

NET622

Formative Assessment: 2

Roles and Group Members:

Presenter: Ettienne Nell
(20230128@ctucareer.co.za)


Coordinator: Vuyisile Jonas
(20230597@ctucareer.co.za)

Research: Willie De Klerk
(20230254@ctucareer.co.za)

CTUTRAINING.AC.ZA | 0861 100 395 | ENQUIRY@CTUTRAINING.CO.ZA

1. Declaration of Authenticity

A critical aspect of any assignment is *authenticity*. Because you are completing much of the work for the assignments *unsupervised*, the examiner must be convinced that it is all your work. For this reason, you must complete the *Declaration of Authenticity* provided in the study guide and have it counter-signed by your manager, mentor, or lecturer.

	The declaration of authenticity is a legal document, and if found that you have made a false declaration, then not only will your results be declared null and void, but you could also have criminal charges brought against you. It is not worth taking the risk!
---	---

Please complete the declaration of authenticity below for all assignments:






DECLARATION OF AUTHENTICITY

All Undersigned Group Members hereby

declare that the contents of this assignment are entirely our own work, completed by us without any paraphrasing/copying, or presented as our own work accessed from any AI Apps, example ChatGPT, Co-Pilot, Perplexity, or any other App.

Activity	Date
Formative Assessment 2	2024/09/12

 Etienne Nel Student (20230128)	 Vuyisile Jonas Student (20230597)	 Willie De Klerk Student (20230254) Signed by: 7e38ac48-8902-42d6-b32e-8740bcbddb0d
--	---	---

Signature: _____

Date: 2024/09/12

Application of OSPF authentication methods

1. Declaration of Authenticity	1
2. Introduction	3
3. Methods.....	3
3.1 Research platforms used	3
3.2 Documentation methods, processes and tools used.....	3
4. Results	4
4.1 OSPF version 2 packet header and supported authentication methods.....	4
4.2 A strategy for securing OSPF version 2 routing information with authentication in environments using IPv4.....	6
4.3 OSPF version 3 packet header and supported authentication methods.....	8
4.4 A strategy for securing OSPF version 3 routing information with authentication in environments using IPv6.....	9
5. Discussion.....	11
6. Conclusion.....	12
7. Table of Figures	12
8. Bibliography	13

2. Introduction

The interior gateway protocol known as OSPF was designed by the working group of the Internet Engineering Task Force (IETF). Through the proper implementation of the OSPF standard, routing table updates can be authenticated.

The implementation of OSPF authentication helps us to mitigate the security threats related to the OSPF routing protocol. An attacker can conceivably make use of OSPF packets to gain unauthorized access to a network if the packets are not protected by the correct implementation of authentication.

Within our research results we have thoroughly outlined the various methods of authentication supported by OSPF version 2 and OSPF version 3 routing protocol. Additionally, we have included proposed strategies for the practical application of authentication in both current versions of OSPF using Cisco Systems networking device operating systems.

3. Methods

3.1 Research platforms used

In our path to understanding the various concepts required to produce our report we made use of our prescribed textbooks outlined in our study guide for this module. Additionally, we have use of Request for Comments (RFC) publications to support our research.

We have gained access to the prescribed books through the online learning platform known as Oreilly Media which was included with our IT Diploma II programme package. We have gained access to the RFC publications through the Internet Engineering Task Force Data Tracker.

3.2 Documentation methods, processes and tools used

Documentation

For the creation of the report, we made use of the Microsoft Word programme that was included with our study package. Upon the completion, group validation and signage of the report, we exported the Word document to pdf format for submission.

We have made use of the Harvard Angilia (2008) citation style to produce our included references and bibliography.

Tools used

Graphical Network Simulator-3 (GNS3)

We have made use of the GNS3-all-in-one software (GUI) in addition to the GNS3 virtual machine (VM) as it allowed us to conduct our research of the application of OSPF authentication without having to pay for expensive hardware. It is trusted by many large enterprises, and it can be used to verify real world deployments. (docs.gns3.com, 2024)

Microsoft Hyper-V

To run our GNS3 VM we have made use of Microsoft Hyper-V and Microsoft Hyper-V manager. This functionality requires us to have Windows 10 (Pro or Enterprise) or Windows 11 (Pro or Enterprise). We have made use of Windows 11 Pro. (scooley, 2024)

Wireshark

We have made use of the Wireshark application as it allowed us to capture data from the ethernet links between our GNS3 appliances for analysis purposes. (wireshark.org, 2024)

