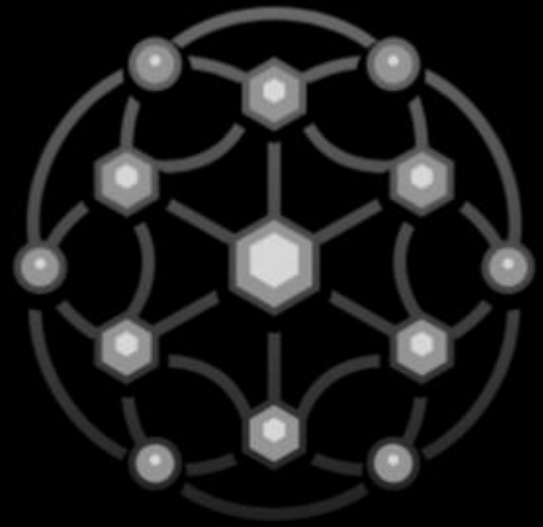


OSPF

IMPLEMENTING OSPF AUTHENTICATION

NET622 FA2 TOPIC 4

Introduction

The implementation of OSPF authentication helps us to mitigate security threats related to the OSPF routing protocol.

An attacker can make use of OSPF packets to gain unauthorized access to a network if the packets are not protected by the correct implementation of authentication.

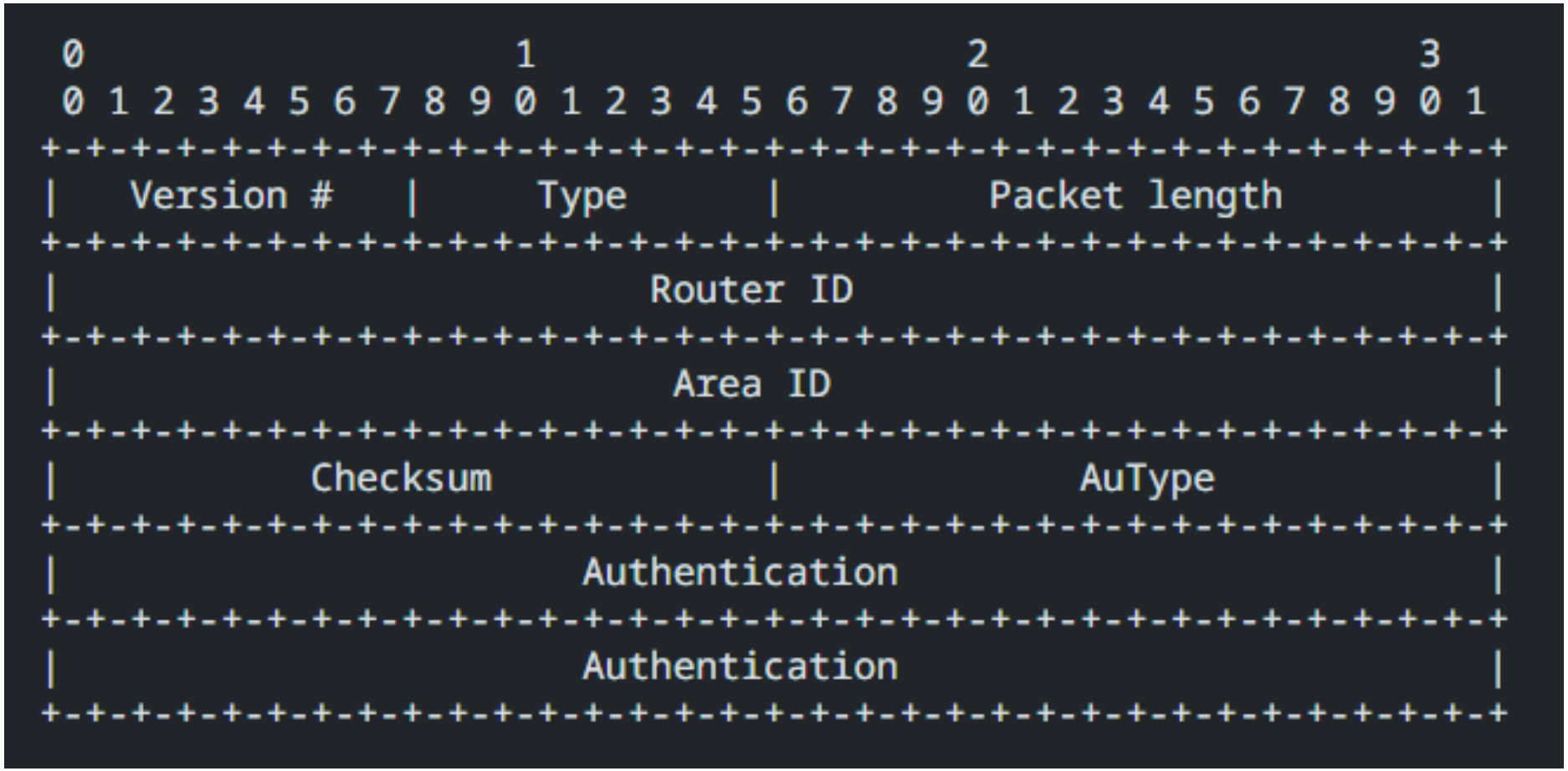
OSPF authentication can be found within the OSPF packet header which is included with all OSPF packet types

We will have a primary focus on OSPFv2 whilst mentioning changes in OSPFv3 authentication.

