Tautvydas Juodikis

PROJECT FOR USING CISCO DMVPN

Enabling the chance to use a proper VPN module

Bachelor's thesis

Bachelor of

Engineering

Information Technology

2025

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor or Engineering
Author	Tautvydas Juodikis
Thesis title	Project for using Cisco enabling the chance to use a proper VPN module
Year	2025
Pages	**40**
Supervisor	Matti Juutilainen

ABSTRACT

Organizations operating across multiple locations require secure, efficient, and scalable communication over public networks. With the increasing adoption of remote work and cloud-based services, reliance on VPNs has grown substantially. However, many companies still rely on outdated protocols such as PPTP and frequently fail to implement essential security measures, including the replacement of default device credentials. These shortcomings continue to expose networks to growing cybersecurity threats and the potential for data loss.

The primary objective of this thesis was to implement a secure Dynamic Multipoint Virtual Private Network (DMVPN) solution using Cisco technologies. The implementation focused on deploying DMVPN with the support of GNS3 for network simulation and Zabbix for real-time performance monitoring. These tools enabled the design, validation, and observation of a scalable VPN framework within a virtualized environment, prior to physical deployment.

The study included an analysis of various VPN protocols, assessing their advantages and limitations in terms of security, performance, and scalability. DMVPN was selected for its ability to dynamically establish encrypted tunnels while minimizing manual configuration complexity. The study also addressed hardware compatibility concerns and highlighted the suitability of Cisco routers due to their native support for core technologies such as IPsec, multipoint GRE (mGRE), and Next Hop Resolution Protocol (NHRP).

The key outcome was a fully operational DMVPN simulation that demonstrated secure and scalable site-to-site communication. The results demonstrate the significance of proper VPN configuration and the use of modern protocols in ensuring network resilience. This thesis offers practical guidance for organizations seeking to strengthen their network infrastructure through adaptable and secure VPN technologies.

Keywords: DMVPN, GNS3 CISCO, PPTP, SSH, VPN, Ethernet

CONTENTS

1 INTRODUCTION

Many organisations and institutions are not centralised. In the contemporary world, many businesses often occupy multiple office spaces and spread their operations nationally and, in some cases, abroad. Many companies are spread across different geographical locations, and the issue of physical distance often requires them to implement their own VPN for security purposes. Although many companies do not take all the necessary security measures when configuring VPNs, they still rely on them. Administrations, for example, sometimes fail to change the default passwords of equipment that they receive. Recently, due to the rising percentage of cybersecurity crime that large companies face, the need to innovate has risen exponentially. The use of outdated and insecure VPN protocols, such as PPTP, is expected to decline as organizations increasingly prioritize network security. Without a good VPN, companies always run the risk of losing critical documents, such as sensitive business records and customer data, if someone breaks in and takes advantage of a faulty system. Companies are also faced with the challenge of keeping up with modern business needs such as mobility and cloud computing. The basic purpose of a private network VPN is to provide protection within an open communications network infrastructure. VPNs aim to ensure that sensitive information transmitted over a network, such as a local area network (LAN) or a work environment, remains confidential and only accessible to authorised users. A VPN system integrated into a communication system can provide a high level of security, guaranteeing a secure connection implemented through encryption and decryption. (Riadi, 2019).

1.1 RESEARCH OBJECTIVE

This thesis will use various methods and materials. The main challenge is the disparaging and often conflicting information among manufacturers about implementations and the capabilities of their equipment. For this reason, the study will primarily focus on the popular and commonly available Cisco ecosystem. Cisco was selected not only for its industry dominance but also because its equipment supports the core technologies necessary for this study,

such as IPsec encryption, mGRE (multipoint GRE), and NHRP (Next Hop Resolution Protocol).

Technical requirements and market research will be leveraged in this study to implement a relevant and viable solution. Another key method in this study will be a documentation analysis which involves obtaining information from various resources.

1.2 RISK ASSESSMENT

The primary challenge in all network analysis lies in the fact that general guidelines are limited and often require evaluation on a case-by-case basis. Varying business needs may require non-standard secure approaches which the DMVPN protocol may not be capable of addressing. Not all hardware or software environments will respond identically to the planned DMVPN configurations, as compatibility issues may arise depending on the router model and firmware version. The selection of routers is also limited, as not all models support the features required for the implementation examined in this study.

2 THEORETICAL FRAMEWORK

The theoretical framework provides the necessary context for understanding the rationale behind choosing DMVPN as the preferred solution. By analysing different VPN models and how they compare in terms of security, scalability, and performance, the limitations and strengths of each approach can be more clearly understood in real-world environments. Before fully delving into DMVPN, existing VPN modules are compared, and their advantages and disadvantages are introduced.

2.1 What is a VPN

A VPN is a private network created within the public infrastructure (Figure 1), such as the Internet (Ferguson et al., 1998). The definition reveals a critical flaw – although the network appears private, it is still public and accessible to anyone interested in private data. Therefore, as the number of users grows, it is important to maintain appropriate security measures and techniques. Most modern systems rely on the tunnel method, as illustrated in Figure 1, with L2TP and PPTP being the most common tunnel protocols.

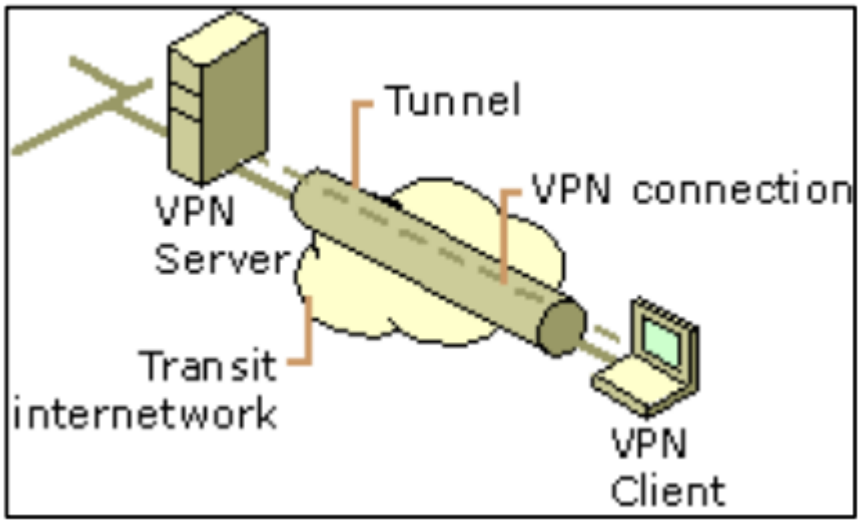

Figure 1. VPN example, (Microsoft, 2009)

In order to simulate PTP, data is wrapped in a header which provides routing information, allowing the encapsulated data to traverse a shared or public transport network to reach its destination. On the other hand, to simulate a private network, the data being sent is encrypted for confidentiality. Packets intercepted on a shared or public network are indecipherable without the encryption keys. The part of the connection which contains private data is known as the tunnel. There are two primary types of VPNs relevant for this study: remote access VPNs and site-to-site VPNs. Remote access VPNs allow individual users to connect securely to a corporate network from a remote location, whereas site-to-site VPNs connect entire networks, often between branches of a company, allowing communication as if the networks were

physically connected. DMVPN falls under the latter category and is, therefore, explored in this thesis. (Microsoft, 2009).

2.2 VPN protocols

2.2.1 OpenVPN

OpenVPN is an open-source VPN protocol belonging to the OpenVPN organization and was in 2001 (Yonan, 2002). The protocol is known for its robust security toolset and flexibility. OpenVPN is widely used in secure remote connections and encrypted IoT. OpenSSL is included within OpenVPN and provides extra security. The main advantages of OpenVPN comprise modern encryption methods, which offer protection from most censorship techniques such as firewalls and deep packet inspection, as well as transparency, flexibility, and free unlimited usage owing to its open-source nature (VeePN, 2023). Because it is open-source, developers and system administrators can review and customize the codebase to suit specific use cases. This allows for faster identification and patching of security vulnerabilities compared to many proprietary VPN solutions.

The main disadvantages are slow connection speed due to the codebase size (a common open-source development problem) and fairly complex configuration and usage.