4. Results

4.1 OSPF version 2 packet header and supported authentication methods

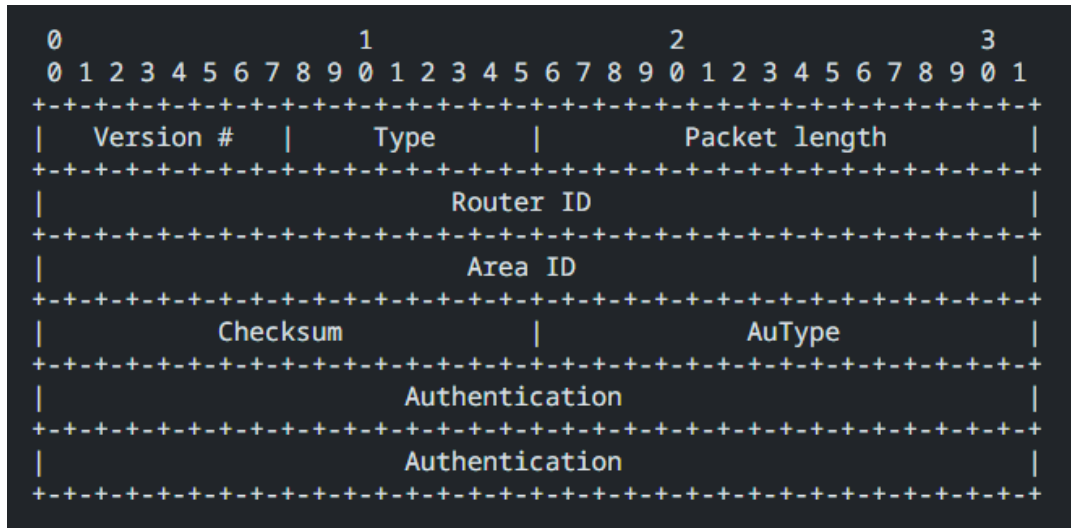


Figure 1 OSPFv2 Packet header Moy, J. (1998, April). RFC 2328 OSPF Version 2 | Appendix A.3 OSPF Packet Formats A.3.1 The OSPF packet header p. 190 - 192. Retrieved 09 06, 2024, from Internet Engineering Task Force (IETF) Data Tracker

Authentication Methods supported by OSPFv2

Null authentication

- The null authentication type (0) denotes routing exchanges that are not authenticated.
- The authentication field will be empty.
- Due the authentication field being empty, a router will not inspect the authentication field when it receives the packet.
- A checksum is used to detect data corruption, excluding the authentication field. (auth data)

(Moy, 1998, pp. 227 - 231)

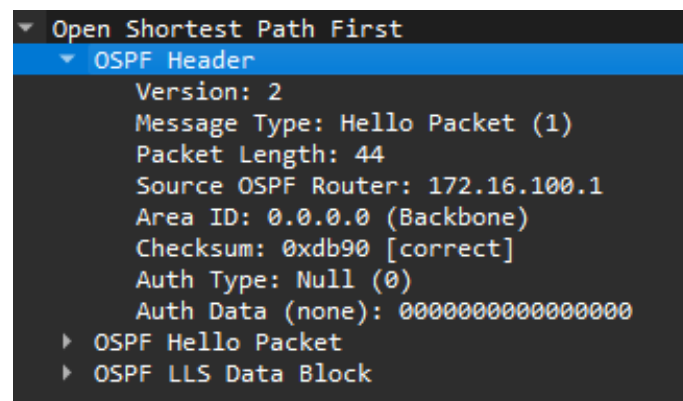


Figure 2 Wireshark Capture of OSPFv2 authentication (null authentication 0)

Simple password authentication:

- The simple password authentication type (1) is also known as plaintext authentication.
- It is a clear 64-bit password.
- This type of authentication helps to mitigate the threat of routers unintentionally joining a routing domain.
- It requires each router to be configured before it can participate.
- Simple password authentication is vulnerable to passive attacks such as sniffing, thus anyone with physical access can learn the password, affecting the security of the network.

