halabi & Mcpherson, 2000) and vendor validated designs.

2) Interior Gateway Protocols

I. OSPF (OSPFv2 & OSPFv3)

Open Shortest Path First is a link state routing protocol defined in (Moy, 1998) for IPv4 and (Ferguson, Lindem, & Moy, 2008) for IPv6. OSPF builds a complete

map of the topology by exchanging Link State Advertisements and uses Dijkstra Shortest Path First algorithm to compute optimal routes. It supports hierarchical area design, route summarization, and fast convergence, making it suitable for large enterprise environments such as GHN sites in England and Luxembourg.

II. Enhanced Interior Gateway Routing Protocol

EIGRP is an advanced distance vector protocol utilizing the Diffusing Update Algorithm for loop free and rapid convergence. Cisco technical documentation describes EIGRP as a hybrid protocol offering unequal cost load balancing and distributed neighbor discovery (Cisco, 2017). It is used within GHN Bahrain and China, where multi subnet hierarchy and summarization are required.

III. Named EIGRP

Named EIGRP is the modern implementation of EIGRP introduced by Cisco to unify IPv4 and IPv6 configuration under a single address family structure. Instead of configuring multiple EIGRP processes, Named EIGRP uses one logical instance with separate address families, improving scalability and reducing configuration complexity. Cisco documentation notes that Named EIGRP centralizes interface configuration under “af-interface” sections, supports per address family features, and aligns with current best practices for dual stack enterprise networks (Cisco, 2024).

Within GHN, Named EIGRP is also employed as the internal routing protocol for GHN DMVPN Phase 3 overlay. Its support for rapid convergence, unequal cost load balancing, and per interface control makes it a strong fit for hub and spoke topologies. Named EIGRP integrates seamlessly with DMVPN because it operates efficiently over GRE multipoint tunnels, responds correctly to NHRP shortcuts, and minimizes routing overhead across dynamic spoke to spoke paths. This ensures stable and scalable routing over the encrypted IPsec secured WAN.

3) Exterior Gateway Protocols

Border Gateway Protocol

BGP is the inter domain routing protocol of the internet, defined in (Rekhter, Hares, & Li, 2006). It enables communication between autonomous systems by exchanging path attributes and enforcing routing policies. BGP supports both iBGP and eBGP and plays a crucial role in GHN where each country operates its own AS. BGP policy driven nature allows GHN to control outbound and inbound routes, maintain redundancy through the ISP, and ensure deterministic inter site connectivity.

4) VPN Tunneling and Overlay Encryption

1. GRE Tunneling

Generic Routing Encapsulation creates a virtual point to point or multipoint tunnel used to transport various protocols over IP networks. Defined in (Farinacci, Li, Meyer, Hanks, & Traina, 2000), GRE provides encapsulation but no encryption, making it ideal as a foundation for overlay routing in DMVPN.

2. DMVPN Phase 3

Dynamic Multipoint VPN is a Cisco framework combining mGRE tunnels, NHRP (Cole, Naganand Doraswamy, Katz, Luciani, & Piscitello, 2022), and IPsec. Phase 3 enables spoke to spoke dynamic tunnels through NHRP redirect/shortcut mechanisms, reducing hub load and improving performance in distributed environments. Cisco DMVPN design guide identifies Phase 3 as the most scalable version due to its ability to support large mesh topologies (Design, 2008). GHN uses Phase 3 to enable efficient HD telemedicine traffic between international sites (Cisco Systems, 2020).

3. IPsec Encryption

IPsec is a suite of protocols that provides encryption, authentication, and integrity for IP traffic. (Seo & Kent, 2005), outlines its architecture while (Kent, 2005) defines ESP as the main component responsible for encrypting data. IPsec ensures compliance with international healthcare data protection requirements, which demand confidentiality and encryption (Cisco Systems, 2020).

5) Layer 2 and Layer 3 Security and Redundancy

Layer 2 switching provides segmentation, VLAN isolation, trunking, redundancy, and loop prevention within GHN sites. Spanning Tree Protocol, defined by the IEEE standards (IEEE, 2018; IEEE, 2004), prevents switching loops by selectively blocking redundant paths. Security enhancements such as BPDU Guard, Loop Guard, and Port Security are recommended by major vendors to mitigate misconfigurations and protect enterprise switching domains against common Layer 2 attacks (Vyncke, 2006), (Senecal, n.d.).

VLAN Trunking Protocol is used to manage and propagate VLAN information across GHN switches, reducing administrative overhead in multi switch environments. Inter VLAN routing is implemented using Layer 3 interfaces SVIs to enable communication between isolated VLANs while enforcing routing policies and segmentation. Hot Standby Router Protocol, defined in (Li, Cole, Morton, & Li, 1998), provides first hop redundancy by allowing two or more routers to share a virtual default gateway, ensuring continuous end user connectivity even during device or link failures.

Used and Considered Technologies

The chosen technologies for this project were selected because they meet industry requirements for secure wide area networking, are suitable for a distributed multinational setting, and are applicable to current enterprise network design. Because GHN relies on encrypted inter-site communication and spans multiple autonomous systems, the solution required technologies that could offer scalability, interoperability, and robust cryptographic protection. This section describes the platforms, protocols, and frameworks selected during the design and implementation phases, as well as several choices that were explored but eventually rejected. Each chosen technology was assessed using RFC standards, and academic literature to ensure dependability, viability, and adherence to best practices in WAN engineering.

Technology	Purpose
 EVE-NG	EVE-NG was selected Because it is the only platform that can handle the entire GHN system without collapsing. Packet Tracer is too simplistic; it can't emulate IPsec or DMVPN Phase 3, run actual iOS images, or support Windows Server services like DNS, DHCP, FTP, or web hosting (Cisco, 2023). despite that GNS3 is more powerful, scaling it to a multi-site WAN with redundant DMVPN hubs, BGP route reflectors, and complete routing stacks makes it unreliable and resource-intensive (GNS3 Technologies, 2016). EVE-NG is the only platform that provides realistic routing, security testing, and dependable end-to-end simulation for GHN because it runs real multi-vendor images, supports complex L2/L3 topologies, integrates Windows Server 2019 cleanly, and remains stable under large enterprise grade topologies (EVE-NG, 2023).
	By managing VLAN segmentation, Trunking, Ethernet frame forwarding, and other crucial access

 Cisco Layer 2 & 3 Switches and Router	layer functions, Cisco Layer 2 switches and routers serve as the basis of business network infrastructure. With support for technologies like VLANs, STP, port security, and other access layer controls necessary for safe and reliable LAN architecture, Cisco Catalyst Layer 2 switches offer high-performance switching for campus and branch environments (Cisco, n.d.). Cisco routers serve as the foundation for scalable WAN architectures by providing advanced Layer 3 packet forwarding, WAN connectivity, routing protocol support (OSPFv3, EIGRP, BGP), and secure remote site communication (Cisco, n.d.); (Cisco ASR 1000 Series Aggregation Services Routers," 2024)). Cisco Layer 2 switches and routers work together to give modernized multi-site networks like GHN the performance, security features, and dependability they need.
 Windows Server 2012 R2	Windows Server 2012 R2 provides GHN with a centralized enterprise platform that delivers identity management, secure FTP services, IIS-based web hosting, and DNS name resolution across all sites (AnirbanPaul, 2016; John-Hart, 2025). IIS offers modular and stable hosting for internal portals and applications, while DNS ensures that all internal systems including web services, email, and branch applications remain reachable throughout the multi-site WAN. Controlled file transfers for IT operations, configuration distribution, and documentation are handled through the built in FTP service. Linux-based DNS, web, and FTP stacks such as Bind9, Apache, and vsftpd were evaluated as alternatives. Although these tools are powerful, flexible, and free, the project required Windows

	Server experience, consistent integration with Active Directory, and a unified GUI-driven management approach that aligns with supervisor expectations and enterprise training objectives (Ubuntu, 2016; Apache, 2020). As a result, Windows Server 2012 R2 offered the most coherent, centralized, and enterprise-oriented solution for GHN's operational requirements.
H Mail Server	GHN makes utilize hMailServer, an open source email platform that provides SMTP, POP3, and IMAP features with small resource consumption, simple administration, and no licensing fee, making it a suitable choice for a regulated multiple site WAN environment (hMailServer, n.d.). Because of its high resource requirements, high licensing prices, and complicated setup, Microsoft Exchange Server was not chosen for GHN's real operational demands (Microsoft, 2016)
Thunderbird	GHN use Thunderbird to access the internal hMailServer. It provides a cross platform, lightweight, open source program that can handle SMTP, IMAP, and POP3 connections, enabling employees to send, receive, and manage business email with confidence (Thunderbird, 2025). The confidentiality and integrity of GHN's internal communications are maintained by its built in security features, which include TLS support, certificate checking, and phishing prevention. Because of its modular interface and plugin ecosystem, which enable customization without additional licensing fees, Thunderbird is also appropriate for use in academic and business settings.

	GHN maintains a straightforward, reliable, and affordable solution that seamlessly connects with the Windows Server 2012 R2-based hMailServer deployment by utilizing Thunderbird rather than more complex commercial email clients.
 WinRadius	WinRadius is an open source AAA platform used in GHN to provide centralized authentication, authorization, and accounting for all network devices. AAA is a fundamental requirement in enterprise networks because it ensures that only authorized personnel can access or modify device configurations, and it establishes full accountability by recording every authenticated action taken on the infrastructure. By integrating WinRadius into GHN, administrative access is unified, secure, and traceable across all branches, and reinforcing operational integrity throughout the simulated multi-site environment.
 Windows 7	Windows 7 is utilized within GHN as a lightweight workstation platform for performing administrative tasks such as accessing routers and switches over SSH and Telnet, as well as running RADIUS AAA server. Although it is an older operating system, Windows 7 remains suitable environments due to its low resource requirements, stable networking stack, and compatibility with a wide range of legacy administrative tools *(Stanek, 2010)*. It is built in networking utilities and support for third party SSH/Telnet clients such as PuTTY allow network administrators to manage GHN devices efficiently. Additionally, using Windows 7 for the lightweight RADIUS service provides a simple method for

	testing AAA authentication flows without the overhead of deploying a full Windows Server instance. This makes Windows 7 a practical and resource efficient choice for GHN.
Windows 10 Pro	Client operating systems representing end users within the network, used for testing login behavior, user experience, FTP Server, Web access, E-mail and domain.
VMware pro	A virtualization software that allows users to run virtual machines on their computers. Used to host the EVE-NG virtual environment
PuTTY	An SSH and telnet client is Used to access and configure routers, switches using the CLI

Table 2 Project Technologies

Related Work & Literature Review

Examining academic research, industry studies, and protocol standards related to secure multi site WAN communication is the purpose of this literature evaluation. The evaluation focuses on four main areas because GHN is a multi country environment that needs dynamic routing, encrypted interbranch communication, and a scalable overlay framework.

The evaluation focuses on four key areas:

- Routing theory and multi-site WAN networks.
- Overlays based on DMVPN and VPN.
- Security and performance standards in scenarios similar to healthcare.
- Equipment and platforms for supporting and simulating such infrastructures.

Additionally, the paper highlights gaps in the existing literature and describes how GHN provides a comprehensive, repeatable multi country WAN architecture that incorporates enterprise services, VPN overlays, and routing.

1) Routing theory and multi-site WAN networks

The foundation for enterprise and multi-domain network design has been set by foundational routing literature. While (Forouzan, 2013) describes the behavior of link state and distance vector algorithms used inside enterprise networks, (Huitema, 2000) describes hierarchical routing, path selection, and WAN interconnectivity. Although they do not address actual deployment across various autonomous systems, these publications provide as the theoretical basis for GHN's IGP and BGP design.

OSPF is discussed in (Moy, 1998) and (Ferguson, Acee Lindem, & Moy, 2008), addressing multi-area design, LSAs, and SPF computation for IPv4 and IPv6 networks (Moy, 1998; Coltun et al., 2008). A Border Gateway Protocol 4 (BGP-4), 2006 elaborates BGP, which is the international standard for routing data exchange between autonomous systems. Although they offer protocol definitions rather than integrated multiple-country

WAN architectures, these RFCs support GHN's use of OSPFv2, OSPFv3, EIGRP, and MP-BGP for multi-regional routing.

Convergence and scalability are impacted by protocol choice, according to results of assessments amongst internal routing protocols. (Badhan, Ara, Halima, Debnat, & Islam, 2024) show that EIGRP works better in specific hierarchical topologies, which validates GHN's choice to implement EIGRP in China and Bahrain. nonetheless, these studies do not look at mixed-IGP, multi-AS infrastructures with VPN overlays; instead, they look at individual protocols in confined lab settings.

GHN's requirement for strong route rules enforcement is further backed by BGP security studies. The dangers of incorrect settings and hijacking assaults between autonomous systems are emphasized by (Kundu, Atallah, & Bertino, 2010). While pertinent, these works do not offer an end to end multi-country WAN solution; instead, they highlight security problems.

In conclusion, the routing literature has solid theoretical foundations but lacks realistic multi-AS, multi-protocol WAN architectures that are comparable to GHN.

2) Overlays based on DMVPN and VPN

The foundational standard for encrypting WAN traffic continues to be IPsec. While (Kent, 2005) describes the ESP protocol used for guaranteeing confidentiality, integrity, and authentication, (Seo & Kent, 2005) outlines the security architecture for network layer protection (Kent & Seo, 2005; Kent, 2005). The cryptographic framework for protecting GHN's inter-site tunnels is provided by these standards.

Routed traffic is usually encapsulated behind IP tunnels using GRE, which was defined in (Farinacci, Li, Hanks, Meyer, & Traina, 2000) (Farinacci et al., 2000). Shortcut resolution is made possible by NHRP, which is an essential part of scalable dynamic overlay (Cole, Naganand Doraswamy, Katz, Luciani, & Piscitello, 2022). Although both protocols are necessary for tunnel formation, they do not by themselves offer the structure necessary for enterprise VPN scalability.

The most significant research study is by (Marah, Khalil, Elarabi, and Ilyas ,2021), who reviewed the performance of DMVPN Phase 3 and showed its scalability benefits, especially its capacity to provide spoke-to-spoke shortcuts and minimize hub congestion. GHN's decision to use DMVPN Phase 3 for inter-branch communication across four global sites is directly supported by this. However, their study does not integrate DMVPN with multi-AS BGP, enterprise services, or health care requirements; instead, it concentrates mostly on latency and throughput measurements.

Actual installation techniques and operational factors for DMVPN deployments are described in Cisco's DMVPN design guide (Design, 2008). Despite being highly beneficial, it fails to present just one enterprise WAN design that integrates server services, routing, and encryption.

As a result, despite VPN research supports GHN's selection of IPsec and DMVPN, it does not have a thorough implementation that is equivalent to GHN's.

3) Security and performance standards in scenarios similar to healthcare

Healthcare networks depend on strong confidentiality, integrity, and availability given the sensitive nature of patient data. (Kruse, Smith, Vanderlinden, & Nealand, 2017) emphasize that access control, encryption, and reliable connectivity are all essential for securing EHRs. Their findings support GHN’s usage of IPsec encrypted tunnels and robust inter site routing.

nonetheless, rather than WAN routing or VPN overlays, research on healthcare usually focuses on protecting data, regulatory structures, and application security. As a result, it inspires powerful encryption and segmentation but provides limited architectural direction for establishing a multi-country healthcare type WAN.

GHN solves this gap by designing an encrypted, multi-AS, multi-IGP infrastructure specifically geared to healthcare-related requirements, including low latency and safe inter-branch communication.

4) Equipment and platforms for supporting and simulating such infrastructures

Network designs are often validated using simulation environments prior to the actual deployment. Sophisticated business topologies may be evaluated in controlled environments thanks to EVE-NG's support for virtualized multi-vendor routers, servers, and firewalls (EVE-NG, 2023). However, rather than complete multi-country deployments, academic research primarily documents small-scale topologies or isolated protocol demonstration.

Enterprise services like as DNS, IIS, FTP, and identity management are being thoroughly explained in Windows Server documentation, whereas Linux-based alternatives Bind9, Apache and vsftpd are frequently used in open-source environments (Ubuntu, 2016; Apache, 2020). Nevertheless, previous research usually examines these kinds of services separately rather than how they work within a more comprehensive WAN design.

Email infrastructure research address lightweight solutions such as hMailServer and secure clients like Thunderbird, which offer encrypted IMAP/SMTP connection (Thunderbird, 2025). Nevertheless, the integration of it into a distributed WAN design is not addressed in this research.

Routing, VPN overlays, business servers, AAA RADIUS, and email services are all uniquely utilized by GHN within a single simulated multi-country environment.

Related Work

Research addressing WAN scalability frequently depends on MPLS L3VPN. (Rekhter, Hares, & Li, 2006) emphasize it is strong separation and scalability but highlight its reliance on provider infrastructure, making it unsuitable For GHN because of it is high cost, not quickly scalable and relay on ISP instead of within GHN architecture. Routing studies like those by Badhan, Ara, Halima, Debnat, and Islam (2024) examine protocol performance separately without taking into account the integration issues that arise in multi-AS setups.

VPN research examines IPsec, GRE, and DMVPN performance independently (Marah, Khalil, Elarabi, & Ilyas, 2021), but no studies combine these pieces into a multi-country design. Similar to this, the research on healthcare places a high value on encryption and dependability without going into detail on routing or WAN infrastructure (Kruse, Smith, Vanderlinden, & Nealand, 2017).

The usage of EVE-NG for protocol testing is documented in simulation literature (EVE-NG, 2023), but large scale infrastructures that replicate global WANs with enterprise services are rarely deployed.

Gaps Identified

Across the literature, the following gaps emerge:

- Protocols are evaluated individually rather than in integrated architectures.
- DMVPN Phase 3 research lacks multi-AS, multi-protocol implementations.
- Healthcare research addresses security but not WAN routing or overlays.
- Simulation studies do not document complex enterprise grade multi site designs.

GHN's Contribution

GHN fills these gaps by presenting a complete multi country WAN solution integrating:

1) Four autonomous systems connected via MP-BGP.
2) Mixed IGPs EIGRP, Name EIGRP, OSPFv2 and OSPFv3.
3) DMVPN Phase 3 with IPsec encryption.
4) Windows Server 2012 R2 services DNS, IIS, FTP and Email
5) RADIUS AAA using Windows 7.
6) Thunderbird as a secure email client

This level of integration does not exist in current literature, making GHN a unique academic and practical contribution.

Design

Introduction

This strategy illustrates the whole process of evaluating, designing, and engineering the GHN WAN solution. The project involved constructing a global, secure, scalable routing infrastructure that connects Bahrain, England, Luxembourg, and China using modern IGPs, MP-BGP, DMVPN Phase-3 over IPsec, and enterprise grade services such as DNS, WEB, FTP, DHCP, and Email.

The approach used a practical architectural methodology, combining:

1. gathering requirements (research, project brief, and interviews).

2. Architectural design of routing domains, addressing, DMVPN topologies, and security layers.

3. Using EVE-NG for iterative development and simulation, each component (IGPs, BGP, tunnels, server services, Layer 2 security) is tested.

4. Testing and verification, including failover, convergence, encryption, end to end reachability, and service performance.

Solution Design & System Architecture

Solution Design

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

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

- **Bahrain** primary regional hub and main data center, 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 allow centralized security policies with minimal disturbance to the network in each site.

Packet Flow Diagram

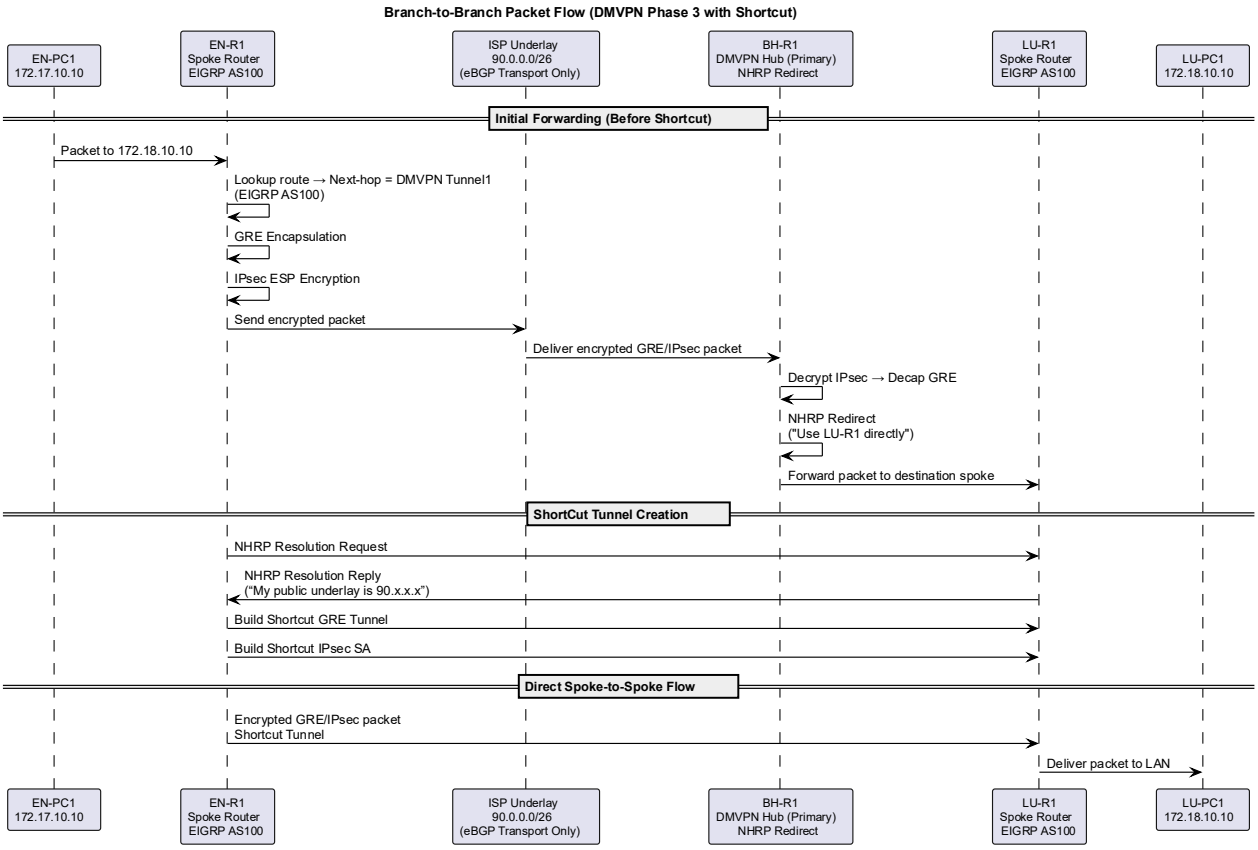

Figure 1 Packet Flow Diagram

The packet flow diagram illustrates the exact path that data travels across the Global Health Network, from a server or endpoint at a particular point to a destination at another. It displays the locations of routing decisions, encryption, and protocol transitions as packets travel via VLANs, access switches, distribution routers, DMVPN/IPsec overlays, and the ISP backbone. This figure combines the logical routing architecture with real operational packet movement.

At the local site, traffic begins inside a relevant VLAN user, server, or management before being sent by the access switch toward the router's SVI or physical sub interface. The diagram shows that Layer 2 traffic remains local, while Layer 3 traffic is routed to the distribution or core router, where the next hop is determined by the IGP EIGRP, OSPFv2, or OSPFv3, depending on the location. Internal routing decisions are determined based on the site's routing table, which summarizes local prefixes and indicates which packets must exit the site over a DMVPN tunnel.

Packets are wrapped inside GRE and then encrypted using IPsec ESP when inter-site communication is necessary. This transition is clearly depicted in the diagram: the outer IPsec header secures the inside of the packet after it has been wrapped in GRE. DMVPN Phase 3 ensures that packets meant for remote branches do not always flow through the hub. Rather, NHRP generates dynamic shortcuts that enable spoke-to-spoke communication when needed. This minimizes latency, improves bandwidth utilization, and optimizes performance for HD video calls, medical file transfers, and other vital healthcare applications.

Once encrypted, packets cross the ISP backbone. The graphic demonstrates how the ISP functions strictly as an IP transport network; it does not inspect or alter the encrypted payload. BGP at the WAN edges manages route advertisement and guarantees each independent system to contact faraway GHN networks without disclosing unwanted internal details. The packet flow illustration also shows that the IGP operating locally at each site determines the best local exit choice, while BGP handles next-hop resolution.

The process is reversed at the destination location. The original payload is sent into the local routing domain after the packet has been decrypted and the GRE encapsulation removed. The router forwards it toward the relevant VLAN, and the access switch finally delivers it to the end host or server. This end-to-end flow illustrates how GHN ensures service availability, confidentiality, and integrity for all inter-site communications.

When everything is considered, the packet flow diagram provides an accurate, end-to-end perspective of how user traffic, medical records, and service requests flow via GHN's infrastructure. It covers security layers, routing logic, DMVPN behavior, encryption borders, and interoperability between all four overseas sites, demonstrating how the network accomplishes secure, efficient, and predictable communication.

System Architecture

Network Topology Diagram

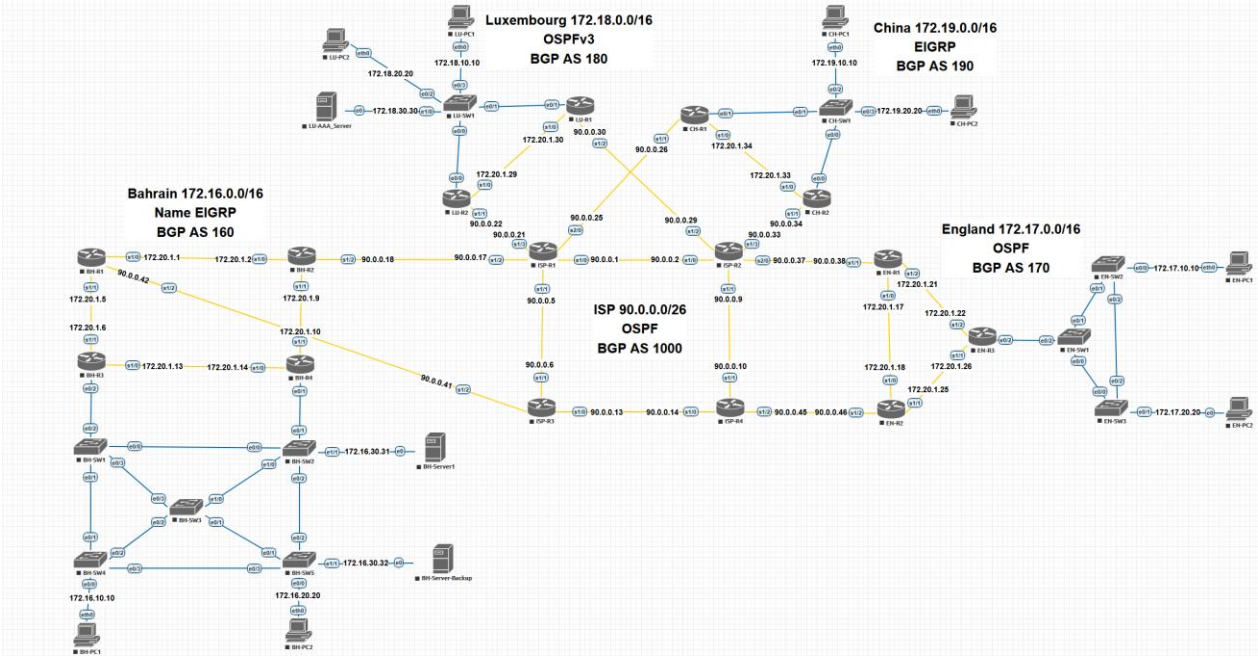

Figure 2 Network Topology Diagram

The figure illustrates the whole WAN architecture installed for the Global Health Network. Its layout interconnects the four international sites Bahrain, England, Luxembourg, and China through an ISP core utilizing the public network 90.0.0.0/26. Every country performs inside its own networking domain with a specific IPv4 block:

- Bahrain: 172.16.0.0/16 (AS160, Named EIGRP)
- England: 172.17.0.0/16 (AS170, OSPFv2)
- Luxembourg: 172.18.0.0/16 (AS180, OSPFv3)
- China: 172.19.0.0/16 (AS190, EIGRP)

Each site maintains its own IGP according to the topology's hierarchical, multi-AS architecture, whereas MP-BGP is used by the autonomous systems to share global routing

data. This method allows for controlled and safe inter-site communications while isolating internal routing complexity at each branch.

For the access layer, every branch uses VLAN segmentation for users, servers, and management. Local branch routers handle routing between VLANs, ensuring that local traffic remains within the site while global traffic, if required, is routed over the WAN via a DMVPN tunnel.

The ISP cloud gives a redundant way for all sites, with two routers at each country connecting into the ISP backbone. This guarantees uninterrupted service availability even in the event of link or node failures and removes single points of failure.

The topology diagram additionally illustrates the positioning of important services:

- Bahrain hosts fundamental web, DNS, FTP, and corporate email servers.
- Luxembourg hosts the central AAA server.
- All sites have user VLANs, management VLANs, and local access switches.

The entire solution design depends upon this topology. It creates routing domains, deals with the WAN overlay, shows redundancy paths, and maps the locations of key services throughout GHN's global network.

Deployment Diagram

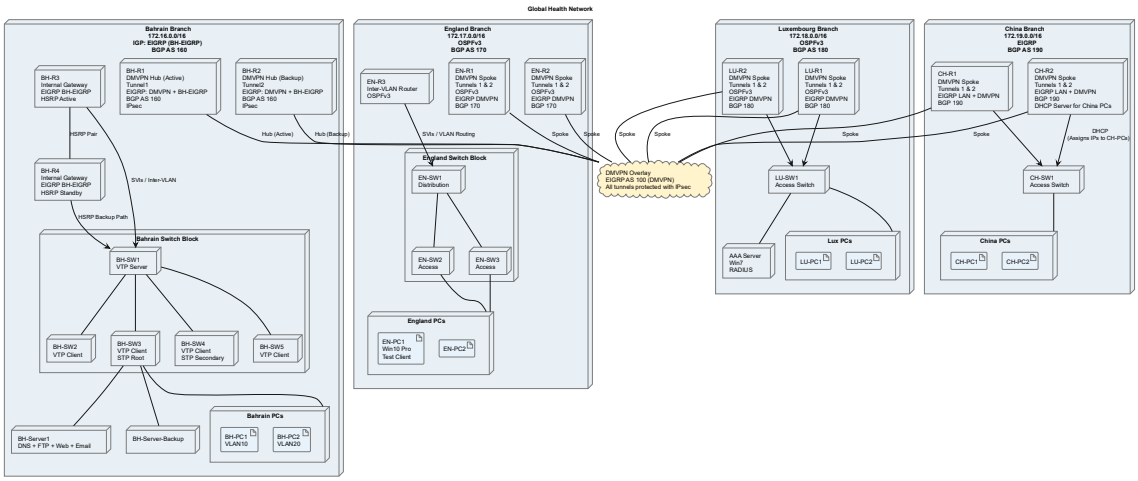

Figure 3 Deployment Diagram

The deployment diagram illustrates the complete physical and logical location of all networking components and services functioning within the Global Health Network. Along with the routing protocols and security measures operating between each component, it shows the actual routes of communication between routers, switches, servers, and the DMVPN/IPsec overlay.

Every GHN site in Bahrain, England, Luxembourg, and China is constructed using a standard architecture pattern that is reflected in the updated diagram: an access layer that offers direct endpoint connectivity, a distribution layer that manages inter-VLAN routing and summarization, and a core routing layer that handles WAN connectivity. The routers depicted in the diagram end the WAN interfaces, DMVPN tunnel interfaces, IPsec profiles, and local VLAN sub interfaces. All traffic is forwarded to the local distribution router by the access switches, which also enforce Layer 2 security.

The dual-hub DMVPN Phase-3 architecture implemented in Bahrain is highlighted in the diagram. Both Tunnel 1 and Tunnel 2 originate from Bahrain's main routers, forming redundant encrypted overlays. China, Luxembourg, and England are all isolated locations that join the overlays as spokes. IPsec-protected mGRE tunnels over the ISP backbone are made possible by this design, and dynamic spoke-to-spoke communication is made possible using NHRP shortcuts. The diagram clearly depicts how all inter site traffic is safeguarded and how Phase 3 optimization minimizes latency for HD video conferencing and data transfers.

Routing protocols are mapped exactly as deployed. Bahrain and China operate EIGRP, England employs OSPFv2, and Luxembourg operates OSPFv3. As indicated, these IGPs only operate within their local locales. At each WAN edge, the core routers establish eBGP sessions with the ISP AS1000, enabling regulated route exchange between GHN's AS160, AS170, AS180, and AS190. The deployment diagram shows the implementation of inter-AS policy routing, next hop reachability, and BGP adjacency between sites.

The diagram additionally highlights where important services are located. Bahrain hosts the DNS, web IIS, FTP, email server, and DHCP services, installed on their own server VLANs. The core AAA/RADIUS server, which is utilized for device authentication on all routers, is located in Luxembourg. The traffic flow between servers and branch devices traveling through the local interfaces, routed via branch IGPs, then encrypted across the DMVPN overlay is precisely displayed.

Each component in the diagram corresponds to deployed configuration pieces, including:

- Routers provide eBGP peering, IPsec profiles, DMVPN tunnel interfaces, IGP adjacencies, and inter-VLAN routing.

- Switches: port security enforcement, STP protection, trunk connectivity, and VLAN segmentation.

- Servers: DNS zones, IIS hosting, FTP settings, hMail SMTP/IMAP, DHCP scopes, AAA policies.

Overall, the deployment diagram provides an accurate, complete picture of how GHN's WAN, LAN, DMVPN overlays, server services, and security measures work together to build a secure, encrypted, resilient transnational healthcare network.

UML Diagrams

Introduction

This section illustrates the UML diagrams designed for the Global Health Network solution. System behaviour, user interaction, and the structural connections among all network components are all visualized using UML. The Use Case Diagram, which shows how various stakeholders interact with the system and the services offered throughout the network, and the Architecture Diagrams, which illustrate the structural arrangement of routers, tunnels, and protocols within the GHN infrastructure, are the two main viewpoints that are highlighted in the diagrams in this section. When combined, these diagrams offer a clear picture of the system's internal design as well as how it is used.

Use Case Diagram

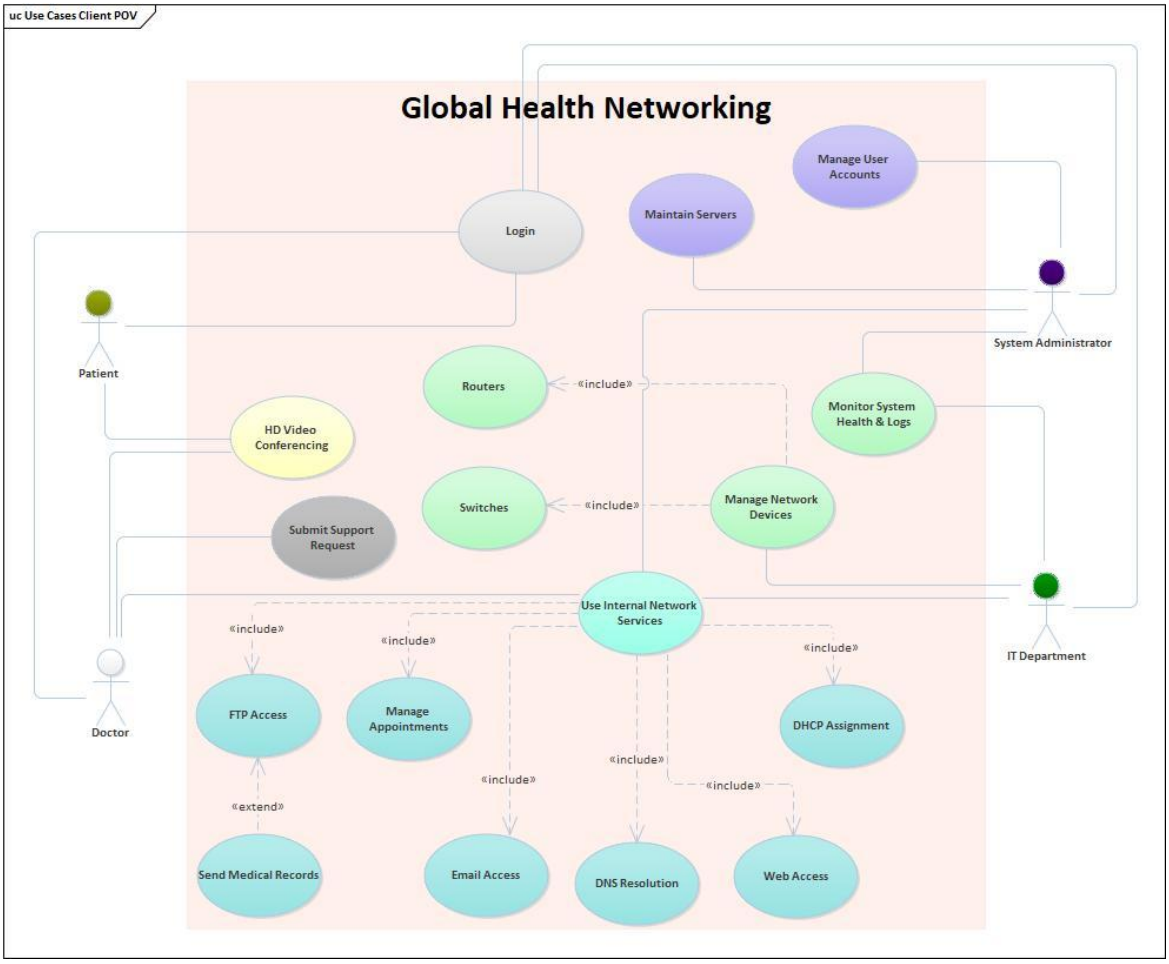

Figure 4 Use Case Diagram

The use case diagram illustrates the way different actors engage with the GHN system, and the services offered by all branches. It recognizes four major actors: Patients, Doctors, System Administrators, and the IT Department. Each actor interacts with the system through different responsibilities that support medical services, network operations, and administrative activities.

Patients communicate mostly through user facing services such as HD Video Conferencing and Login, reflecting GHN's focus on remote medical access. Doctors have expanded access, including FTP services, Email, Web Access, and the ability to Send Medical Records, which is an extension of the FTP Access use case.

System Administrators are responsible for backend administration tasks such as Maintaining Servers, Managing User Accounts, Monitoring System Health & Logs, and Managing Network Devices. By managing devices, assigning DHCP addresses, and monitoring internal service utilization, the IT department ensures the network's continuous operation.

At the heart of the diagram is Use Internal Network Services, which links every technical task like DNS Resolution, Email Access, Web Access, Appointments Management, and DHCP. These services are presented as part of the broader operational ecosystem, highlighting how GHN staff and users depend on basic infrastructure services for daily operations.

In the end, the Use Case Diagram gives a high level overview of the system's functional behavior, illustrating clearly how medical users and technical staff interact with GHN's internal services and network components.

Architecture Diagram

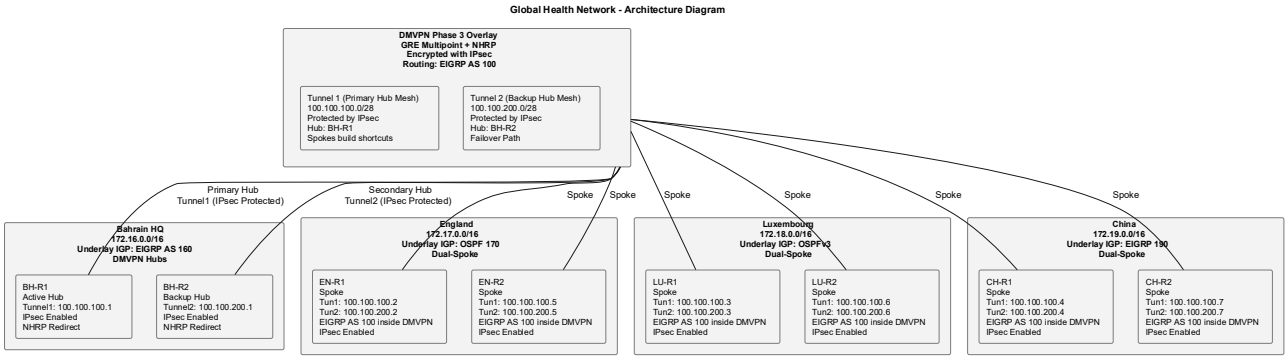

Figure 5 Architecture Diagram

The GHN's hierarchical layout and the interactions between all of its primary components throughout the global infrastructure are depicted in the Architecture Diagram. It depicts the layered organization of routers, switches, and DMVPN across IPsec tunnels, illustrating the protocols responsible for routing, encryption, and service delivery between Bahrain, England, Luxembourg, and China.

The Core, Distribution, and Access layers are distinctly separated for each site. DMVPN tunnels are terminated by the core routers, which are connected to the ISP backbone. Distribution routers manage internal traffic control, summarization, and inter-VLAN routing. Access switches give connectivity to users, servers, and management endpoints through their associated VLANs.

The dual hub DMVPN system implemented in Bahrain, where two DMVPN domains, Tunnel 1 and Tunnel 2, offer redundancy and dynamic spoke-to-spoke communication for China, England, and Luxembourg, is shown as well in the architecture diagram. GRE encapsulation, NHRP shortcuts, and IPsec encryption are all part of this architecture, ensuring safe and efficient inter-site communication.

Routing domains are clearly separated:

1. Bahrain and China run EIGRP
2. England runs OSPFv2
3. Luxembourg runs OSPFv3

whereas eBGP sessions with the ISP AS1000 handle all inter-site communication. This system keeps internal routing complexity from seeping outside of each site and guarantees uniform policy management.

The Architecture Diagram, which illustrates how routers, switches, tunnels, VLANs, and services cooperate to create a safe and highly available global healthcare network, offers a clear and thorough overview of GHN's structural design.

Implementation

By setting up the important routing, security, and service components needed for inter-site communication, the implementation phase concentrates on turning the GHN network architecture into a functional system. The setup of routers and switches on EVE-NG, the implementation of routing protocols, the creation of encrypted DMVPN tunnels, and the integration of essential Windows Server services such as DNS, DHCP, FTP, web, and internal email are all highlighted in this chapter.

To show how the network was constructed as well as how the various parts function together, just the most important configuration activities and system behaviours are outlined below. Appendix III Detailed Implementation contains comprehensive setup instructions, command outputs, and device setups.

Environment Setup

Simulation Environment

The full GHN topology was implemented in EVE-NG Community Edition, chosen due to its ability to emulate IOS routers, L2/L3 switches, and server VMs.

Resources allocated:

- 20 GB RAM
- 4 vCPUs
- 250 GB storage SSD
- Cisco IOS router and L2/L3 switch images
- Windows Server 2012R2, Windows 7 and Windows 10 images

This resource allocation was chosen because it balances performance with the need to run multiple routers, switches, and server VMs simultaneously.

Base Device Initialization

All routers and switches were configured with:

- Hostnames
- Interface IP addressing
- SSH access
- Domain name
- Password encryption
- Logging and timestamps
- Banner MOTD
- Routing protocol for the LAN (EIGRP /Name EIGRP/ OSPF / OSPFv3)
- Routing protocol for the WAN (MP-EBGP)

This gives a uniformly baseline for all GHN devices.

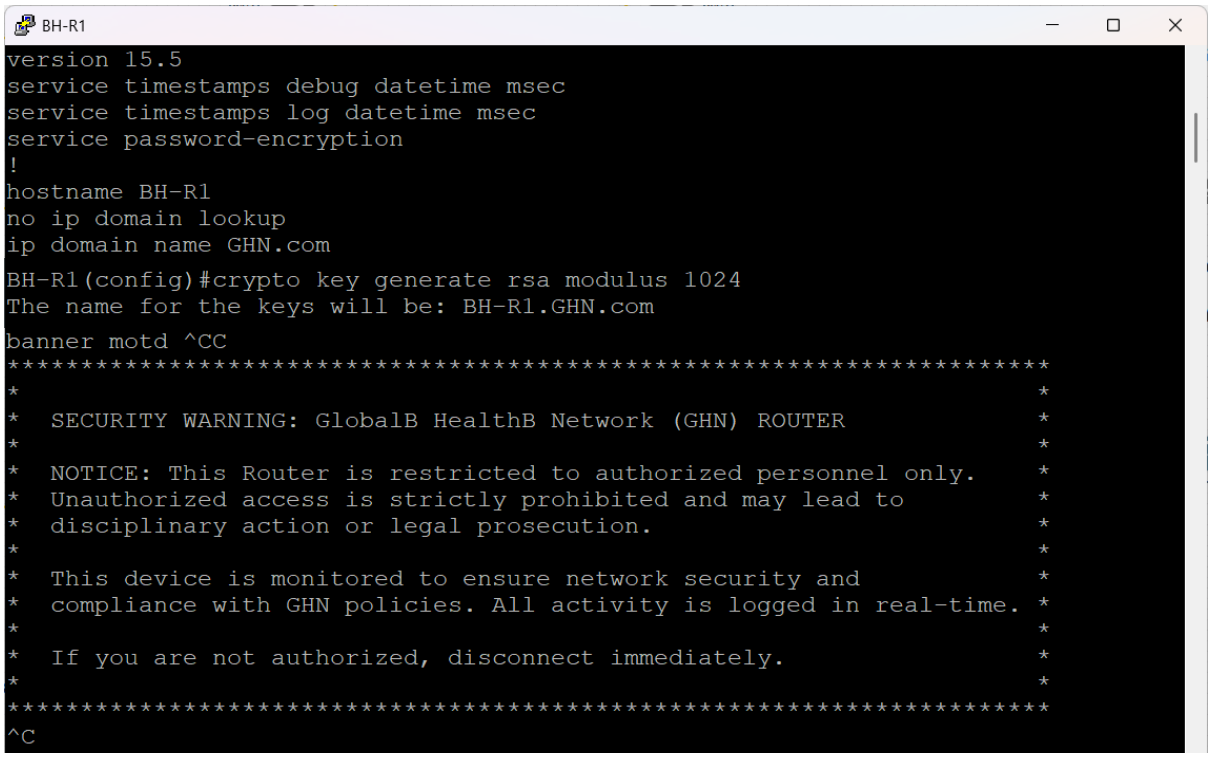

Figure 6 Base Device Configuration

The figure shows a sample of the Base Device Configuration on all GHN devices.

Core Routing Implementation

Each GHN site uses a dedicated IGP that fits its needs.

Bahrain – Named EIGRP (AS160)

Bahrain operates as a regional hub and DMVPN hub, requiring fast convergence and unequal load support.

Bahrain uses Named EIGRP to support scalability and flexible configuration

Implementation details:

- Activated “BH-EIGRP” under the address-family
- Advertised inter-router /30 links
- Advertised VLAN SVIs for local subnets
- Verified neighborship, IP route and topology

The figure below represents Bahrain branch

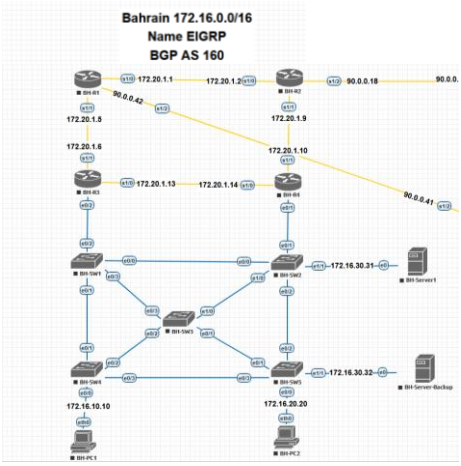

Figure 7 Bahrain Branch

```
key chain BHEIGRP
 key 16
  key-string 7 05090707334D470739001E15191C
  cryptographic-algorithm hmac-sha-256
```

Figure 8 EIGRP key-chain

EIGRP Key-chain configuration

The figure shows the EIGRP authentication key-chain bahrain@eigrp configured on BH-R1. This key-chain defines the cryptographic parameters used by EIGRP to authenticate routing updates, preventing unauthorized devices from injecting routes into the BH routing domain.

EIGRP Named-mode Configuration

The figures below show the EIGRP named-mode configuration on BH-R1,BH-R2, BH-R3, BH-R4 for the internal AS 160. The router uses the BH-EIGRP process to manage all routing inside the Bahrain branch. Named-mode gives clean hierarchy: global settings, address-family settings, and per-interface settings.

At the top, the default AF-interface applies HMAC-SHA-256 authentication with key-chain BHEIGRP to all EIGRP-enabled interfaces unless explicitly overridden. This is the control-plane security mechanism that protects routing updates from tampering or unauthorized routers.

The router-ID is manually set to 1.1.16.1 for BH-R1, 1.1.16.2 for BH-R2, 1.1.16.3 for BH-R3, and 1.1.16.4 for BH-R4 providing deterministic neighbor selection, stable EIGRP operations, and consistent logs.

This configuration shows a clean, segmented EIGRP deployment: authenticated internal links, controlled exceptions, explicit network advertisements, and proper hierarchical design under the named-mode structure.

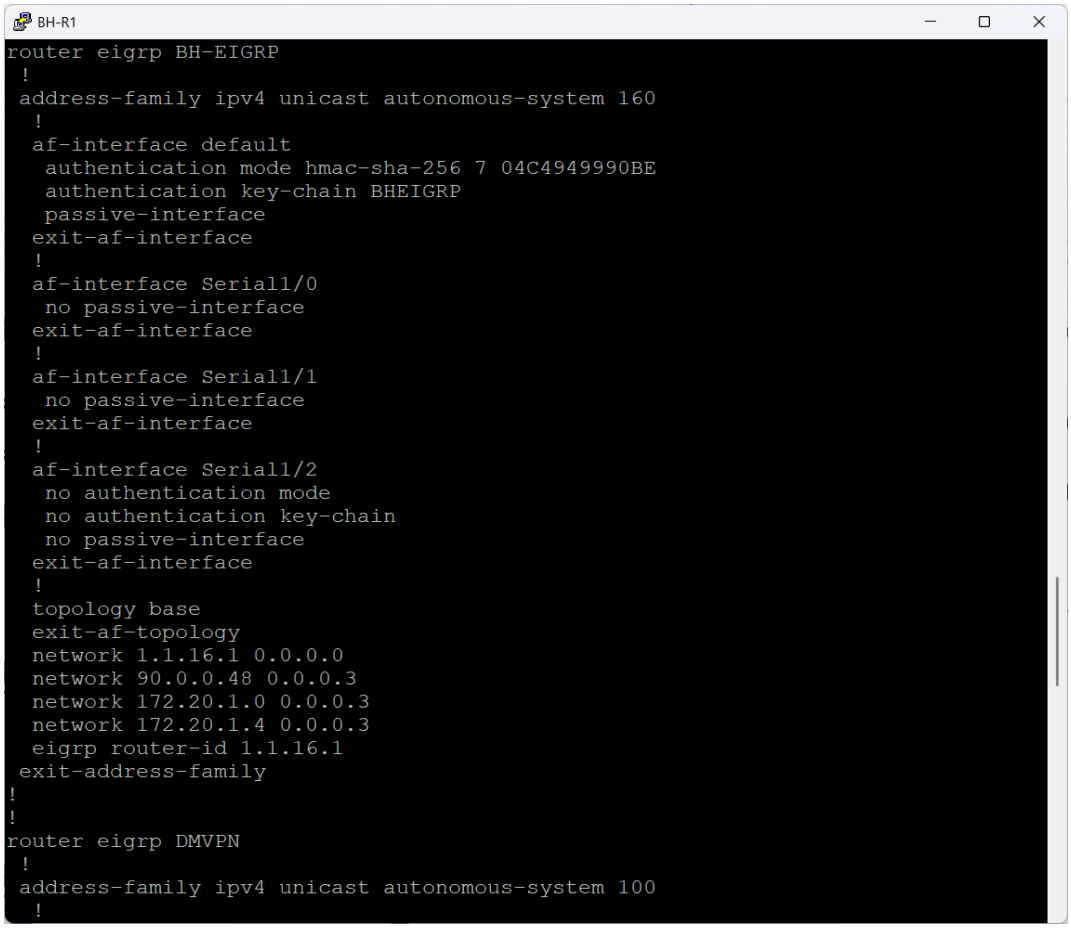

Figure 9 BH-R1 EIGRP Implementation

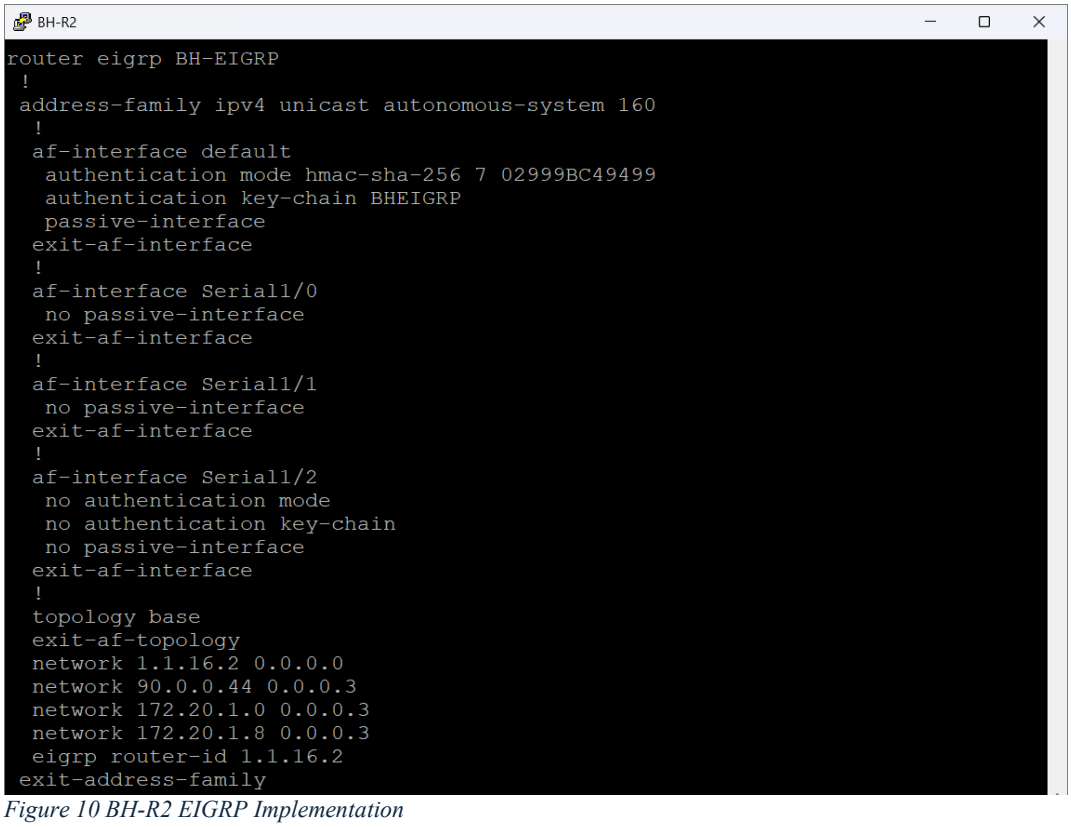

Figure 10 BH-R2 EIGRP Implementation

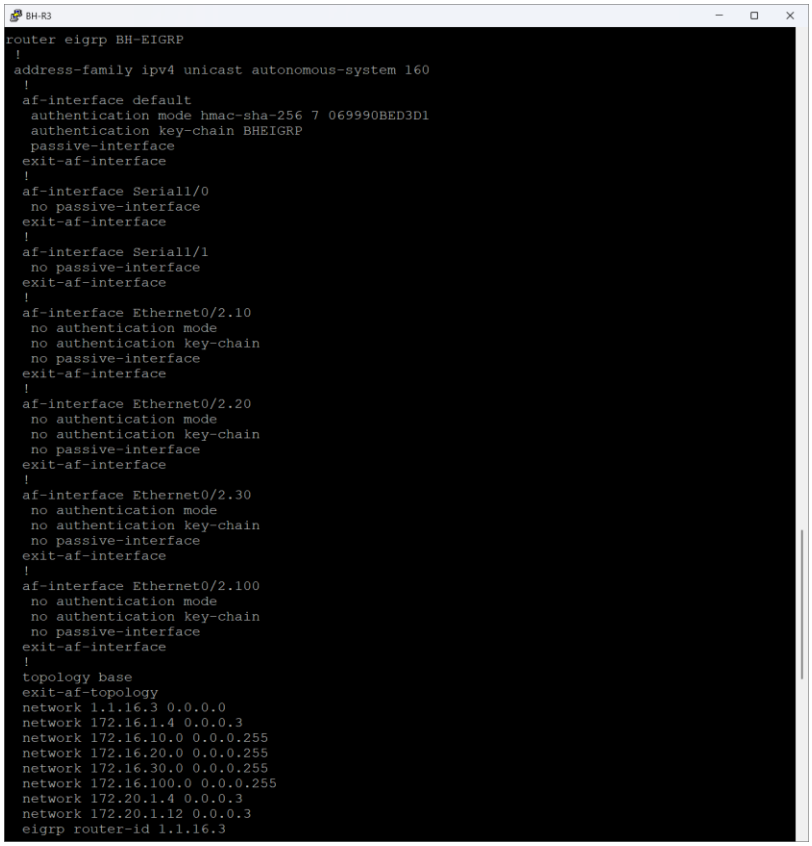

Figure 11 BH-R3 EIGRP Implementation

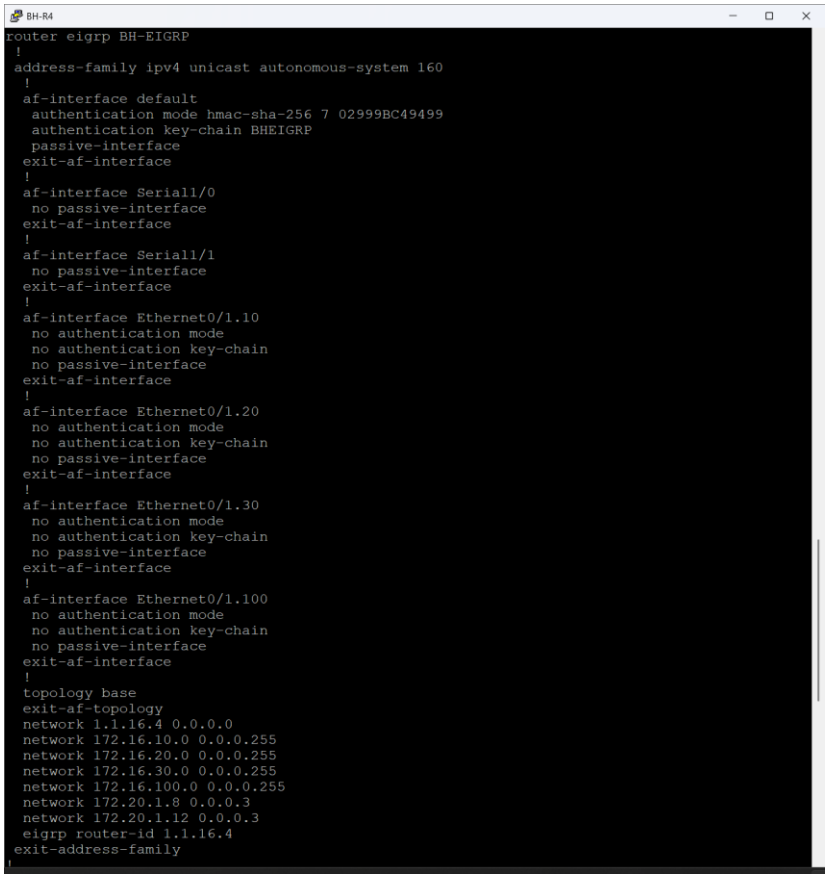

Figure 12 BH-R4 EIGRP Implementation

EIGRP adjacencies

The figures below show the EIGRP adjacencies and routing tables across BH-R1, BH-R2, and BH-R4 within the Bahrain domain AS 160. These outputs confirm that the internal routing plane is fully operational, stable, and synchronized across all core routers.

Across BH-R1 and BH-R2, each router forms two EIGRP adjacencies via the Serial links, demonstrating correct interface configuration, matching AS numbers, and matching authentication parameters. The SRTT and RTO values remain low and stable, which indicates a healthy control-plane with no retransmission problems. The uptime counters show that the neighbors have been stable since convergence.

Each route is marked D, confirming it is an internal EIGRP route with an administrative distance of 90. Metrics differ slightly between BH-R1 and BH-R2 depending on their interface bandwidths and SRTT values, but both routers correctly calculate equal-cost paths when appropriate.

The BH-R4 output confirms the same behaviour, but from the perspective of the core switch/router. BH-R4 forms multiple EIGRP adjacencies over Ethernet links, validating that the Layer-3 switching core is participating fully in the routing domain. Its routing table matches the learned prefixes seen on BH-R1 and BH-R2, which proves that the internal BH routing fabric is converged and consistent end to end.

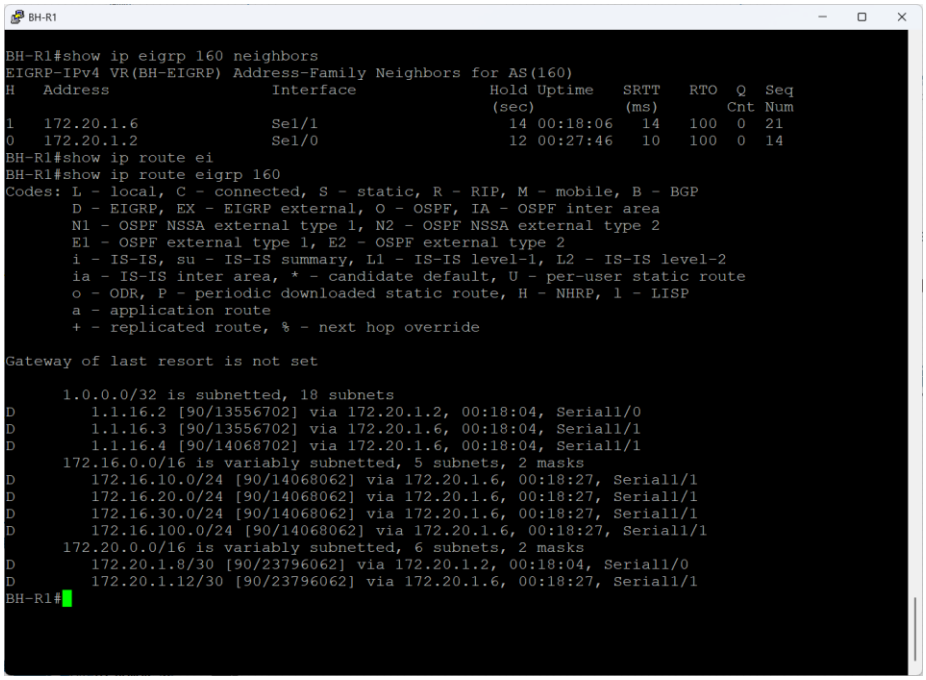

Figure 13 BH-R1 EIGRP Neighbor

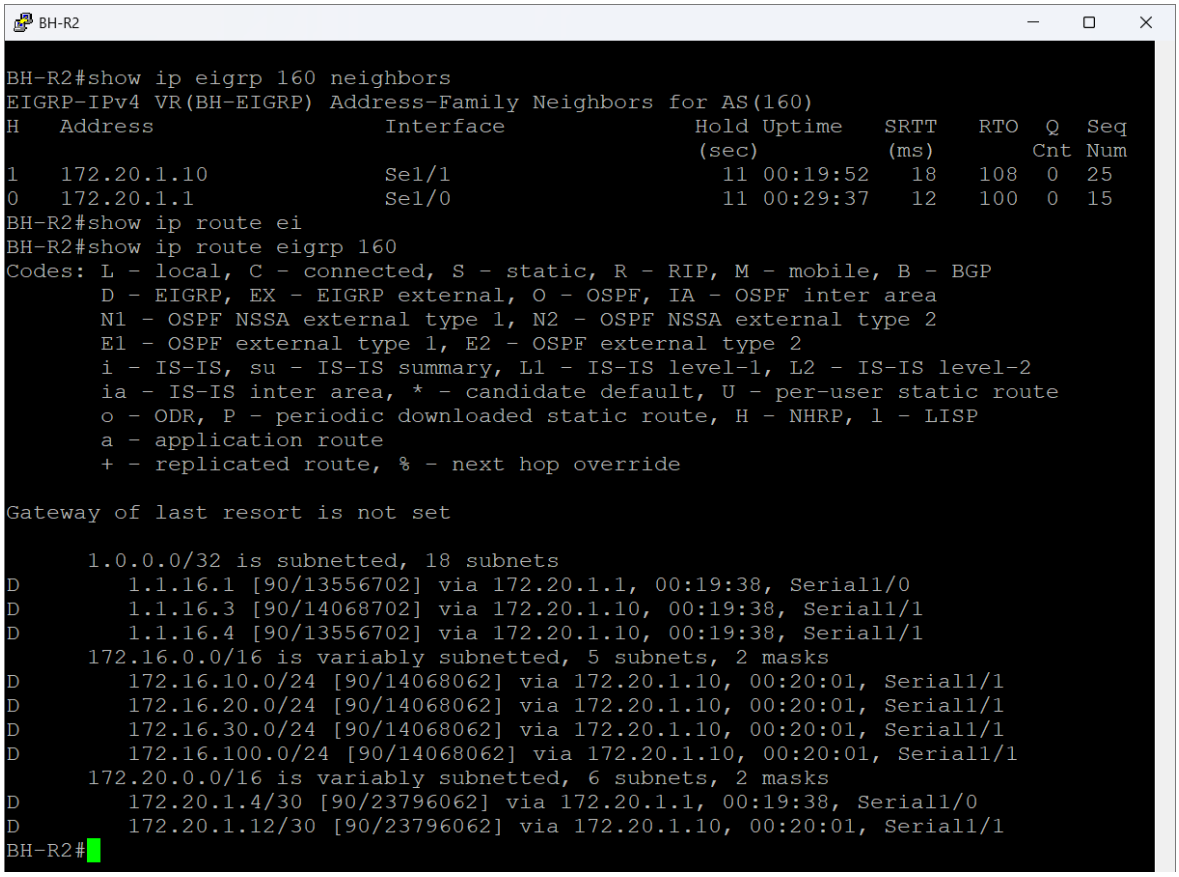

Figure 14 BH-R2 EIGRP Neighbor

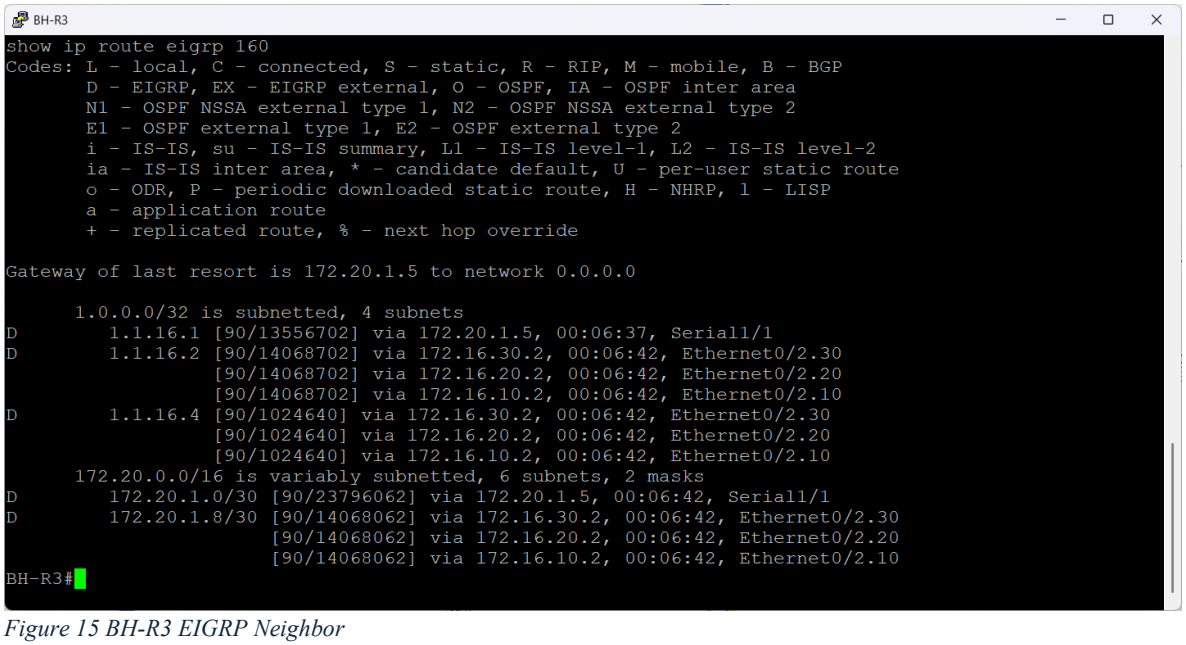

Figure 15 BH-R3 EIGRP Neighbor

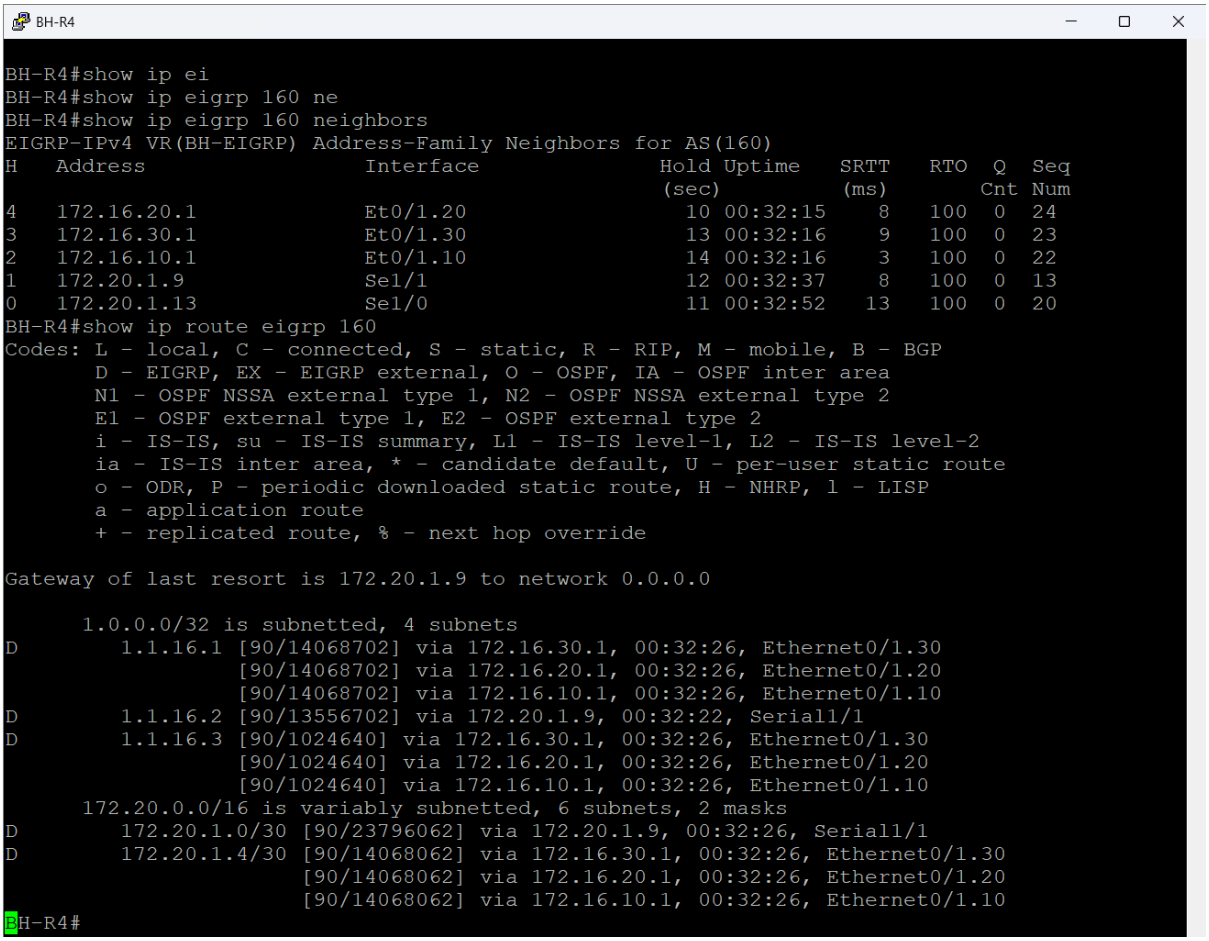

Figure 16 BH-R4 EIGRP Neighbor

EIGRP Neighbors

The figures below show the EIGRP neighbor adjacency tables across all Bahrain routers participating in AS 160. These outputs confirm that every router in the BH routing domain has successfully discovered and established adjacencies with its directly connected peers.

BH-R1 forms two adjacencies over Serial1/1 and Serial1/0 toward the BH core. Both neighbors show stable uptime and low SRTT values, proving that authentication, timers, and interface configurations are correct.

BH-R2 mirrors the same behaviour. It forms adjacencies with BH-R1 over the same WAN links in the opposite direction. Metrics match the topology layout and confirm consistent EIGRP named-mode behaviour between the two routers.

BH-R3 shows a larger neighbor table because it connects the BH distribution/core layer. It forms EIGRP adjacencies over both Ethernet segments VLAN L3 interfaces and Serial links. This confirms that routing is active across all BH internal segments.

BH-R4, acting as the core switch/router, forms five adjacencies: three over internal Layer-3 Ethernet interfaces and two over Serial interfaces. Even though the Ethernet links naturally have higher SRTT due to bandwidth and interface type, the adjacencies remain stable, with zero drops and synchronized sequence numbers.

Together, these tables prove that the BH EIGRP domain is fully converged, stable, and aligned with the designed network topology. Each router has full visibility of its immediate neighbors, forming the foundation for correct routing propagation throughout the Bahrain area.

BH-R1

```
BH-R1#show ip eigrp 160 neighbors
EIGRP-IPv4 VR(BH-EIGRP) Address-Family Neighbors for AS(160)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   172.20.1.6              Se1/1                    10 00:05:09   15   100  0  25
0   172.20.1.2              Se1/0                    14 00:11:05   13   100  0  14
BH-R1#
```

Figure 17 BH-R1 EIGRP Neighbor

BH-R2

```
show ip eigrp 160 neighbors
EIGRP-IPv4 VR(BH-EIGRP) Address-Family Neighbors for AS(160)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   172.20.1.10             Se1/1                    10 00:05:54   16   100  0  20
0   172.20.1.1              Se1/0                    14 00:11:50   10   100  0  15
BH-R2#
```

Figure 18 BH-R2 EIGRP Neighbor

BH-R3

```
BH-R3#show ip eigrp 160 neighbors
EIGRP-IPv4 VR(BH-EIGRP) Address-Family Neighbors for AS(160)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
4   172.16.20.2             Et0/2.20                 10 00:06:06    9   100  0  23
3   172.16.10.2             Et0/2.10                 13 00:06:06    7   100  0  22
2   172.16.30.2             Et0/2.30                 14 00:06:06    9   100  0  21
1   172.20.1.5              Se1/1                    14 00:06:26   15   100  0  14
0   172.20.1.14             Se1/0                    12 00:06:35   15   100  0  19
BH-R3#
```

Figure 19 BH-R3 EIGRP Neighbor

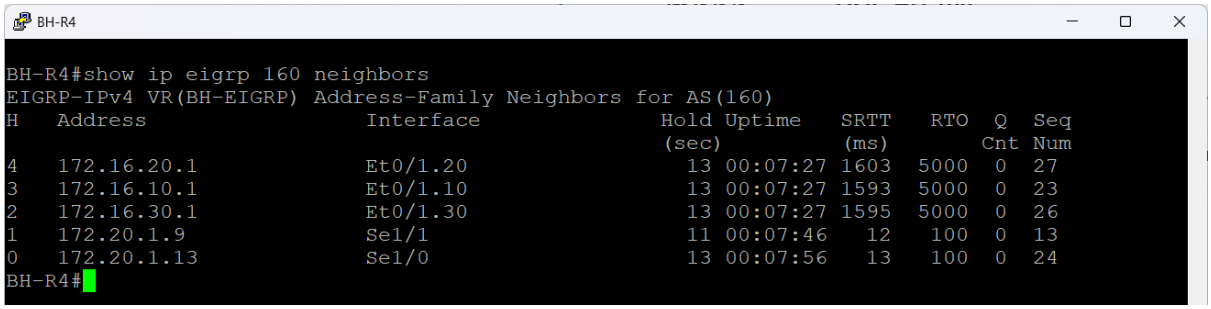

Figure 20 BH-R4 EIGRP Neighbor

EIGRP Topology Table

These figures below show the EIGRP topology tables for BH-R1 and BH-R3. The topology table contains all routes learned by EIGRP including feasible successors and reflects the router's full understanding of the network before the best routes are selected for the routing table.

Across both routers, all entries appear in Passive (P) state. This is critical: Passive means the routes are stable and fully converged. There are no Active (A) routes, which confirms no ongoing recalculation, no flapping neighbors, and no missing paths.

Each prefix shows:

1. Feasible Distance (FD): the overall cost of the best path.

2. Successors: the next-hop chosen as the best path.

3. Feasible Successors if present: backup loop-free paths that allow instant failover.

Multiple paths per network: BH-R3 and BH-R1 receive routes from both Serial and Ethernet interfaces, demonstrating proper multipath learning and visibility across the entire BH domain.

On BH-R3, routes such as 172.20.1.8/30, 172.16.20.0/24, and 1.1.16.x show multiple successors and multiple feasible successors, confirming that the router has full redundancy

across all internal segments. BH-R1 mirrors the same behaviour, receiving consistent metrics and successors from BH-R2 and BH-R3.

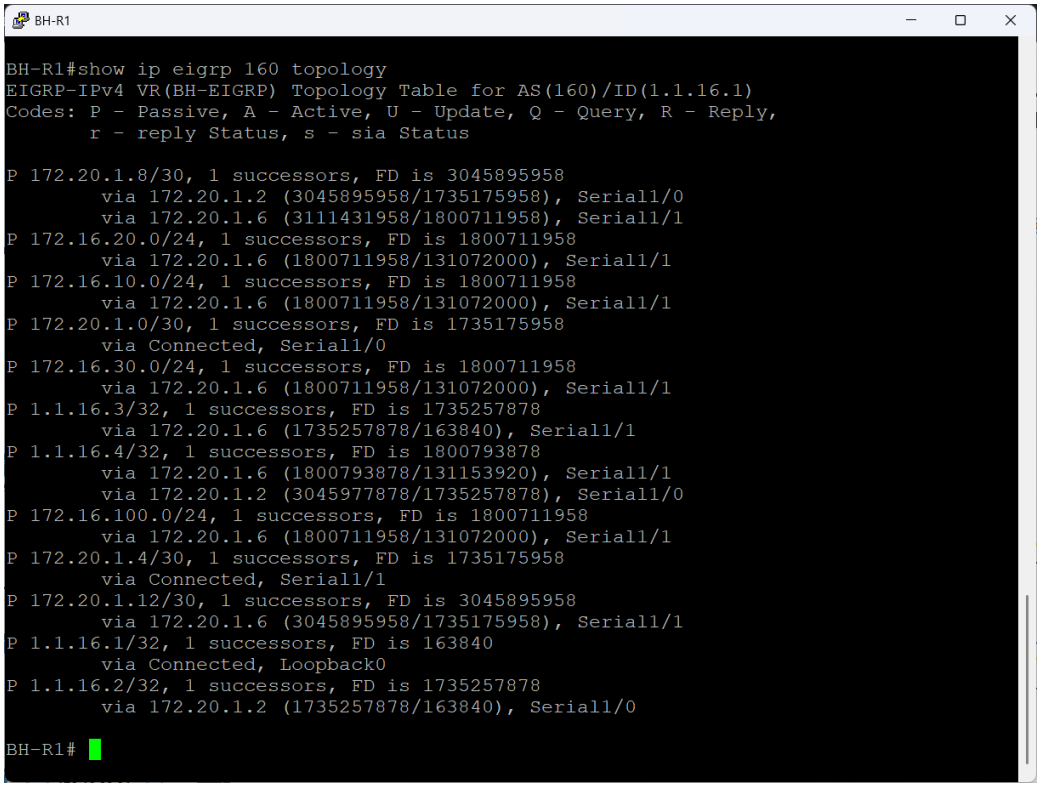

Figure 21 BH-R1 EIGRP Topology Table

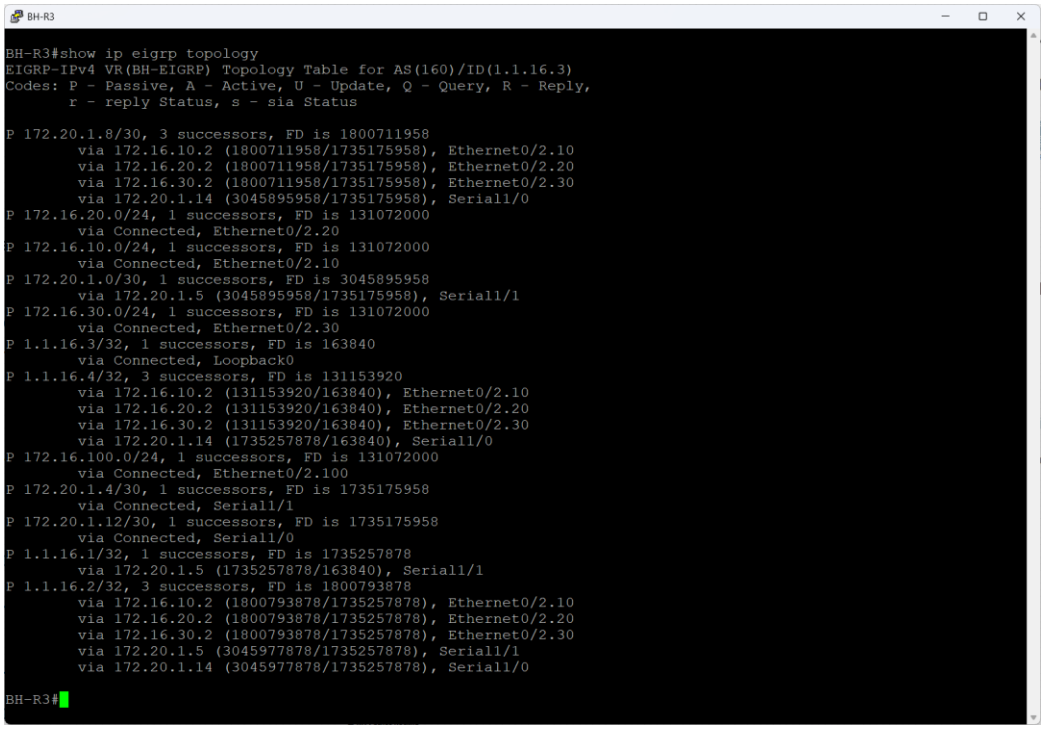

Figure 22 BH-R3 EIGRP Topology Table

England – OSPFv2 (AS170)

England operates IPv4-only, making OSPFv2 appropriate.

Implementation details:

- Interfaces placed into Area 0
- Loopback used as Router-ID
- Passive interfaces applied to LAN ports

The figure below shows England branch

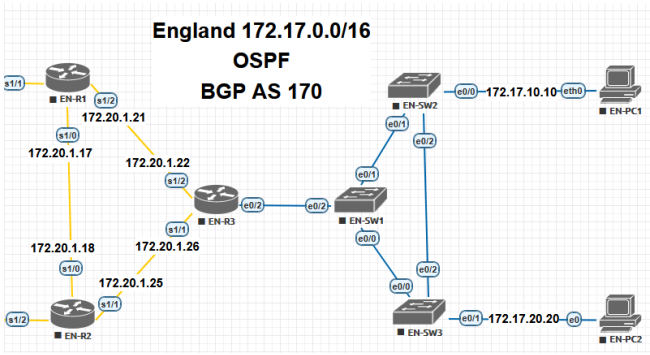

Figure 23 England Branch

OSPF Authentication and Routing Configuration

The figures below show the OSPF authentication and routing configuration for the England site, operating under OSPF process 170.

A key-chain named englandOSPF is defined using HMAC-SHA-256, which provides cryptographic integrity for all OSPF hello packets and LSAs across the internal EN domain. This prevents unauthorized routers from forming adjacencies or injecting routes.

Each England router EN-R1, EN-R2, EN-R3 is configured with:

- A manually defined router-ID from the 1.1.17.x block for deterministic adjacency formation.
- passive-interface default for security and control-plane reduction, ensuring only specific interfaces participate in OSPF.
- Selective no passive-interface commands on the Serial links and Loopback0 so neighbor formation occurs only where needed.
- Network statements matching the England LAN blocks and point to point links, all placed inside Area 0, creating a simple and stable single-area design.

EN-R1 injects a default route into the England OSPF domain using

default-information originate always

which ensures internal routers maintain reachability to external destinations using DMVPN tunnel.

EN-R2 advertises the same core subnets as EN-R1 but uses different Serial interfaces reflecting it is topology position. Its configuration mirrors R1's structure to maintain consistency and predictable OSPF behaviour.

EN-R3 introduces additional internal LAN segments 172.17.10.0/24, 172.17.20.0/24, 172.17.30.0/24 and advertises these directly into Area 0. This shows R3's role as a distribution router for the England LANs.

Across all routers, the consistent use of SHA-256 authentication, router-ID structure, and passive-interface discipline confirms a clean OSPF deployment with predictable adjacencies and minimal control-plane exposure.

```
key chain englandOSPF
 key 17
  key-string 7 0301550C0A0E2F486E060A1511
  cryptographic-algorithm hmac-sha-256
```

Figure 24 England OSPF key-chain

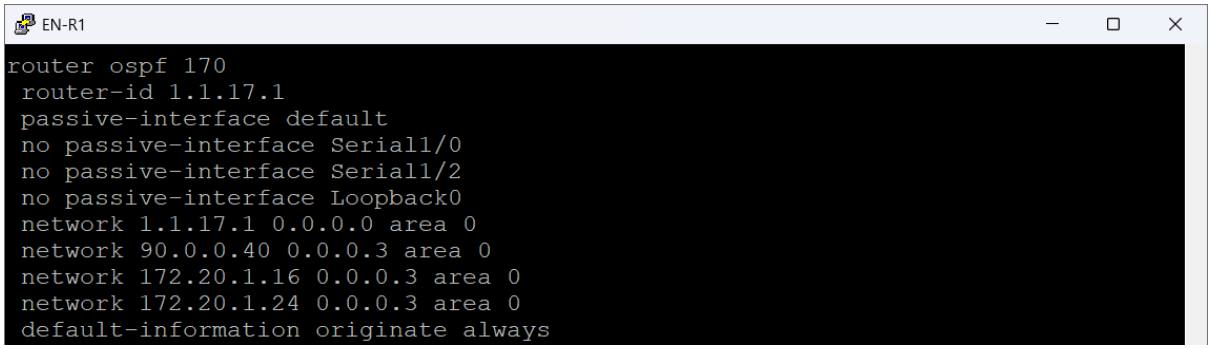

Figure 25 EN-R1 England OSPF Configuration

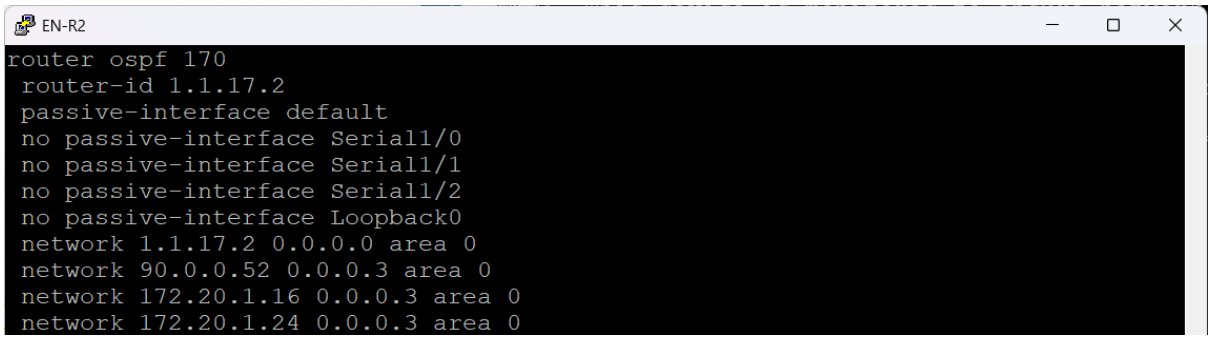

Figure 26 EN-R3 England OSPF Configuration

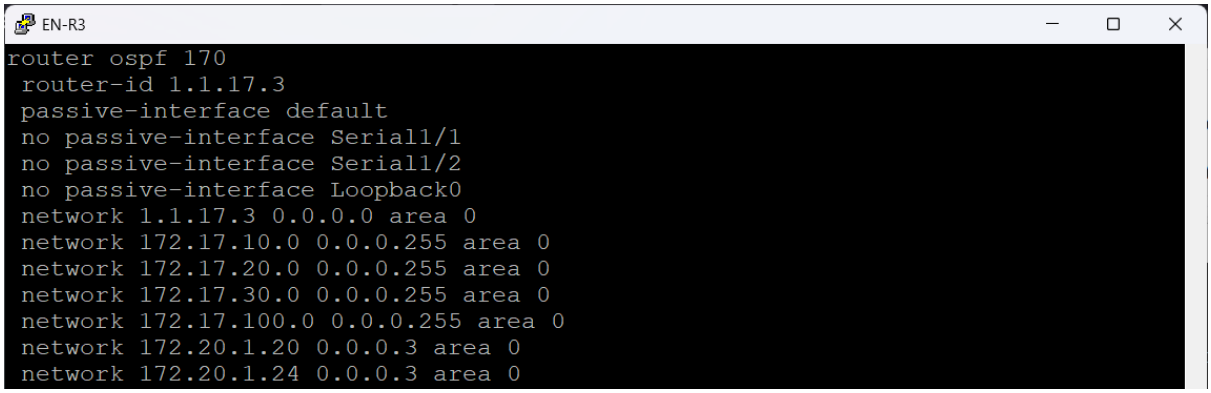

Figure 27 EN-R3 England OSPF Configuration

OSPF Neighbor Adjacencies Verification

These figures below show the OSPF neighbor adjacencies for the England site OSPF process 170. All three routers EN-R1, EN-R2, and EN-R3 form FULL adjacencies with their directly connected peers, confirming that OSPF is operating exactly as designed.