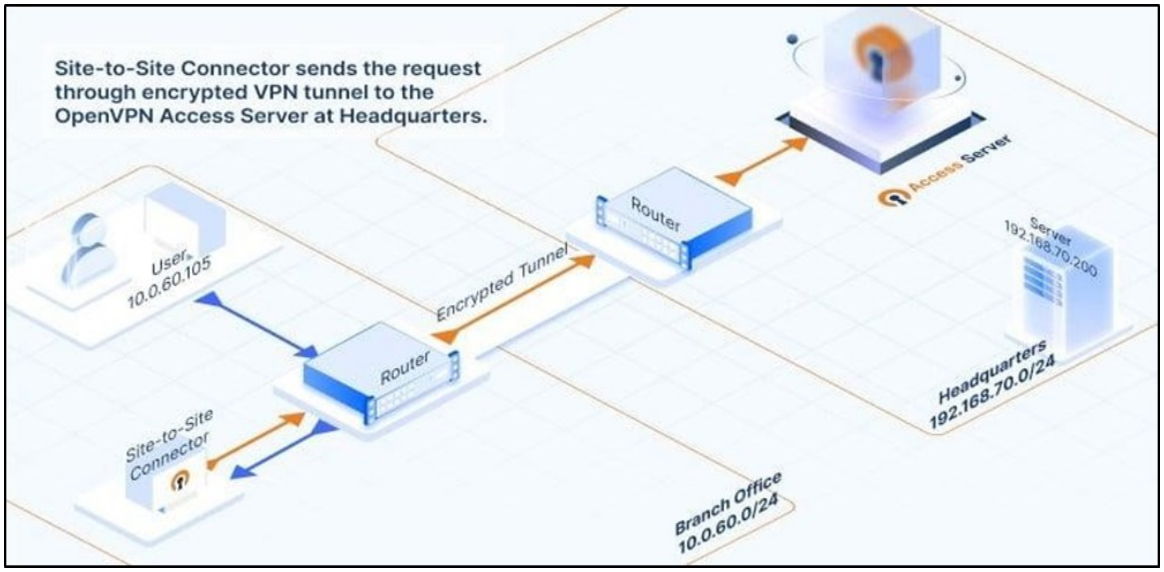

Figure 2. OpenVPN working principle (OpenVPN, 2024)

Despite its complexity, OpenVPN remains a preferred option for users who prioritize privacy. It is particularly suitable in scenarios where security is more important than speed.

2.2.2 WireGuard

WireGuard is a modern open-source VPN protocol created in 2015 by Jason A. Donenfeld (Grauer, 2021). It uses cutting-edge cryptography and network code to create an encrypted tunnel between two devices based on their public keys. This allows for fast and secure communication, even when the client device's IP address changes. One of WireGuard's most significant innovations is its minimalistic codebase which contains approximately 4,000 lines of code compared to hundreds of thousands in traditional VPN protocols such as OpenVPN or IPsec. It is important to mention that the NordVPN NordLynx protocol is based on a modified version of WireGuard. Unlike OpenVPN, WireGuard offers a much smaller codebase, and thus, is significantly faster (Wherry, 2023). WireGuard is also known for its easy configuration. However, one of the main drawbacks is that the VPN is not a standalone program and requires numerous additional tools to function properly, particularly on Windows. Additionally, WireGuard lacks built-in obfuscation support which is necessary to bypass deep packet inspection in certain regions.

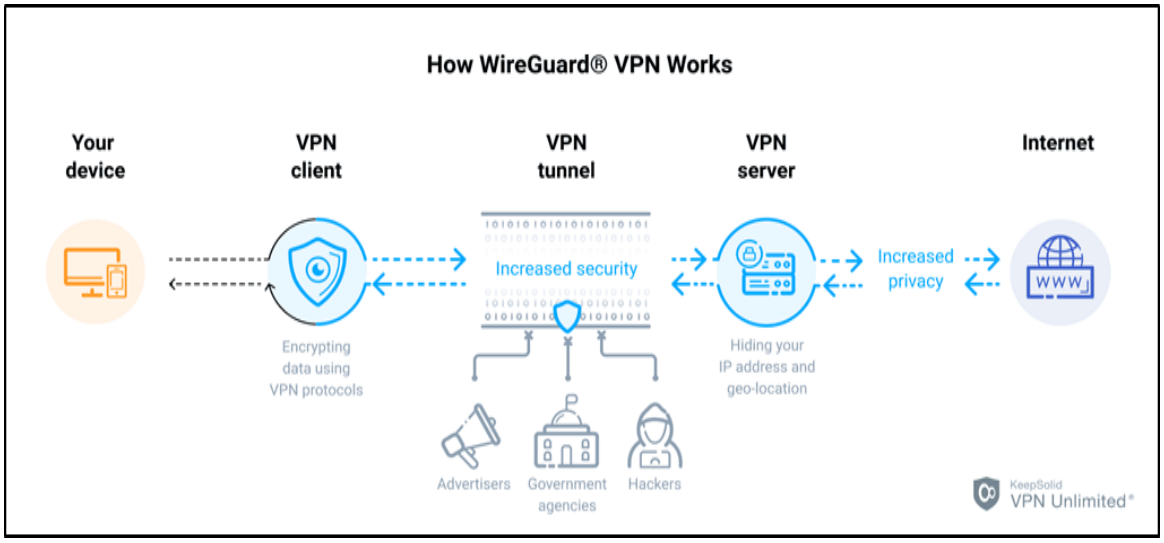

Figure 3. WireGuard working principle (VPN unlimited)

WireGuard is a secure VPN protocol designed with contemporary cryptographic standards. It uses modern, well-tested cryptography, and its code is simplified, thus having fewer bugs and misconfigurations. However, it is important to note that WireGuard's security still largely depends on how well it has been implemented.

2.2.3 L2TP/IPsec

L2TP/IPsec is a combination of two protocols: Layer 2 Tunnelling Protocol (L2TP) and Internet Protocol Security (IPsec). L2TP is a tunnelling protocol that does not use any encryption method by nature, so it is often embedded with IPsec to provide additional security. IPsec is a set of protocols that provide authentication and encryption of data transmitted over public networks, ensuring data privacy and security (Holm, 2017; WireX, 2023; Zenarmor, 2024). Despite its strengths, L2TP/IPsec has seen declining usage in recent years, largely due to the rise of faster and more flexible protocols such as WireGuard and OpenVPN. It is still widely recognized for its strong security and ease of setup. It is supported by most modern devices and platforms, and it supports multi-threading to improve performance. It also provides protection against man-in-the-middle attacks and supports AES-256 encryption algorithms which are considered among the most secure. (Maximilian Holm, 2017). On the downside, L2TP/IPsec can only communicate over UDP, making it easy to block. It can be slower than OpenVPN due to its double encapsulation. There are concerns that IPsec could be intentionally weakened by the NSA or compromised by the NSA (Holm, 2017). Additionally, proper installation and configuration are vital to maintaining a secure L2TP/IPsec VPN.

2.2.4 PPTP

PPTP is one of the oldest VPN protocols. It was developed in 1999 by Microsoft Corporation (Globytė, 2023).

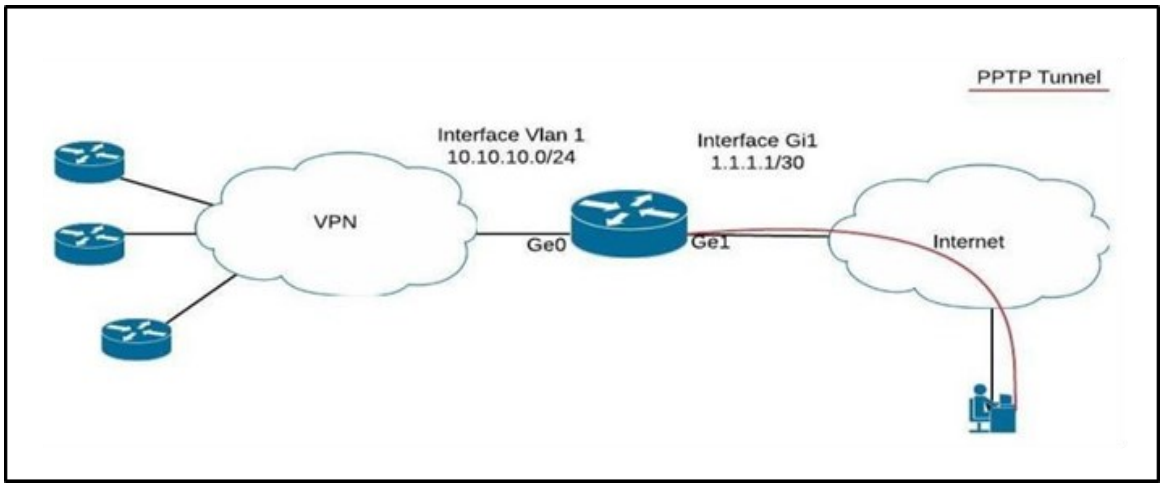

Figure 4. PPTP working principle (Buenning, 2004)

PPTP has a mixed reputation, with many pros and cons. It offers several practical benefits and is known for its ease of use and accessibility, even for users with minimal technical knowledge. Due to its long history, PPTP enjoys broad compatibility across all major operating systems. (Savickaitė, 2022). Additionally, owing to its simple structure, PPTP typically offers faster speeds than more modern VPN protocols.

However, PPTP also comes with significant drawbacks. It is no longer considered secure due to outdated encryption algorithms, inadequate security measures, and vulnerabilities in authentication methods such as MS-CHAP (Ema Globytė, 2023). The protocol's short encryption keys make it susceptible to brute-force attacks, and the lack of strong authentication mechanisms leaves it open to exploitation (VeePN, 2023). Furthermore, PPTP can face connectivity issues caused by firewall restrictions, as it does not rely on standardized VPN port numbers, which may lead to blocked connections (Globytė, 2023).

In today’s cybersecurity environment, PPTP is a rarity due to its high-security risks. Nevertheless, PPTP is still used in certain niche applications where speed is more important than security.