(Moy, 1998, pp. 227 - 231)

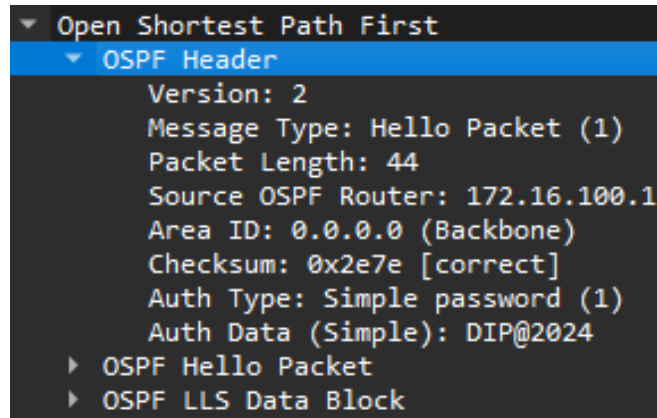


Figure 2 Wireshark Capture of OSPFv2 authentication (Simple password authentication 1)

Cryptographic Authentication:

- With cryptographic authentication type (2) a secret key is configured on all of the routers participating in ospf for the interface/area.
- The algorithms used to generate and verify the message digest are specified by the secret key. (MD5)
- Passive attacks are mitigated since the password is never sent over the network in clear form.
- Additionally, a non-decreasing sequence number is added to protect against replay attacks.

(Moy, 1998, pp. 227 - 231)

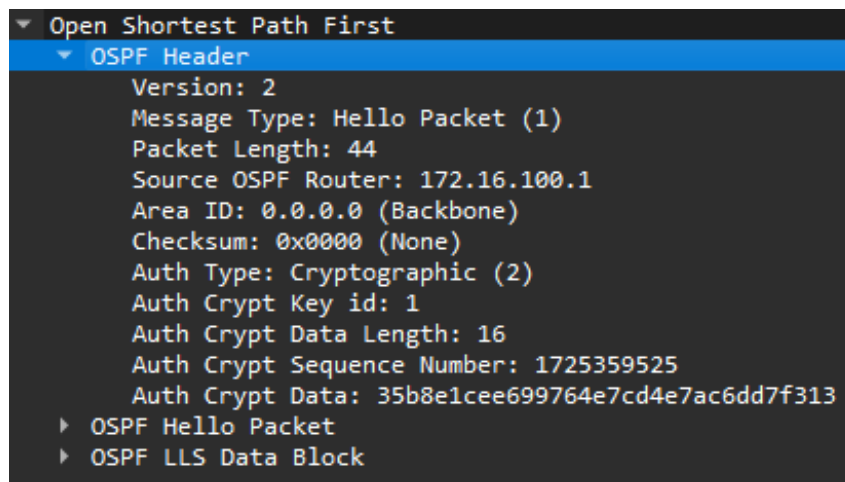


Figure 2 Wireshark Capture of OSPFv2 authentication (Cryptographic Authentication 2)

4.2 A strategy for securing OSPF version 2 routing information with authentication in environments using IPv4

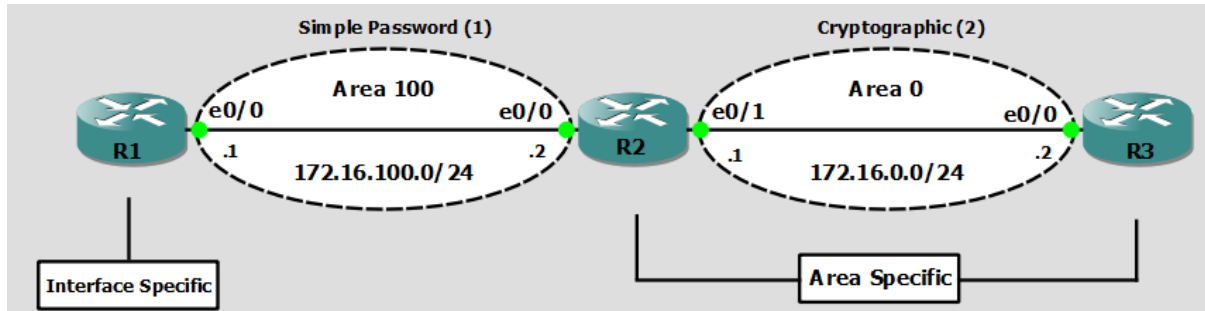


Figure 3 Network Diagram OSPFv2 IPv4 Strategy for securing routing information in environments using IPv4

OSPF authentication can be implemented as interface or area specific configuration. Our strategy involves making use of area specific configuration with the cryptographic authentication type at the routers forming part of area 0. (Simple towards areas)

The simple authentication is still more secure than null as it prevents routers from unintentionally taking part in ospf routing for the area. Additionally, other routers not forming part of area 0 are configured with interface specific authentication and the simple authentication type.