Presentation Agenda

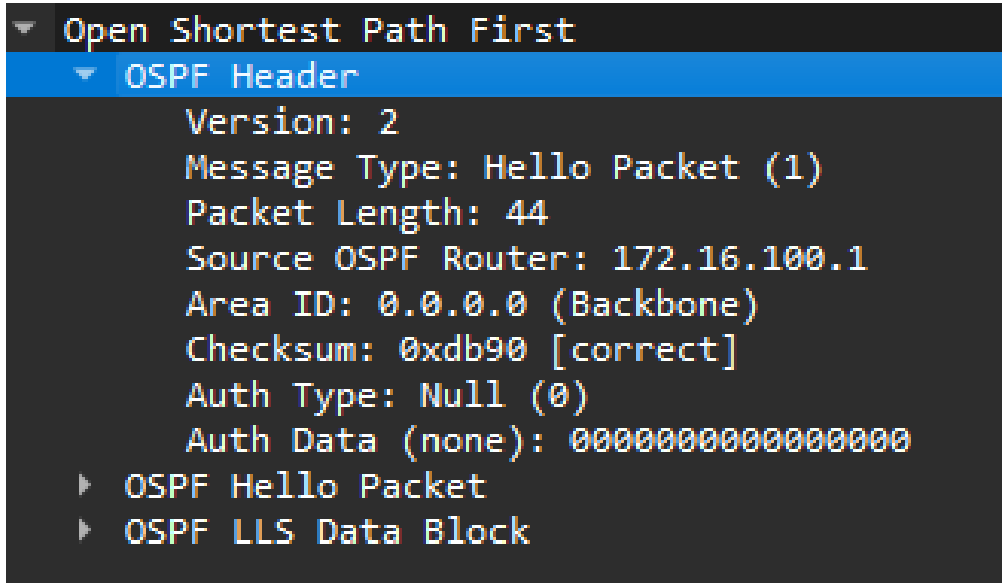
1. OSPF version 2 packet header and supported authentication methods.
2. A strategy for securing OSPF version 2 routing information with authentication in environments using IPv4.
3. OSPF version 3 packet header and supported authentication methods.
4. A strategy for securing OSPF version 3 routing information with authentication in environments using IPv6.

OSPFv2 Packet Header



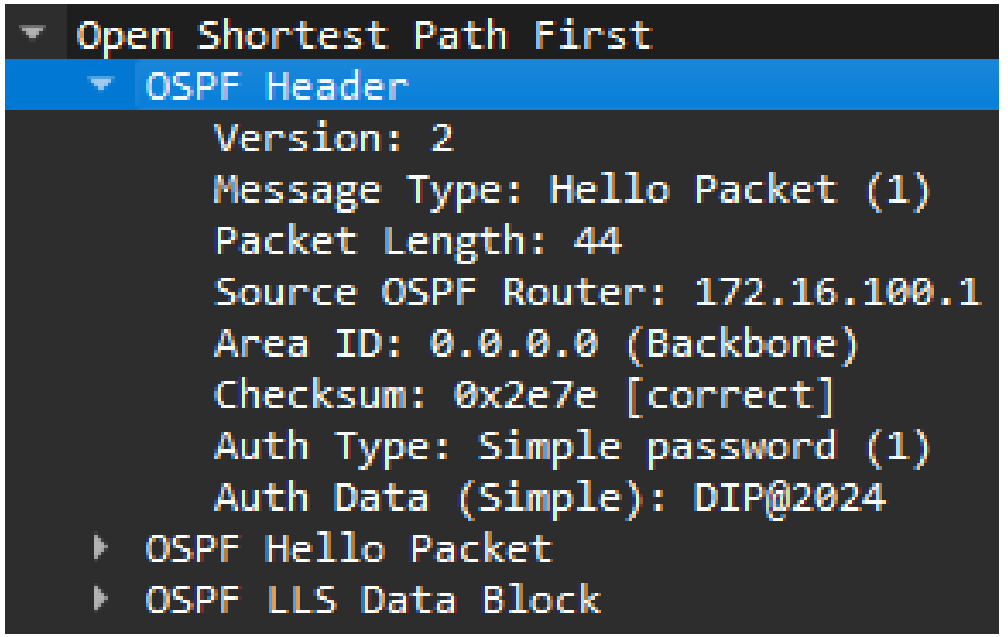
Null authentication

- The null authentication type (0) denotes routing exchanges that are not authenticated.
- The authentication field will be empty.
- Due to 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)