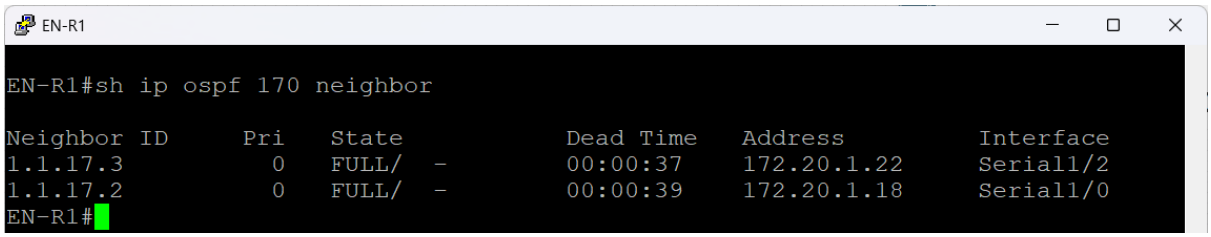

Figure 28 EN-R1 OSPF neighbor adjacencies

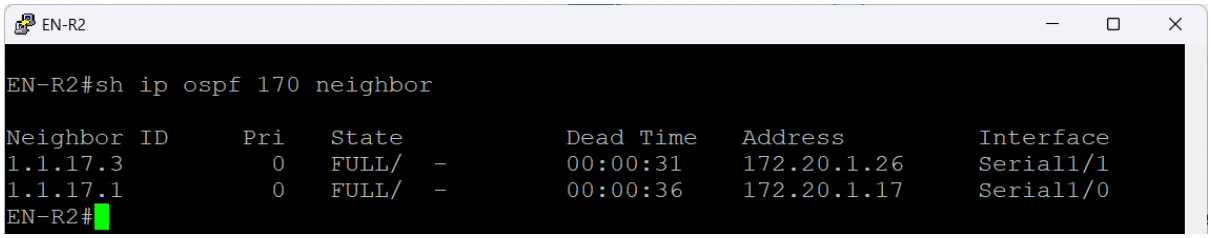

Figure 29 EN-R2 OSPF neighbor adjacencies

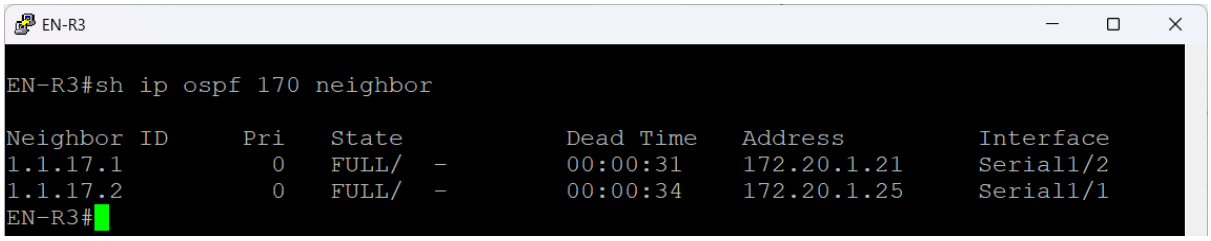

Figure 30 EN-R3 OSPF neighbor adjacencies

OSPF Routing Table Verification

These figures show the OSPF routing tables for all routers in the England site running OSPF process 170. The presence of O-routes across all three devices confirms that each router successfully learned internal England networks from its neighbors, and the OSPF area is fully converged.

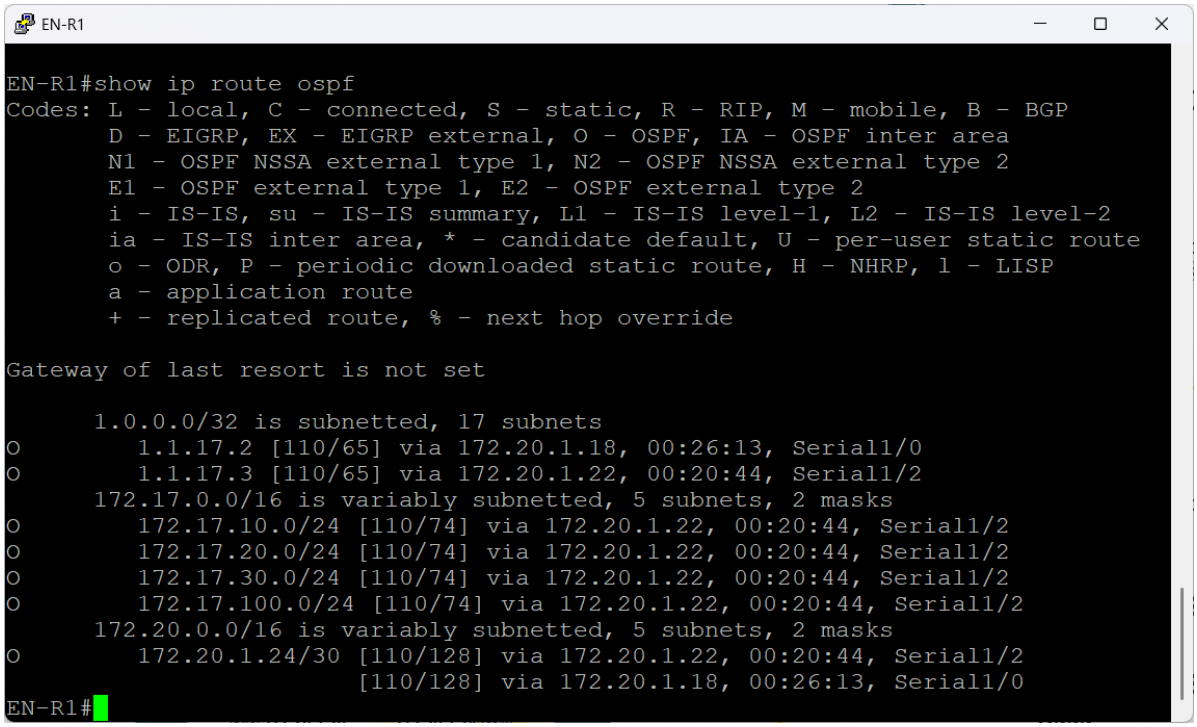

Figure 31 EN-R1 OSPF Routing Table Verification

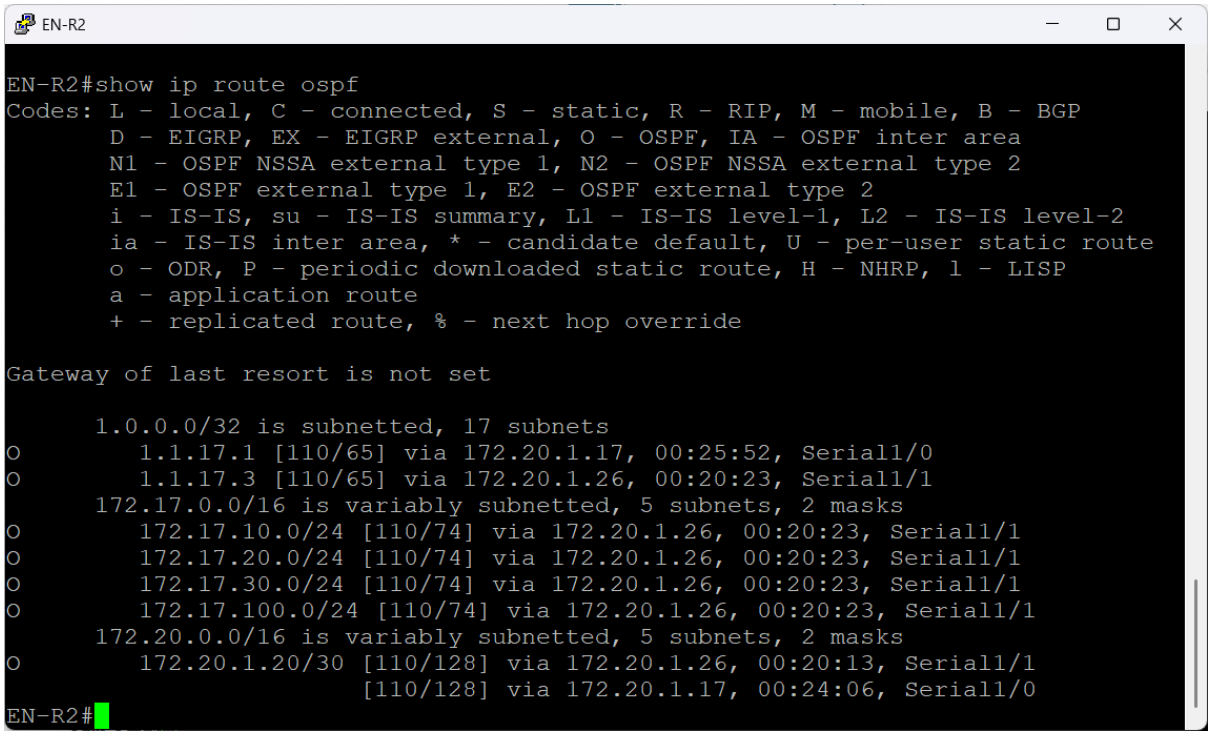

Figure 32 EN-R2 OSPF Routing Table Verification

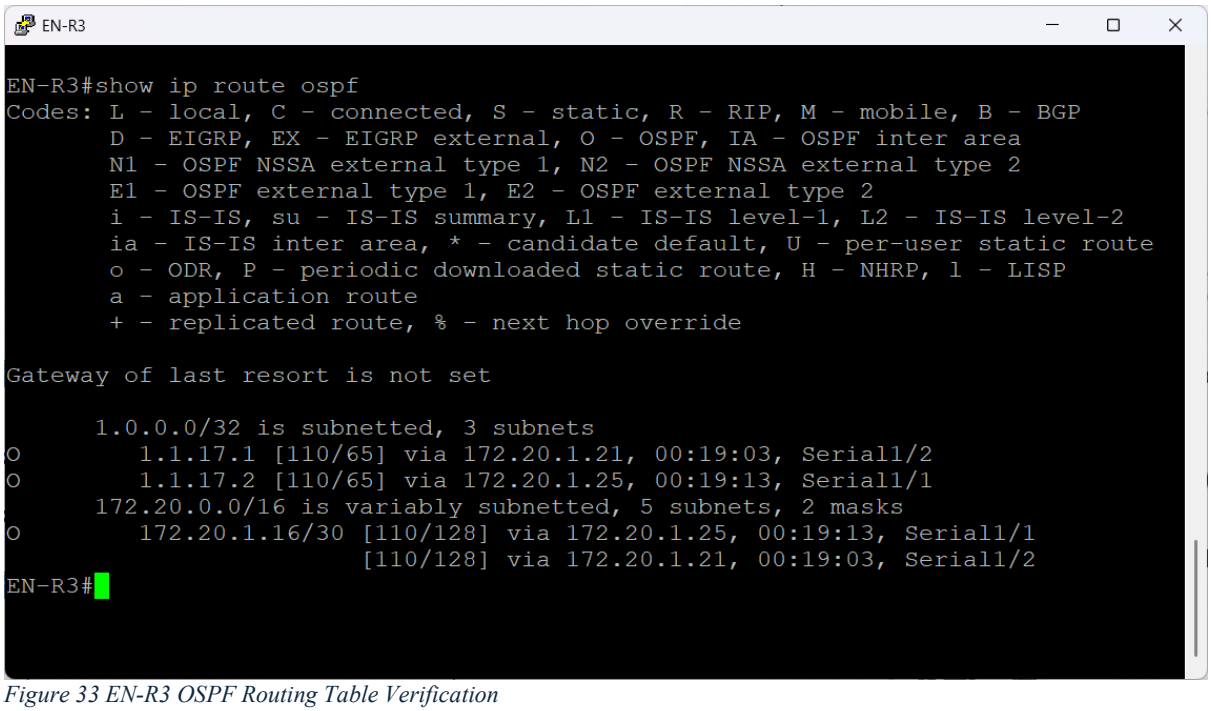

Figure 33 EN-R3 OSPF Routing Table Verification

Luxembourg – OSPFv3 (AS180)

Luxembourg uses OSPFv3 for IPv6-readiness and AAA centralization.

Implementation details:

- Configured OSPFv3 address families
- Advertised server and LAN networks
- Loopback used as Router-ID

The figure below shows Luxembourg branch topology

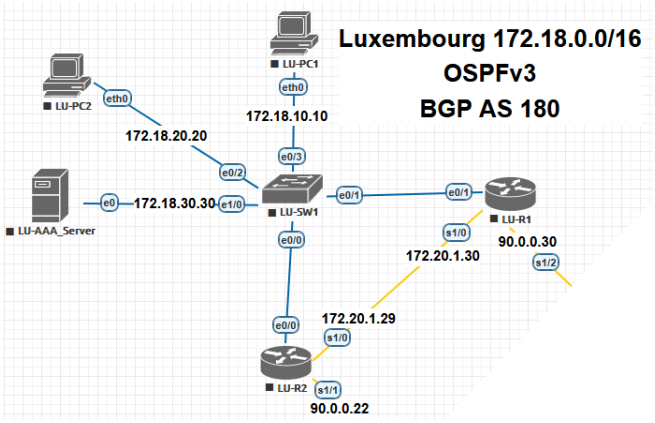

Figure 34 Luxembourg Branch

OSPFv3 Configuration

The below figures show the OSPFv3 configuration for the Luxembourg site, operating under OSPFv3 process 180. Even though OSPFv3 is traditionally used for IPv6, Cisco supports address family IPv4 under OSPFv3, which allows the design to stay consistent while using modern OSPFv3 authentication and packet formats.

Both routers LU-R1 and LU-R2 use:

I. A manually defined router-ID in the 1.1.18.x range for predictable neighbor relationships.

II. passive-interface default to shut down OSPF on every interface except those explicitly allowed.

III. Selective no passive-interface on their Serial interfaces and Loopbacks.

IV. Per-interface OSPFv3 configuration rather than network statements, which is the correct method for OSPFv3.

V. SHA-256 authentication via the key-chain luxembourgOSPFv3, ensuring all OSPF adjacencies and LSAs are cryptographically protected.

This establishes a stable, modern routing domain for the Luxembourg site, aligned with the design approach used across the GHN project.

```
key chain luxembourgOSPFv3
 key 18
  key-string 7 04571E1E0A2C4E411C0B02371D181C023C78
  cryptographic-algorithm hmac-sha-256
```

Figure 35 OSPFv3 key-chain

LU-R1

```
!
interface Loopback0
 ip address 1.1.18.1 255.255.255.255
 ipv6 enable
 ospfv3 180 ipv4 area 0
!
interface Serial1/0
 ip address 172.20.1.30 255.255.255.252
 ipv6 enable
 ospfv3 180 ipv4 area 0
 ospfv3 180 ipv4 authentication key-chain luxembourgOSPFv3
 serial restart-delay 0
router ospfv3 180
 !
 address-family ipv4 unicast
  passive-interface default
  no passive-interface Serial1/0
  no passive-interface Loopback0
  router-id 1.1.18.1
 exit-address-family
```

Figure 36 LU-R1 OSPFv3 Configuration

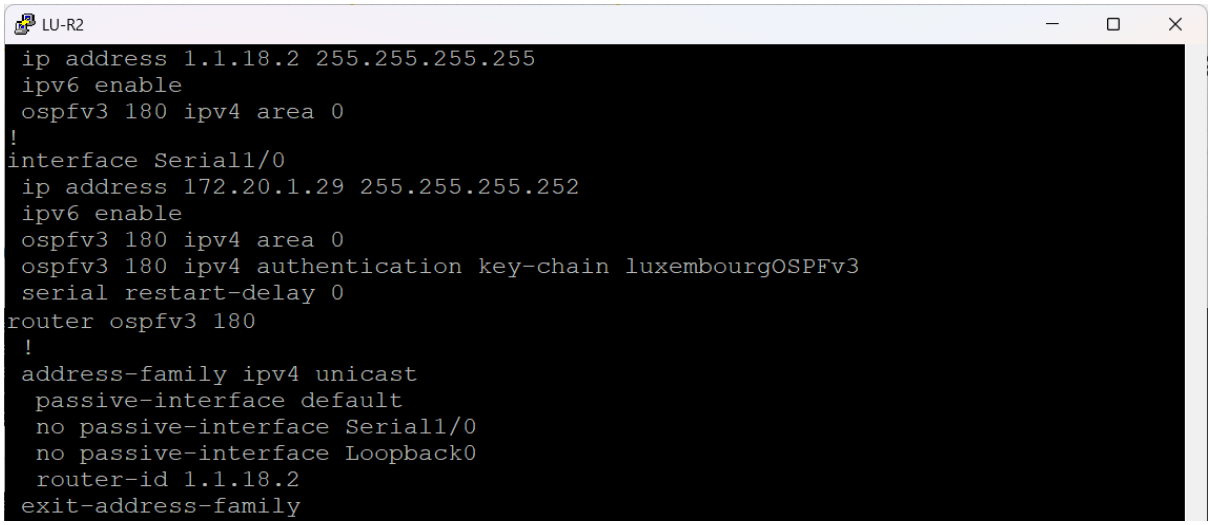

Figure 37 LU-R2 OSPFv3 Configuration

OSPFv3 Neighbor

These figures below show the OSPFv3 neighbor adjacency for the Luxembourg routers operating under OSPFv3 process 180 IPv4 address-family. Both LU-R1 and LU-R2 form a FULL adjacency over their Serial1/0 link, confirming that the OSPFv3 configuration is correct and stable.

- LU-R1 recognizes LU-R2 as neighbor 1.1.18.2 on interface Serial1/0.
- LU-R2 recognizes LU-R1 as neighbor 1.1.18.1 on the same interface.

The FULL/ state is the highest adjacency state in OSPF, indicating that the routers have:

- Exchanged and synchronized LSDBs (link-state databases).
- Completed the DBD (Database Description) exchange.
- Matching authentication settings (HMAC-SHA-256 via the key-chain).
- Matching interface parameters (hello/dead timers, MTU, network type).

- The dead-timer countdown shows normal behaviour and confirms active hello communication.

This verifies that the Luxembourg OSPFv3 domain is functioning correctly, the link between both routers is stable, and all IPv4 routes under the OSPFv3 AF will be properly exchanged.

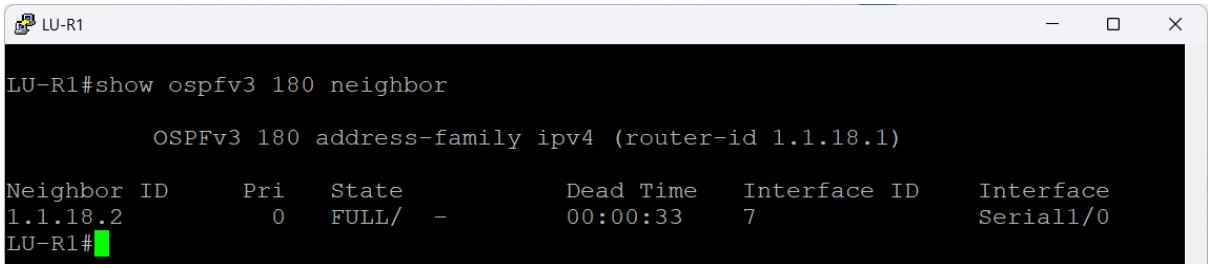

Figure 38 LU-R1 OSPFv3 Neighbor Verification

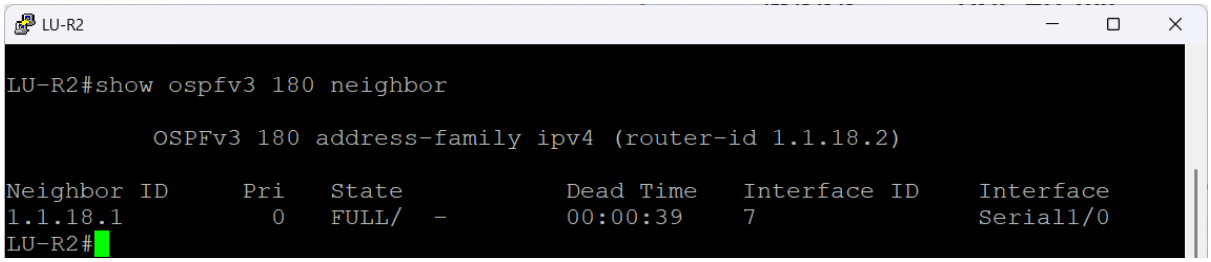

Figure 39 LU-R2 OSPFv3 Neighbor Verification

OSPFv3 Routing Table

These figures show the IPv4 routing table learned through OSPFv3 (address-family ipv4) on both Luxembourg routers under process 180. Because the Luxembourg topology is minimal only LU-R1 and LU-R2 connected by a single point to point Serial link the OSPFv3 routing table contains exactly one learned route on each router the peer's loopback address.

Even though Luxembourg has only two routers, this verification demonstrates that the routing domain is functioning exactly as required, with OSPFv3 distributing IPv4 reachability in a secure and stable manner.

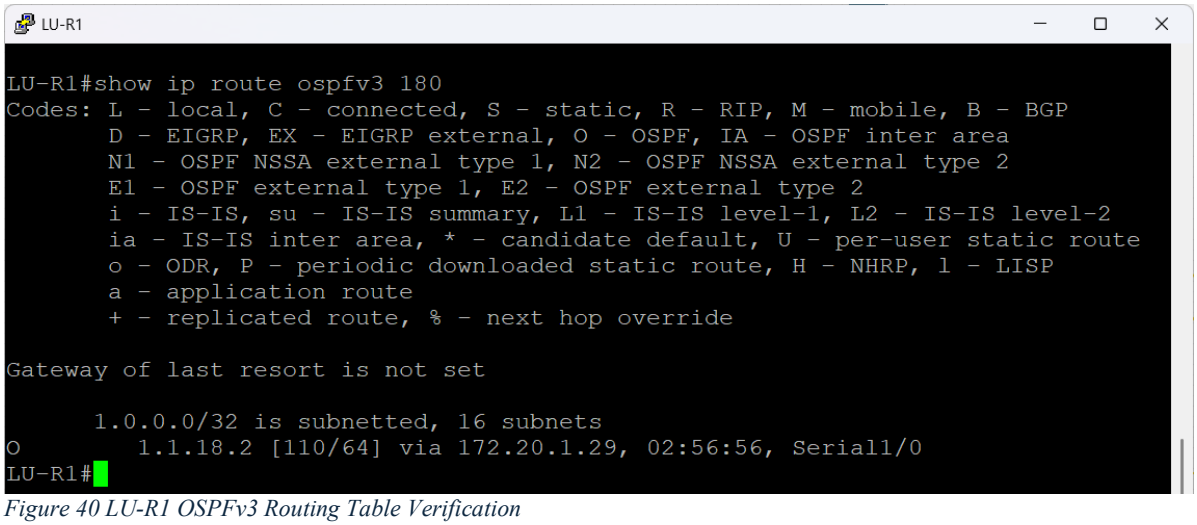

Figure 40 LU-R1 OSPFv3 Routing Table Verification

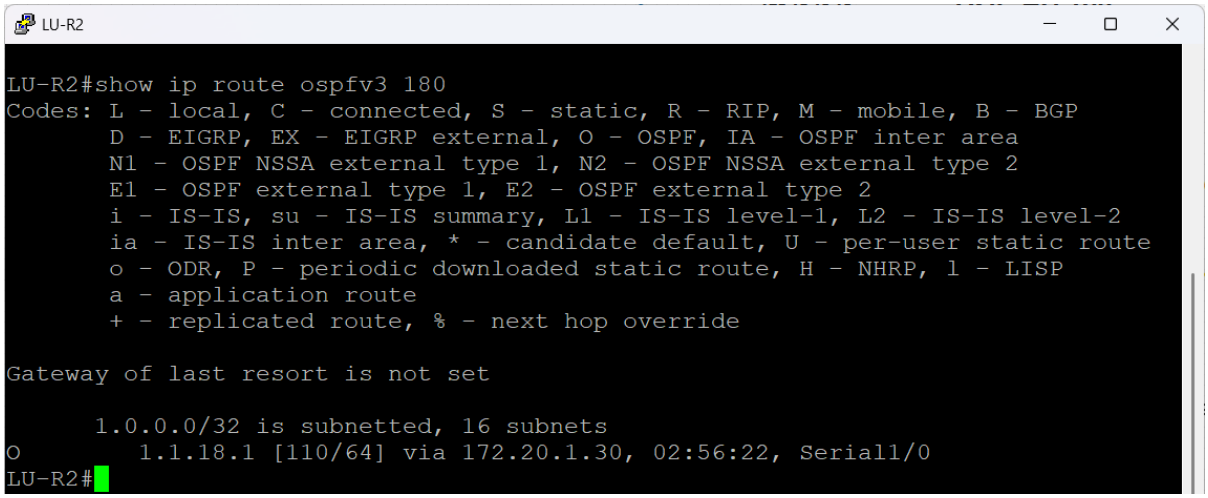

Figure 41 LU-R2 OSPFv3 Routing Table Verification

China – EIGRP (AS190)

China uses classic EIGRP for IPv4 only routing.

Implementation details:

- Enabled EIGRP
- Advertised local LANs

The figure below shows China branch topology

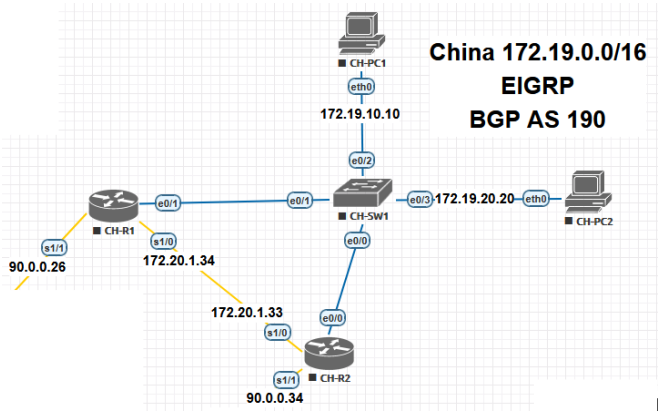

Figure 42 China Branch

EIGRP configuration

These figures below show the EIGRP configuration for the China site, running under AS 190, along with the HMAC-SHA-256 authentication key-chain used to secure the routing domain.

China uses classic EIGRP rather than named-mode, but the design still follows GHN's standard routing structure: clear network advertisement, strict interface control, and deterministic router-IDs.

Both routers advertise:

- Their router-ID loopbacks (1.1.19.x/32)
- China's internal LAN networks (172.19.10.0/24, 172.19.20.0/24, 172.19.30.0/24, 172.19.100.0/24)

- The China backbone /30 network (172.20.1.32/30)

- The ISP-facing /30 network from the 90.0.0.x block

passive-interface default is applied to lock down all interfaces, and only required ones Serial1/0, Serial1/1, and Loopback0 are activated with no passive-interface. This protects the control plane and reduces unwanted EIGRP hellos.

```
key 19
 key-string 7 01100E0D550A260A284B5C19
 cryptographic-algorithm hmac-sha-256
```

Figure 43 China EIGRP key-chain

CH-R1

```
router eigrp 190
 network 1.1.19.1 0.0.0.0
 network 90.0.0.28 0.0.0.3
 network 172.19.10.0 0.0.0.255
 network 172.19.20.0 0.0.0.255
 network 172.19.30.0 0.0.0.255
 network 172.19.100.0 0.0.0.255
 network 172.20.1.32 0.0.0.3
 passive-interface default
 no passive-interface Serial1/0
 no passive-interface Loopback0
 no passive-interface Serial1/1
 eigrp router-id 1.1.19.1
```

Figure 44 CH-R1 EIGRP Configuration

CH-R2

```
router eigrp 190
 network 1.1.19.2 0.0.0.0
 network 90.0.0.36 0.0.0.3
 network 172.19.10.0 0.0.0.255
 network 172.19.20.0 0.0.0.255
 network 172.19.30.0 0.0.0.255
 network 172.19.100.0 0.0.0.255
 network 172.20.1.32 0.0.0.3
 passive-interface default
 no passive-interface Serial1/0
 no passive-interface Loopback0
 no passive-interface Serial1/1
 eigrp router-id 1.1.19.2
```

Figure 45 CH-R2 EIGRP Configuration

EIGRP Routing Table

These figures show the EIGRP routing tables for CH-R1 and CH-R2 under AS 190. Because the China site contains only two routers connected by a single point to point link, each router learns exactly one EIGRP route the peer's loopback address used as the router-ID.

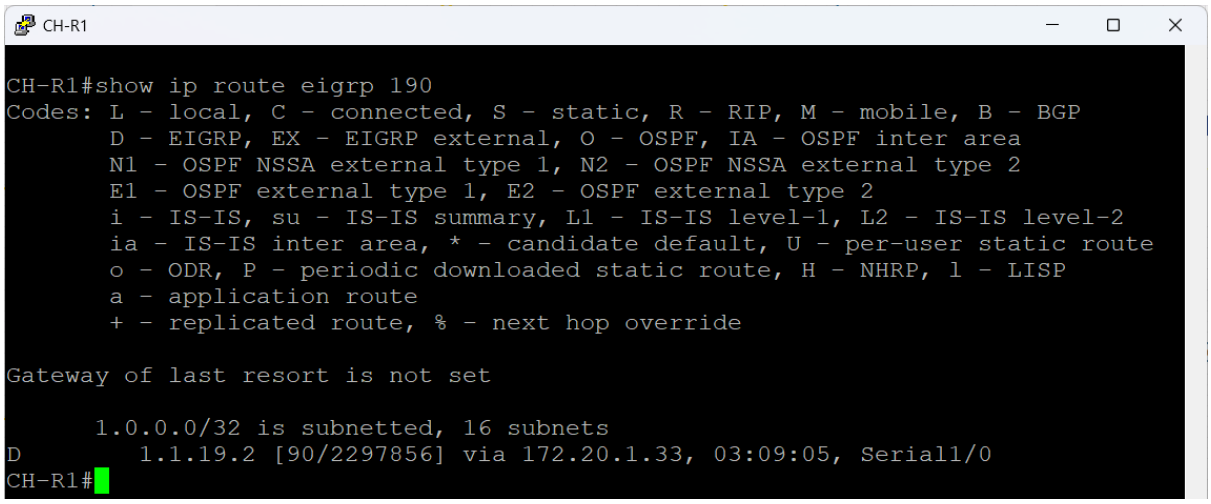

Figure 46 CH-R1 EIGRP Routing Table Verification

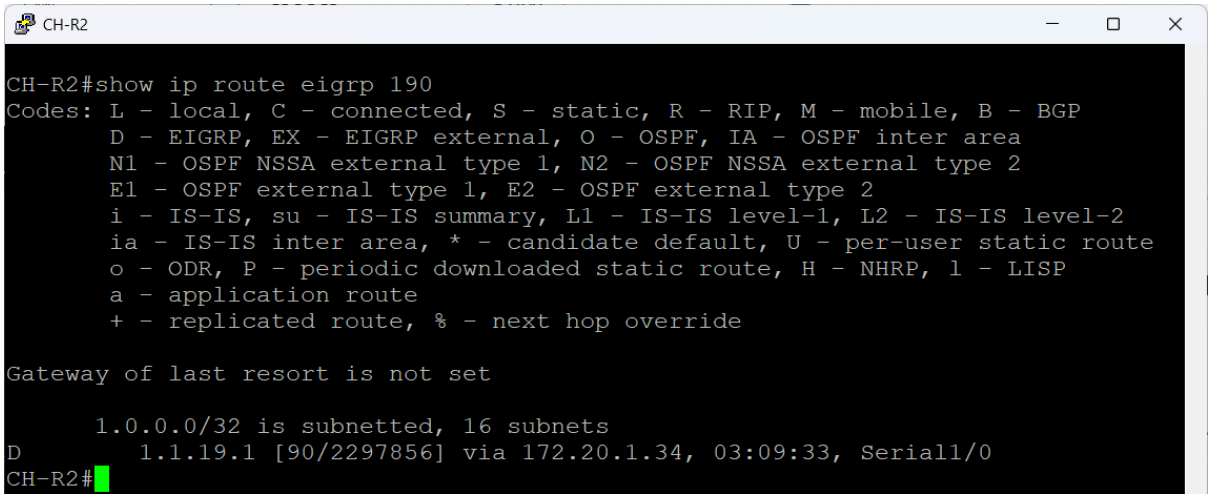

Figure 47 CH-R2 EIGRP Routing Table Verification

EIGRP Topology Tables

These figures below show the EIGRP topology tables for CH-R1 and CH-R2. The topology table contains all routes learned by EIGRP including feasible successors and reflects the router's full understanding of the network before the best routes are selected for the routing table.

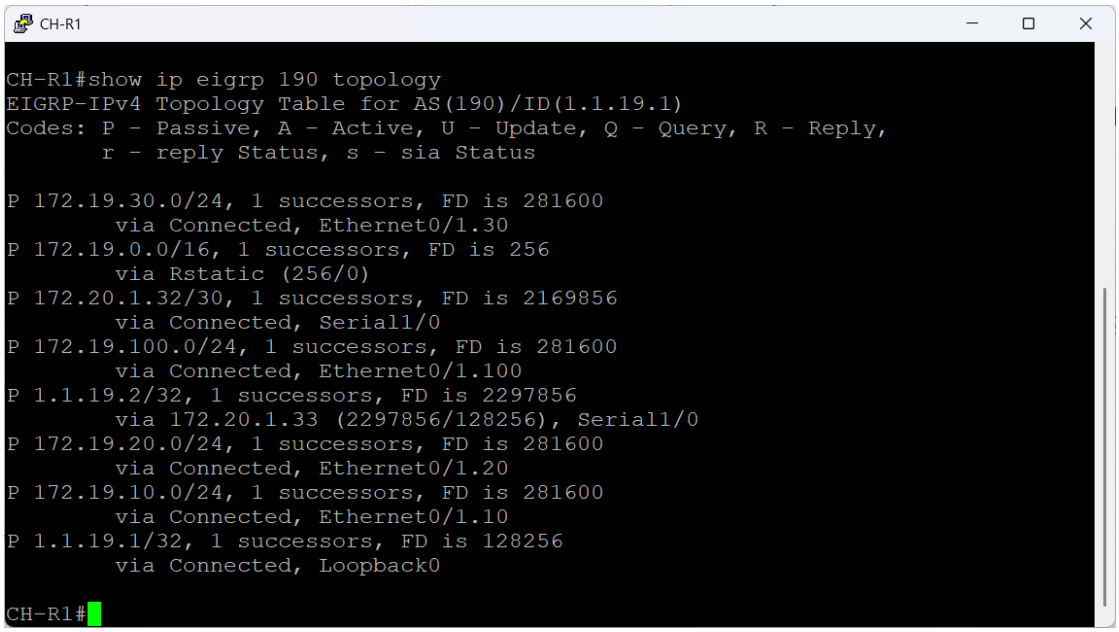

Figure 48 CH-R1 EIGRP Topology Table

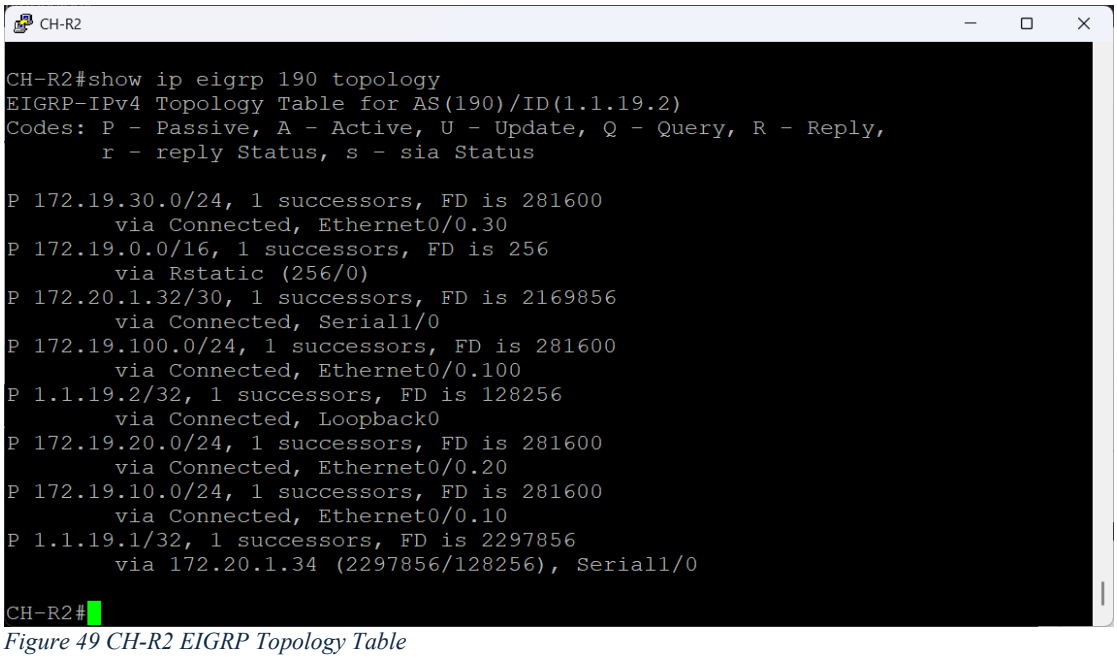

Figure 49 CH-R2 EIGRP Topology Table

ISP Backbone – OSPF (AS1000)

The ISP runs OSPF and IBGP as a simple backbone for carrier operations

The figure below shows the ISP core routers

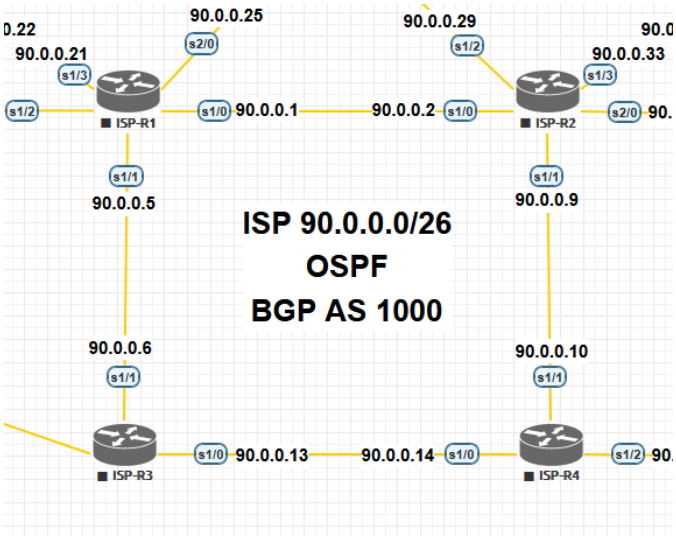

Figure 50 ISP Core Routers

These figures below show how the ISP core routers R1, R2, R3, and R4 are built using a combination of OSPF as the internal routing protocol and iBGP/EBGP as the service edge routing system.

1. OSPF Configuration IGP for the ISP Backbone

   Each ISP router runs OSPF process 100 with a unique router-ID sourced from Loopback0.
   The internal links between ISP routers are advertised in Area 0, forming a single, flat backbone.

   The purpose of OSPF here is simple:

   - Provide fast, stable internal reachability between Loopbacks.

   - Ensure that all BGP update-source Loopbacks are routable across the ISP.

- The no passive-interface commands guarantee OSPF adjacencies on the serial links and allow dynamic formation of neighbor relationships.

2. BGP Design Inside the ISP AS 1000

All ISP routers participate in iBGP within AS1000 using their Loopback0 interfaces for reliable peering update-source Loopback0.

External sites Bahrain AS160, England AS170, Luxembourg AS180, China AS190 connect via EBGP on the 90.0.0.0/26 subnets.

Key points demonstrated by the configs:

- ISP-R2: Primary Route Reflector for ISP-R1, ISP-R3, and ISP-R4

  This removes the requirement for a full iBGP mesh.
  route-reflector-client entries clearly show which peers rely on R2 for route reflection.

  R2 learns external prefixes from AS170/AS180/AS190 and redistributes them across the network.

- ISP-R3: Backup Route Reflector

  ISP-R3 mirrors R2's function with a secondary cluster-ID 1.1.1.2, preventing routing loops.
  It provides redundancy: if R2 fails, internal BGP routes still propagate through R3.

  ISP-R3 is also an edge device, holding EBGP sessions with AS160 and AS190.

3. Address-Family IPv4 Behavior

Inside the address-family ipv4 section, you advertise:

- Loopback prefixes (1.1.x.x/32) for BGP stability
- Customer links (90.0.x.x/30)
- ISP internal segments 10.x.x.x/32, 20.x.x.x/32, 30.x.x.x/32, and 40.x.x.x/32

next-hop-self is applied on all EBGP to iBGP learned routes, so the ISP backbone always forwards traffic to the correct exit point.

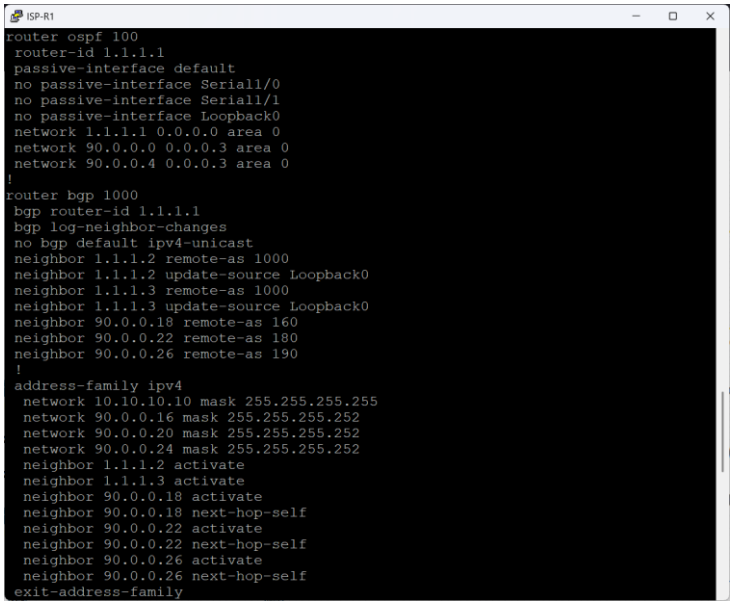

Figure 51 ISP-R1 Configuration

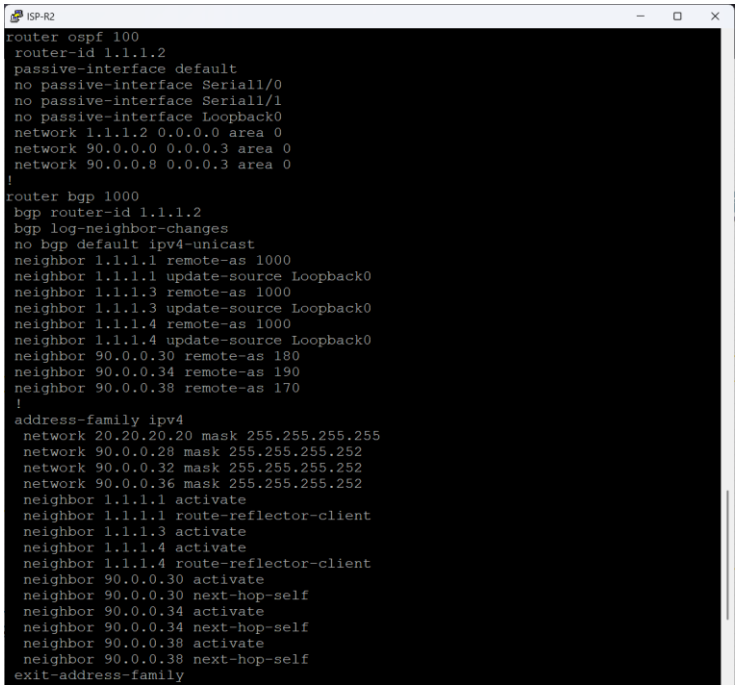

Figure 52 ISP-R2 Configuration

ISP-R3

```
router ospf 100
 router-id 1.1.1.3
 passive-interface default
 no passive-interface Serial1/0
 no passive-interface Serial1/1
 no passive-interface Loopback0
 network 1.1.1.3 0.0.0.0 area 0
 network 90.0.0.4 0.0.0.3 area 0
 network 90.0.0.12 0.0.0.3 area 0
!
router bgp 1000
 bgp router-id 1.1.1.3
 bgp cluster-id 1.1.1.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.1 remote-as 1000
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 1.1.1.2 remote-as 1000
 neighbor 1.1.1.2 update-source Loopback0
 neighbor 1.1.1.4 remote-as 1000
 neighbor 1.1.1.4 update-source Loopback0
 neighbor 90.0.0.42 remote-as 160
 !
 address-family ipv4
  network 30.30.30.30 mask 255.255.255.255
  network 90.0.0.40 mask 255.255.255.252
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 route-reflector-client
  neighbor 1.1.1.2 activate
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 route-reflector-client
  neighbor 90.0.0.42 activate
  neighbor 90.0.0.42 next-hop-self
 exit-address-family
```

Figure 53 ISP-R3 Configuration

ISP-R4

```
router ospf 100
 router-id 1.1.1.4
 passive-interface default
 no passive-interface Serial1/0
 no passive-interface Serial1/1
 no passive-interface Loopback0
 network 1.1.1.4 0.0.0.0 area 0
 network 90.0.0.8 0.0.0.3 area 0
 network 90.0.0.12 0.0.0.3 area 0
!
router bgp 1000
 bgp router-id 1.1.1.4
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.2 remote-as 1000
 neighbor 1.1.1.2 update-source Loopback0
 neighbor 1.1.1.3 remote-as 1000
 neighbor 1.1.1.3 update-source Loopback0
 neighbor 90.0.0.46 remote-as 170
 !
 address-family ipv4
  network 40.40.40.40 mask 255.255.255.255
  network 90.0.0.44 mask 255.255.255.252
  neighbor 1.1.1.2 activate
  neighbor 1.1.1.3 activate
  neighbor 90.0.0.46 activate
  neighbor 90.0.0.46 next-hop-self
 exit-address-family
```

Figure 54 ISP-R4 Configuration

BGP WAN Implementation

Autonomous System Design

All GHN sites connect only to the ISP via EBGP.
There is no IBGP between GHN branches.

AS assignments:

- AS160 – Bahrain
- AS170 – England
- AS180 – Luxembourg
- AS190 – China
- AS1000 – ISP Backbone

EBGP Peering

Peering was established on 90.0.0.0/26 WAN links between each site and the ISP.

These figures below show how each customer site (Bahrain AS160, England AS170, Luxembourg AS180, China AS190) connects to the ISP backbone (AS1000).
The design is intentionally simple and realistic: every customer site forms one EBGP session toward the ISP and advertises only its loopback prefix.

Figure 55 BH-R1 EBGP Configurations

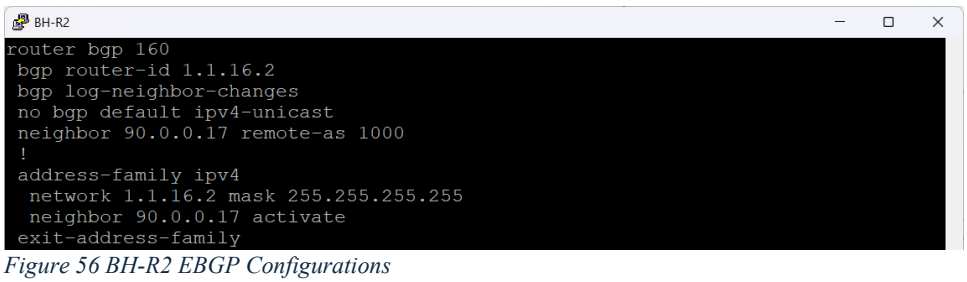

Figure 56 BH-R2 EBGP Configurations

EN-R1

```
router bgp 170
 bgp router-id 1.1.17.1
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 90.0.0.37 remote-as 1000
 !
 address-family ipv4
  network 1.1.17.1 mask 255.255.255.255
  neighbor 90.0.0.37 activate
 exit-address-family
```

Figure 57 EN-R1 EBGP Configurations

EN-R2

```
router bgp 170
 bgp router-id 1.1.17.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 90.0.0.45 remote-as 1000
 !
 address-family ipv4
  network 1.1.17.2 mask 255.255.255.255
  neighbor 90.0.0.45 activate
 exit-address-family
```

Figure 58 EN-R2 EBGP Configurations

LU-R1

```
router bgp 180
 bgp router-id 1.1.18.1
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 90.0.0.29 remote-as 1000
 !
 address-family ipv4
  network 1.1.18.1 mask 255.255.255.255
  neighbor 90.0.0.29 activate
 exit-address-family
```

Figure 59 LU-R1 EBGP Configurations

LU-R2

```
router bgp 180
 bgp router-id 1.1.18.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 90.0.0.21 remote-as 1000
 !
 address-family ipv4
  network 1.1.18.2 mask 255.255.255.255
  neighbor 90.0.0.21 activate
 exit-address-family
```

Figure 60 EN-R2 EBGP Configurations

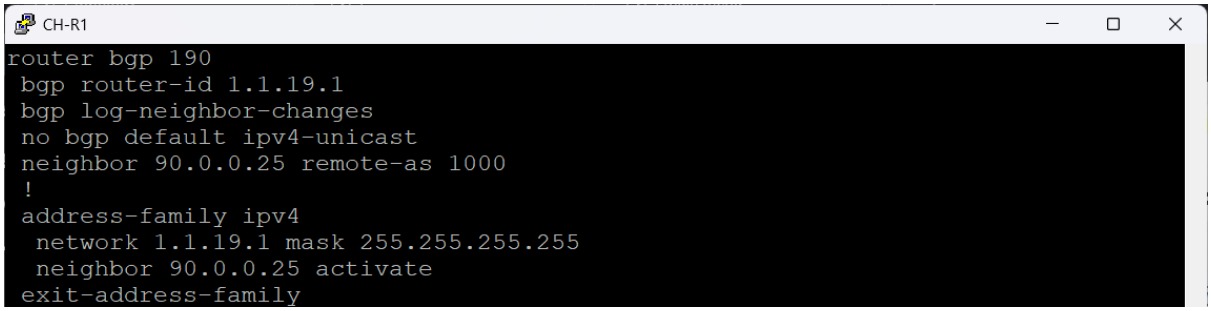

Figure 61 CH-R1 EBGP Configurations

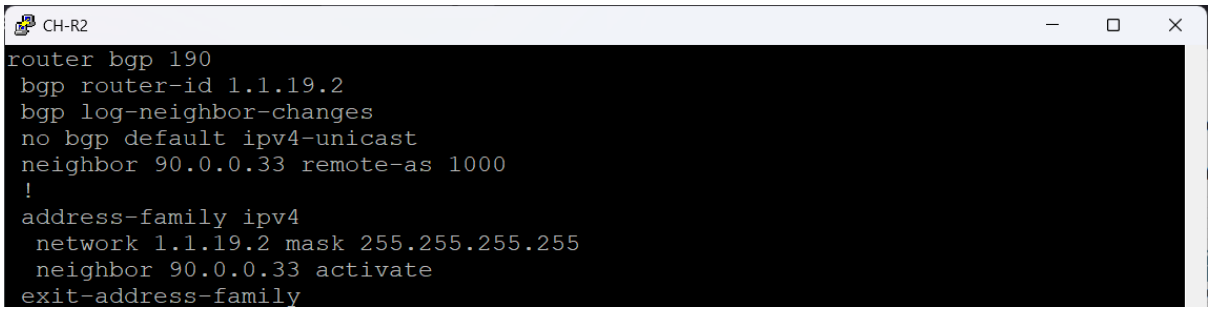

Figure 62 CH-R2 EBGP Configurations

BGP Summary

These figures below confirm that each customer site (AS160, AS170, AS180, AS190) has a fully established EBGP session with the ISP (AS1000) and is successfully receiving all global routes reflected through the ISP backbone.

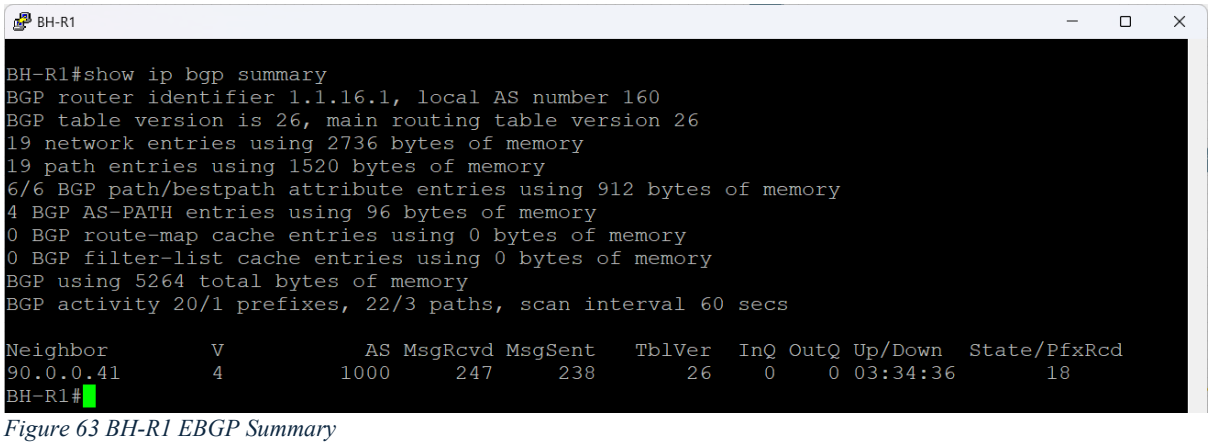

Figure 63 BH-R1 EBGP Summary

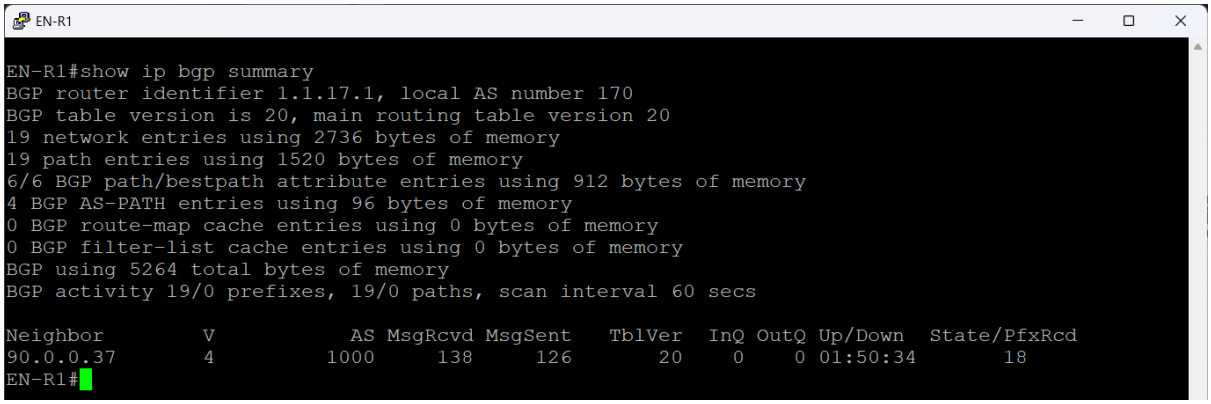

Figure 64 EN-R1 EBGP Summary

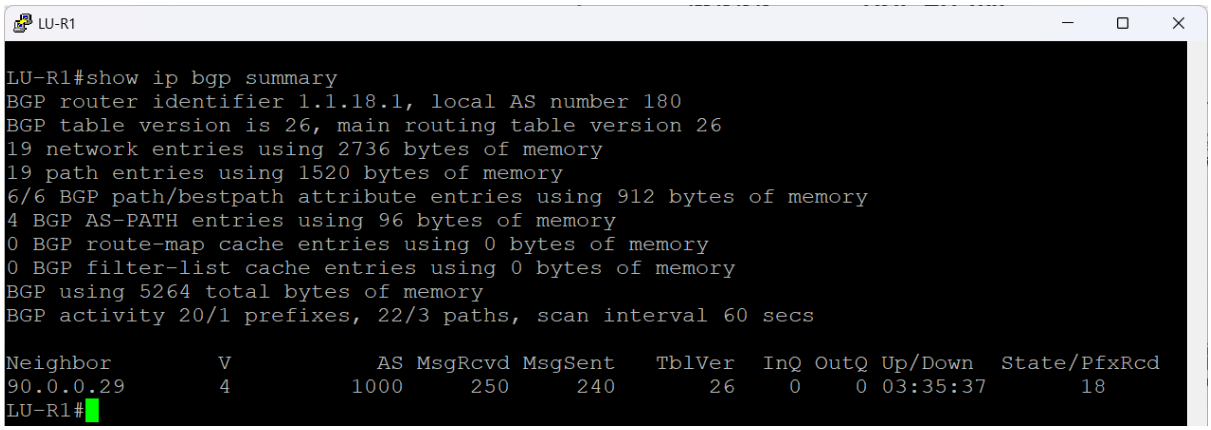

Figure 65 LU-R1 EBGP Summary

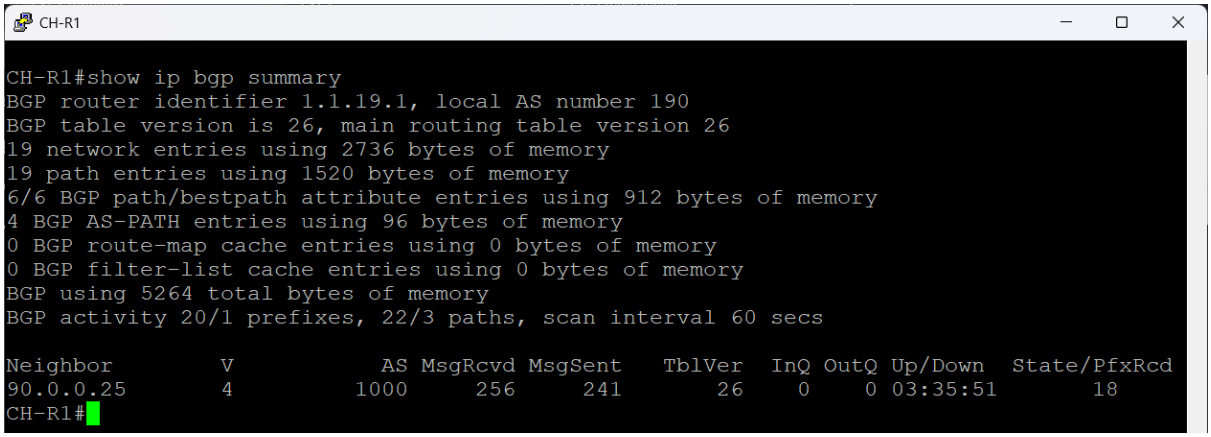

Figure 66 CH-R1 EBGP Summary

BGP Routing Tables

These BGP tables confirm that every customer router is receiving a complete and correct routing view from the ISP. Each router sees:

1. All loopback prefixes from every site (BH, EN, LU, CH)
2. All ISP infrastructure prefixes (10.x.x.x, 20.x.x.x, 30.x.x.x, 40.x.x.x)
3. All WAN /30 networks used between the ISP and the customers
4. Their own local loopback as best-path (indicated by next-hop 0.0.0.0 and weight 32768)
5. All remote paths marked as internal (i) because they come from iBGP route-reflection inside the ISP before being sent over EBGP

This output proves that the full BGP architecture works exactly as designed.

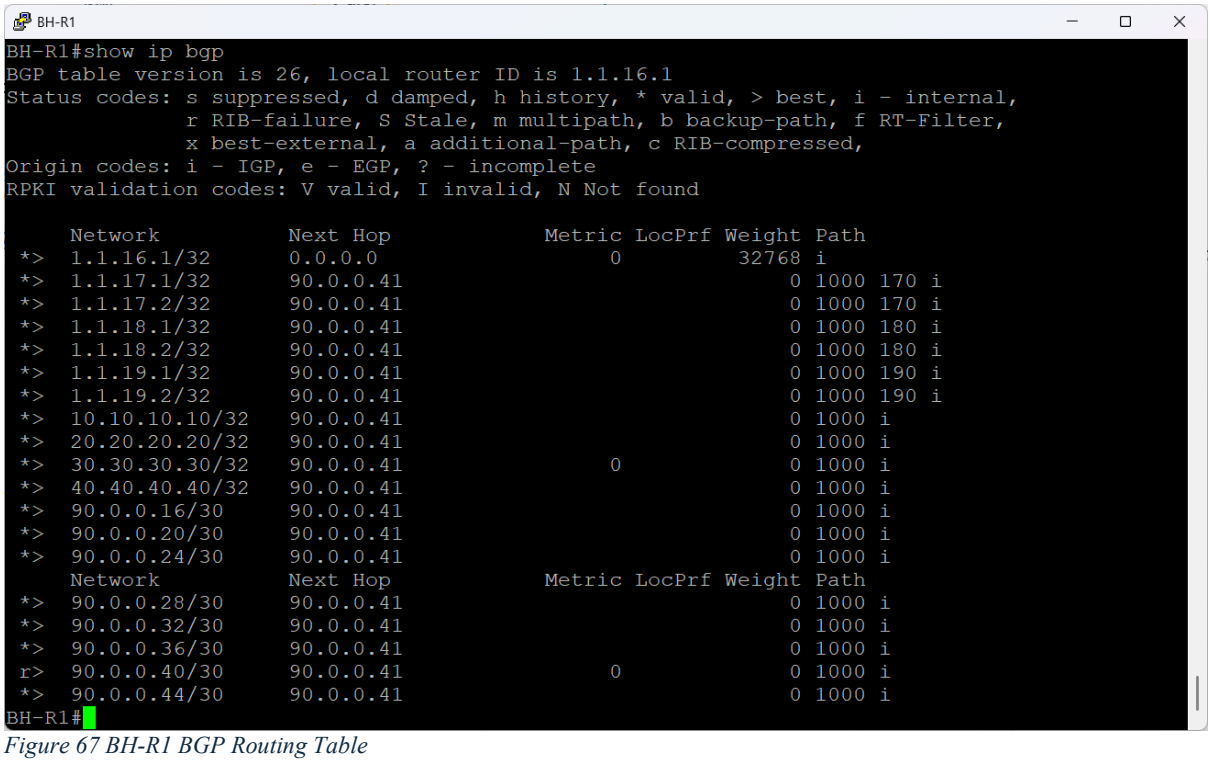

Figure 67 BH-R1 BGP Routing Table

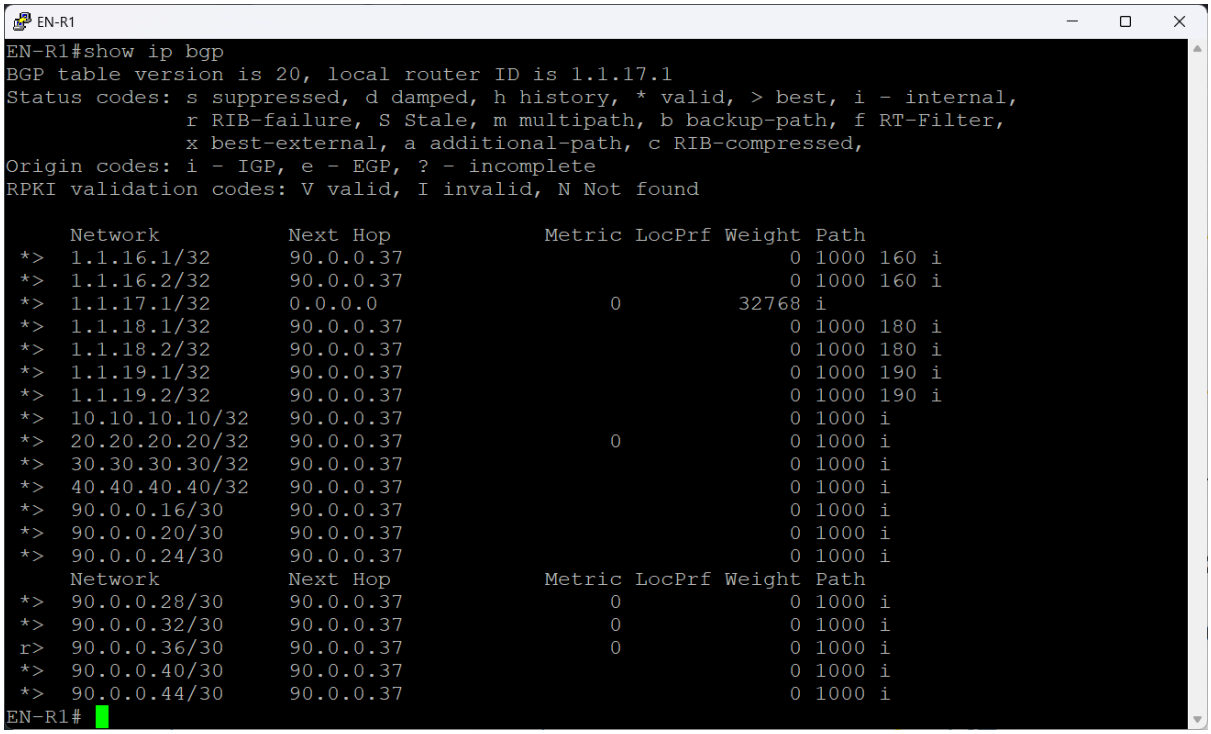

Figure 68 EN-R1 BGP Routing Table

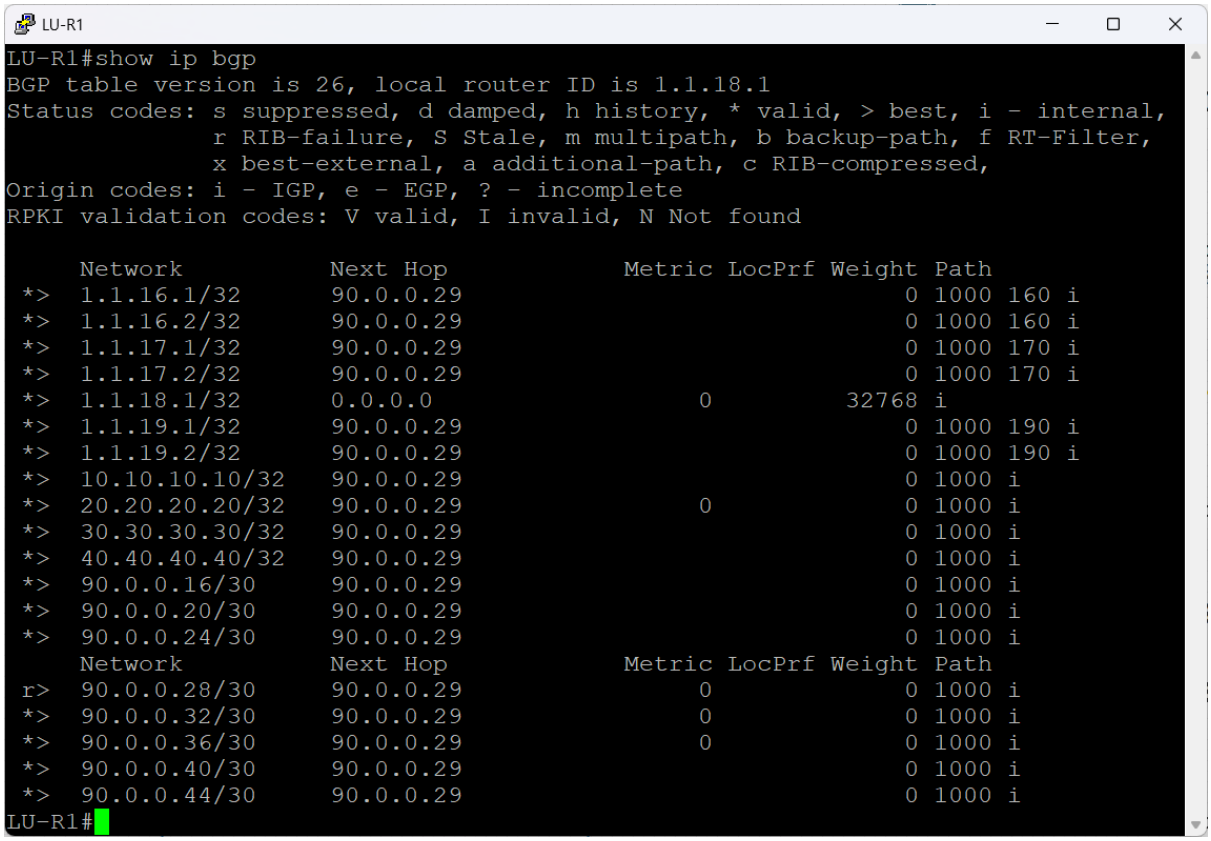

Figure 69 LU-R1 BGP Routing Table

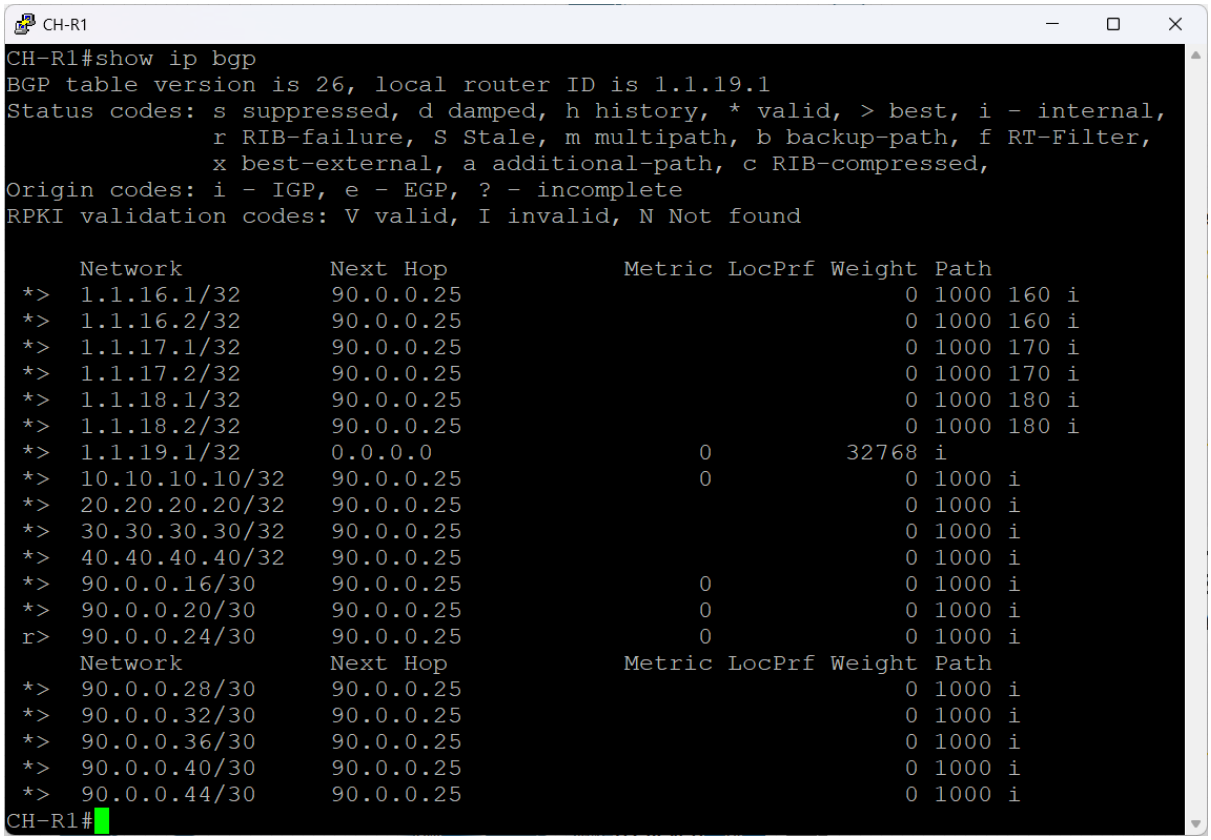

Figure 70 CH-R1 BGP Routing Table

DMVPN Phase 3 & IPsec Implementation

GHN uses a **dual-hub DMVPN Phase 3** design:

- **Hub 1:** BH-R1 → Tunnel1
- **Hub 2:** BH-R2 → Tunnel2
- **Spokes:** England, Luxembourg, China

Advantages:

- Automatic spoke-to-spoke shortcuts
- Failover between Tunnel1 and Tunnel2
- Scalable with minimal configuration on spokes

GRE & NHRP Configuration

These figures below show the complete DMVPN Phase-3 design used to interconnect all branches (Bahrain, England, Luxembourg, China) securely over the ISP backbone.
The design uses **two independent DMVPN Hubs**, giving you high availability, load distribution, and resilience:

- **DMVPN Hub 1 → Tunnel Key 100 → Network-ID 1**
- **DMVPN Hub 2 → Tunnel Key 200 → Network-ID 2**

Each site participates in both Hubs, but with different tunnel sources, keys, and NHRP servers. This creates dual-hub dual-Hubs redundancy for a GHN enterprise WAN.

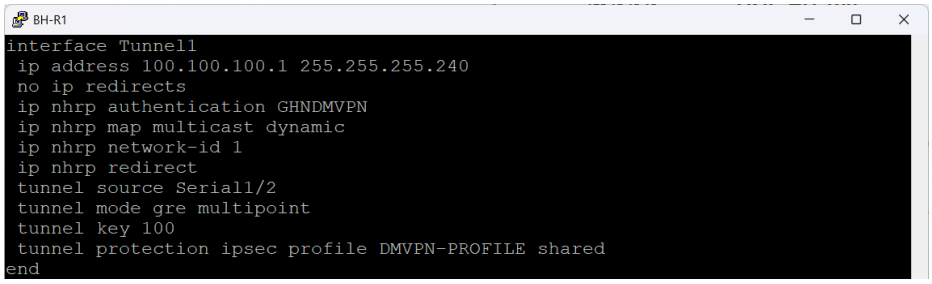

Figure 71 BH-R1 DMVPN Hub 1 Configuration

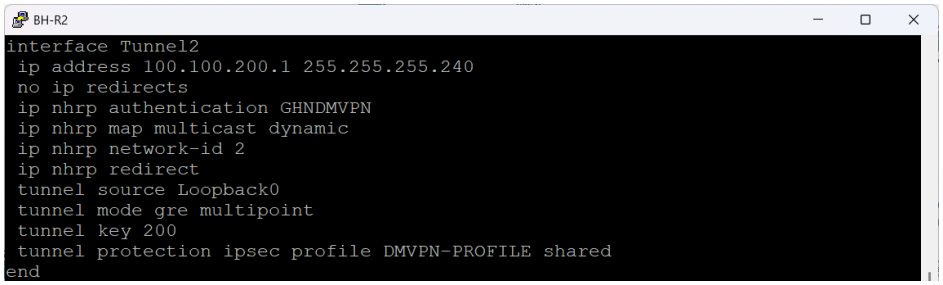

Figure 72 BH-R2 DMVPN Hub 2 Configuration

EN-R2

```
interface Tunnel1
 ip address 100.100.100.5 255.255.255.240
 no ip redirects
 ip nhrp authentication GHNDMVPN
 ip nhrp map multicast 90.0.0.42
 ip nhrp map 100.100.100.1 90.0.0.42
 ip nhrp network-id 1
 ip nhrp nhs 100.100.100.1
 ip nhrp shortcut
 delay 1000
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE shared
end
!
interface Tunnel2
 ip address 100.100.200.5 255.255.255.240
 no ip redirects
 ip nhrp authentication GHNDMVPN
 ip nhrp map multicast 1.1.16.2
 ip nhrp map 100.100.200.1 1.1.16.2
 ip nhrp network-id 2
 ip nhrp nhs 100.100.200.1
 ip nhrp shortcut
 delay 5000
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 200
 tunnel protection ipsec profile DMVPN-PROFILE shared
end
```

Figure 73 EN-R2 DMVPN Spoke Configuration

LU-R2

```
interface Tunnel1
 ip address 100.100.100.6 255.255.255.240
 no ip redirects
 ip nhrp authentication GHNDMVPN
 ip nhrp map multicast 90.0.0.42
 ip nhrp map 100.100.100.1 90.0.0.42
 ip nhrp network-id 1
 ip nhrp nhs 100.100.100.1
 ip nhrp shortcut
 delay 1000
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE shared
end
!
interface Tunnel2
 ip address 100.100.200.6 255.255.255.240
 no ip redirects
 ip nhrp authentication GHNDMVPN
 ip nhrp map multicast 1.1.16.2
 ip nhrp map 100.100.200.1 1.1.16.2
 ip nhrp network-id 2
 ip nhrp nhs 100.100.200.1
 ip nhrp shortcut
 delay 5000
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 200
 tunnel protection ipsec profile DMVPN-PROFILE shared
end
```

Figure 74 LU-R2 DMVON Spoke Configuration

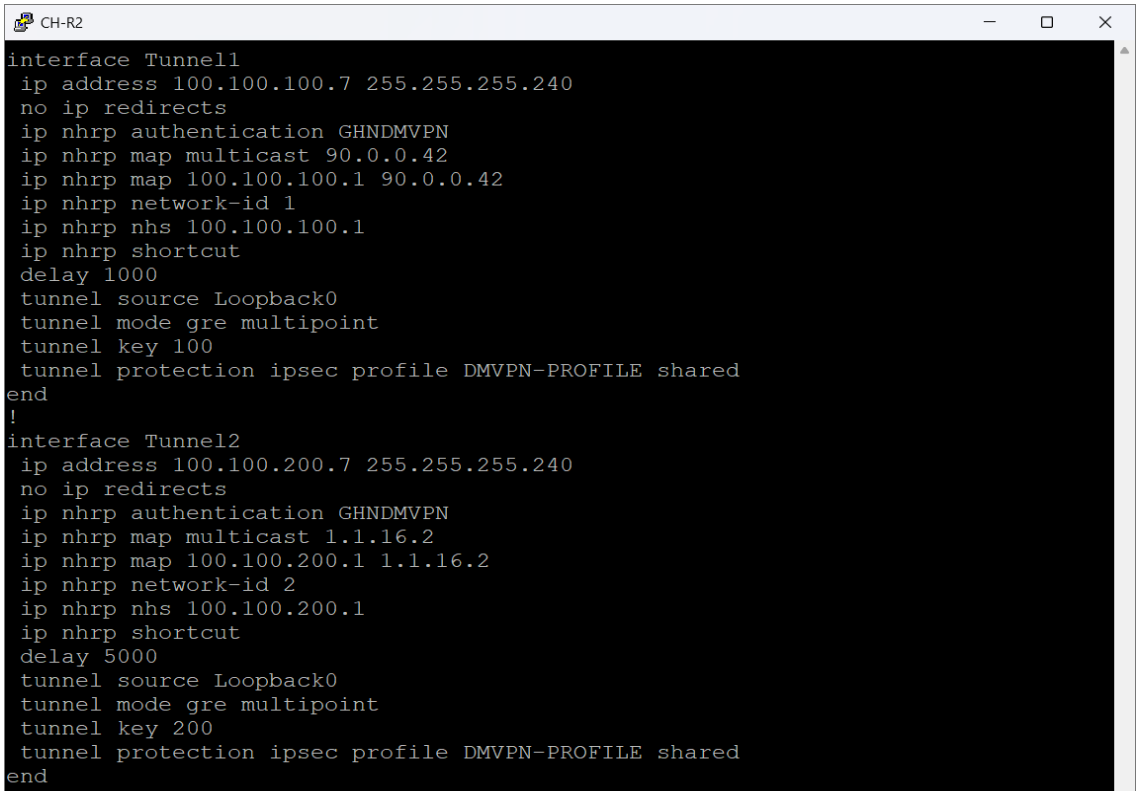

Figure 75 CH-R2 DMVPN Spoke Configuration

DMVPN EIGRP Configuration

These figures below show how EIGRP is used as the dynamic routing protocol running across both DMVPN clouds. Every branch (BH, EN, LU, CH) participates in EIGRP AS 100, using named-mode configuration for scalability and clarity.

The goal of this design is simple:

- Allow all branches to exchange internal LAN prefixes through the DMVPN tunnels
- Provide automatic failover between the two DMVPN Hubs
- Support Phase-3 spoke-to-spoke forwarding without routing loops

Tunnel-Specific Behavior

On the hubs, under Tunnel1 and Tunnel2, you see:

- no next-hop-self
- no split-horizon

This is mandatory for DMVPN:

- Split-horizon off allows spokes to learn routes from other spokes through the hub.

- No next-hop-self ensures the real tunnel next-hop is preserved so Phase-3 shortcuts can form.

Without these two commands, DMVPN would break or behave like Phase-1.

Each router advertises the tunnel networks depending on which hub it participates in
This is what allows:

- Hub 1 (key 100) and hub 2 (key 200) to run in parallel
- Automatic failover when one hub is unavailable
- Redundancy at the routing layer, not just the tunnel layer

Redistribution of Static Routes

Each router redistributes static routes into EIGRP:

- redistribute static metric 100000 10 255 1 1500

To advertise the site's internal LAN prefix into EIGRP through a static pointing to Null0

Each branch uses its own LAN range:

- BH → 172.16.0.0/16
- EN → 172.17.0.0/16
- LU → 172.18.0.0/16
- CH → 172.19.0.0/16

Spoken Behavior (EN-R2, LU-R2, CH-R2)

Spoke do not disable split-horizon or next-hop-self.

This is because spokes send updates upward only not laterally and hubs must maintain next-hop integrity for Phase-3 NHRP shortcuts.

BH-R1

```
router eigrp DMVPN
 !
 address-family ipv4 unicast autonomous-system 100
  !
  af-interface Tunnel1
   no next-hop-self
   no split-horizon
  exit-af-interface
  !
  topology base
   redistribute static metric 100000 10 255 1 1500
  exit-af-topology
  network 1.1.16.100 0.0.0.0
  network 100.100.100.0 0.0.0.15
  eigrp router-id 1.1.16.100
 exit-address-family
!
ip route 172.16.0.0 255.255.0.0 Null0
```

Figure 76 BH-R1 DMVPN EIGRP Configuration

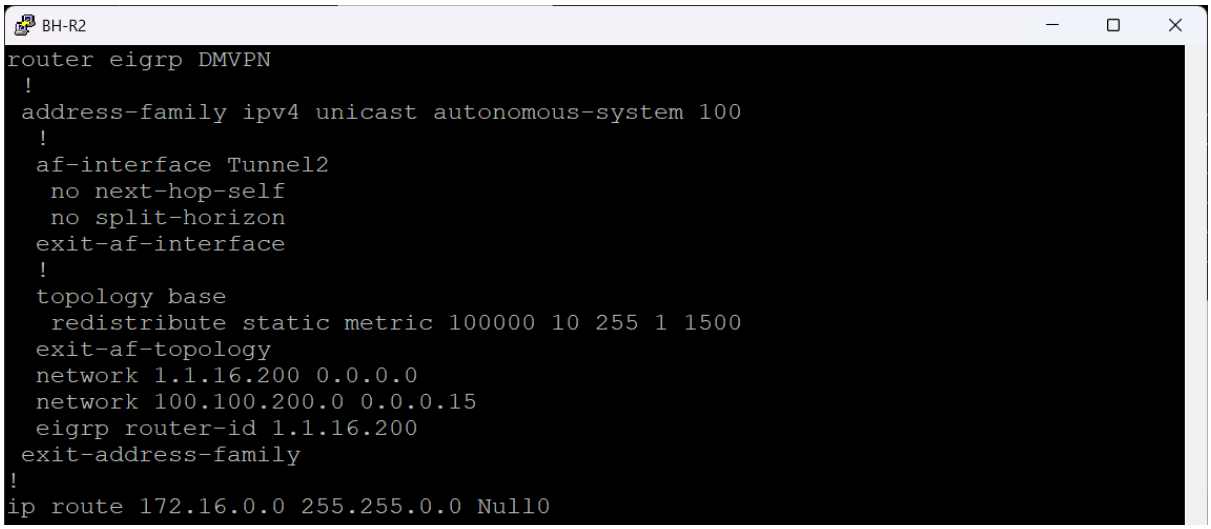

Figure 77 BH-R2 DMVPN EIGRP Configuration

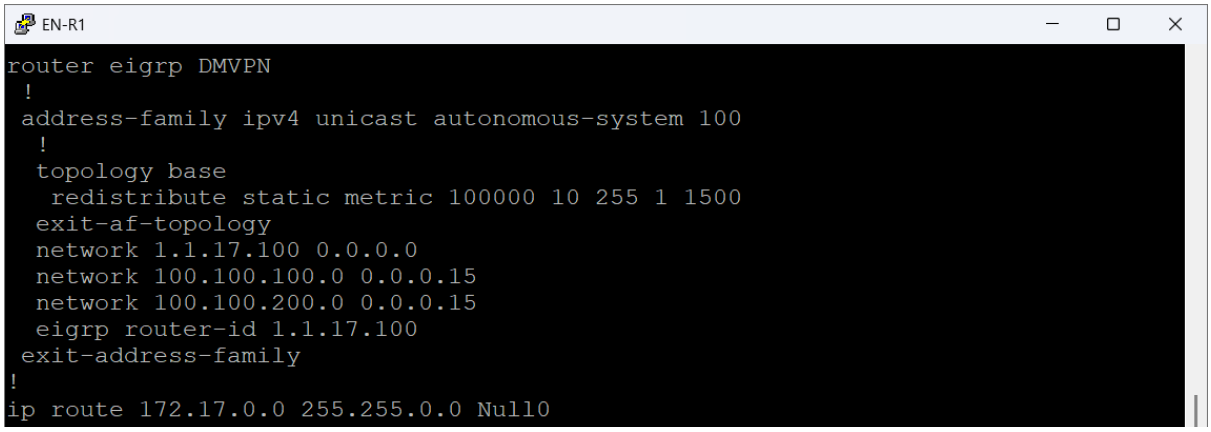

Figure 78 EN-R1 DMVPN EIGRP Configuration

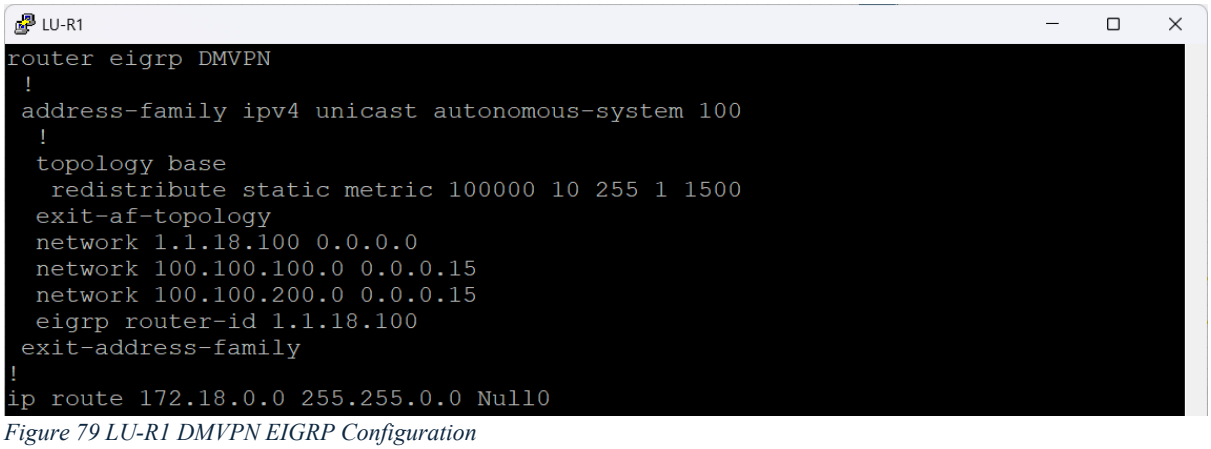

Figure 79 LU-R1 DMVPN EIGRP Configuration

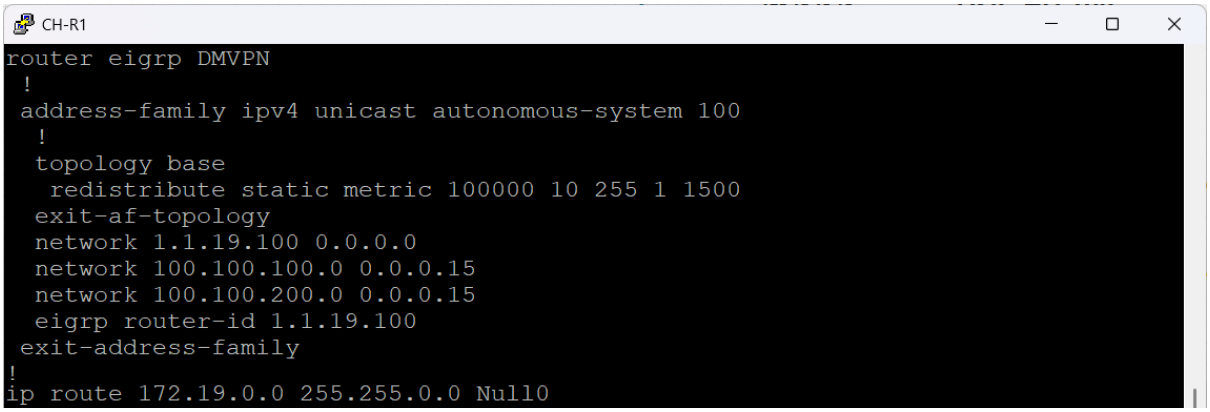

Figure 80 CH-R1 DMVPN EIGRP Configuration

EIGRP Routing Tables

These routing tables confirm that the DMVPN overlay is fully operational, both clouds are active, spoke-to-hub and hub-to-spoke routing is functioning, and all sites learn each other's prefixes through EIGRP AS 100.