2.2.5 DMVPN

DMVPN stands for Dynamic Multipoint Virtual Private Network, and it is a VPN protocol that Cisco first introduced in the late 2000s to enhance network connectivity and security (Francis, 2021). This protocol is characterized by its hub-and-spoke topology which serves as the foundation for its operation (Parmenter, 2021). Unlike traditional VPN configurations, DMVPN offers a more flexible and dynamic approach to establishing virtual private network connections. It enables the seamless interconnection of multiple spoke sites while allowing for the automatic creation of secure tunnels between them based on traffic demand. This eliminates the necessity for continuous manual configuration at both the hub and spoke locations, making network management more efficient and scalable. The phases for the design of the protocol are introduced below.

Phase 1. This phase uses the Next Hop Resolution Protocol (NHRP) to allow branch routers to register with the hub. The hub is the only router that uses a Generic Routing Encapsulation (GRE) multipoint interface. All branch routers use standard point-to-point GRE tunnel interfaces. As a result of this configuration, direct communication between branch routers is not possible. All traffic is routed through a central node, which acts as the core communication point in the network (Network Lessons, 2024).

Phase 2 is designed to overcome some of the limitations found in Phase 1 by enabling direct communication between spoke routers. Unlike in Phase 1, where all traffic had to pass through the central hub, Phase 2 allows spoke routers to establish direct connections with one another when needed. In order to achieve this, all spoke routers utilize Generic Routing Encapsulation (GRE) multipoint tunnels, which make it possible for them to communicate without relying entirely on the hub as an intermediary. This improvement enhances network efficiency by reducing unnecessary traffic through the hub and optimizing data transfer between spokes (NetworkLessons, 2024).

Phase 3 is founded on the principles of Phase 1 and Phase 2 by introducing a hierarchical topology. This phase retains the advantages of the previous phases while providing a more scalable solution, making it well-suited for larger network deployments. This means that companies can scale up their networks with ease. One of its key features is the ability to create full-mesh Generic Routing Encapsulation (GRE) or IPsec tunnels in a dynamic manner, reducing reliance on the hub while still maintaining centralized control. Additionally, Phase 3 simplifies network configuration by allowing the use of a standardized template, making it easier to manage large-scale VPNs with dynamic routing capabilities (NetworkLessons, 2024).

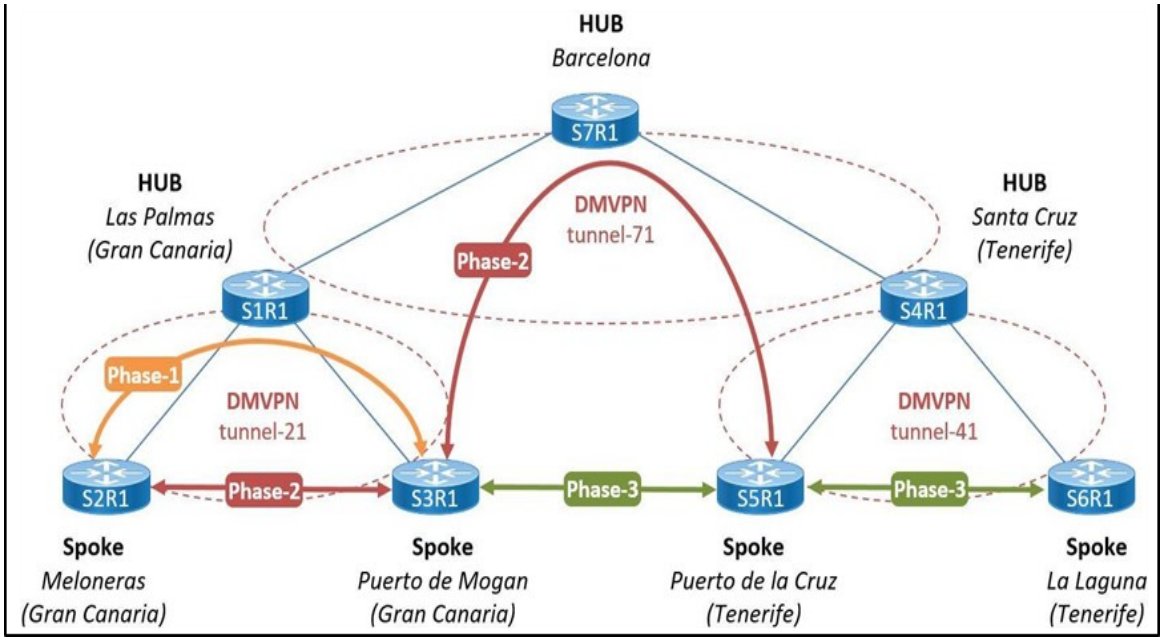

Figure 5. DMVPN and all its phases illustrated (Nir Ben-Dvora, 2016)

The benefits of DMVPN are numerous. First of all, the simplified configuration makes it easier to set up and manage the hub router by using a single multipoint GRE (mGRE) interface and an IPsec profile. This allows the hub to handle all spoke routers regardless of how many spokes are connected.

Secondly, instead of routing all traffic through the hub, spoke routers can establish dynamic spoke-to-spoke tunnels when necessary. This reduces network congestion, administrative overhead, and improves overall flexibility.

Finally, DMVPN enhances security by supporting optional IPsec encryption, ensuring that data transmitted through VPN tunnels remains confidential and protected from unauthorized access. This strengthens the security and integrity of network communications (firewall, 2024).

2.3 VPN monitoring software

Based on the VPN analysis, DMVPN seems to be the best choice for ensuring a safe and stable VPN connection with no static device configuration. Therefore, to install and configure DMVPN. The required software includes PuTTY for remote connections and Zabbix, Nagios, or Grafana for network monitoring.

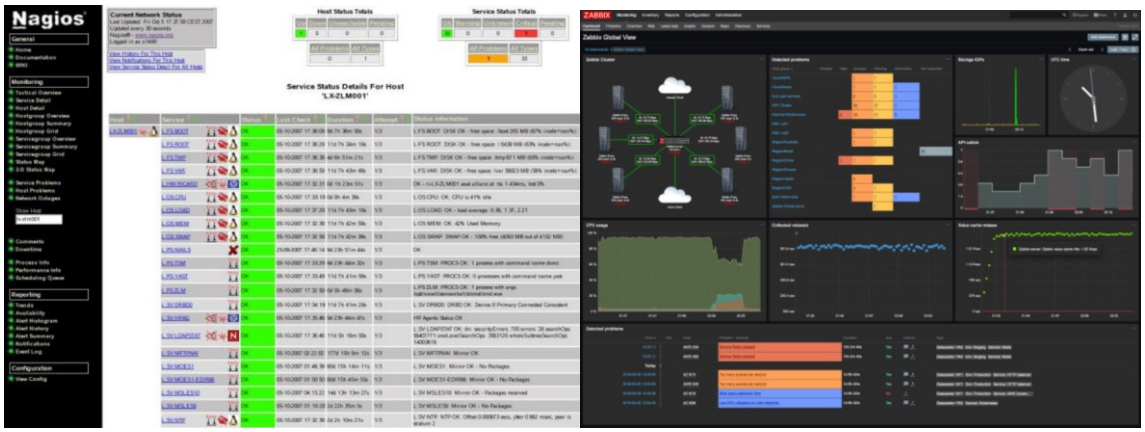

Figure 6. VPN monitoring software (Nagios - left, Zabbix - right)

Figure 7. VPN monitoring software Grafana

Program comparisons are presented in Table 1. Zabbix was chosen due to the simplicity of the interface and ease of use. Also, the GNS3 network simulator will be used to test out the network before full implementation.

Program	Price	Security	DMVPN Compatibility	User Experience
Zabbix	Free (Commercial support option available)	Offers secure data collection and monitoring capabilities	Although DMVPN compatibility is not a direct feature of these tools, they can be configured for DMVPN connectivity.	Known for its user-friendly interface and ease of use
Nagios	Basic version free	Ensures reliable security measures		The interface is comprehensive, but there is a steep learning curve.
Grafana	Open-source program. Paid version has more features	more focused on visualization rather than security features, but can be integrated with security tools to increase protection		Offers a balance between comfort and functionality

Table 1. VPN monitoring software comparison

3 IMPLEMENTATION

In this section, the implementation process of the proposed DMVPN solution is described. The key objective is to validate the feasibility of DMVPN in a simulated setup that closely mirrors a real-world scenario.

3.1 Hardware

Implementation was carried out using the Cisco 4221 router. It was chosen due to its global command set which is well documented and widely used.

Figure 8. CISCO 4221 router

The main features of the router are presented below.

Versatility: CISCO 4221 can support a variety of network tools in a single device, such as wireless WAN, wireless LAN, and integrated switch ports.

Performance: The bandwidth of the Cisco 4221 starts at 35 Mbps and can be upgraded to 75 Mbps, providing sufficient bandwidth for many small and medium-sized businesses.

Security: The router has built-in security features such as a firewall, VPN acceleration, and network contention management, providing robust protection for branch networks and users.

Scalability: The Cisco 4221 supports bandwidth and network interface module upgrades, allowing for future expansion as business needs change. This scalability ensures that the router can grow with the business, making it a long-term solution for small and medium-sized businesses.

Affordability: The Cisco 4221 offered a competitive price-performance ratio, making it an attractive choice for small and medium-sized businesses.

Based on these features, the Cisco 4221 router was deemed the most suitable choice for this study. In addition, a fibre optic SFP module was used to support high-speed and long-range data transmission. A single-mode fibre optic cable was selected due to its small core diameter, which enables greater transmission distances. When combined with Ubiquiti Networks hardware, the setup allowed signal transmission over distances of up to 10 kilometres.