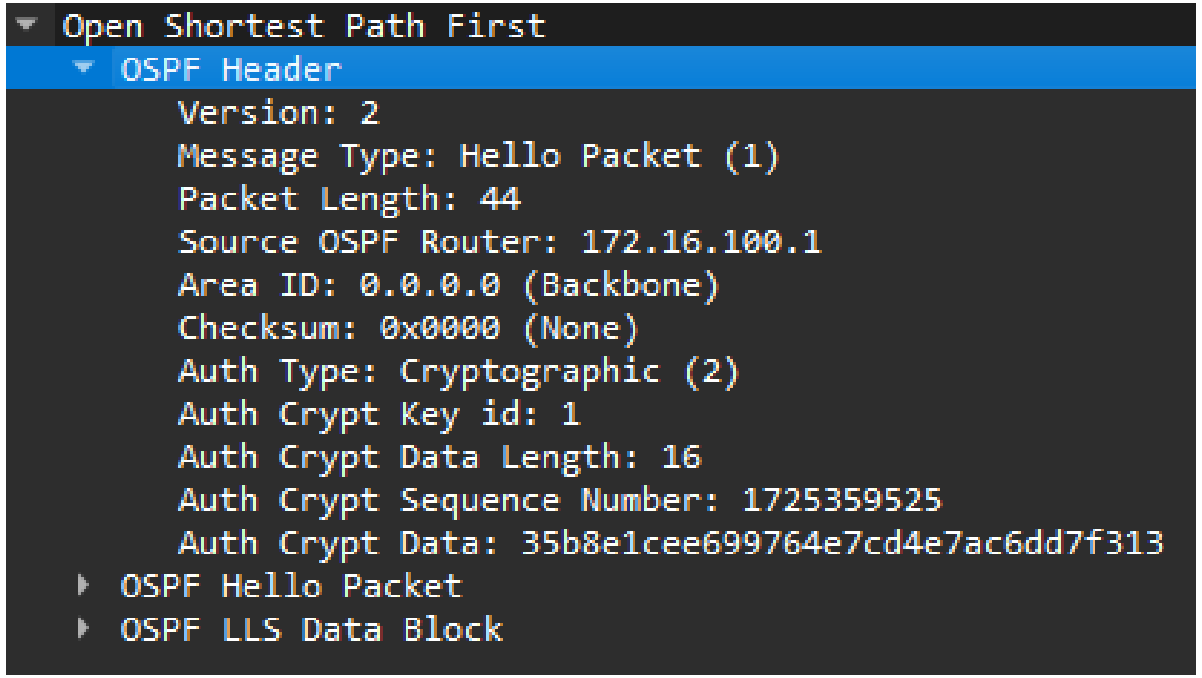
Simple password authentication

- 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.



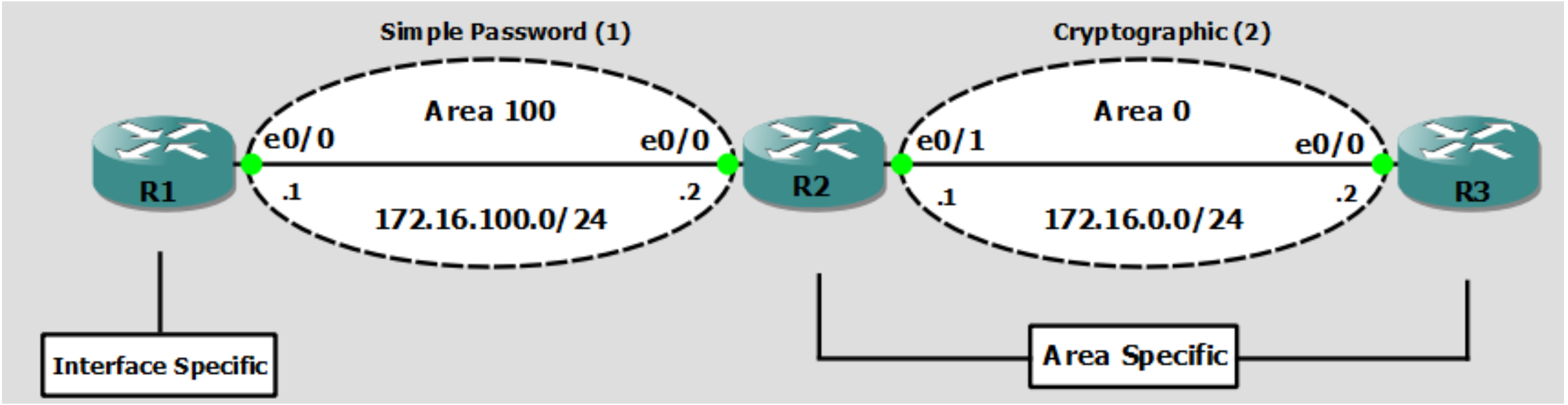
Cryptographic Authentication

- With cryptographic authentication type (2) a secret key is configured on all of the routers participating in ospf for the interface/area.
- The key is used to generate/verify a message digest.
- 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.

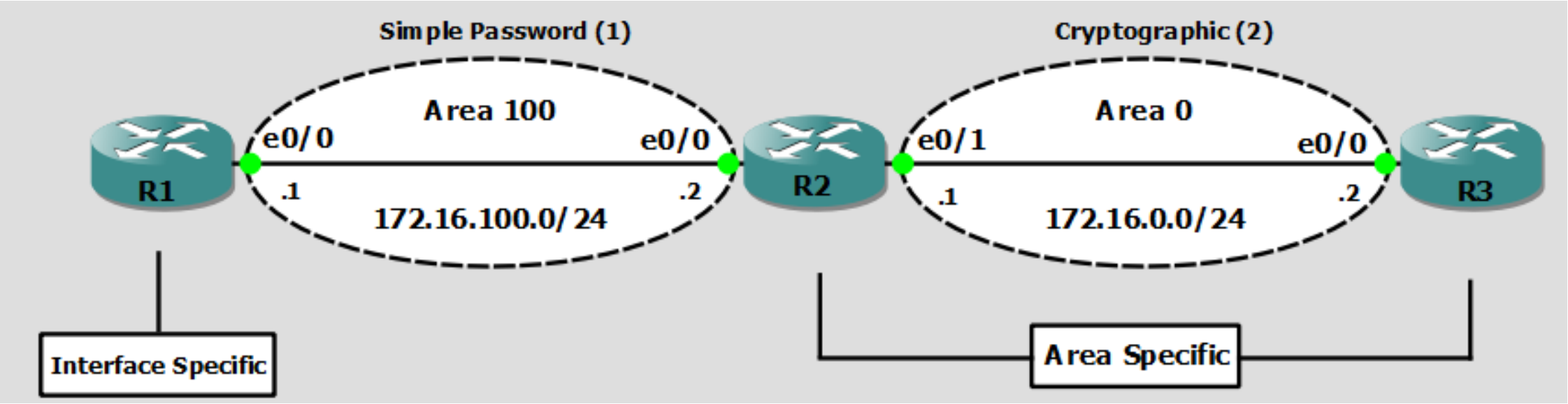


Strategy for securing OSPFv2 with authentication

- 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.