Across BH, EN, LU, and CH routers, the show ip route eigrp 100 output shows:

- All Loopback /32 Routes Are Successfully Learned
- Dual DMVPN Hubs Are Working
- External EIGRP Routes Show Correct LAN Prefix Propagation
- Multiple Possible Paths Confirm Phase-3 Behavior

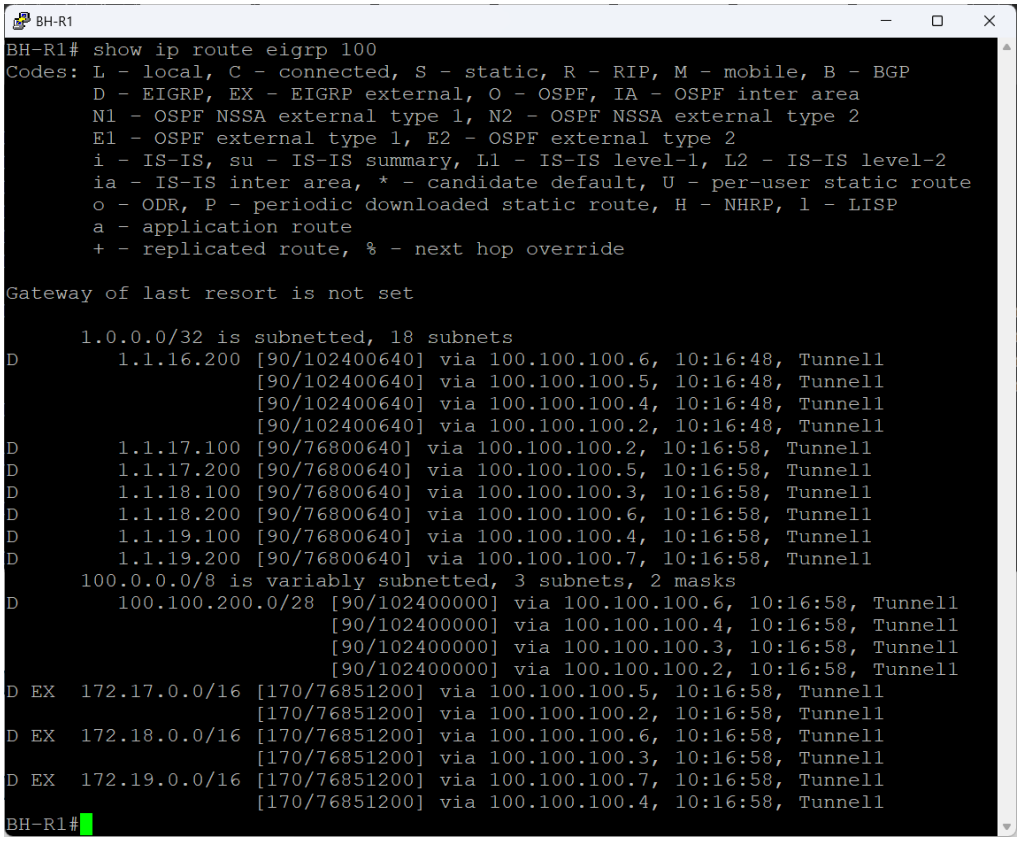

Figure 81 BH-R1 EIGRP Routing Table

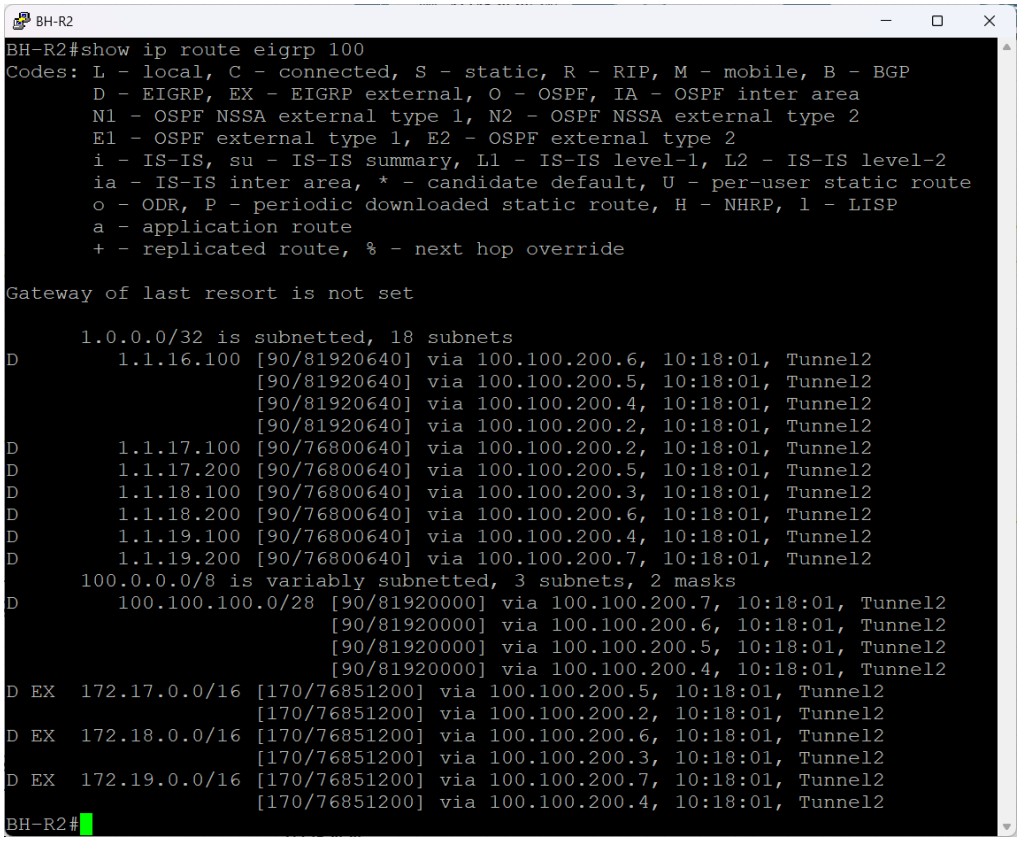

Figure 82 BH-R2 EIGRP Routing Table

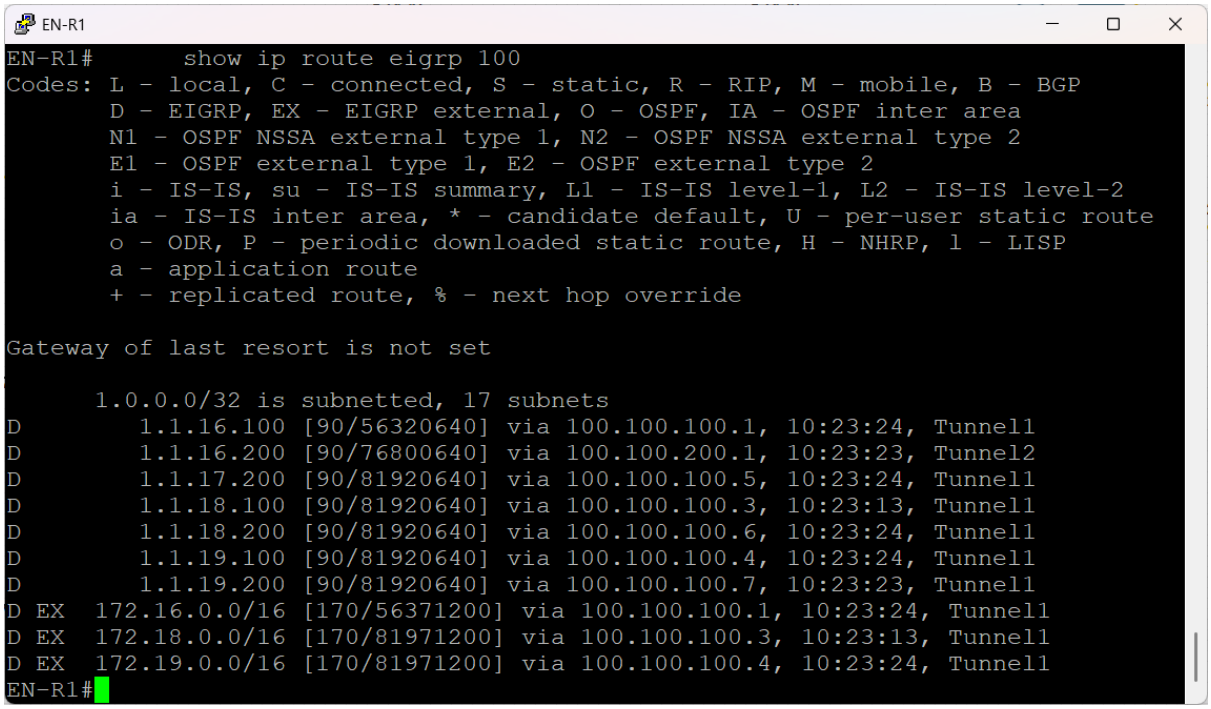

Figure 83 EN-R1 EIGRP Routing Table

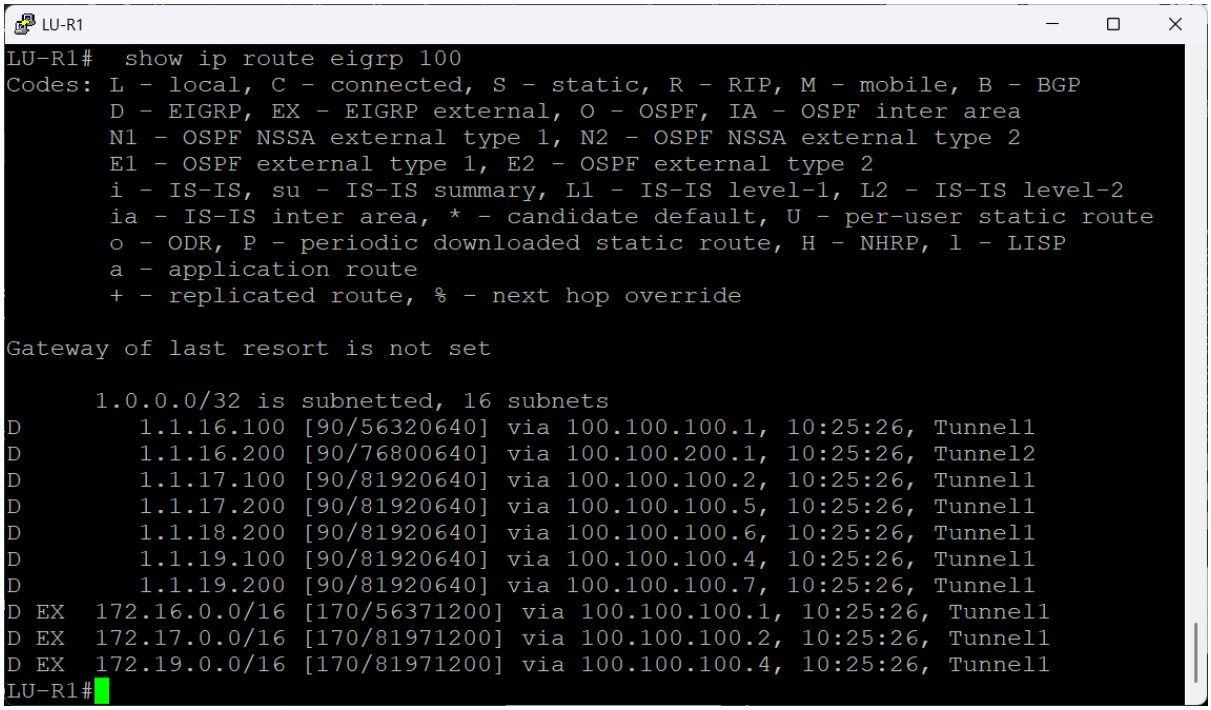

Figure 84 LU-R1 EIGRP Routing Table

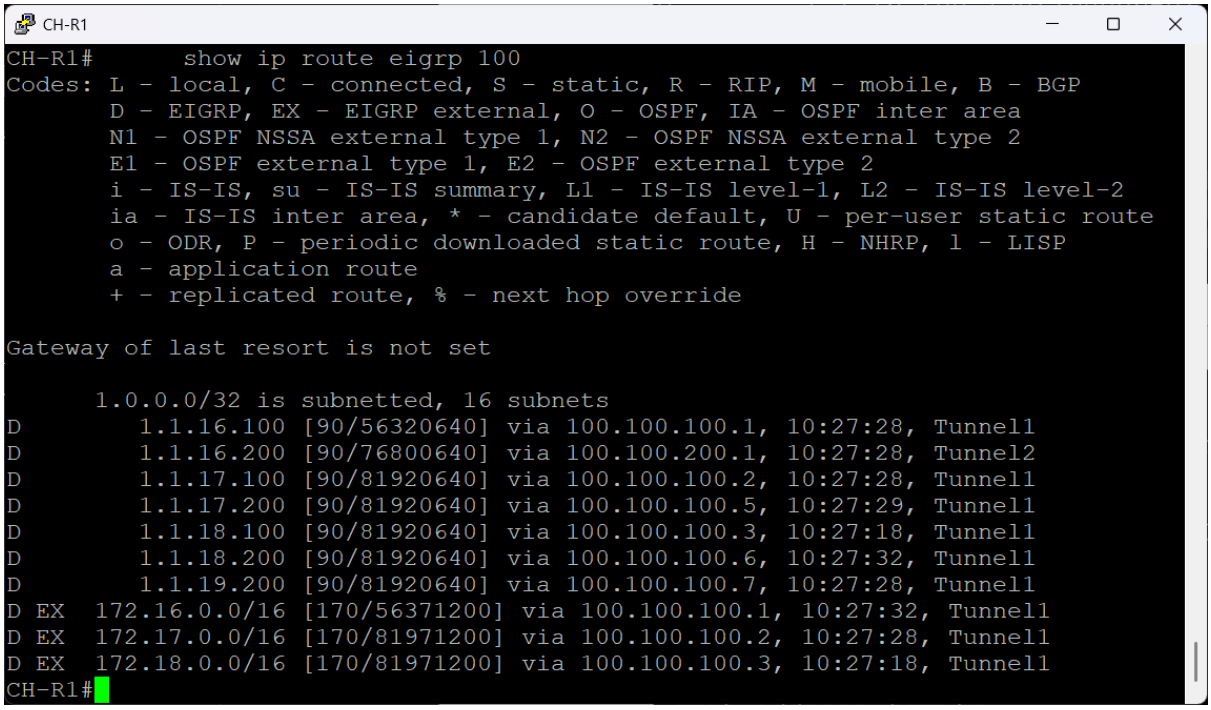

Figure 85 CH-R1 EIGRP Routing Table

DMVPN Verification

In this section will focus on verification of the DMVPN tunnel connectivity by

- Tunnel reachability
- Spoke-to-spoke pings
- NHRP table correctness

DMVPN Status Outputs

These DMVPN outputs confirm that dual hub DMVPN Phase-3 design is fully operational. Both Bahrain routers (BH-R1 and BH-R2) behave as hubs, while England, Luxembourg, and China operate as spokes. In the figures below the England show only one spoke for demonstration the other spoke has the same configuration just deferent ip address.

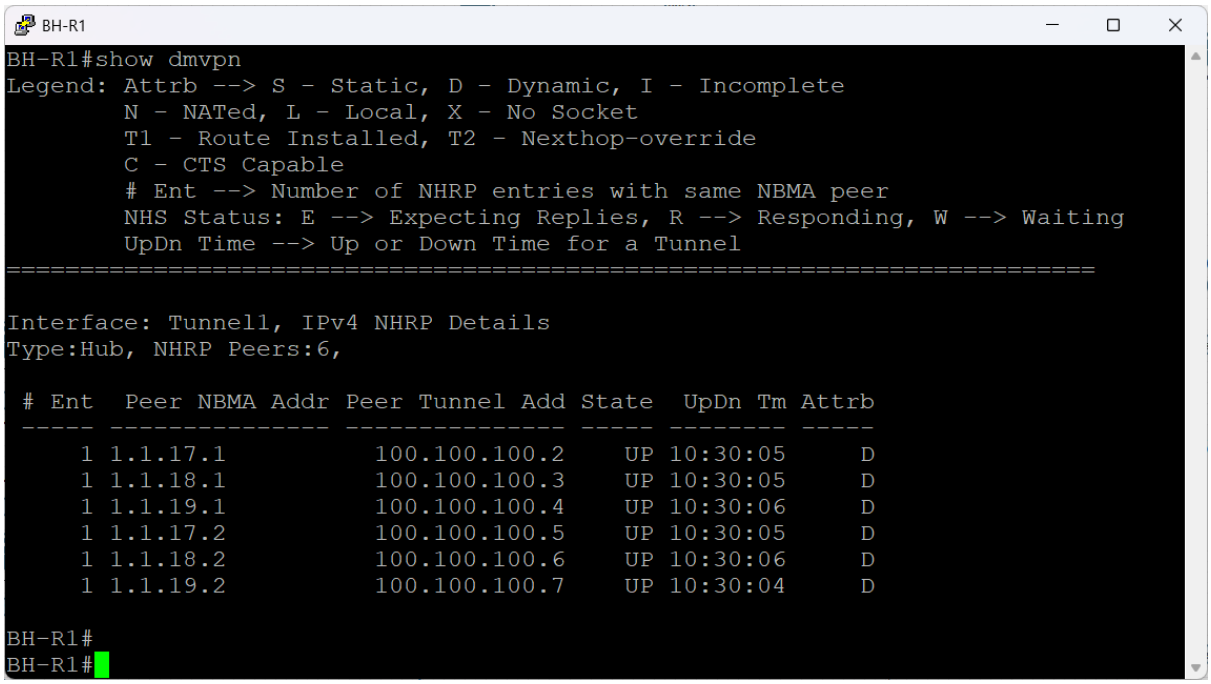

Figure 86 BH-R1 DMVPN Status Output

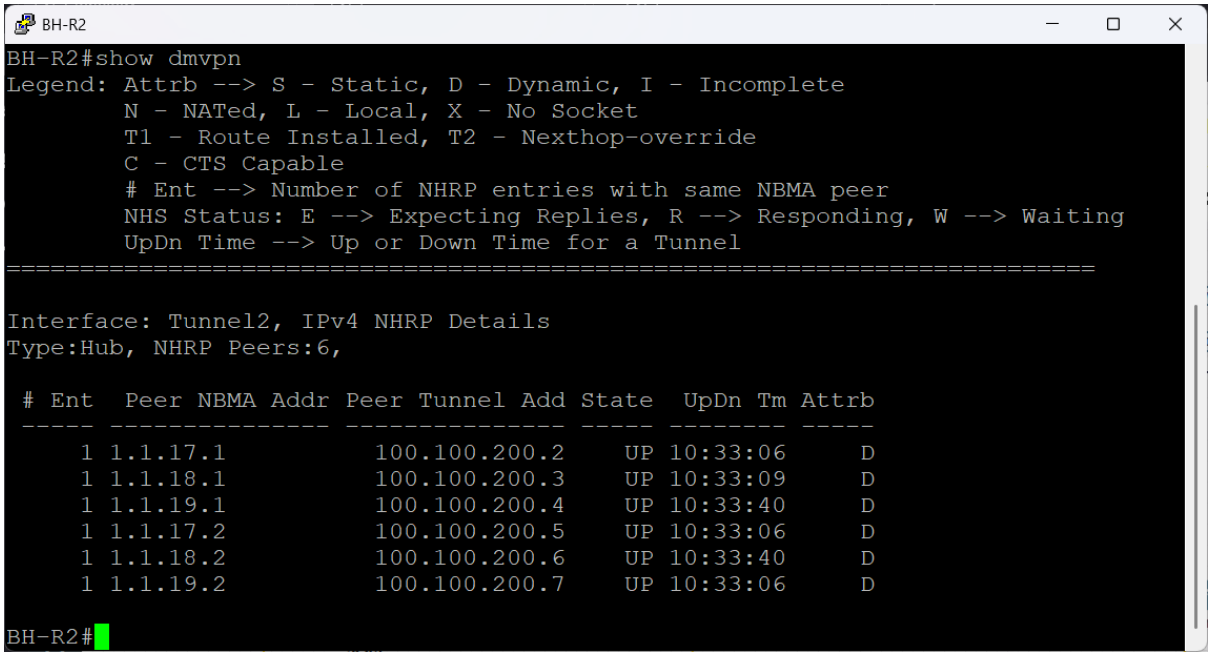

Figure 87 BH-R2 DMVPN Status Output

The figure below shows EN-R2 is a spoke with two DMVPN tunnels:

- Tunnel1 → Primary Hub (BH-R1)
- Tunnel2 → Backup/Secondary Hub (BH-R2)

DT1 shows:

- DMVPN Phase-3 dynamic shortcut
- EN-R2 received an NHRP redirect from the hub
- Then EN-R2 built a direct spoke-to-spoke tunnel
- Traffic between these sites no longer passes through the hub

D shows:

- Normal dynamic NHRP entry
- Usually the first stage before DT1 forms or when traffic hasn't triggered a shortcut yet

So EN-R2 is successfully:

- Talking to BH-R1 hub1
- Building direct adjacency tunnels to other spokes
- Running full Phase-3 behaviour

Tunnel 2 it is the backup DMVPN.

- Only one peer is expected (BH-R2)
- It is UP
- It becomes active when Tunnel1 or Hub1 fails

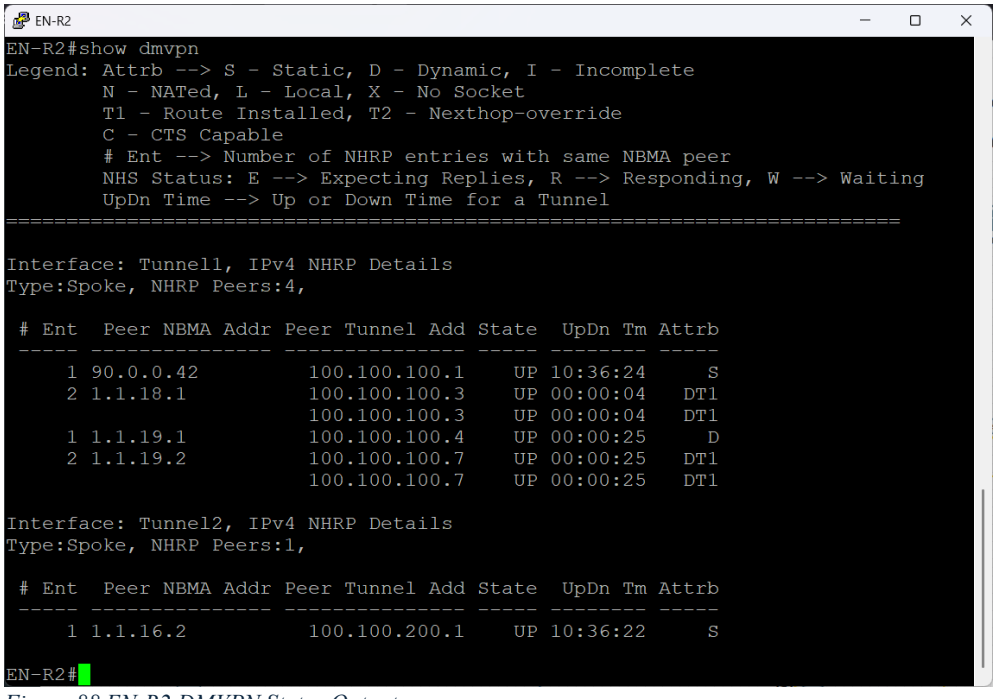

Figure 88 EN-R2 DMVPN Status Output

DMVPN NHRP Behavior

The figures below show a sample of each spoke registers its tunnel address with both hub routers using the NHRP. The hubs store these dynamic mappings and act as the authoritative NHS for the entire overlay.

A hub's NHRP table contains:

- Dynamic entries for all spokes
- NBMA addresses identifying the public/DMVPN transport source
- Correct tunnel endpoints
- State = UP for all peers
- Mode = dynamic

Each spoke contains:

- One static NHRP mapping to the hub
- Dynamic mappings for all other spokes
- DT1 flags, confirming Phase 3 shortcut capability
- S flag for the hub entry static

The implemented DMVPN Phase 3 solution operates:

- Hubs correctly maintain all NHRP registrations
- Spokes establish shortcut tunnels dynamically
- Dual-hub redundancy is functional
- EIGRP routing converges cleanly across the overlay
- No routing loops, no NHRP failures, no tunnel drops

This configuration provides a scalable, redundant, and fully optimized WAN for multi-site communication.

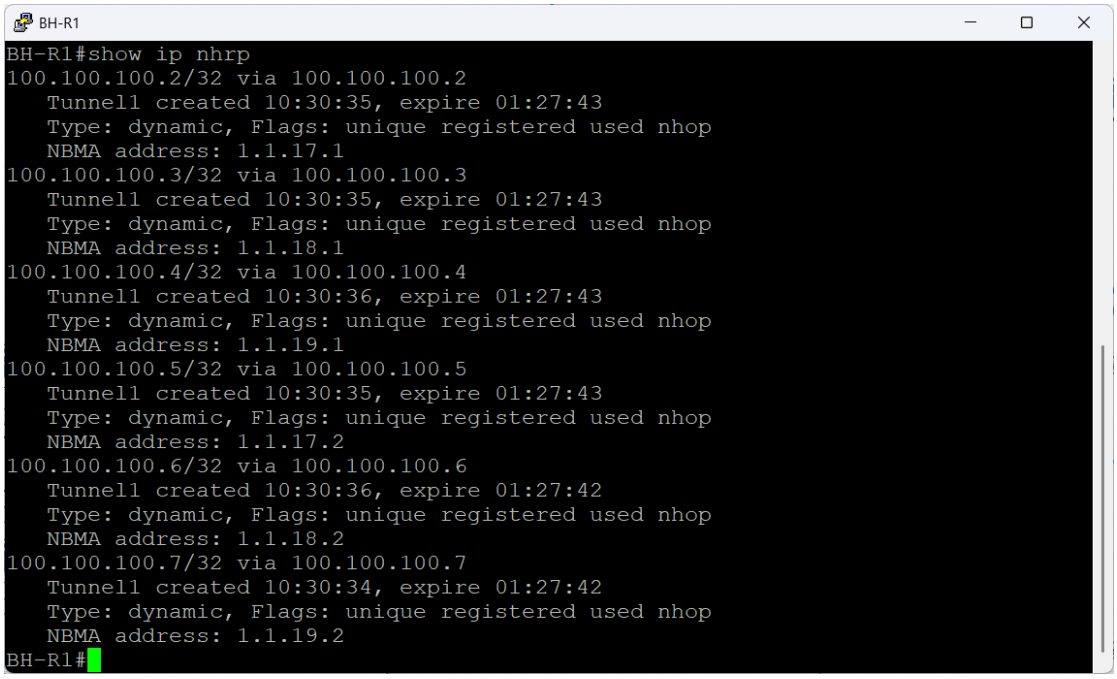

Figure 89 BH-R1 DMVPN NHRP Behavior

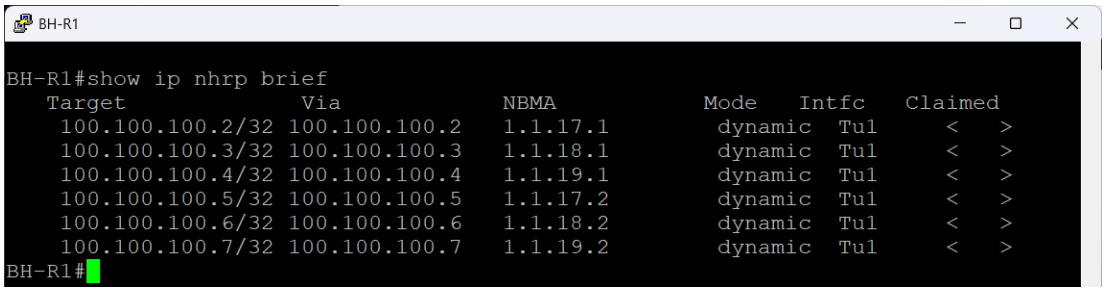

Figure 90 BH-R1 DMVPN NHRP Brief

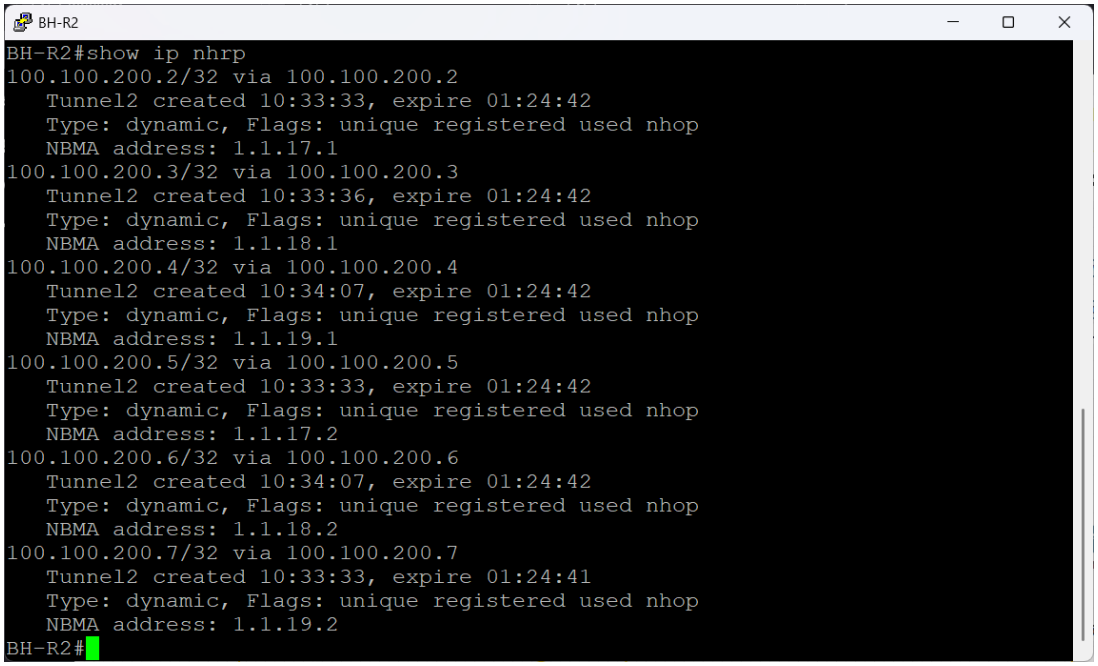

Figure 91 BH-R2 DMVPN NHRP Behavior

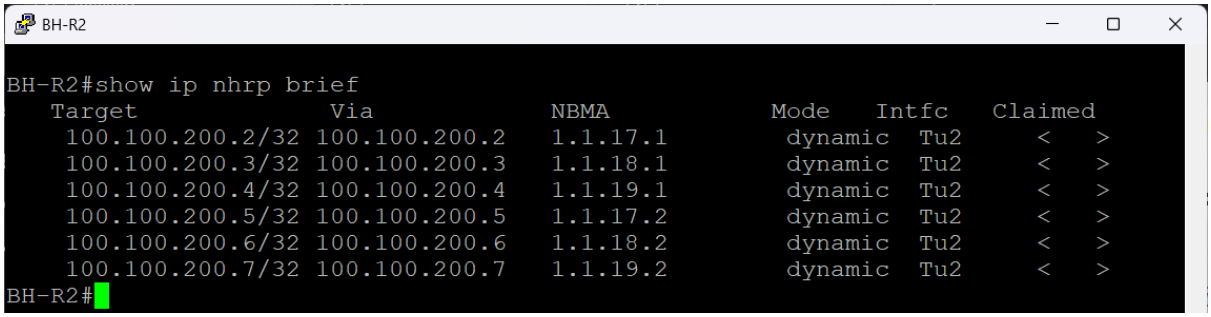

Figure 92 BH-R2 DMVPN NHRP Brief

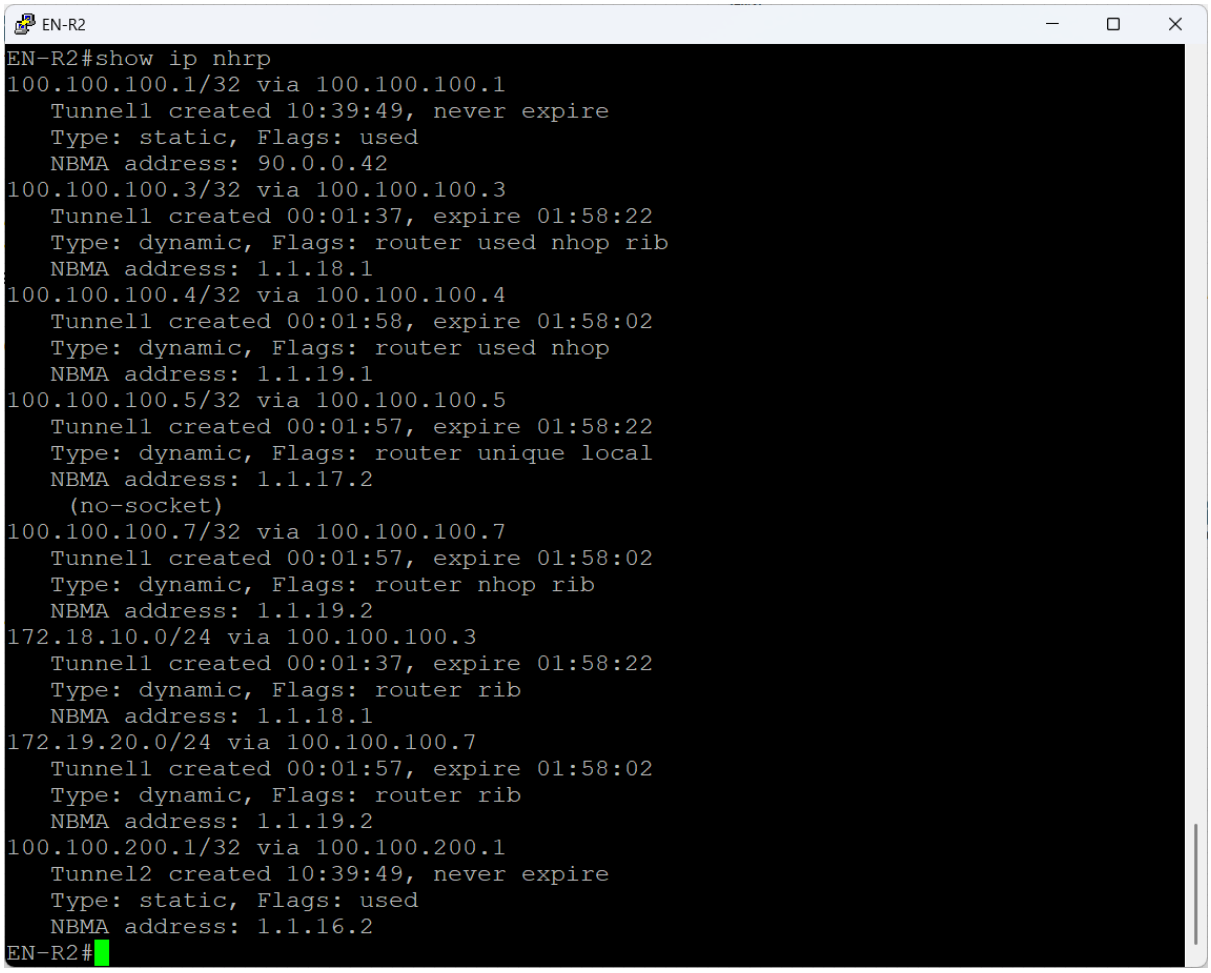

Figure 93 EN-R2 DMVPN NHRP Behavior

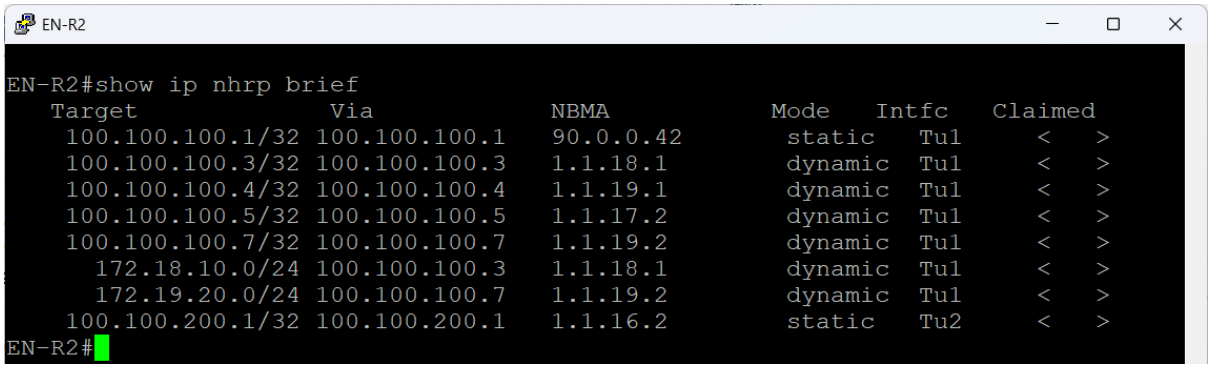

Figure 94 EN-R2 DMVPN NHRP Brief

DMVPN Tunnel Interface Verification

The figures below show interface tunnel command to confirm that every DMVPN tunnel in the GHN network is fully operational, correctly sourced, and protected by IPsec.

The outputs taken from BH-R1, BH-R2 and EN-R2 as a sample to prove five essential things:

- Tunnel State & Connectivity
- Correct Tunnel Addressing & Source
- GRE Characteristics:
  - multi-GRE confirms DMVPN Phase 3 operation.
  - MTU 1472 shows headroom for GRE & IPsec overhead, preventing fragmentation.
  - TTL 255 ensures end to end GRE reachability.
- IPsec Integration
- Traffic Counters Validate Active Forwarding

These outputs collectively validate that:

- DMVPN Phase 3 GRE tunnels are established correctly.
- NHRP, tunnel protection, and IPsec are functioning.
- Both hubs and all spokes are forwarding traffic without errors.
- Tunnel MTU, addressing, and source configuration are aligned with best practices.
- The dual-hub, dual-tunnel architecture is fully operational and stable.

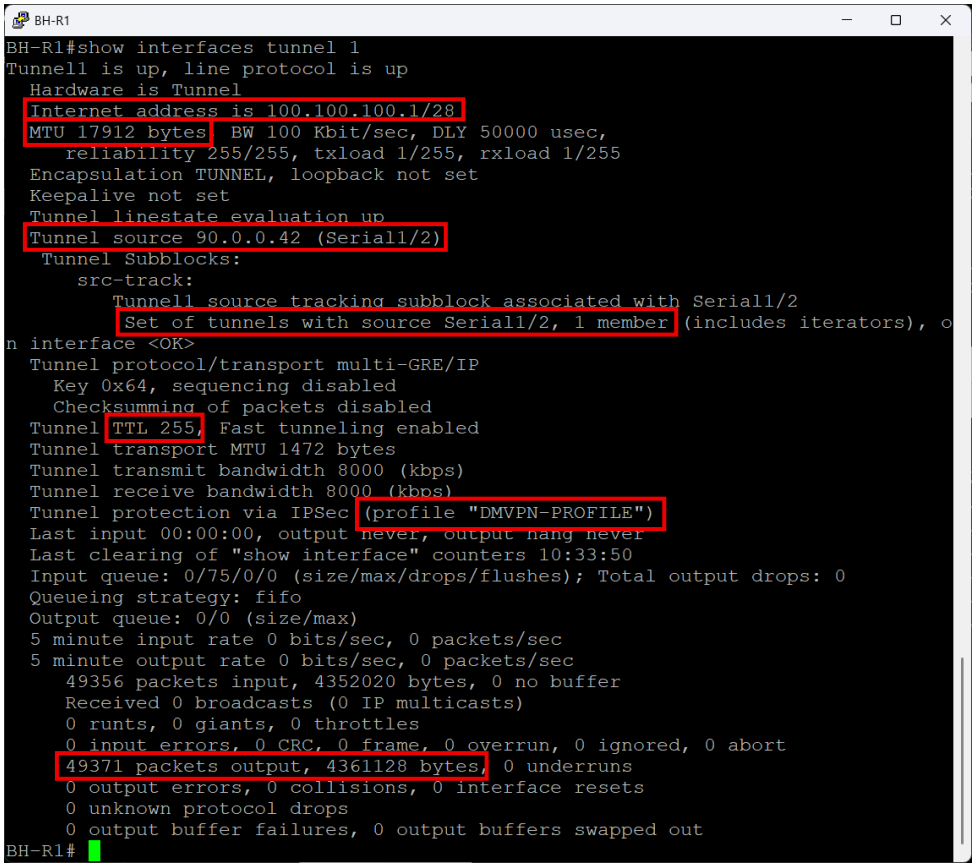

Figure 95 BH-R1 DMVPN Tunnel 1 Interface Verification

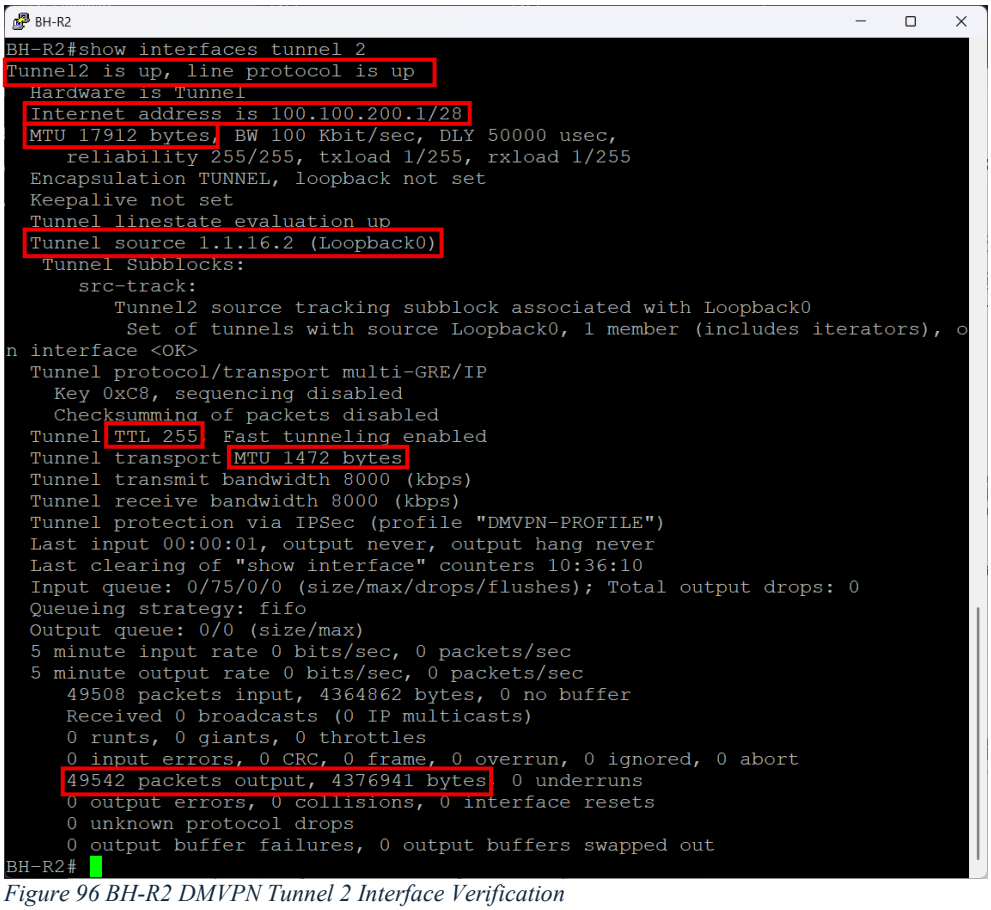

Figure 96 BH-R2 DMVPN Tunnel 2 Interface Verification

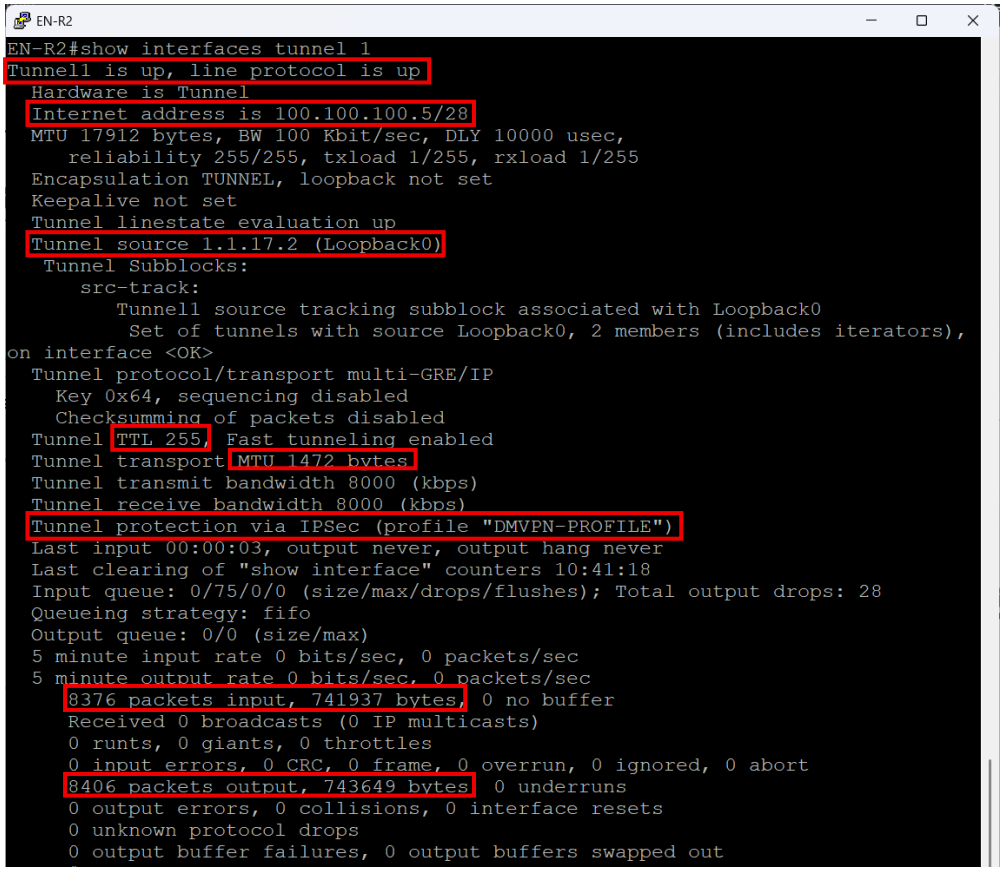

Figure 97 EN-R2 DMVPN Tunnel 2 Interface Verification

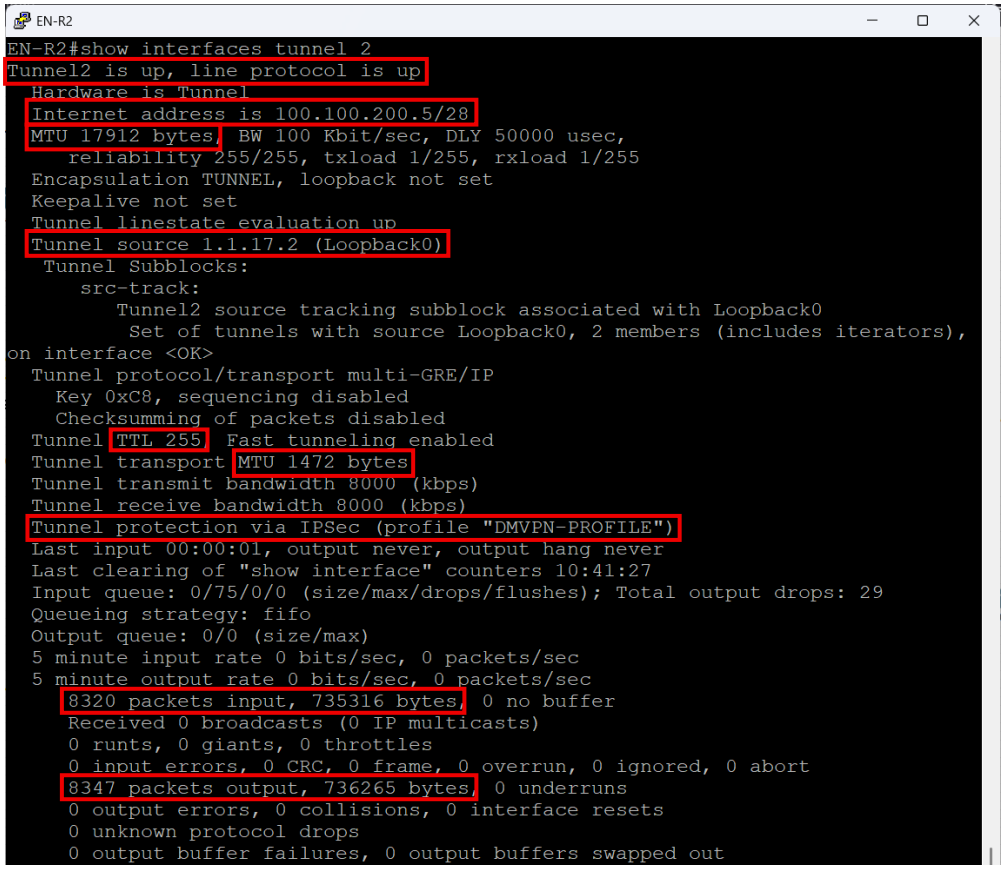

Figure 98 EN-R2 DMVPN Tunnel 2 Interface Verification

DMVPN Phase 3 Verification

The two figure below show a sample of how the DMVPN phase three is working for the first traceroute it goes to the hub and the second traceroute goes directly to the spoke that indicated of the shortcut form the spoke and the redirect form the hubs is doing their jobs and the H in the show ip route command represent that the next hop has been changed using the NHRP protocol as it should be.

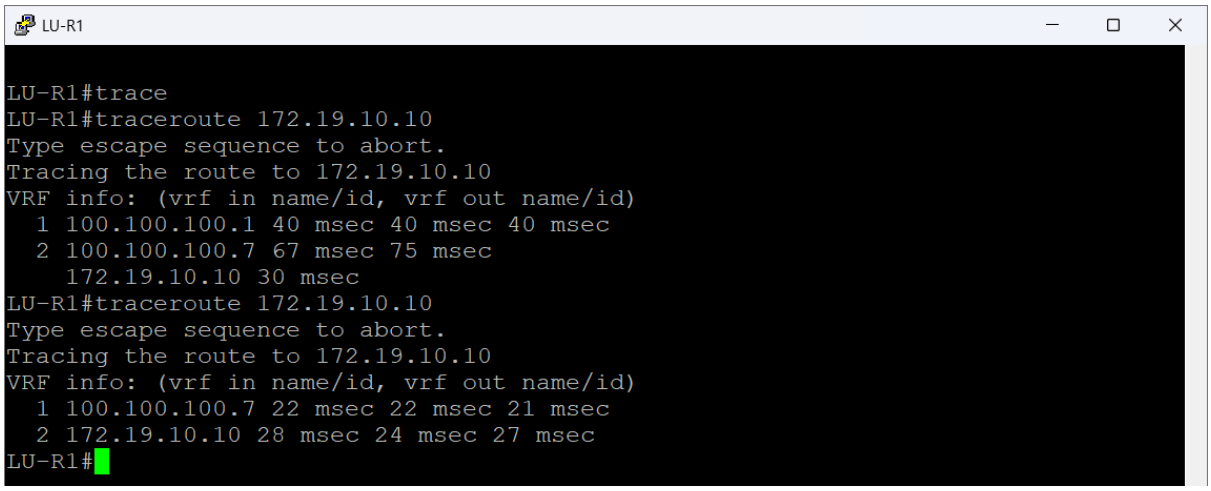

Figure 99 EN-R2 DMVPN Phase 3 verification

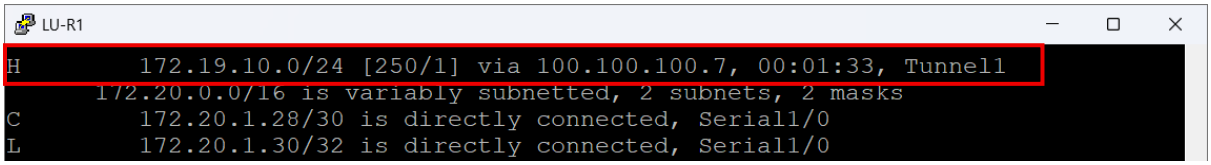

Figure 100 EN-R2 DMVPN Phase 3 verification

DMVPN Failover Verification

The below figure shows if one of the hubs goes down the other will take full control of the spokes and show a sample of a spoke LU-R2 routers that has the EIGRP of the DMVPN change all the next hop traffic from tunnel 1 to tunnel 2 that indicated the failover hubs is working as it should be.

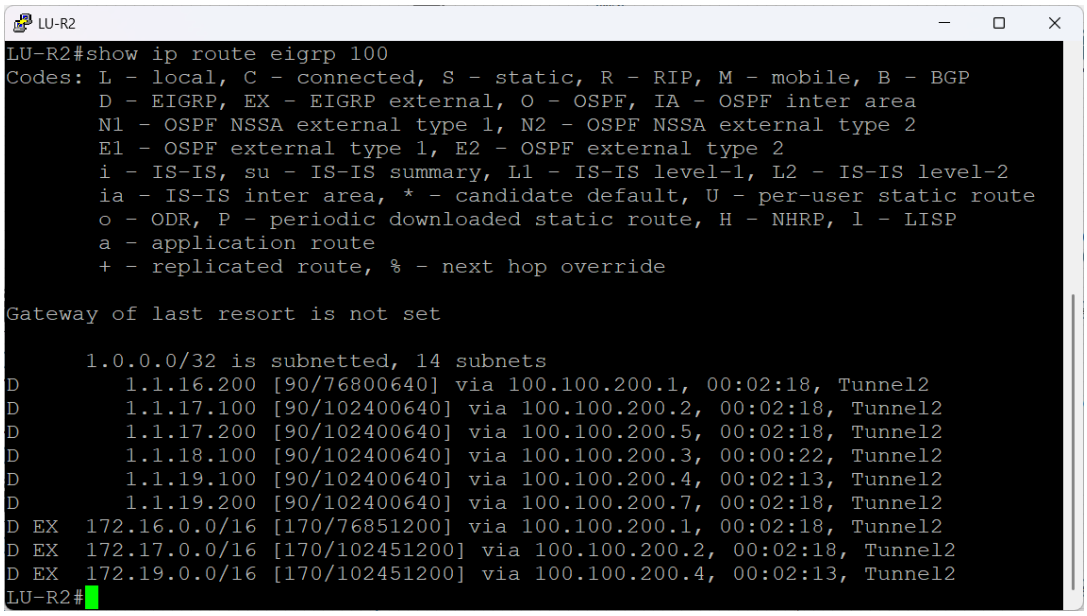

Figure 101 EN-R2 DMVPN Failover Verification

IPsec encryption Configuration

Each piece of data passing through the DMVPN tunnels between GHN sites is secured by IPsec encryption. IPsec guarantees confidentiality, integrity, and authentication for each packet sent over the WAN, while DMVPN offers the overlay and dynamic tunnelling. With established Security Associations and active encrypted traffic moving between the hubs and spokes, this part confirms that IPsec is not just enabled but fully functional. The verification outputs show that IKE negotiation was successful and verify to the DMVPN tunnels' end-to-end protection utilizing robust cryptographic parameters.

Each tunnel was secured using:

- AES-256 encryption
- SHA hashing
- DH 14
- Lifetime 3600 seconds

ISAKMP/IPsec Configuration

These below figures show the DMVPN IPsec Phase-1 and Phase-2 security configuration applied across the Bahrain BH-R1, BH-R2 hubs and a sample for a spoke, LU-R1. The configuration ensures that every DMVPN tunnel is protected with strong encryption, authentication, and integrity, forming a secure overlay across the public and ISP networks

A single crypto isakmp key statement for every remote neighbor is included in each router. In a lab setting, this manual pre-shared key method ensures that each DMVPN node has a matching key for every other node. While LU-R1 specifies both hub addresses in addition to all other spokes for complete Phase-1 reachability, BH-R1 and BH-R2 list all spoke public IPs.

The Phase-2 protection for GRE-encapsulated DMVPN traffic is defined by the transform-set. In this case, ESP-SHA-HMAC ensures integrity while ESP-AES-256 encrypts the packets. Since the GRE header is located outside of the IPsec encryption, the mode is set to transport, which is the proper architecture for DMVPN.

In the end, the transform-set is bound to DMVPN by the IPsec profile. Every GRE packet is automatically encrypted and authenticated before leaving the router due to the application of this profile under each Tunnel interface. A completely encrypted multipoint DMVPN network with equal crypto settings throughout all hubs and spokes is the result.

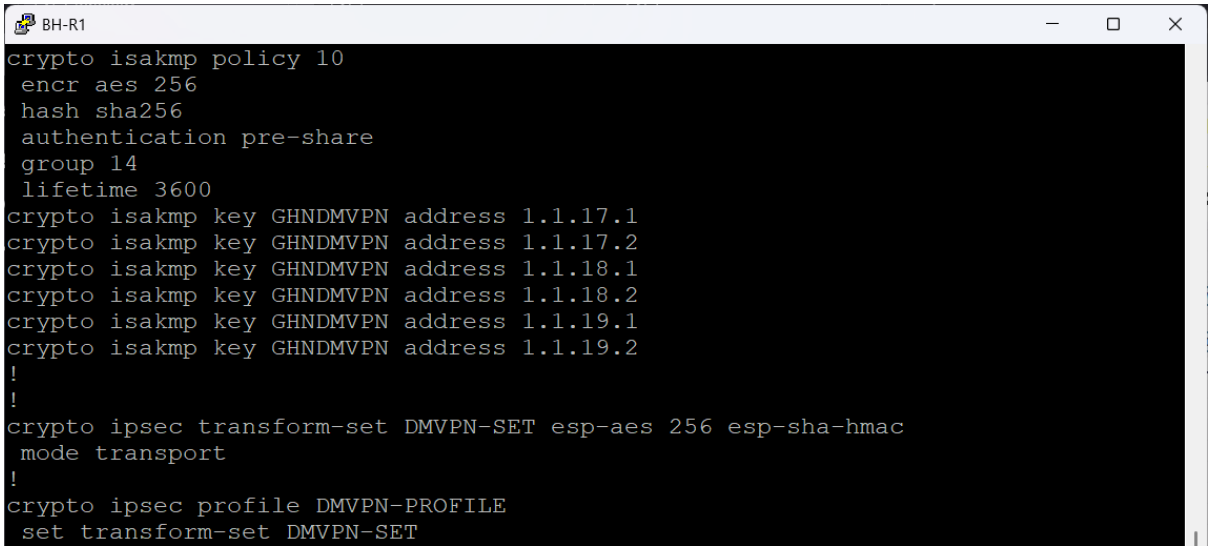

Figure 102 BH-R1 ISAKMP/IPsec Configuration

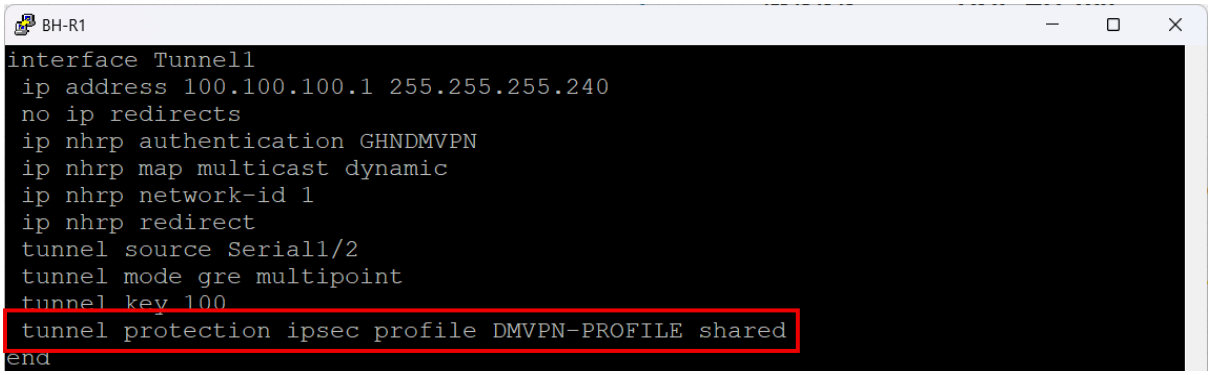

Figure 103 BH-R1 IPsec tunnel 1 Configuration

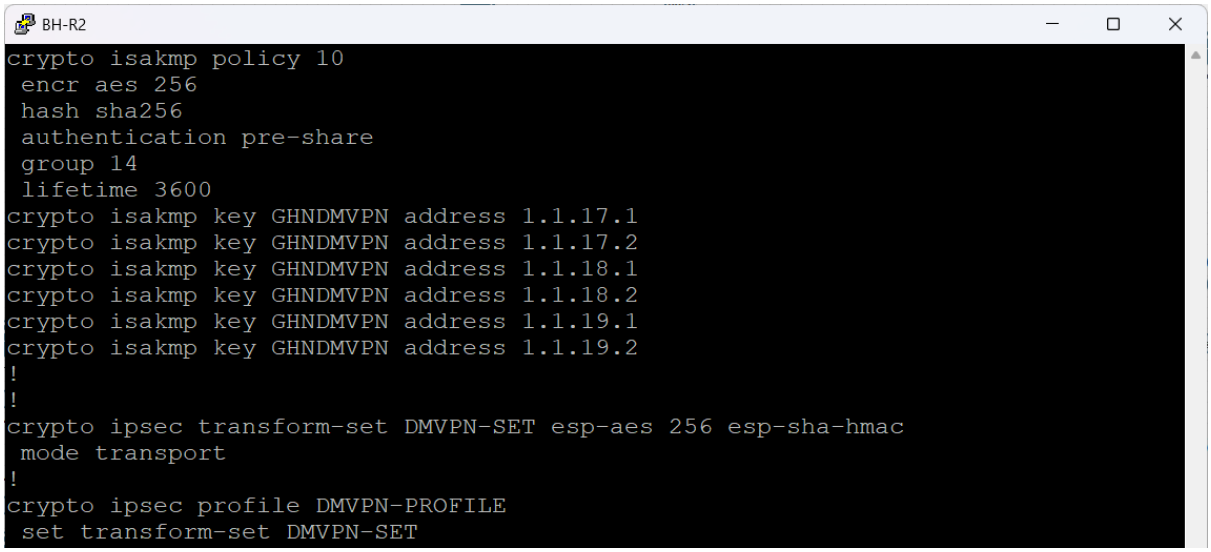

Figure 104 BH-R2 ISAKMP/IPsec Configuration

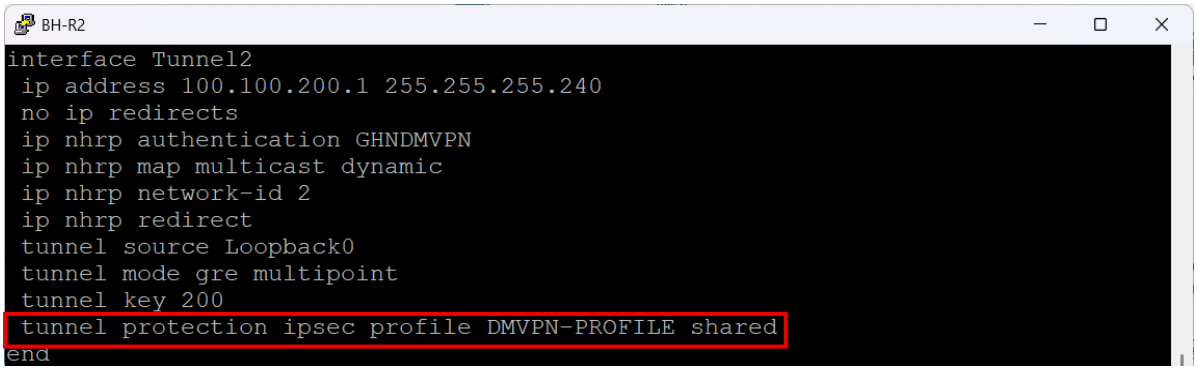

Figure 105 BH-R2 IPsec tunnel 2 Configuration

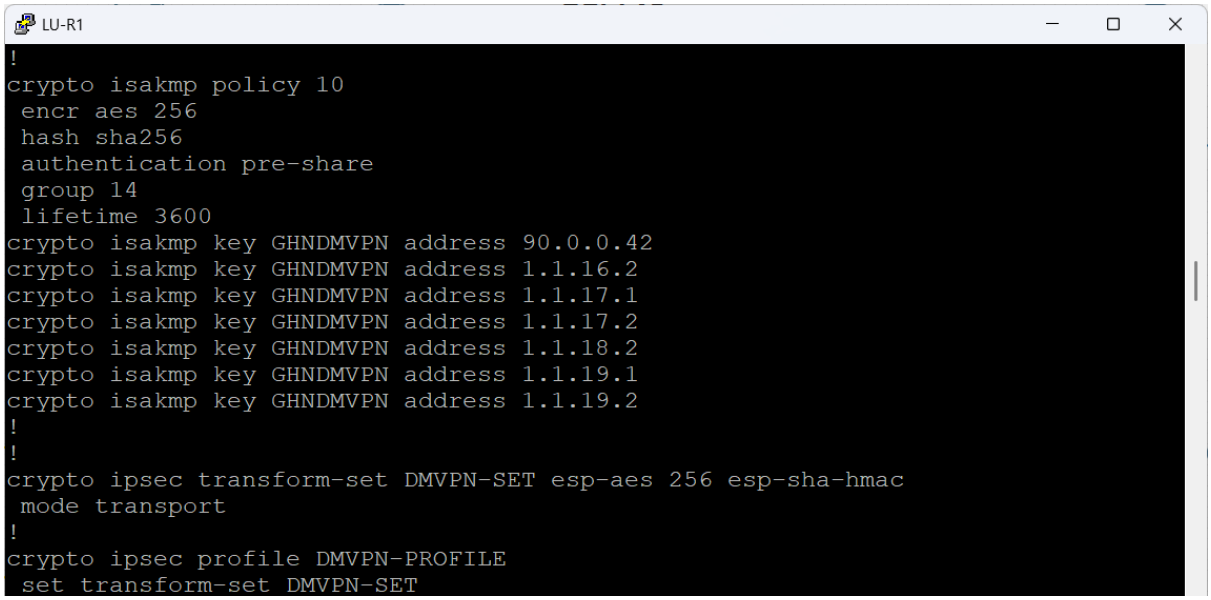

Figure 106 LU-R1 ISAKMP/IPsec Configuration

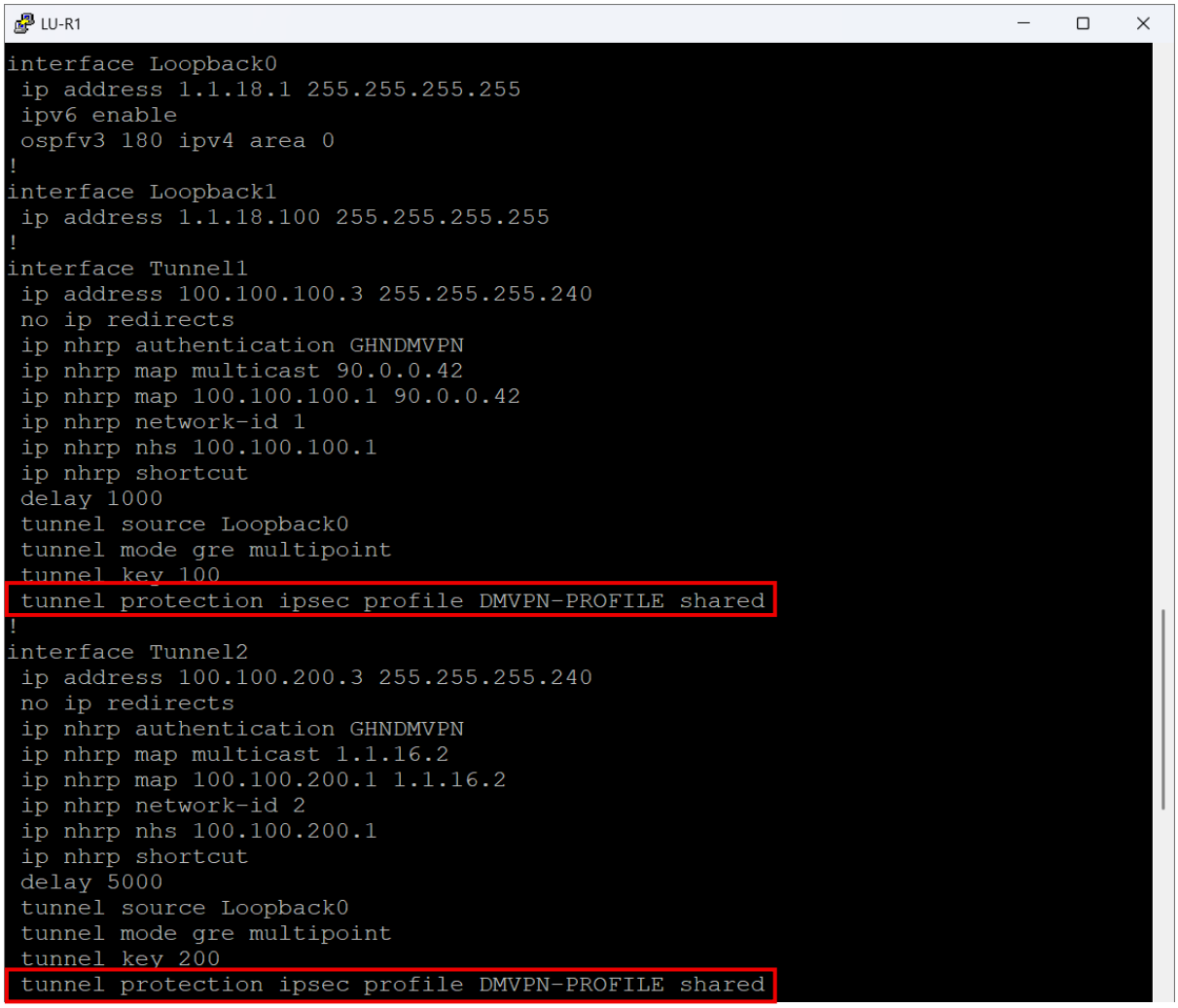

Figure 107 LU- R1 IPsec tunnel 1&2 Configuration

ISAKMP SA Verification

BH-R1 displays a solid DMVPN hub. Each spoke on the router has an active ISAKMP SA. Every session appears in QM_IDLE, indicating that the SA is always prepared to traffic encrypted and that Phase-1 and Phase-2 are both operational and stable. The existence of several ACTIVE sessions verifies that all remote spokes can access the hub and that all devices have the same pre-shared keys and ISAKMP parameters.

There are no active ISAKMP sessions on the secondary hub, BH-R2. In a dual-hub configuration, where the second hub serves as a backup, this is typical. Only when BH-R1 is inaccessible or when traffic specifically passes through the secondary tunnel will spokes initiate ISAKMP sessions with BH-R2. In line with the expected failover behaviour, the empty output verifies that BH-R2 is not presently being used as a termination destination.

The sample spoke router, LU-R1, displays active SAs for every DMVPN node it connects to. The state QM_IDLE, like BH-R1, signifies that Phase-1 is finished, the negotiation was successful, and the tunnel is prepared for encrypted GRE/DMVPN traffic. This validates that the spoke is appropriately forming secure sessions with the hub and other spokes when needed, as well as its crypto setup is valid and balanced.

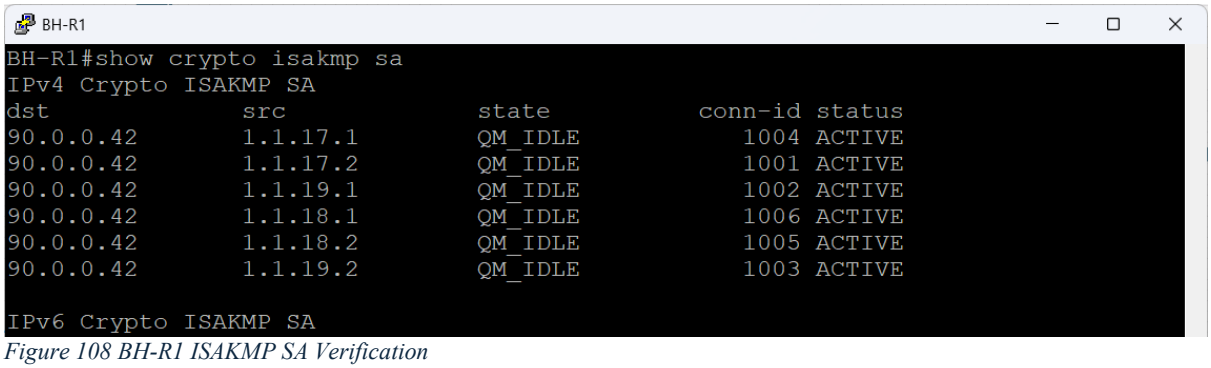

Figure 108 BH-R1 ISAKMP SA Verification

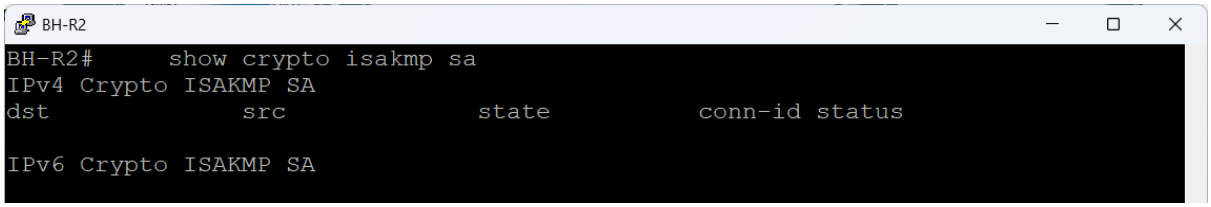

Figure 109 BH-R2 ISAKMP SA Verification

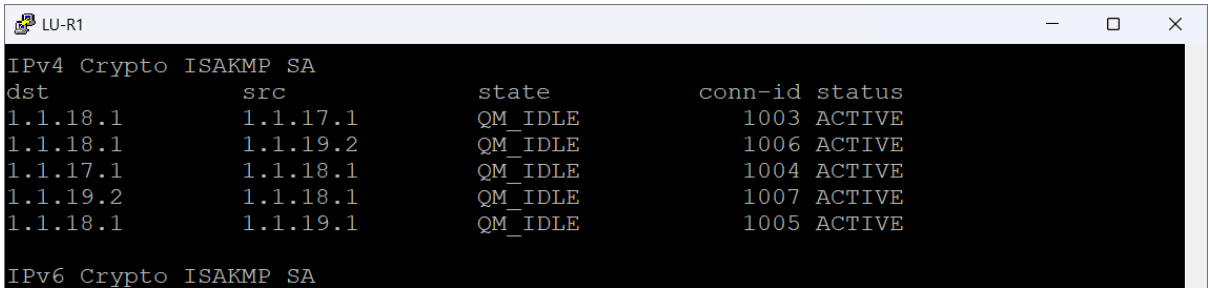

Figure 110 LU-R1 ISAKMP SA Verification

IPsec SA Verification

The following numbers verify that DMVPN traffic is, in truly, encrypted and decrypted over IPsec tunnels. Although Phase-1 only displays the security of the control plane, this output demonstrates that the data plane is completely functional.

On BH-R1 and BH-R2, counts for encaps, encrypt, decaps, and decrypt increase consistently. This indicates that traffic from the spokes is being actively processed by the hubs. Following decryption and verification, each packet originating from a spoke is routed via the DMVPN hub. There is no packet loss or crypto failure because the encrypt/decaps numbers match.

The spoke router LU-R1 displays the same behavior, however on a lesser scale. The numbers are low before traffic is sent. The IPsec SA displays activity as soon as the router pings an internal destination (172.17.10.10).
While the ping is running, the #pkts encrypt and #pkts decrypt values rise in real time.
This is the purest evidence that:

1) DMVPN GRE packets are entering the IPsec profile.
2) IPsec is successfully encrypting outbound traffic toward the hub.
3) The hub is returning encrypted packets.
4) The spoke is correctly decrypting and validating every packet.

The recent increase in digest and verify counters attests to the flawless operation of ESP-SHA-HMAC integrity checks. A stable DMVPN/IPsec deployment should exhibit no drops, failures, or compression failures.

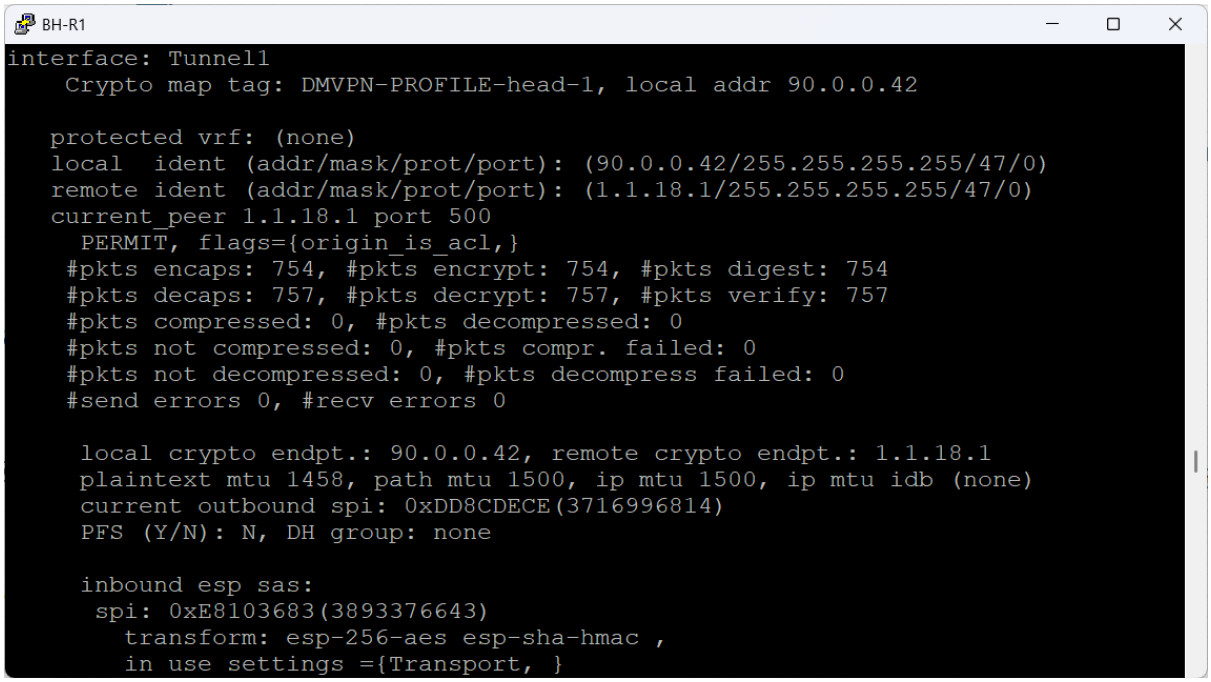

Figure 111 BH-R1 IPsec SA Verification

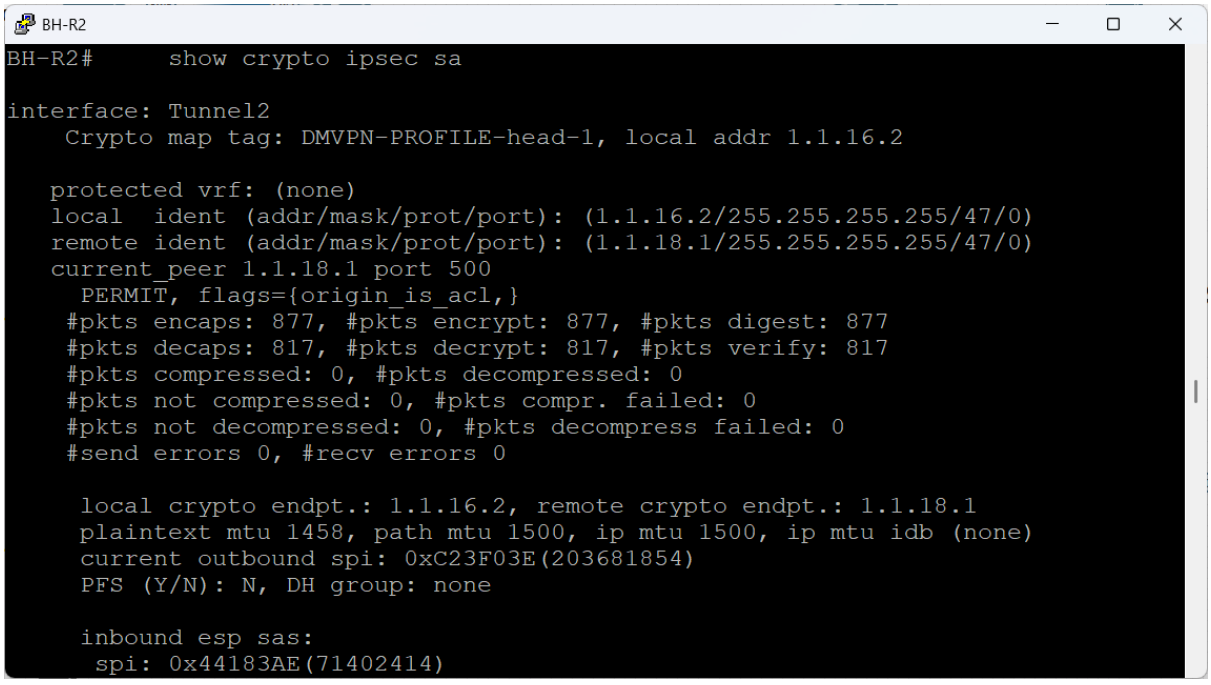

Figure 112 BH-R2 IPsec SA Verification

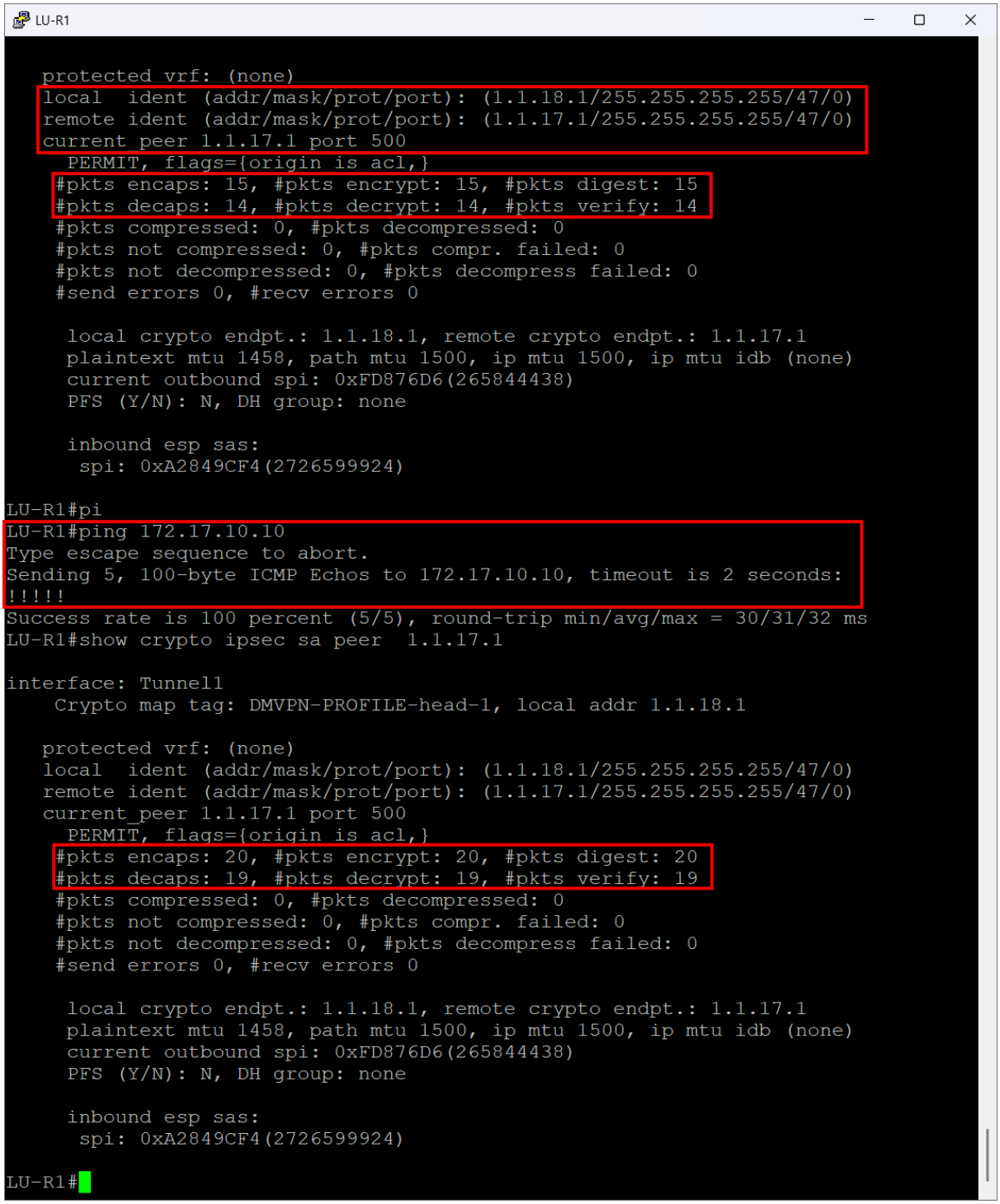

Figure 113 LU-R1 IPsec SA Verification

LAN Implementation

The key switching tasks used are covered in this section. The network was divided into VLANs, and L3 SVIs were used to facilitate inter-VLAN routing so that each VLAN could connect to its layer 3 router gateway. To secure the switching domain against frequent attacks and setup errors, L2 security rules were implemented all the fingers show below is a sample for the GHN.

VLAN Configuration

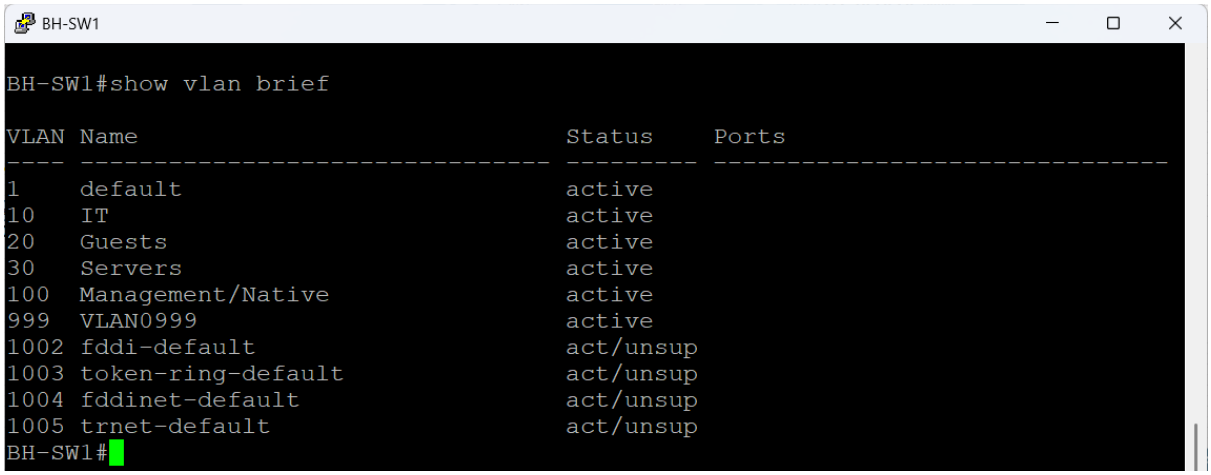

Figure 114 BH-SW1 VLAN Configuration

The figure above shows the VLAN segmentation used on BH-SW1 as a sample figure, which offers virtual traffic separation within the Bahrain branch. A functional department or a particular security zone is represented by each VLAN.

VLANs	
Vlan Name	Vlan Number
IT	10
Guests	20
Servers	30
Management/Native	100
Unused Ports	999

Table 3 Vlan Table

the table shows the vlan name with it representing numbers ensuring that end user devices, guest clients, and server infrastructure are isolated at Layer 2. VLAN 100 is used as the

management/native VLAN, allowing controlled switch and AP management traffic without mixing it with user data. VLAN 999 is configured as the black hole or unused VLAN, following security best practices to prevent unauthorized access on unused switch ports.

The output confirms that all production VLANs are active and operational.

VTP Configuration

As an example for GHN branches, these figures below show the VTP configuration for Bahrain access-layer switches. In order to provide consistent VLAN management throughout the branch, the switches are grouped under the same VTP domain, Bahrain.

BH-SW1 is the main device in charge of generating, changing, and storing VLAN data since it is running in VTP Server mode. All switches inside the domain automatically receive any VLAN modifications performed on BH-SW1. The configuration revision number attests to the proper tracking and synchronization of updates.

The exact same VTP password, bahrain@vtp, is used by both switches to stop unwanted devices from introducing false VLAN information into the network. Those switches that are authorized can take part in VLAN distribution thanks to VTP verification. The VTP domain name and password are displayed in the table below:

VTP	
VTP Domain	VTP Password
Bahrain	bahrain@vtp
England	england@vtp

Table 4 VTP Table

Because BH-SW2 to BH-SW4 are in VTP Client mode, they are unable to establish or alter VLANs locally. Rather, it downloads every piece of VLAN data from the server. This arrangement lowers the possibility of a mistake, streamlines management, and ensures consistent VLAN configuration throughout the branch.

