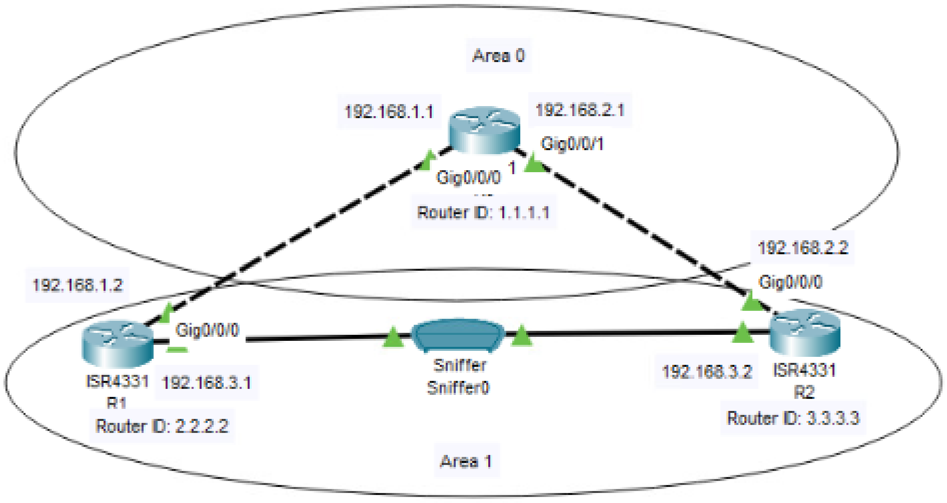
Topology:

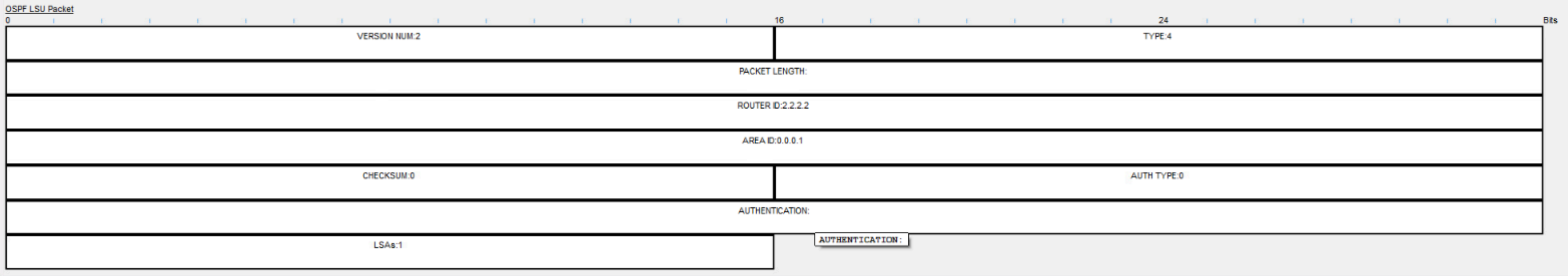


Types of Auth:

Note: In the early stages of our network topology, I used OSPF without any form of authentication. This made the network vulnerable to potential security risks. However, I slowly improved security and began implementing plaintext authentication, which was a fundamental step toward safeguarding the routing updates. Later, I enhanced the security measures by switching to MD5 authentication, which uses a cryptographic hash function to verify the authenticity of OSPF messages. Finally, I implemented SHA-256 authentication for OSPF to ensure the highest level of security.