R1 Configuration



1. OSPF Process Configuration

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

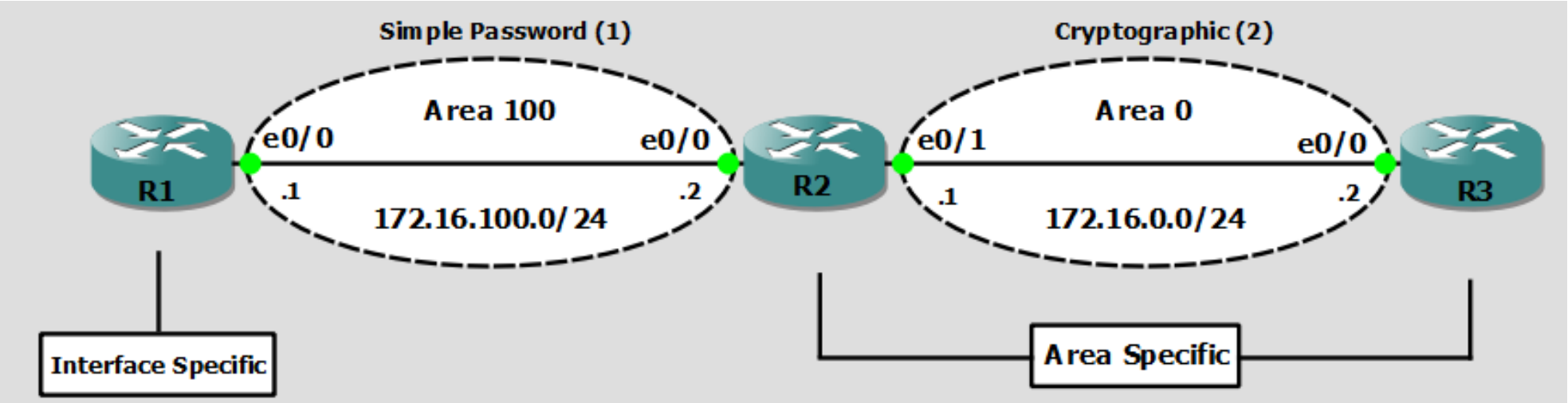
2. Interface Configuration

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

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#
```

R2 Configuration



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
!
```

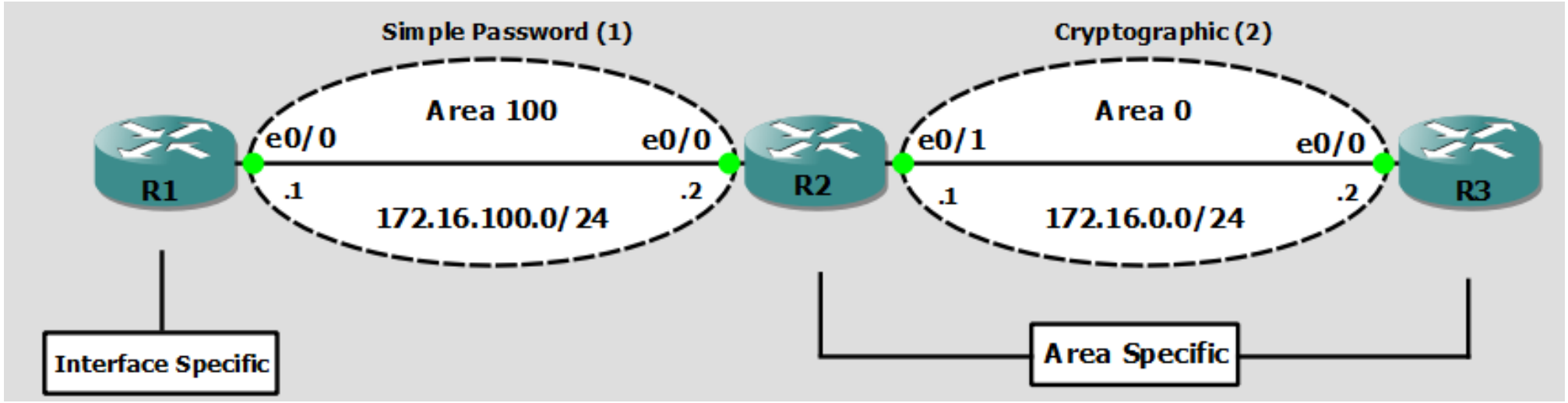
2. Interface Configuration

```
!
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
```