All things taken into account, these results verify that the Bahrain switching environment employs a centralized VLAN management model: BH-SW1 manages the VLAN database,

whereas BH-SW2 to BH-SW4 and further downstream switches function as synchronized clients protected by VTP verification.

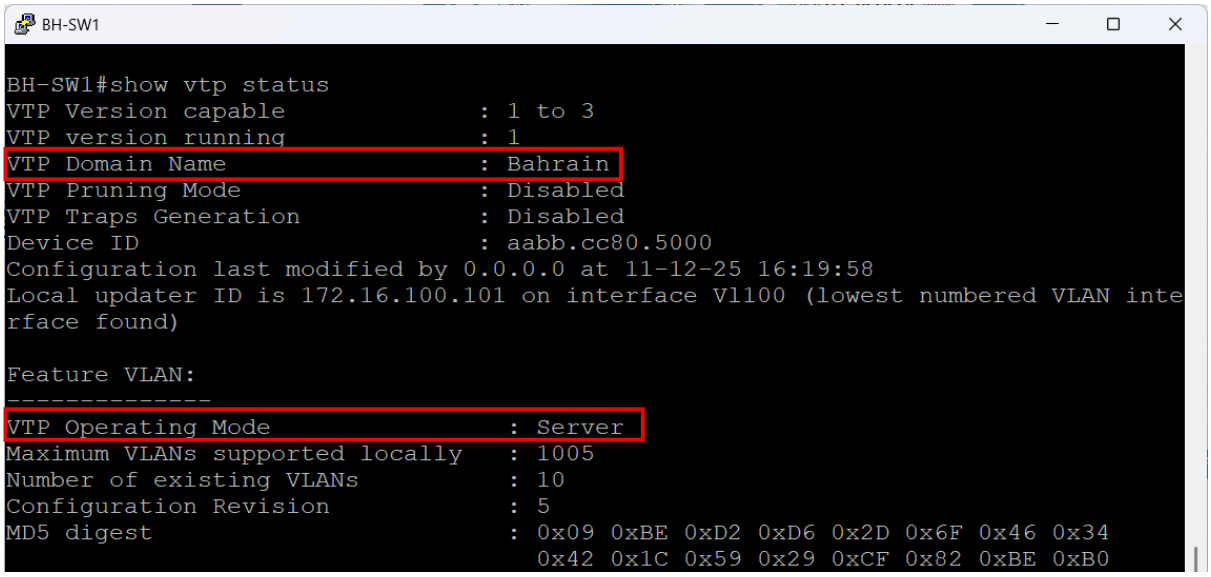

Figure 115 BH-SW1 VTP Configuration

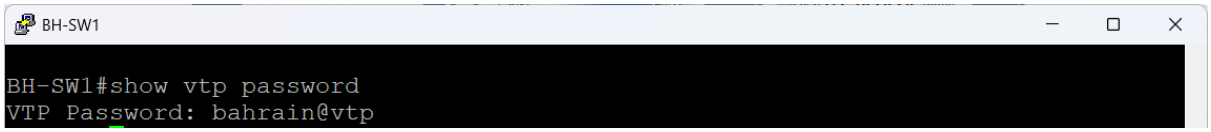

Figure 116 BH-SW1 VTP Password Configuration

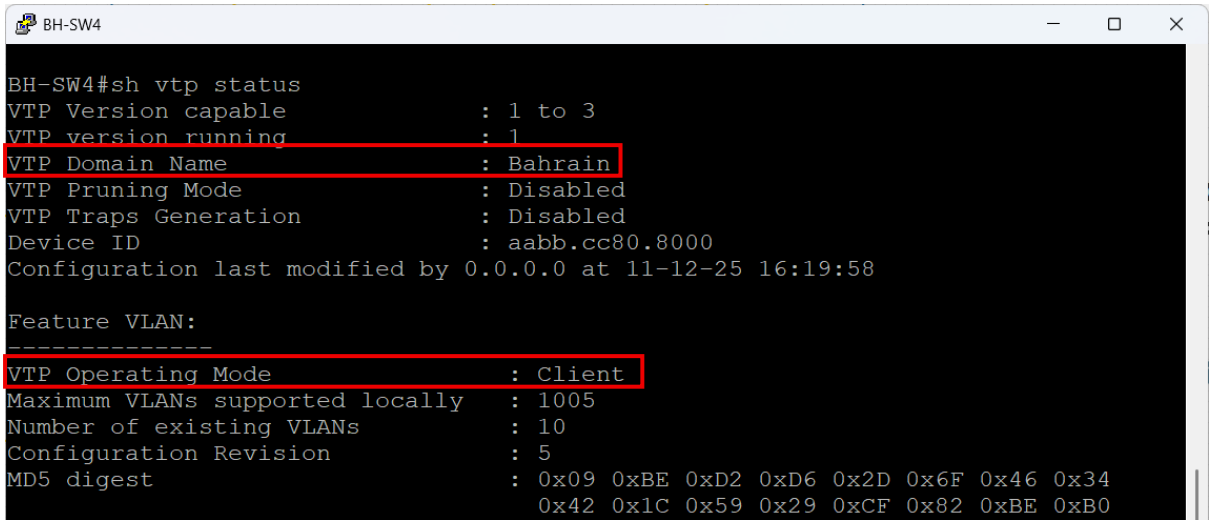

Figure 117 BH-SW4 VTP Configuration

Figure 118 BH-SW4 VTP Password Configuration

Trunk Interface verification

The inter-switch links in the Bahrain LAN as a sample are correctly functioning as IEEE 802.1Q trunks, allowing different VLANs to communicate between the switches, as shown in the two figures below. To match the management/native VLAN established throughout the site and avoid mismatched-native warnings, all trunk interfaces utilize VLAN 100 as the native VLAN.

All VLANs (1–4094) are permitted on each trunk, according to the "VLANs allowed on trunk" section. However, the active VLANs are those that were formed and distributed via VTP: 10 (IT), 20 (Guests), 30 (Servers), 100 (Management), and 999 (Unused/Blackhole).

These VLANs are present in the local VTP domain and have been transmitted over the trunk links without being cut down as demonstrated by the "allowed and active" part.

The spanning-tree section confirms that the VLANs on this list are in the forwarding state, which indicates that they are actively taking part in Layer 2 forwarding and that there are no STP blockages brought on by loops or incorrect configurations. Because VLAN 999 is designated for unused ports and is not intended for user traffic, it only shows when necessary.

In general, the result verifies that all pertinent Layer-2 segments may communicate between switches without any STP conflicts or pruning, trunking is consistent between BH-SW1 and BH-SW3, and VLAN propagation is operating through VTP.

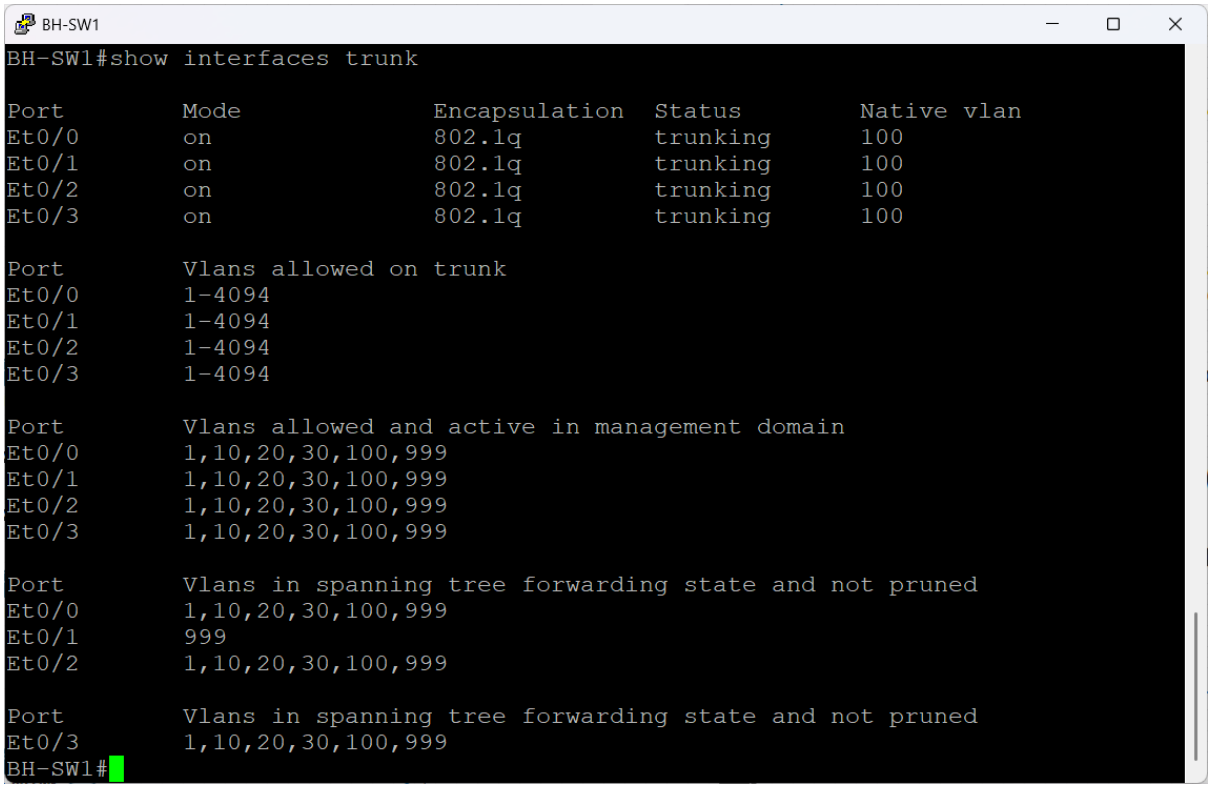

Figure 119 BH-SW1 Trunk Interface verification

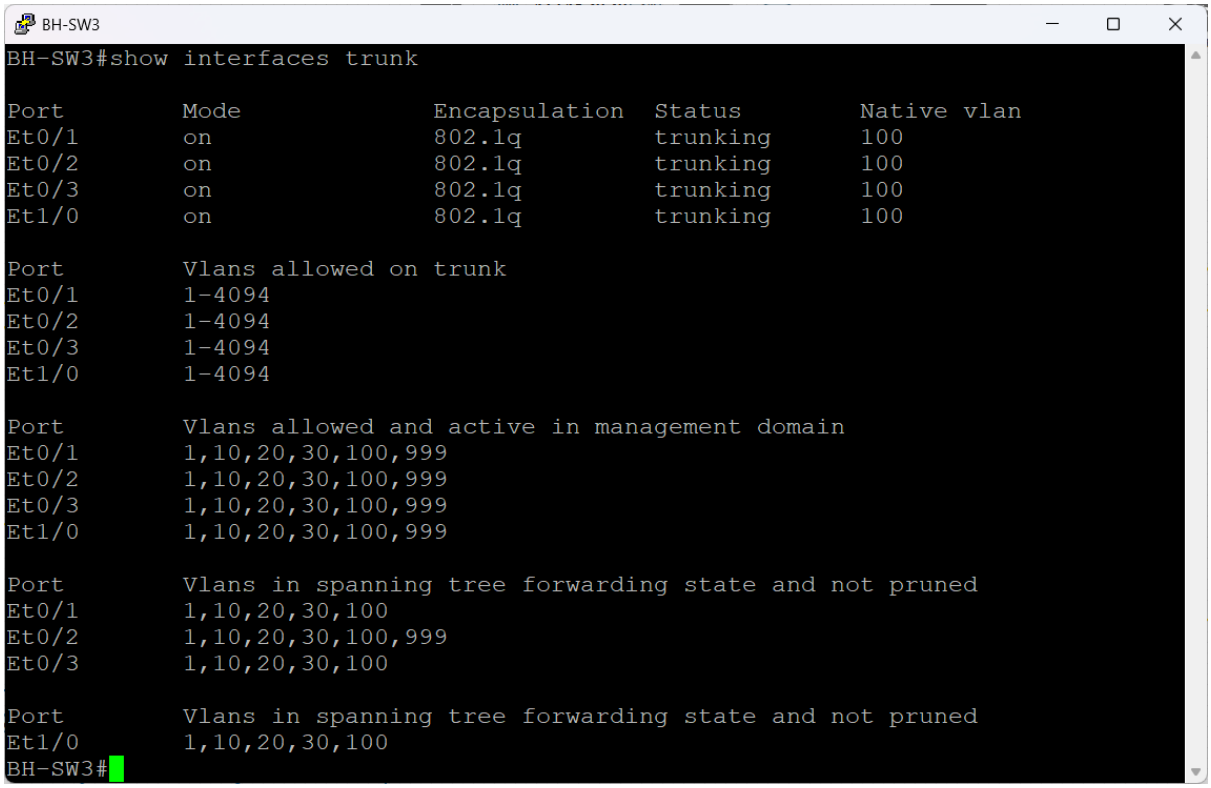

Figure 120 BH-SW3 Trunk Interface verification

Inter-VLAN Routing

In order to enable devices in different VLANs to connect with one another while preserving logical separation of the network, inter-VLAN routing is used. Since each VLAN functions as a separate broadcast domain, many GHN services and applications need traffic to flow between the user, server, and administrative networks. By forwarding packets between VLANs according to their designated IP subnets, inter-VLAN routing enables this communication. The GHN infrastructure's Inter-VLAN routing configuration and verification are described in this section.

Inter Vlan & HSRP configuration

A traditional router on a stick design is used for inter-VLAN routing at the Bahrain branch that shows as a sample. All VLANs are terminated by BH-R3 and BH-R4 via sub interfaces, each of which is marked with the proper 802.1Q encapsulation. The IT, Guest, Server, and Management networks use these sub-interfaces as their Layer 3 gateways.

While HSRP offers a shared virtual gateway (.254), the router itself offers a real IP address within each VLAN. End devices point to the virtual IP and are unaware of which actual router is in use. While BH-R3 is active, it manages all routing between VLANs IT to servers, Guests to internet-only, and Management to infrastructure. In the event that the active router fails, BH-R4 is prepared to take over right away.

Within the switch, traffic that enters a VLAN is tagged and sent to the router via the trunk link. The router uses the virtual gateway's routing logic to send the packet out toward the destination VLAN after it reaches the correct sub interface and completes the Layer-3 lookup. This minimizes broadcast domains, maintains centralized routing, and guarantees uniform policy enforcement over all internal networks.

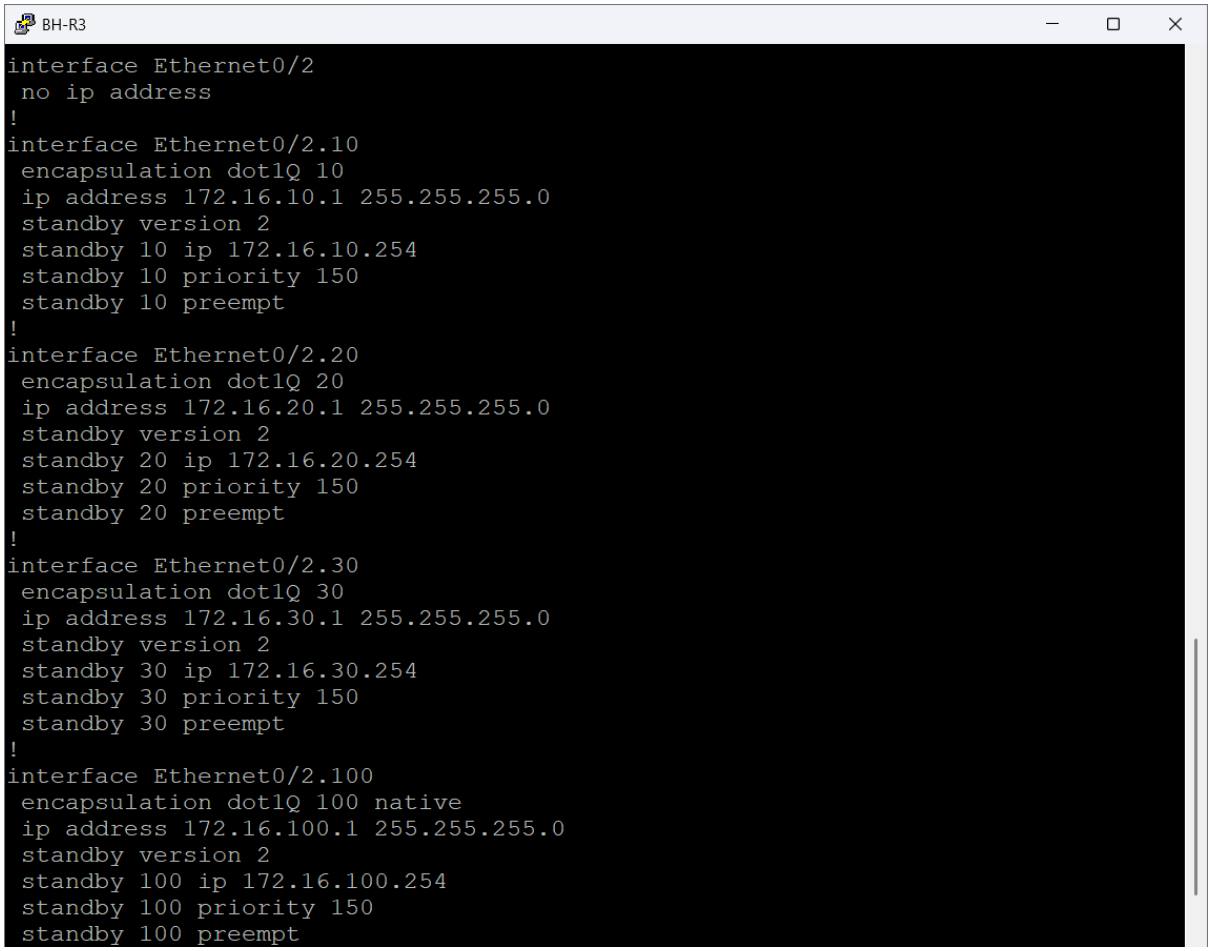

Figure 121 BH-R3 Inter Vlan & HSRP configuration

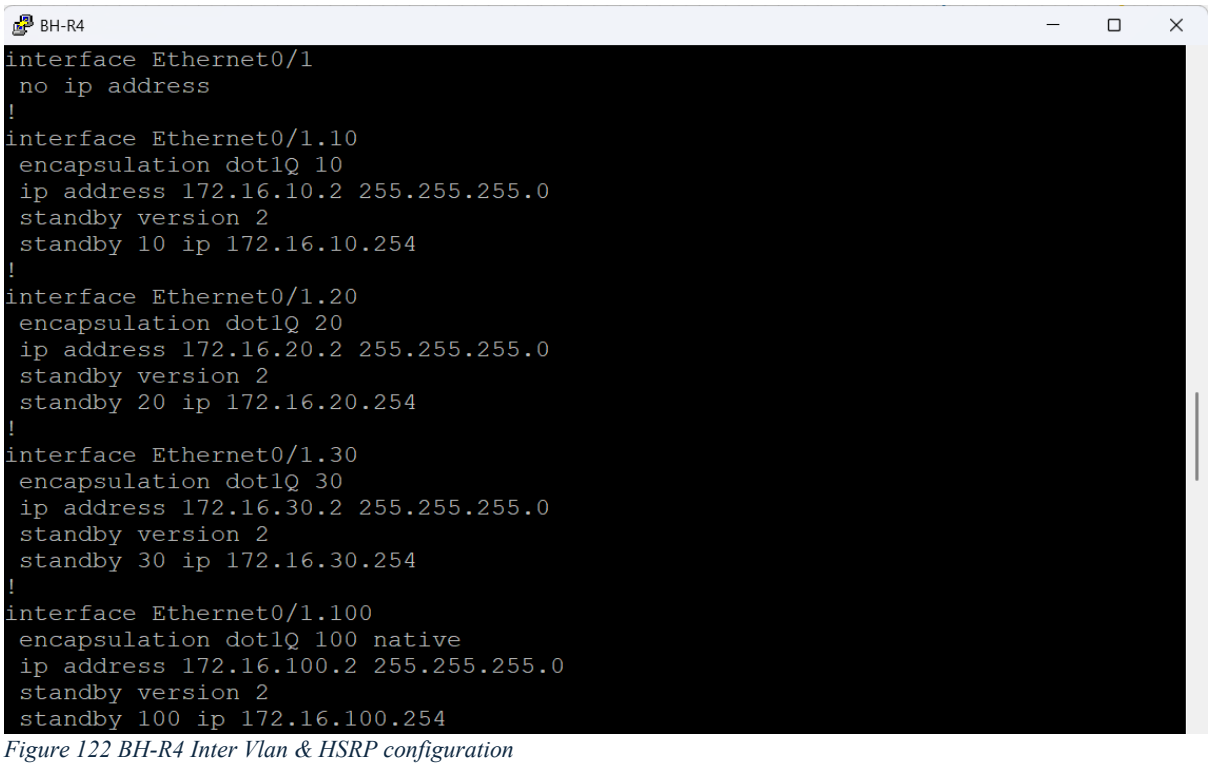

Figure 122 BH-R4 Inter Vlan & HSRP configuration

Access Layer and Trunk Configuration

The configuration of the Bahrain access layer switches as an example for VLAN segmentation, uplink trunking, and secure user access is depicted in the following pictures. VLANs 10, 20, 30, and 100 are carried toward the distribution routers via all uplink interfaces, which are set up as 802.1Q trunks. In order to minimize mismatched native VLAN problems and to align with the management network throughout the site, the native VLAN is continuously set to VLAN 100.

Strong Layer 2 security is applied to user-facing interfaces on BH-SW2. To remove any possibility of illegitimate physical connections, unused ports are administratively shut off and allocated to VLAN 999. Active access ports use sticky MAC learning and a five-device cap to ensure port security. This shields the network from simple Layer-2 assaults, unauthorized device movement, and MAC spoofing. The sticky MAC table is periodically refreshed by an aging timer to prevent stale entries and maintain a clean setup.

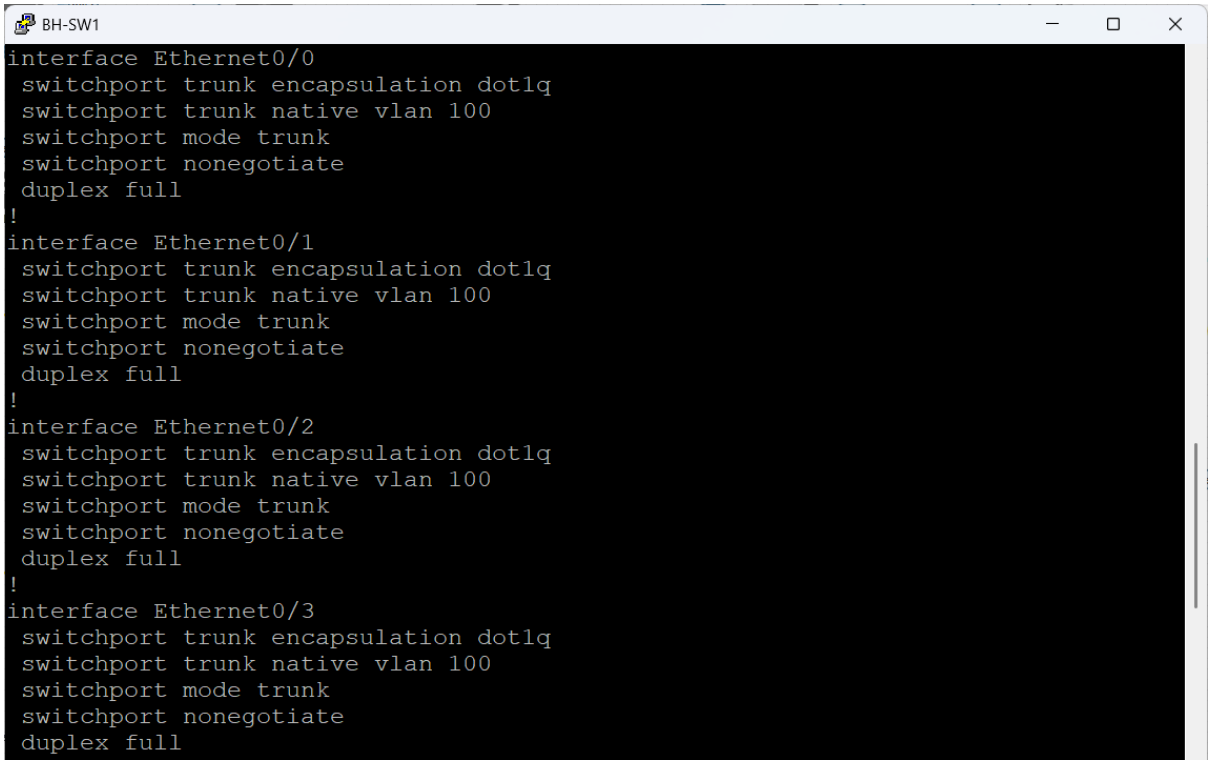

Figure 123 BH-SW1 Access Layer and Trunk Configuration

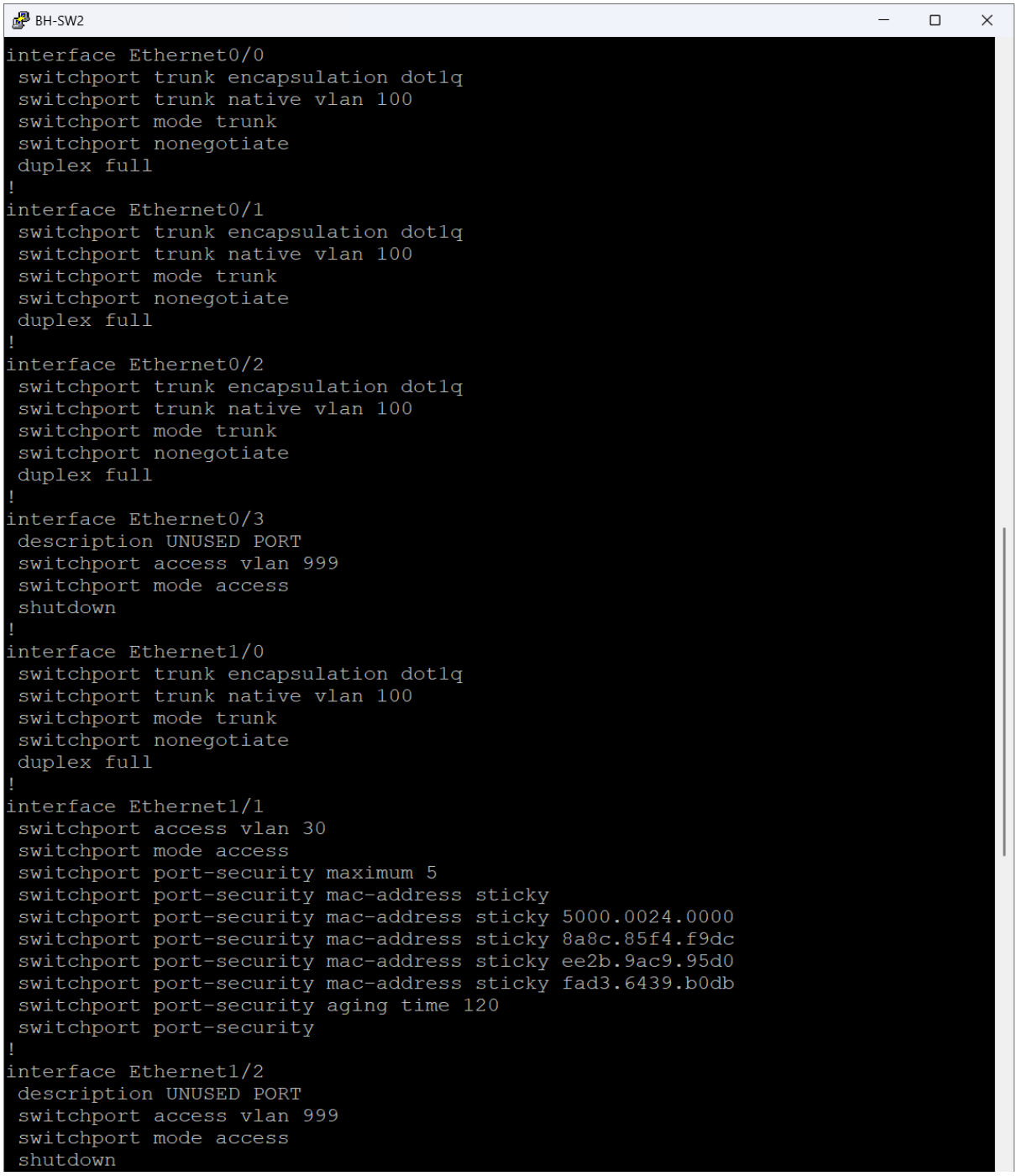

Figure 124 BH-SW2 Access Layer and Trunk Configuration

HSRP Gateway Redundancy verification

The results below confirm that HSRP is operating properly in every VLAN in the Bahrain branch. For all VLANs (10, 20, 30, and 100), BH-R3 is the active gateway. Because preempt is enabled and its priority is set to 150, it always assumes the active role whenever it becomes available. All end hosts use its virtual gateway IP addresses, which terminate in.254, as their default gateway.

The setup is mirrored by BH-R4, however it uses the default HSRP priority of 100. As anticipated, it shows up in the standby status for VLANs 10, 20, and 30, prepared to take over right away in the event that BH-R3 fails. As expected, VLAN 100 shows it as active. This offers straightforward load allocation, with BH-R3 managing user and server VLANs and BH-R4 managing administrative traffic.

The standby brief output confirms:

• The virtual gateway addresses are correctly configured.

• Each router understands its role (Active or Standby).

• Preemption is enabled where required to enforce deterministic failover.

This validates that the branch gateway design provides seamless redundancy, zero-touch failover, and balanced handling of internal traffic without interrupting end users.

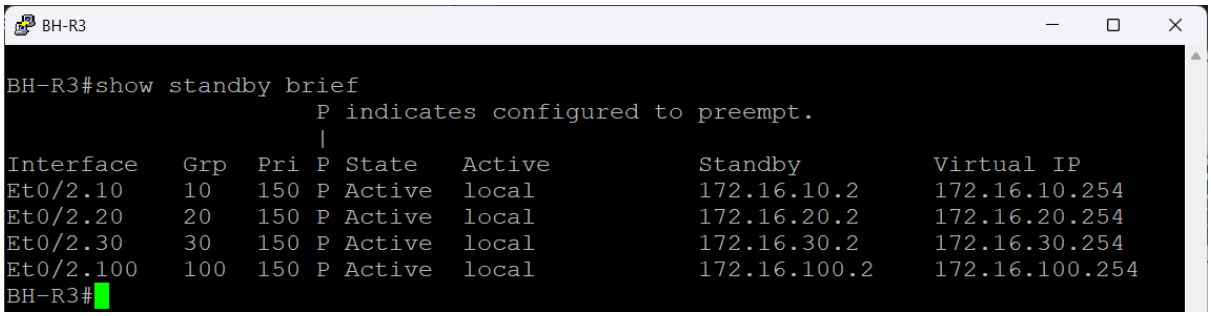

Figure 125 BH-R3 HSRP Gateway Redundancy verification

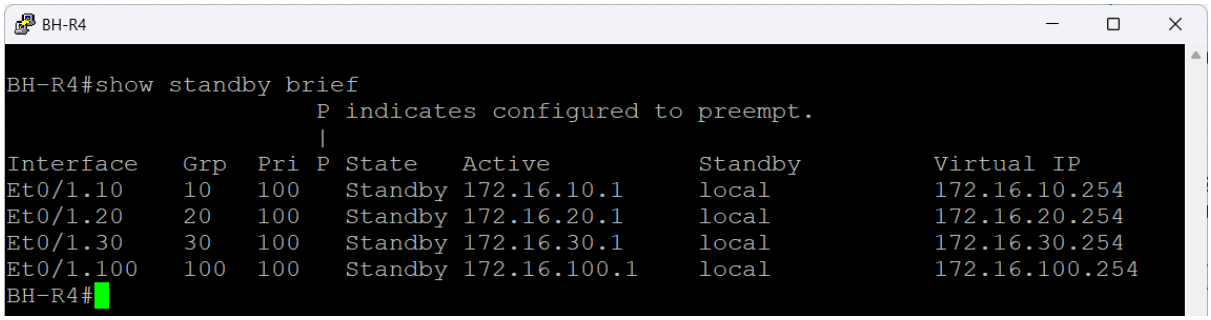

Figure 126 BH-R4 HSRP Gateway Redundancy verification

L3 SVIs

For every VLAN in the GHN network, SVIs are set up to offer Layer-3 capabilities. Devices within that subnet are able to send traffic outside of their local segment since each SVI serves as the default gateway for the associated VLAN. The routing device becomes in charge of forwarding packets between VLANs and guaranteeing appropriate network segmentation by giving each SVI an IP address. The SVI configuration needed to enable Layer-3 communication throughout the GHN network is described in this section.

VLAN 100 SVI configuration

The management VLAN interface (VLAN 100) set up on the Bahraini switches can be seen in the below images as an example. Within the VLAN 100 subnet (172.16.100.0/24), each switch is given a distinct management IP address that enables administrative control, remote access, and monitoring. The HSRP virtual IP address 172.16.100.254, which offers gateway redundancy via BH-R3 and BH-R4, is the default gateway for all switches.

Now that HSRP is fully functional on VLAN 100, management traffic from any switch can switch between routers without interruption. This verifies that first-hop redundancy protects the management network and that the Layer 2 domain for VLAN 100 is operating properly throughout the switching architecture.

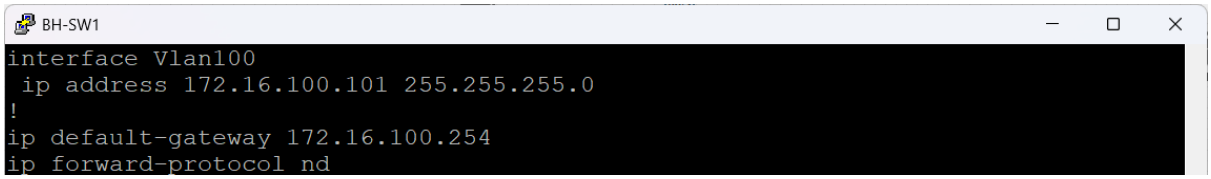

Figure 127 BH-SW1 VLAN 100 SVI configuration

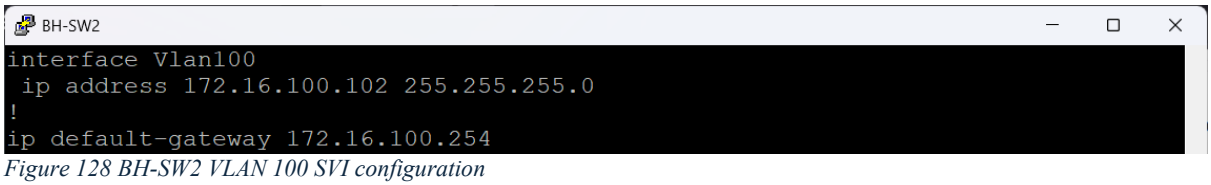

Figure 128 BH-SW2 VLAN 100 SVI configuration

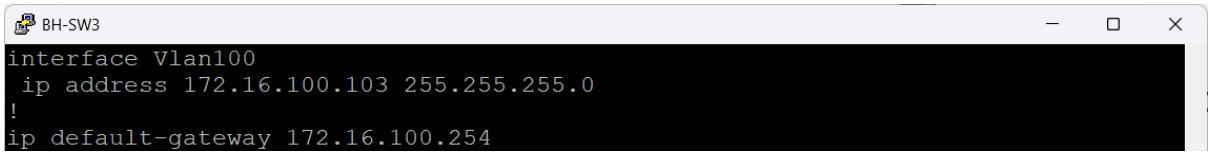

Figure 129 BH-SW3 VLAN 100 SVI configuration

Interface Summary verification

The operational interfaces of the four Bahraini routers are shown in the following figures, each of which has a distinct function in the routing and redundancy design of the site. All remote branch tunnels are terminated by the dual DMVPN hubs, BH-R1 and BH-R2. The DMVPN tunnel interfaces that create the overlay network, loopback interfaces for routing identification, and WAN serial links toward the ISP are among their active interfaces. Since internal VLAN gateways are purposefully concentrated on BH-R3 and BH-R4, the LAN-facing Ethernet ports on these two routers are still inactive.

For every VLAN in Bahrain, BH-R3 and BH-R4 serve as the Layer-3 gateway pair. Sub interfaces for VLANs 10, 20, 30, and 100 are hosted by both routers, each of which carries HSRP to offer first-hop redundancy for user, server, and management networks. BH-R4 serves as Standby and is prepared to take over right away in the event that BH-R3 becomes unavailable. BH-R3, which is configured with the higher priority, assumes the Active duty. To ensure smooth routing between the LAN and the DMVPN core, their WAN-side serial interfaces connect upstream toward the DMVPN hubs.

When taken as a whole, the interface summaries verify that WAN links, DMVPN tunnels, VLAN gateways, and redundancy mechanisms are all operational and performing as intended. This confirms that the Bahrain site is fully functioning within the framework of the Global Health Network.

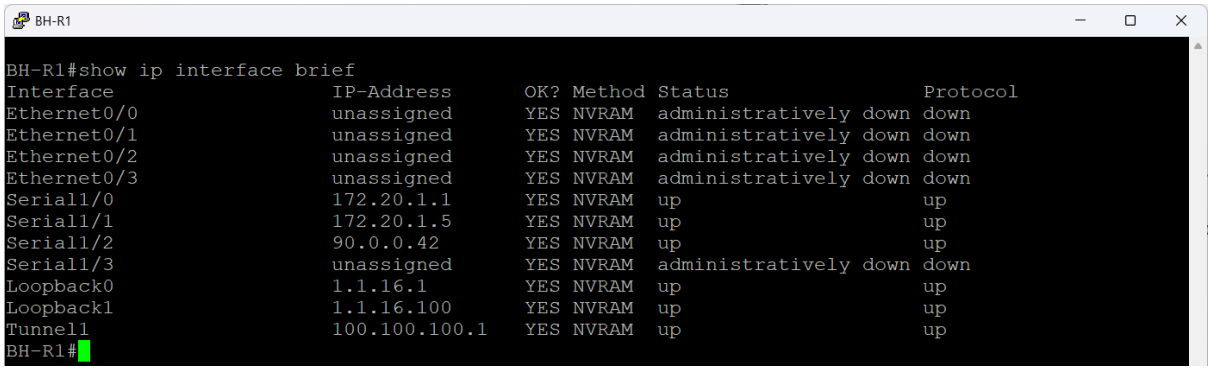

Figure 130 BH-R1 Interface Summary verification

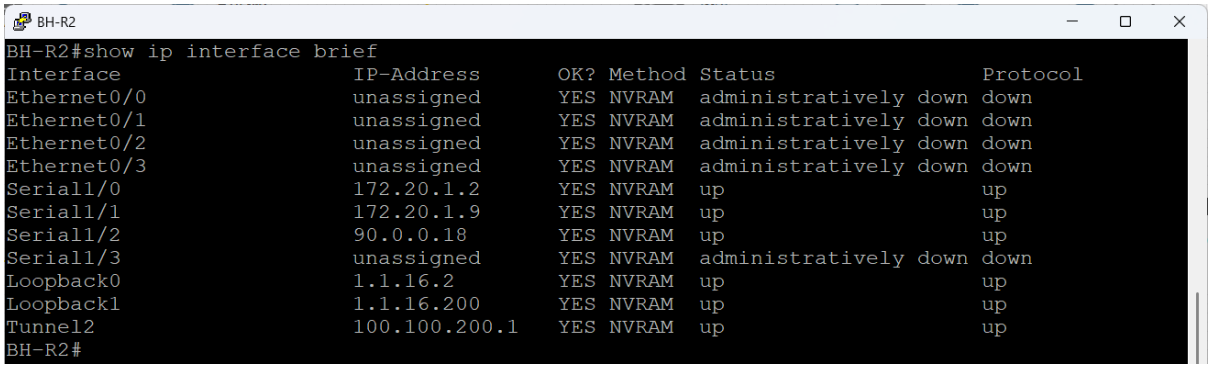

Figure 131 BH-R2 Interface Summary verification

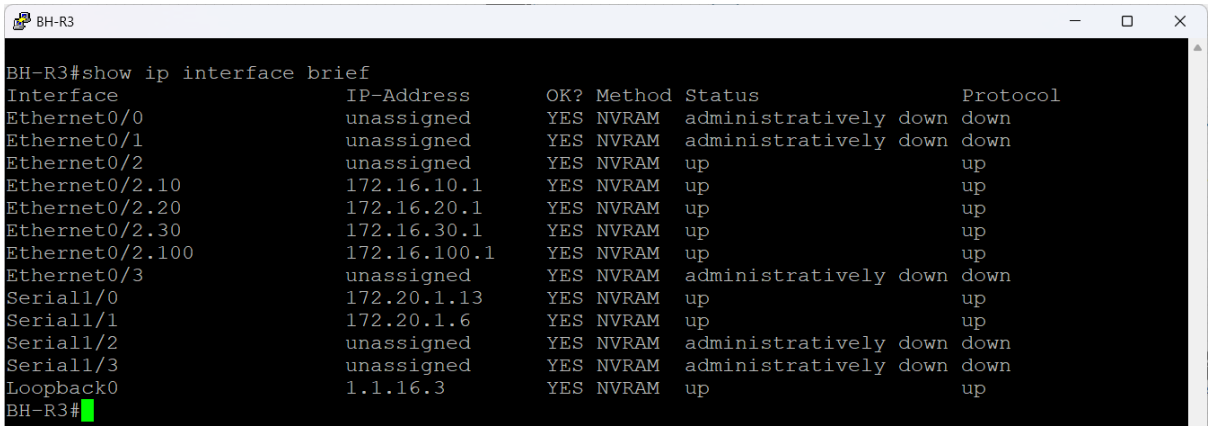

Figure 132 BH-R3 Interface Summary verification

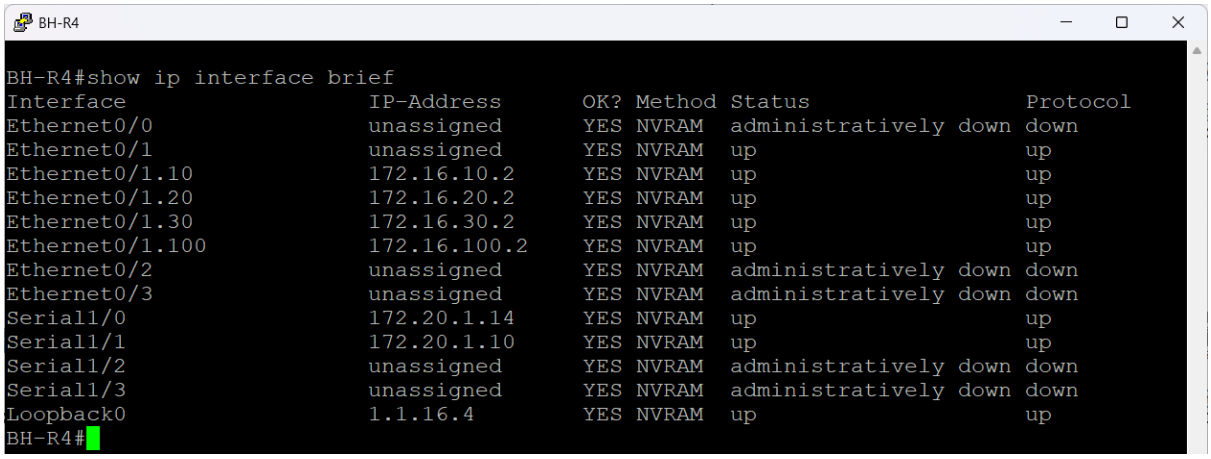

Figure 133 BH-R4 Interface Summary verification

L2 Security

Layer 2 security is used to defend the switching infrastructure against common attacks such broadcast control, topology disruption, and unauthorized device connections. Applying fundamental security measures improves the stability and dependability of the LAN even when Layer 2 doesn't include built-in authentication or encryption. These controls aid in ensuring that the switching topology stays constant and that only authorized traffic enters the network. The Layer 2 security elements set up in the GHN environment are described in this section along with their function in preserving a safe and reliable LAN.

Security Configuration

An example of Layer 2 security, STP, trunking, and management configurations used on BH-SW3 and BH-SW4 is shown in the figures below. VLANs 1, 10, 20, 30, and 100 were given distinct STP priorities by each switch. In the Bahrain switching topology, this guarantees deterministic root bridge selection and avoids STP instability. To keep a predictable Layer 2 structure and stop unauthorized devices from manipulating topology, STP protection methods including PortFast, bpduguard, and root guard are activated.

In order to maintain a fixed trunk state, trunk interfaces are set up using 802.1Q encapsulation, VLAN 100 as the native VLAN, and switchport nonegotiate to disable DTP. To safeguard the STP root position and prevent unintentional root takeover by downstream switches, Root Guard is implemented on uplink ports.

To lessen the attack surface, access ports including unused or isolated ports are administratively shut down and assigned to the black hole VLAN 999. Additionally, BH-SW4 exhibits port security with maximum address limitations, aging timers, and sticky MAC learning, offering an extra degree of defense against MAC flooding and unwanted hosts.

With a distinct IP address and the HSRP virtual gateway 172.16.100.254 as the default gateway, both switches have a management SVI on VLAN 100. To protect the remote connection to the switch, SSH security parameters are defined, such as session timeout, retry limitations, and version enforcement. When combined, these configurations offer a hardened

Layer 2 environment with dependable management access, secure trunking, port protection, and organized STP behavior.

When combined, these configurations provide a robust and secure access layer: access ports are strictly regulated to guarantee that only legitimate endpoints can connect, and trunks forward all necessary VLANs to the routing core. This structure protects the branch network from common LAN-level attacks and maintains consistency in the VLAN design.

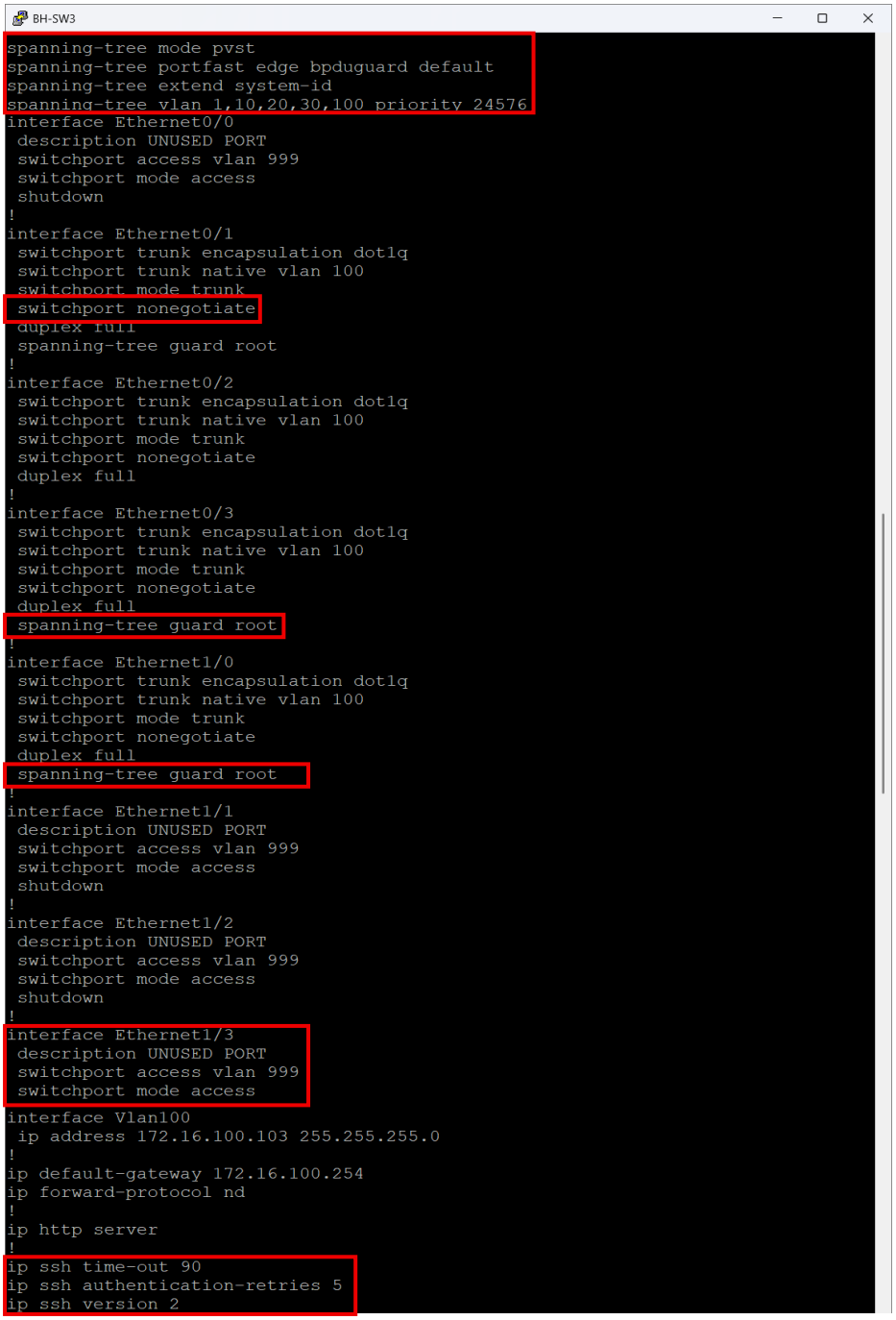

Figure 134 BH-SW3 Security Configuration

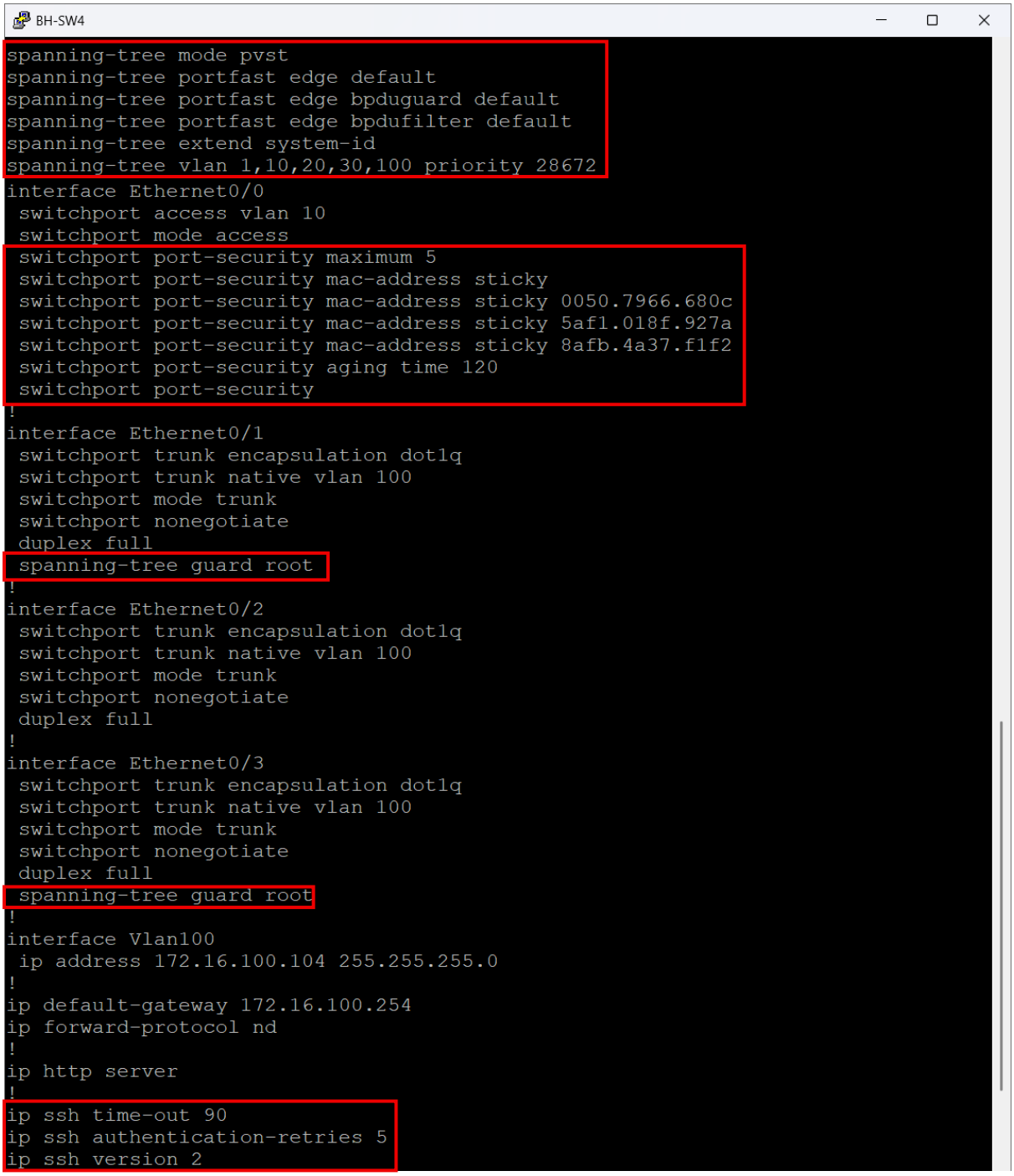

Figure 135 BH-W4 Security Configuration

Port Security Status verification

These figures below show a sample of the operating status of port security on BH-SW2 and BH-SW4. The access interfaces of both switches have port security enabled, which restricts each port to a maximum of five learned MAC addresses and uses the sticky MAC function to automatically record valid devices. The ports are in a Secure-up state, which means that no infractions have happened, and the permitted MAC addresses have been successfully learned.

The violation mode on both switches is set to shut down, meaning the interface will disable itself if an unauthorized device attempts to connect. An aging timer of 120 minutes is applied using absolute aging, allowing stale MAC entries to be removed automatically without compromising security. The zero violation count confirms that no security events have been triggered and that all connected hosts match the expected MAC address profiles.

By preventing illegal devices from connecting to the network and preserving operational stability for permitted hosts, these outputs together confirm that port-level access control is operating as intended.

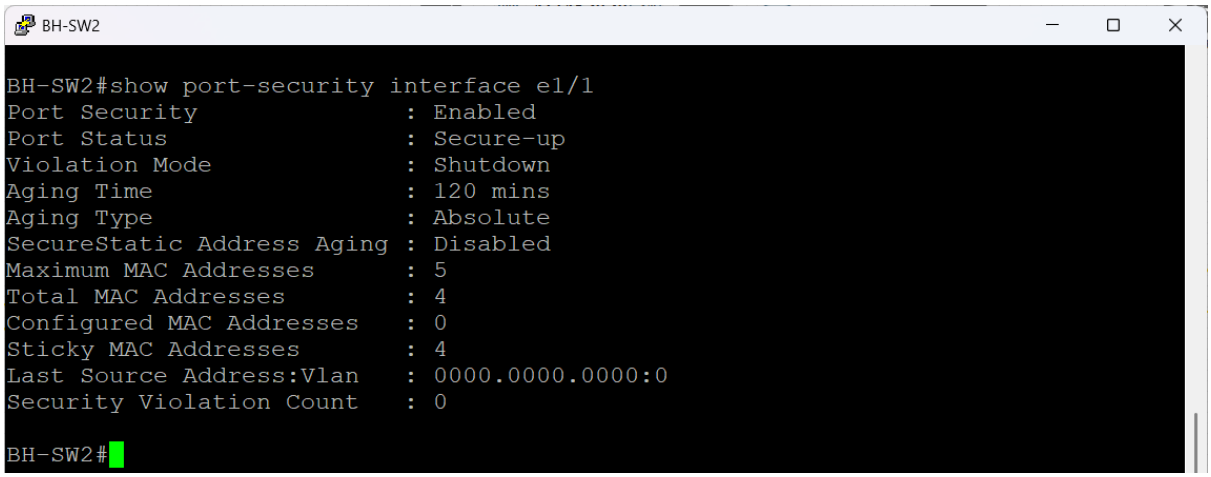

Figure 136 BH-SW2 Port Security Status verification

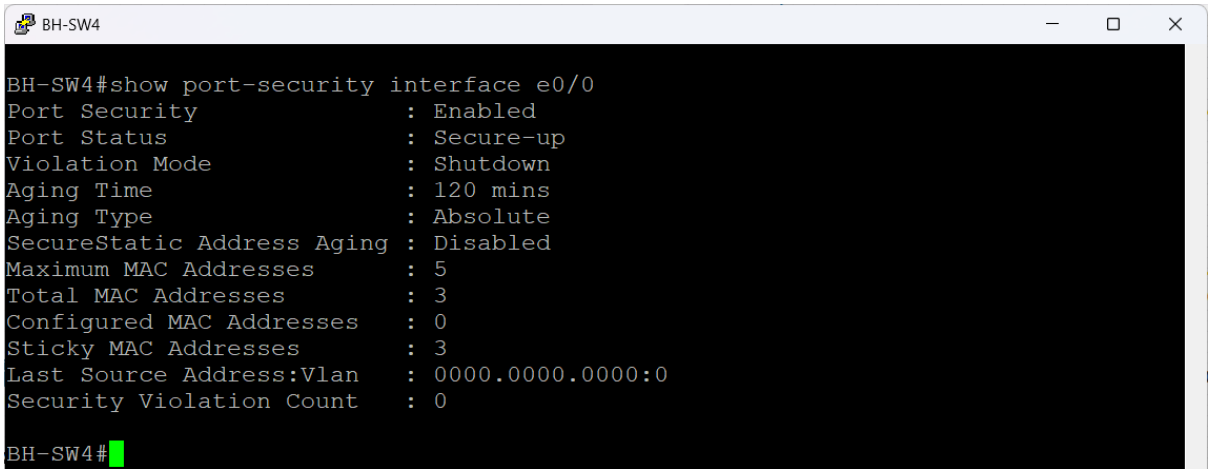

Figure 137 BH-SW4 Port Security Status verification

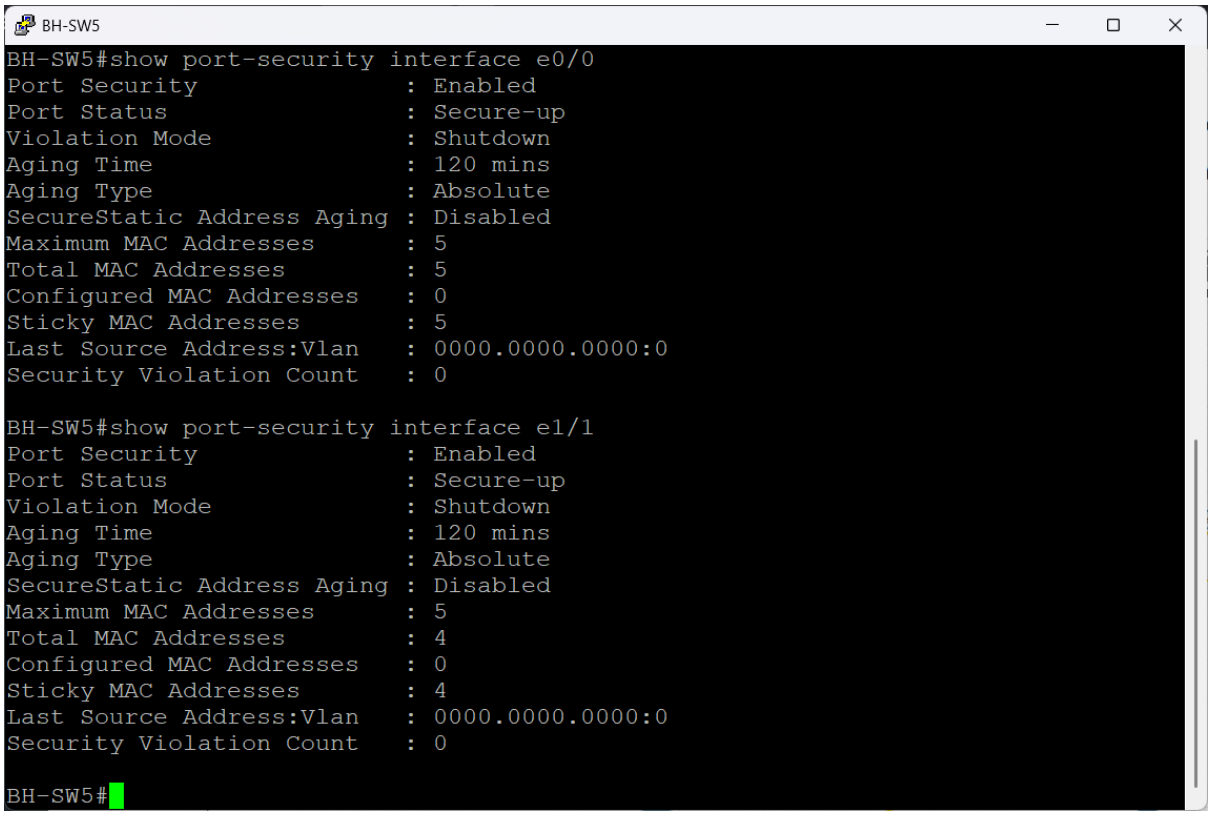

Figure 138 BH-SW5 Port Security Status verification

Server & Services Implementation

The deployment and setup of the centralized server infrastructure utilized throughout the GHN network are covered in this section. After installation and configuration, Windows Server 2012R2 was set up to provide web hosting, file transfer, email, authentication, domain name resolution, and automated network management. Active Directory, DNS, IIS, FTP, hMailServer, DHCP, AAA, RBAC, and secure management access are installed and configured after the essential server setup, which is the first step in the methodical implementation of each service. The main procedures used to deploy and validate these services in the GHN environment are described in the next subsections.

Windows Server basic configuration

The IP setup of the client and server computers at the Bahrain site's is displayed in the following below figures. BH-Server1, running Windows Server 2012 R2, has the address 172.16.30.31/24 and is located in the Servers VLAN (VLAN 30). The HSRP virtual IP 172.16.30.254, which is supplied by BH-R3 and BH-R4, serves as its default gateway. Key enterprise services like Active Directory, DNS, FTP, web services, and internal apps for the Bahrain branch are hosted by BH-Server as a component of the server architecture.

BH-Client is an example of a typical end user workstation in the England site (VLAN 20) running Windows 10 Pro. It is IP address is 172.17.20.20/24, and it is default gateway is 172.17.20.254. In order to validate routing, inter-VLAN communication, HSRP redundancy, and end to end service connectivity, the client is used to show how user devices interact with the server architecture throughout the multi site DMVPN network.

When taken as an entire system, these outputs verify that the server and client are fully integrated into the GHN enterprise network for authentication, service access, cross-site communication, and application delivery, receive accurate addressing from their specific VLANs, and are linked to the appropriate HSRP gateways.

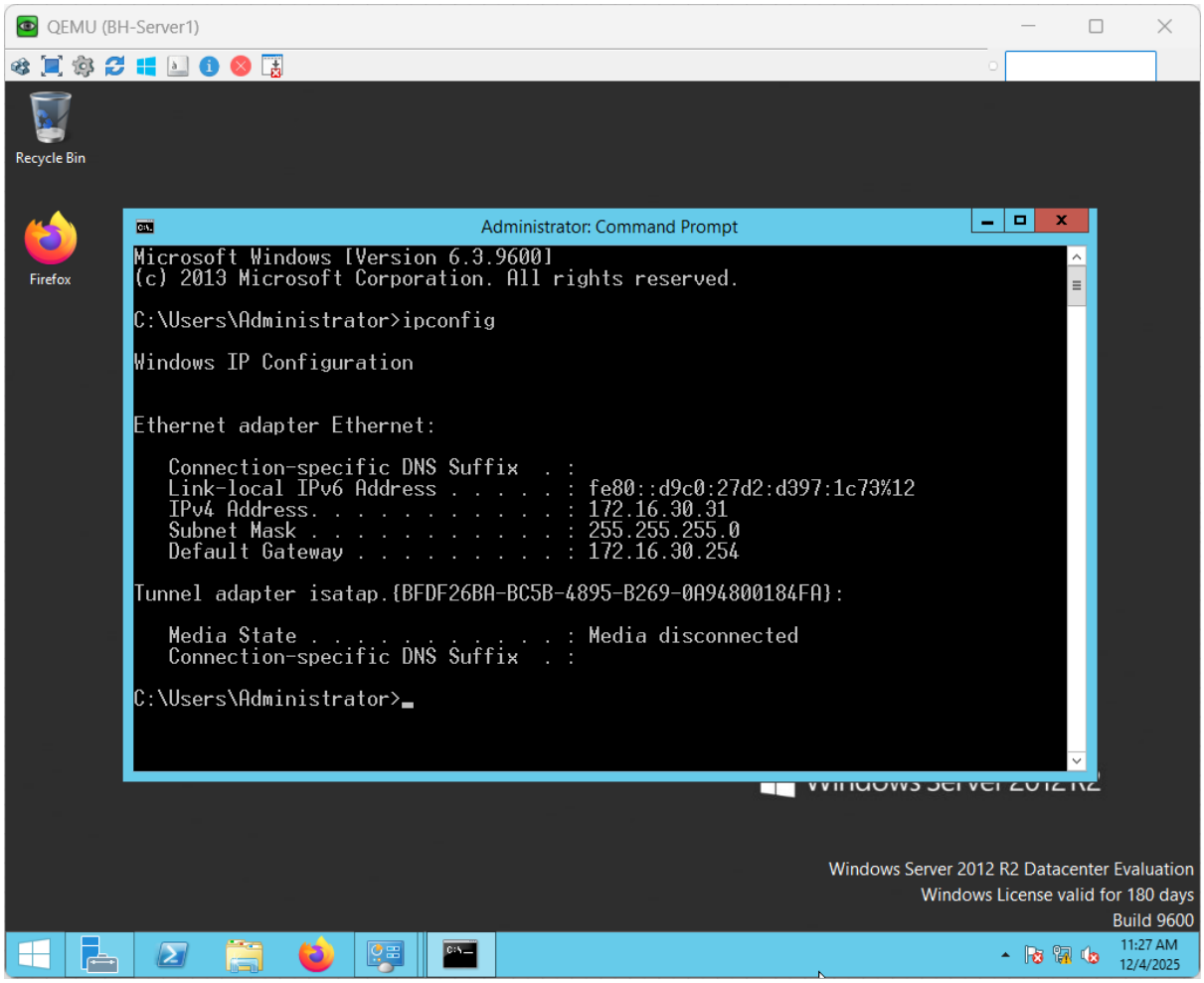

Figure 139 BH-Server1 Windows Server IP Address

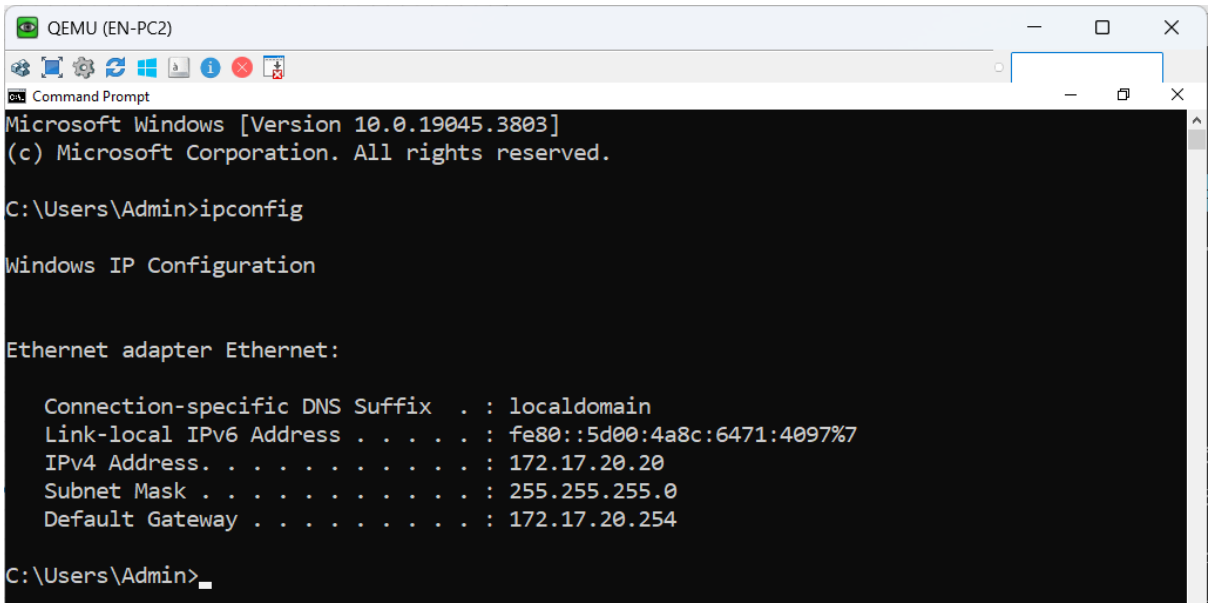

Figure 140 EN-PC2 Windows 10 pro IP Address

Windows Server Services Installation

BH-Server acts as the central service point for the Bahrain site, providing identity management, internal DNS resolution, and web, FTP hosting for GHN. The figures below show the installation and activation of the key server roles: Active Directory Domain Services, IIS Web Server, and the FTP service.

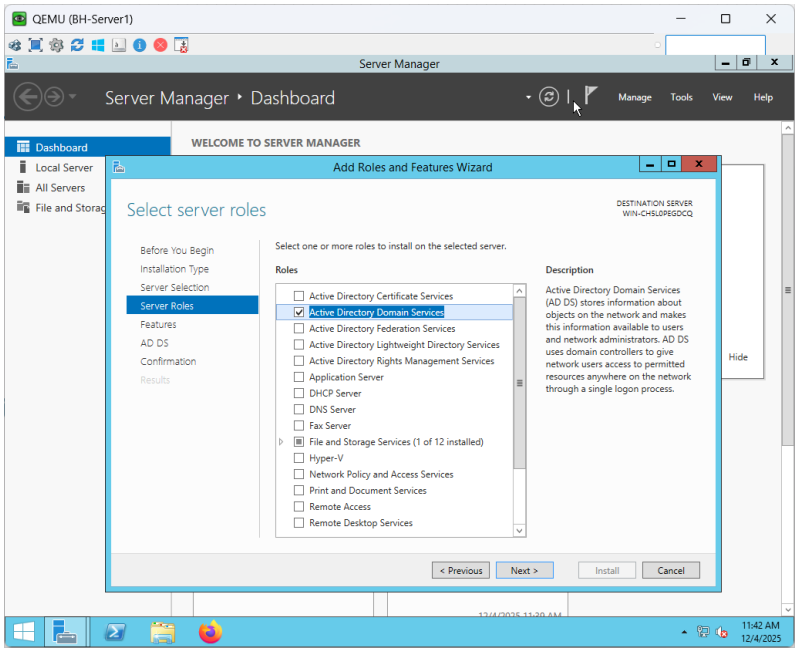

Figure 141 BH-Server1 Active Directory Domain Services installation part 1

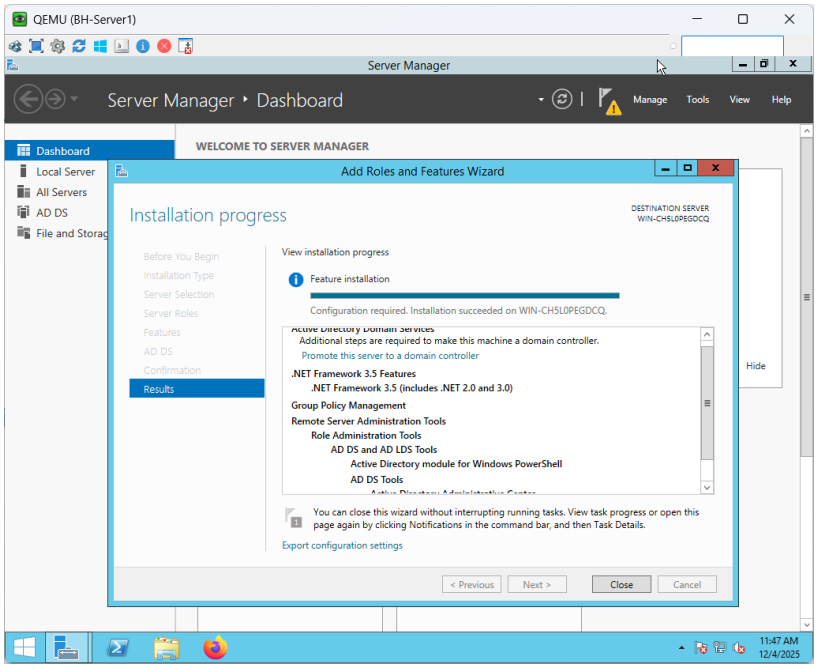

Figure 142 BH-Server1 Active Directory Domain Services installation part 2

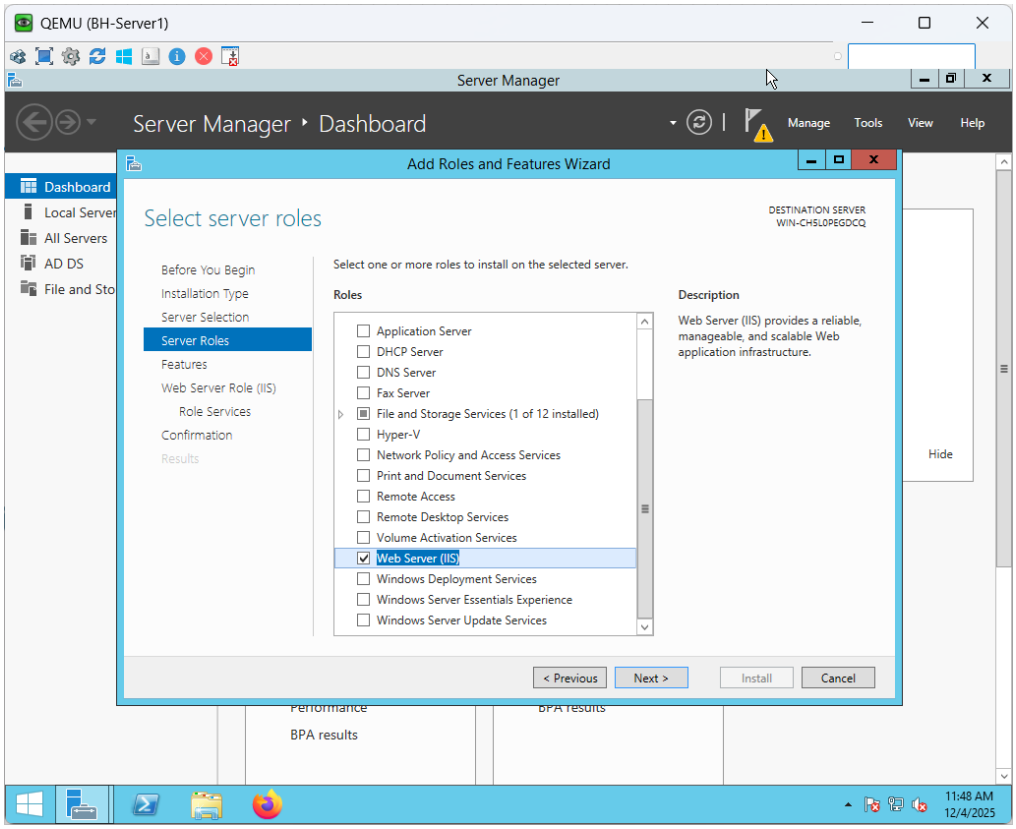

Figure 143 BH-Server1 IIS Web Server installation part 1

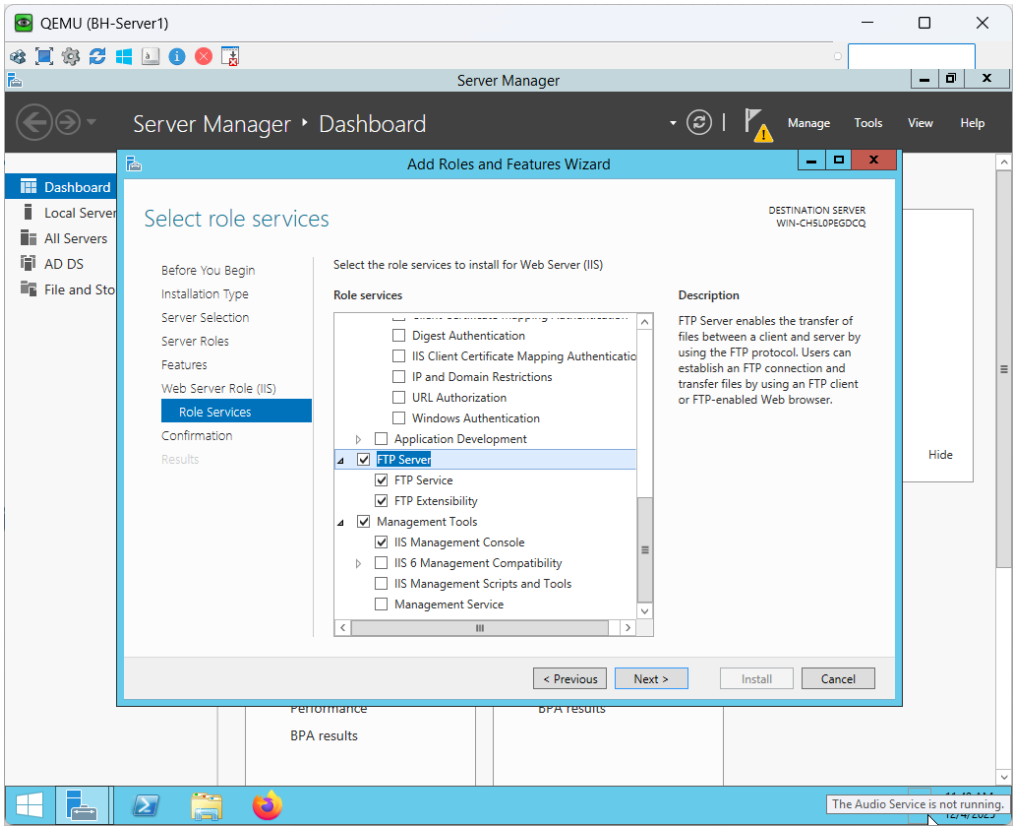

Figure 144 BH-Server1 IIS Web Server & FTP installation part 2

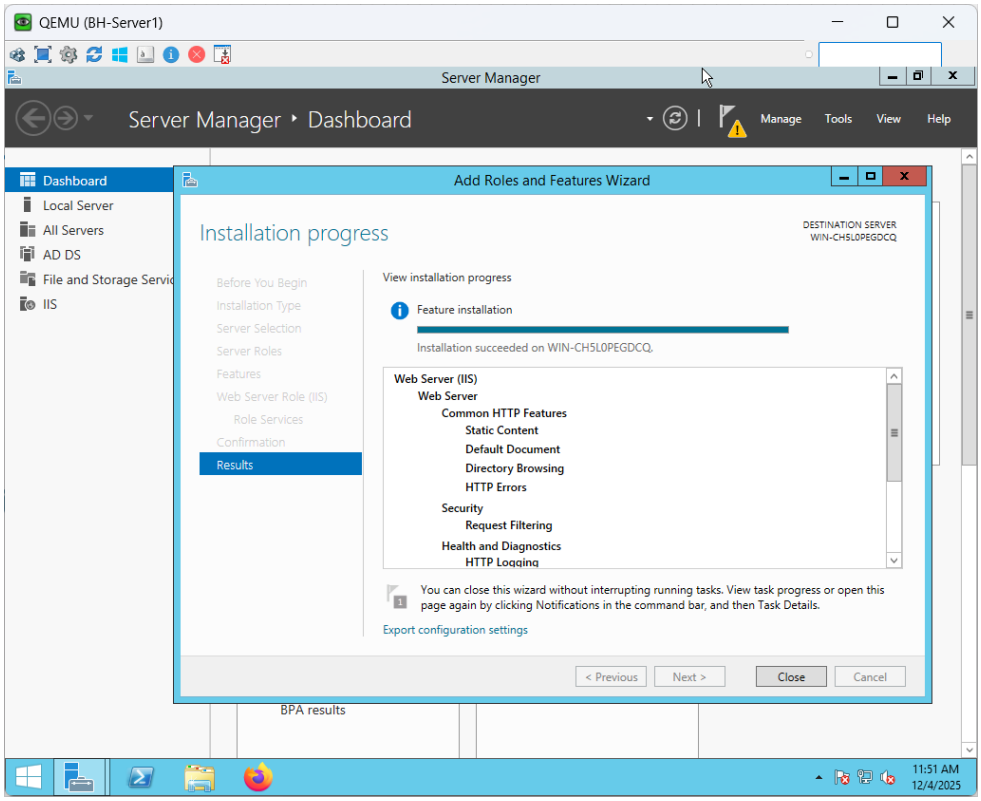

Figure 145 BH-Server1 IIS Web Server & FTP installation part 3

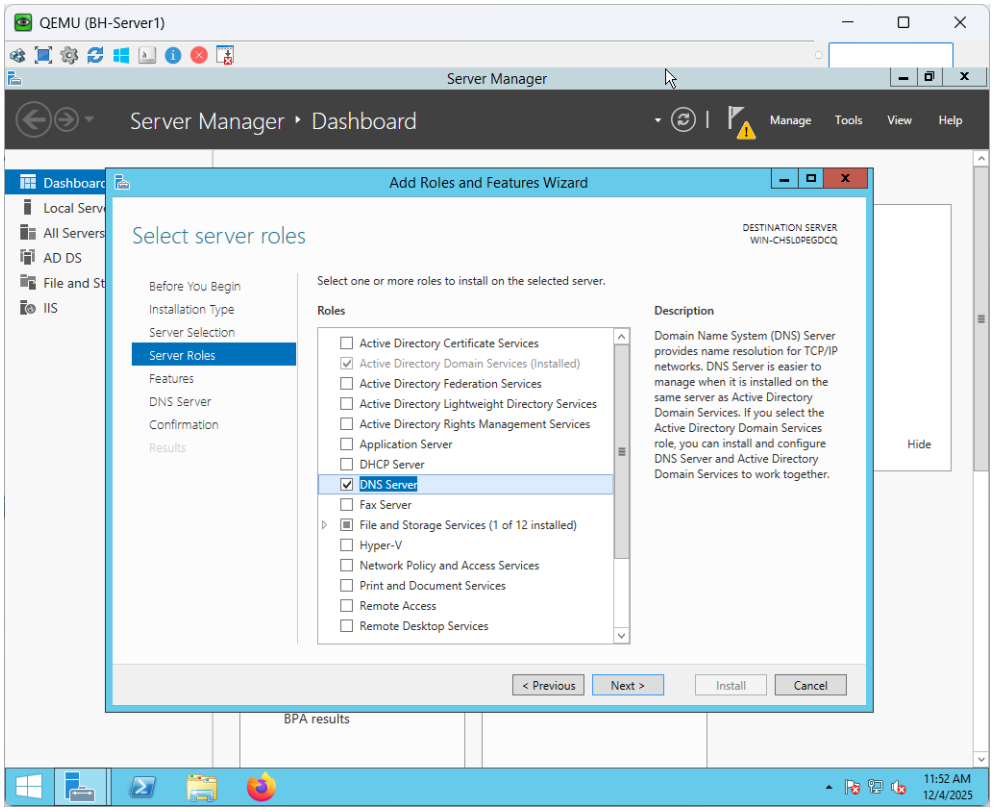

Figure 146 BH-Server1 DNS Server installation part 1

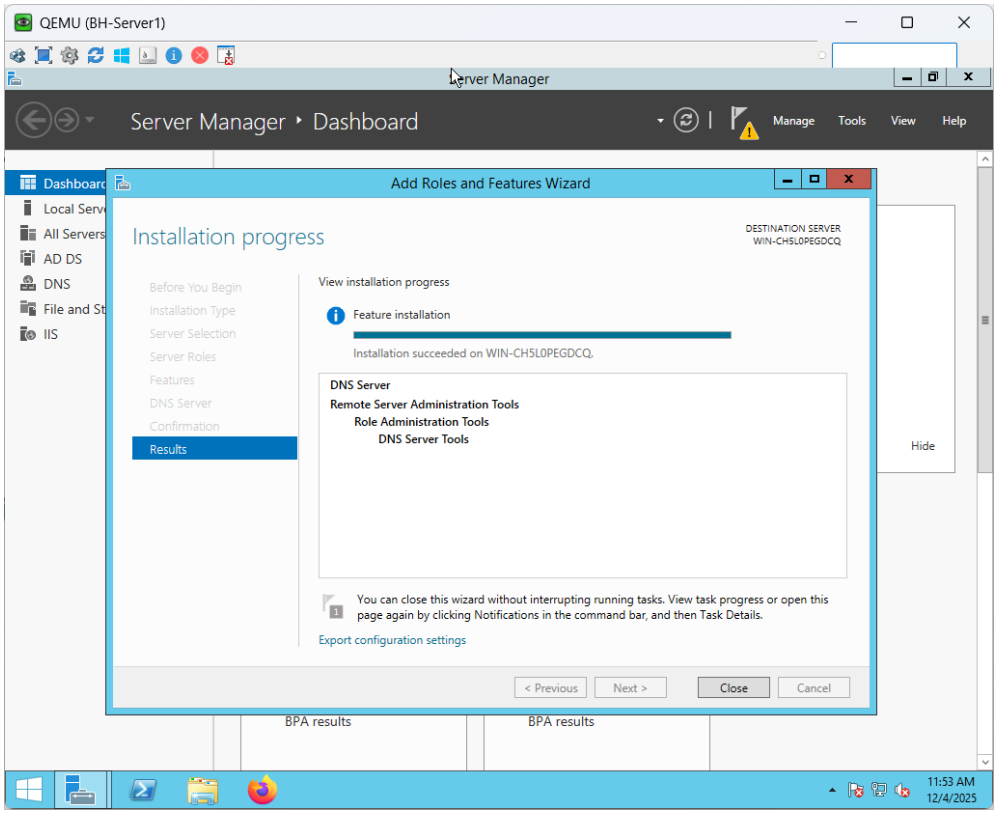

Figure 147 BH-Server1 DNS Server installation part 2

Active Directory Setup

The complete Active Directory Domain Services implementation on BH-Server is depicted in the figures below. The server is positioned as the new GHN.com forest's first domain controller, creating the Bahrain site's identity and authentication framework. The setting registers GHN as the NetBIOS domain name, activates the DNS role, and sets the forest and domain functional level to Windows Server 2012 R2. The server is prepared for promotion and rebooting once the DSRM password has been entered, and all requirements have been verified. This procedure establishes the central directory structure that is necessary for secure resource access, policy enforcement, and login for all GHN sites client and services.