3.2 Software

GNS3 is a widely used open-source simulation tool in network engineering. The software is an open-source platform designed for simulating both network hardware and software components. Its simulation capabilities were used to design the DMVPN topology without requiring physical hardware, which helped economize both time and resources. GNS3 was used to simulate the necessary routers and switches, configure tunnelling and security protocols, and test their behaviour in a controlled environment. GNS3 supports Cisco software and hardware which is essential in the framework of this study.

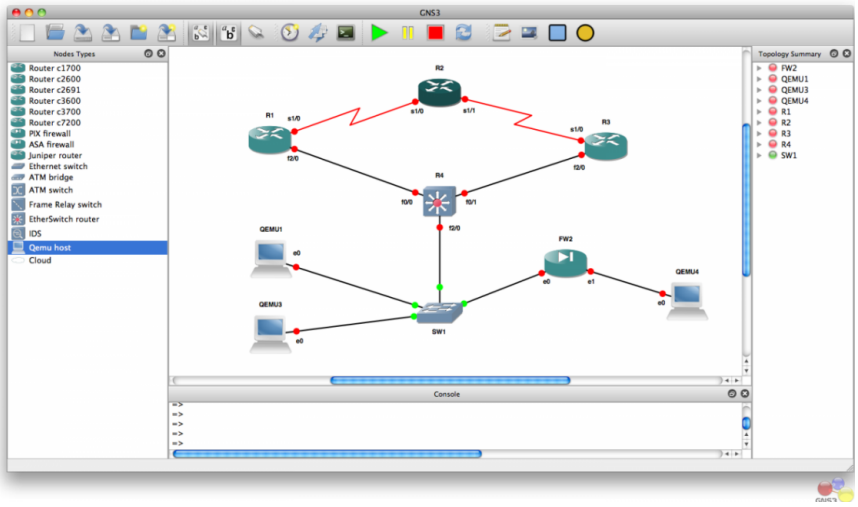

Figure 9. GNS3 network simulator

PuTTY is a free-of-charge open-source terminal emulator, serial console and remote file transfer software. In this study, it was primarily used to establish remote PC and server connections through the Secure Shell (SSH) protocol (Nir Ben-Dvora) which provided the required encryption and security (Loshin, 2021).

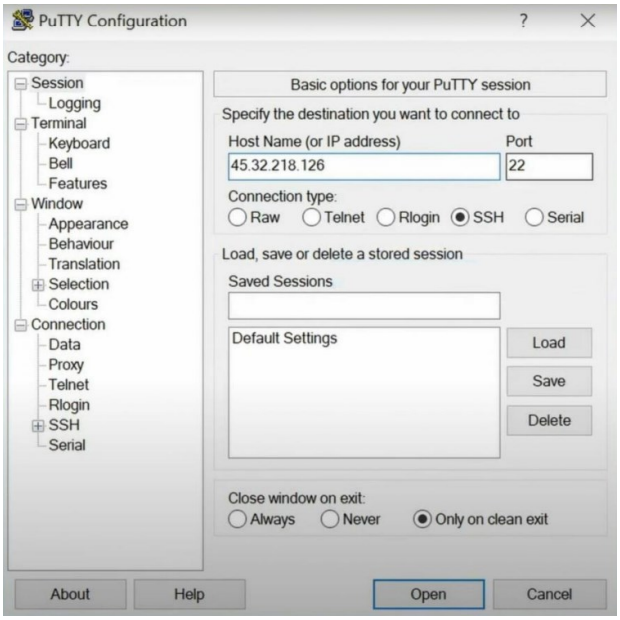

Figure 10. PuTTY virtual terminal tool

3.3 Implementation overview Summary

The DMVPN implementation was designed to create a more secure data environment, improve data transfer performance over long distances, and enhance network reliability. PuTTY was used as an SSH client to establish secure connections and configure DMVPN devices, while Zabbix was employed for monitoring network activity and identifying potential issues. IPsec encryption was applied to ensure secure communication across the network. GNS3 served as the primary network emulation tool, enabling pre-deployment testing of the DMVPN configuration. This allowed validation of the setup prior to physical implementation and helped minimize the risk of misconfiguration or deployment failure.

4 PROJECT REALIZATION

The following section introduces the software tools used in this study and describes how they were integrated into the implementation process.

4.1 Software

The foundation of this study is the implementation of a Dynamic Multipoint Virtual

Private Network (DMVPN). The subsystem includes software tools used to implement, configure, and monitor the DMVPN environment. The primary components of the information subsystem are as follows:

Zabbix:enables efficient monitoring of network traffic to help minimize disruptions and performance bottlenecks.

PuTTY:to act as the primary tool for configuring and managing router settings.

4.1.1 Information flow

The information flow inside the network is described in Figure 11.

A request was initiated from one endpoint to another located in a different department. The corresponding data packet was forwarded to the local router. An NHRP Resolution Request message was generated and sent to the DMVPN hub. In this case, the communication occurred between two DMVPN spokes. The DMVPN hub identified the mapping between the tunnel IP address and the NBMA (Next Hop Resolution Protocol) address of the destination spoke. Upon receiving this information, a dynamic IPsec tunnel was established between the two spokes. The encrypted tunnel then securely transmitted the packet to the receiving router, where it was routed to its intended destination. The same process was repeated to facilitate the return communication from the destination endpoint.

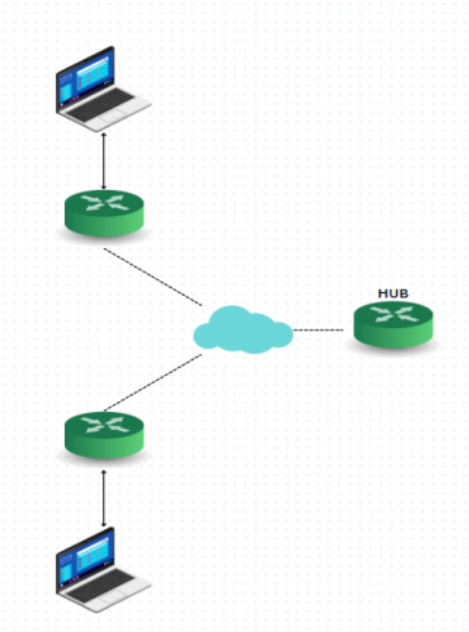

Figure 11. Information Flow

4.1.2 User Interface

Zabbix includes a built-in user interface that meets usability and functionality requirements; therefore, it was selected for use in this study.

Figure 12. Zabbix user interface

Zabbix provides a web-based interface that is accessible through valid login credentials and a direct network connection. A detailed description of the interface is beyond the scope of this thesis; therefore, readers are referred to the official Zabbix documentation for further information.

4.2 GNS3 Network Simulation

GNS3 software server will be used to speed up and facilitate the implementation of a real DMVPN network.

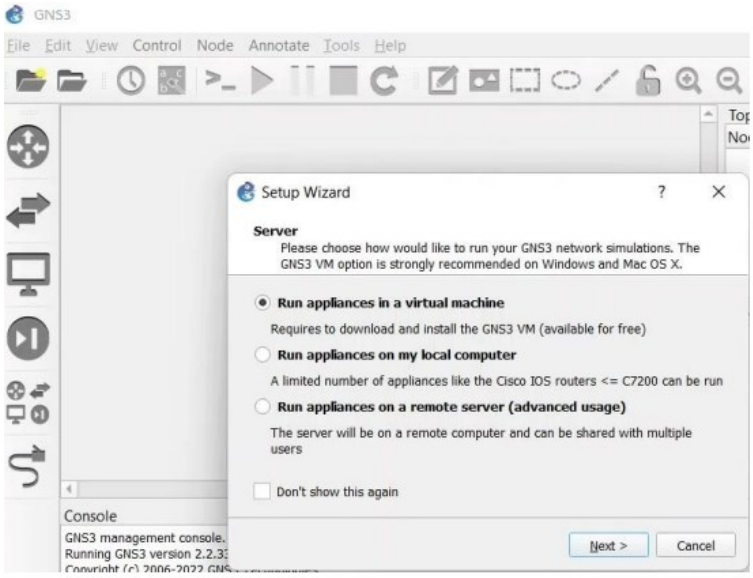

Figure 13. GNS3 setup screen

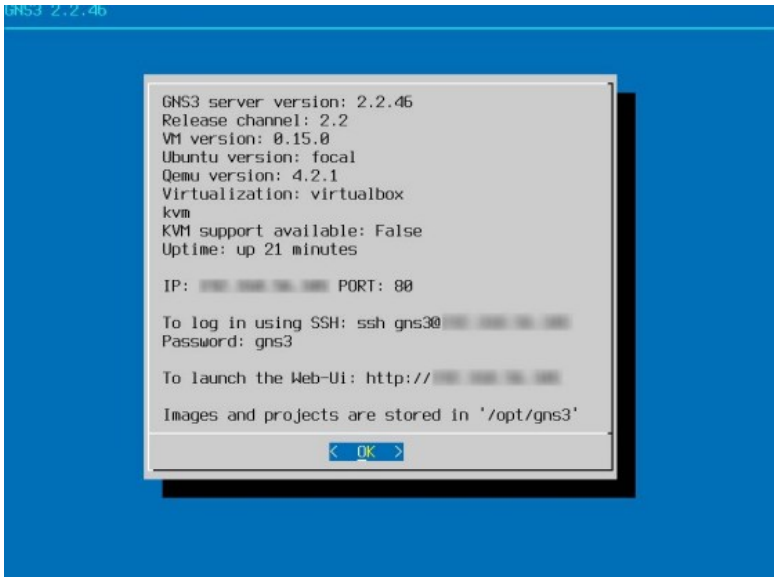

Figure 14. GNS3 information screen

After downloading the necessary software, a virtual machine setup was selected due to the lack of access to a remote server at the time of deployment. The local machine was not suitable for DMVPN testing, as it lacked the required tools and processing capacity. Remote server access was made available later, allowing the deployment to proceed in a more stable environment. The next step involved the creation of the network topology. Due to hardware availability constraints, only a limited set of Cisco device models could be used.