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#
```

R3 Configuration



1. OSPF Process Configuration

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

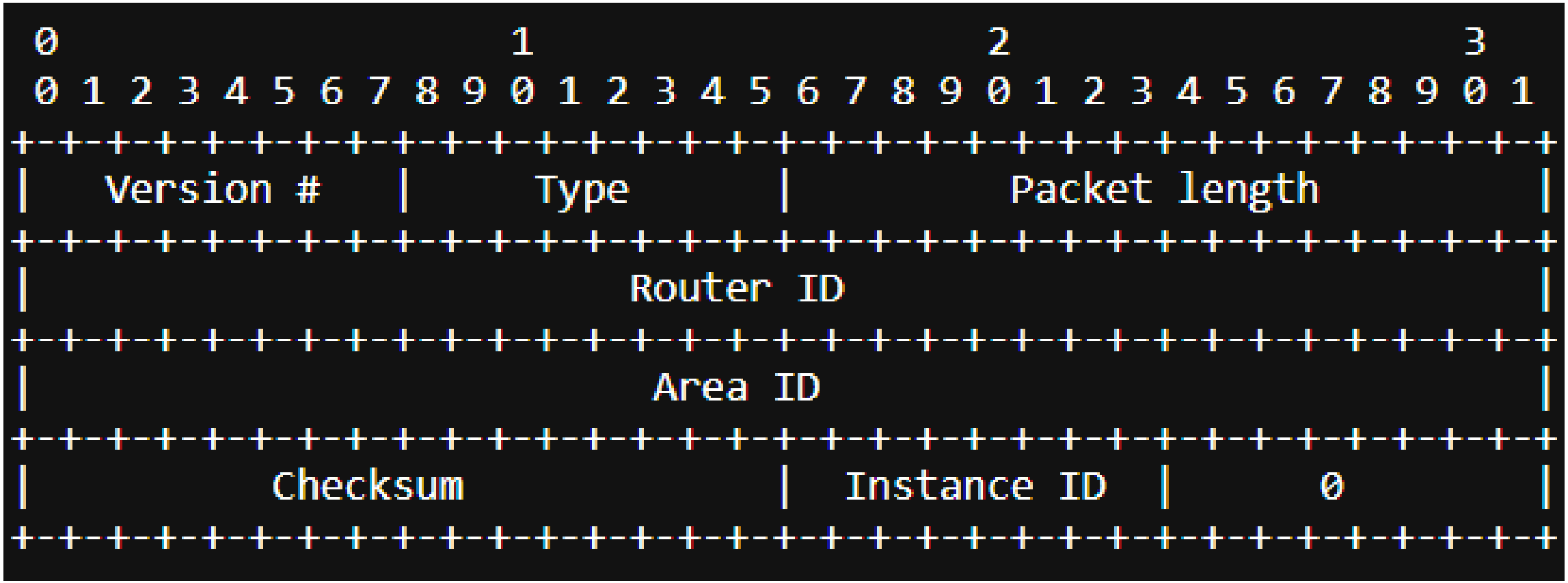
2. Interface Configuration