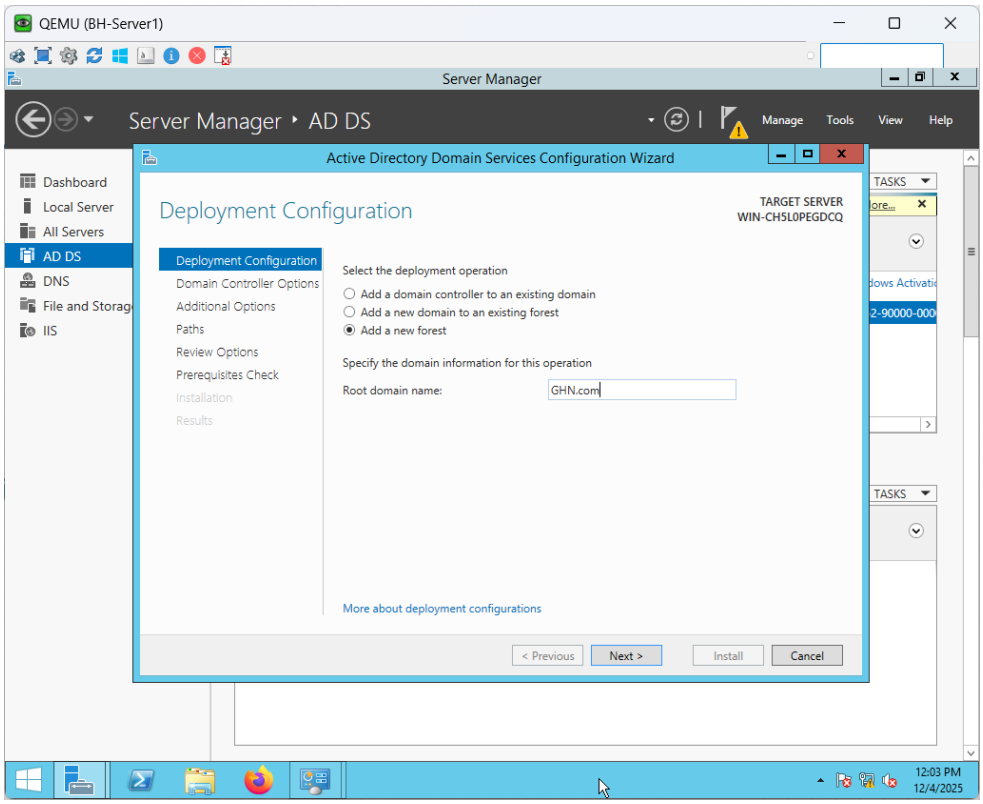

Figure 148 BH-server1 AD-DS Deployment Part 1

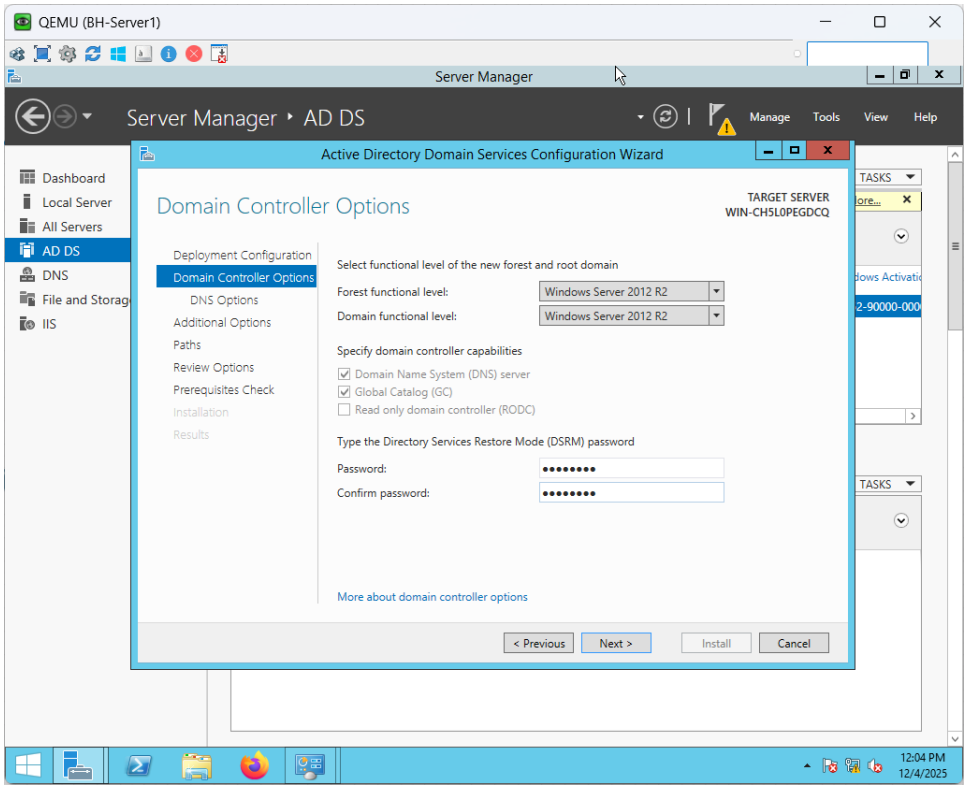

Figure 149 BH-server1 AD-DS Deployment Part 2

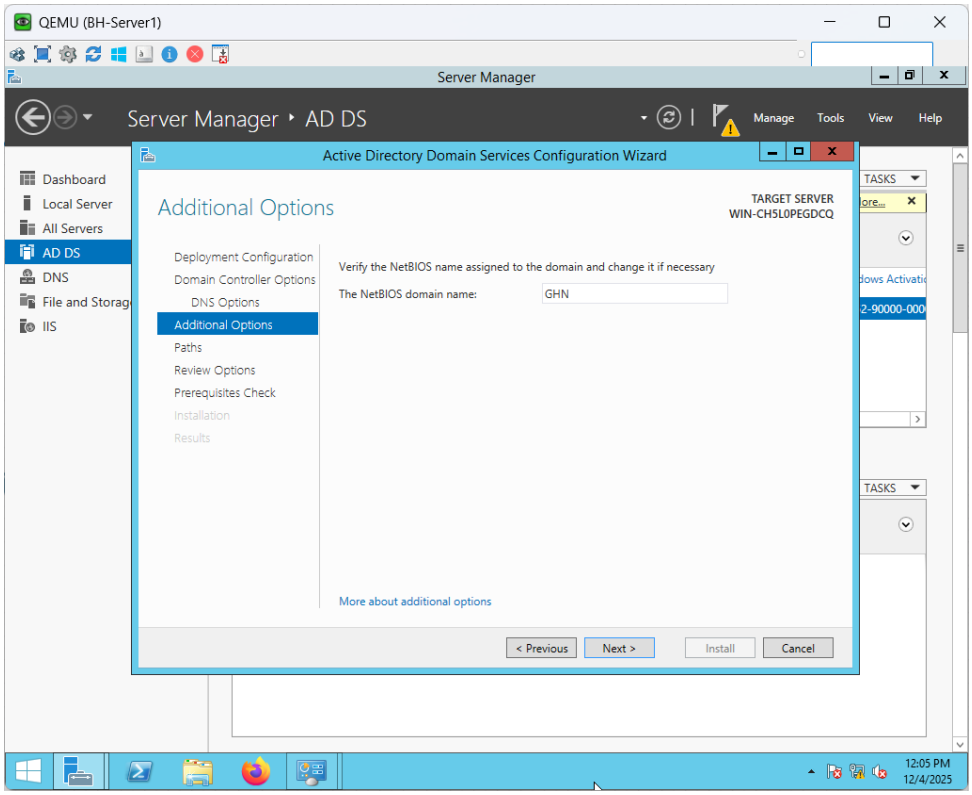

Figure 150 BH-server1 AD-DS Deployment Part 3

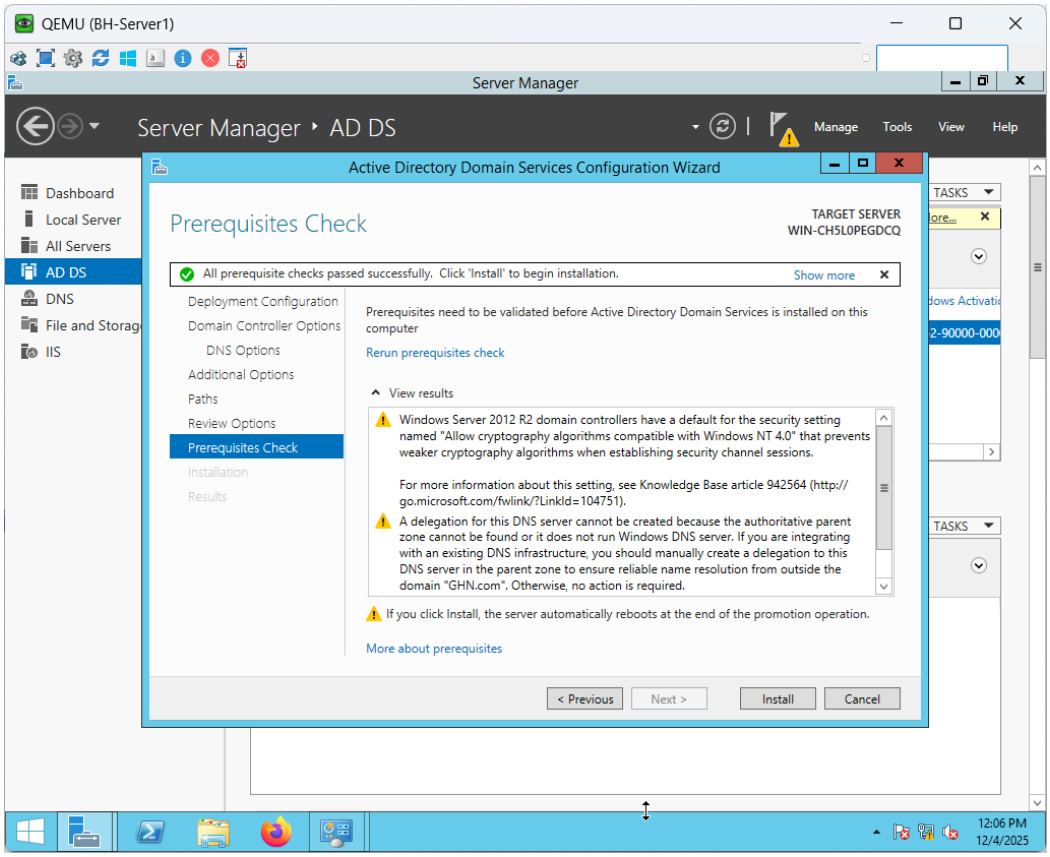

Figure 151 BH-server1 AD-DS Deployment Part 4

Active Directory Setup verification

By verifying the successful promotion of the domain controller and authenticating client enrolment, the Active Directory deployment on BH-Server1 was confirmed. The server verified that the domain controller role was active and reachable on the network by authenticating using the domain context (GHN\Administrator) after installing AD DS and rebooting.

To verify end-to-end AD operation, a Windows 10 workstation was immediately connected to the GHN.com domain. The client successfully authenticated using domain credentials after resolving the domain via DNS and communicating with the domain controller across the routed network. The message "Welcome to the GHN.com domain" attests to the successful completion of the domain join procedure. This demonstrates that the Bahrain site is offering centralized authentication and identity services as planned and that Active Directory, DNS, inter-VLAN routing, and gateway redundancy are all operating as anticipated.

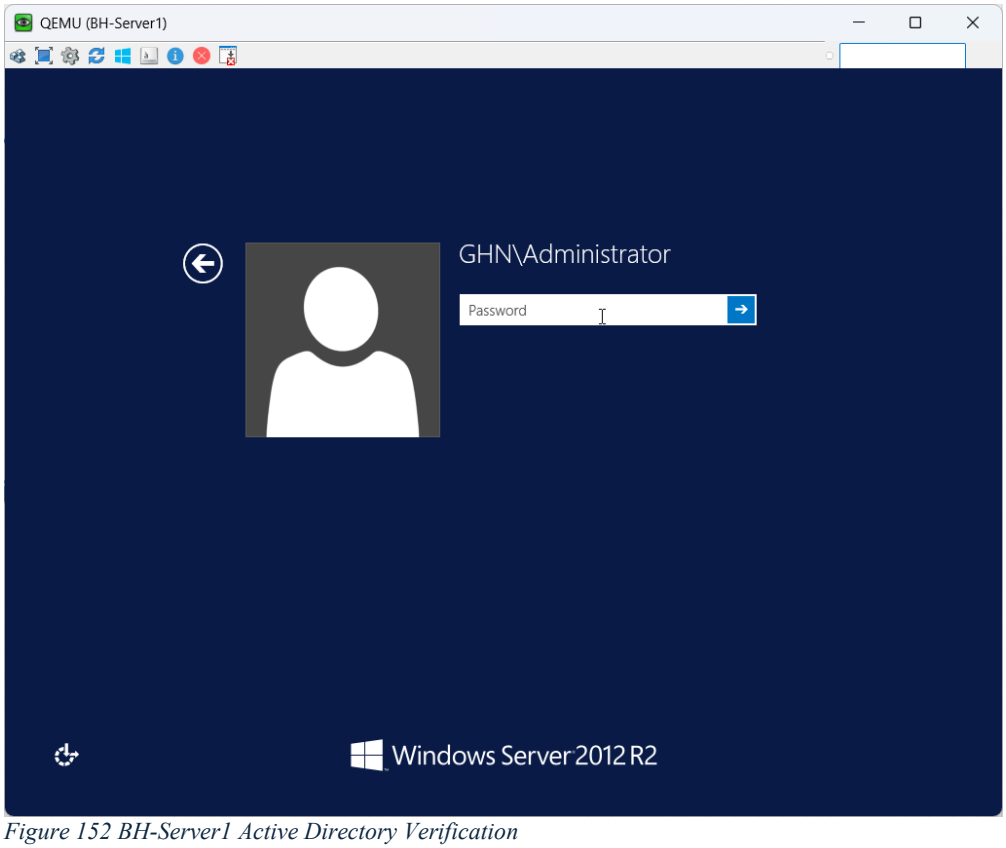

Figure 152 BH-Server1 Active Directory Verification

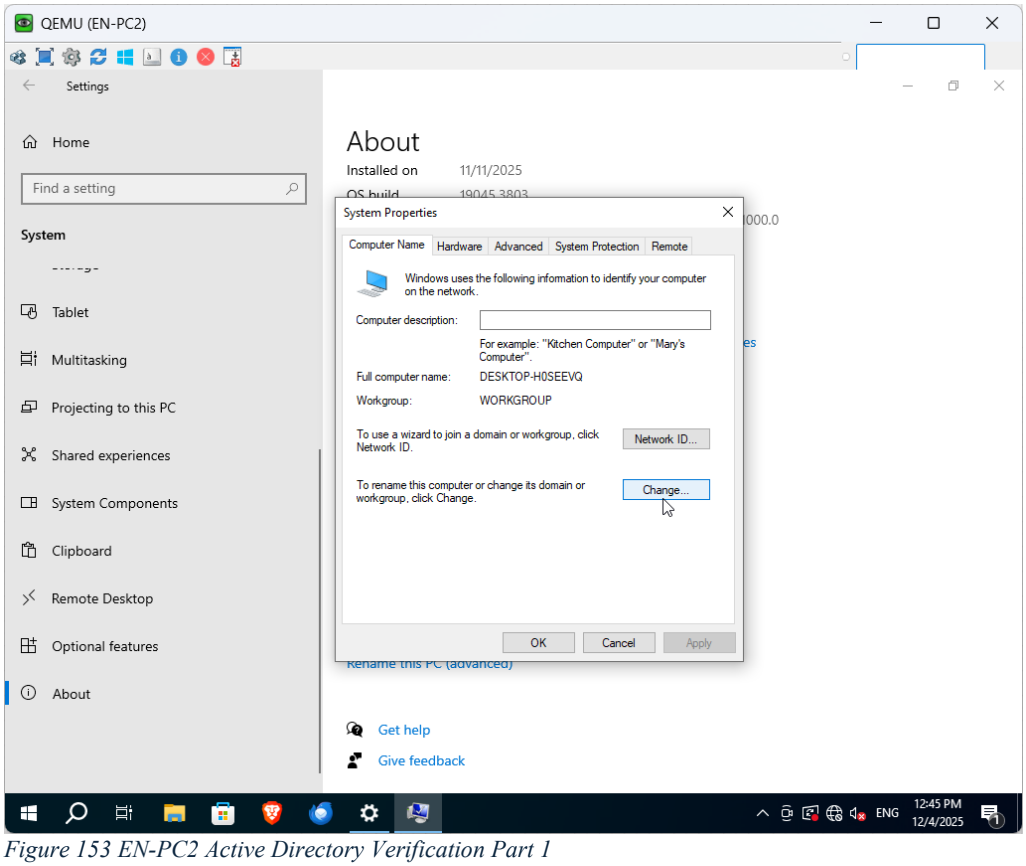

Figure 153 EN-PC2 Active Directory Verification Part 1

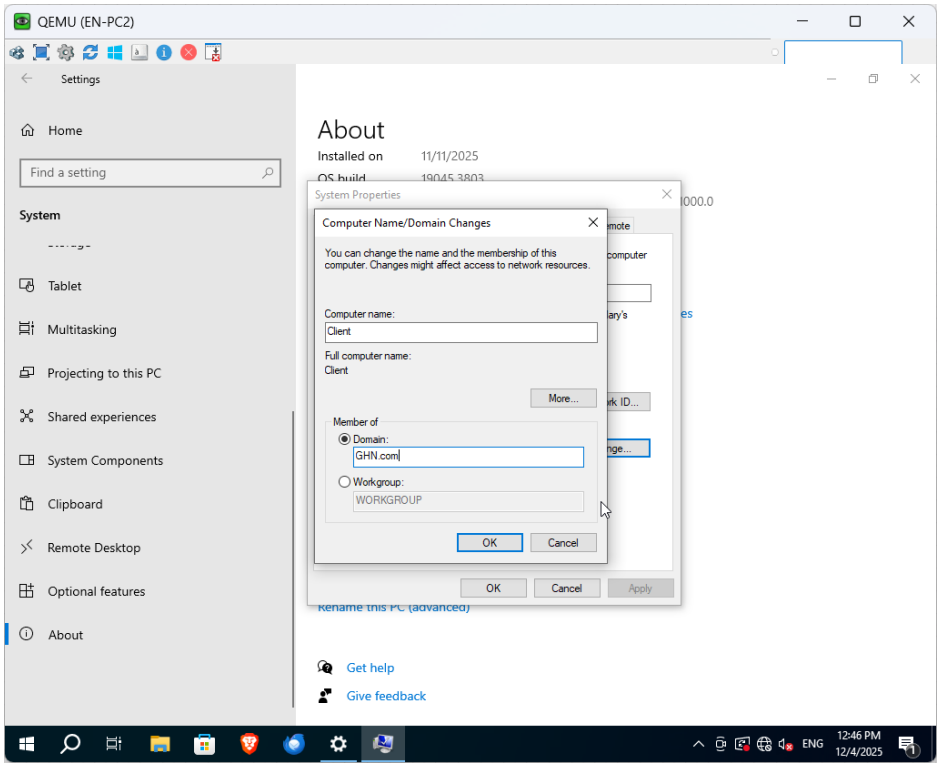

Figure 154 EN-PC2 Active Directory Verification Part 2

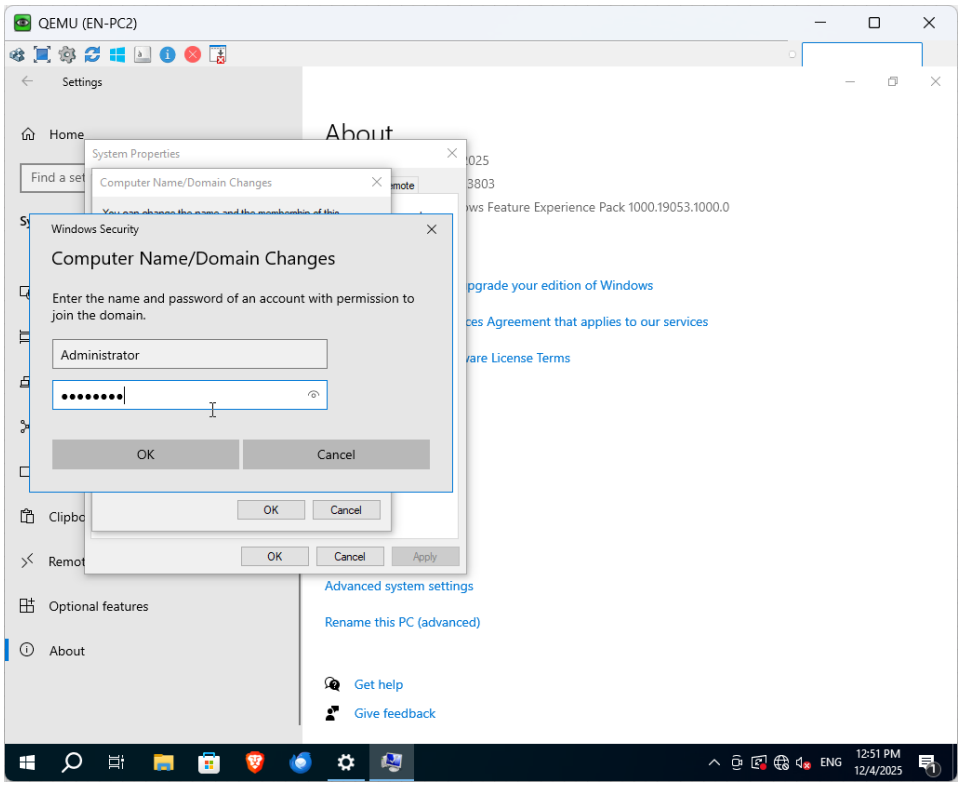

Figure 155 EN-PC2 Active Directory Verification Part 3

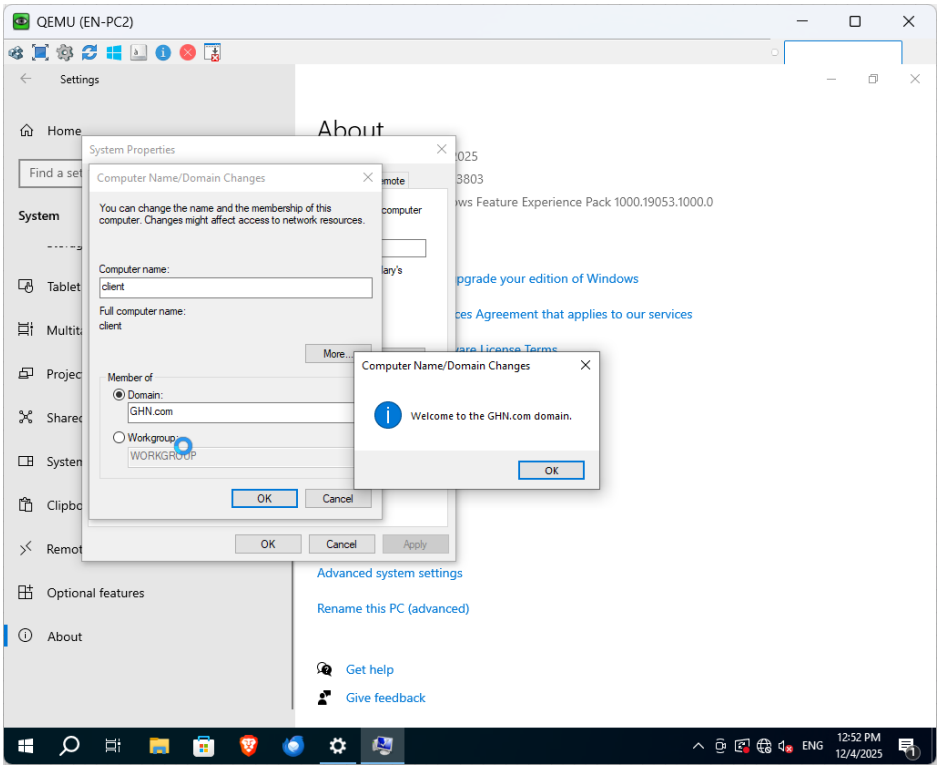

Figure 156 EN-PC2 Active Directory Verification Part 4

DNS Setup

The below figures show DNS service on BH-Server1 was verified to ensure proper name resolution across the Bahrain site and full integration with Active Directory. GHN.com and _msdcs.GHN.com, two crucial forward lookup zones that were both automatically established as Active Directory–Integrated zones, are displayed in the DNS Manager. The fact that their status is "Running" indicates that the server is successfully managing DNS queries and facilitating domain operations.

The existence of these zones indicates that all necessary SRV, host, and service records that AD DS uses for client authentication, domain joins, and service discovery were successfully published by the domain controller. DNS updates are safely replicated within the directory and support dynamic updates from domain members due to the zones' AD integration. This configuration guarantees reliable internal name resolution, domain controller location, and GHN.com domain authentication for both servers and clients .

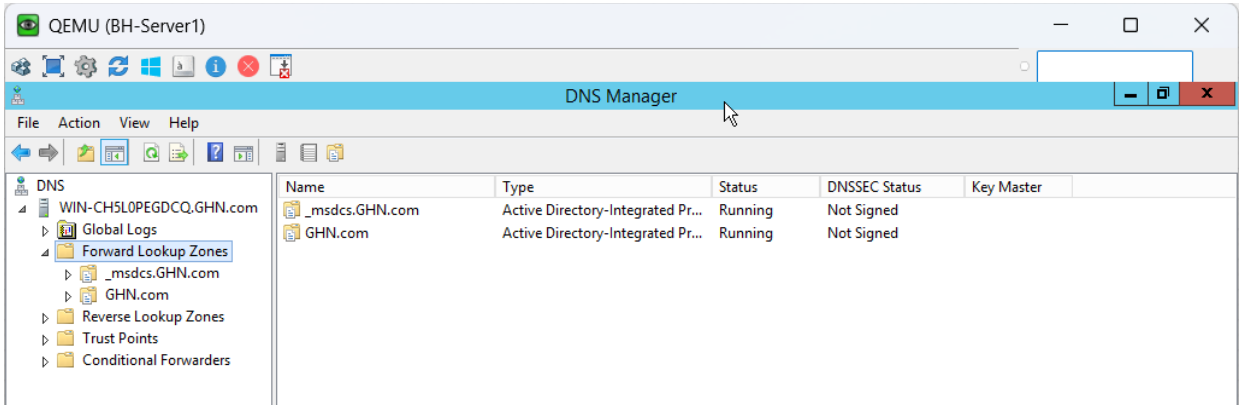

Figure 157 BH-Server 1 DNS Server Configuration Verification

DNS Resolution Verification

The figure below shows domain controller successfully resolves **GHN.com** to its own IP address (172.16.30.31). DNS on the server is functioning correctly and responding instantly.

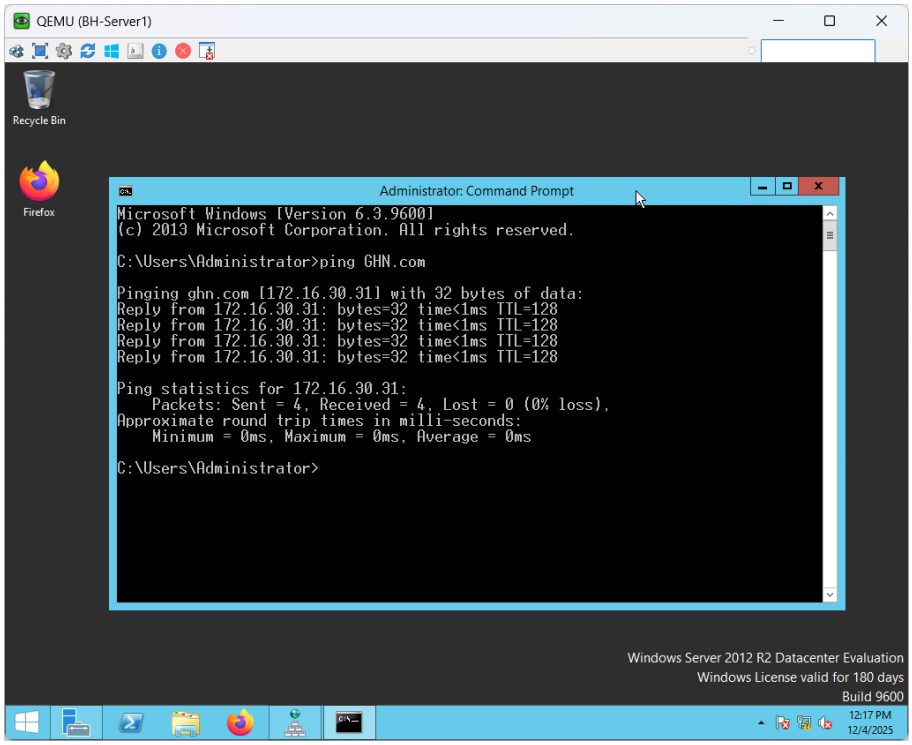

Figure 158 BH-Server1 DNS Resolution Verification

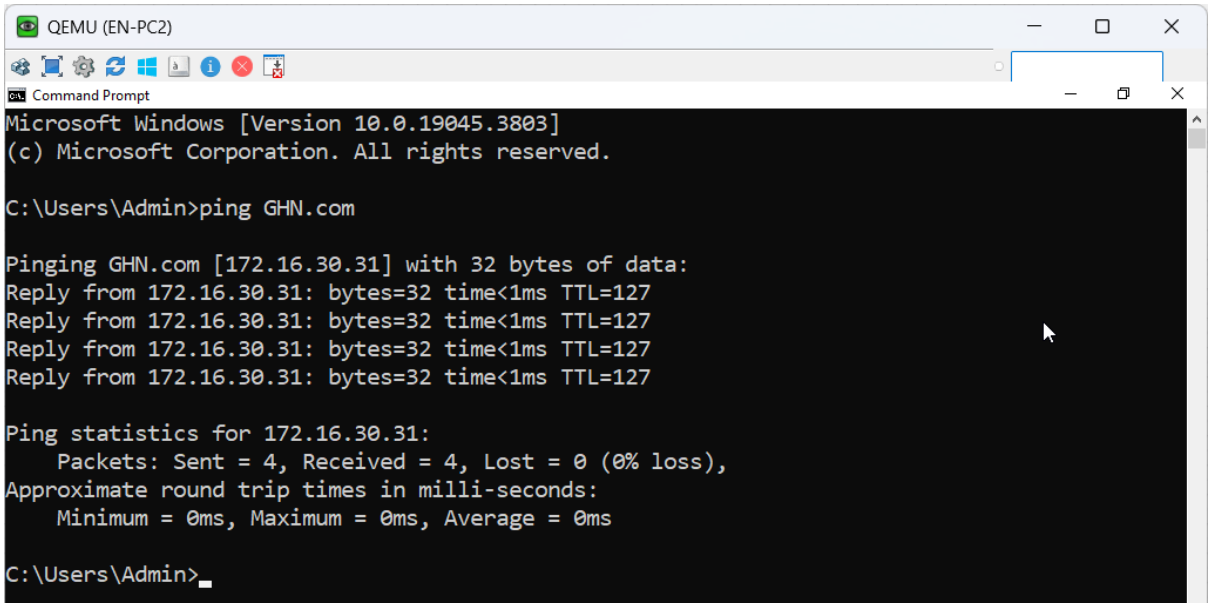

Figure 159 EN-PC2 DNS Resolution Verification

The figure above shows the Windows 10 client resolves **GHN.com** through the DNS server without delay, confirming proper DNS reachability and end-to-end name resolution inside the GHN network.

IIS Web Server Setup

The below figures show that the IIS role was set up on BH-Server1 for providing internal web hosting for the Global Health Network environment. Following the setup, the necessary website files, such as HTML pages, pictures, CSS, and JavaScript assets, were added to the web root folder (C:\inetpub\wwwroot). The server verified that IIS was functioning properly by delivering all content locally without any further configuration problems.

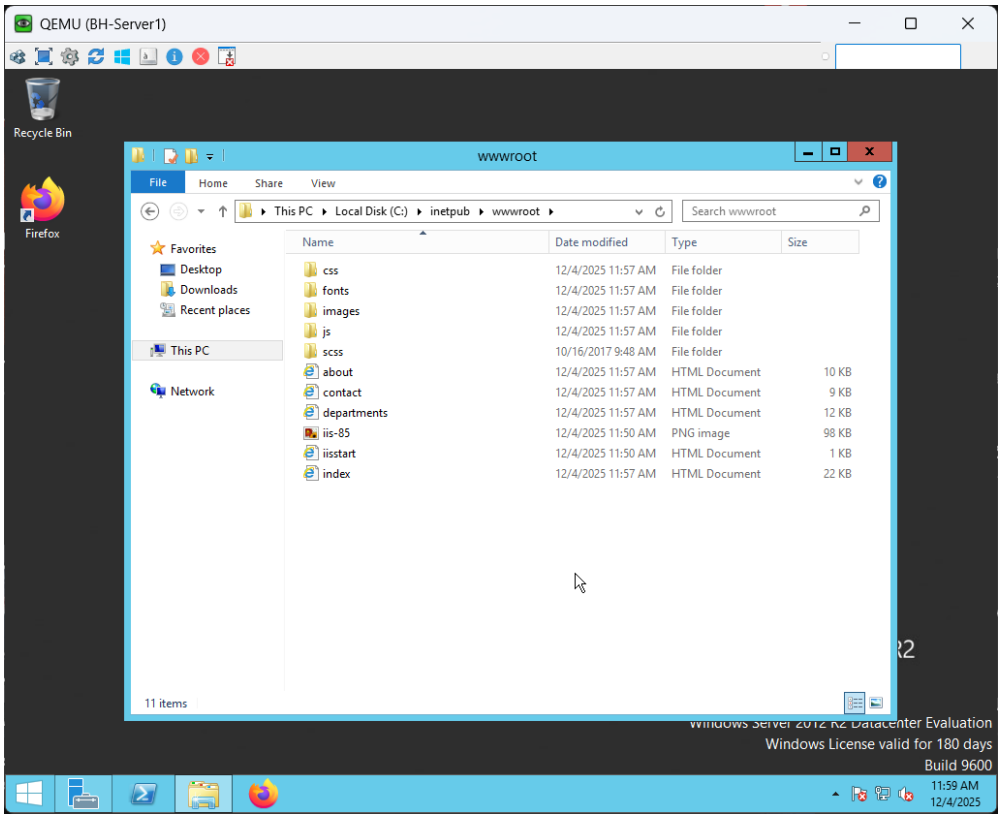

Figure 160 BH-Server1 Website Files

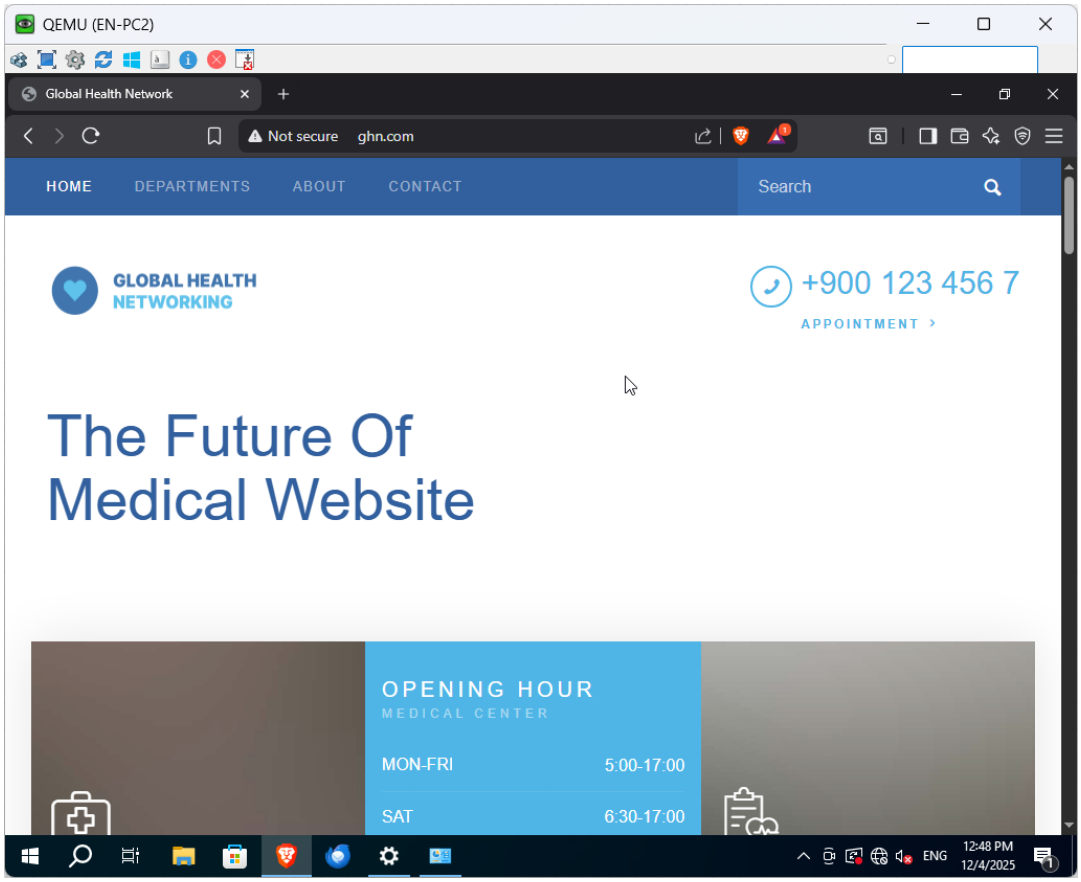

Figure 161 EN-PC2 Accessing GHN Website

The above figures show that the client side (EN-PC2) successfully loaded the entire internal website using the domain name GHN.com, demonstrating that DNS, routing, and IIS were all operational. In order to confirm that the hosting environment was reliable and accessible from other sites inside the GHN network, the website rendered correctly and all page elements loaded through IIS without any delay.

This verifies that the IIS Web Server deployment is finished and functioning properly throughout the network.

FTP Server Setup

The figures below will show how IIS was used to set up the FTP service on BH-Server1. All FTP content and departmental file uploads were stored in a special directory called C:\GHN-FTP. A newly created FTP site called GHN was set up using IIS Manager and connected to the server's internal IP address, 172.16.30.31, on port 21.To enforce user logins, Basic Authentication was turned on. Clients within the GHN network can upload and download files as needed thanks to the site's read/write access for authenticated users.

The FTP site is online and running with the proper bindings and path, according to the final IIS view. All FTP traffic will be encrypted and sent through the DMVPN tunnel.

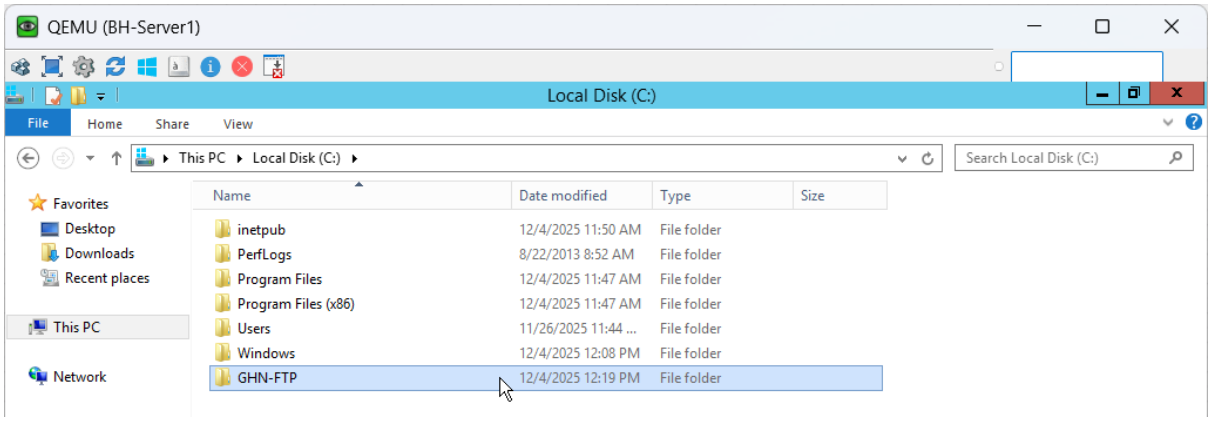

Figure 162 BH-Server1 FTP Server Setup Part 1

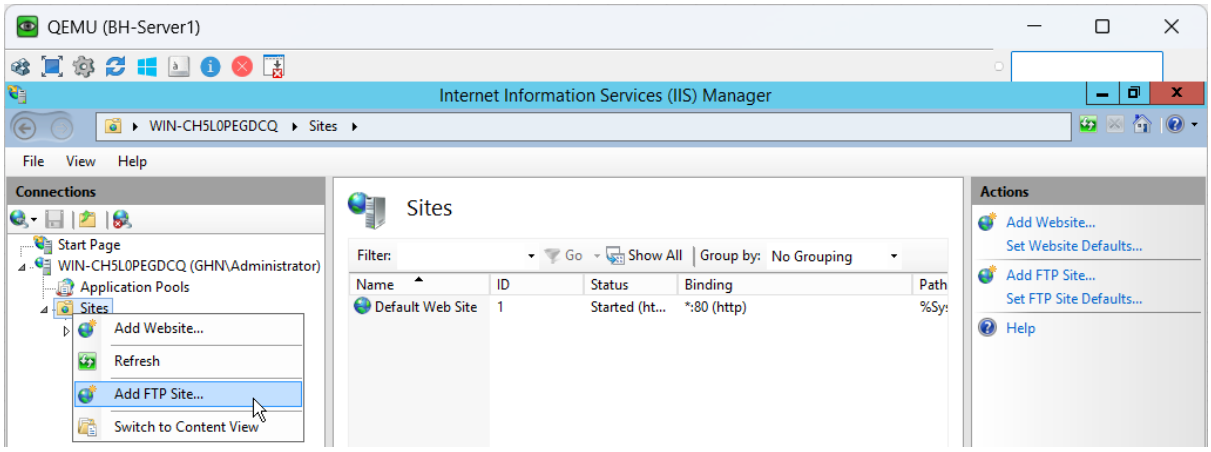

Figure 163 BH-Server1 FTP Server Setup Part 2

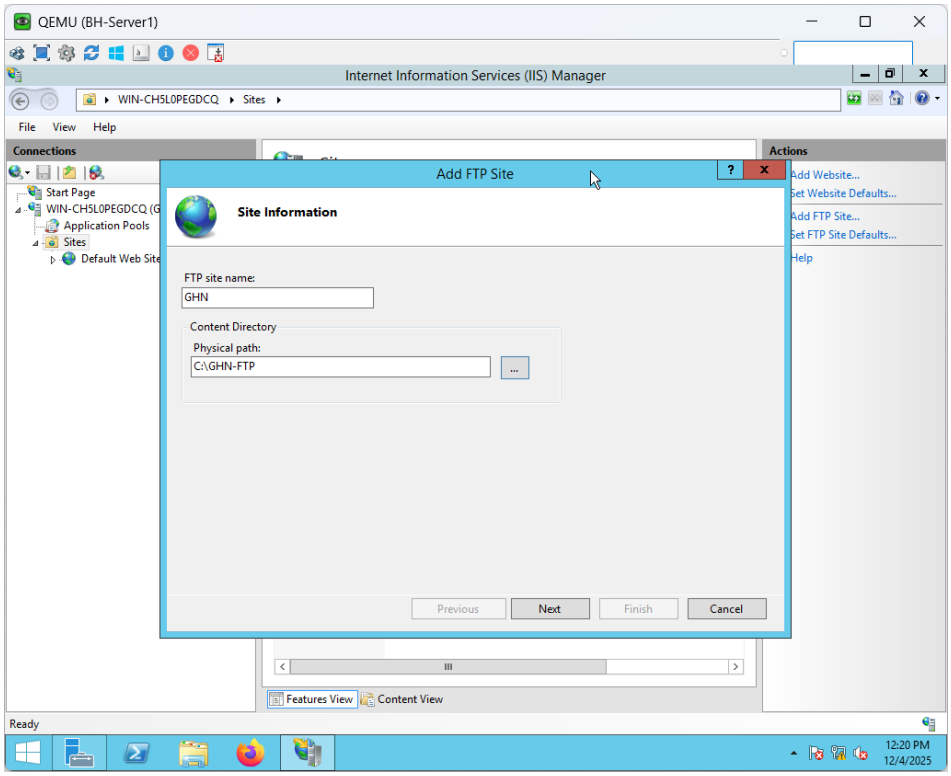

Figure 164 BH-Server1 FTP Server Setup Part 3

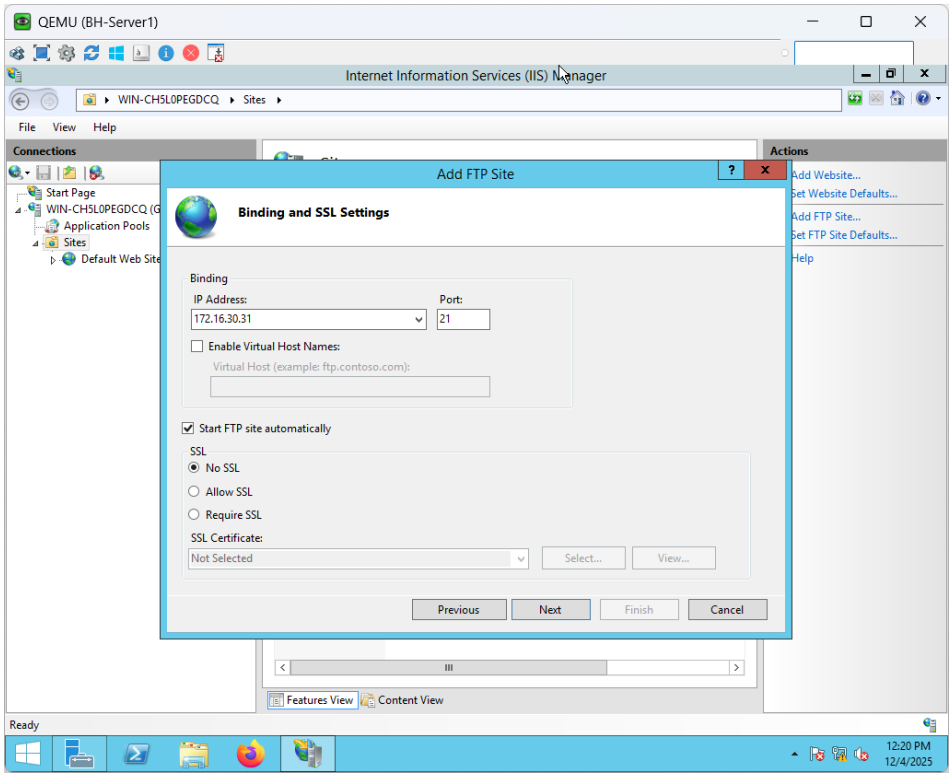

Figure 165 BH-Server1 FTP Server Setup Part 4

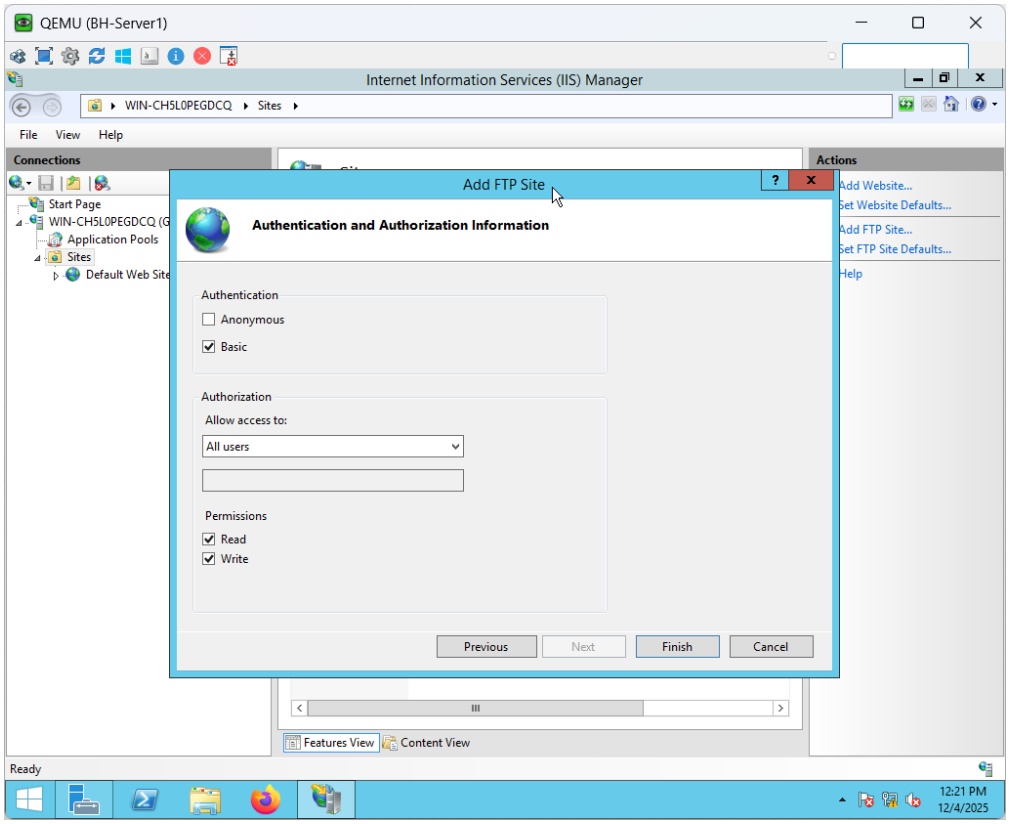

Figure 166 BH-Server1 FTP Server Setup Part 5

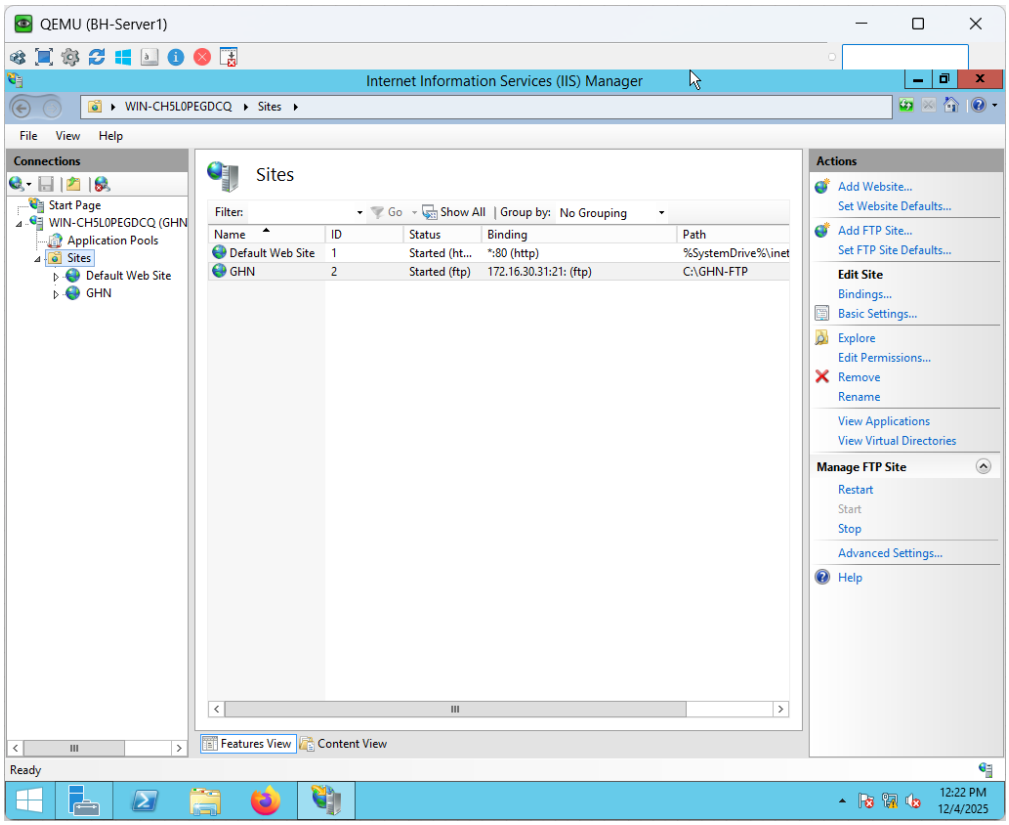

Figure 167 BH-Server1 FTP Server Setup Part 6

FTP Server Verification

The figures below show the FTP Server Verification to ensure that file storage and retrieval between the BH-Server and client computers function properly, the FTP service was thoroughly tested. To verify write permissions and server-side accessibility, a test text file was made directly on the BH-Server within the C:\GHN-FTP directory.

The FTP service was then accessed by a Windows 10 client using the server IP 172.16.30.31 and an authenticated login (Administrator credentials). The test file was successfully obtained by the client, which then opened it and showed the original server-side content. The client demonstrated complete read/write functionality over the network by editing the file and saving the modifications back to the FTP location.

ultimately, the BH-Server opened the identical file again and verified that the client's edits were accurately mirrored. This confirms that IIS FTP settings, directory permissions, routing, and FTP authentication are all operating as planned.

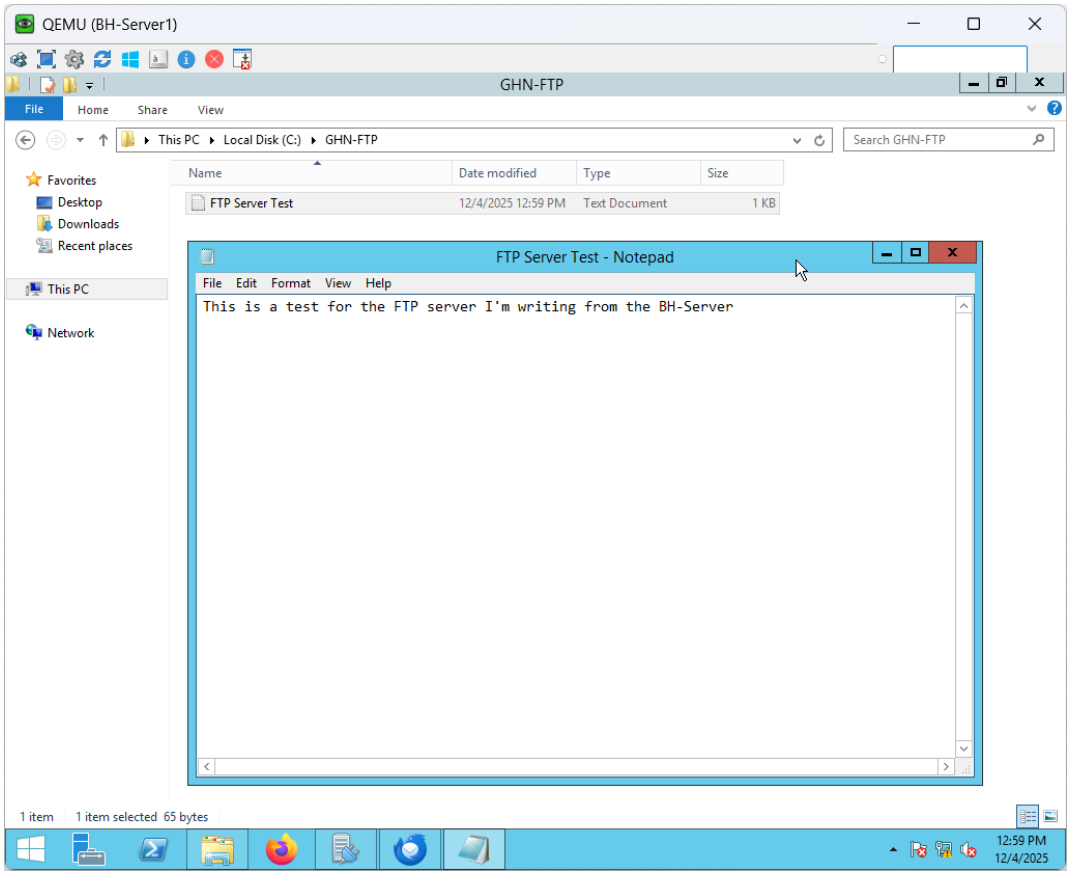

Figure 168 BH-Server1 FTP Server Verification Part 1

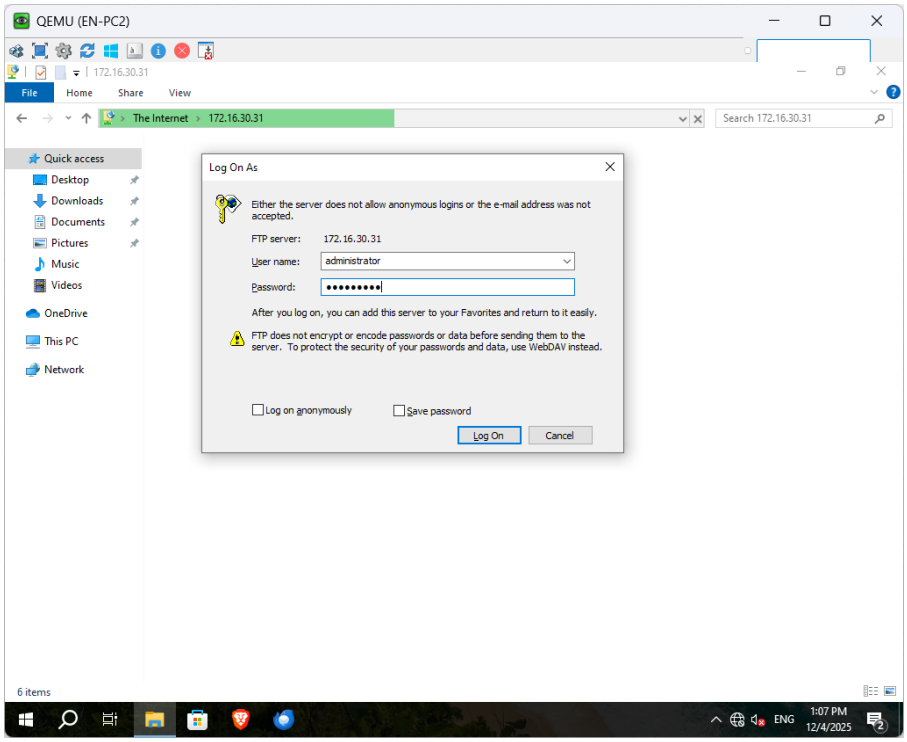

Figure 169 EN-PC2 FTP Server Verification part 1

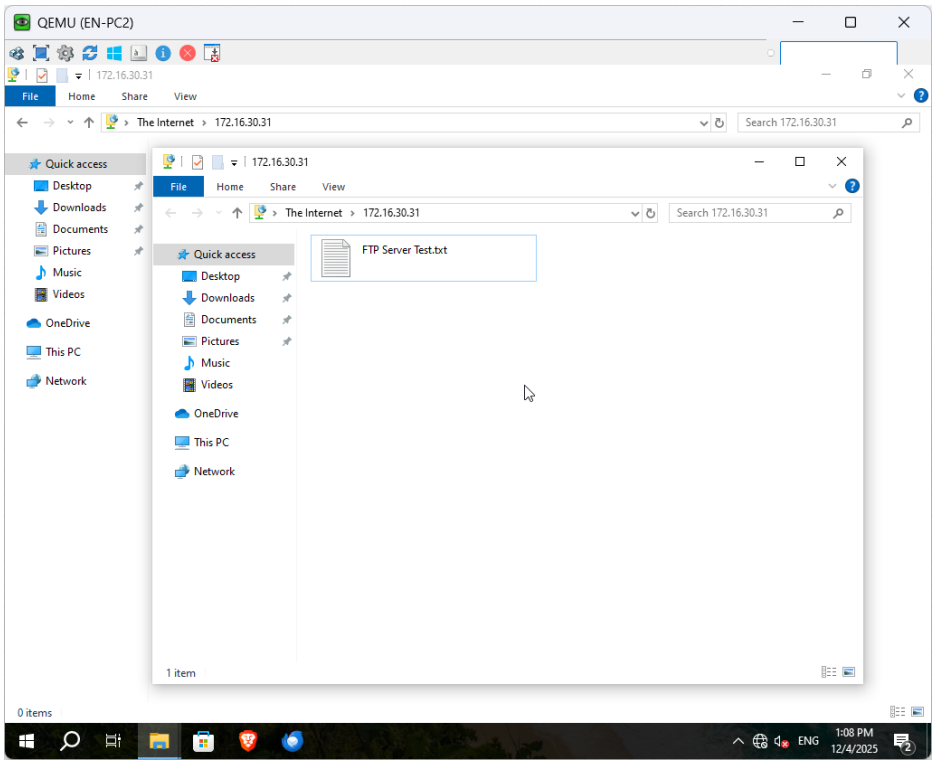

Figure 170 EN-PC2 FTP Server Verification Part 2

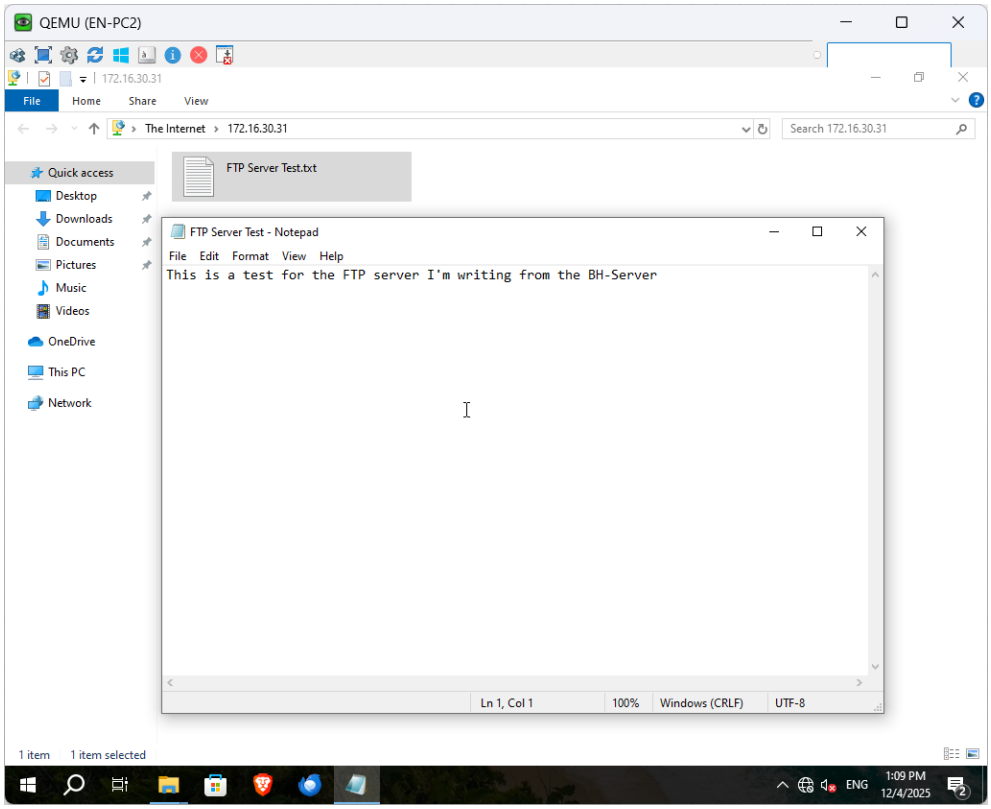

Figure 171 EN-PC2 FTP Server Verification Part 3

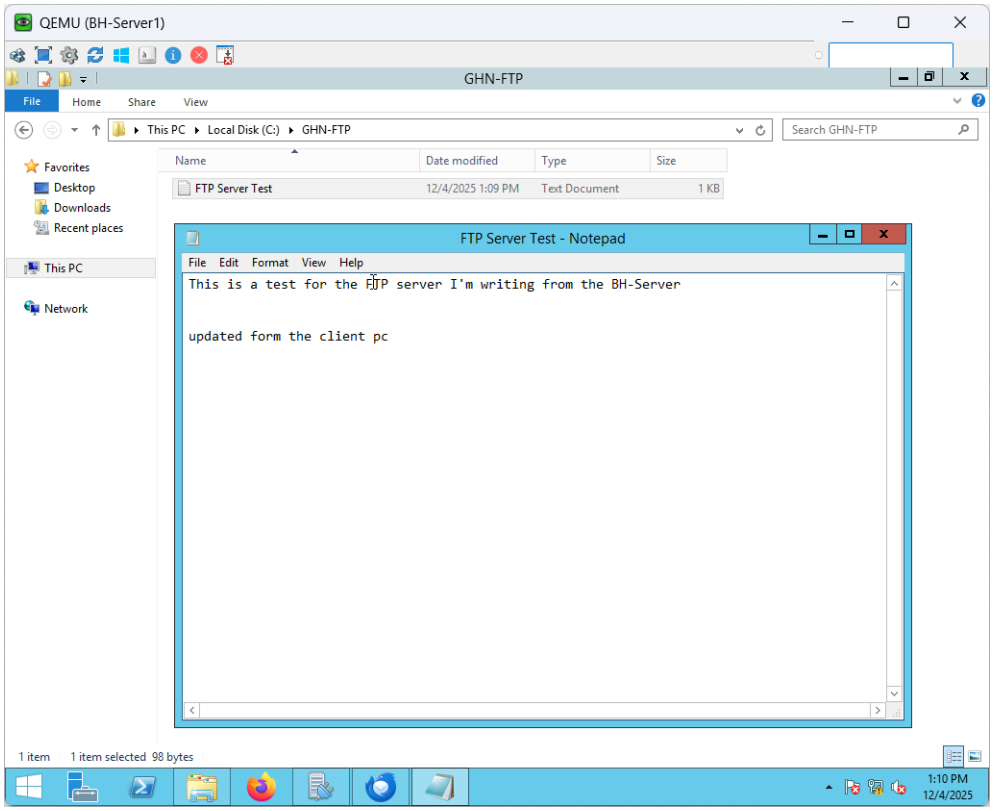

Figure 172 BH-Server1 FTP Server Verification Part 2

Email (hMailServer) Setup

The complete configuration of the GHN internal mail system using hMailServer is shown in the figures below. This entails setting up the GHN.com domain, downloading and installing the mail server, and setting up user mailboxes. These procedures confirm that the mail service is completely functional and lay the groundwork for internal email communication within the GHN network.

hMailServer Installation

hMailServer, a lightweight and resource-efficient solution that matches the project's requirements, is used to create the mail server for GHN. Downloading version 5.6.8 from the official website and starting the setup wizard are the first steps in the installation process. To enable complete management from the same virtual machine, the server and administrative tools are installed.

To save on the overhead of setting up external SQL servers, the built-in Microsoft SQL Compact database engine is chosen during setup. The key credential needed to access and set up the mail server is a master administrative password.

The hMailServer Administrator automatically opens after installation is finished, requesting the hostname and login information so that server configuration can start.

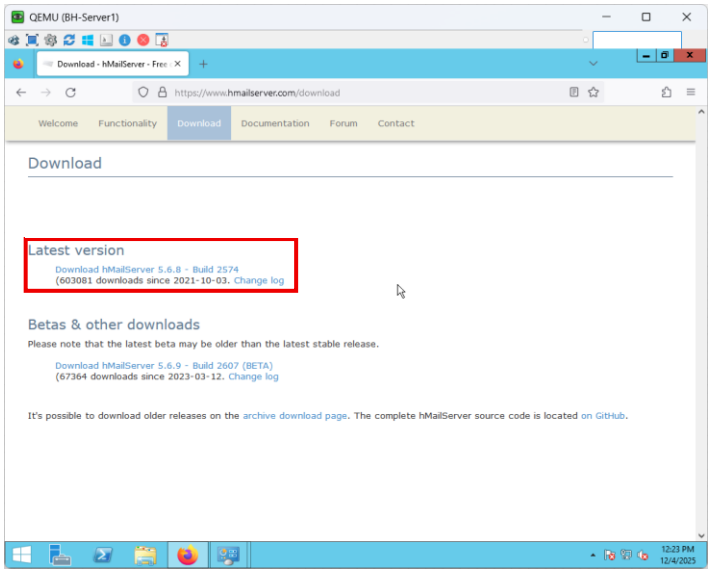

Figure 173 hMailServer Installation Part 1

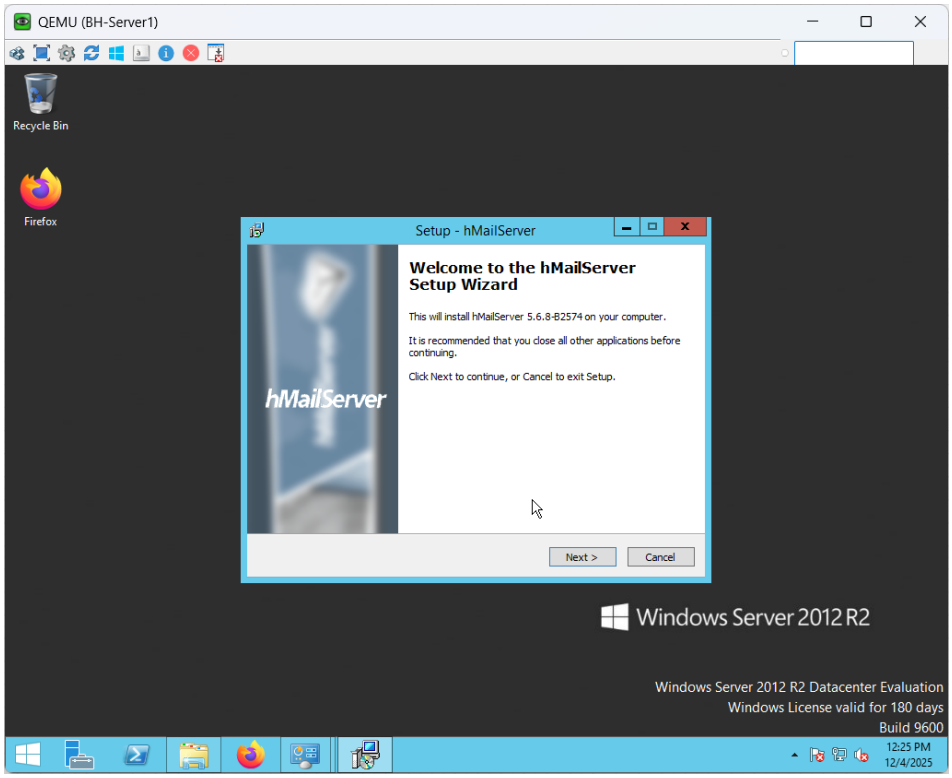

Figure 174 hMailServer Installation Part 2

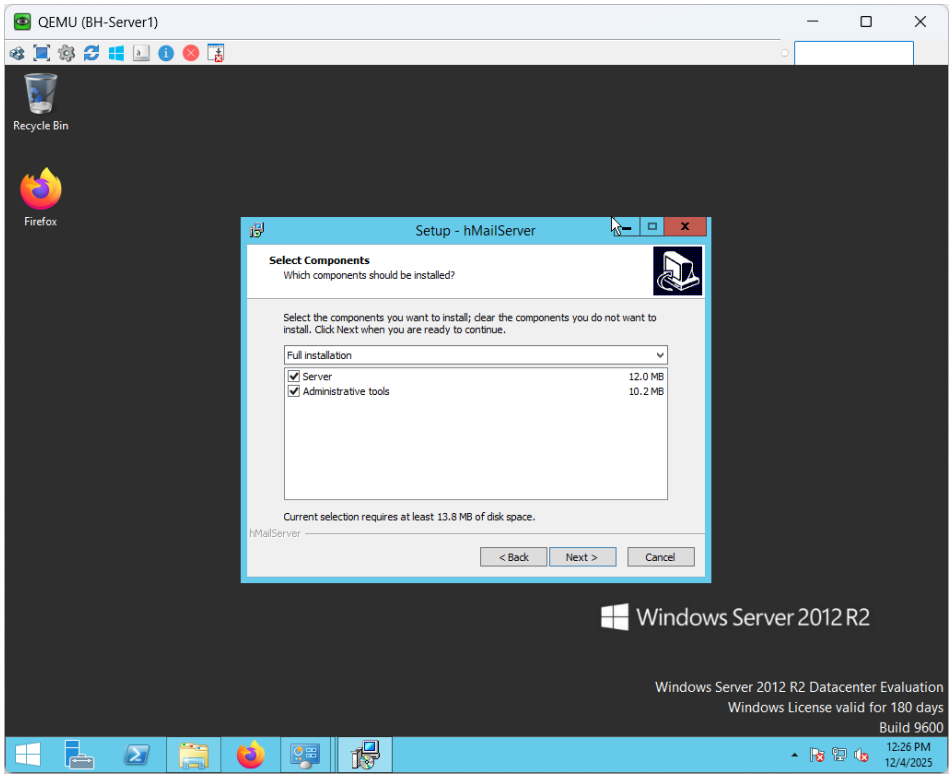

Figure 175 hMailServer Installation Part 3

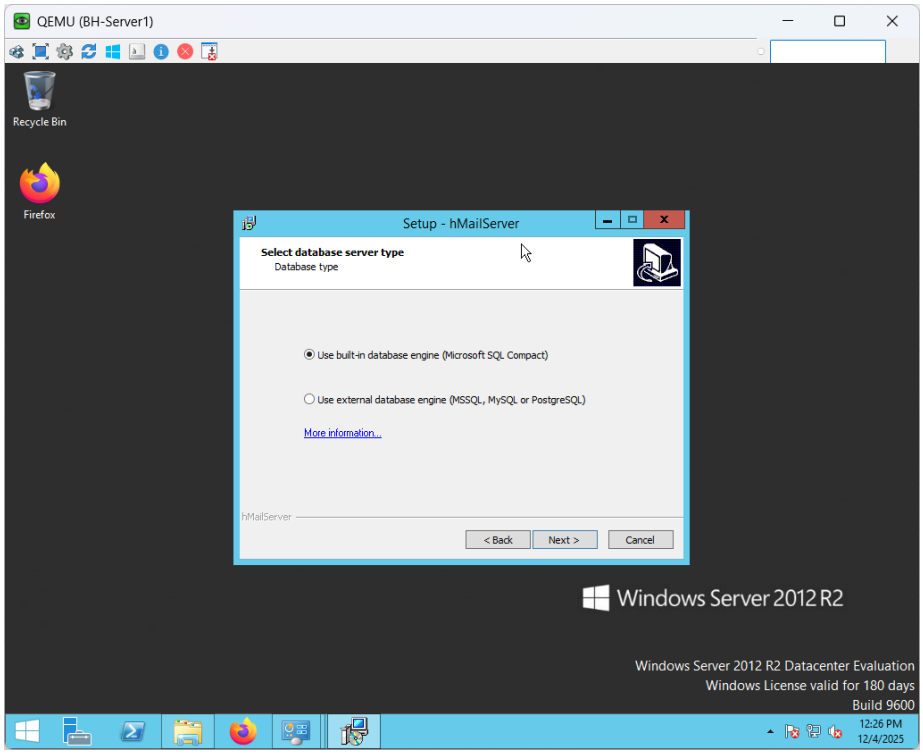

Figure 176 hMailServer Installation Part 4

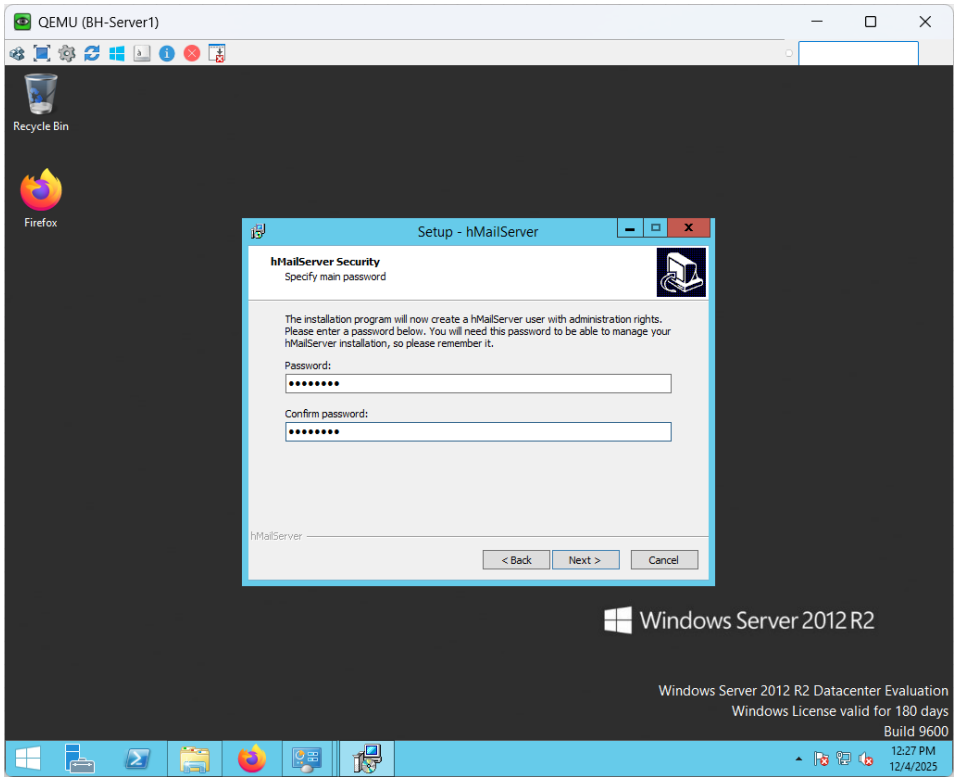

Figure 177 hMailServer Installation Part 5

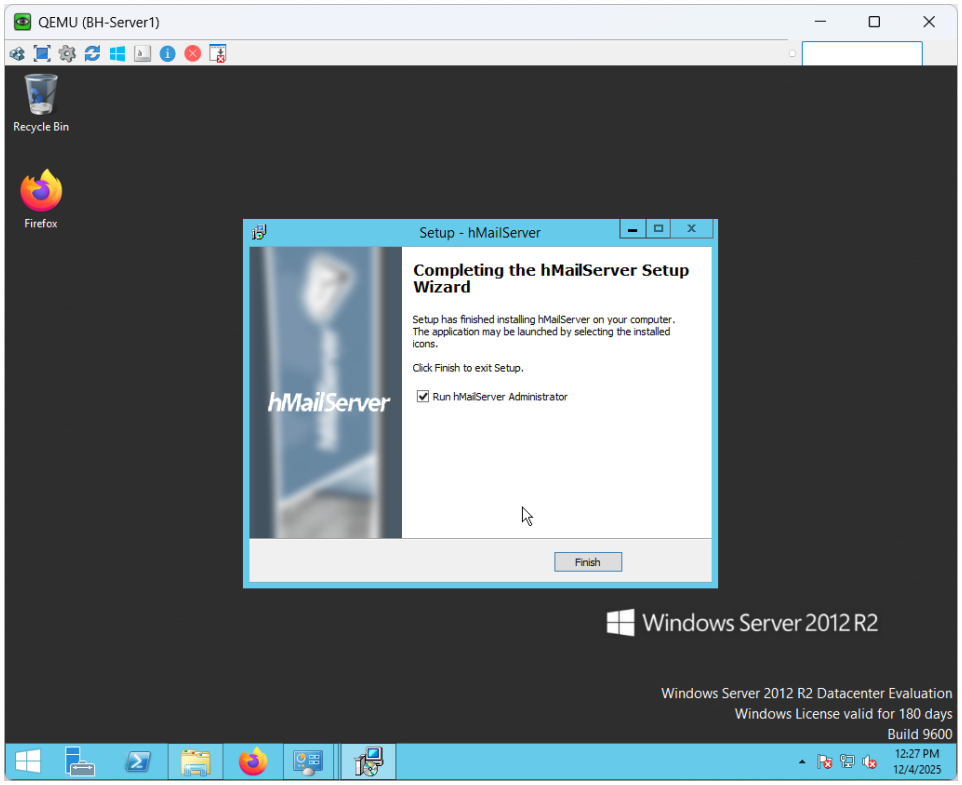

Figure 178 hMailServer Installation Part 6

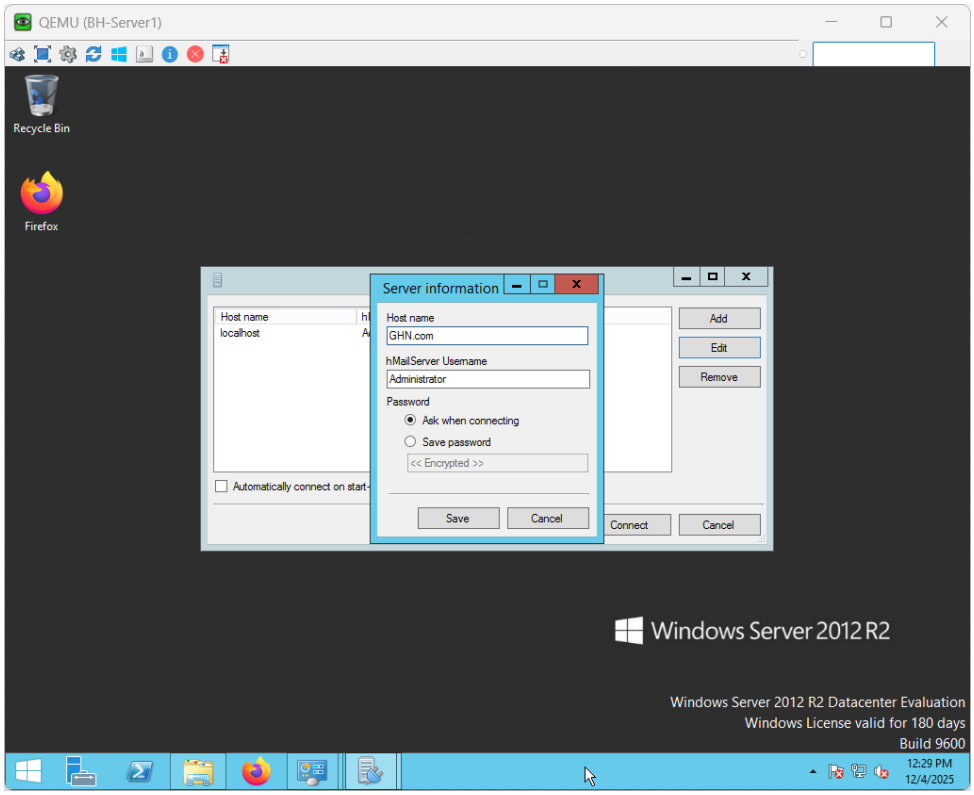

Figure 179 hMailServer Installation Part 7

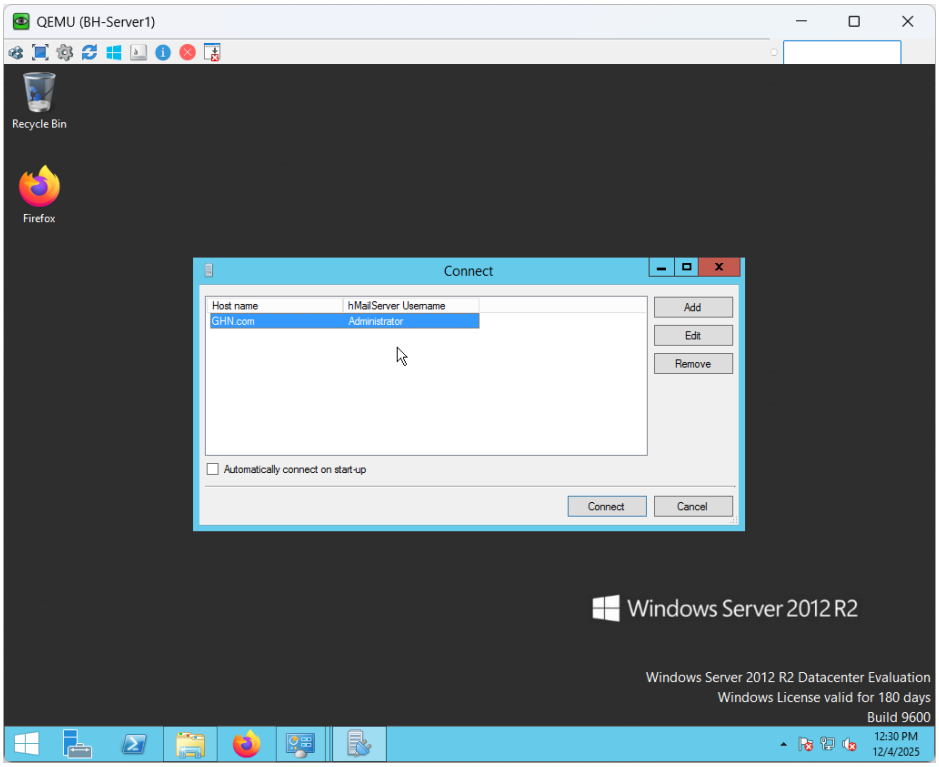

Figure 180 hMailServer Installation Part 8

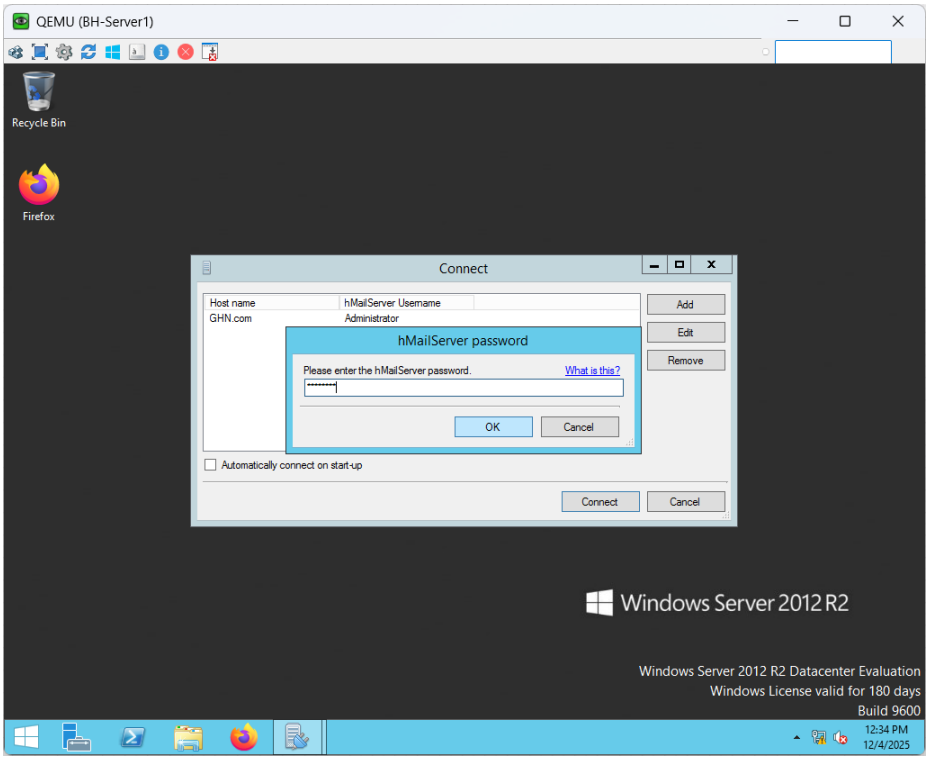

Figure 181 hMailServer Installation Part 9

Domain Configuration

The finger below shows the environment, a new email domain called GHN.com is created. This domain serves as the parent for all user mailboxes and represents Global Health Networking's internal mail system. The domain is activated and prepared for account provisioning when it has been created.

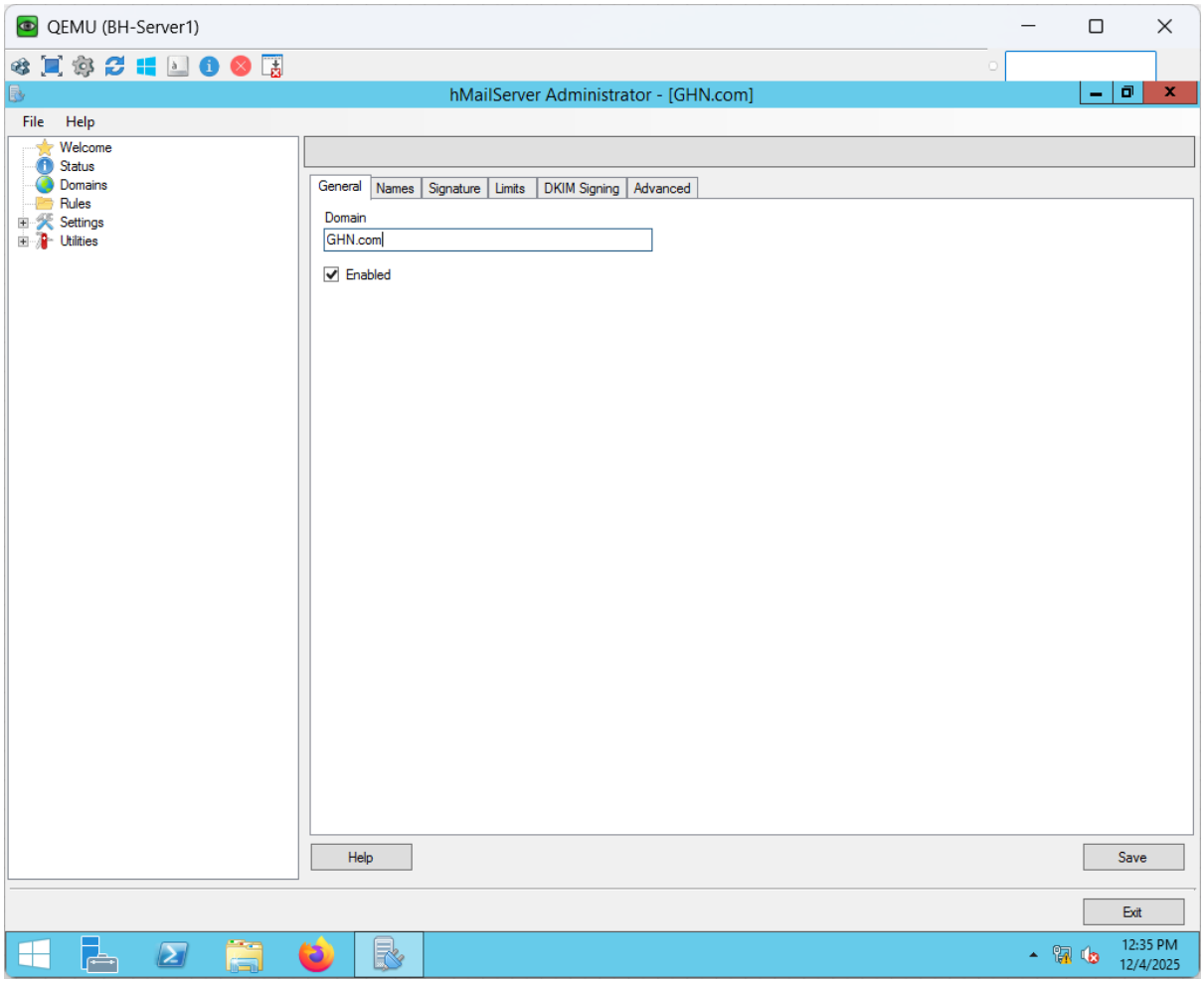

Figure 182 hMailServer Domain Configuration

User Mailbox Creation

The fingers below show the GHN.com domain now has two added internal mail accounts:

- Ali@GHN.com
- Hussain@GHN.com

Every account is configured to the default user administration level, given a password, and enabled. These accounts will be included in the testing process to verify SMTP/POP3/IMAP functionality and are used for internal communication.