It should be noted that this strategy could be adjusted based on the specific environment requirements. Our reference for this strategy and configuration: (Edgeworth & Lacoste, 2023)

R1 Configuration

R1 does not form part of the backbone area, thus it will be configured with interface specific plain text / simple password authentication. This will aid in preventing routers from unintentionally joining the routing domain.

Something worth noting down is that the password can only be set as an interface parameter and it must be set individually for every interface, as if it was left out the interface would default to a null value.

1. OSPF Process Configuration

```
!
router ospf 1
 network 172.16.100.0 0.0.0.255 area 100
!
```

Figure 4 OSPFv2 IPv4 Strategy R1 OSPF Process Configuration

2. Interface Configuration

```
!
interface Ethernet0/0
 ip address 172.16.100.1 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key DIP@2024
!
```

Figure 5 OSPFv2 IPv4 Strategy R1 Interface Configuration

3. Authentication Verification


```
R1#show ip ospf interface | include line | authentication | key
Ethernet0/0 is up, line protocol is up
  Simple password authentication enabled
R1#
```

Figure 6 OSPFv2 IPv4 Strategy R1 Authentication Verification

R2 Configuration

R2 forms part of the backbone area, as such it has been configured with area specific cryptographic authentication. This configuration takes place within the OSPF process.

1. OSPF Process Configuration

```
!
router ospf 1
 area 0 authentication message-digest
 area 100 authentication
 network 172.16.0.0 0.0.0.255 area 0
 network 172.16.100.0 0.0.0.255 area 100
!
```

Figure 7 OSPFv2 IPv4 Strategy R2 OSPF Process Configuration

2. Interface Configuration

```
!
interface Ethernet0/0
 ip address 172.16.100.2 255.255.255.0
 ip ospf authentication-key DIP@2024
!
interface Ethernet0/1
 ip address 172.16.0.1 255.255.255.0
 ip ospf message-digest-key 1 md5 DIP@2024
!
```

Figure 8 OSPFv2 IPv4 Strategy R2 Interface Configuration

3. Authentication Verification

```
R2#show ip ospf interface | include line|authentication|key
Ethernet0/1 is up, line protocol is up
  Cryptographic authentication enabled
  Youngest key id is 1
Ethernet0/0 is up, line protocol is up
  Simple password authentication enabled
R2#
```

Figure 9 OSPFv2 IPv4 Strategy R2 Authentication Verification

R3 Configuration

R3 forms part of the backbone area and has received area specific cryptographic authentication.

1. OSPF Process Configuration

```
!
router ospf 1
 area 0 authentication message-digest
 network 172.16.0.0 0.0.0.255 area 0
!
```

Figure 10 OSPFv2 IPv4 Strategy R3 OSPF Process Configuration

2. Interface Configuration

OSPFv3 neighbor authentication does not use Internet key exchange to form the IPsec security association values. Due to this we need to manually configure the IPsec SPI hash algorithm and keys. (Edgeworth & Lacoste, 2023)