```
!
interface Ethernet0/0
 ip address 172.16.0.2 255.255.255.0
 ip ospf message-digest-key 1 md5 DIP@2024
!
```

3. Authentication Verification

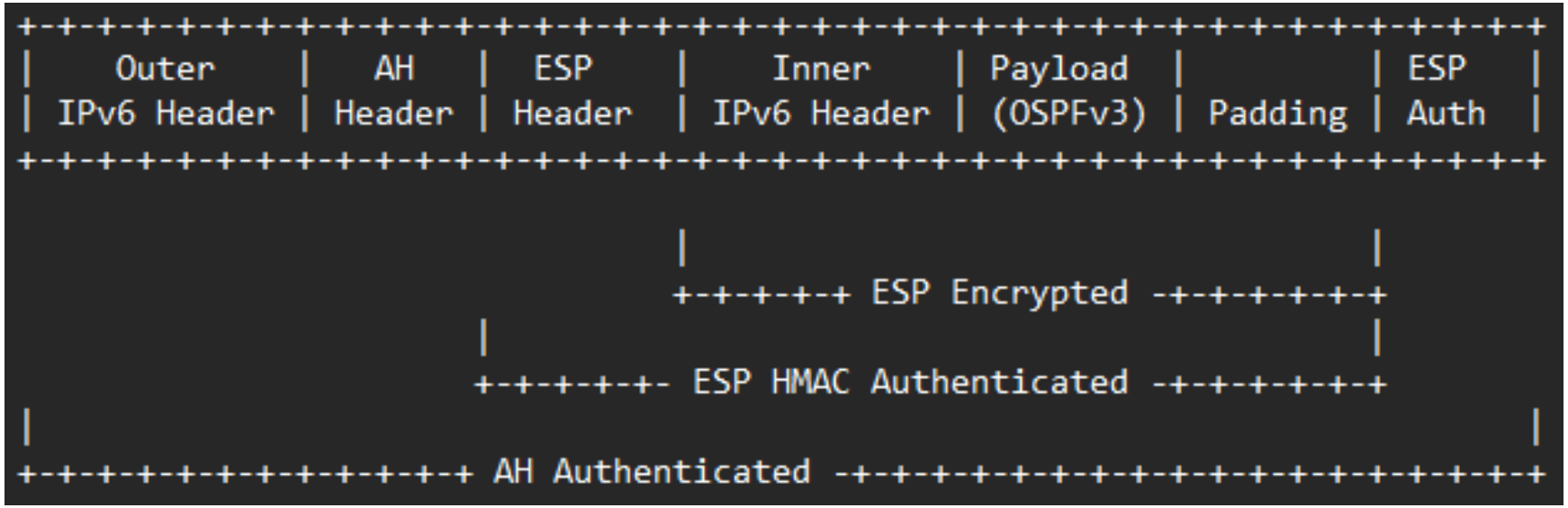
```
R3#show ip ospf interface | include line|authentication|key
Ethernet0/0 is up, line protocol is up
  Cryptographic authentication enabled
    Youngest key id is 1
R3#
```

Changes within OSPFv3 Packet Header



- OSPFv3 does not natively support authentication as it has been removed from the protocol.
- Both the Authentication type and Authentication fields have been removed.

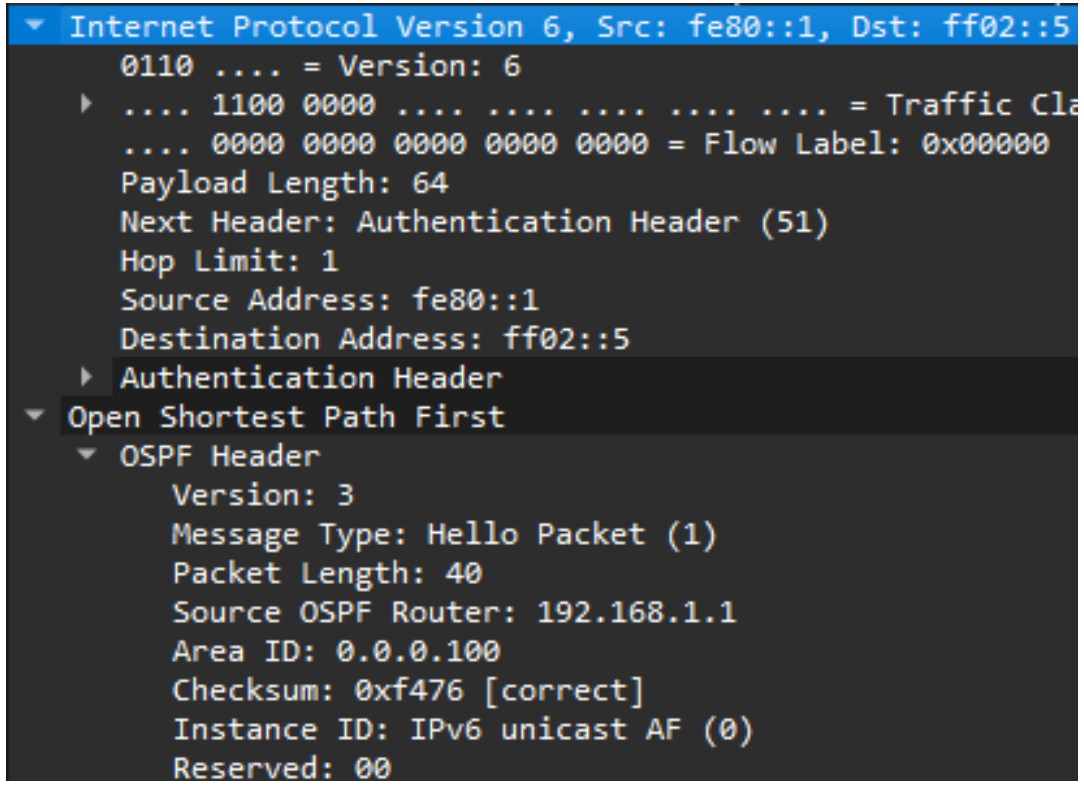
Changes within OSPFv3 Authentication



- OSPFv3 utilizes the IP Authentication Header and the IP Encapsulating Security Payload to ensure that the confidentiality and integrity of routing exchanges are maintained.
- OSPv3 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.