The following hardware was selected:

- 3 Cisco7200 routers (should be 4221 but there were none close to it) (R1-3)
- 3rd layer router Cisco3660 (DMVPN) (HUB)

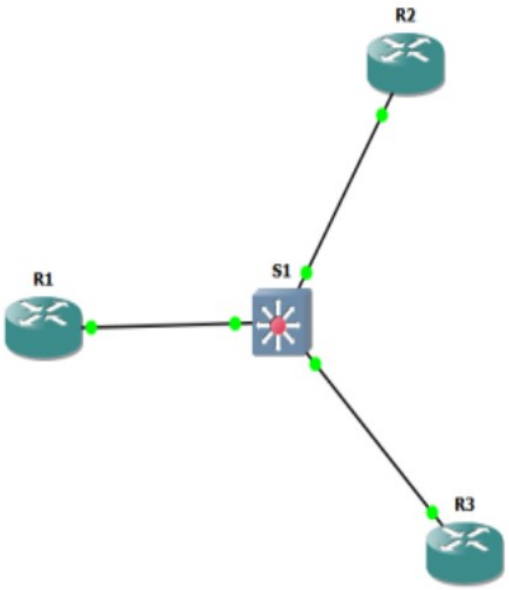

Figure 15. Starting topology

4.2.1 DMVPN phase 1

An initial setup is needed to turn this topology into a DMVPN network, which follows a hub-and-spoke architecture where all spoke-to-spoke traffic must pass through the hub.

R1 router configuration:

The configuration of a Cisco router is shown in Figure 24: Appendix1, specifically in the context of a Dynamic Multipoint Virtual Private Network (DMVPN) Hub. The configuration includes several key elements:

Basic Router Setup:
- The router is named R1.
- Domain lookup is disabled to prevent unnecessary DNS queries.
- A message-of-the-day (MOTD) banner is configured.
- Console and VTY line settings include exec-timeout, synchronous logging, and user authentication with privilege level 15.

Physical Interface Configuration:
- GigabitEthernet 0/1 is assigned the IP address 192.0.2.1/30, which is likely used as a WAN interface.

DMVPN Tunnel Configuration:

- Tunnel 1 is created in multipoint mode, allowing multiple remote spokes to connect.
- The tunnel source is set to GigabitEthernet 0/1.
- Tunnel IP address: 100.100.1.1/29.
- NHRP (Next Hop Resolution Protocol) is enabled with authentication and dynamic mapping, which allows spokes to register dynamically with the hub.
- The bandwidth is set to 4000 kbps, ensuring proper bandwidth allocation for DMVPN traffic.

Figure 25 appendix 1 shows additional configuration for DMVPN (Dynamic Multipoint Virtual Private Network), specifically focusing on EIGRP (Enhanced Interior Gateway Routing Protocol) routing over the DMVPN tunnel. The following section outlines the current process:

- MTU and TCP Adjustments:
  - MTU is set to 1400, ensuring proper packet fragmentation for DMVPN.
  - THE TCP MSS (Maximum Segment Size) is adjusted to 1360, which prevents packet fragmentation issues over the tunnel.
- EIGRP Routing Configuration for DMVPN:
  - The router is running two EIGRP processes, each for different networks:
    - DMVPN_TUNNEL_NET (AS 68) for routing within the DMVPN tunnel.
    - DMVPN_TRANS_NET (AS 168) for the transit network.
  - DMVPN_TUNNEL_NET (AS 68) Configuration:
    - Router ID: 1.1.1.1
    - Network 100.100.100.0/29, which corresponds to the tunnel interface.
    - No split-horizon on Tunnel 1, allowing routing updates to be sent between spokes.
  - DMVPN_TRANS_NET (AS 168) Configuration:
    - Router ID: 10.1.1.1
    - Network 192.0.2.0/30, likely part of the physical network for communication between DMVPN hubs and spokes.

R2 router configuration:

(Figure 25-27 appendix) shows the configuration process of the DMVPN spoke router R2. This router is set up to connect to a DMVPN hub (likely R1).
This section provides a detailed breakdown:

- Basic Router Setup:
    - The router's hostname is set to R2.
    - Domain lookup is disabled to prevent delays when mistyping commands.
    - A banner message is configured:
      "R2, Implement DMVPN Spoke 1"
      This indicates that R2 is a spoke in a DMVPN topology.
- Console and VTY Line Configuration:
    - Exec-timeout is set to 0 0, preventing automatic logouts.
    - Logging synchronously ensures that system messages do not interrupt command input.
    - Privilege level 15 grants full administrative access.
    - A password ("cisco123") is configured for security.

Cisco router designated as R2 operates as a spoke router within the DMVPN setup. Its configuration aims to enable R2 to securely and efficiently communicate with the central DMVPN hub, typically router R1. This setup ensures dynamic creation of GRE tunnels and robust VPN functionality, allowing spoke-to-spoke communication through the hub and direct tunnels as needed.

The hostname identifies the router as R2, and providing a name is critical when you start working within a network of multiple routers.

```
Router(config)# hostname R2
```

This command prevents delays caused by unintended DNS queries resulting from typing errors.

```
R2(config)# no ip domain-lookup
```

exec-timeout 0 0: Prevents automatic logout from inactivity.
logging synchronous: Ensures system messages don't interrupt command entry.
Privilege level 15: Grants full administrative privileges.

password cisco123: Sets a password for secure router access.

```
R2(config)# line con 0
R2(config-line)# exec-timeout 0 0
R2(config-line)# logging synchronous
R2(config-line)# privilege level 15
R2(config-line)# password cisco123
```

R3 router configuration:

Router R3 functioned as a spoke router within the implemented DMVPN topology. The configuration objective was to enable dynamic communication between R3 and the DMVPN central hub, resulting in a stable and efficient VPN network. Configuration Overview (Figures 28–29, Appendix): The images illustrate key configuration steps that mirror those applied to Router R2, ensuring consistency across all spoke routers.

Sets the name of the router.

```
Router(config)# hostname R3
```

Prevents domain lookup delays caused by mistyped commands which I personally do often.

```
R3(config)# no ip domain-lookup
```

exec-timeout 0 0: Ensures continuous administrative access without automatic timeouts.

logging synchronous: Keeps console output neat and readable by preventing command interruptions by system messages.

privilege level 15: Grants the highest-level administrative permissions, allowing full router control.

password cisco123: Sets a secure password to prevent unauthorized console access.

```
R3(config)# line con 0
R3(config-line)# exec-timeout 0 0
R3(config-line)# logging synchronous
```

```
R3(config-line)# privilege level 15
R3(config-line)# password cisco123
```

DMVPN router configuration:

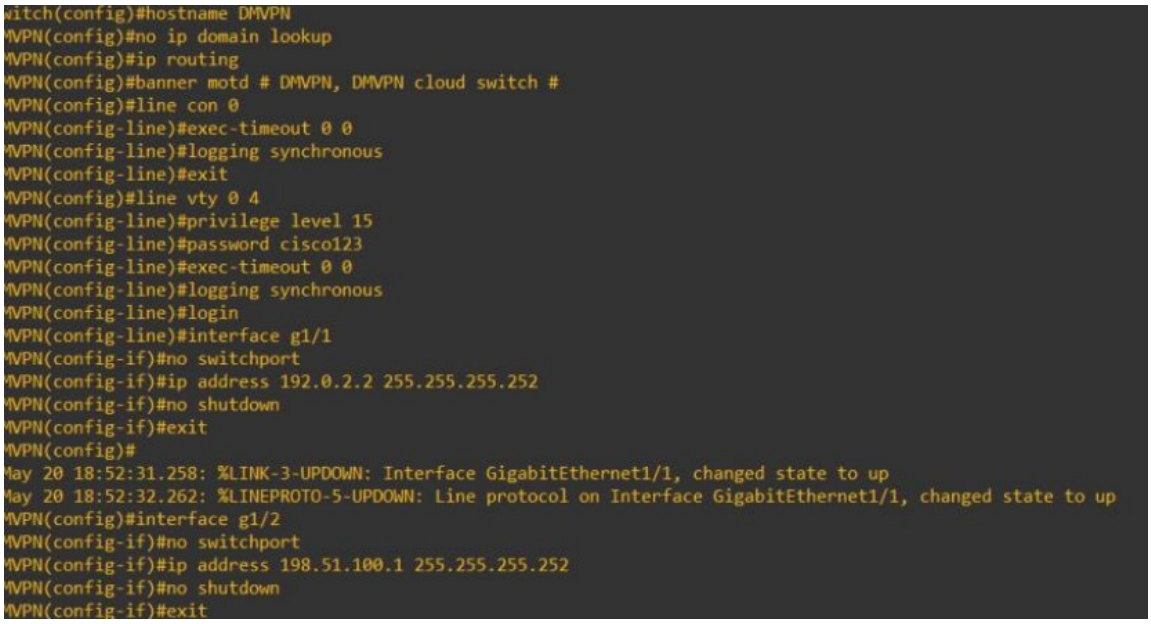

Figure 16. DMVPN router configuration

Upon completion of the router configuration, the implemented network topology was tested. Initially, R1 attempted to communicate with both R2 and R3.

```
R1#ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/7/10 ms
```

```
R1#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/9/13 ms
```