OSPFv3 Wireshark Capture

1. Configured with Authentication Header

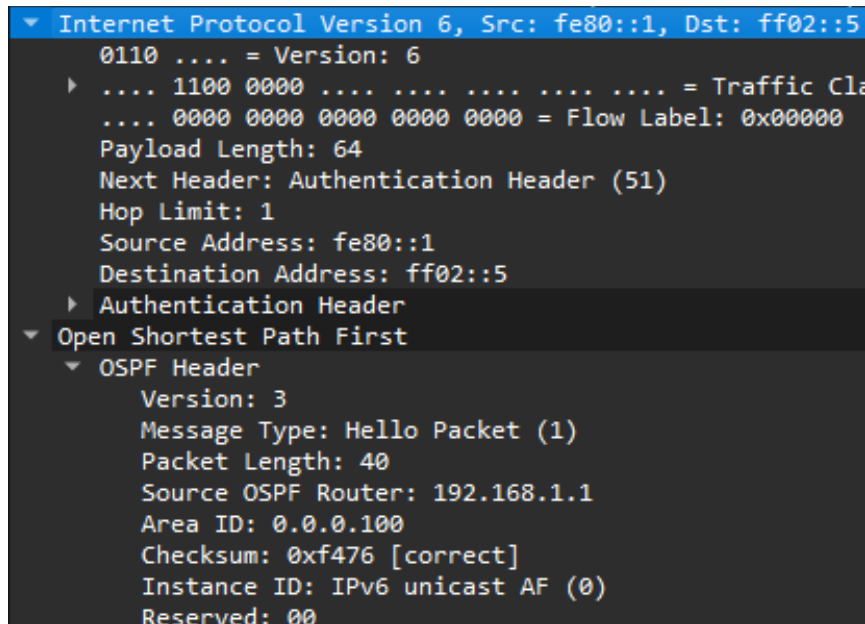


Figure 15 Wireshark Capture of the Authentication Header being implemented along with the visual display of changes to the OSPFv3 header

We can see that the authentication header used for authentication is present within the packet. We can also see that the OSPF header has changed in OSPFv3 as the fields used for authentication by OSPFv2 have been completely removed.

2. Configured with ESP Header

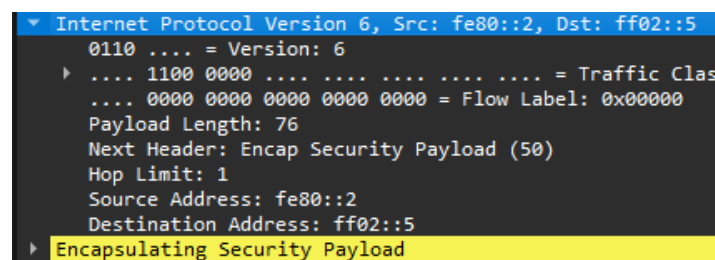


Figure 16 Wireshark Capture of the Encapsulating Security Payload Header being used to protect routing information

We can see that the ESP header used is present, providing authentication and encryption by encapsulating the routing information.

4.4 A strategy for securing OSPF version 3 routing information with authentication in environments using IPv6.

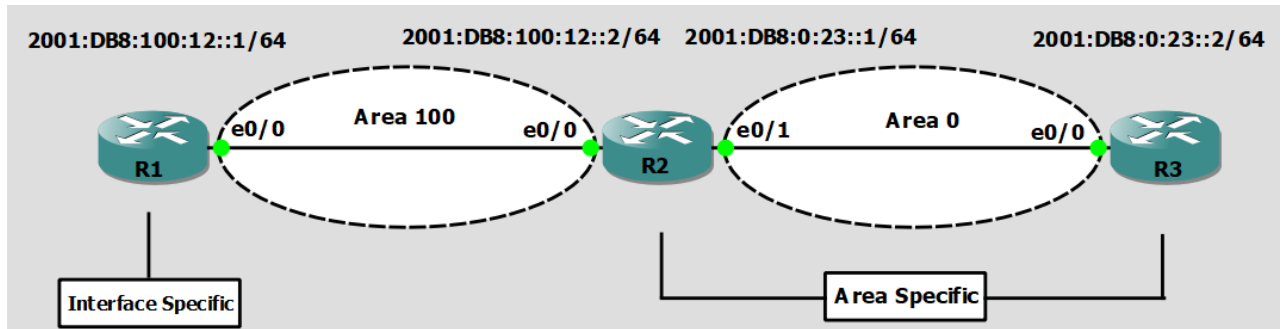


Figure 17 Network Diagram OSPFv3 IPv6 Strategy for securing routing information with authentication in IPv6 environments

We use area specific configuration on R2 and R3 as they form part of the backbone area. Furthermore, we use interface specific configuration on R1. We implemented OSPFv3 authentication with our configuration, making use of the IPv6 authentication header and the SHA-1 hashing algorithm.

Our reference for the strategy and configuration: (Edgeworth & Lacoste, 2023)

R1 Configuration

For the application of authentication on R1 we have made use of interface specific configuration, leaving the OSPFv3 process configuration to be minimal. Within snippet 2 it is visible that we have made use of authentication (using authentication header) and not encryption (which would use esp header). We have made use of the SHA-1 hashing algorithm.