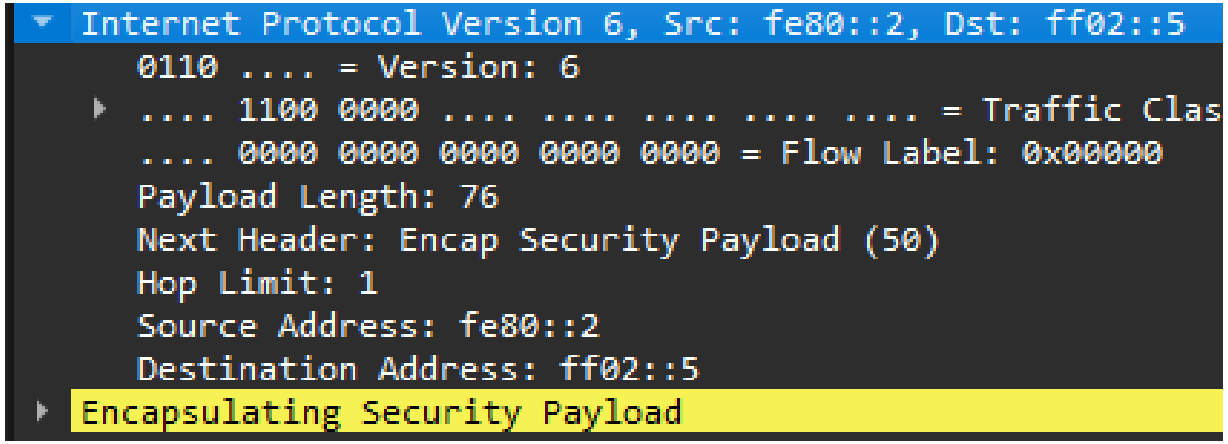
OSPFv3 Wireshark Capture

1. Configured with Authentication Header



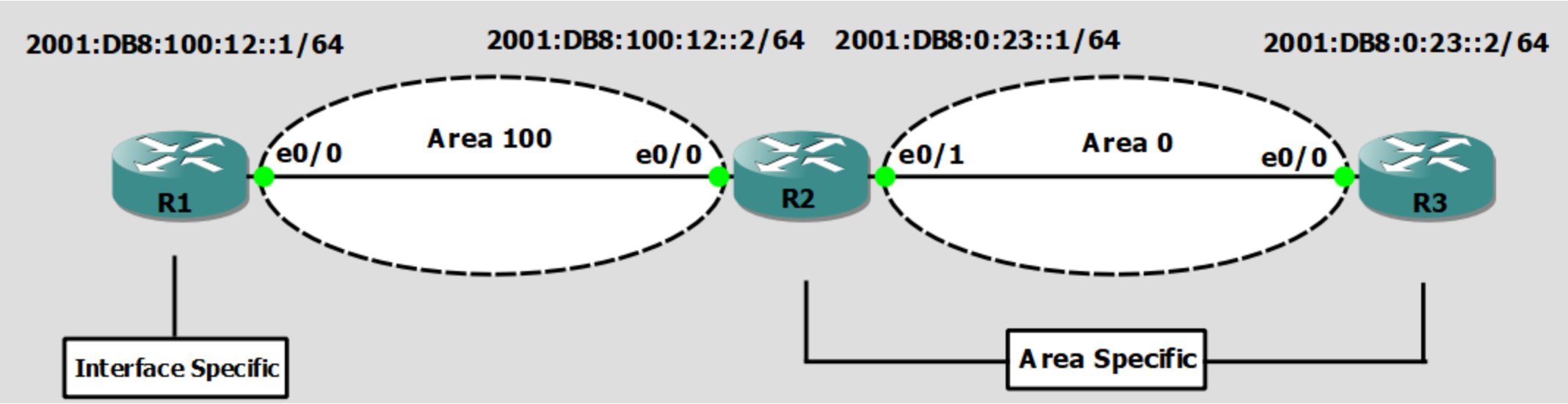
- We can see that the authentication header used for authentication is present within the packet.
- We can also see that the OSPF header has changed in OSPFv3 as the fields used for authentication by OSPFv2 have been completely removed.

2. Configured with ESP Header



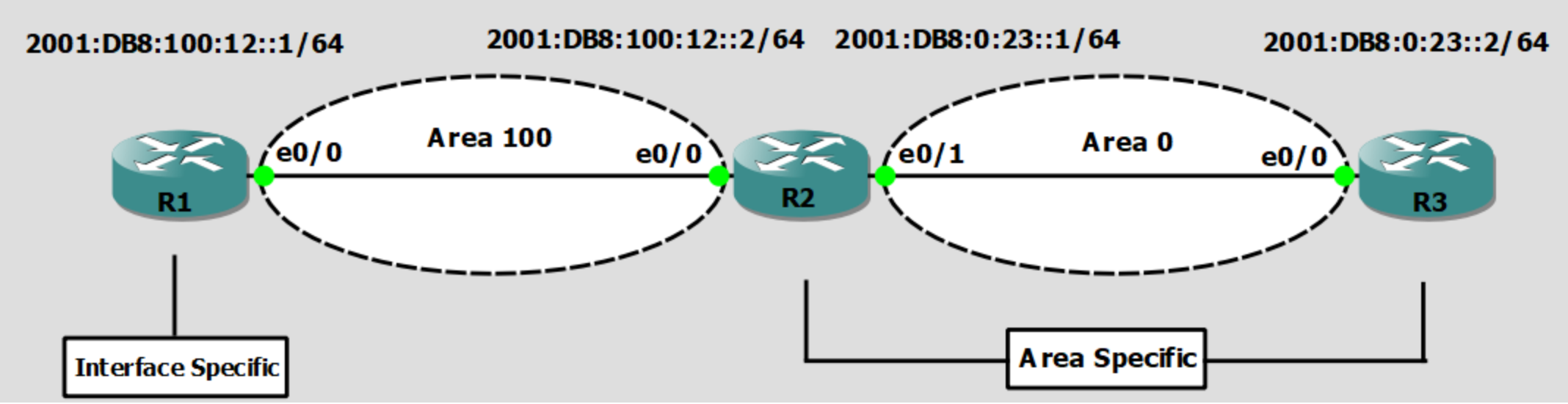
- We can see that the ESP header is used present, providing authentication and encryption by encapsulating the routing information.

OSPFv3 Authentication Strategy



- 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.

R1 Configuration



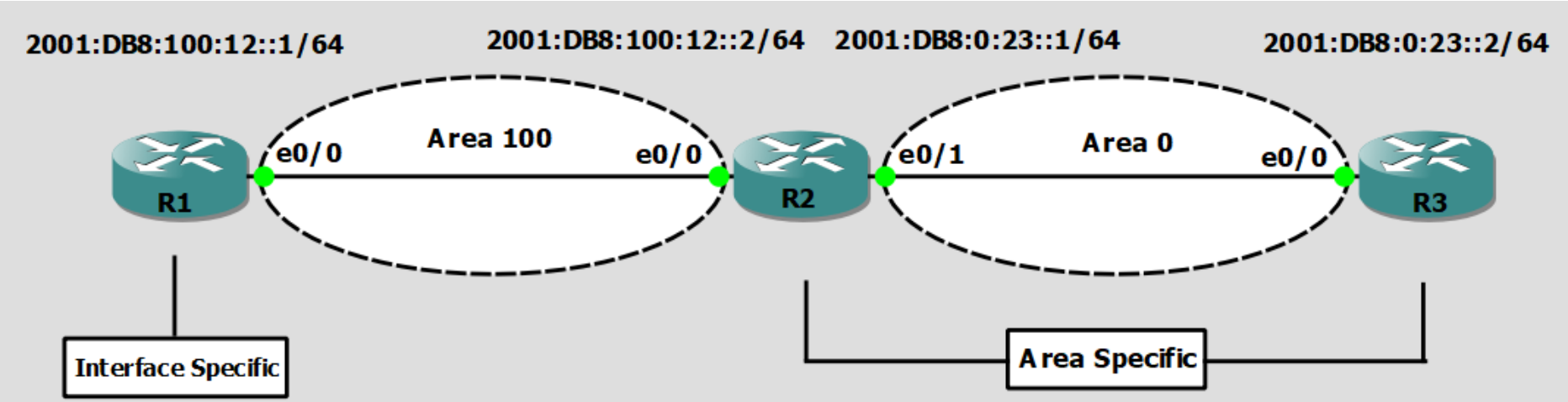
1. OSPF Process Configuration

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

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
```