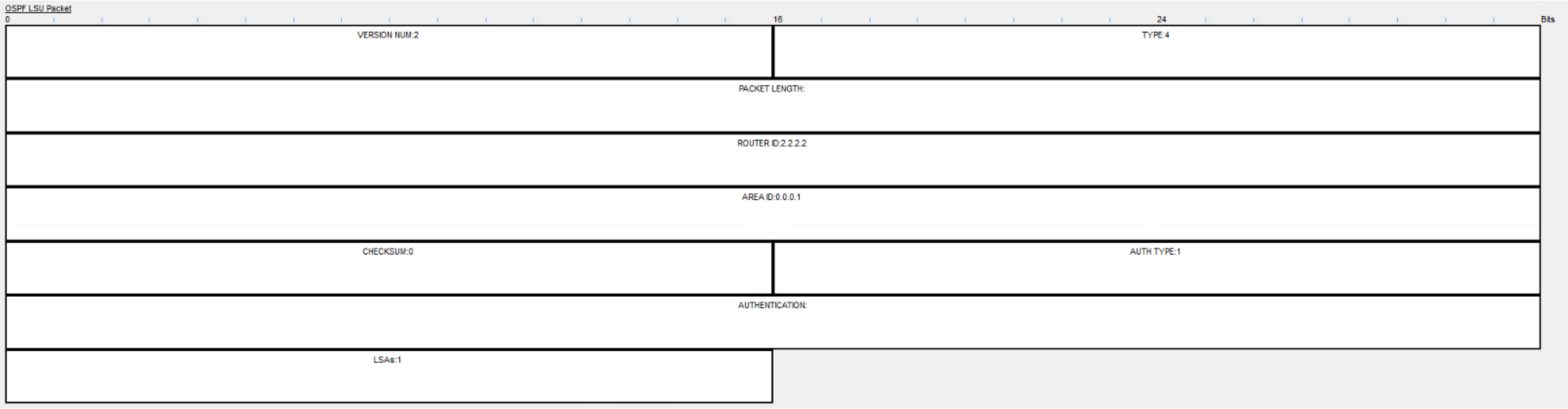
Also, due to the limitation of packet tracer software. I was not able to capture some parts.

1. **No Authentication:** The packet shows an Auth Type of 0, meaning no authentication.


OSPF LSU Packet

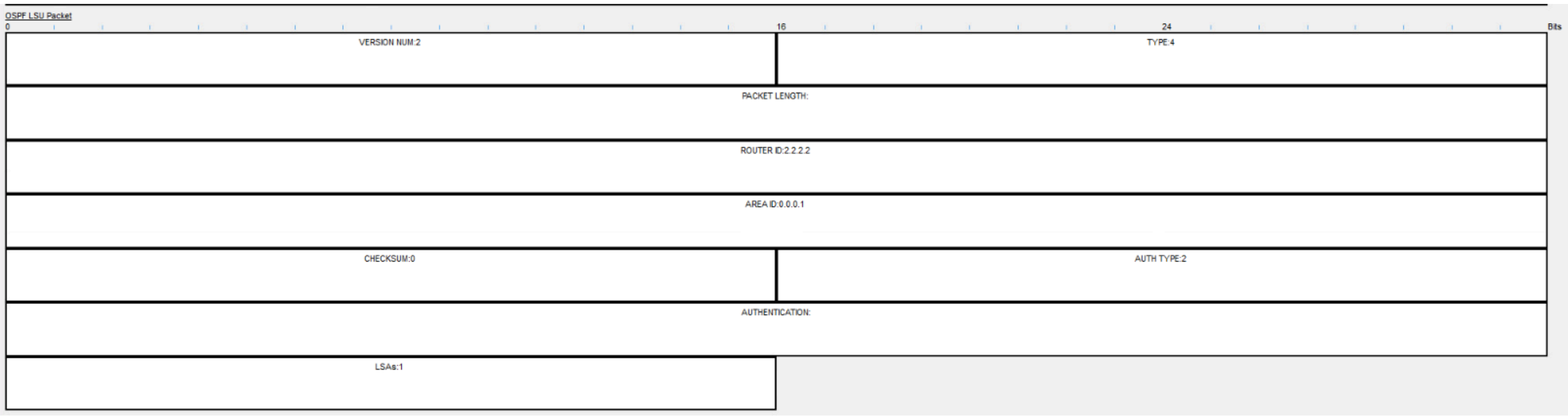
0	16	24	Bits
VERSION NUM:2	TYPE:4		
PACKET LENGTH:			
ROUTER ID:2.2.2.2			
AREA ID:0.0.0.1			
CHECKSUM:0	AUTH TYPE:0		
AUTHENTICATION:			
LSAs:1	AUTHENTICATION:		