1. OSPF Process Configuration

```
!
router ospfv3 1
 router-id 192.168.1.1
!
```

Figure 18 OSPFv3 IPv6 Strategy R1 OSPF Process Configuration

2. Interface Configuration

```
interface Ethernet0/0
 no ip address
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:100:12::1/64
 ospfv3 encryption null
 ospfv3 authentication ipsec spi 500 sha1 0123456789012345678901234567890123456789
 ospfv3 1 ipv6 area 100
```

Figure 19 OSPFv3 IPv6 Strategy R1 Interface Configuration

R2 Configuration

The configuration of our second router is different in comparison to R1 since we have to add more configuration under the ospf process since area-based authentication configuration takes place inside the ospf process configuration. This has led to a minimal amount of configuration needed on the interfaces.

1. OSPF Process Configuration

```
!
router ospfv3 1
router-id 192.168.2.2
area 100 authentication ipsec spi 500 sha1 0123456789012345678901234567890123456789
area 0 authentication ipsec spi 502 sha1 0123456789012345678901234567890123456789
!
```

Figure 20 OSPFv3 IPv6 Strategy R2 OSPF Process Configuration

2. Interface Configuration

```
interface Ethernet0/0
no ip address
ipv6 address FE80::2 link-local
ipv6 address 2001:DB8:100:12::2/64
ospfv3 1 ipv6 area 100
!
interface Ethernet0/1
no ip address
ipv6 address FE80::2 link-local
ipv6 address 2001:DB8:0:23::1/64
ospfv3 1 ipv6 area 0
```

Figure 21 OSPFv3 IPv6 Strategy R2 Interface Configuration

R3 Configuration

Just like our second router, R3 will form part of the backbone area, therefore it is receiving area specific configuration, in accordance with our strategy.

1. OSPF Process Configuration

```
!
router ospfv3 1
router-id 192.168.3.3
area 0 authentication ipsec spi 500 sha1 0123456789012345678901234567890123456789
!
```

Figure 22 OSPFv3 IPv6 Strategy R3 OSPF Process Configuration

2. Interface Configuration

```
interface Ethernet0/0
no ip address
ipv6 address FE80::3 link-local
ipv6 address 2001:DB8:0:23::2/64
ospfv3 1 ipv6 area 0
!
```

Figure 23 OSPFv3 IPv6 Strategy R3 Interface Configuration

5. Discussion

Our findings were made to the best of our knowledge and interpretation of the proposed questions. We answered the questions with a relative estimation of the mark allocation. Through the research that we have conducted we have gained vital insight into the application of authentication with regards to the OSPF routing protocol.

6. Conclusion

Choosing the correct authentication methods, implemented with the correct corresponding authentication strategy is important in a business IT environment where there are routers running OSPF who need to exchange routing information with neighboring routers. Network administrators must pay a great deal of attention while configuring OSPF authentication to ensure that it is done correctly.

In an environment making use of IPv4 and OSPFv2 it is best to avoid null authentication (0) and to take careful consideration as to the application of authentication in either interface or area specific configuration. Passwords for authentication can only be set as an interface parameter and it needs to be configured for each individual interface.

In an environment making use of IPv6 and OSPFv3 it is best to include authentication rather than leaving it empty. This can be achieved by either the implementation of just authentication with the authentication header or if the environment calls for stricter security measures, the addition of encryption when making use of the encapsulating security payload header which will provide encryption along with authentication. Due to the unique implementation of authentication for OSPFv3, network administrators are required to manually configure the IPsec SPI hash algorithm and keys.

7. Table of Figures

Figure 1 OSPFv2 Packet header Moy, J. (1998, April). RFC 2328 OSPF Version 2 Appendix A.3 OSPF Packet Formats A.3.1 The OSPF packet header p. 190 - 192. Retrieved 09 06, 2024, from Internet Engineering Task Force (IETF) Data Tracker.....	4
Figure 3 Wireshark Capture of OSPFv2 authentication (Cryptographic Authentication 2)	5
Figure 4 Network Diagram OSPFv2 IPv4 Strategy for securing routing information in environments using IPv4	6
Figure 5 OSPFv2 IPv4 Strategy R1 OSPF Process Configuration.....	6
Figure 6 OSPFv2 IPv6 Strategy R1 Interface Configuration.....	6
Figure 7 OSPFv2 IPv4 Strategy R1 Authentication Verification	7
Figure 8 OSPFv2 IPv4 Strategy R2 OSPF Process Configuration.....	7
Figure 9 OSPFv2 IPv4 Strategy R2 Interface Configuration.....	7
Figure 10 OSPFv2 IPv4 Strategy R2 Authentication Verification	7
Figure 11 OSPFv2 IPv4 Strategy R3 OSPF Process Configuration.....	7
Figure 12 OSPFv2 IPv4 Strategy R3 Interface Configuration.....	8
Figure 13 OSPFv2 IPv4 Strategy R3 Authentication Verification	8
Figure 14 OSPFv3 Packet Header Ferguson, D., Lindem, A., & Moy, J. (2008, July). RFC 5340 OSPF for IPv6 Appendix A. OSPF Data Formats A.3.1 The OSPF Packet Header p. 60. Retrieved 09 07, 2024, from Internet Engineering Task Force (IETF) Data Tracker.....	8
Figure 15 IPv6 IPsec Packet Format (Design is RFC inspired sourced from e-book) Edgeworth, B. & Lacoste, R., 2023. <i>CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide, Second Edition Chapter 9. OSPFv3, OSPFv3 Configuration (Level 1 Section 4)</i> . [Online] Available at: https://learning.oreilly.com/library/view/ccnp-enterprise-advanced/9780138217570/ch09.xhtml#ch09lev1sec4 [Accessed 06 09 2024].....	8
Figure 16 Wireshark Capture of the Authentication Header being implemented along with the visual display of changes to the OSPFv3 header.....	9