R2 Configuration



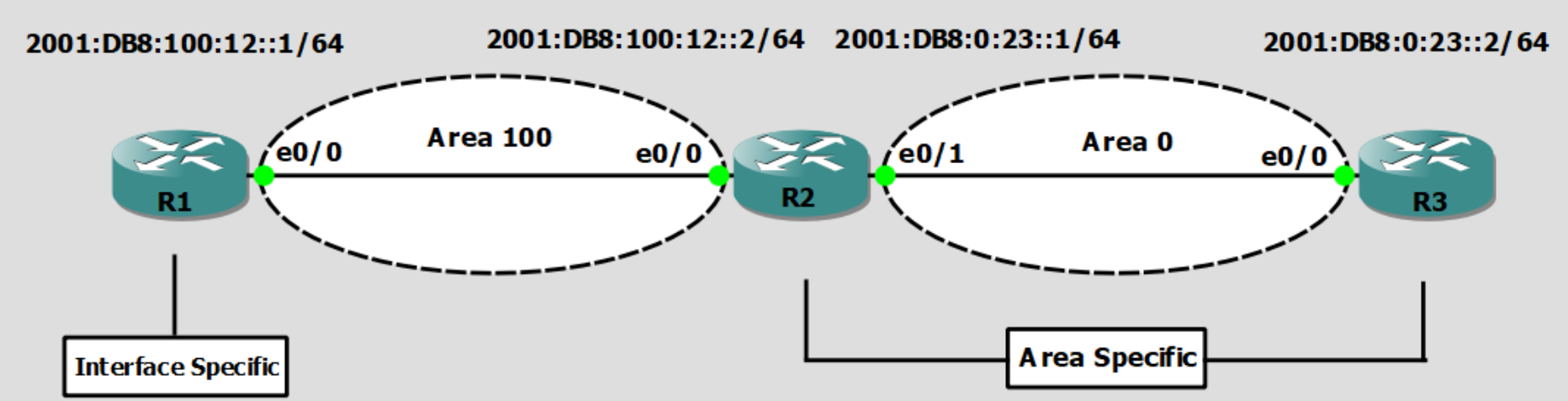
1. OSPF Process Configuration

```
!
router ospfv3 1
 router-id 192.168.2.2
 area 100 authentication ipsec spi 500 sha1 01234567890123456789012345678901234567890
 area 0 authentication ipsec spi 502 sha1 01234567890123456789012345678901234567890
 !
```

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
```

R3 Configuration



1. OSPF Process Configuration

```
!
router ospfv3 1
 router-id 192.168.3.3
 area 0 authentication ipsec spi 500 sha1 01234567890123456789012345678901234567890
 !
```

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
!
```

Conclusion

- The implementation of OSPF authentication helps us to mitigate security threats related to the OSPF routing protocol.
- OSPFv2 authentication is configured using authentication data and authentication type fields found within the OSPFv2 packet header.
- OSPFv3 authentication takes place through the utilization of IP Encapsulating Security Payload and IP authentication header.
- Understanding the different types of authentication supported by OSPF is of great importance to maintain integrity and confidentiality within a business networking environment.

Team Members

Ettienne Nell (20230128@ctucareer.co.za)

Vuyisile Jonas (20230597@ctucareer.co.za)

Willie de Klerk (20230254@ctucareer.co.za)

References

Software Tools Used

learn.microsoft.com. (2024, 09 06). Introduction to Hyper-V on Windows. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/virtualization/hyper-von-windows/about/
www.brandcrowd.com. (2024, 09 06). BrandCrowd Logo Maker. Retrieved from https://www.brandcrowd.com/logo-maker
www.gns3.com. (2024, 09 06). Download GNS3. Retrieved from www.gns3.com: https://www.gns3.com/software/download
www.gns3.com. (2024, 09 06). GNS3 VM for Microsoft Hyper-V. Retrieved from www.gns3.com: https://www.gns3.com/software/download-vm
www.microsoft.com. (2024, 09 06). Microsoft. Retrieved from Windows 11 Professional Edition: https://www.microsoft.com/en-us/d/windows-11-pro/dg7gmgf0d8h4
www.wireshark.org. (2024, 09 06). Wireshark :Download Page. Retrieved from Download Page: https://www.wireshark.org/download/win64/

Reference material

Edgeworth, B., & Lacoste, R. (2023, October). CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide, 2nd Edition | Chapter 6. OSPF, Authentication (Level 1 Section 8). Retrieved 09 06, 2024, from learning.oreilly.com: https://learning.oreilly.com/library/view/ccnp-enterpriseadvanced/9780138217570/ch06.xhtml#ch06lev1sec8

Edgeworth, B., & Lacoste, R. (2023, October). CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide, Second Edition | Chapter 9. OSPFv3, OSPFv3 Configuration (Level 1 Section 4). Retrieved 09 06, 2024, from learning.oreilly.com: https://learning.oreilly.com/library/view/ccnp-enterpriseadvanced/9780138217570/ch09.xhtml#ch09lev1sec4

Ferguson, D., Lindem, A., & Moy, J. (2008, July). RFC 5340 OSPF for IPv6 | 2. Differences from OSPF for IPv4 2.6. Authentication Changes pp. 7 - 8. Retrieved 09 06, 2024, from Internet Engineering Task Force (IETF) Data Tracker: https://datatracker.ietf.org/doc/rfc5340/

Ferguson, D., Lindem, A., & Moy, J. (2008, July). RFC 5340 OSPF for IPv6 |Appendinx A. OSPF Data Formats A.3.1 The OSPF Packet Header p. 60. Retrieved 08 07, 2024, from Internet Engineering Task Force (IETF) Data Tracker: https://datatracker.ietf.org/doc/rfc5340/

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: https://datatracker.ietf.org/doc/rfc2328/

Moy, J. (1998, April). RFC 2328 OSPF Version 2 | Appendix D. Authentication pp. 227- 231. Retrieved 09 06, 2024, from Internet Engineering Task Force (IETF) Data Tracker: https://datatracker.ietf.org/doc/rfc2328/