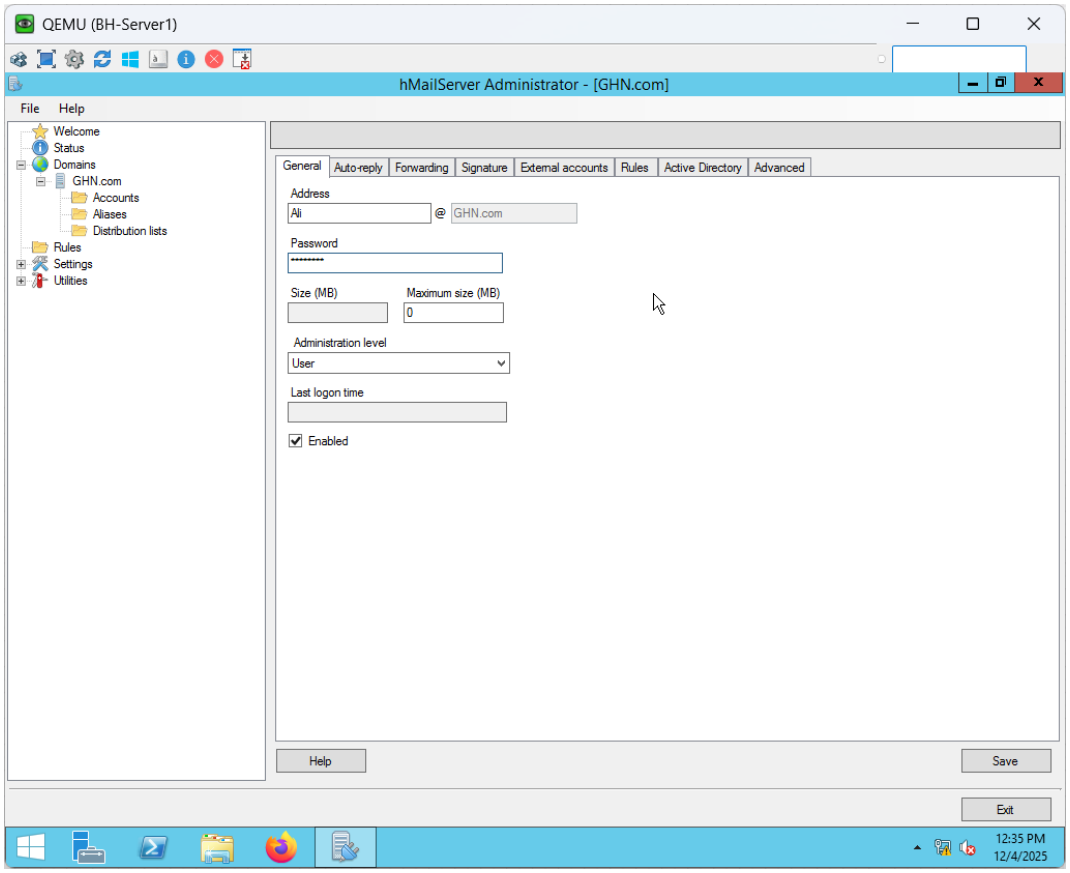

Figure 183 hMailServer Email Account Creation Part 1

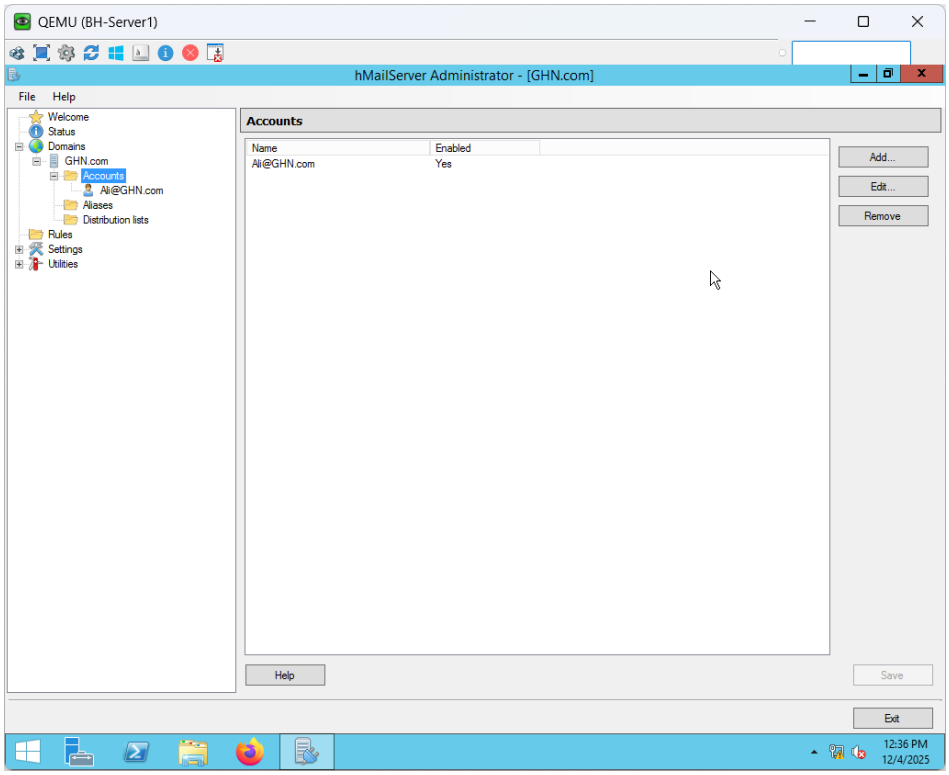

Figure 184 hMailServer Email Account Creation Part 2

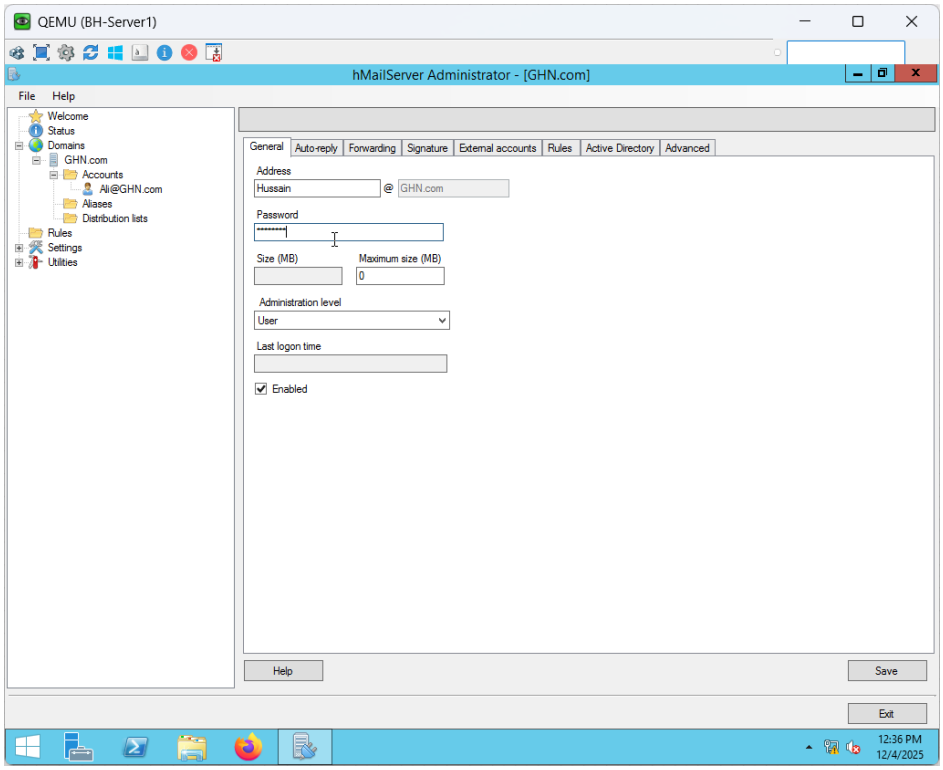

Figure 185 hMailServer Email Account Creation Part 3

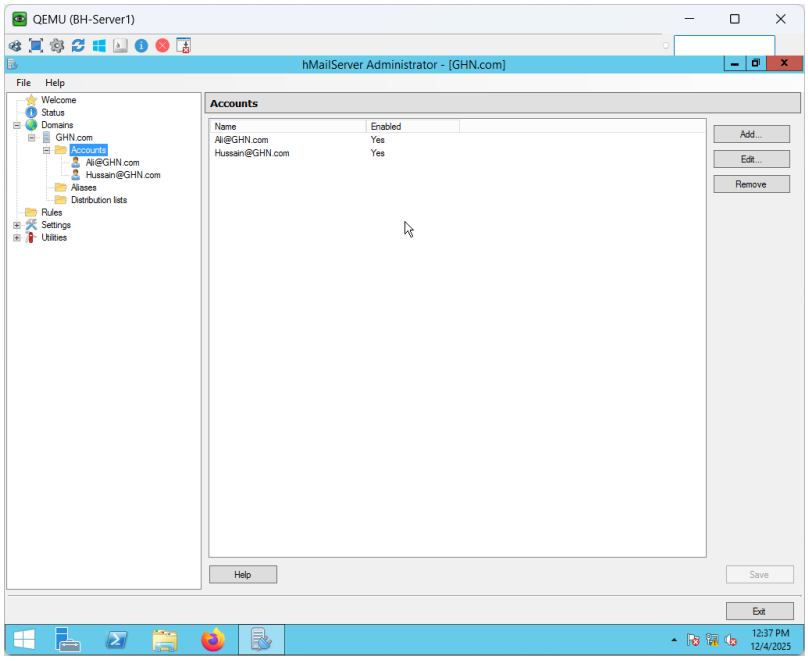

Figure 186 hMailServer Email Account Creation Part 4

Thunderbird Installation

In order for customers to access and verify their GHN.com mailboxes, a local mail client is necessary to finish the email service setup. Thunderbird serves as the lightweight email client, enabling complete IMAP/SMTP configuration and end to end hMailServer deployment testing. The figures below that follow demonstrate how to download and install Thunderbird on Bh-Server1 and EN-PC2 before setting up user mail accounts.

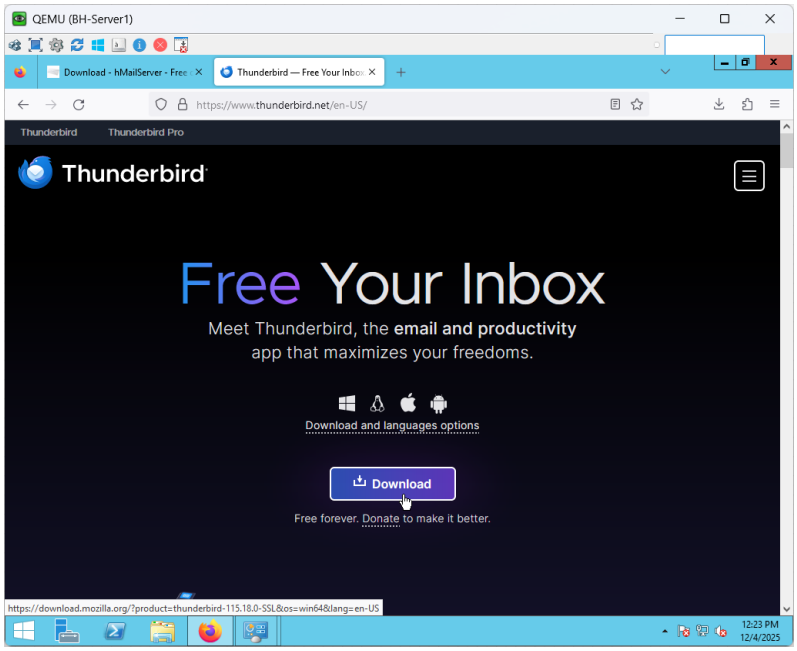

Figure 187 BH-Server1 Thunderbird Installation Part 1

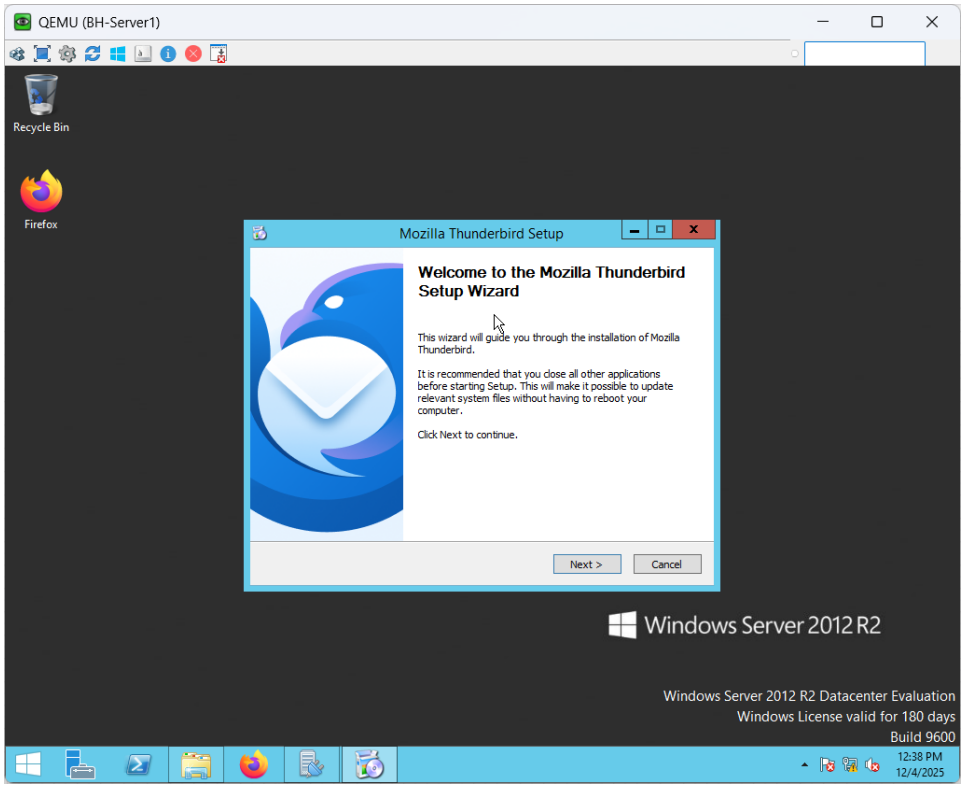

Figure 188 BH-Server1 Thunderbird Installation Part 2

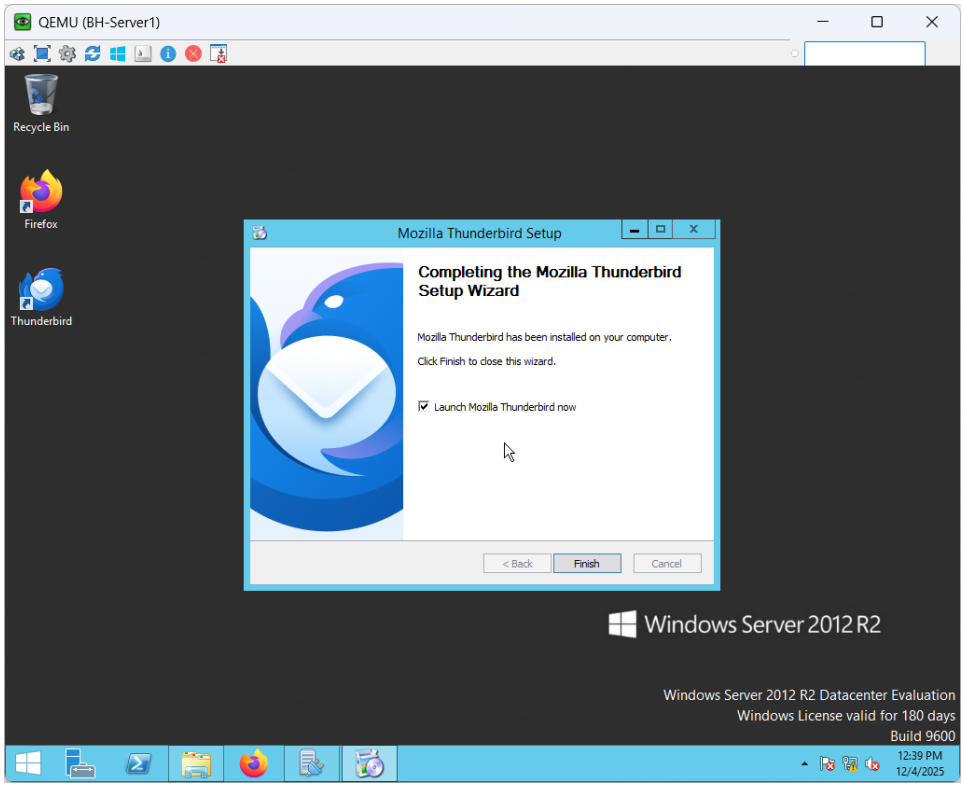

Figure 189 BH-Server1 Thunderbird Installation Part 3

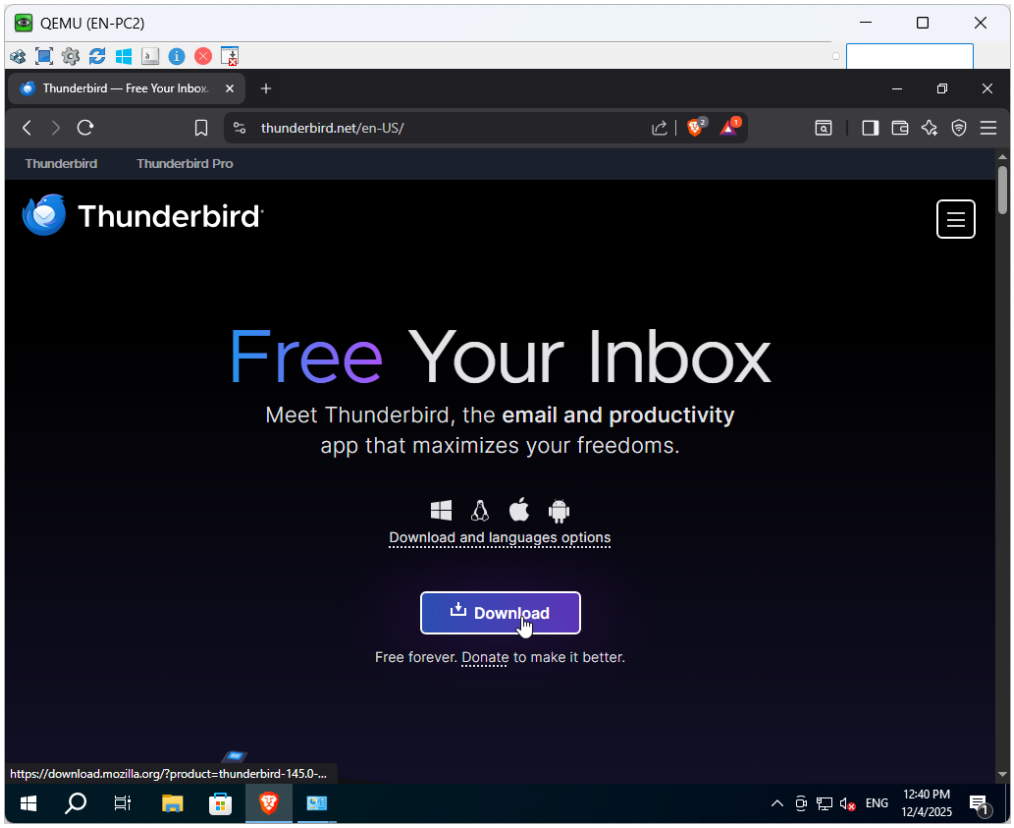

Figure 190 EN-PC2 Thunderbird Installation Part 1

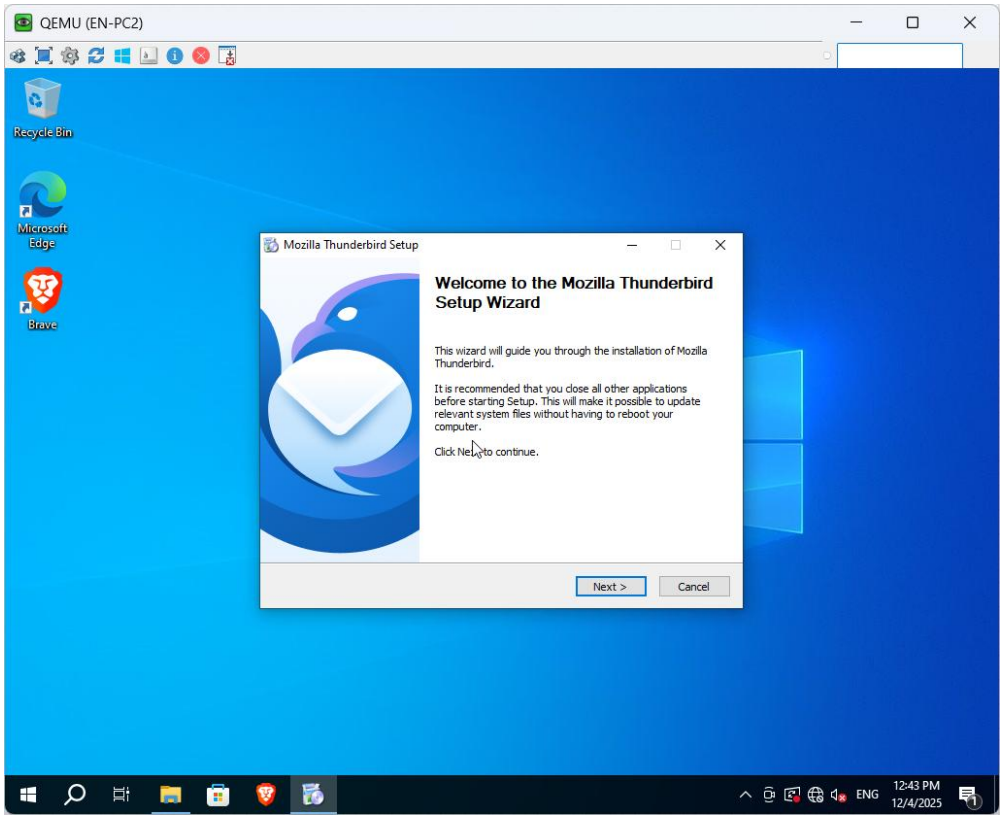

Figure 191 EN-PC2 Thunderbird Installation Part 2

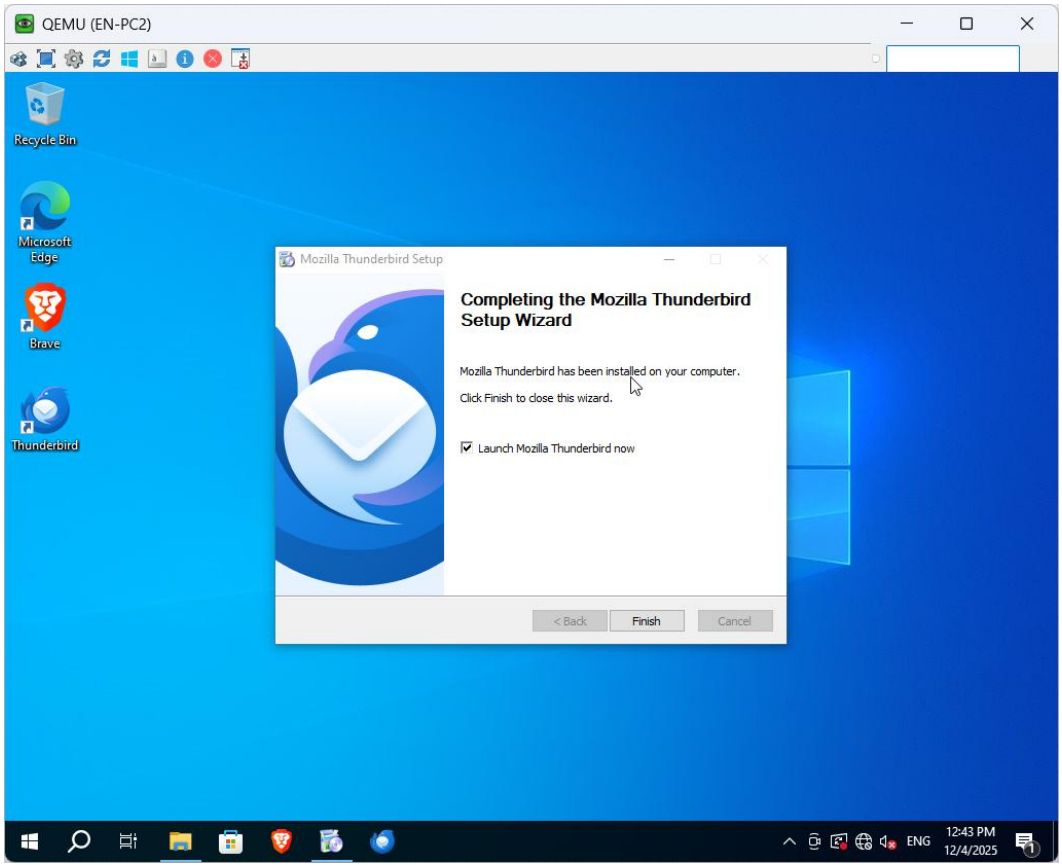

Figure 192 EN-PC2 Thunderbird Installation Part 3

Email Client Configuration

The figures below show Thunderbird was installed and used as the email client on both the server and the client PC to confirm that the hMailServer accounts are operational and accessible over the GHN network. The installation process, automatic account detection, and the successful setup of IMAP mailboxes for every user. This attests to the mail service's functionality, domain integration, and accessibility from many endpoints.

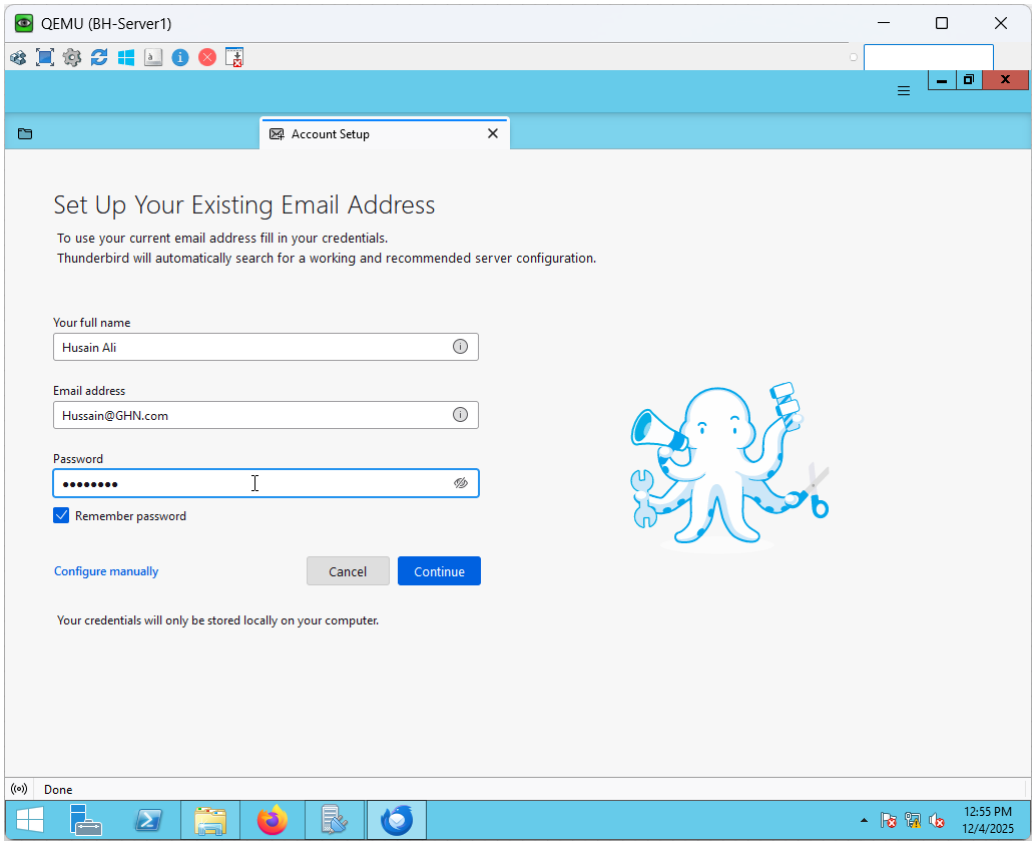

Figure 193 Hussain Email Client Configuration Part 1

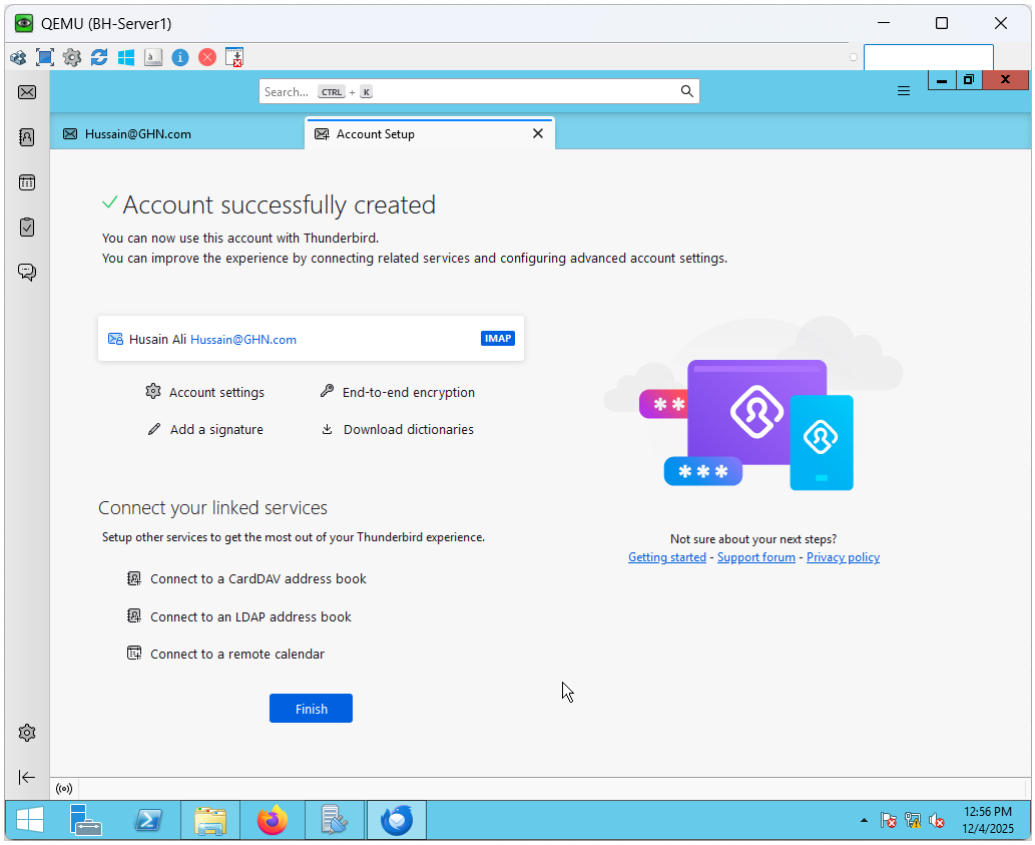

Figure 194 Hussain Email Client Configuration Part 2

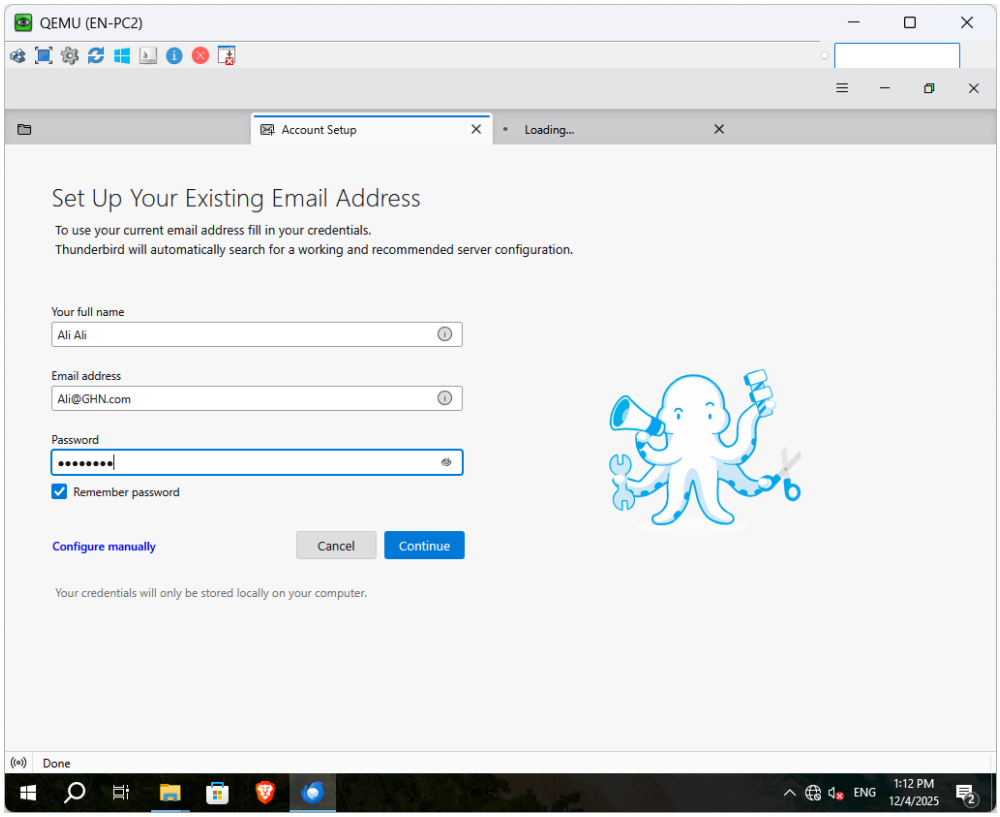

Figure 195 Ali Email Client Configuration Part 1

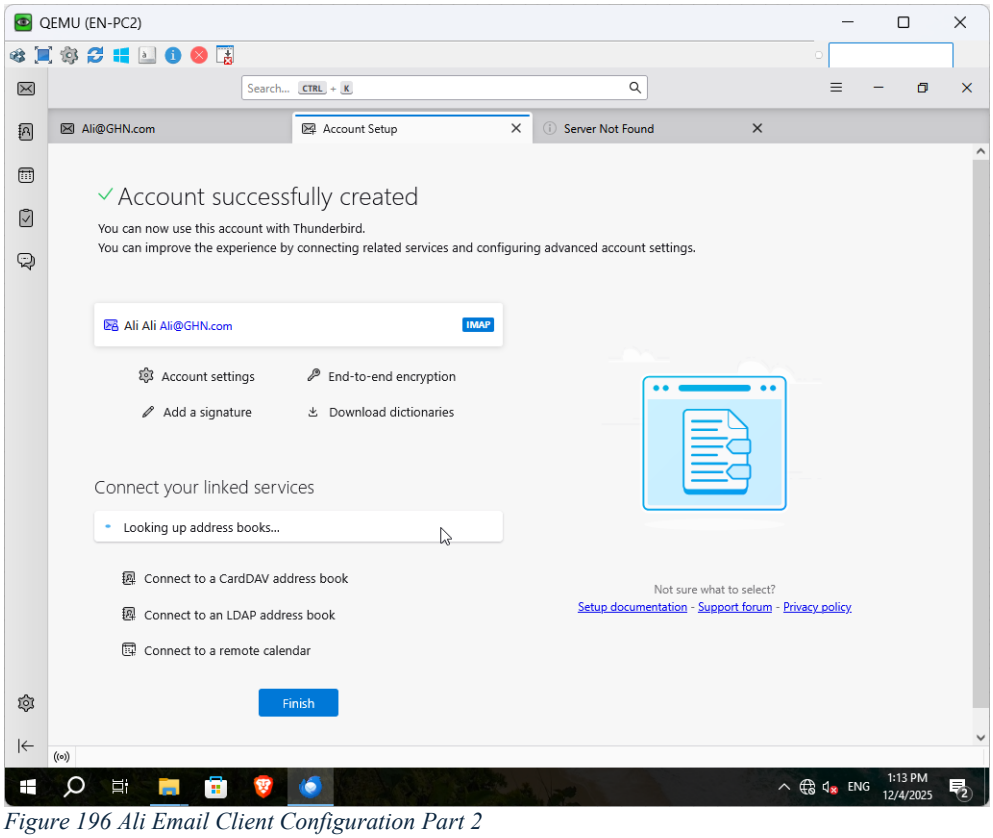

Figure 196 Ali Email Client Configuration Part 2

Email Server Verification

The figures below Verifying that the email accounts were capable of being utilized by real end users came next once they were created in hMailServer. To test IMAP connectivity, account authentication, and end-to-end email transmission, Thunderbird was installed on both the client PC and the server. Thunderbird correctly recognized the server settings once each user checked in with their designated GHN.com credentials. To verify that the mail service is fully functional across the network, test mails were sent between the users while both accounts were active.

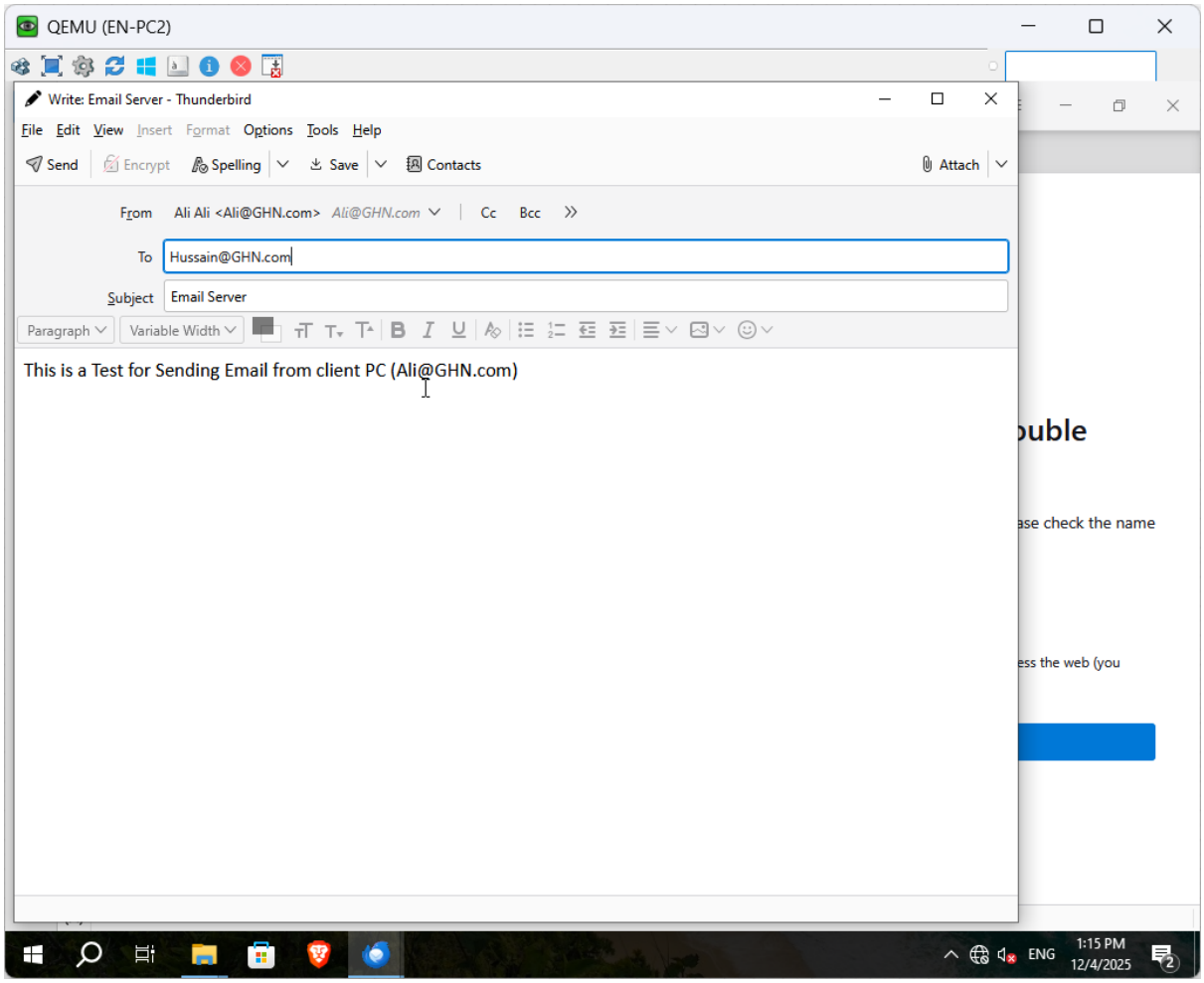

Figure 197 Email Server Verification Part 1

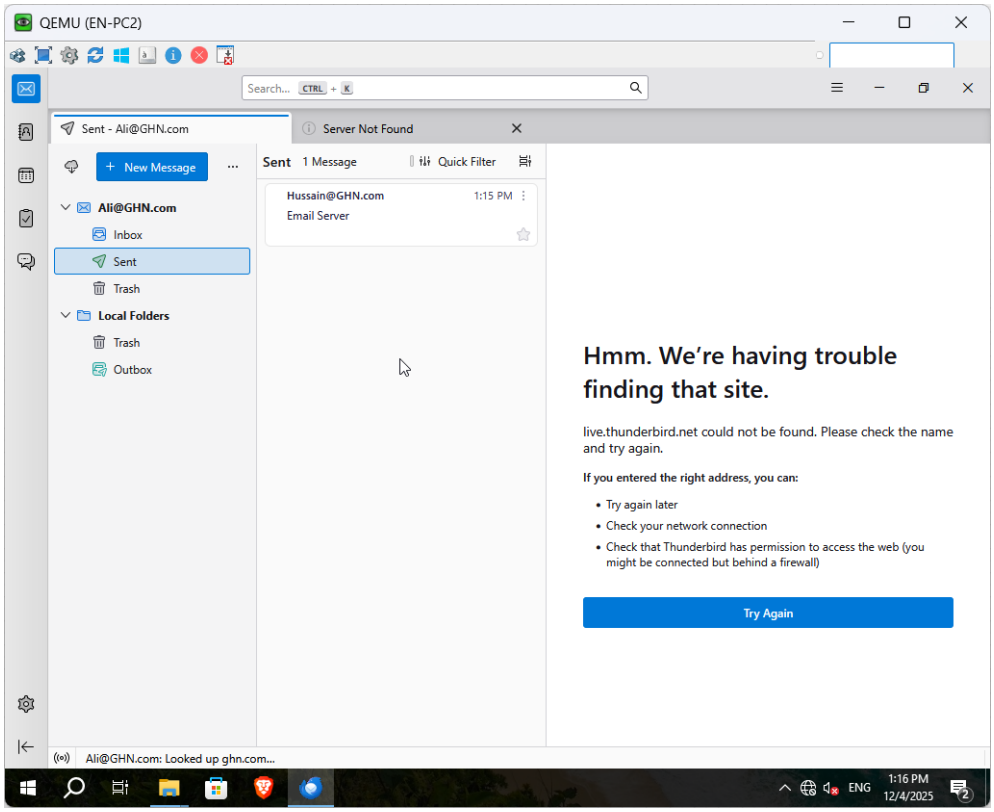

Figure 198 Email Server Verification Part 2

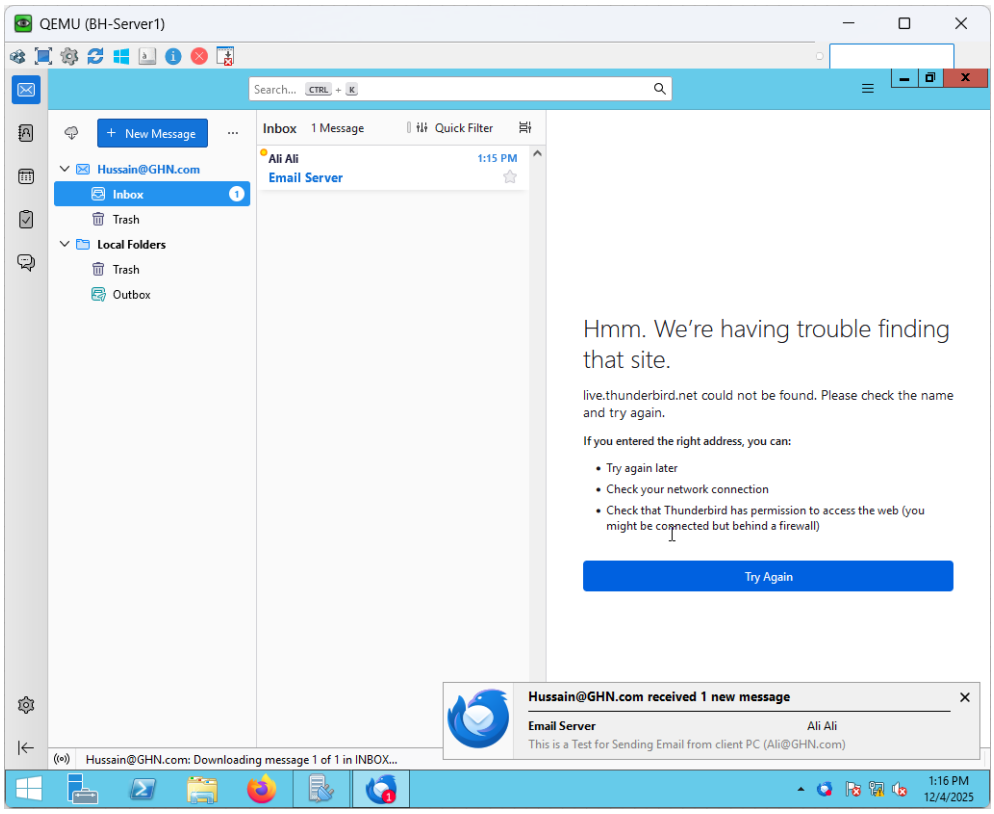

Figure 199 Email Server Verification Part 3

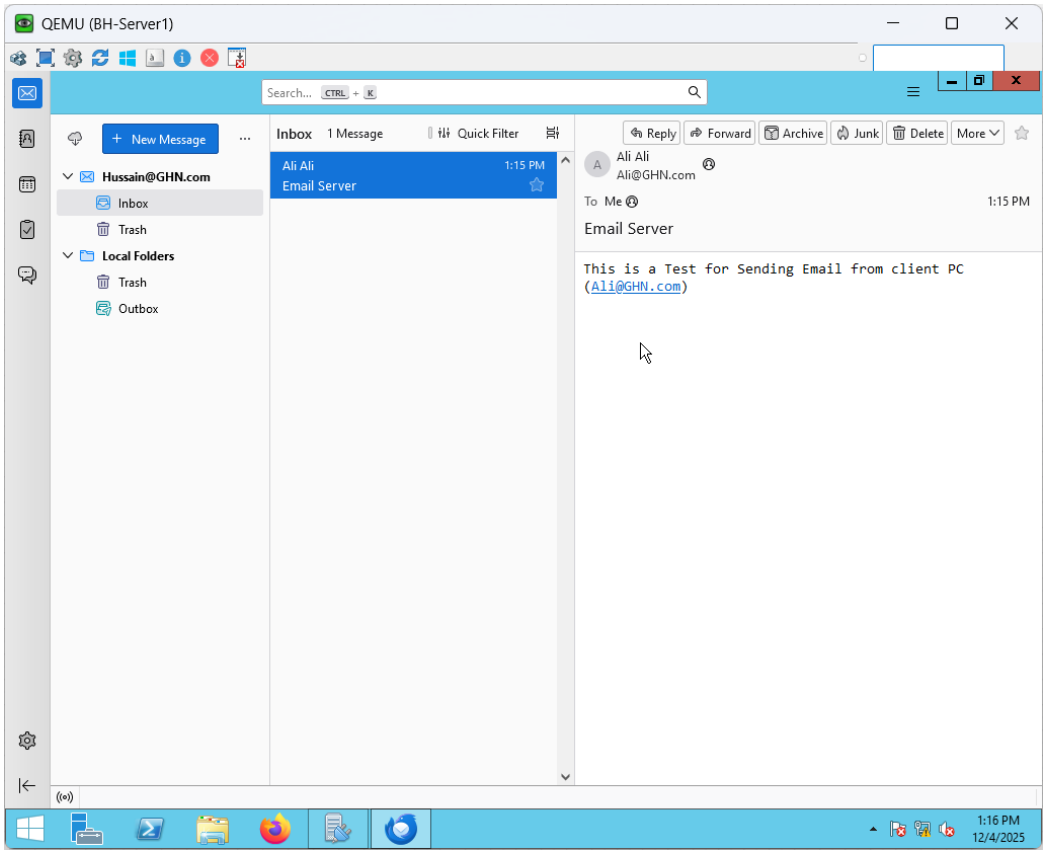

Figure 200 Email Server Verification Part 4

DHCP Setup

Throughout the GHN infrastructure, the DHCP service is set up to automate IP address issuance and minimize manual configuration. DHCP guarantees that client devices receive accurate and consistent addressing information by specifying scopes, lease periods, and crucial network parameters like gateways. This reduces setup errors, increases scalability, and makes network administration easier. As an example, the setup and verification of the DHCP service China branch are described in the following subsection.

This figures below verifies that internal PCs are receiving IPv4 addresses from the branch router via DHCP. For the IT network and the Guests network, two distinct DHCP pools were set up, each with its own subnet, default gateway, and prohibited addresses. Both client PCs were able to successfully acquire valid IP addresses in their respective VLANs and the appropriate default gateways after turning on DHCP on the router. The DHCP service is operating as intended, as demonstrated by a brief ping test between the two clients that reveals full reachability within the local LAN.

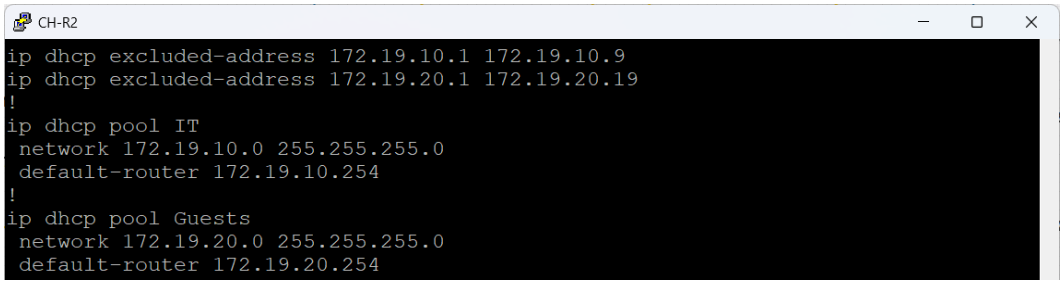

Figure 201 CH-R2 DHCP configuration

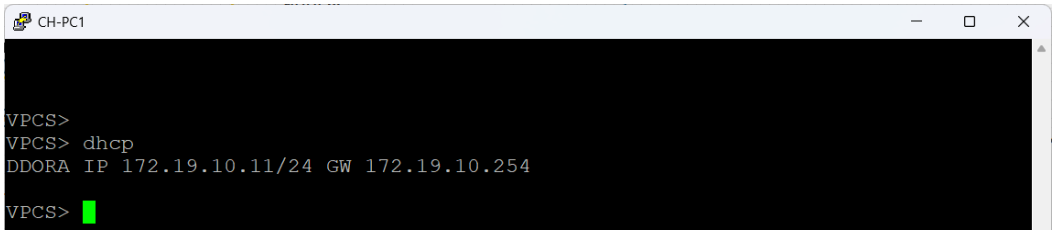

Figure 202 CH-PC1 DHCP Assigned

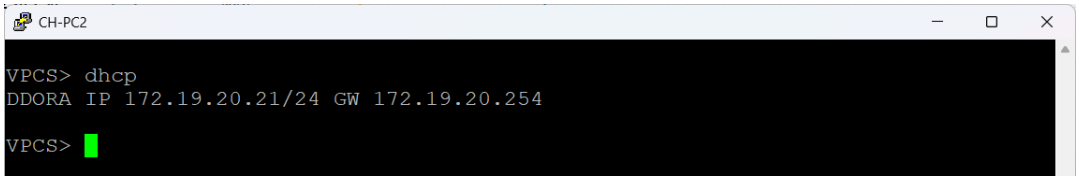

Figure 203 CH-PC2 DHCP Assigned

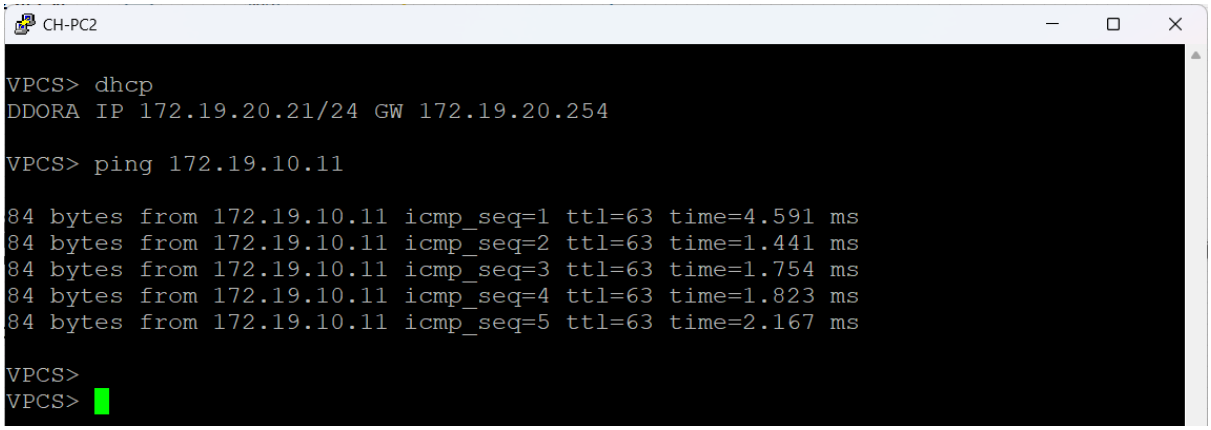

Figure 204 CH-PC2 DHCP Verification

AAA Setup

The purpose of the AAA service is to centralize accounting, authorization, and authentication for network device access throughout the GHN ecosystem. AAA makes guarantee that only authorized individuals may control switches, routers, and other vital services by utilizing a dedicated server to verify user credentials and enforce role-based permissions. This strategy improves operational security, raises responsibility, and offers a consistent way to manage administrative access. The configuration and integration of AAA into the GHN network are explained in this section.

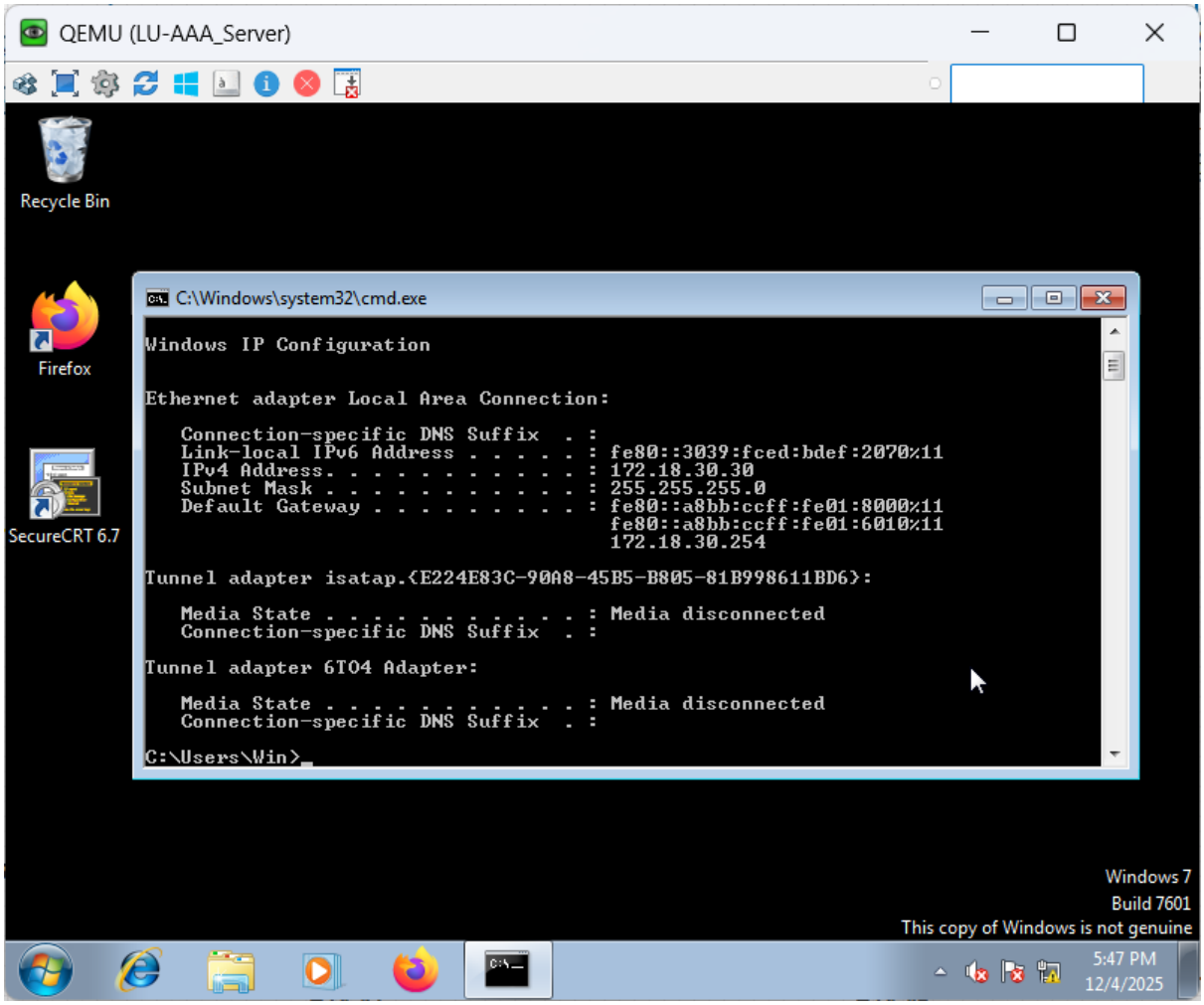

Figure 205 LU-AAA_Server IP Address

The above figure shows the IP address Assigned to the LU-AAA_Server

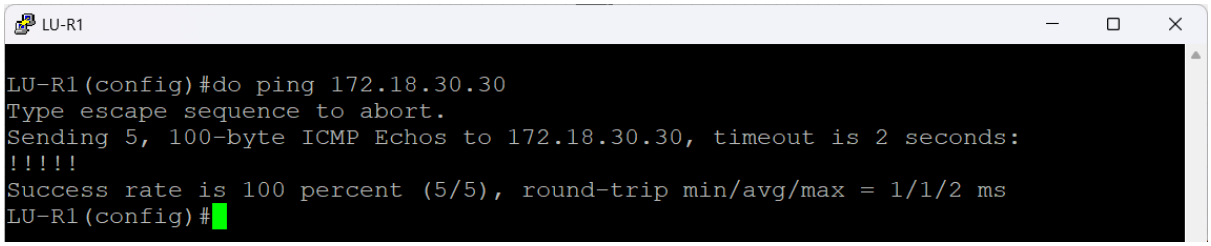

Figure 206 LU-R1 Ping Verification

The above figure verifies the reachability between the router and the AAA server and that is an important thing to consider before configuring the WinRadius Server

WinRadius User Creation

By adding local RADIUS users and verifying their credentials using the integrated authentication tester, the figures below demonstrate that the AAA server is completely functional. The entire procedure creating a user, setting up their credentials, and sending an Access-Request packet to make sure the server reacts appropriately is depicted in the figures. This confirms that the RADIUS service is operational, accessible, and capable of authenticating networked devices.

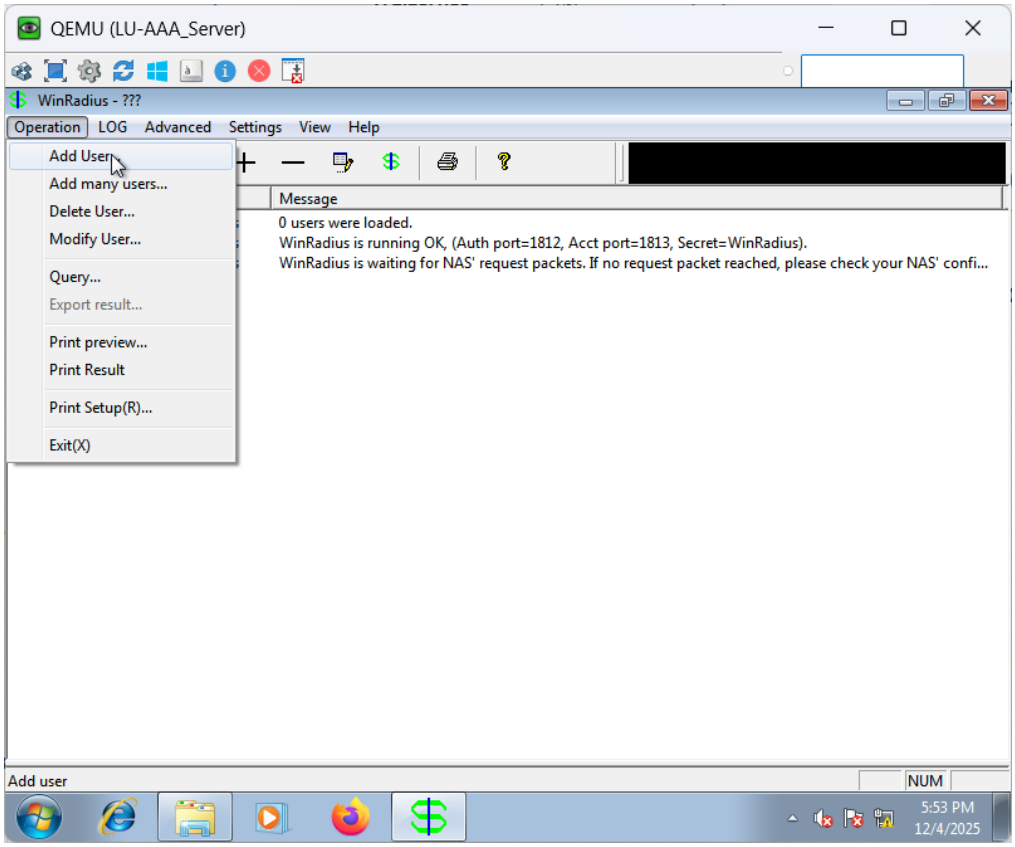

Figure 207 WinRadius User Creation Part 1

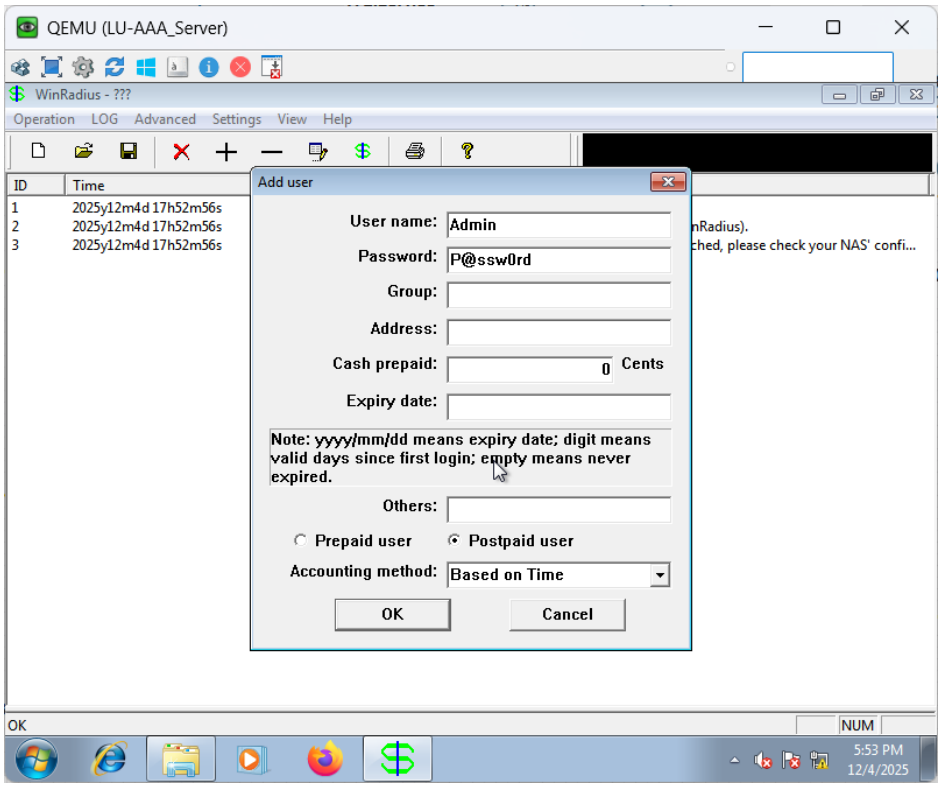

Figure 208 WinRadius User Creation Part 2

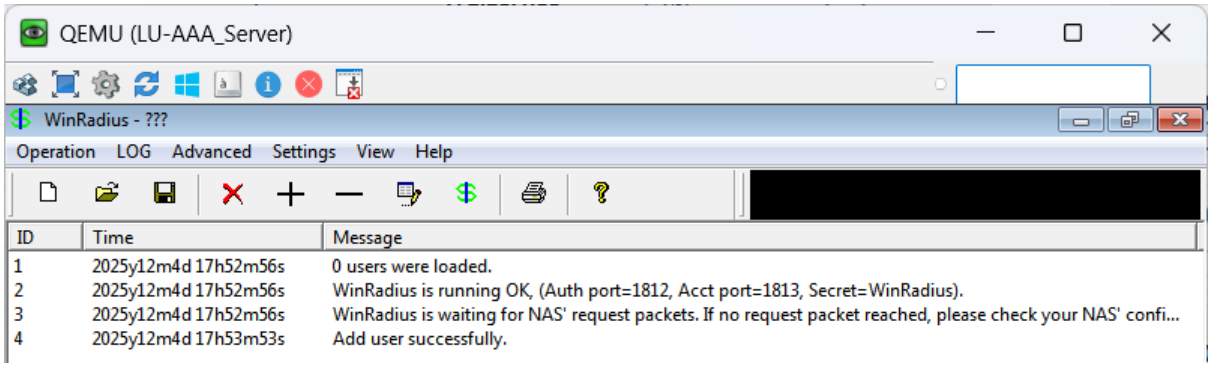

Figure 209 WinRadius User Creation Part 3

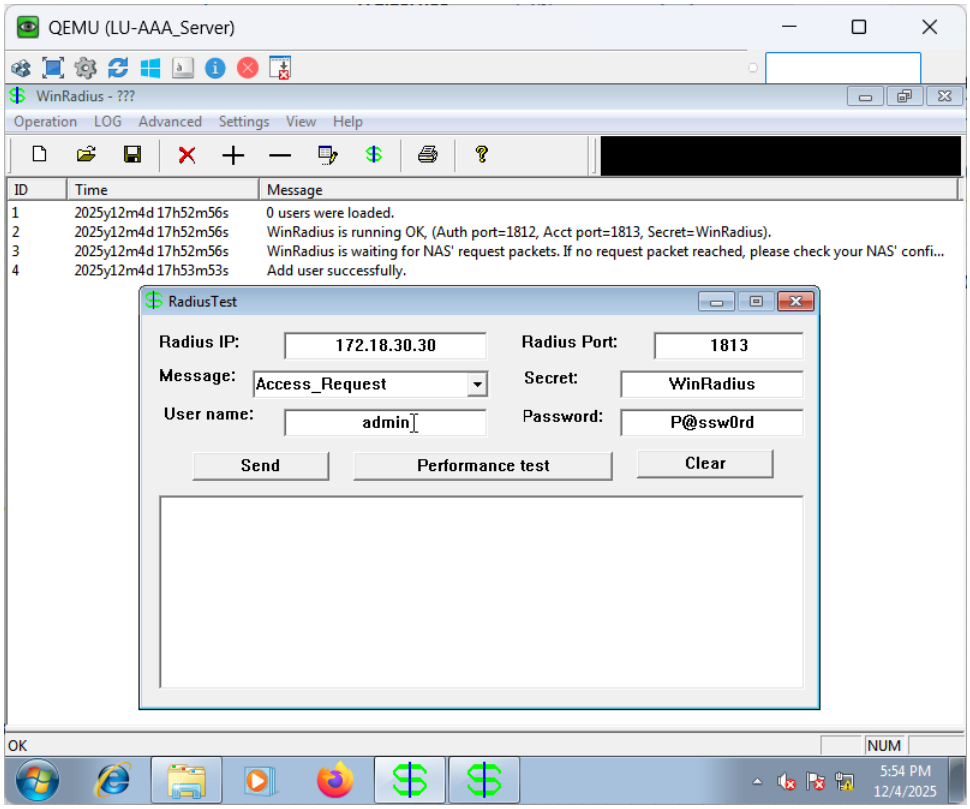

Figure 210 WinRadius User Authentication Verification Part 1

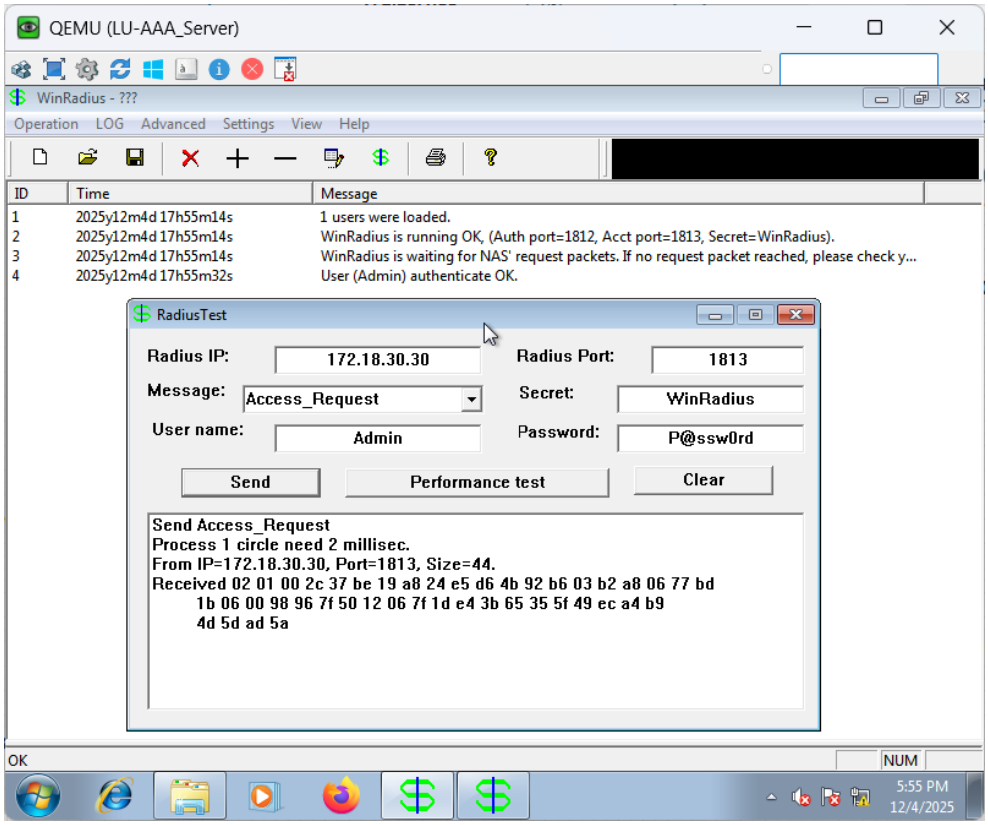

Figure 211 WinRadius User Authentication Verification Part 2

Network device AAA Configuration

the figures below show that the LU-AAA RADIUS server is used by the router to authenticate every attempt at login. In order to guarantee that the device is still reachable even in the event that the AAA server is unreachable, the setup also contains encrypted secrets and a local fallback account.

Setting a secure enable secret and turning on AAA (aaa new-model) are the first steps in the configuration process. To serve as a backup authentication method, a local administrative user with privilege level 15 is created.

The AAA server's IP address (172.18.30.30) and ports 1812 (authentication) and 1813 (accounting) are then used for establishing the RADIUS server inside the radius server configuration block. Type 7 password encryption is used to store the shared secret.

LU-Server is a login method. It tells the router to use the RADIUS server for authentication first, then switch to the local database and activate password if RADIUS is not available. Every console login request is then enforced by AAA by applying this method list to the console line.

This setup guarantees secure access control, appropriate redundancy, and centralized authentication.

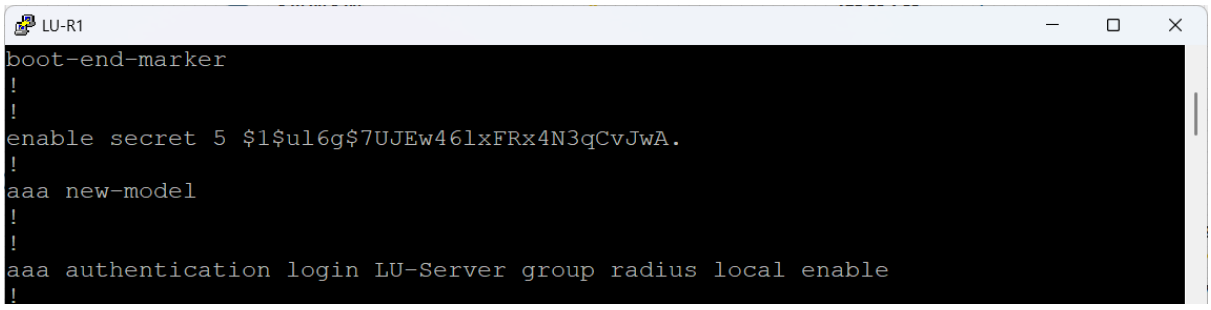

Figure 212 LU-R1 AAA Configuration Part 1

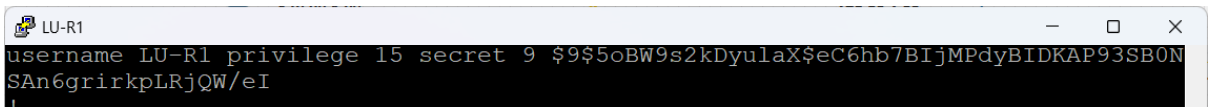

Figure 213 LU-R1 AAA Configuration Part 2

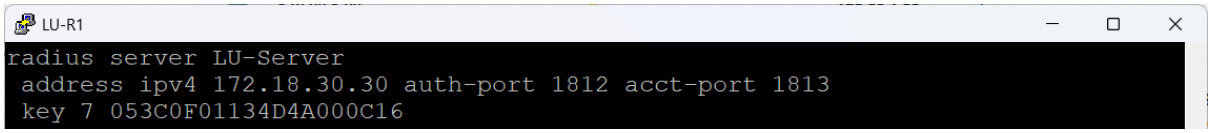

Figure 214 LU-R1 AAA Configuration Part 3

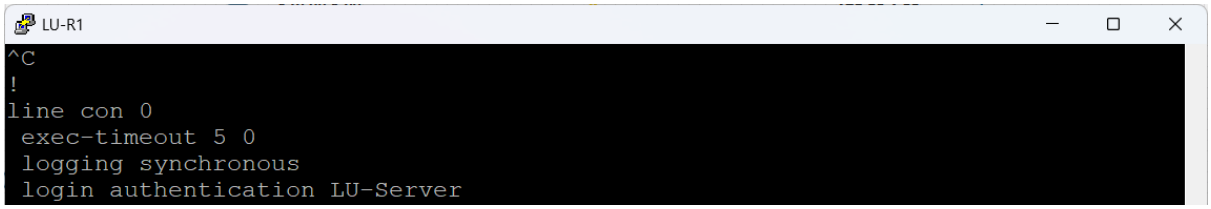

Figure 215 LU-R1 AAA Configuration Part 4

AAA Authentication Verification

The figures below demonstrate that verifying that the router is successfully authenticating users against the WinRadius server is the last step. The router transmits the login credentials to the RADIUS server, which uses the configured user database to determine whether to grant or reject access.

In the successful check, WinRadius recorded the request as "User (Admin) authenticate OK" after the Admin account successfully authenticated over the router. This verifies the functionality of the shared secret, RADIUS communication, and AAA setup.

A second attempt to log in with user 1 was purposefully unsuccessful. WinRadius responded "Unknown username" and the router denied the login since this username doesn't exist in the RADIUS database. This confirms that the authentication control is correctly applied and that unauthorized users cannot obtain access.

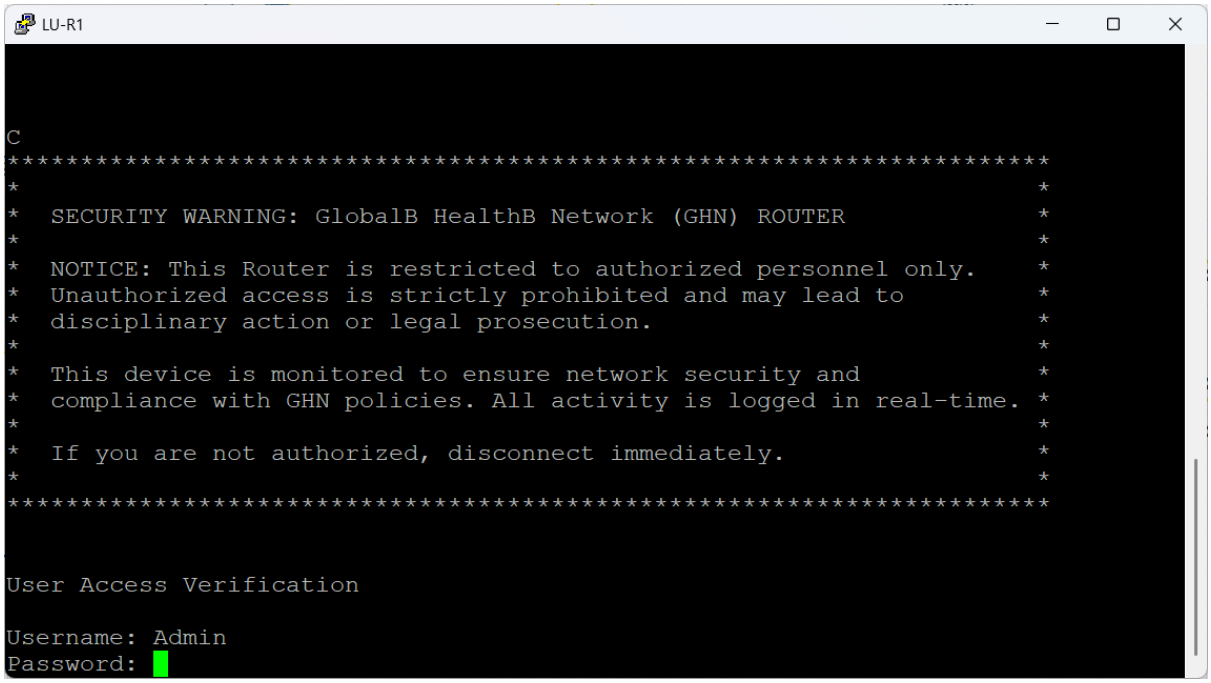

Figure 216 AAA Authentication Verification Part 1

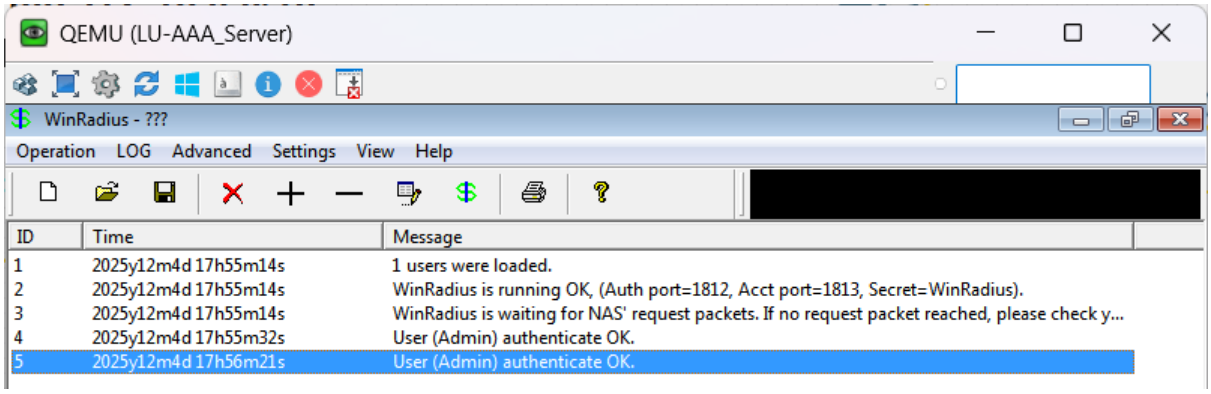

Figure 217 AAA Authentication Verification Part 2

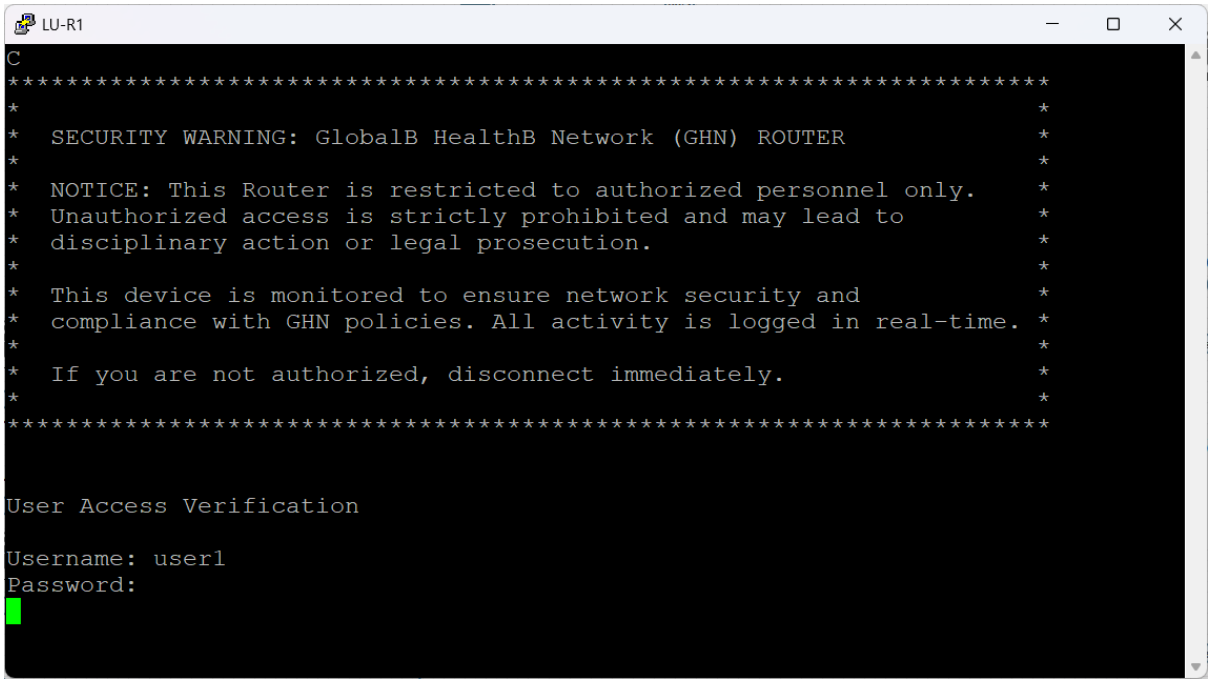

Figure 218 AAA Authentication Verification Part 3

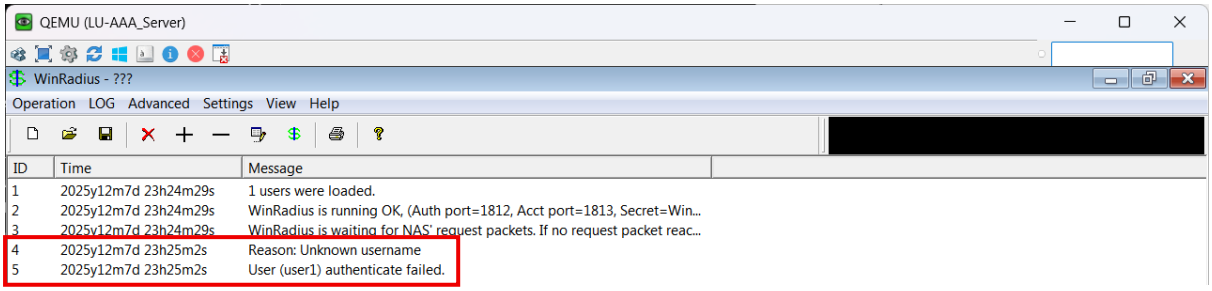

Figure 219 AAA Authentication Verification Part 4

Role Based Access Setup

Role based access is set up to grant structured and regulated administrative permissions on servers and network devices. To ensure that each administrator can only carry out the responsibilities allocated to them, specialized roles are created with defined capabilities rather than giving every authorized user complete powers. In the GHN environment, this improves security, lowers the possibility of misconfiguration, and offers greater responsibility. The implementation and verification of role-based access are described in this section.

Tester View Configuration

The below figure shows for users that want visibility into the router but are unable to make any changes, this view defines a restricted-privilege role named Tester. Essential operational commands, primarily those related to monitoring and diagnostics, are selectively whitelisted by the configuration. Ping, traceroute, neighbor detection, interface status, routing tables, VLAN data, and system logs are among the safe utilities it contains.

This guarantees that support personnel may troubleshoot visibility issues and confirm network status without exposing the router to illegal configuration modifications.

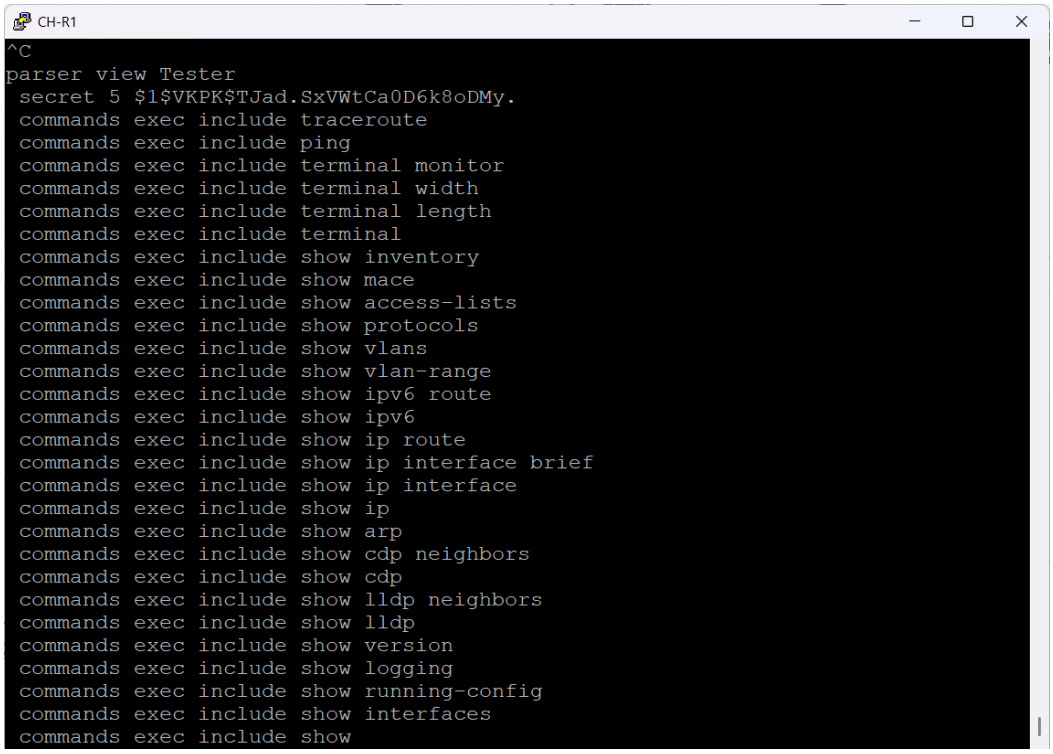

Figure 220 Tester View Configuration

Tester View Verification

The Tester view was designed to limit the user to diagnostic only instructions while forbidding configuration changes, as seen in the figures below. The view was enabled on CH-R1 for validation after the parser-view configuration was applied.

The router appropriately dropped into the restricted view when it was engaged, verifying that the user could only use the permitted EXEC commands, including ping, traceroute, display, and basic terminal controls. The deliberate blocking of any configuration level operations shows that the privilege separation was implemented as intended.

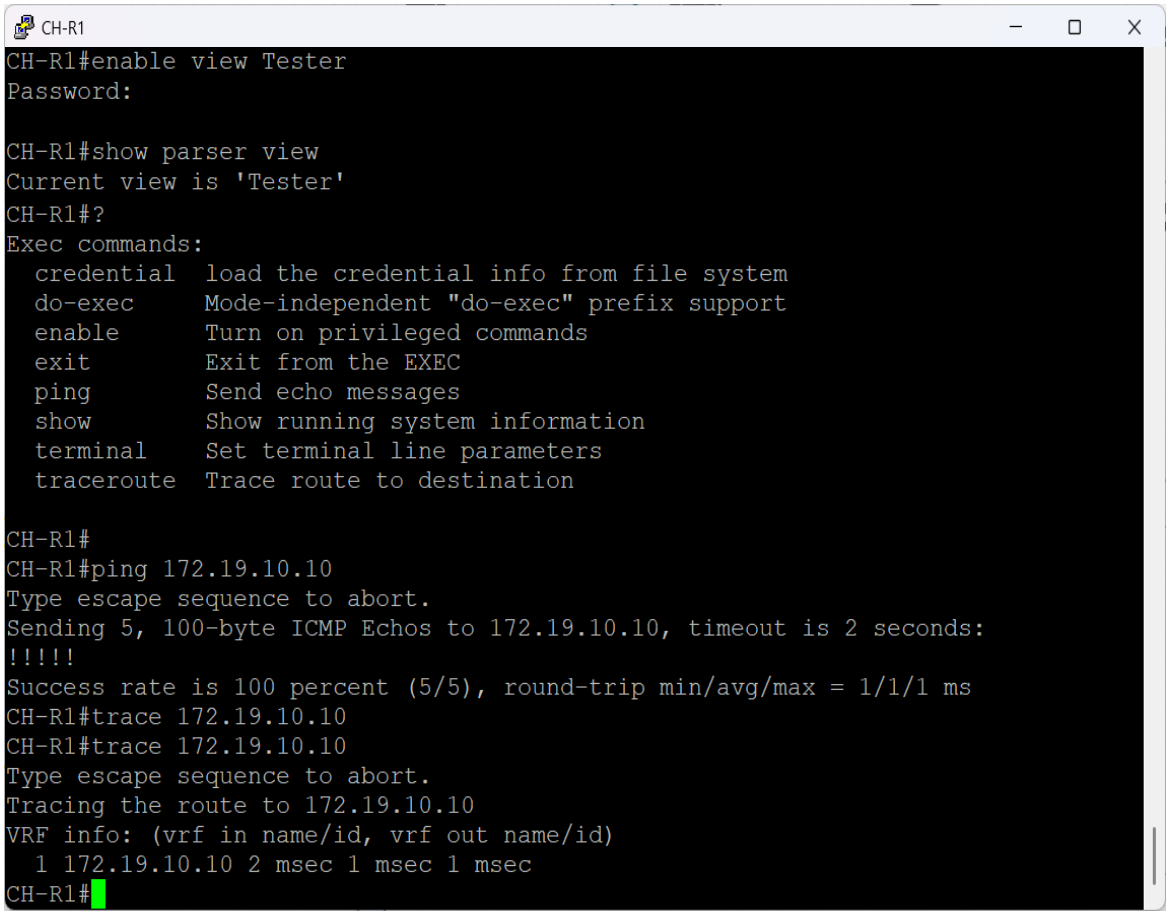

Figure 221 Tester View Verification

SSH Setup

In the GHN setup, SSH has been set up to offer safe remote management access to network devices. SSH safeguards administrative sessions over LAN and WAN links and stops unwanted credential interception by encrypting all login and management traffic. This configuration guarantees that all device management is carried out via encrypted channels and replaces insecure protocols like Telnet. The GHN network's SSH configuration and verification procedures are described in this section.