Figure 17 Wireshark Capture of the Encapsulating Security Payload Header being used to protect routing information	9
Figure 18 Network Diagram OSPFv3 IPv6 Strategy for securing routing information with authentication in IPv6 environments.....	10
Figure 19 OSPFv3 IPv6 Strategy R1 OSPF Process Configuration.....	10
Figure 20 OSPFv3 IPv6 Strategy R1 Interface Configuration.....	10
Figure 21 OSPFv3 IPv6 Strategy R2 OSPF Process Configuration.....	11
Figure 22 OSPFv3 IPv6 Strategy R2 Interface Configuration.....	11
Figure 23 OSPFv3 IPv6 Strategy R3 OSPF Process Configuration.....	11
Figure 24 OSPFv3 IPv6 Strategy R3 Interface Configuration.....	11

8. Bibliography

docs.gns3.com, 2024. *Getting Started with GNS3*. [Online]
Available at: <https://docs.gns3.com/docs/>
[Accessed 11 09 2024].

Edgeworth, B. & Lacoste, R., 2023. *CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide, 2nd Edition | Chapter 6. OSPF, Authentication (Level 1 Section 8)*. [Online]
Available at: <https://learning.oreilly.com/library/view/ccnp-enterprise-advanced/9780138217570/ch06.xhtml#ch06lev1sec8>
[Accessed 06 09 2024].

Edgeworth, B. & Lacoste, R., 2023. *CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide, Second Edition | Chapter 9. OSPFv3, OSPFv3 Configuration (Level 1 Section 4)*. [Online]
Available at: <https://learning.oreilly.com/library/view/ccnp-enterprise-advanced/9780138217570/ch09.xhtml#ch09lev1sec4>
[Accessed 06 09 2024].

Ferguson, D., Lindem, A. & Moy, J., 2008. *RFC 5340 OSPF for IPv6 | 2. Differences from OSPF for IPv4 2.6. Authentication Changes pp. 7 - 8*. [Online]
Available at: <https://datatracker.ietf.org/doc/rfc5340/>
[Accessed 06 09 2024].

Ferguson, D., Lindem, A. & Moy, J., 2008. *RFC 5340 OSPF for IPv6 | Appendix A. OSPF Data Formats A.3.1 The OSPF Packet Header p. 60*. [Online]
Available at: <https://datatracker.ietf.org/doc/rfc5340/>
[Accessed 07 08 2024].

Moy, J., 1998. *RFC 2328 OSPF Version 2 | Appendix A.3 OSPF Packet Formats A.3.1 The OSPF packet header p. 190 - 192*. [Online]
Available at: <https://datatracker.ietf.org/doc/rfc2328/>
[Accessed 06 09 2024].

Moy, J., 1998. *RFC 2328 OSPF Version 2 | Appendix D. Authentication pp. 227 - 231*. [Online]
Available at: <https://datatracker.ietf.org/doc/rfc2328/>
[Accessed 06 09 2024].

scooley, m. d. p. B. H. d. s., 2024. *Introduction to Hyper-V on Windows*. [Online]
Available at: <https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/>
[Accessed 11 09 2024].

wireshark.org, 2024. *About Wireshark*. [Online]
Available at: <https://www.wireshark.org/about.html>
[Accessed 11 09 2024].