2. **Plaintext Authentication:**


OSPF LSU Packet

0	16	24	Bits
VERSION NUM:2	TYPE:4		
PACKET LENGTH:			
ROUTER ID:2.2.2.2			
AREA ID:0.0.0.1			
CHECKSUM:0	AUTH TYPE:1		
AUTHENTICATION:			
LSAs:1			

3. **MD5 Authentication:**



OSPF LSU Packet

0 16 24 Bits

VERSION NUM:2 | TYPE:4

PACKET LENGTH:

ROUTER ID:2.2.2.2

AREA ID:0.0.0.1

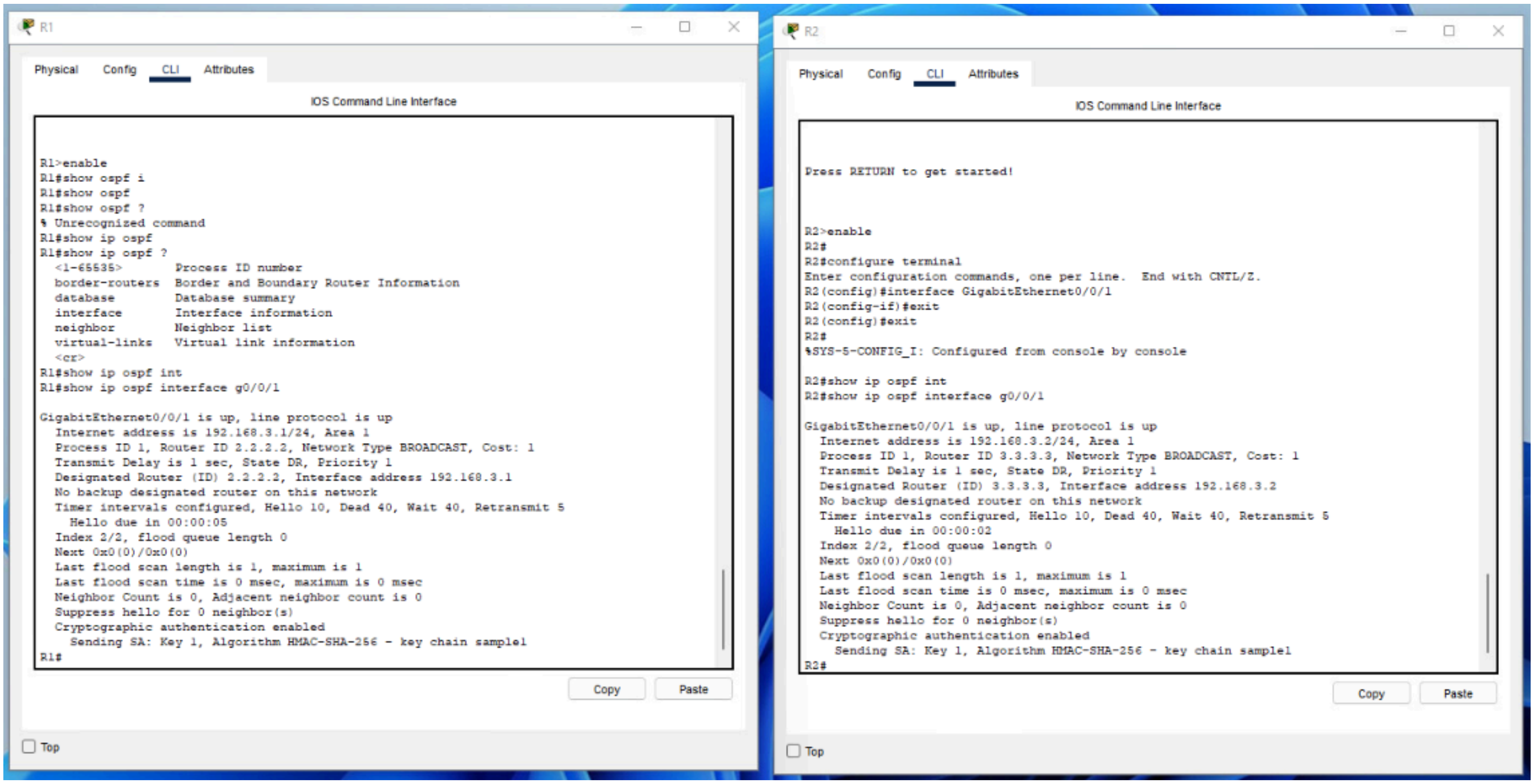
CHECKSUM:0 | AUTH TYPE:2

AUTHENTICATION:

LSAs:1

4. SHA-256 Authentication:

- This type of authentication is fairly new, and due to the limitation of packet tracer, no oscp traffic with this type of authentication was captured. However, the screenshot below shows that this type of authentication was implemented.



```
R1>enable
R1#show ospf i
R1#show ospf
R1#show ospf ?
% Unrecognized command
R1#show ip ospf
R1#show ip ospf ?
  <1-65535>       Process ID number
  border-routers  Border and Boundary Router Information
  database        Database summary
  interface       Interface information
  neighbor        Neighbor list
  virtual-links   Virtual link information
  <cr>
R1#show ip ospf int
R1#show ip ospf interface g0/0/1

GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 1
  Process ID 1, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain sample1
R1#
```

```
Press RETURN to get started!


R2>enable
R2#
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface GigabitEthernet0/0/1
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip ospf int
R2#show ip ospf interface g0/0/1

GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 192.168.3.2/24, Area 1
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.3.2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain sample1
R2#
```

OSPF authentication is used to secure the exchange of routing information between routers. Its purpose is to prevent routers from accepting routing updates from unauthenticated sources, which could lead to network outages or unauthorized redirection of sensitive data. Without authentication, malicious actors could introduce incorrect routing information, potentially causing serious harm to the network.

In Gabi talks from 2011 and 2013, the evolution of OSPF authentication shows a progression towards more secure forms of authentication.:

1. No Authentication (Type 0): By default, OSPF does not have any authentication mechanism enabled. In this mode, OSPF sends routing information without any encryption, making it vulnerable to attacks. Since there's no way to verify the source of the routing updates, they could potentially be malicious or inaccurate. Therefore, it is highly recommended to use authentication mechanisms to ensure the integrity of OSPF updates.

2. Plaintext Authentication (Type 1): Having no authentication is a security risk, that's why plaintext authentication is used in OSPF networks. In this method, a password is included in the OSPF packets, and routers must have matching passwords to accept OSPF updates from each other. However, this method is not completely secure as the password is sent in clear text, which can be intercepted and read by anyone with access to the network.

3. MD5 Authentication (Type 2): This method is a significant improvement in terms of security. Instead of transmitting a password in plain text, a cryptographic hash of the OSPF packet, along with a shared secret key, is created using the MD5 algorithm. The hash is then sent with the packet, and the receiving router uses the same key to generate the hash on its side. If the hashes match, the packet is considered authentic. This technique prevents the password from being exposed on the network, and safeguards against certain types of attacks.

4. SHA-256 Authentication: The most secure method discussed involves using the Secure Hash Algorithm 256 (SHA-256). Although not typically supported in OSPFv2, SHA-256 has been recommended in various talks, including Gabi's, as part of OSPFv3 implementations for IPv6 or newer extensions for IPv4. This method employs a more secure hashing algorithm than MD5, providing enhanced protection against hash collision attacks and ensuring that routing updates are from a trustworthy source.

As network security threats continue to evolve, the mechanisms for securing OSPF have also improved. The use of advanced authentication methods is now more crucial than ever to ensure the security of routing information in enterprise and service provider networks, protecting its confidentiality and integrity.