SSH Configuration

The router's SSH configuration, which replaces insecure remote access procedures and guarantees encrypted administration sessions throughout the GHN network, is depicted in the images below. SSH version 2 is automatically activated when the device's domain name is defined, and RSA keys are generated. Setting SSH timeouts, restricting authentication retries, and implementing AAA—which verifies each remote login via the RADIUS server—all strengthened security measures. After that, the VTY lines were limited to SSH-only, and users who had been verified were subject to privilege level enforcement. All remote management traffic is guaranteed to be encrypted, authenticated, and completely compatible with the project's security requirements thanks to this configuration.

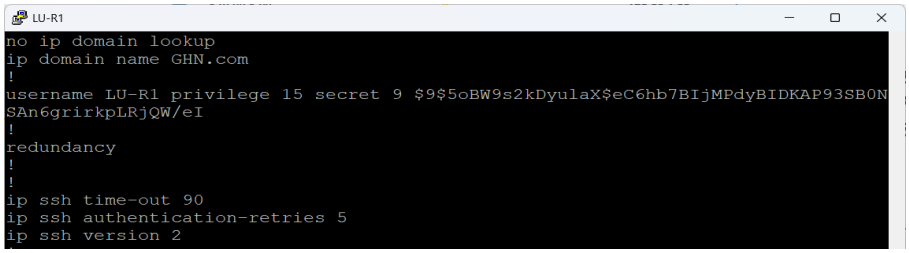

Figure 222 LU-R1 SSH Configuration Part1

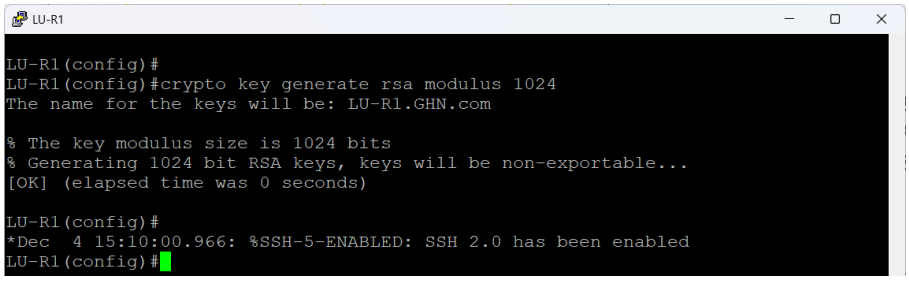

Figure 223 LU-R1 SSH Configuration Part 2

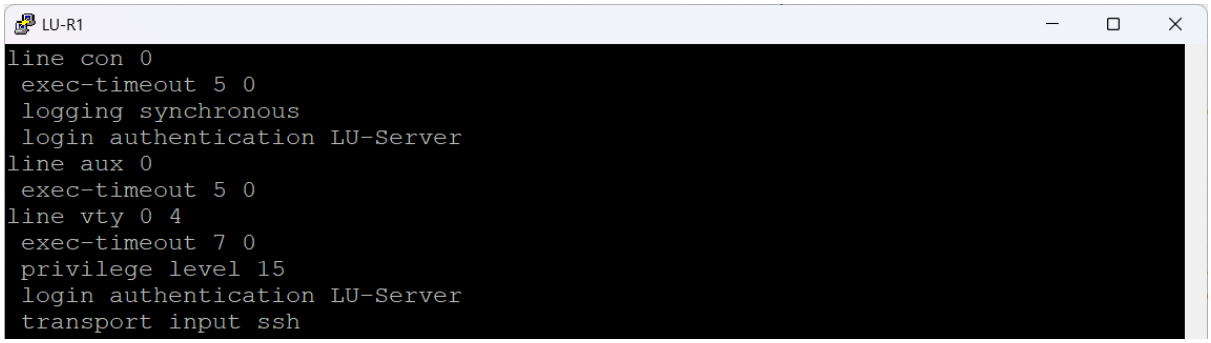

Figure 224 LU-R1 SSH Configuration Part 3

SSH Verification

The secure remote access from a client computer is depicted in the figures below. The router's administration IP address for LU-R1 was entered using PuTTY with port 22 and SSH as the chosen protocol. The router confirmed that SSH access is being enforced through the RADIUS server by prompting for the preset AAA credentials as soon as the session was initiated.

Secure CLI access to the router was made possible by the admin user's successful authentication. An active SSH session was confirmed by running the show ssh command on the router, which displayed the username and encryption techniques in use. This attests to SSH's complete functionality, encryption, and integration with centralized AAA authentication.

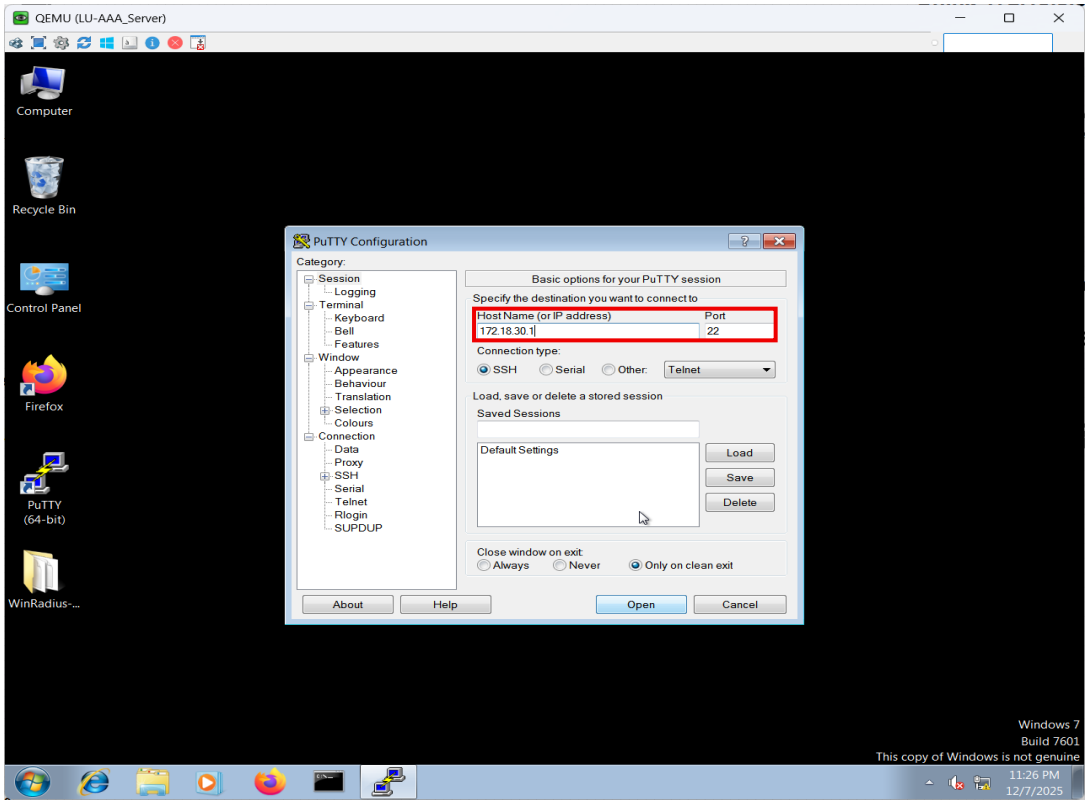

Figure 225 SSH Verification Part 1

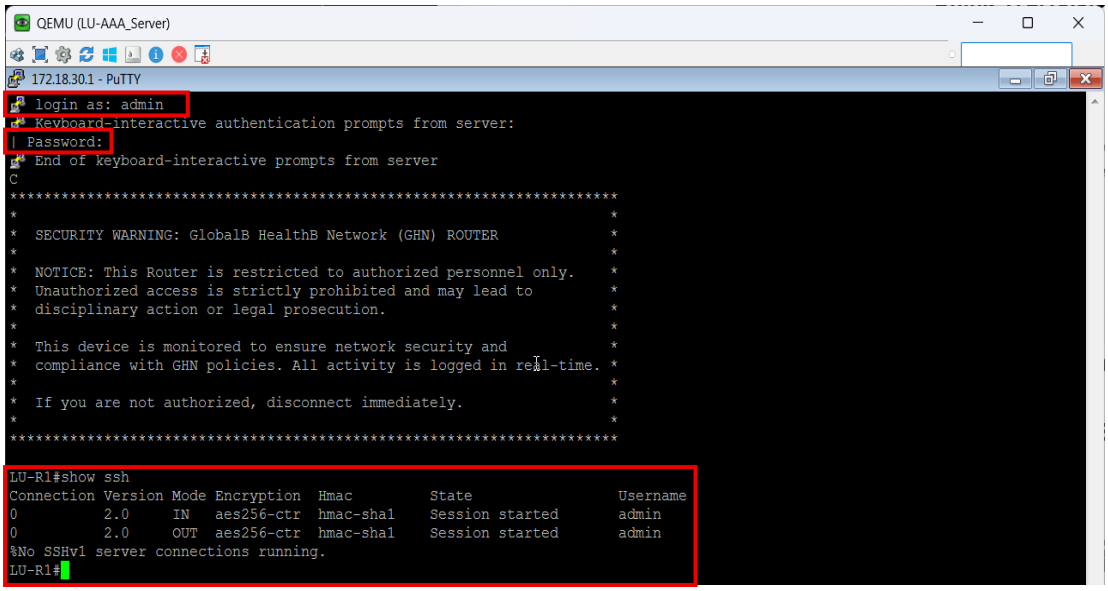

Figure 226 SSH Verification Part 2

Testing

For the purpose of to verify that the Global Health Network infrastructure fulfills the functional, technical, and operational requirements outlined in the Project plan and Network Design Document, testing was carried out. Testing concentrated on confirming connectivity, routing stability, secure communication, service availability, and overall system capability due to the network's vital role in enabling international healthcare services.

EVE-NG was used to conduct all experiments in a controlled simulated environment. By contrasting anticipated system behaviour with actual reported results, test results were objectively recorded.

Test Plan

The test plan outlines the approach and specifications needed to confirm that the GHN network is operating correctly. Instead of load or penetration testing, testing was restricted to the elements that were part of the project's scope and concentrated on confirming typical operating behavior.

The test plan covered the following functional areas:

- Internal routing protocol operation within each site.
- Inter-domain routing and WAN connectivity across the ISP network.
- Secure WAN communication using DMVPN and IPsec.
- LAN segmentation and inter-VLAN routing.
- Availability of core network services.
- Overall system acceptance against project objectives.
- Conduct usability testing to assess the Server services (FTP, WEB, Email, DNS)
- Ensuring all system functionalities are operating as planned.

Test execution followed predefined scenarios to ensure repeatability and consistency. Command outputs, logs, and verification evidence were captured and are provided in the implementation and Appendices.

Participants

A small number of participants were chosen to represent technical personnel in charge of verifying and examining enterprise network infrastructure during the testing phase. Participants were selected based on their technical expertise and capacity to understand network behaviour while undergoing testing.

As the GHN solution is a backend infrastructure system with no direct end-user interface, participants were not selected from general healthcare staff. Instead, testing focused on administrative and operational validation.

Participant Name	Age	Gender	Background
Ali Ahmed	24	Male	ICT graduate with knowledge of enterprise networking, routing protocols, and WAN technologies.
Noor Hassan	23	Female	Information Systems student with academic exposure to network design and basic service validation.
Khalid Yousif	27	Male	Information Systems student with academic exposure to network design and basic service validation.

Table 5 Testing Participants

The participants carried out test scenarios and documented observed results in accordance with the test plan's intended results.

Functionality Test Cases and results

To ensure that every significant part of the GHN network functions as planned, functionality testing was carried out. By contrasting the anticipated system behaviour with the actual observed outcome during testing, each test scenario verifies a particular network function.

No.	Test Scenarios	Expected Result	Actual Result	Status
1	Verify internal routing within Bahrain site using EIGRP	EIGRP neighbors establish and routes are exchanged	EIGRP adjacency formed and routes learned	Pass

2	Verify internal routing within England site using OSPF	OSPF neighbors establish and advertise internal networks	OSPF neighbors stable and routes exchanged	Pass
3	Verify internal routing within Luxembourg site using OSPFv3	OSPFv3 neighbors establish and exchange routing information	OSPFv3 adjacencies formed	Pass
4	Verify BGP peering between GHN sites and ISP network	BGP sessions establish successfully	All BGP sessions established	Pass
5	Verify end-to-end connectivity across GHN WAN	All sites can reach each other	End-to-end connectivity verified	Pass
6	Verify DMVPN tunnel establishment	DMVPN tunnels establish between hub and spokes	All tunnels operational	Pass
7	Verify IPsec encryption over WAN links	WAN traffic is encrypted	IPsec security associations active	Pass
8	Verify VLAN isolation	Devices in different VLANs are isolated	VLAN isolation enforced	Pass
9	Verify inter-VLAN routing	Authorized VLANs communicate via Layer 3 routing	Inter-VLAN routing operational	Pass
10	Verify DNS name resolution	DNS queries resolve across all sites	DNS resolution successful	Pass
11	Verify FTP, Web, and Email services	Services accessible from all sites	Services operational	Pass
12	Verify DHCP address allocation	Clients receive valid IP addresses	DHCP functioning correctly	Pass
13	Verify AAA authentication	Authorized users authenticate successfully	AAA authentication successful	Pass
14	Verify DNS load balancing	DNS queries distributed across two servers	Test could not be completed due to insufficient system resources	Fail

Table 6 Functionality Test Cases and Result

Test Cases verification

The functionality testing carried out to confirm the Global Health Network's proper operation following implementation is presented in this section. Every test case was created to verify a certain system function, such as enterprise service availability, secure WAN communication, routing behaviour, and inter-site connectivity. Verification was based on observed system behaviour and operating results, and the tests were carried out in the EVE-NG simulation environment. When appropriate, evidence figures are included to show that each test case was executed successfully.

Internal routing within Bahrain site using EIGRP:

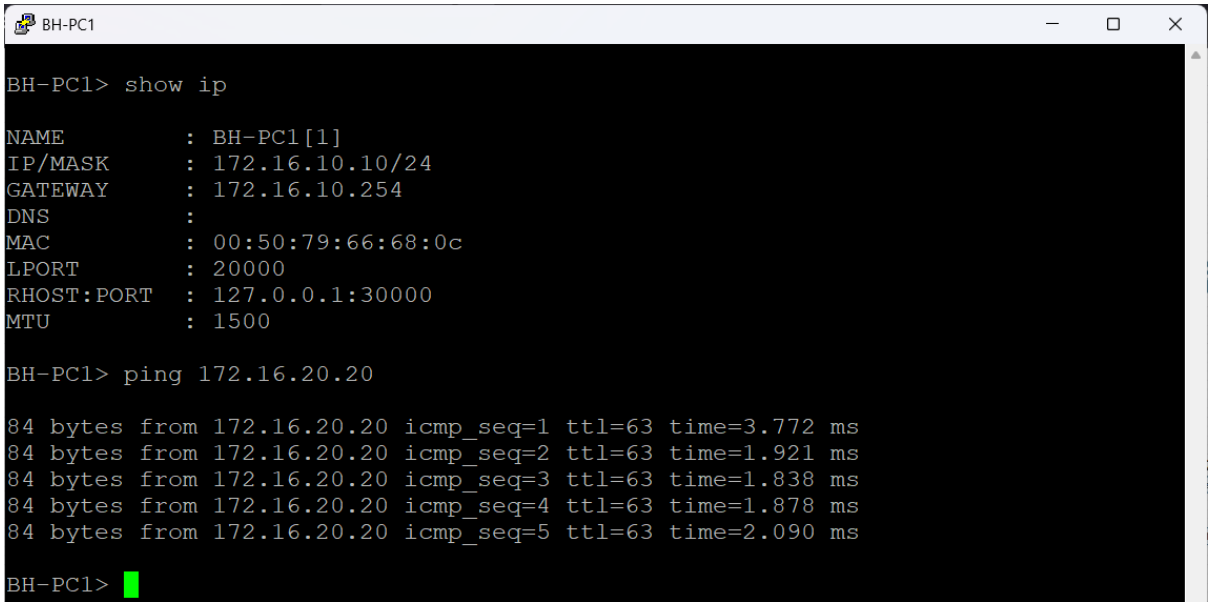

Figure 227 Verify internal routing within Bahrain site using EIGRP

This test was carried out to confirm that the EIGRP internal routing within the Bahrain site is operating properly. The purpose was to verify that end devices in the Bahrain branch's different VLANs and subnets could effectively interact via the internal routing system.

Host BH-PC1, which has the IP address 172.16.10.10/24 and a default gateway of 172.16.10.254, was used to conduct the test. ICMP echo requests were sent to a destination site on a separate internal subnet (172.16.20.20) in order to test connectivity.
As shown in Figure above, all ICMP echo requests were successfully received,

The results above verify that the Bahrain site's EIGRP adjacencies are active and that internal routers are correctly exchanging routing data. The Bahrain internal routing design fulfills its functional requirements, as confirmed by the successful end-to-end communication.

Result: Pass

End to End WAN connectivity:

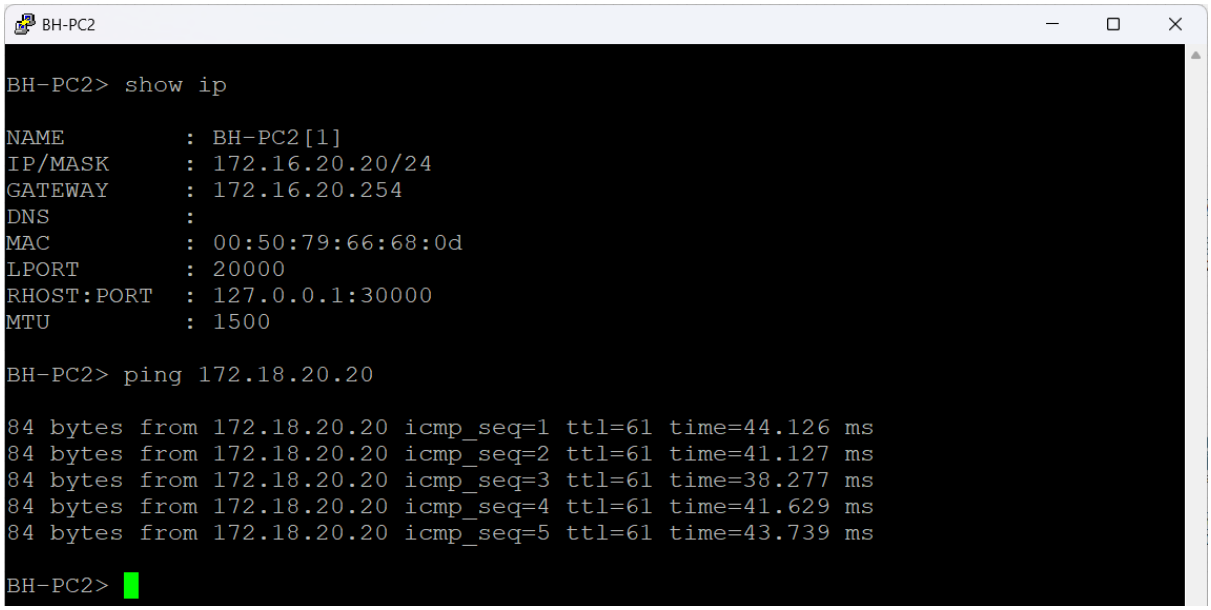

Figure 228 Verify inter-domain routing and WAN connectivity 1

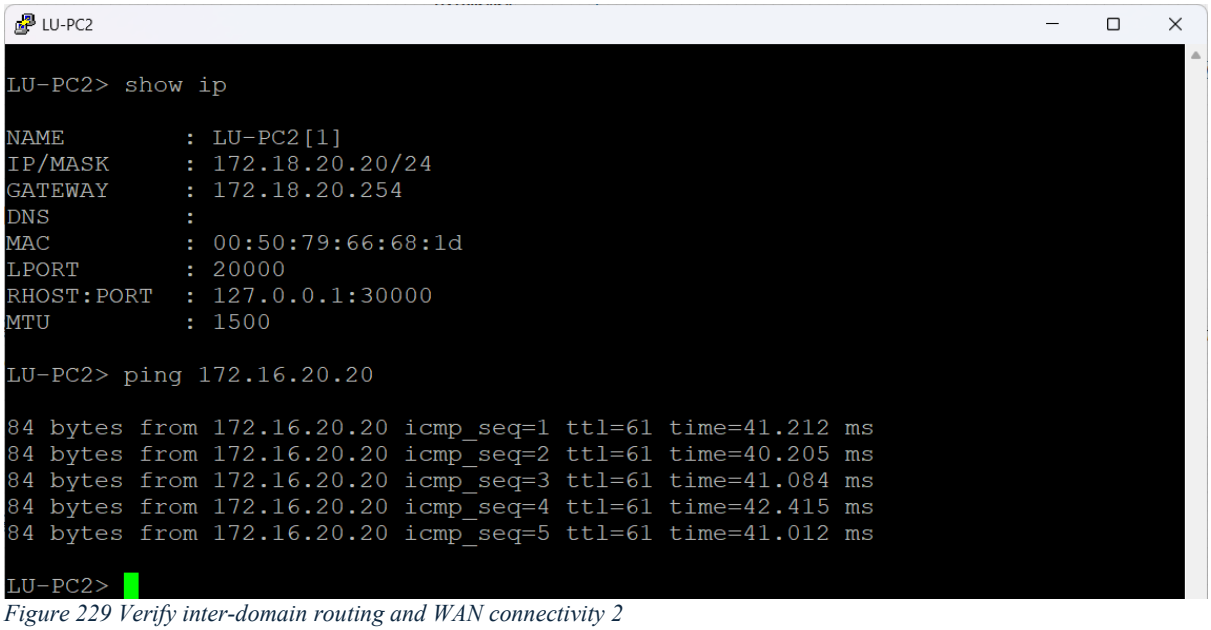

Figure 229 Verify inter-domain routing and WAN connectivity 2

Verifying end-to-end IP connectivity across geographically dispersed locations over the GHN WAN was the aim of this test. The goal was to verify that inter-site routing, DMVPN tunnelling, and BGP-based WAN routing allow for effective communication across hosts in various branches.

To verify forward-path connection across the WAN, ICMP echo requests were made from BH-PC2 in the Bahrain site (172.16.20.20/24) to a server in the Luxembourg site

(172.18.20.20). To confirm bidirectional connectivity, the test was subsequently conducted again from LU-PC2 in the direction of the Bahraini host. ICMP requests were successfully transmitted in both directions, as the figures demonstrate.

These findings verify that the WAN design satisfies the functional need for worldwide connectivity and is functioning properly.

Result: Pass

DMVPN Tunnel Establishment:

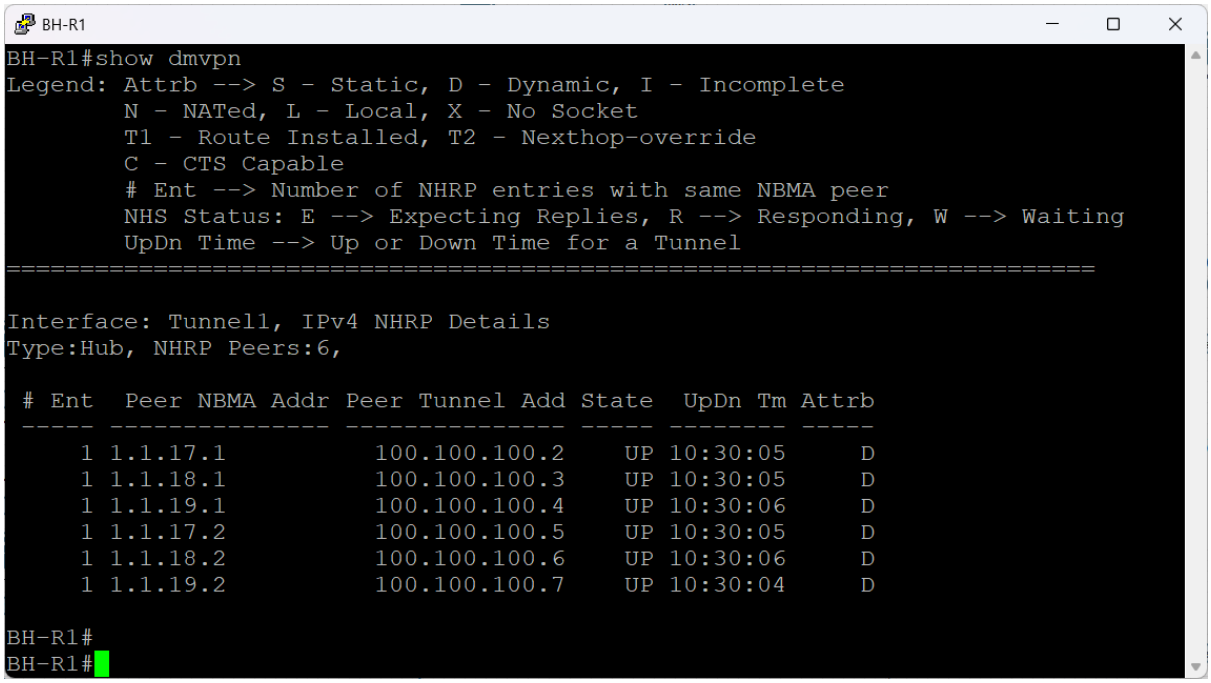

Figure 230 Verify DMVPN tunnel establishment 1

This test was designed to confirm that the DMVPN infrastructure between the GHN hub and spoke sites is properly set up and functioning. Confirming effective tunnel creation, NHRP registration, and dynamic peer finding across the WAN overlay were the main objectives of the test.

The main DMVPN hub router BH-R1 and a spoke router EN-R2 were used for verification. The DMVPN tunnel interface (Tunnel1) on BH-R1 functions in hub mode and keeps active NHRP peer entries for each connected spoke, as seen in the figure. Stable tunnel connectivity and successful registration of all remote sites are confirmed by the listing of several peers in the UP state with dynamic attributes.

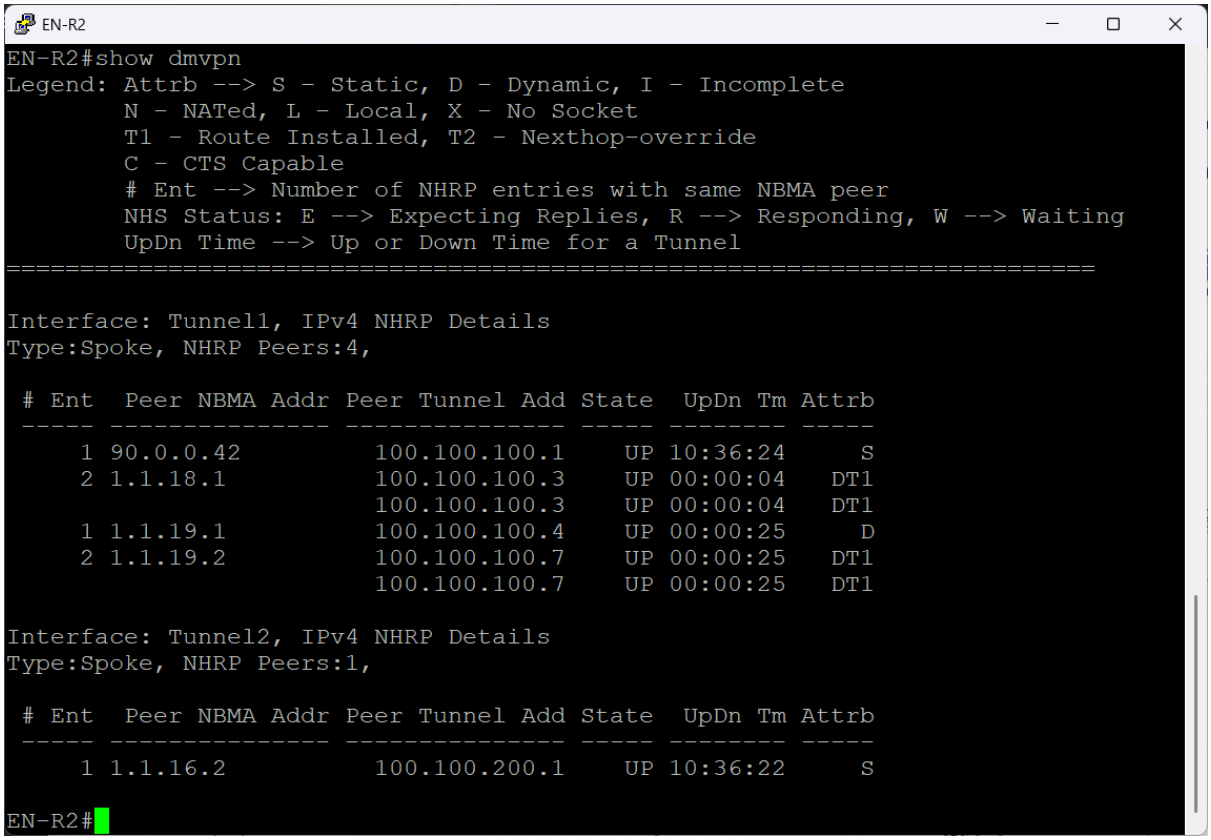

Figure 231 Verify DMVPN tunnel establishment 2

Tunnel1 and Tunnel2 are successfully formed toward the redundant hub routers, according to DMVPN verification on the spoke router EN-R2. The graphic illustrates that NHRP peer entries are in the UP state and have properties that prove active spoke-to-hub communication, such as dynamic registration and next-hop override. Multiple NHRP entries confirm proper DMVPN Phase 3 operation and allow dynamic spoke-to-spoke communication when needed.

These findings verify that the DMVPN overlay is operating as intended, providing dependable hub-and-spoke connectivity and scalable inter-site communication.

Result: Pass

IPsec Encryption Over WAN Links:

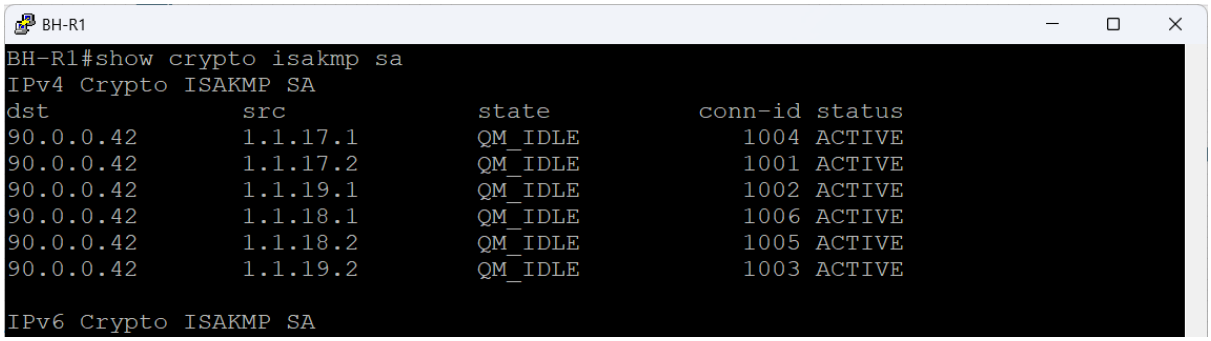

Figure 232 Verify IPsec encryption 1

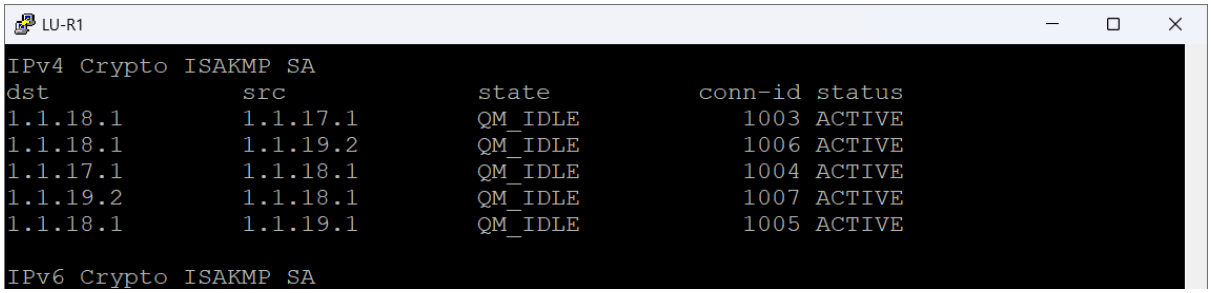

Figure 233 Verify IPsec encryption 2

The purpose of this test was to verify that the Global Health Network actively uses IPsec for both negotiation and encryption of inter-site WAN traffic. The goal was to confirm that encrypted communication functions properly over the DMVPN overlay and that IPsec Security Associations are effectively created.

The DMVPN hub router BH-R1 and the remote router LU-R1 were first verified using the display crypto isakmp sa command. The numbers demonstrate that every ISAKMP session is in the QM_IDLE state with an ACTIVE status, signifying a successful Phase 1 negotiation and preparedness for the exchange of encrypted data.

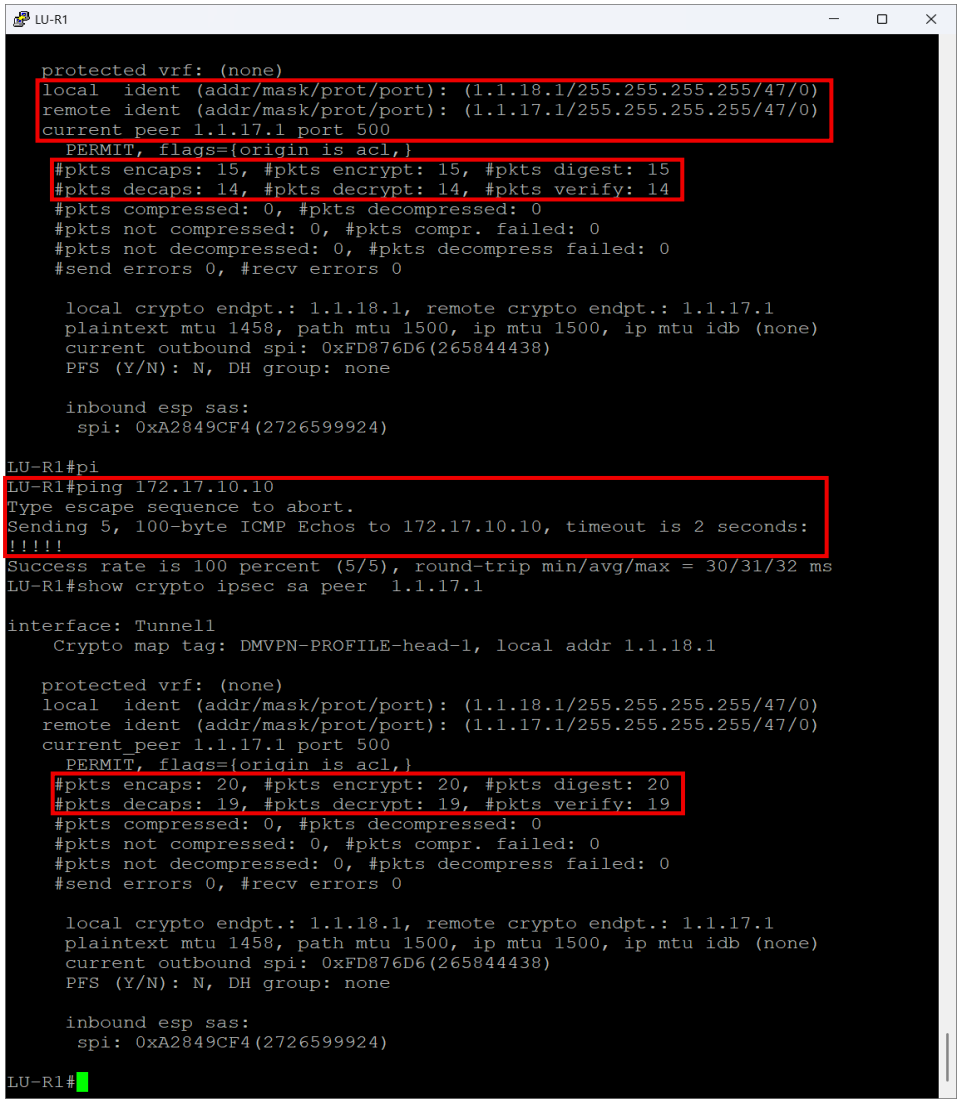

Figure 234 Verify IPsec encryption 3

On LU-R1, active IPsec data-plane encryption was confirmed using the display crypto ipsec sa peer command. Packet counts for encapsulation, encryption, decapsulation, decryption, and verification are rising, as seen in the figure, indicating that traffic is actively being encrypted and decrypted rather than sitting about.

These findings verify that IPsec encryption is completely functional throughout the GHN WAN.

Result: Pass

DNS Service Reachability

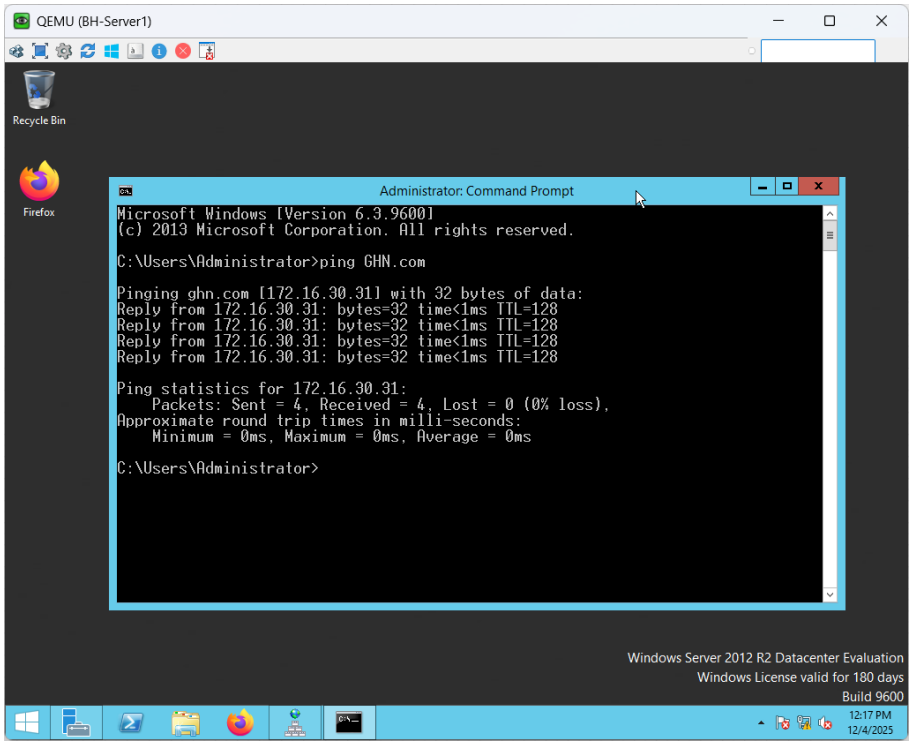

Figure 235 Verify DNS name resolution services

This test confirms that the Global Health Network's DNS name resolution is operating properly. BH-Server1 sent ICMP echo requests to the domain name GHN.com in order to complete a DNS search.

The domain name was successfully resolved to the IP address 172.16.30.31, as seen in the above figure, and all ICMP requests were answered without packet loss. This verifies that internal systems can access and use the DNS service.

Result: Pass

Web Service Accessibility

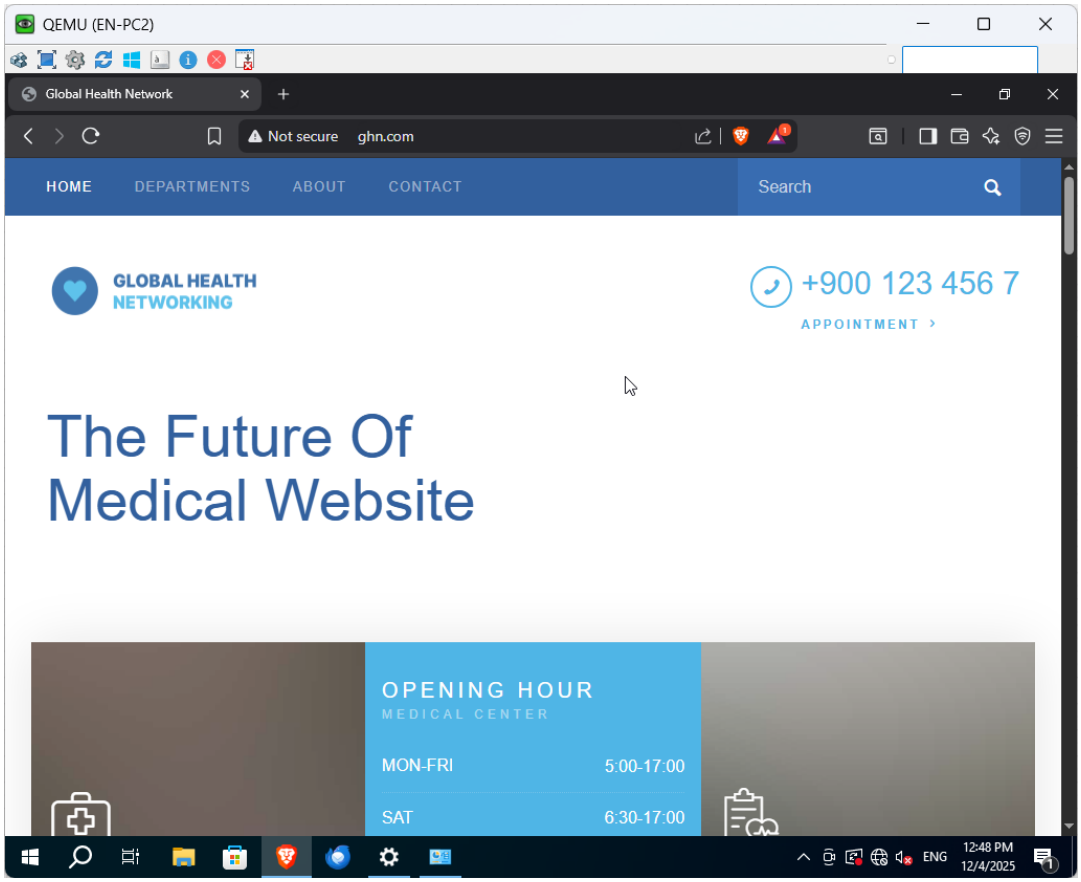

Figure 236 Verify WEB using DNS services

This test confirms that a remote location can access the GHN web service. The test was conducted using EN-PC2 by using a web browser to reach the domain ghn.com.

The web site loaded successfully, as seen in Figure above, indicating that DNS resolution and HTTP connectivity are operating properly and that the web service is reachable over the WAN.

Result: Pass

FTP Service Functionality:

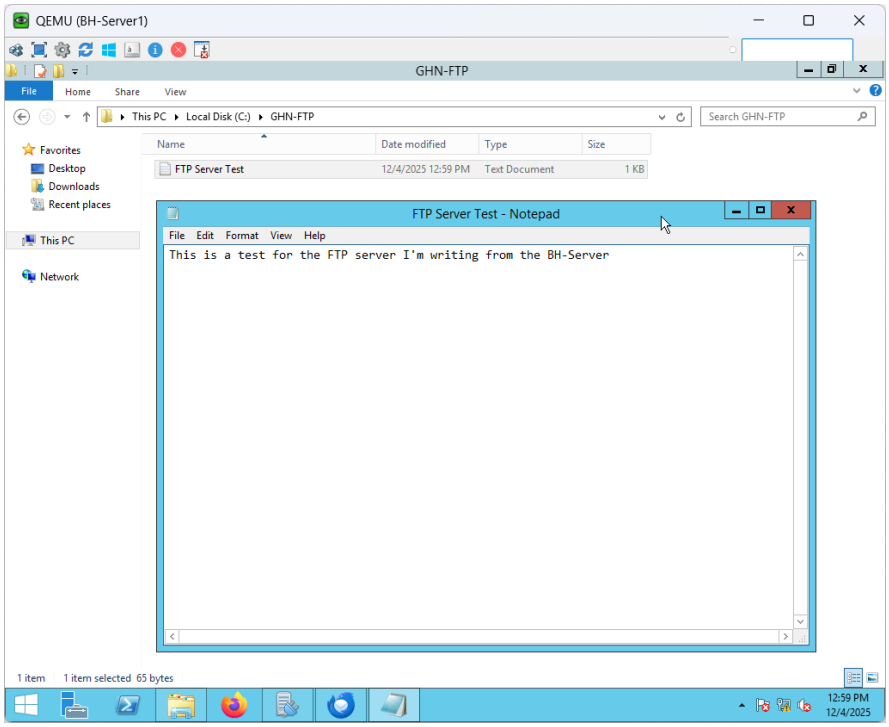

Figure 237 Verify FTP services 1

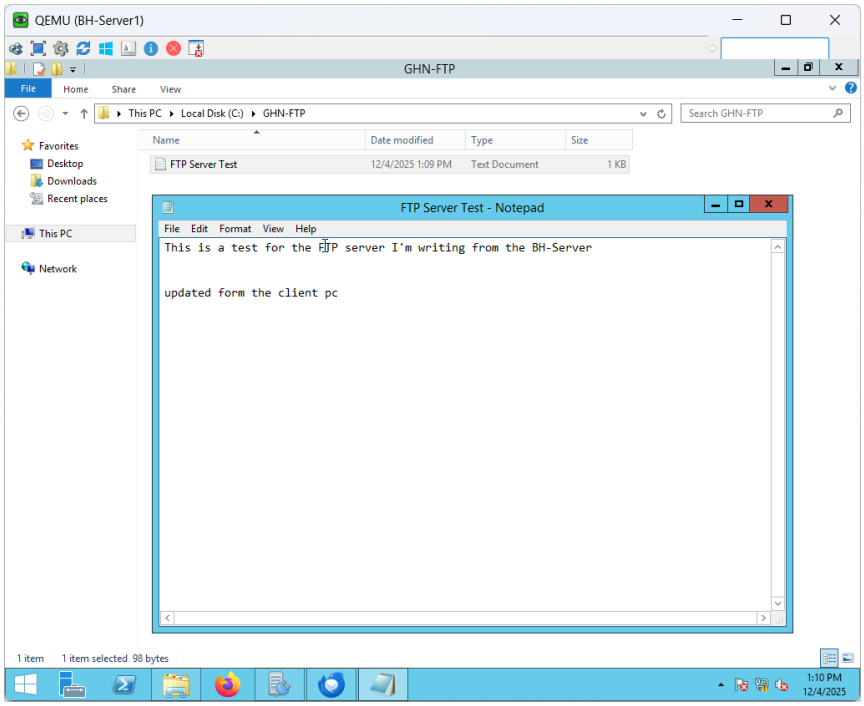

Figure 238 Verify FTP services 2

This test confirms that the Global Health Network's FTP service is functional and reachable. A file on the FTP server directory was created and modified in order to conduct the test from

BH-Server1.

The file was successfully generated and modified, as seen in the above figure, demonstrating that the FTP service supports file transfer and write activities as planned.

Result: Pass

Email Service Operation

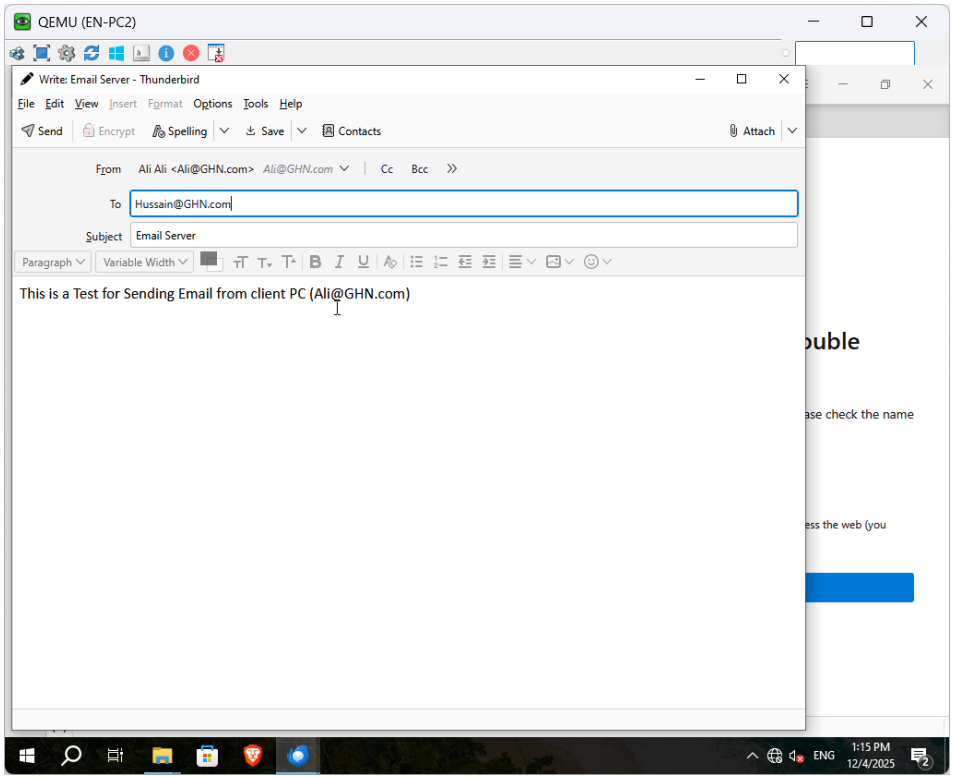

Figure 239 Verify Email services 1

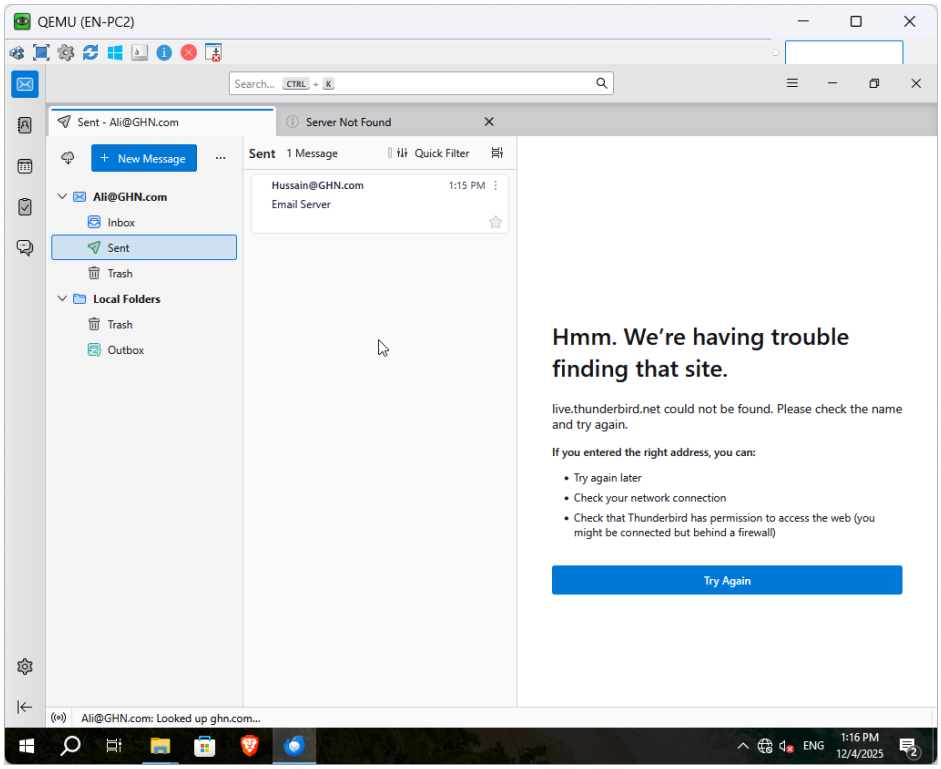

Figure 240 Verify Email services 2

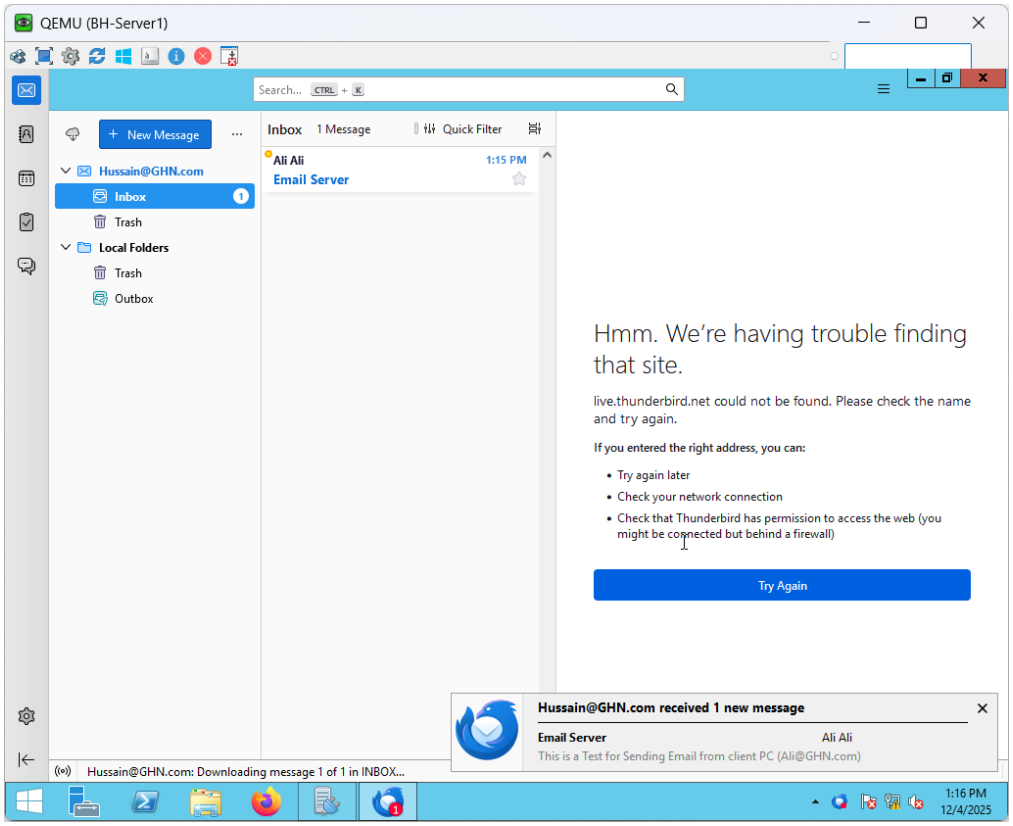

Figure 241 Verify Email services 3

This test confirms that the email service is functional throughout the Global Health Network. EN-PC2 sent an email to Hussain@GHN.com from the account Ali@GHN.com.

The message was successfully sent from the client and received in the inbox on BH-Server1, as seen in the preceding figures, indicating proper email transmission and delivery across the WAN.

Result: Pass

DHCP Address Allocation

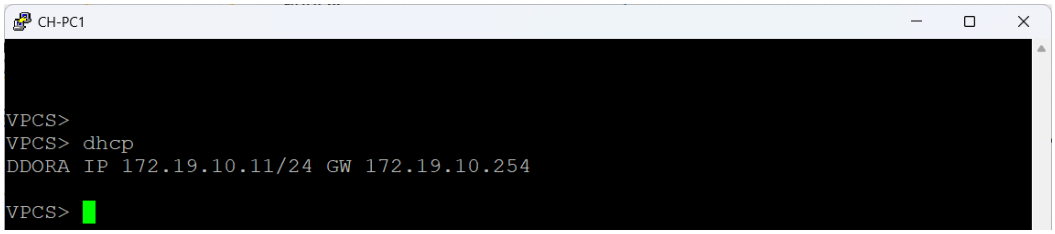

Figure 242 Verify DHCP address allocation 1

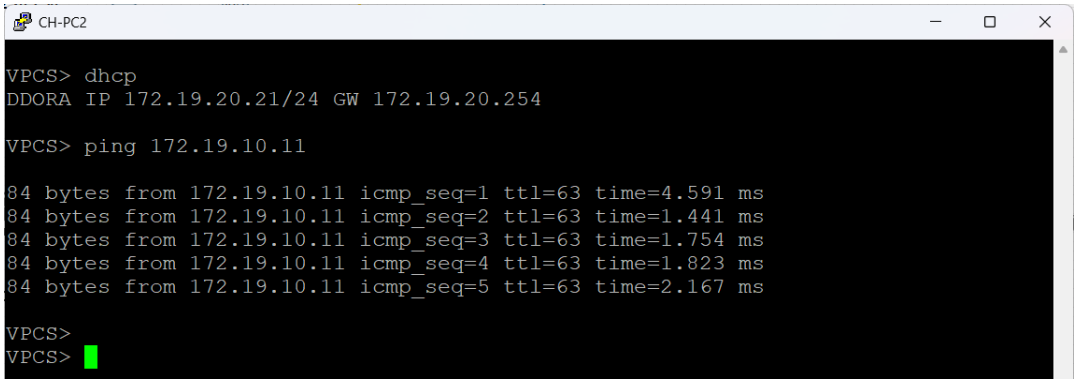

Figure 243 Verify DHCP address allocation 2

This test confirms that client devices are appropriately assigned IP configuration by the DHCP service. CH-PC1 and CH-PC2 sent out DHCP requests.

The DHCP server successfully provided both clients with valid IP addresses and default gateways, as seen in the aforementioned figures. Successful ICMP transmission provided additional confirmation of the clients' connectivity.

Result: Pass

AAA authentication

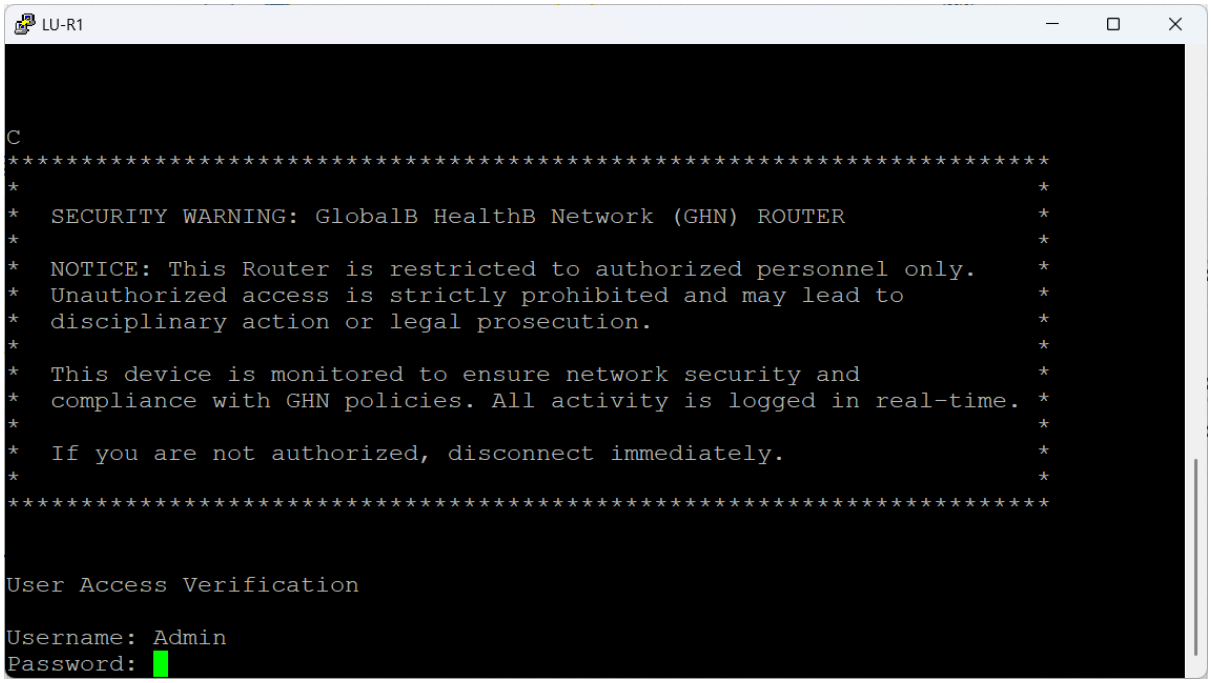

Figure 244 Verify AAA authentication 1

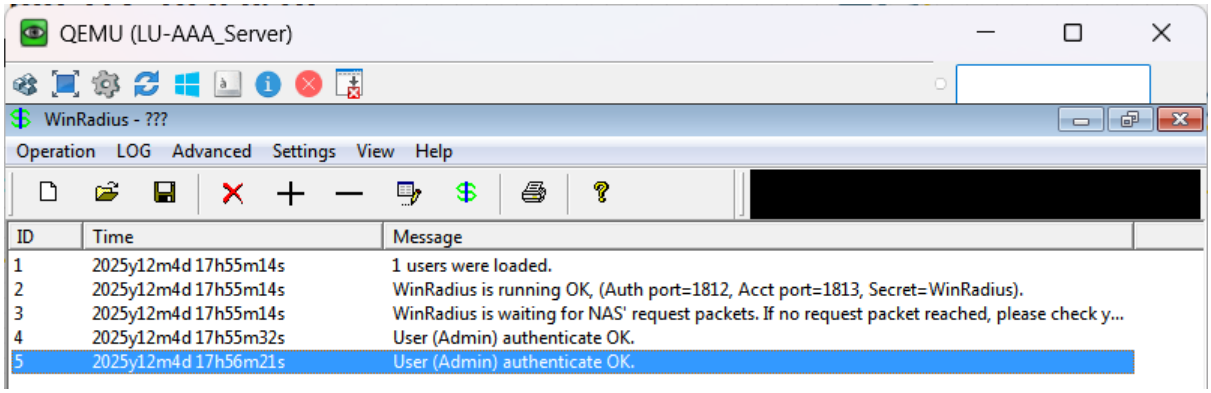

Figure 245 Verify AAA authentication 2

This test relies on the AAA infrastructure to confirm authentication. The user account Admin was used to attempt an administrator login to LU-R1.

The router successfully allowed access after requesting user credentials, as seen in the aforementioned figures. The user's successful authentication using the RADIUS service is confirmed by corresponding authentication records on the LU-AAA Server.

Result: Pass

Secure Device Access (SSH)

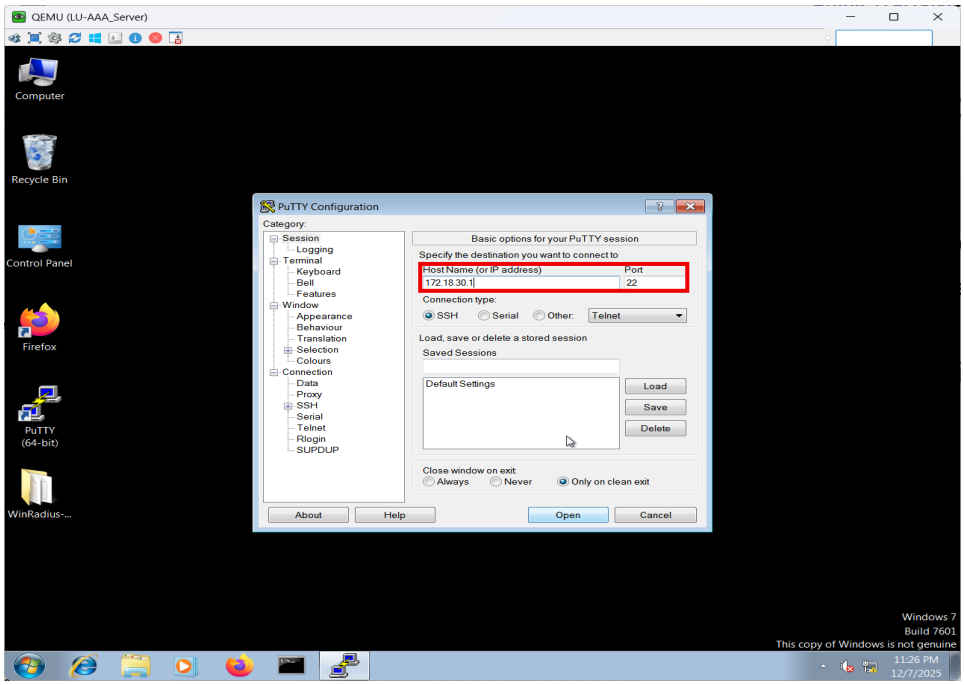

Figure 246 Verify SSH access 1

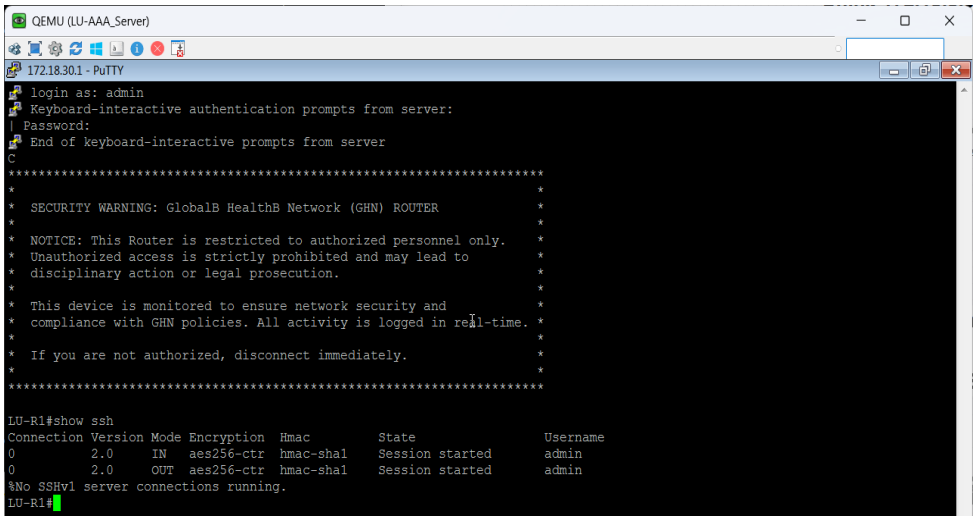

Figure 247 Verify SSH access 2

This test confirms SSH-based secure remote administrative access to network devices. The Admin account was used to start an SSH session from LU-AAA-Server to LU-R1.

The user was authenticated and given access when the SSH connection was successfully established, as seen in Figure X. The active SSH session verifies that centralized authentication is used to enforce secure remote management.

Result: Pass

Acceptance Tests Process and Results

Acceptance testing was conducted after successful completion of functionality testing to confirm that the GHN system meets the defined project requirements and operational expectations. Rather than focusing on specific technical elements, the acceptance process validated the system from an operational and user perspective by assessing overall connectivity, service availability, security, and usability across all GHN sites.

No.	Participant	Process	Result
1	Ali Ahmed	Verified end-to-end connectivity between Bahrain, England, Luxembourg, and China sites	All sites were able to communicate successfully with stable connectivity across the WAN
2	Noor Hassan	Reviewed routing behavior and inter-site communication during normal operation	Routing remained stable and no unexpected route loss or reconvergence issues were observed
3	Khalid Yousif	Validated secure WAN communication using DMVPN and IPsec	Encrypted tunnels were established successfully, and WAN traffic was securely transmitted
4	Ali Ahmed	Confirmed availability of core network services (DNS, FTP, Web, Email, DHCP, AAA)	All core services were accessible from remote sites and operated as expected
5	Noor Hassan	Evaluated DNS load balancing using multiple DNS servers	DNS load balance could not be fully validated due to simulation resource limitations; however, DNS resolution remained functional

Table 7 Acceptance Test Process and Results

The GHN network fulfills all primary project goals concerning connection, security, and service availability, according to the acceptance testing results. The system was considered

operationally satisfactory within the specified project scope, despite the fact that DNS load balancing was not fully implemented due to environmental constraints.

Usability testing results and statistics

The GHN network is technically usable and manageable for network administrators, according to the results of usability testing. Essential services could be verified using common administrative procedures and tools, and core infrastructure components reacted predictably to configuration changes.

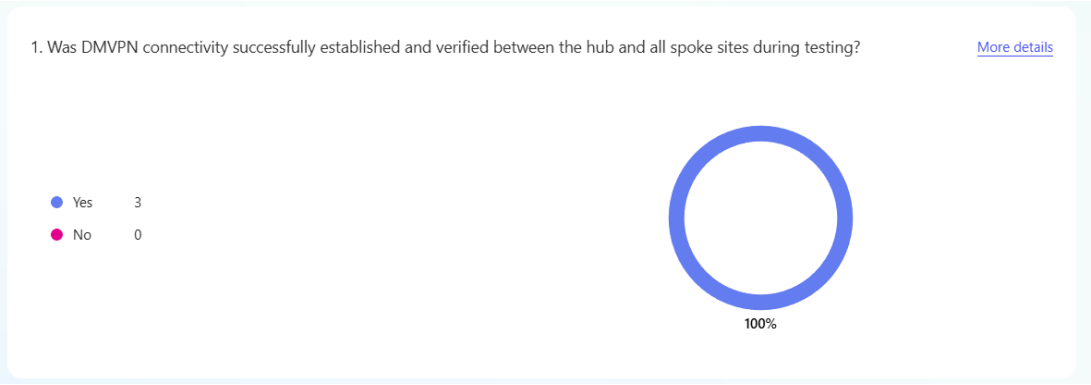

Figure 248 Usability Test 1

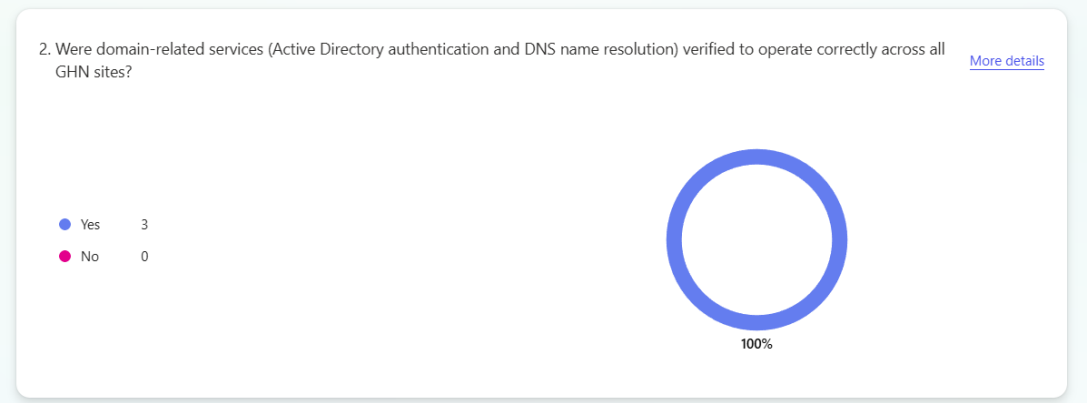

Figure 249 Usability Test 2

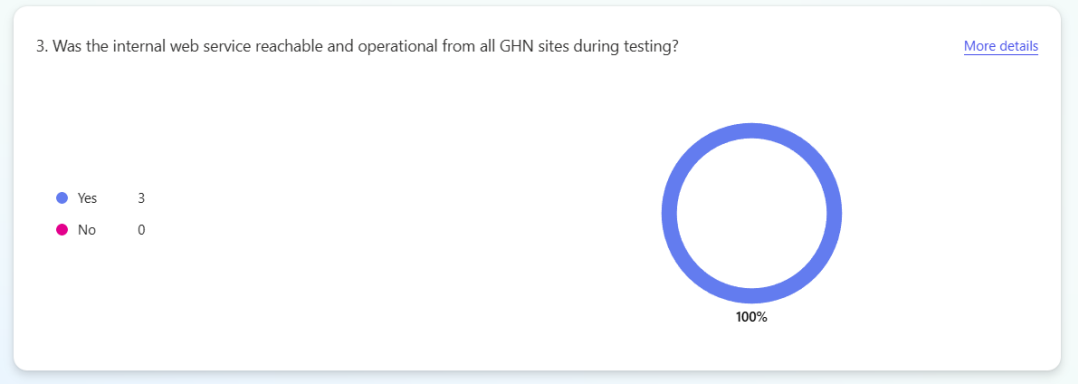

Figure 250 Usability Test 3

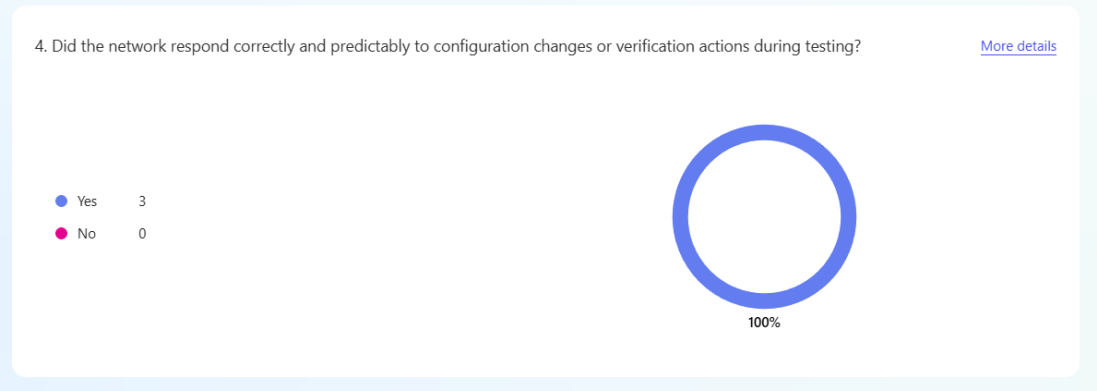

Figure 251 Usability Test 4

Discussion, LESPI, and Conclusion

This section analyses the Global Health Network project's overall results by considering the solution that was put into practice, the goals that were accomplished, and the difficulties that arose throughout the design, implementation, and testing stages. It addresses how well the system achieved its initial objectives and looks at practical limitations found during the course of the project. The Legal, Ethical, Social, and Professional Issues (LESPI) related to implementing a global healthcare network are also examined in this section, with a focus on data privacy, professional responsibility, and societal impact. The chapter wraps up the thesis by summarizing important discoveries, thinking back on individual learning objectives, evaluating the project's applicability in the Bahraini environment, and suggesting possible avenues for future improvement.

System Functionality

The deployed Global Health Network solution demonstrates that an advanced, multi-protocol WAN infrastructure can effectively serve worldwide healthcare activities. The network effectively combines EIGRP, OSPFv2, OSPFv3, EBGP, and IPsec with DMVPN Phase 3 to offer securely, scalable, and reliable connectivity across geographically dispersed locations. During testing, core services like Active Directory, DNS, DHCP, IIS web hosting, FTP, email, and AAA authentication functioned uniformly among all branches.

Dynamic path selection and quick convergence were made possible by the routing structure, which is essential for real-time services like HD video conferencing that specialized physicians employ. Since IPsec encryption guaranteed the confidentiality and integrity of sensitive healthcare data during transfer, redundancies at the routing and tunnelling levels decreased the possibility of single points of failure. Overall, the system verified the viability of implementing an enterprise-grade WAN for a global healthcare setting and satisfied the functional criteria specified in the project objectives.

Summary of Achieved Objectives

No.	Objectives	Status	Description
1	Design and implement an advanced WAN routing solution for Global Health Network	Achieved	An enterprise-grade WAN was successfully designed and implemented using EIGRP, OSPFv2, OSPFv3, EBGP, and DMVPN Phase 3, enabling reliable connectivity between all global sites.
2	Improve network reliability and availability across international locations	Achieved	Redundant routing paths and dual DMVPN hubs were implemented, ensuring high availability and fast convergence in case of link or device failure.
3	Secure inter-site communication for sensitive healthcare data	Achieved	IPsec encryption was deployed over DMVPN tunnels, ensuring confidentiality and integrity of data exchanged between global healthcare sites.
4	Support centralized network services for all branches	Achieved	Centralized services including Active Directory, DNS, DHCP, IIS web services, FTP, email, and AAA authentication were successfully accessed from all connected locations.
5	Enable stable network performance for HD video conferencing	Achieved	The routing architecture supported real-time traffic; however, full performance validation under heavy load was limited due to simulation and hardware constraints.
6	Ensure compliance with healthcare and data protection standards	Achieved	The network design considered ISO/IEC 27001 principles and aligned with HIPAA, GDPR, and Bahrain Personal Data Protection Law requirements.
7	Demonstrate CCNP-level routing and WAN design knowledge	Achieved	Advanced routing concepts were practically applied, tested, verified, and documented within a realistic enterprise healthcare scenario.

Table 8 Summary of Achieved Objectives Table

Project Issues

A few of practical problems that arose throughout the Global Health Network project's execution had an immediate effect on system selection and design choices.

The adoption of Windows Server 2019 for centralized services was one of the main problems. Windows Server 2019 was unable to function consistently in the EVE-NG environment due to a lack of simulation power, which led to instability during service installation and operation. Windows Server 2012 R2, which offers complete functionality for Active Directory, DNS, DHCP, IIS, FTP, and AAA services while remaining stable under the existing resource limits, was chosen as a substitute to address the issue.

Following the AAA server's setting up, a second problem emerged. When Windows 10 first underwent testing as a platform for WinRadius, its performance in managing authentication services was unreliable. Service availability was impacted by compatibility and stability problems. The issue was fixed by upgrading to Windows 7, which showed improved stability and smooth WinRadius integration, enabling uniform AAA authentication across network devices.

Resources demand in the EVE-NG simulation environment was another problem. The host system was extremely stressed by running several routers, encrypted DMVPN tunnels, and Windows-based servers at the same time. Occasionally, this led to slower service responsiveness and longer boot times. By carefully allocating resources, starting virtual machines in stages, and restricting the number of active nodes during testing, the problem was resolved. Higher-capacity virtualization systems or specialized hardware would address this in a production setting.

Dependencies sequence and service verification were additional implementation challenges. Some services, like DNS that depends on Active Directory and AAA authentication, needed to be configured in a specific order in order to work properly. Initial authentication and resolution issues resulted from trying to authenticate dependent services before finishing core setups. Restructuring the implementation process to ensure that key services were fully functioning prior adding dependent components was the solution to this problem. To overcome this obstacle, thorough documentation and logical validation were essential.

All things taken into account, the difficulties were overcome by intelligent technological decisions and flexibility, enabling the project to proceed effectively while upholding functional and security standards.

Backup Plan

A backup plan was taken into consideration as part of the overall design to reduce operating potential risks. In the case of a hub or tunnel failure, the DMVPN architecture's redundant hub routers offered automated failover. To enable quick recovery from misconfigurations or system corruption, configurations backups and defined rollback procedures were created.

This strategy might be expanded in a real-world deployment by integrating monitoring systems to proactively identify errors, automating configuration management tools, and keeping off-site configuration backups. These actions would improve the GHN infrastructure's resilience even more.

Future Work

Future upgrades could greatly increase the network's performance and resilience. Prioritizing video conferences and medical data above less important traffic would be possible with the implementation of QoS regulations. To maximize bandwidth usage and regulate traffic flows over the WAN, MPLS Traffic Engineering could be implemented.

It is also possible to incorporate additional security features like firewall, intrusion detection systems, centralized logging, and more precise role-based access controls. The network would be more in line with current healthcare IT trends and potential organizational expansion if the design were expanded to incorporate cloud-based services or hybrid connectivity models.

Synopsis of my experience

Significant technological and professional development was made possible by this project. It improved my comprehension of secure network architecture, WAN design principles, and advanced routing protocols. Beyond technical expertise, the project improved my capacity to organize, record, and oversee a sophisticated ICT solution under practical limitations like time, money, and legal obligations.

My ability to solve problems and think critically was enhanced by working through design choices, resolving problems, and verifying outcomes. The experience is quite similar to what is anticipated of an architect or network engineer in an enterprise healthcare setting.

Bahraini Perspectives

From a Bahraini standpoint, this project supports healthcare innovation, digital transformation, and the growth of local ICT competence, all of which are in line with Bahrain Vision 2030. Enhanced patient care, virtual medical services, and productivity in operations in the Kingdom are all directly impacted by a dependable and secure healthcare network.

The suggested solution shows how cutting-edge networking technology can be practically implemented while adhering to regional data protection regulations and Bahrain's regulatory and cultural framework. It also emphasizes how local businesses may develop and oversee advanced ICT infrastructures in-house, lowering their need on outside suppliers.

Legal, Ethical, Social, and Professional Issues (LESPI)

Legal Issues

Healthcare rules and data protection legislation were carefully taken into account when designing the project. One of the main requirements was adherence to international standards including GDPR and HIPAA as well as Bahrain's Personal Data Protection Law. Patient data is maintained private and secure during transport as well as access due to IPsec encryption, AAA-controlled access, and centralized authentication via Active Directory.

Ethical Issues

The initiative placed a strong emphasis on handling sensitive healthcare data responsibly. The network wasn't created for supplementary uses such unapproved data analysis or AI training, but rather only for assisting healthcare operations. Throughout the design and implementation process, patient privacy, data integrity, and limited access were considered essential responsibilities.

Social Issues

From a social standpoint, workers may initially find it difficult to implement an advanced network infrastructure because of new procedures and technology. To reduce opposition and interruption, training and precise documentation are crucial. Over time, the enhanced network increases patient access to specialist medical treatments and increases collaboration among healthcare providers.

Professional Issues

The project followed industry standards and ICT best practices in a professional manner. Throughout, ethical responsibility, systematic testing, and accurate documentation were upheld. Providing a solution that enhances healthcare services without adding needless risk demonstrates professional responsibility and dedication to improvement.

Conclusion

This thesis established that the operational, security, and performance needs of a multinational healthcare business can be successfully supported by an advanced CCNP-level WAN design. The deployed solution gave Global Health Network a scalable, secure, and resilient network architecture while effectively addressing the shortcomings of the prior basic routing system.

Although several limitations were noted, the overall results supported the project's goals and hypothesis. In addition to representing the technical proficiency and professional preparedness needed in contemporary ICT and networking professions, the work offers a solid basis for future improvements and practical implementation.

References

A Border Gateway Protocol 4 (BGP-4). (2006). https://doi.org/10.17487/rfc4271

AnirbanPaul. (2016). Networking documentation. Retrieved November 23, 2025, from Microsoft.com website: https://learn.microsoft.com/en-us/windows-server/networking/

Apache. (2020). Welcome! - The Apache HTTP Server Project. Retrieved November 23, 2025, from Apache.org website: https://httpd.apache.org/

Badhan, I., Ara, H., Halima, L., Debnat, S., & Islam, M. (2024). COMPARATIVE PERFORMANCE INVESTIGATION OF EIGRP, OSPF, AND RIP ROUTING PROTOCOL FOR CAMPUS AREA NETWORK USING CISCO PACKET TRACERAND OPNET MODELER. International Journal of Advanced Smart Sensor Network Systems (IJASSN), 14(1). https://doi.org/10.5121/ijassn.2024.14101

Cisco. (2017, September). Enhanced Interior Gateway Routing Protocol. Retrieved from Cisco website: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html

Cisco. (2024, October). IP Routing Configuration Guide, Cisco IOS XE 17.x - EIGRP [Cisco IOS XE 17]. Retrieved from Cisco website: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/ip-routing/b-ip-routing/m_ire-enhanced-igrp.html

Cisco. (2025, August). Cisco SD-WAN. Retrieved November 23, 2025, from Cisco website: https://www.cisco.com/site/us/en/products/networking/sdwan-routers/index.html

Cisco. (n.d.). Switches: Support and Downloads. Retrieved November 23, 2025, from Cisco website: https://www.cisco.com/c/en/us/support/switches/category.html

Cisco . (2007). SCALABLE DMVPN DESIGN AND IMPLEMENTATION GUIDE. Retrieved from https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/5991-discussions-wan-routing-switching/319468/1/dmvpn_design_guide(1).pdf

Cisco . (2023). Cisco Packet Tracer. Retrieved November 23, 2025, from Netacad.com website: https://www.netacad.com/cisco-packet-tracer

Cisco . (n.d.). Articles | Cisco Press. Retrieved from www.ciscopress.com website: https://www.ciscopress.com/articles/

Cisco ASR 1000 Series Aggregation Services Routers. (2024, September). Retrieved November 23, 2025, from Cisco website: https://www.cisco.com/site/us/en/products/networking/sdwan-routers/asr-1000-series-aggregation-services-routers/index.html

Cisco Systems, I. (2020). Dynamic Multipoint VPN Configuration Guide, Cisco IOS XE Gibraltar 16.12.x. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16-12/sec-conn-dmvpn-xe-16-12-book.pdf

Cole, B. A., Naganand Doraswamy, Katz, D., Luciani, J. V., & Piscitello, D. M. (2022). RFC 2332: NBMA Next Hop Resolution Protocol (NHRP). Retrieved November 21, 2025, from IETF Datatracker website: https://datatracker.ietf.org/doc/html/rfc2332

Design, C. (2008). Dynamic Multipoint VPN (DMVPN) Design Guide (Version 1.1). Retrieved from https://community.cisco.com/legacyfs/online/legacy/3/9/5/26593-DMVPNbk.pdf

European Union. (2016, April 27). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from Europa.eu website: https://eur-lex.europa.eu/eli/reg/2016/679/oj

EVE-NG. (2023). EVE-NG documentation and user guide. EVE-NG Ltd. Retrieved from https://www.eve-ng.net/index.php/documentation/

Farinacci, D., Li, T., Hanks, S., Meyer, D., & Traina, P. (2000). Generic Routing Encapsulation (GRE). https://doi.org/10.17487/rfc2784

Farinacci, D., Li, T., Meyer, D., Hanks, S., & Traina, P. (2000, March). Generic Routing Encapsulation (GRE). Retrieved from datatracker.ietf.org website: https://datatracker.ietf.org/doc/html/rfc2784

Ferguson, D., Acee Lindem, & Moy, J. (2008). RFC 5340: OSPF for IPv6. Retrieved November 30, 2025, from IETF Datatracker website: https://datatracker.ietf.org/doc/html/rfc5340

Ferguson, D., Lindem, A., & Moy, J. (2008, July 1). OSPF for IPv6. Retrieved November 13, 2023, from IETF website: https://datatracker.ietf.org/doc/html/rfc5340

Forouzan, B. A. (2013). Data Communications and Networking (5th ed.). New York, Ny: Mcgraw-Hill.

GNS3 Technologies. (2016). Getting Started with GNS3 | GNS3 Documentation. Retrieved November 23, 2025, from Gns3.com website: https://docs.gns3.com/docs/

Government of Bahrain. (2023). Bahrain economic Vision 2030. Retrieved from Bahrain.bh website: https://www.bahrain.bh/wps/portal/en/

Halabi, S., & Mcpherson, D. (2000). Internet Routing Architectures, Second Edition. Retrieved from https://cdn.preterhuman.net/texts/manuals/Internet%20Routing%20Architectures%202nd%20Ed.pdf

hMailServer. (n.d.). Functionality - hMailServer - Free open source email server for Microsoft Windows. Retrieved from www.hmailserver.com website: https://www.hmailserver.com/functionality

Huitema, C. (2000). Routing in the Internet. Prentice Hall.