Figure 17. R1, R2 and R3 communication attempt results

In the second test, the traceroute command was used to determine the path taken by packets from R2 to R3, revealing each hop along the route.

```
R2#traceroute 172.16.3.1
Type escape sequence to abort.
Tracing the route to 172.16.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 100.100.100.1 8 msec 8 msec 10 msec
  2 100.100.100.3 18 msec 18 msec 16 msec
```

Figure 18. Traceroute results

4.2.2 DMVPN Phase 2

The objective was to trace the path from R2 to the destination IP address 172.16.3.1, and this was successfully completed. The second attempt, using the "traceroute" function (which shows the steps of the packet's journey), obtains the packet's path from R2 to R3. The results are shown below:

```
R2#traceroute 172.16.3.1
Type escape sequence to abort.
Tracing the route to 172.16.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 100.100.100.1 8 msec 8 msec 10 msec
  2 100.100.100.3 18 msec 18 msec 16 msec
```

Figure 19. R2 to R3 traceroute first attempt results

The command is run a second time to ensure stability and for us to be certain that everything works in order.

```
R2(config)#exit
R2#
*May 20 20:21:19.163: %SYS-5-CONFIG_I: Configured from console by console
R2#traceroute 172.16.3.1
Type escape sequence to abort.
Tracing the route to 172.16.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 100.100.100.1 13 msec 8 msec 8 msec
  2 100.100.100.3 17 msec 21 msec 21 msec
R2#
```

Figure 20. R2 to R3 traceroute second attempt results

It was observed that a direct spoke-to-spoke connection was established during the second test. The tunnel closed after approximately ten minutes of inactivity (the default timeout setting) and reopened dynamically when a new data packet was detected. Following this, the routing table was examined. On R2, the show route command was executed which displayed all EIGRP routes present in the routing table at that time.

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        100.100.100.0/29 is directly connected, Tunnel1
L        100.100.100.2/32 is directly connected, Tunnel1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Loopback1
L        172.16.2.1/32 is directly connected, Loopback1
D        172.16.3.0/24 [90/102400640] via 100.100.100.1, 00:32:06, Tunnel1
      192.0.2.0/30 is subnetted, 1 subnets
D        192.0.2.0 [90/15360] via 198.51.100.1, 00:32:14, GigabitEthernet0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Loopback0
L        192.168.2.1/32 is directly connected, Loopback0
D     192.168.3.0/24 [90/16000] via 198.51.100.1, 00:32:14, GigabitEthernet0/1
      198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.51.100.0/30 is directly connected, GigabitEthernet0/1
L        198.51.100.2/32 is directly connected, GigabitEthernet0/1
      203.0.113.0/30 is subnetted, 1 subnets
D        203.0.113.0 [90/15360] via 198.51.100.1, 00:32:14, GigabitEthernet0/1
R2#
```

Figure 21. EIGRP routes in the routing table

EIGRP output (Figure 21) indicated that the next-hop interface to the 172.16.3.0 network remained unchanged. However, the route was marked with a percentage symbol (%), signifying that NHRP had replaced the original next-hop entry with its own resolved value. An NHRP route entry also appeared in the routing table, indicating that the R3 interface was considered directly connected by NHRP. The

command shows ip route next-hop-override | begin Gateway was used to verify the specific next-hop value being applied.

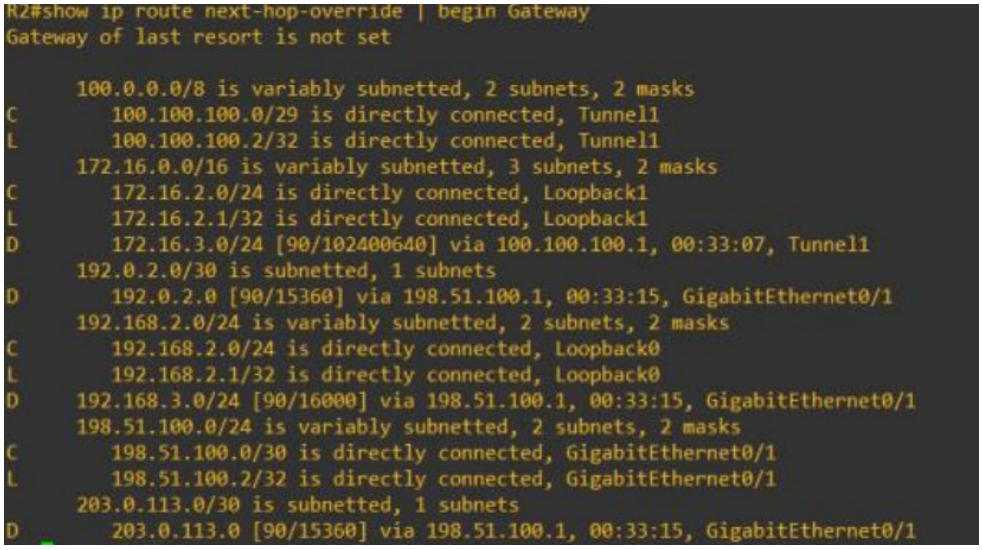

Figure 22. Next hop value

The next hop value is marked NHO (next hop override). This indicates that the next hop to 172.16.3.0 is R3 via the spoke-to-spoke tunnel.

4.2.3 DMVPN Phase 3

In this phase further configuration is needed, but the operation of Phase 3 will be verified using “show DMVPN detail” and opening a spoke-to-spoke tunnel.

```
R2#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel1 is up/up, Addr. is 100.100.100.2, VRF ""
   Tunnel Src./Dest. addr: 192.168.2.1/192.0.2.1, Tunnel VRF ""
   Protocol/Transport: "GRE/IP", Protect ""
   Interface State Control: Disabled
   nhrp event-publisher : Disabled

IPv4 NHS:
100.100.100.1  RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1 192.0.2.1         100.100.100.1    UP 00:33:39     S   100.100.100.1/32


Crypto Session Details:
--------------------------------------------------------------------------------

Pending DMVPN Sessions:
```

Figure 23. Verification results using DMVPN details

The first entry represented a static tunnel between R2 and the hub router. The DLX flag indicated that the entry referred to a local network. The DT1 entry defined a route through the overlay network, while the DT2 entry specified the next-hop value used to reach the destination network. In summary, all tests demonstrated that the simulated network was functional and suitable for deployment.

5 CONCLUSION

The primary objective of this thesis was to analyse, design, and implement a Dynamic Multipoint Virtual Private Network (DMVPN) configuration using Cisco routers virtualized within the GNS3 environment. The configurations were thoroughly tested to validate functionality, scalability, and security, within scenarios that closely simulated real-world deployment conditions. Organisations with geographically distributed locations or remote operations may benefit from adopting DMVPN as it streamlines network management and supports adaptability to evolving infrastructure requirements. Future extensions of this study could investigate more advanced implementations, such as deploying DMVPN in larger network environments, testing interoperability with multi-vendor

equipment, or integrating advanced routing protocols, and automated network management systems.

This thesis aims to contribute to a deeper understanding of modern networking technologies, VPN security strategies, and the practical aspects of network configuration and management. It provided relevant technical knowledge applicable to professional roles in network administration and cybersecurity. Several VPN protocols were presented and reviewed during this study. Among them, Dynamic Multipoint Virtual Private Network (DMVPN) was selected due to its hub-and-spoke architecture, which enables scalable and flexible communication. DMVPN provides a dynamic virtual private network framework and integrates with IPsec for encrypted, secure communication. These characteristics made it the most suitable option for the implementation carried out in this thesis.

In this study applications relevant to the DMVPN network were examined. In order to accelerate and simplify the deployment process, the GNS3 simulation platform was used during the implementation phase. The use of virtualisation helped minimise potential issues prior to real-world deployment and ensured greater stability during testing.

The DMVPN router configuration was evaluated as part of the implementation process. The multipoint GRE (mGRE) setup, which was successfully tested and verified to be operational, played a critical role in the initial phase of DMVPN deployment. Testing confirmed that an NHRP route entry appeared in the routing table, indicating that the R3 interface was identified as directly connected via NHRP. Subsequent tests demonstrated that the simulated network was functional and ready for full implementation.

The implementation plan outlined key strategies for executing the DMVPN configuration. Anticipated outcomes of a successful deployment included increased network flexibility, reduced configuration overhead, and an improved

security posture. Additionally, the use of GNS3 and Zabbix not only supported the testing and monitoring of the network but also demonstrated the practical relevance of the implementation for deployment in realistic network environments.

The results of the study demonstrate that DMVPN is a reliable and scalable solution, especially for organisations with distributed branches and mobile workforces. In the future, a more thorough analysis of performance metrics, failover strategies and integration with cloud infrastructure may further enhance the system’s robustness and practical adoption.

REFERENCES

Andrea, H. (2024) *PPTP Remote Access VPN Configuration on Cisco Routers.* [WWW document] Available at: https://example.com/pptp-cisco-config [Accessed 31 March 2025].

Antonelli, S., Girolamo, D., dell'Agnello, L., Gregori, D., Guizzunti, G., Ricci, P., Rosso, F., Sapunenko, V., Veraldi, R., Veronesi, P., Vistoli, C., Finzi, G. & Zani, S. (2011) *INFN-CNAF Monitor and Control System.* [WWW document] Available at: https://example.com/infn-monitor [Accessed 31 March 2025].

Ashtari, H. (2023) *PPTP vs. L2TP: Top 5 Differences To Know.* [WWW document] Available at: https://www.spiceworks.com/tech/networking/articles/pptp-vs-l2tp/amp/ [Accessed 31 March 2025].

Buenning, M. (2024) *What is PPTP (Point-to-Point Tunneling Protocol)?* [WWW document] Available at: https://www.ninjaone.com/it-hub/endpoint-security/what-is-pptp-point-to-point-tunneling-protocol/ [Accessed 31 March 2025].

Conran, M. (2015) *Design Guide DMVPN Phases.* [WWW document] Available at: https://network-insight.net/2015/02/03/design-guide-dmvpn-phases/ [Accessed 31 March 2025].

Edgeworth, B., Prall, D., Barozet, J.M., Lockhart, A. & Ben-Dvora, N. (2016) *Cisco Intelligent WAN (iWAN).* Cisco Press.

Efrika, H. (2021) *Setting Up L2TP VPN Client in Mikrotik WiFi Router.* [WWW document] Available at: https://hariesef.medium.com/setting-up-l2tp-vpn-client-in-mikrotik-wifi-router-b3068093014d [Accessed 31 March 2025].

Ferguson, P. & Huston, G. (1998) *What is a VPN?* [White paper] Available at: https://www.potaroo.net/papers/vpn.pdf [Accessed 31 March 2025].

firewall. (2024) *Understanding Cisco Dynamic Multipoint VPN - DMVPN, MGRE, NHRP.* [WWW document] Available at: https://www.firewall.cx/cisco/cisco-services-technologies/cisco-dmvpn-intro.html [Accessed 31 March 2025].

Francis, E.C. (2021) *What is DMVPN (Dynamic Multipoint VPN), NHRP, mGRE and How to Configure.* [WWW document] Available at: https://community.cisco.com/t5/networking-blogs/what-is-dmvpn-dynamic-multipoint-vpn-nhrp-mgre-and-how-to/ba-p/4487443 [Accessed 31 March 2025].

Globytė, E. (2023) *What is PPTP (Point-to-Point Tunneling Protocol)?* [WWW document] Available at: https://nordvpn.com/blog/what-is-pptp-protocol/ [Accessed 31 March 2025].

Grafana. (n.d.) *Kubernetes Views Global.* [Dashboard] Available at: https://grafana.com/grafana/dashboards/15757-kubernetes-views-global/ [Accessed 31 March 2025].

Grauer, Y. (2021) *How One Hacker's Push to Secure the Internet Became a Crucial Part of Mac, Linux, and Windows Operating Systems.* [WWW document] Available at: https://www.protocol.com/enterprise/daniel-bernstein-internet-encryption [Accessed 31 March 2025].

Holm, M. (2017) *Pros and Cons of Different VPN Protocols.* [WWW document] Available at: https://www.ovpn.com/en/blog/pros-and-cons-of-different-vpn-protocols [Accessed 31 March 2025].

Krasteva, M. (2023) *OpenVPN Explained: Best Features, Use-Cases and a WireGuard Comparison.* [WWW document] Available at: https://www.independent.co.uk/advisor/vpn/openvpn-explained [Accessed 31 March 2025].

Loshin, P. (2021) *Secure Shell (SSH).* [WWW document] Available at: https://www.techtarget.com/searchsecurity/definition/Secure-Shell [Accessed 31 March 2025].

Microsoft Corporation. (2009) *Windows 2000 Server.* [WWW document] Available at: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742566(v=technet.10) [Accessed 31 March 2025].

NetworkLessons. (2024) *Introduction to DMVPN.* [WWW document] Available at: https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn [Accessed 31 March 2025].

OpenVPN. (2024) *Site-to-Site VPN Routing with Access Server.* [WWW document] Available at: https://openvpn.net/vpn-server-resources/site-to-site-routing-explained-in-detail/ [Accessed 31 March 2025].

Parmenter, T. (2021) *What is a Dynamic Multipoint Virtual Private Network (DMVPN)?* [WWW document] Available at: https://www.techtarget.com/searchnetworking/definition/dynamic-multipoint-VPN-DMVPN [Accessed 31 March 2025].

PCmag. (2024) *SFP.* [WWW document] Available at: https://www.pcmag.com/encyclopedia/term/sfp [Accessed 31 March 2025].

Red Hat. (2019) *What is Open Source?* [WWW document] Available at: https://www.redhat.com/en/topics/open-source/what-is-open-source [Accessed 31 March 2025].

Rodier, R. (2021) *Point-to-Point (P2P) Connectivity: What You Need to Know.* [WWW document] Available at: https://lightyear.ai/blogs/point-to-point-connectivity [Accessed 31 March 2025].

Santitoro, R. (n.d.) *Metro Ethernet Services – A Technical Overview.* [WWW document] Available at: https://web.archive.org/web/20181222184046/http://www.mef.net/Assets/White_Papers/Metro-Ethernet-Services.pdf [Accessed 31 March 2025].

Savickaitė, M. (2022) *What is a PPTP VPN and Why It's the Wrong Choice.* [WWW document] Available at: https://surfshark.com/blog/what-is-pptp [Accessed 31 March 2025].

semperfinein. (2020) *An Introduction to DMVPN.* [WWW document] Available at: https://artofnetworkengineering.com/2020/08/21/an-introduction-to-dmvpn/ [Accessed 31 March 2025].

Stele, M. (2021) *VirtualBox Connection from Host to VM Through NAT and NATNetwork.* [WWW document] Available at: https://stele-miha.medium.com/virtualbox-connection-from-host-to-vm-through-nat-and-natnetwork-aa15289bfc01 [Accessed 31 March 2025].

Sussex University. (n.d.) *PuTTY.* [WWW document] Available at: https://www.sussex.ac.uk/its/services/software/owncomputer/putty [Accessed 31 March 2025].

TechTarget. (2016) *Cisco Systems, Inc.* [WWW document] Available at: https://www.techtarget.com/whatis/definition/Cisco-Systems-Inc [Accessed 31 March 2025].

VeePN. (2023) *What is a PPTP VPN? (and Is It Secure Enough for Your Needs?).* [WWW document] Available at: https://veepn.com/blog/what-is-pptp-vpn/ [Accessed 31 March 2025].

VeePN. (2023) *What is OpenVPN and Should You Use It?* [WWW document] Available at: https://veepn.com/blog/what-is-openvpn/ [Accessed 31 March 2025].

Wherry, J. (2023) *What is WireGuard?* [WWW document] Available at: https://cybernews.com/what-is-vpn/wireguard-protocol/ [Accessed 31 March 2025].

WireX. (2023) *L2TP: Network Protocol Explained.* [WWW document] Available at: https://wirexsystems.com/resource/protocols/l2tp [Accessed 31 March 2025].

Yonan, J. (2002) *OpenVPN/openvpn2-historical-cvs.* [WWW document] Available at: https://github.com/OpenVPN/openvpn2-historical-cvs/blob/d32aa83c2adc6f9fb70e2f0cc32c344f4864e95d/CHANGES#L20 [Accessed 31 March 2025].

Zenarmor. (2024) *What is L2TP? Understanding the Role of L2TP in Network Technologies.* [WWW document] Available at: https://www.zenarmor.com/docs/network-security-tutorials/what-is-l2tp [Accessed 31 March 2025].

Zola, A. & Scarpati, J. (2023) *Cisco IOS (Cisco Internetwork Operating System).* [WWW document] Available at: https://www.techtarget.com/searchnetworking/definition/Cisco-IOS-Cisco-Internetwork-Operating-System [Accessed 31 March 2025].

DMVPN router configurations:

R1 router configuration:

```
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
*May 20 18:17:02.917: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Config Wizard)
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, Implement DMVPN Hub #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#privilege level 15
R1(config-line)#password cisco123
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#interface g0/1
R1(config-if)#ip address 192.0.2.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface tunnel 1
R1(config-if)#tunnel mode gre multipoint
R1(config-if)#tunnel source g0/1
R1(config-if)#tunnel key 999
R1(config-if)#ip address 100.100.100.1 255.255.255.248
R1(config-if)#ip nhrp network-id 1
R1(config-if)#ip nhrp authentication NHRPauth
R1(config-if)#ip nhrp map multicast dynamic
R1(config-if)#bandwidth 4000
*May 20 18:19:39.631: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
R1(config-if)#bandwidth 4000
```

Figure 24. R1 configuration A