IEEE. (2018). IEEE Standards Association. Retrieved November 21, 2025, from IEEE Standards Association website: https://standards.ieee.org/ieee/802.1D/3387/

Jensen, T. (2021, June 23). Getting started with EVE-NG. Retrieved November 23, 2025, from Cavelab blog website: https://blog.cavelab.dev/2021/06/getting-started-with-eve-ng/

John-Hart. (2025). IIS documentation. Retrieved November 23, 2025, from Microsoft.com website: https://learn.microsoft.com/en-us/iis/

juniper, N. (2023, October 1). Reference architecture: Enterprise WAN network design. Retrieved from juniper.net website: https://www.juniper.net/documentation/us/en/software/nce/enterprise-wan-ref-architecture/enterprise-wan-ref-architecture.pdf

Kent, S. (2005, December). RFC 4303: IP Encapsulating Security Payload (ESP). Retrieved November 21, 2025, from IETF Datatracker website: https://datatracker.ietf.org/doc/html/rfc4303

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security Techniques for the Electronic Health Records. Journal of Medical Systems, 41(8). https://doi.org/10.1007/s10916-017-0778-4

Kundu, A., Atallah, M., & Bertino, E. (2010). Data in the Cloud: Authentication of Trees, Graphs, and Forests Without Leaking. Retrieved from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2010-06.pdf

Li, D., Cole, B. A., Morton, P., & Li, T. (1998, March). RFC 2281: Cisco Hot Standby Router Protocol (HSRP). Retrieved November 21, 2025, from IETF Datatracker website: https://datatracker.ietf.org/doc/html/rfc2281

Mannee, D., Hanneke van Helvoort, & Frans De Jongh. (2020). The Feasibility of Measuring Lung Hyperinflation With a Smart Shirt: An in Vitro Study. IEEE Sensors Journal, 20(24), 15154–15162. https://doi.org/10.1109/jsen.2020.3010265

Marah, H. M., Khalil, J. R., Elarabi, A., & Ilyas, M. (2021). DMVPN Network Performance Based on Dynamic Routing Protocols and Basic IPsec Encryption. 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). https://doi.org/10.1109/icecce52056.2021.9514142

Microsoft. (2016). Exchange documentation. Retrieved November 23, 2025, from Microsoft.com website: https://learn.microsoft.com/en-us/exchange/

Moy, J. (1998, April). OSPF version 2 (RFC 2328). Internet Engineering Task Force. Retrieved from datatracker.ietf.org website: https://datatracker.ietf.org/doc/html/rfc2328

Putty icon. (2025). Retrieved November 23, 2025, from Wikimedia.org website: https://upload.wikimedia.org/wikipedia/commons/thumb/3/30/PuTTY_Icon_upstream.svg/1200px-PuTTY_Icon_upstream.svg.png

Rekhter, Y., Hares, S., & Li, T. (2006, January 1). A Border Gateway Protocol 4 (BGP-4). Retrieved October 21, 2021, from IETF website: https://datatracker.ietf.org/doc/html/rfc4271

Router Icon. (2025). Retrieved November 23, 2025, from Clipartmax.com website: https://www.clipartmax.com/png/middle/44-447054_router-visio-cisco-router-icon.png

Senecal, L. (n.d.). Layer 2 Attacks and Their Mitigation. Retrieved from https://www.cisco.com/c/dam/global/fr_ca/training-events/pdfs/L2-security-Bootcamp-final.pdf

Seo, K., & Kent, S. (2005, December). RFC 4301: Security Architecture for the Internet Protocol. Retrieved November 21, 2025, from IETF Datatracker website: https://datatracker.ietf.org/doc/html/rfc4301

Stanek, W. R. (2010). Windows 7 : the definitive guide. Sebastopol, Ca: O'reilly.

switch image. (2025). Retrieved November 23, 2025, from Gstatic.com website: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcT34w_tApxbp323ePS-g365lCM6ZP3vdhdetQ&s

Thunderbird. (2025). Thunderbird — Free Your Inbox. Retrieved November 30, 2025, from Thunderbird website: https://www.thunderbird.net/en-US/

thunderbird icon image. (2025). Retrieved November 30, 2025, from S-microsoft.com website: https://store-images.s-microsoft.com/image/apps.35029.14299881443157287.51832ff2-ee23-4073-9058-b88552bc7a10.add5cd70-f8a0-45bc-9b91-ee78550cf20e

U.S. Department of Health and Human Services. (2022). Your rights under HIPAA. Retrieved from HHS.gov website: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

Ubuntu. (2016). BIND9ServerHowto - Community Help Wiki. Retrieved November 23, 2025, from Ubuntu.com website: https://help.ubuntu.com/community/BIND9ServerHowto

Vyncke, E. (2006). Layer 2 Security. Retrieved from www.cisco.com website: https://www.cisco.com/c/dam/global/da_dk/assets/docs/security2006/Security2006_Eric_Vyncke_2.pdf

We, H., Bin, I., & Al Khalifa. (2018). Law No. (30) of 2018 with Respect to Personal Data Protection Law. Retrieved from https://www.pdp.gov.bh/en/assets/pdf/regulations.pdf

windows 7 icon image . (2025). Retrieved November 30, 2025, from Notebookcheck.net website: https://www.notebookcheck.net/fileadmin/Notebooks/News/_nc3/win_7_end_of_life.jpg

Windows 10 Pro image. (2025). Retrieved November 23, 2025, from B-cdn.net website: https://softwarehubs.b-cdn.net/media/2024/07/Windows-10-Professional2.png

windows Server 2012 R2 image. (2025). Retrieved November 30, 2025, from Hosteurope.de website: https://www.hosteurope.de/blog/wp-content/uploads/2015/09/windows2.png

Appendices

Appendix I: System and User Manuals

In this section will demonstrate the manuals for system and user

User manuals

This section describes the steps required for users to access and interact with the GHN network topology using the EVE-NG simulation platform hosted inside VMware.

To access the GHN topology, VMware Workstation must first be launched on the host machine. VMware is used to run the EVE-NG virtual machine, which hosts all network devices, servers, and configurations used in this project.

Figure 252 VMware Icon

The figure above shows the VMware Workstation icon used to start the virtualization environment.

Figure 253 EVE-NG Inside VMware

Once VMware is opened, the EVE-NG virtual machine becomes visible inside the VMware interface. The figure above illustrates the EVE-NG virtual machine listed within VMware before startup. To initiate the environment, the user must power on the EVE-NG virtual machine.

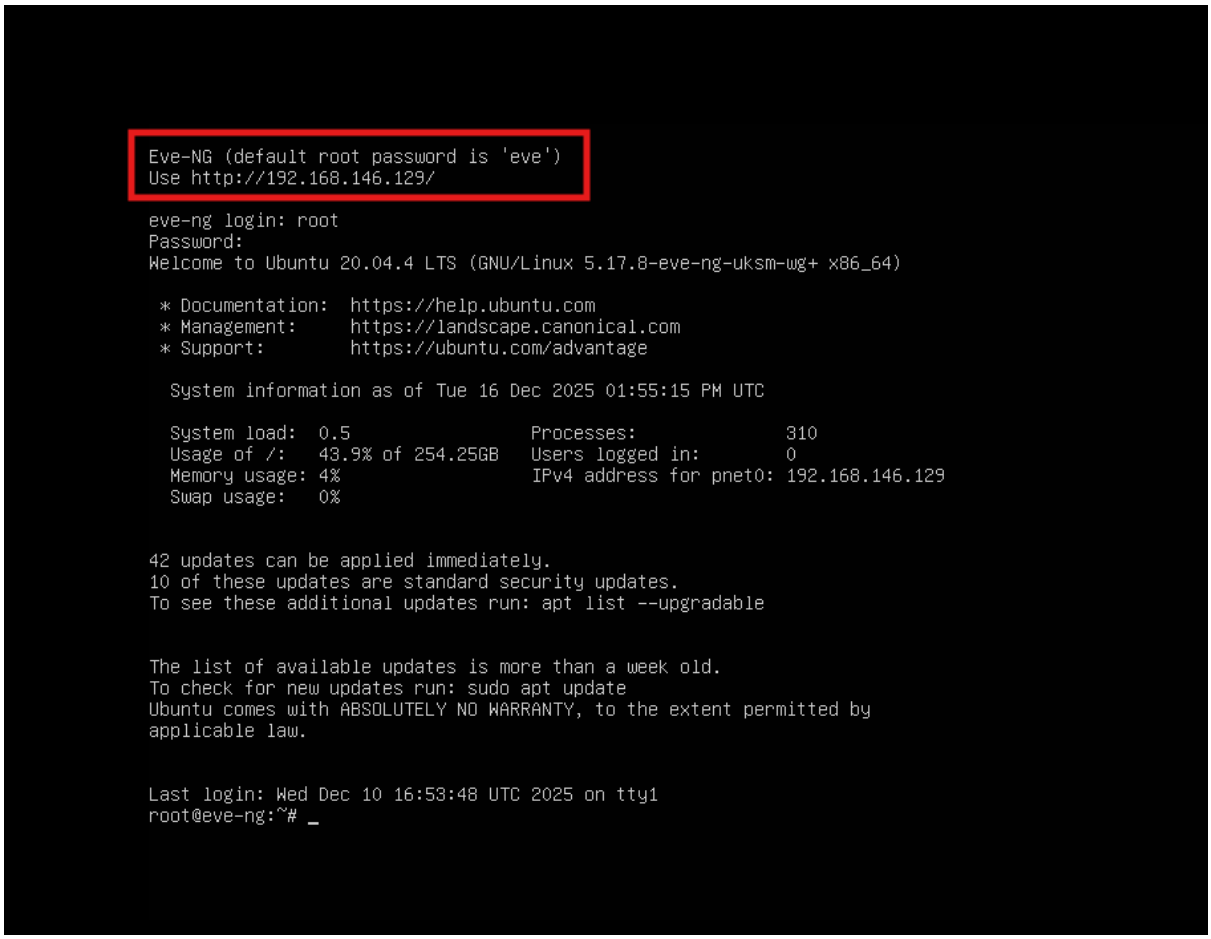

Figure 254 EVE-NG Login Part 1

After the virtual machine finishes booting, EVE-NG prompts for login credentials via the console. The default credentials are:

- **Username:** root
- **Password:** eve

At this stage, the system also displays the IP address assigned to the EVE-NG management interface, which is required to access the web-based GUI. This is shown in figures above.

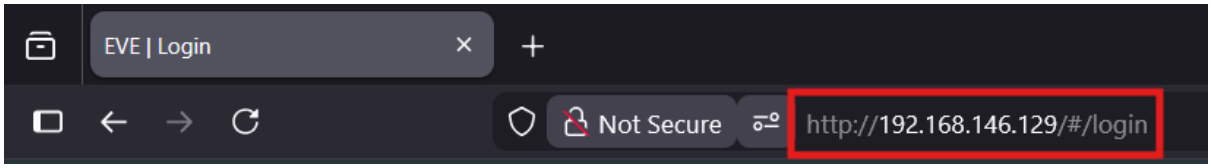

Figure 255 EVE-NG Login Part 2

Using a web browser, the user enters the displayed IP address to access the EVE-NG web interface. The figures above shows the browser-based access to the EVE-NG login page

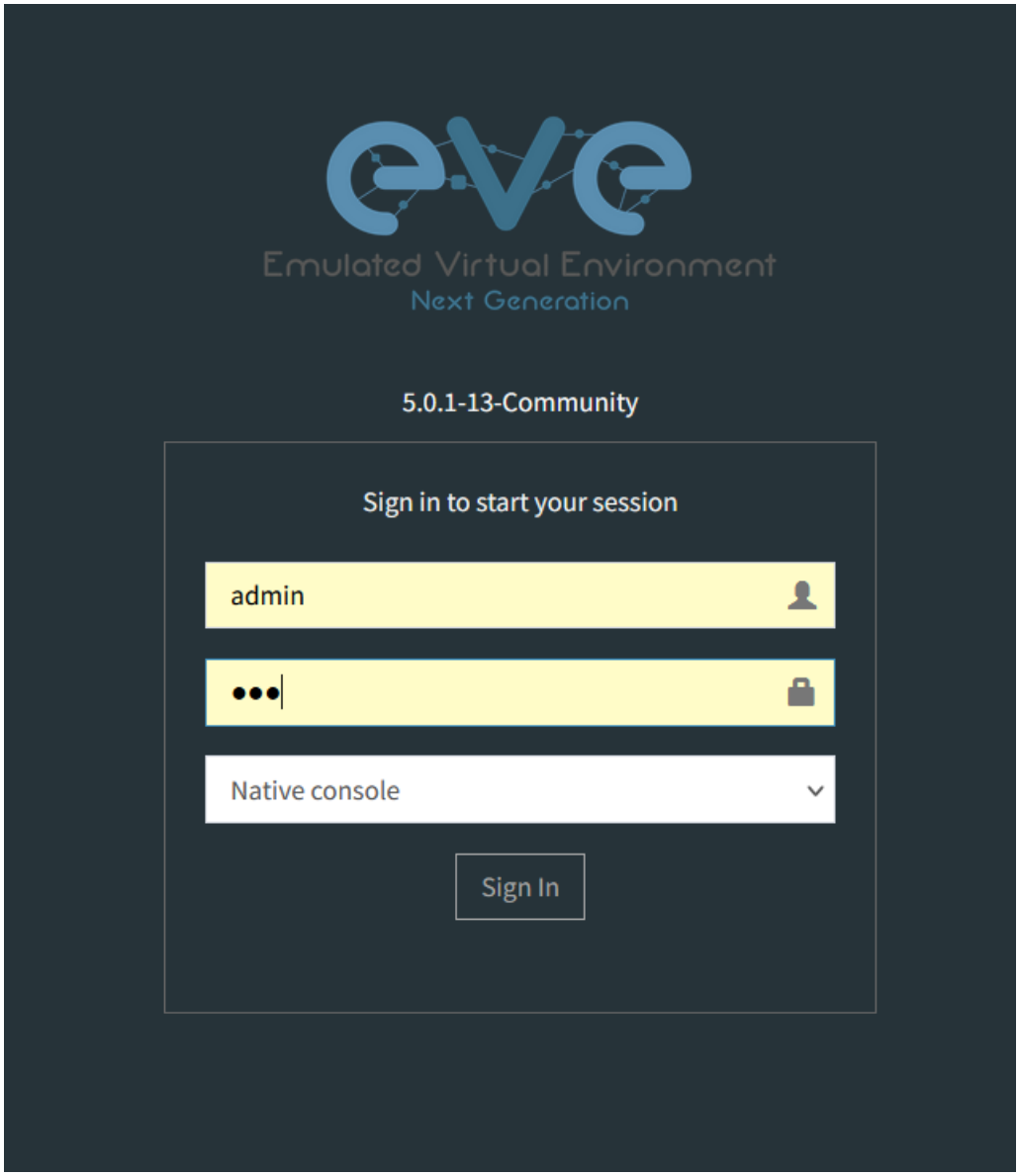

Figure 256 EVE-NG Login Part 3

The web interface requires separate credentials:

- **Username:** admin
- **Password:** eve

Successful authentication leads to the EVE-NG dashboard, as illustrated in figures above.

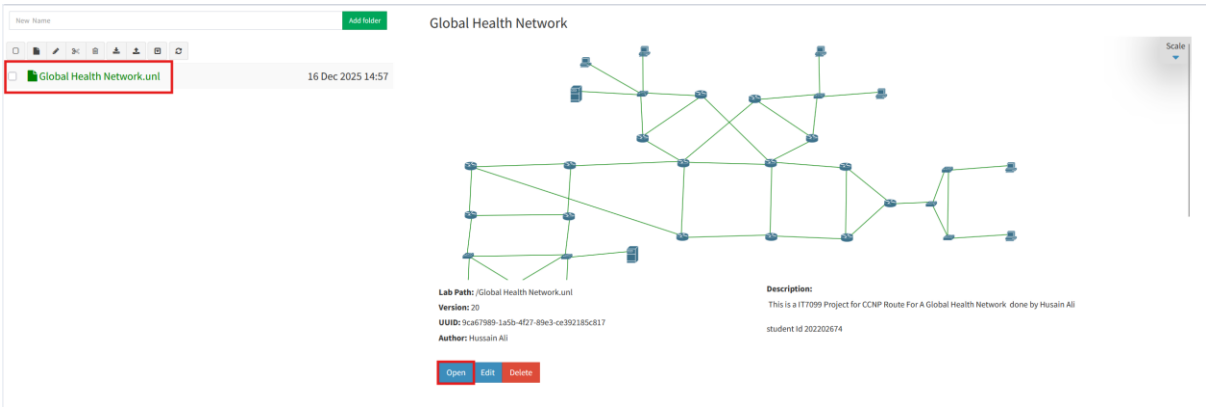

Figure 257 EVE-NG Login Part 4

Once logged in, the user is presented with the list of available labs. The GHN topology can be accessed by selecting the appropriate lab file and clicking *Open*. the figure above shows the GHN topology loaded within the EVE-NG workspace.

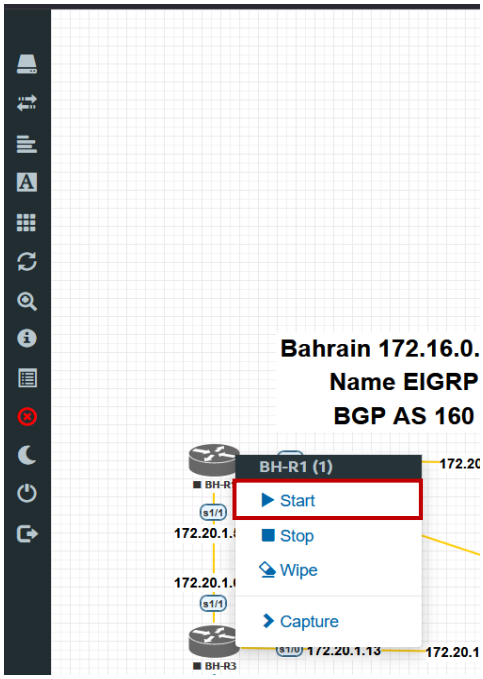

Figure 258 EVE-NG Router Access Part 1

To interact with a network device, the user selects the required router or switch and chooses *Start*. This action powers on the selected device and allows console access for configuration, verification, and testing.

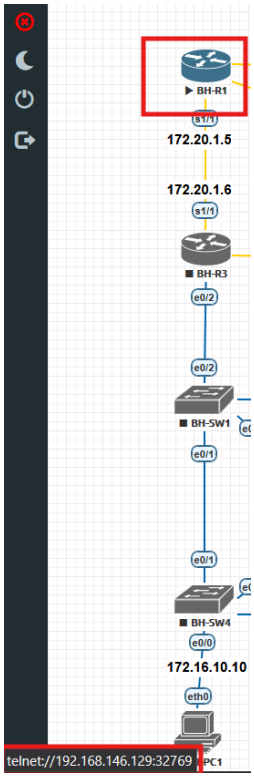

Figure 259 EVE-NG Router Access Part 1

When hovering the mouse cursor over a router icon inside the EVE-NG topology, the system displays the management IP address and port number assigned to that device. This information is required for manual access using an external terminal emulator. As shown in the figure above , the displayed format includes the IP address followed by the TCP port used for Telnet access.

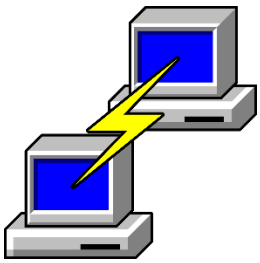

Figure 260 EVE-NG Router Access Part 2

This figure above shows the PuTTY application icon, which is used as the primary terminal emulator for accessing GHN routers and switches. PuTTY supports Telnet and SSH protocols and is used throughout the project to establish command-line access to network devices hosted inside the EVE-NG environment.

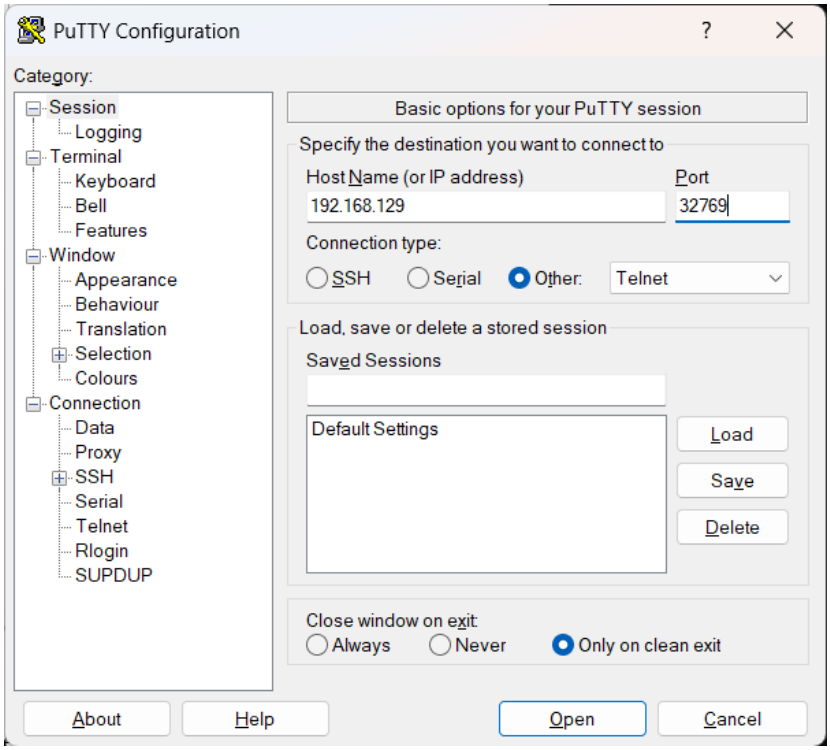

Figure 261 EVE-NG Router Access Part 3

To connect manually, the user opens PuTTY, enters the displayed IP address and port number in the Host Name field, selects Telnet under Connection type, and clicks Open. This establishes a Telnet session to the selected router and provides direct CLI access. The PuTTY configuration screen shown in the figure confirms the correct host, port, and protocol selection required for successful connectivity.

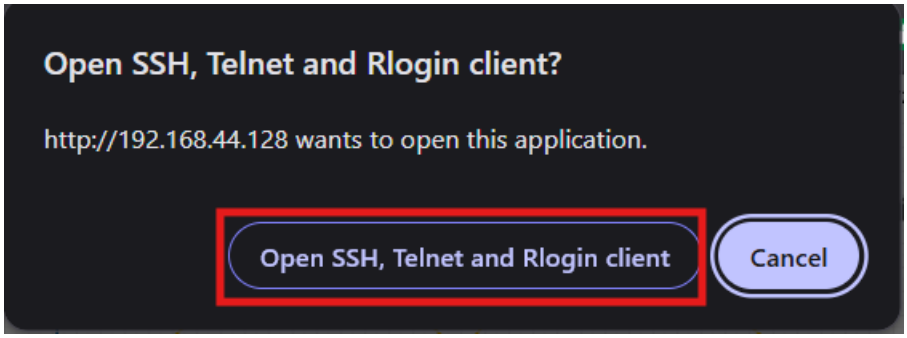

Figure 262 Alternative EVE-NG Router Access

Alternatively, EVE-NG provides browser-based integration for terminal access. When the user clicks directly on a router within the topology, the browser prompts whether to open an SSH, Telnet, or Rlogin client. Upon confirmation, the browser automatically launches PuTTY with the correct connection parameters preconfigured. This method removes the need for manual IP and port entry and ensures faster, error-free access.

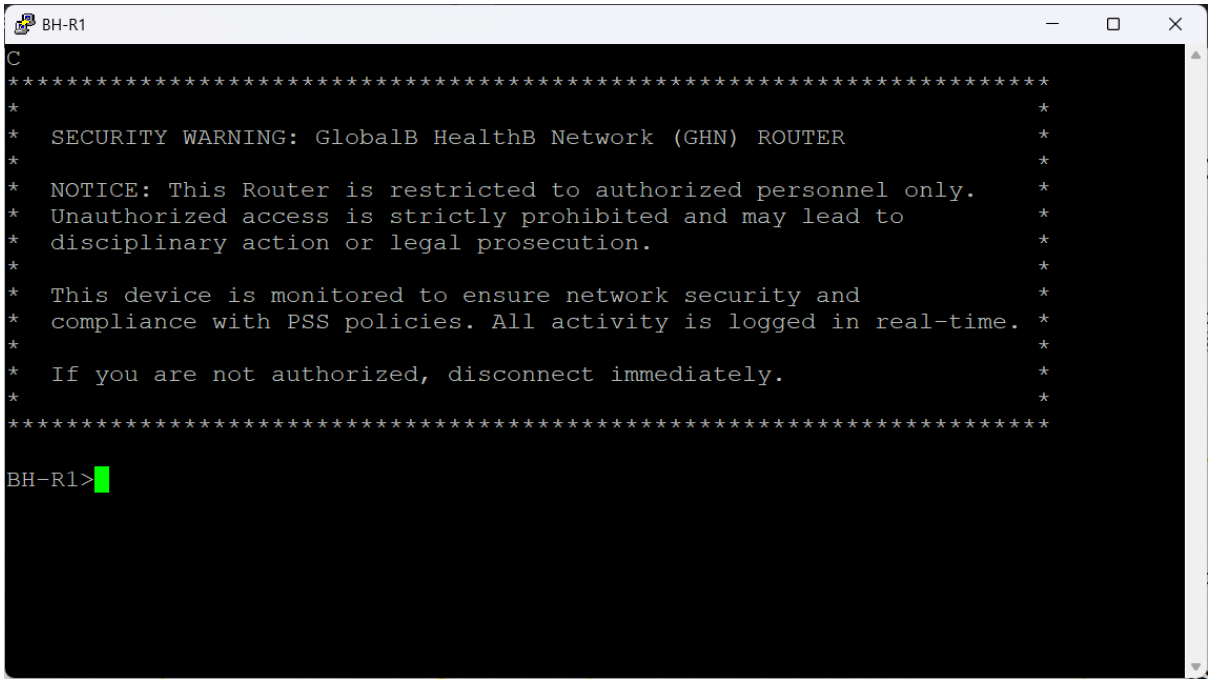

Figure 263 EVE-NG Router Access Part 4

Once the connection is established using either method, the router displays the configured security banner (MOTD) followed by the command-line interface prompt. This confirms successful access and enforces security awareness by notifying users that the device is restricted to authorized personnel only.

System manuals

One of the key system administration tasks is importing router, switch, ISO for windows and Windows Server images into EVE-NG. To perform this task, the **WinSCP** application is used to securely transfer files from the host system to the EVE-NG virtual machine.

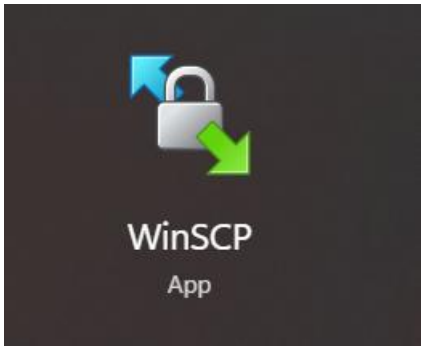

Figure 264 WinSCP icon

The figure above shows the WinSCP application icon used for secure file transfer.

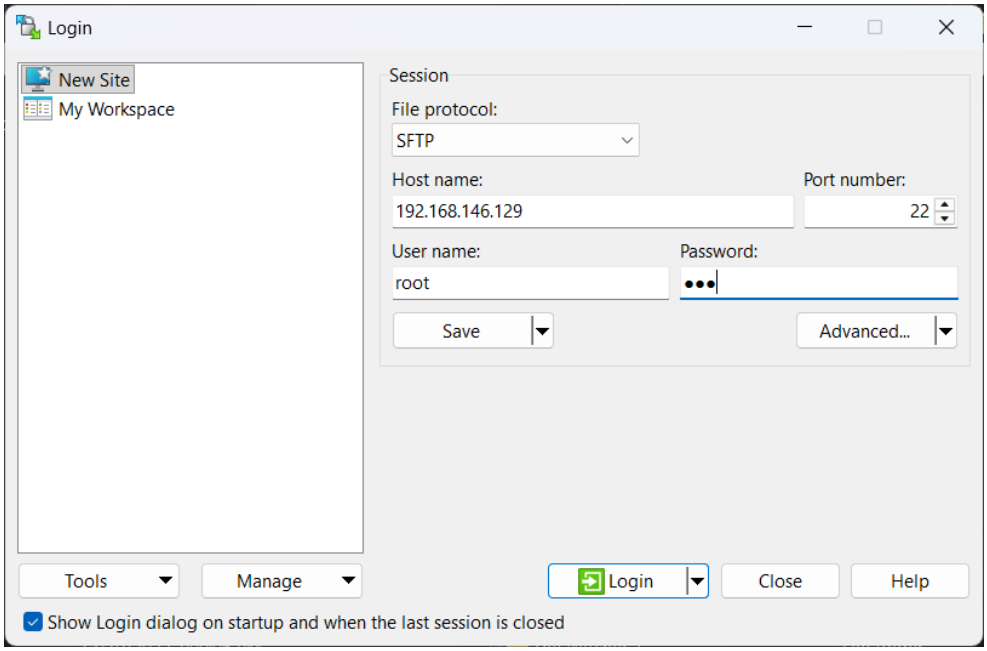

Figure 265 WinSCP Part 1

WinSCP connects to the EVE-NG system using the SSH protocol, allowing administrators to upload IOS images, server images, and supporting files into the appropriate directories on the EVE-NG filesystem. Once images are transferred, they can be integrated into the platform

and used to create or modify network topologies. The figure above shows how to access the EVE-NG VM using WinSCP the username and the password are:

- **Username:** root
- **Password:** eve

Windows Server2012 R2:

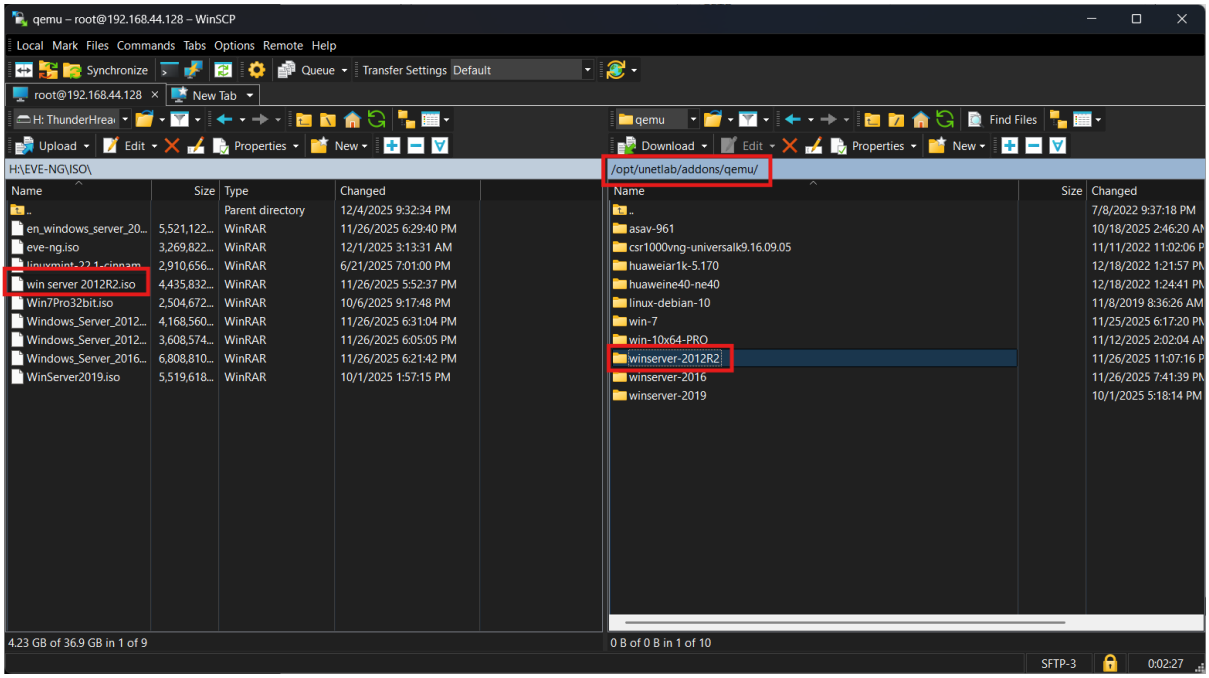

Figure 266 WinSCP Part 2

On the right side, which represents the EVE-NG server, and the left side, which represents your local PC, navigate as follows. From the EVE-NG side, go to the directory:

/opt/unetlab/addons/qemu

Inside this path, create a new directory named: Winserver2012R2

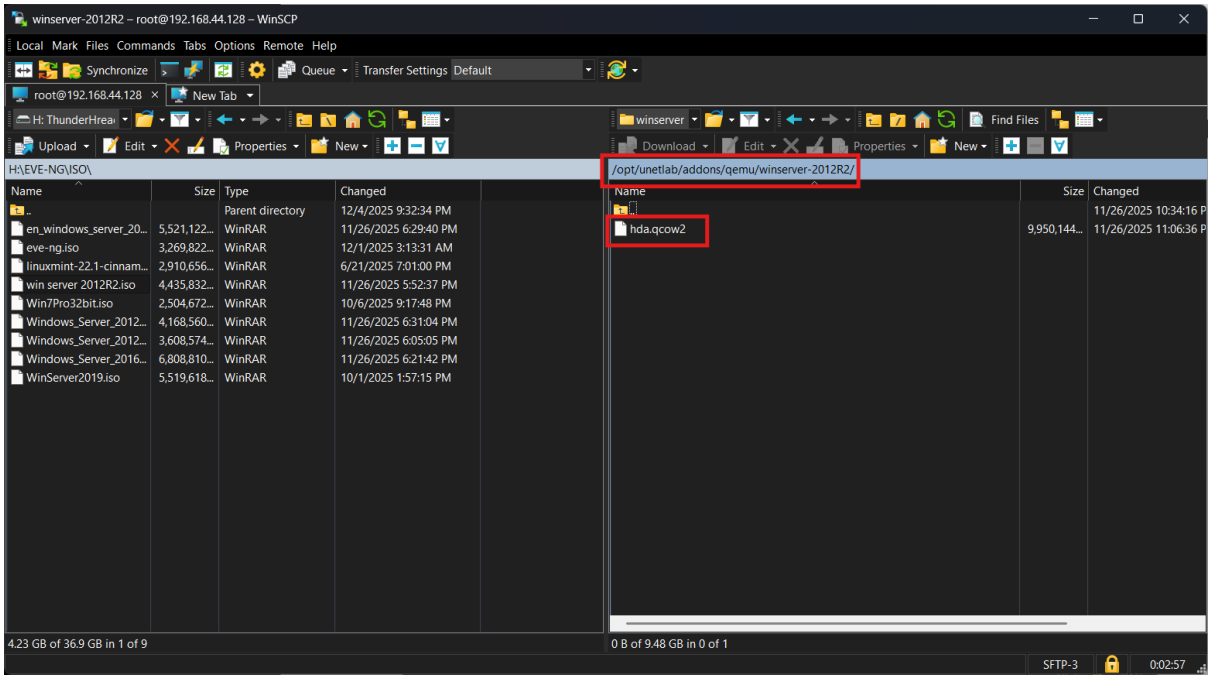

Figure 267 WinSCP Part 3

Inside the Winserver2012R2 directory, copy the Windows Server 2012 R2 image file from your system to the EVE-NG server. After copying, rename the file to hda.qcow2 so that EVE-NG can properly recognize and use it as a QEMU disk image.

Windows 7:

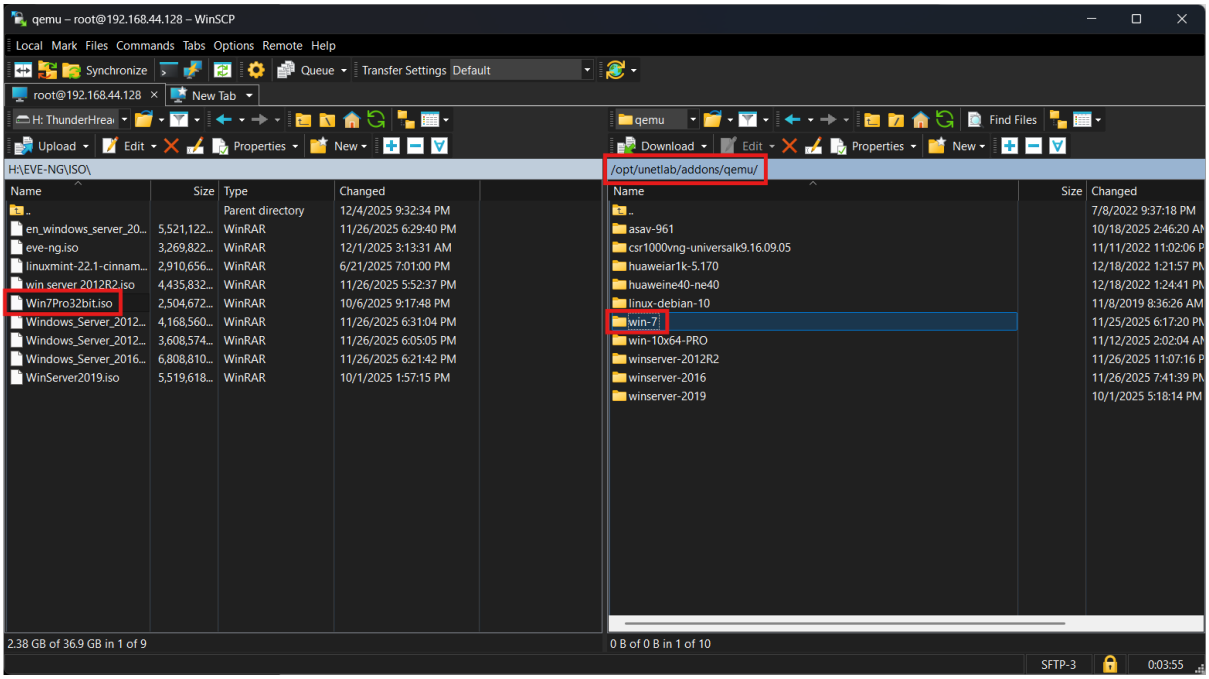

Figure 268 WinSCP Part 4

On the **right side**, which represents the **EVE-NG server**, navigate to the following directory:

/opt/unetlab/addons/qemu

Within this path, create a new directory named: Win-7

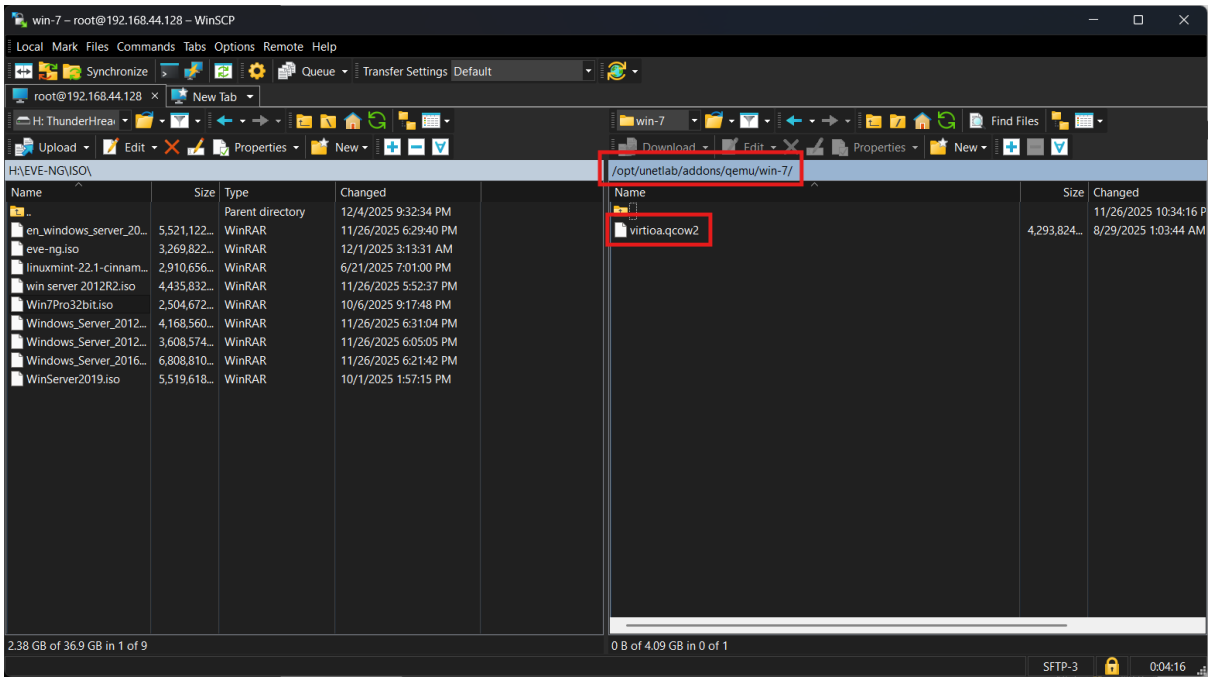

Figure 269 WinSCP Part 5

Inside the Win-7 directory, copy the Windows 7 image file from your system to the EVE-NG server. After copying, rename the file to hda.qcow2 so that EVE-NG can correctly recognize and use it within the EVE-NG environment.

Windows 10 Pro:

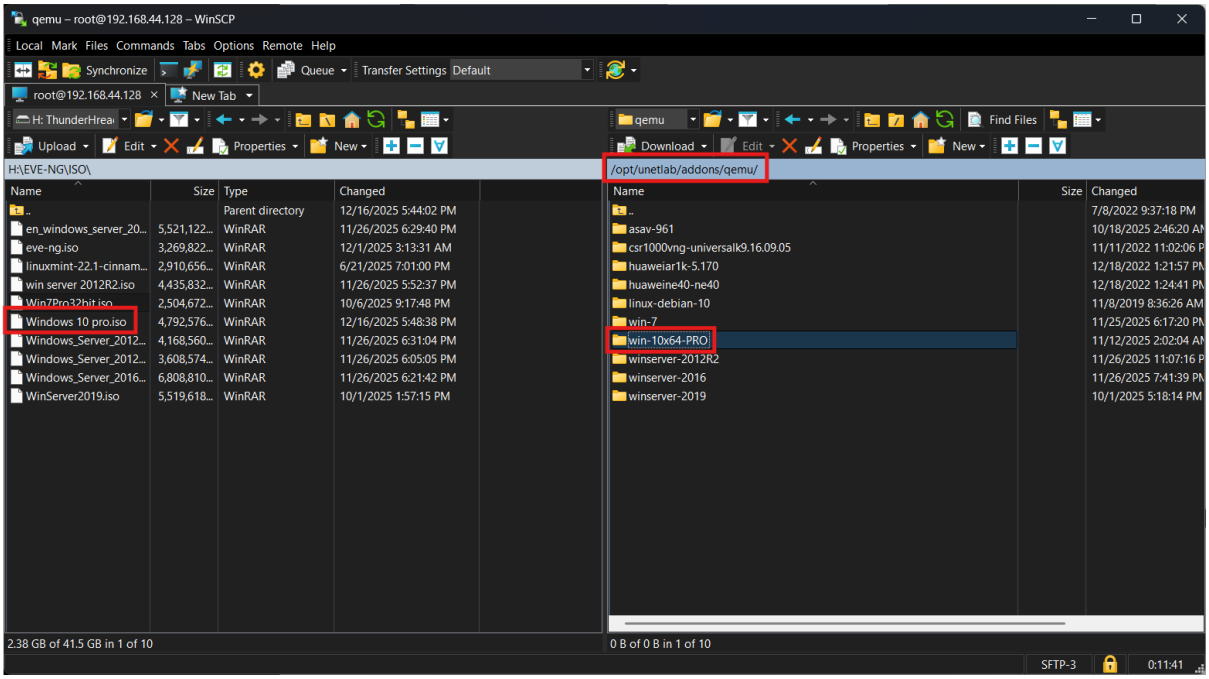

Figure 270 WinSCP Part 6

On the right side, representing the EVE-NG server, navigate to the following directory:

/opt/unetlab/addons/qemu

Within this directory, create a new folder named: Win-10x64-PRO

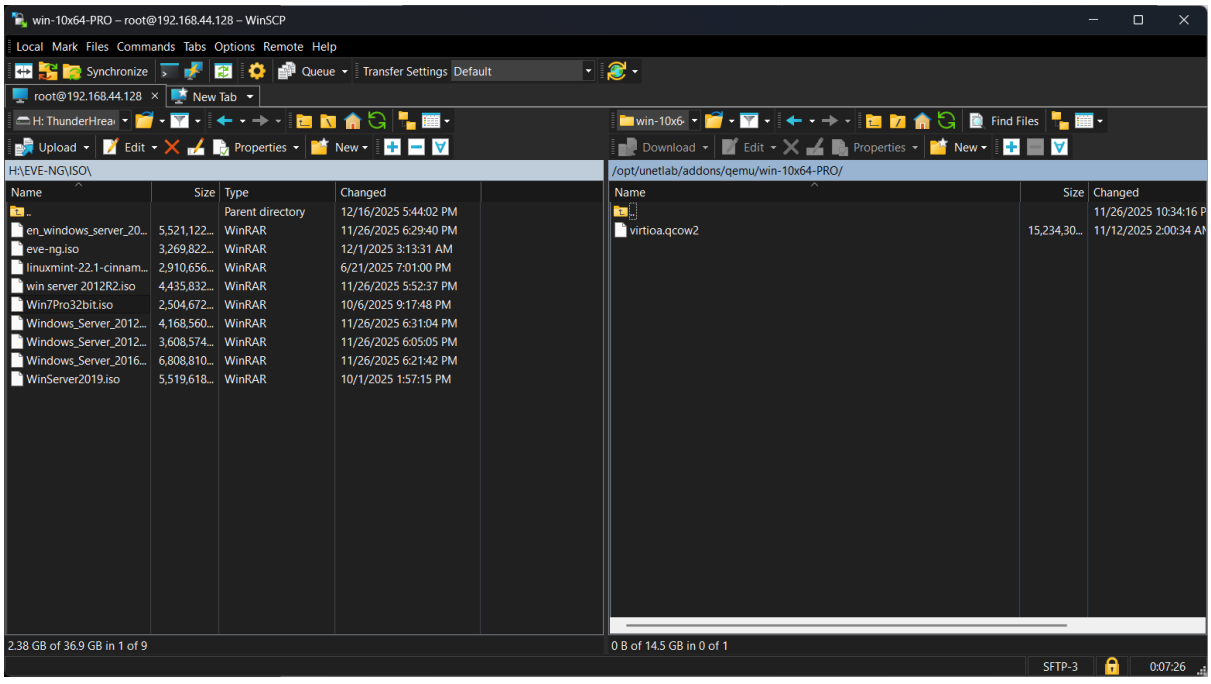

Figure 271 WinSCP Part 7

Inside the Win-10x64-PRO directory, copy the Windows 10 Pro (64-bit) image file from your system to the EVE-NG server. After copying, rename the file to hda.qcow2 so that EVE-NG can correctly recognize and use it as a QEMU disk image.

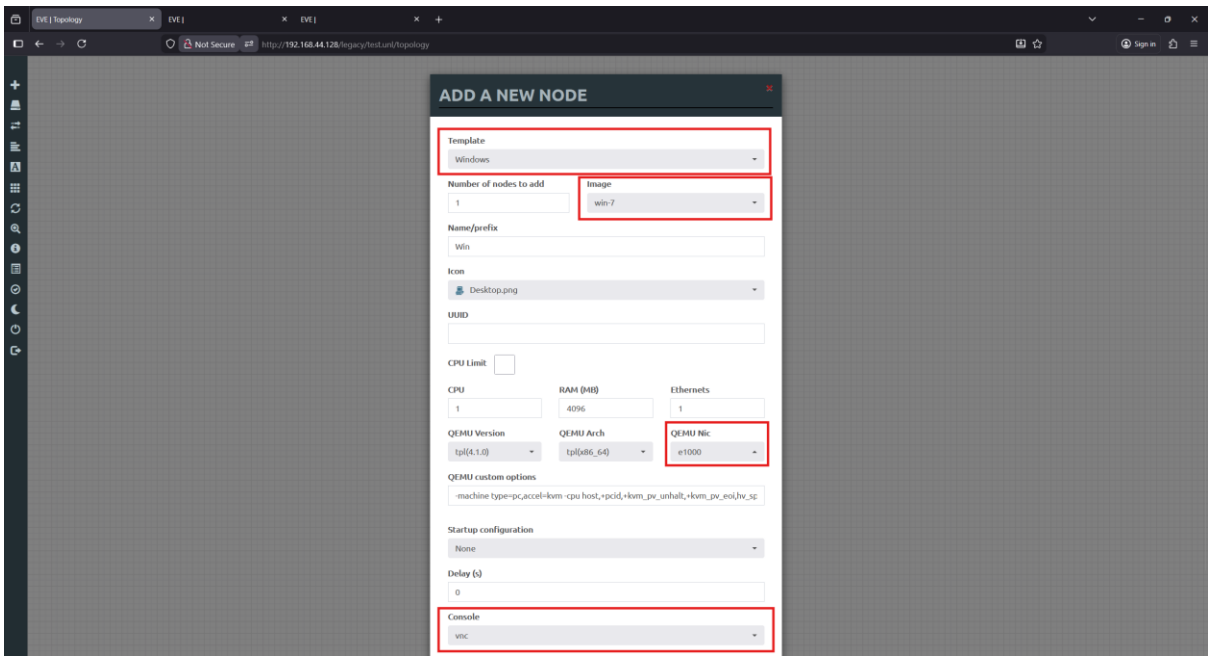

Figure 272 WinSCP verification Part 1

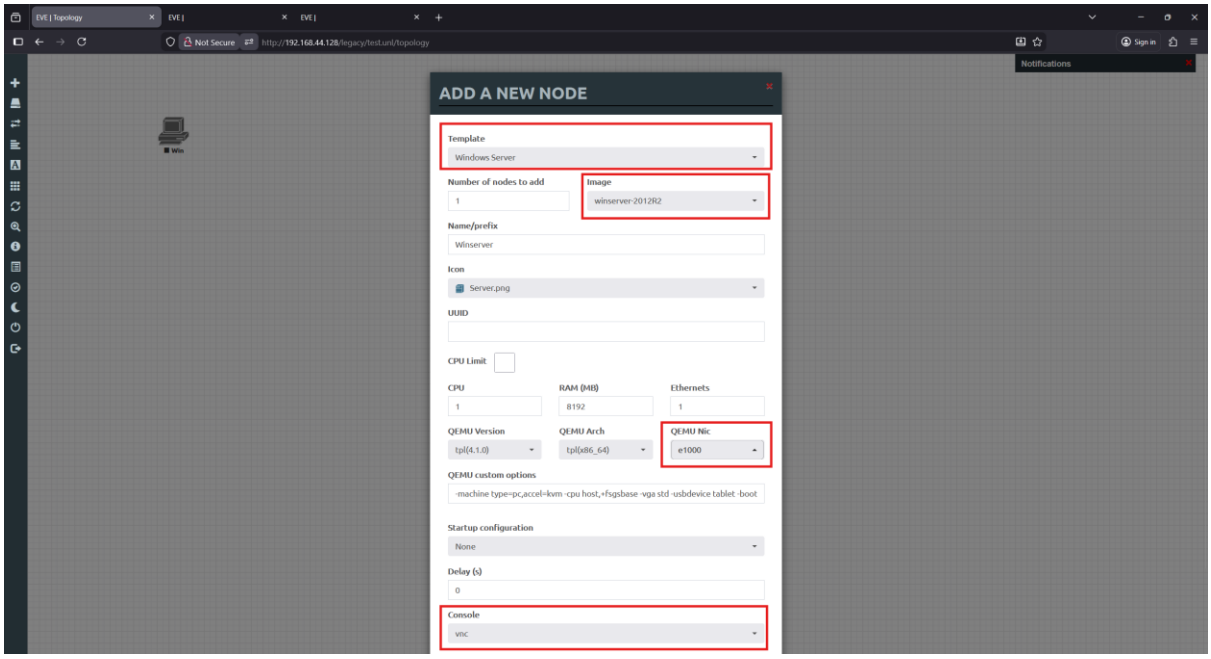

Figure 273 WinSCP verification Part 2

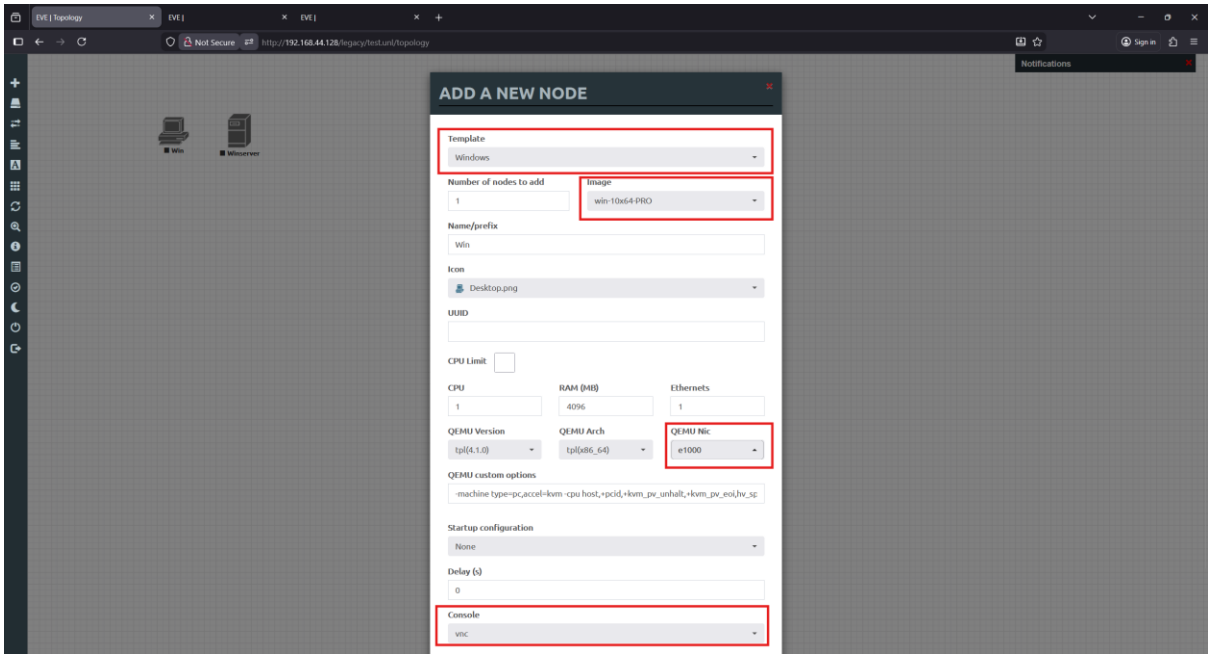

Figure 274 WinSCP verification Part 3

Once the images are in place, they can be accessed directly from EVE-NG.

Click Add an object → Node, then search for Windows Server, Windows 7 Windows 10 Pro. The images will appear in the list, as shown in the figure above.

Selecting an image opens the node configuration window, shown in the figures below. This window allows you to configure key parameters such as the image name, allocated RAM, number of CPUs, network interfaces, and any required QEMU options before deploying the virtual machine.

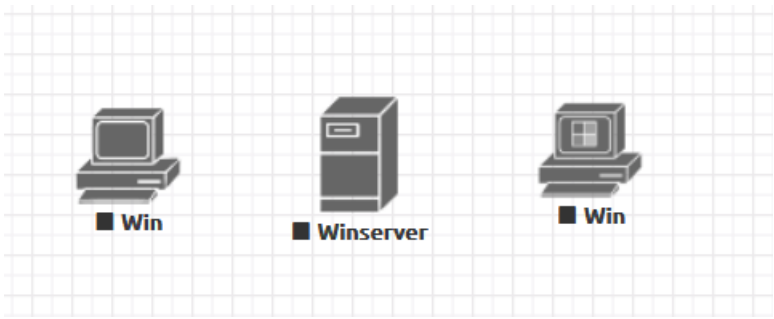

Figure 275 WinSCP verification Part 4

All nodes were added to the lab topology and tested using the VNC console, allowing direct interaction with the operating systems and verification that each virtual machine was functioning correctly.

Cisco IOL Router and switch:

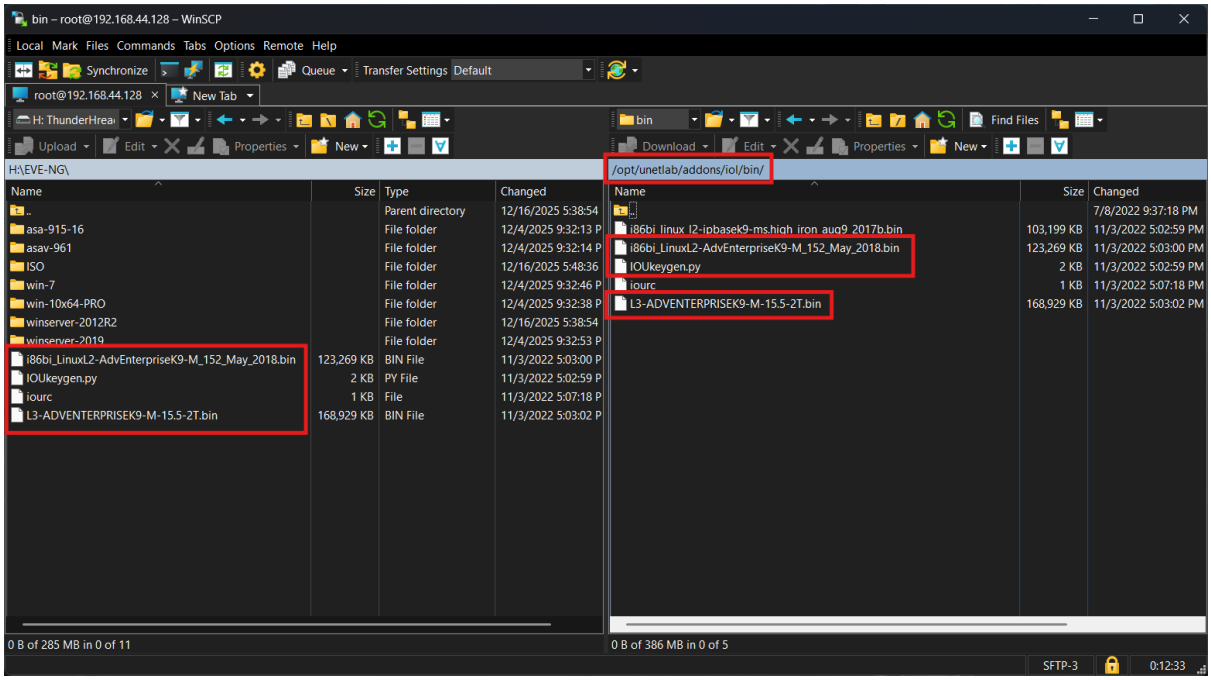

Figure 276 WinSCP IOL

On the right side, which represents the EVE-NG server, navigate to the following directory:

/opt/unetlab/addons/iol/bin

Move the router and switch IOL image files, along with their associated files, into this directory so they can be copied and made available for use within the EVE-NG environment.

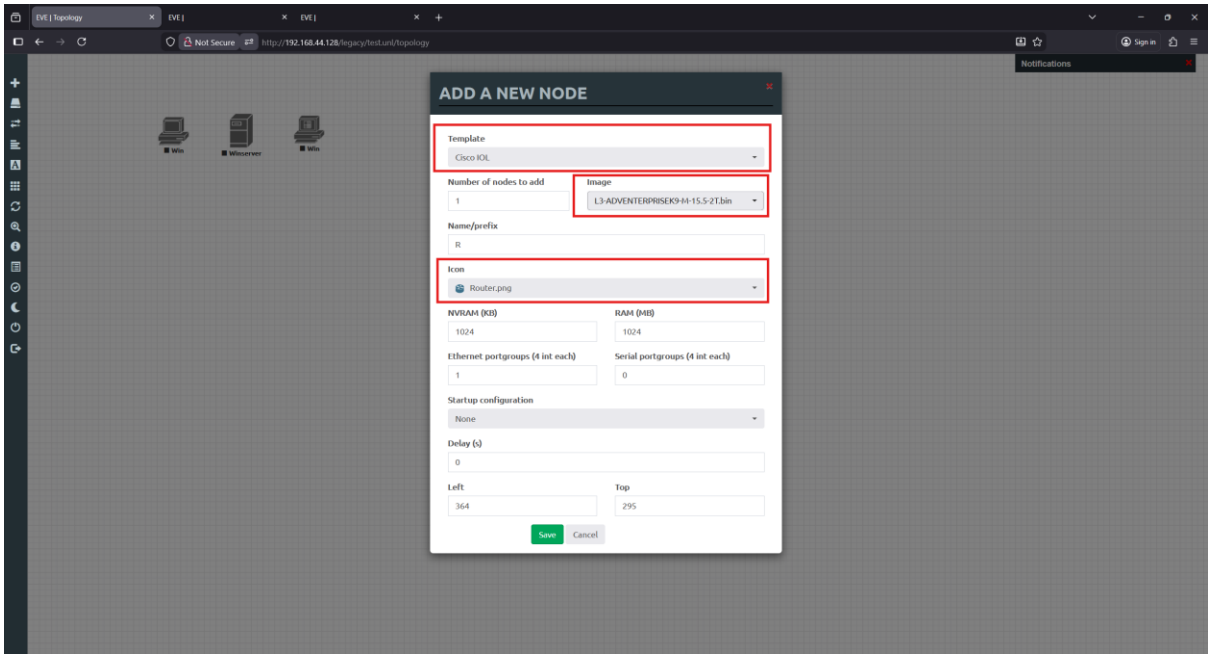

Figure 277 WinSCP IOL Verification Part 1

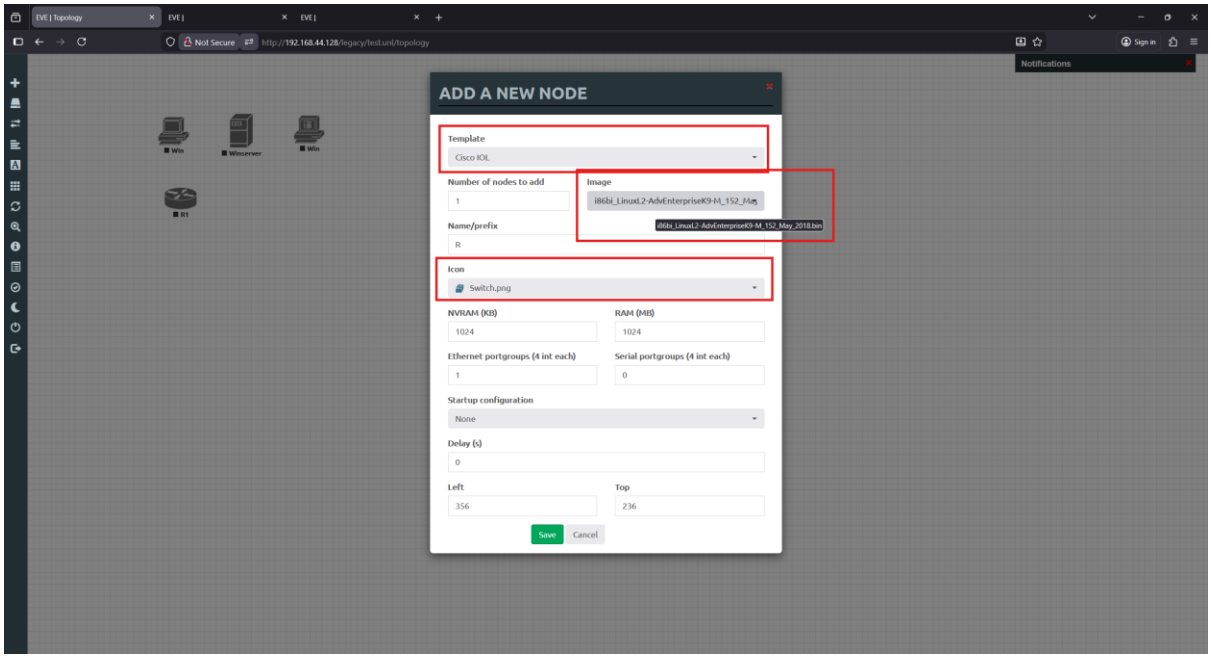

Figure 278 WinSCP IOL Verification Part 2

Once the images are in place, they can be accessed directly from EVE-NG.

Click Add an object → Node, then search for Cisco IOL. The L3 image represents the router, while the L2 2018 image represents the switch. Both will appear in the node selection list, as shown in the figure above.

Selecting either image opens the node configuration window, shown in the figures below. This window allows configuration of parameters such as the image name, allocated RAM, number of CPUs, network interfaces, and other relevant options before adding the node to the lab topology.

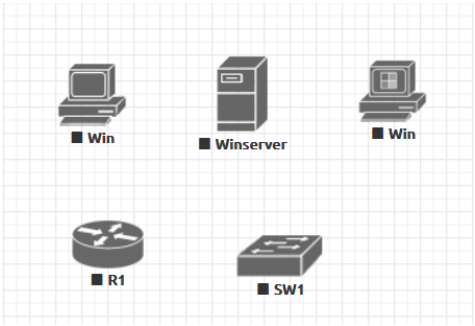

Figure 279 WinSCP IOL Verification Part 3

The figure above shows that the Windows nodes and Cisco IOL devices have been successfully added to the lab topology.

Appendix II: Detailed Design

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 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 organization that requires secure, reliable connectivity between four main locations:

- **Bahrain** primary regional hub and main data center, 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 allow centralized 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 through 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

Table 9 Networks Adders Table

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

Table 10 Bahrain Adders Table

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

Table 11 England Adders Table

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

Table 12 Luxembourg Adders Table

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

Table 13 China Adders Table

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

Table 14 ISP Adders Table

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

Table 15 Router ID Table

VTP	
Bahrain	bahrain@vtp
England	england@vtp

Table 16 VTP Table

VLANs	
IT	10
Guests	20
Servers	30
Management/Native	100

Table 17 VLANs Table

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

Table 18 SSH Table

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

Table 19 DMVPN Tunnels Table

Network Topologies (Logical Design)

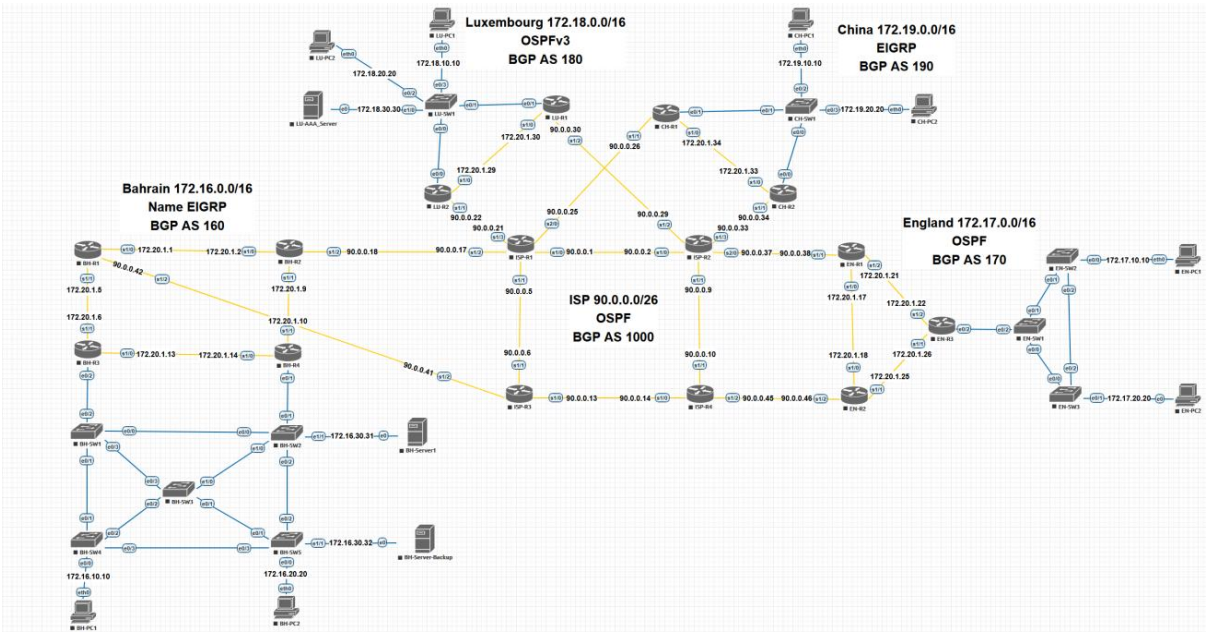

Figure 280 Logical Design

Physical Design

In this section will show the rack design for GHN branches (Bahrain, Luxembourg, China, England)

Bahrain Branch Rack design

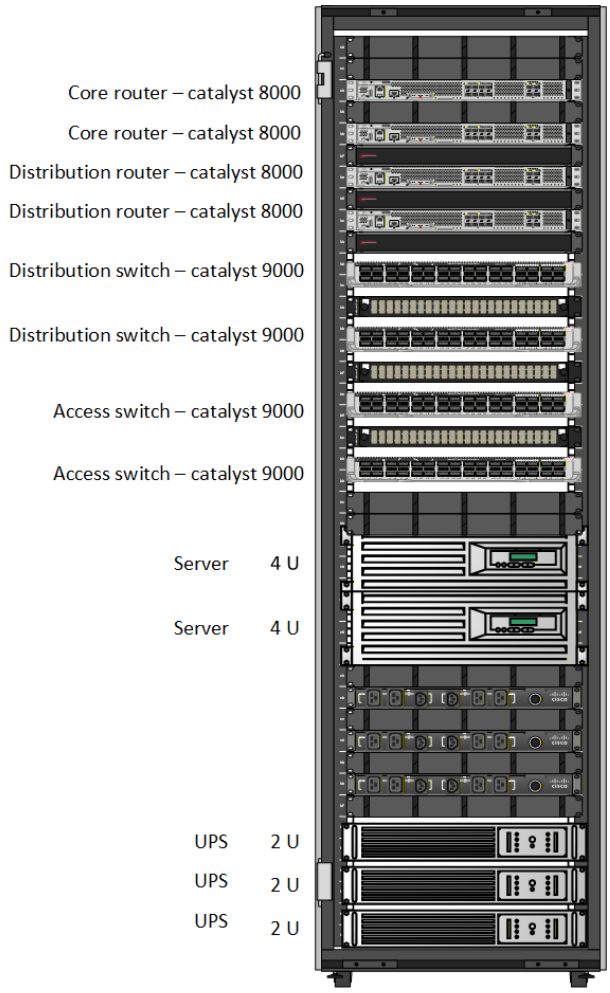

Figure 281 BH Branch Rack design

The Global Health Network's Bahrain (BH) branch is represented by this rack diagram, which matches the implemented topology and complies to conventional rack-mounting procedures. The patch panels and cable management components, which terminate all network connections and maintain cable organization, are located at the top of the rack. The access switch, which enables quick and clean patch connections, is located directly beneath them. Because it manages external connectivity for the Bahrain branch and requires less wiring, the WAN router is positioned beneath the switch.

The Windows Server is positioned in the center of the rack to supply the Bahrain branch with essential network functions like Active Directory, DNS, and DHCP. To facilitate both local backups and centralized storage, the NAS is placed in close proximity to the server. Because of their weight and need for cooling, these devices are positioned lower in the rack.

The UPS is positioned at the bottom of the rack to supply all equipment above it with continuous power. Rack stability is increased and dependable power protection is ensured by placing the UPS at the lowest level. All things considered, this arrangement produces a tidy, useful, and realistic rack design that is appropriate for the Bahrain branch and in line with the Global Health Network deployment.

England Branch Rack design

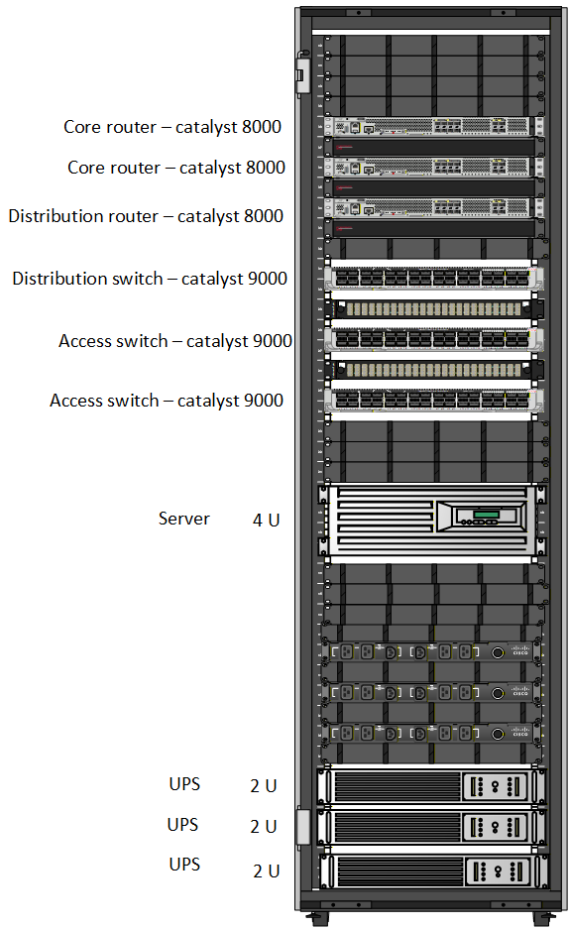

Figure 282 EN Branch Rack design

This rack diagram shows a multilayer network configuration set up in accordance with normal rack-mounting procedures and depicts the England branch (EN). The routing devices, which manage upstream and inter-site communication and need little physical cabling, are located at the top of the rack. The distribution and access switches are positioned closer to one another beneath them in order to effectively aggregate network traffic and maintain brief and well-organized patching.

A 4U server is installed in the lower center area of the rack to supply the England branch's local services. Because of their weight and need for cooling, servers are placed lower in the rack. Several 2U UPS units are mounted at the bottom of the rack to provide continuous power to all equipment above. This arrangement guarantees dependable power protection and increases rack stability.

Overall, the rack design has a clear structure with network devices at the top, computing resources in the middle, and power equipment at the bottom. This makes the England branch's layout tidy, stable, and simple to manage.

Luxembourg Branch Rack design

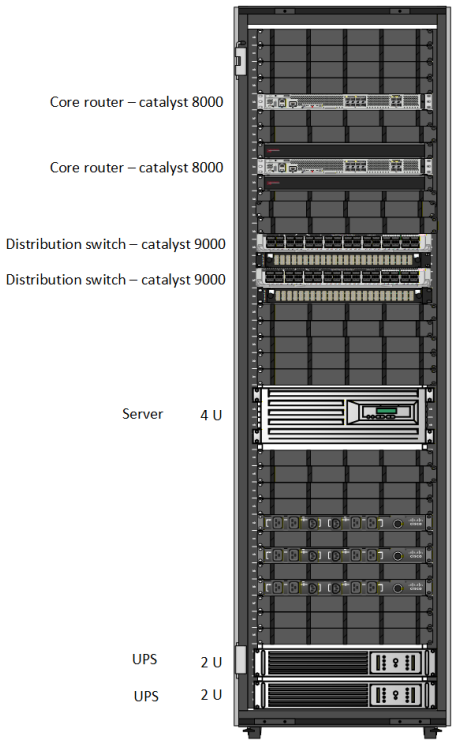

Figure 283 LU Branch Rack design

The Luxembourg (LU) branch is represented by this rack diagram, which adheres to standard rack layout guidelines in line with the network design that has been put into place. The core routers are positioned at the top of the rack to manage WAN and inter-site communication because they are less frequently accessed and require less physical wiring. The distribution switches are positioned beneath them to effectively aggregate network traffic and preserve neat, orderly cabling.

A 4U server is set up in the middle of the rack to supply the Luxembourg branch with local network services. Because of its weight and cooling needs, this server is placed lower in the rack for improved stability and ventilation. Two 2U UPS units are mounted at the base of the rack to provide continuous power to all devices above. Rack stability is enhanced and dependable power protection is guaranteed when the UPS units are positioned at the lowest point. All things considered, the rack design is straightforward, organized, and appropriate for the Global Health Network's Luxembourg location.

China Branch Rack design

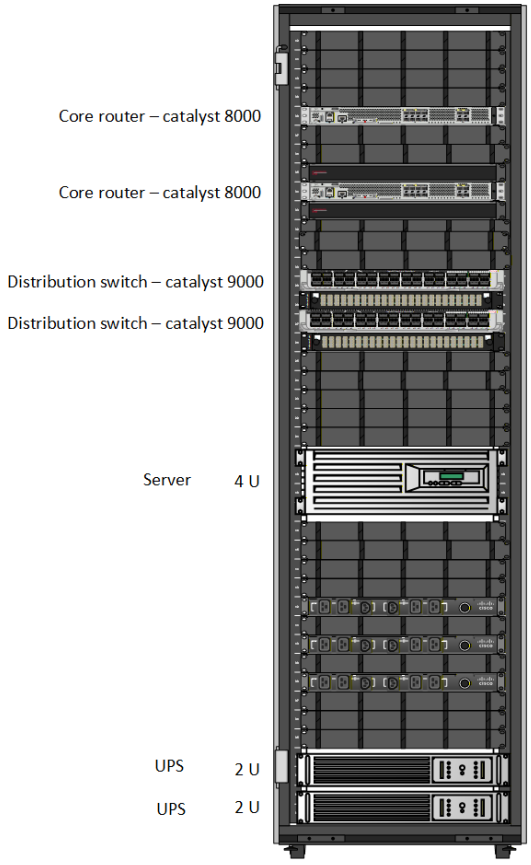

Figure 284 CH Branch Rack design

The above rack diagram, which adheres to established rack-mounting best practices, depicts the Global Health Network's China branch. Two core routers are positioned at the top of the rack to control WAN and inter-site connectivity because these devices are less frequently accessed and require less wiring. The distribution switches are positioned beneath them to effectively aggregate network traffic and keep the wiring in the rack neat.

A 4U server is set up in the middle area to offer local branch services. Because of its weight and cooling needs, the server is positioned lower in the rack to improve stability and airflow. Two 2U UPS units are mounted at the base of the rack to provide continuous power for all equipment above. A clean and useful rack design appropriate for the China branch is produced by placing the UPS units at the lowest level, which guarantees rack stability and dependable power protection.

Layer 2 Design and Features

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

Virtual Local Area Network:

VLANs segment and divide local departments into the network and isolate 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 control 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 summarization 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 routes 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

This section explains how public internet access is provided via the ISP infrastructure and how connection to the internet is included in the Global Health Network. To preserve security, control, and stability, the design isolates customer WAN communication from the ISP's own internet connectivity.

GHN Internet Access Model

The worldwide internet is not directly connected to GHN sites. Each location uses edge routers to connect to the ISP, exchanging routing data via BGP. DMVPN Phase 3 over IPsec is used individually to offer secure inter-site communication.

GHN traffic that is intended for the public internet is routed to the Internet Edge Router of the ISP before leaving for upstream providers. Depending on addressing requirements, the ISP either assigns public IP addresses or performs Network Address Translation (NAT) for GHN traffic.

In addition to lowering exposure and making site design simpler, this centralized internet access paradigm enables uniform security and traffic control throughout all GHN locations.

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 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.
Centralized 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 authorized 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 behavior 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 behavior 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 shut down 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.

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

Deployment Diagram

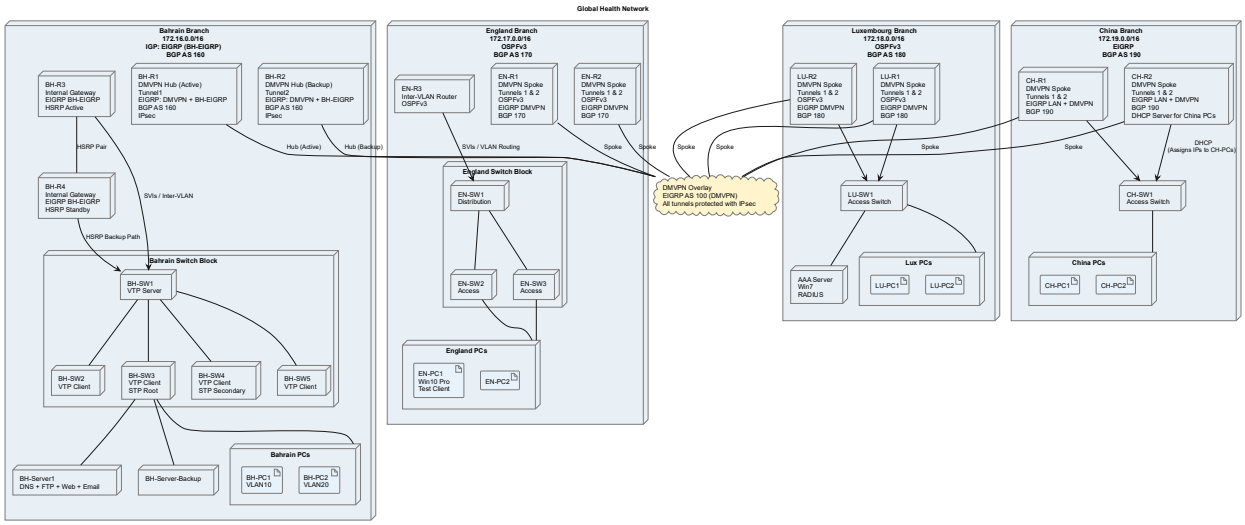

Figure 285 Deployment Diagram

Appendix III: Detailed Implementation

This appendix provides selected configuration outputs to support the implementation of the GHN. It is not practicable to include complete configuration outputs for each device in this document due to the scale and complexity of the deployed multi-site architecture, which includes numerous routers, switches, and server systems.

This appendix contains the full show running-config outputs for two example routers to illustrate implementation consistency and configuration structure. These devices, which include IGP setup, BGP peering, DMVPN, and IPsec configurations, represent the general routing, security, and WAN design used throughout the GHN system.

The remaining servers, switches, and routers complete configuration files are offered individually as digital records and can be accessed via the project **GitHub repository** or in the word object at the end. This method guarantees the thesis's clarity while preserving complete transparency and implementation reproducibility.

BH-R1 Show run

```
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname BH-R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
```

```
!
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
!
!
!
!
!
!
!
!


!
!
!
!
no ip domain lookup
ip domain name GHN.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
```

```
key chain BHEIGRP
 key 16
  key-string 7 05090707334D470739001E15191C
  cryptographic-algorithm hmac-sha-256
!
!
!
!
!
cts logging verbose
!
!
username BH-R1 privilege 15 secret 9
$9$bjVZmxjPNv87pX$l87oDlcxUlTQIPl7Ylzi2g7guAdh6hAfq8v.wSVNLUM
!
redundancy
!
!
ip ssh time-out 90
ip ssh authentication-retries 5
ip ssh version 2
!
!
!
!
!
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key GHNDMVPN address 1.1.17.1
crypto isakmp key GHNDMVPN address 1.1.17.2
```

```
crypto isakmp key GHNDMVPN address 1.1.18.1
crypto isakmp key GHNDMVPN address 1.1.18.2
crypto isakmp key GHNDMVPN address 1.1.19.1
crypto isakmp key GHNDMVPN address 1.1.19.2
!
!
crypto ipsec transform-set DMVPN-SET esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE
 set transform-set DMVPN-SET
!
!
!
!
!
!
!
interface Loopback0
 no shutdown
 ip address 1.1.16.1 255.255.255.255
!
interface Loopback1
 no shutdown
 ip address 1.1.16.100 255.255.255.255
!
interface Tunnel1
 no shutdown
 ip address 100.100.100.1 255.255.255.240
 no ip redirects
 ip nhrp authentication GHNDMVPN
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp redirect
```

```
 tunnel source Serial1/2
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE shared
!
interface Ethernet0/0
 no shutdown
 no ip address
 shutdown
!
interface Ethernet0/1
 no shutdown
 no ip address
 shutdown
!
interface Ethernet0/2
 no shutdown
 no ip address
 shutdown
!
interface Ethernet0/3
 no shutdown
 no ip address
 shutdown
!
interface Serial1/0
 no shutdown
 ip address 172.20.1.1 255.255.255.252
 serial restart-delay 0
!
interface Serial1/1
 no shutdown
 ip address 172.20.1.5 255.255.255.252
 serial restart-delay 0
```

```
!
interface Serial1/2
 no shutdown
 ip address 90.0.0.42 255.255.255.252
 serial restart-delay 0
!
interface Serial1/3
 no shutdown
 no ip address
 shutdown
 serial restart-delay 0
!
!
router eigrp BH-EIGRP
 !
 address-family ipv4 unicast autonomous-system 160
  !
  af-interface default
   authentication mode hmac-sha-256 7 069990BED3D1
   authentication key-chain BHEIGRP
   passive-interface
  exit-af-interface
  !
  af-interface Serial1/0
   no passive-interface
  exit-af-interface
  !
  af-interface Serial1/1
   no passive-interface
  exit-af-interface
  !
  af-interface Serial1/2
   no authentication mode
   no authentication key-chain
```

```
  no passive-interface
 exit-af-interface
 !
 topology base
 exit-af-topology
 network 1.1.16.1 0.0.0.0
 network 90.0.0.48 0.0.0.3
 network 172.20.1.0 0.0.0.3
 network 172.20.1.4 0.0.0.3
 eigrp router-id 1.1.16.1
exit-address-family
!
!
router eigrp DMVPN
 !
 address-family ipv4 unicast autonomous-system 100
  !
  af-interface Tunnel1
   no next-hop-self
   no split-horizon
  exit-af-interface
  !
  topology base
   redistribute static metric 100000 10 255 1 1500
  exit-af-topology
  network 1.1.16.100 0.0.0.0
  network 100.100.100.0 0.0.0.15
  eigrp router-id 1.1.16.100
 exit-address-family
!
router bgp 160
 bgp router-id 1.1.16.1
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
```

```
 neighbor 90.0.0.41 remote-as 1000
 !
 address-family ipv4
  network 1.1.16.1 mask 255.255.255.255
  neighbor 90.0.0.41 activate
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 172.16.0.0 255.255.0.0 Null0
!
!
!
!
control-plane
!
!
!
!
!
!
!
banner motd ————————————————C
**********************************************************************
*                                                                    *
*  SECURITY WARNING: GlobalB HealthB Network (GHN) ROUTER            *
*                                                                    *
*  NOTICE: This Router is restricted to authorized personnel only.   *
*  Unauthorized access is strictly prohibited and may lead to        *
*  disciplinary action or legal prosecution.                         *
*                                                                    *
```

```
*  This device is monitored to ensure network security and           *
*  compliance with PSS policies. All activity is logged in real-time. *
*                                                                    *
*  If you are not authorized, disconnect immediately.               *
*                                                                    *
**********************************************************************
```

```
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 5 0
 login local
line vty 0 4
 exec-timeout 7 0
 privilege level 15
 login local
 transport input ssh
!
!
End
```

BH-R2 Show Run

```
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname BH-R2
!
boot-start-marker
```

```
boot-end-marker
!
!
!
no aaa new-model
!
!
!
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
!
!
!
!
!
!
!
!


!
!
!
!
no ip domain lookup
ip domain name GHN.com
```

```
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
key chain BHEIGRP
 key 16
  key-string 7 070D20445C08100B3717020B163A
  cryptographic-algorithm hmac-sha-256
!
!
!
!
!
cts logging verbose
!
!
username BH-R2 privilege 15 secret 9
$9$MpBZY48rQQXC6H$wxnu8thehoAExLSqBvYO9QMbULfjksKXI1J4kRZXJ6E
!
redundancy
!
!
ip ssh time-out 90
ip ssh authentication-retries 5
ip ssh version 2
!
!
!
!
!
crypto isakmp policy 10
```

```
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key GHNDMVPN address 1.1.17.1
crypto isakmp key GHNDMVPN address 1.1.17.2
crypto isakmp key GHNDMVPN address 1.1.18.1
crypto isakmp key GHNDMVPN address 1.1.18.2
crypto isakmp key GHNDMVPN address 1.1.19.1
crypto isakmp key GHNDMVPN address 1.1.19.2
!
!
crypto ipsec transform-set DMVPN-SET esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE
 set transform-set DMVPN-SET
!
!
!
!
!
!
!
interface Loopback0
 no shutdown
 ip address 1.1.16.2 255.255.255.255
!
interface Loopback1
 no shutdown
 ip address 1.1.16.200 255.255.255.255
!
interface Tunnel2
```

```
 no shutdown
 ip address 100.100.200.1 255.255.255.240
 no ip redirects
 ip nhrp authentication GHNDMVPN
 ip nhrp map multicast dynamic
 ip nhrp network-id 2
 ip nhrp redirect
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 200
 tunnel protection ipsec profile DMVPN-PROFILE shared
!
interface Ethernet0/0
 no shutdown
 no ip address
 shutdown
!
interface Ethernet0/1
 no shutdown
 no ip address
 shutdown
!
interface Ethernet0/2
 no shutdown
 no ip address
 shutdown
!
interface Ethernet0/3
 no shutdown
 no ip address
 shutdown
!
interface Serial1/0
 no shutdown
```

```
 ip address 172.20.1.2 255.255.255.252
 serial restart-delay 0
!
interface Serial1/1
 no shutdown
 ip address 172.20.1.9 255.255.255.252
 serial restart-delay 0
!
interface Serial1/2
 no shutdown
 ip address 90.0.0.18 255.255.255.252
 serial restart-delay 0
!
interface Serial1/3
 no shutdown
 no ip address
 shutdown
 serial restart-delay 0
!
!
router eigrp BH-EIGRP
 !
 address-family ipv4 unicast autonomous-system 160
  !
  af-interface default
   authentication mode hmac-sha-256 7 009B8C999BC4
   authentication key-chain BHEIGRP
   passive-interface
  exit-af-interface
  !
  af-interface Serial1/0
   no passive-interface
  exit-af-interface
  !
```

```
  af-interface Serial1/1
   no passive-interface
  exit-af-interface
  !
  af-interface Serial1/2
   no authentication mode
   no authentication key-chain
   no passive-interface
  exit-af-interface
  !
  topology base
  exit-af-topology
  network 1.1.16.2 0.0.0.0
  network 90.0.0.44 0.0.0.3
  network 172.20.1.0 0.0.0.3
  network 172.20.1.8 0.0.0.3
  eigrp router-id 1.1.16.2
 exit-address-family
!
!
router eigrp DMVPN
 !
 address-family ipv4 unicast autonomous-system 100
  !
  af-interface Tunnel2
   no next-hop-self
   no split-horizon
  exit-af-interface
  !
  topology base
   redistribute static metric 100000 10 255 1 1500
  exit-af-topology
  network 1.1.16.200 0.0.0.0
  network 100.100.200.0 0.0.0.15
```

```
  eigrp router-id 1.1.16.200
 exit-address-family
!
router bgp 160
 bgp router-id 1.1.16.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 90.0.0.17 remote-as 1000
 !
 address-family ipv4
  network 1.1.16.2 mask 255.255.255.255
  neighbor 90.0.0.17 activate
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 172.16.0.0 255.255.0.0 Null0
!
!
!
!
control-plane
!
!
!
!
!
!
!
banner motd ————————————————C
**********************************************************************
```

```
*                                                                *
*  SECURITY WARNING: GlobalB HealthB Network (GHN) ROUTER        *
*                                                                *
*  NOTICE: This Router is restricted to authorized personnel only.    *
*  Unauthorized access is strictly prohibited and may lead to        *
*  disciplinary action or legal prosecution.                         *
*                                                                *
*  This device is monitored to ensure network security and           *
*  compliance with PSS policies. All activity is logged in real-time. *
*                                                                *
*  If you are not authorized, disconnect immediately.               *
*                                                                *
******************************************************************
```

```
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 5 0
 login local
line vty 0 4
 exec-timeout 7 0
 privilege level 15
 login local
 transport input ssh
!
!
end
```

For the Rest of the Show run click on the Word object icon.

Show Run