```
R1(config-if)#ip mtu 1400
R1(config-if)#ip tcp adjust-mss 1360
R1(config-if)#exit
R1(config)#
R1(config)#
R1(config)#router eigrp DMVPN_TUNNEL_NET
R1(config-router)#address-family ipv4 unicast autonomous-system 68
R1(config-router-af)#eigrp router-id 1.1.1.1
R1(config-router-af)#network 100.100.100.0 255.255.255.248
R1(config-router-af)#af-interface tunnel 1
R1(config-router-af-interface)#no split-horizon
R1(config-router-af-interface)#router eigrp DMVPN_TRANS_NET
R1(config-router)#address-family ipv4 unicast autonomous-system 168
R1(config-router-af)#eigrp router-id 10.1.1.1
R1(config-router-af)#network 192.0.2.0 255.255.255.252
R1(config-router-af)#end
```

Figure 25. R1 configuration B

R2 router configuration:

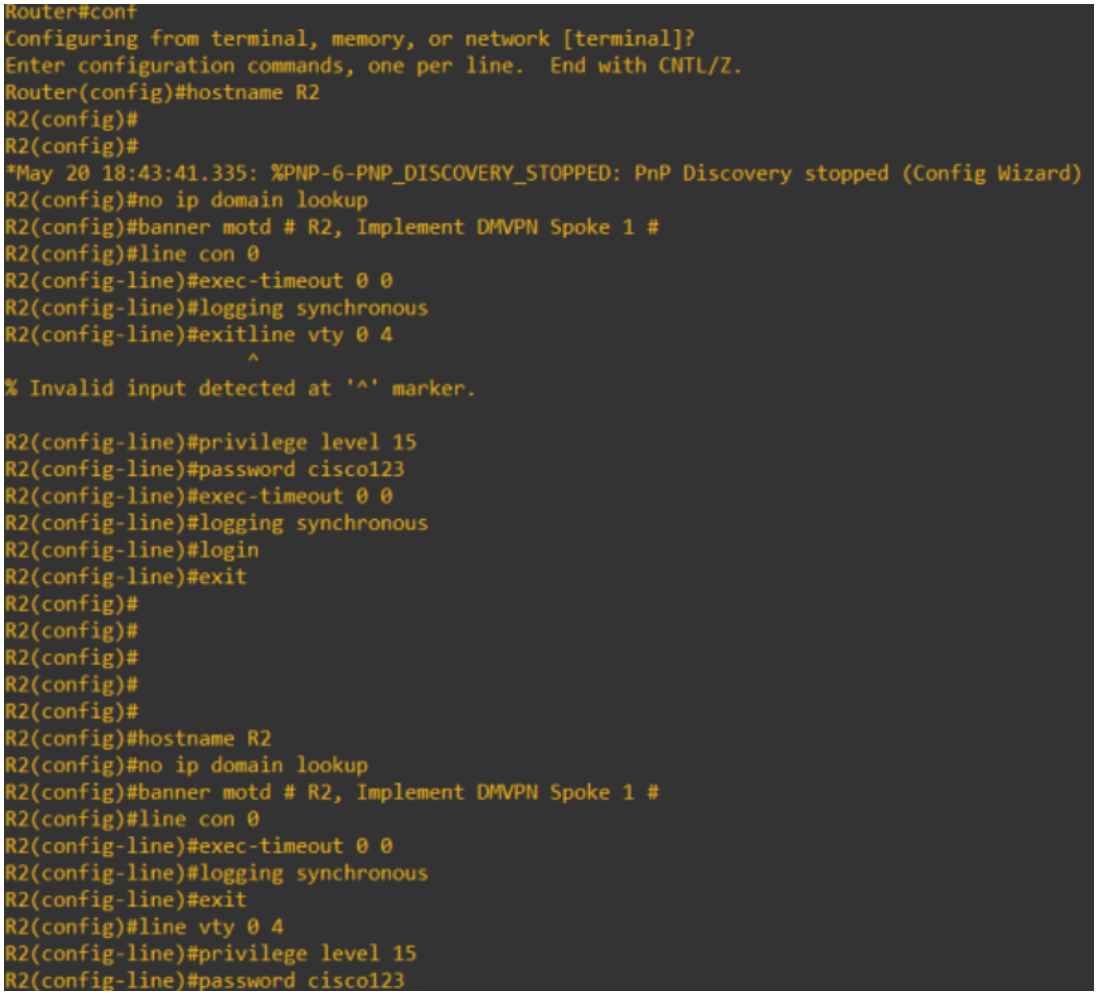

Figure 25. R2 configuration A

```
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#login
R2(config-line)#exit
R2(config)#interface g0/1
R2(config-if)#ip address 198.51.100.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*May 20 18:46:50.910: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*May 20 18:46:51.911: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R2(config)#
R2(config)#
R2(config)#
R2(config)#interface loopback 0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*May 20 18:47:09.668: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config)#
R2(config)#interface loopback 1
R2(config-if)#ip address 172.16.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*May 20 18:47:21.198: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R2(config)#
R2(config)#interface tunnel 1
R2(config-if)#
*May 20 18:47:33.563: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
R2(config-if)#tunnel mode gre ip
R2(config-if)#tunnel source loopback 0
R2(config-if)#tunnel destination 192.0.2.1
R2(config-if)#tunnel key 999
R2(config-if)#ip address 100.100.100.2 255.255.255.248
R2(config-if)#ip nhrp network-id 1
R2(config-if)#ip nhrp authentication NHRPauth
R2(config-if)#ip nhrp nhs 100.100.100.1
R2(config-if)#ip nhrp map multicast 192.0.2.1
R2(config-if)#ip nhrp map 100.100.100.1 192.0.2.1
R2(config-if)#ip mtu 1400
R2(config-if)#ip tcp adjust-mss 1360
R2(config-if)#router eigrp DMVPN_TUNNEL_NET
R2(config-router)#address-family ipv4 unicast autonomous-system 68
R2(config-router-af)#eigrp router-id 2.2.2.2
```

Figure 26. R2 configuration B

```
R2(config-router-af)#network 100.100.100.0 255.255.255.248
R2(config-router-af)#network 172.16.2.0 255.255.255.0
R2(config-router-af)#eigrp stub connected
R2(config-router-af)#router eigrp DMVPN_TRANS_NET
R2(config-router)#address-family ipv4 unicast autonomous-system 168
R2(config-router-af)#eigrp router-id 20.2.2.2
R2(config-router-af)#network 198.51.100.0 255.255.255.252
R2(config-router-af)#network 192.168.2.0 255.255.255.0
R2(config-router-af)#end
```

Figure 27. R2 configuration C

R3 router configuration:

```
Router(config)#
Router(config)#hostname R3
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, Implement DMVPN Spoke 2 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#privilege level 15
R3(config-line)#password cisco123
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#login
R3(config-line)#exit
R3(config)#
R3(config)#
*May 20 18:49:57.751: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Config Wizard)
R3(config)#
R3(config)#interface g0/1
R3(config-if)#ip address 203.0.113.2 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface loopback 0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface loopback 1
R3(config-if)#ip address 172.16.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
*May 20 18:50:08.217: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
*May 20 18:50:08.345: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R3(config-if)#exit
R3(config)#
*May 20 18:50:09.180: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*May 20 18:50:10.181: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R3(config)#
R3(config)#
R3(config)#interface tunnel 1
R3(config-if)#tunnel mode gre ip
```

Figure 28. R3 configuration A

```
R3(config-if)#tunnel source loopback 0
R3(config-if)#tunnel destination 192.0.2.1
R3(config-if)#tunnel key 999
R3(config-if)#ip address 100.100.100.3 255.255.255.248
R3(config-if)#ip nhrp network-id 1
R3(config-if)#ip nhrp authentication NHRPauth
R3(config-if)#ip nhrp nhs 100.100.100.1
R3(config-if)#ip nhrp map multicast 192.0.2.1
R3(config-if)#ip nhrp map 100.100.100.1 192.0.2.1
R3(config-if)#ip mtu 1400
*May 20 18:50:46.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
R3(config-if)#ip mtu 1400
R3(config-if)#
R3(config-if)#
R3(config-if)#ip tcp adjust-mss 1360
R3(config-if)#router eigrp DMVPN_TUNNEL_NET
R3(config-router)#address-family ipv4 unicast autonomous-system 68
R3(config-router-af)#eigrp router-id 3.3.3.3
R3(config-router-af)#network 100.100.100.0 255.255.255.248
R3(config-router-af)#network 172.16.3.0 255.255.255.0
R3(config-router-af)#eigrp stub connected
R3(config-router-af)#router eigrp DMVPN_TRANS_NET
R3(config-router)#address-family ipv4 unicast autonomous-system 168
R3(config-router-af)#eigrp router-id 30.3.3.3
R3(config-router-af)#network 203.0.113.0 255.255.255.252
R3(config-router-af)#network 192.168.3.0 255.255.255.0
R3(config-router-af)#eigrp stub connected
R3(config-router-af)#end
```

Figure 29. R3 configuration B