CSEC 744 Network Security

Name : Shriram Karpoora Sundara Pandian

Course Title : OSPF

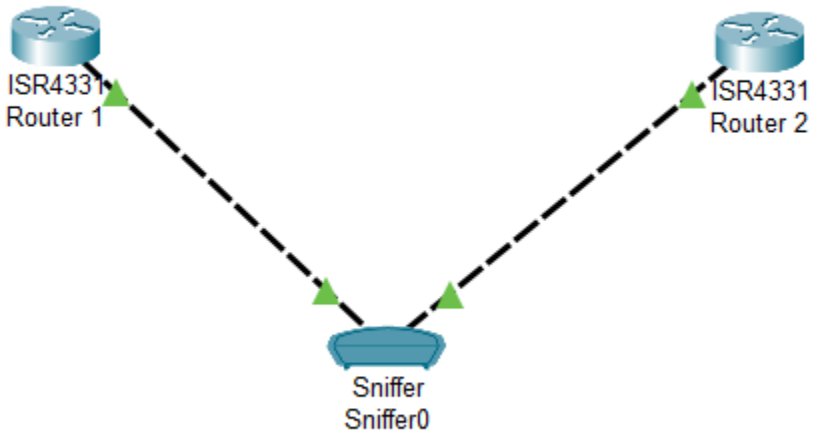
Lab : 9

Type : Freestyle Lab

OSPF (I am using Packet Tracer for this lab)

Topology

- For all four authentication we will have the same topology like below



To keep the demo simple we keep the same topology as it reduces the confusion between configuring routers for authentication.

- The setting for the IP address is also same for all the topologies:

i) For Router 1

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#int g0/1
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
```

For router 2:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/1
Router(config-if)#ip address 192.168.2.1
% Incomplete command.
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#int g0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
```

No authentication

OSPF is by default without any authentication, so we will simply configure the OSPF in this step.

Router 1

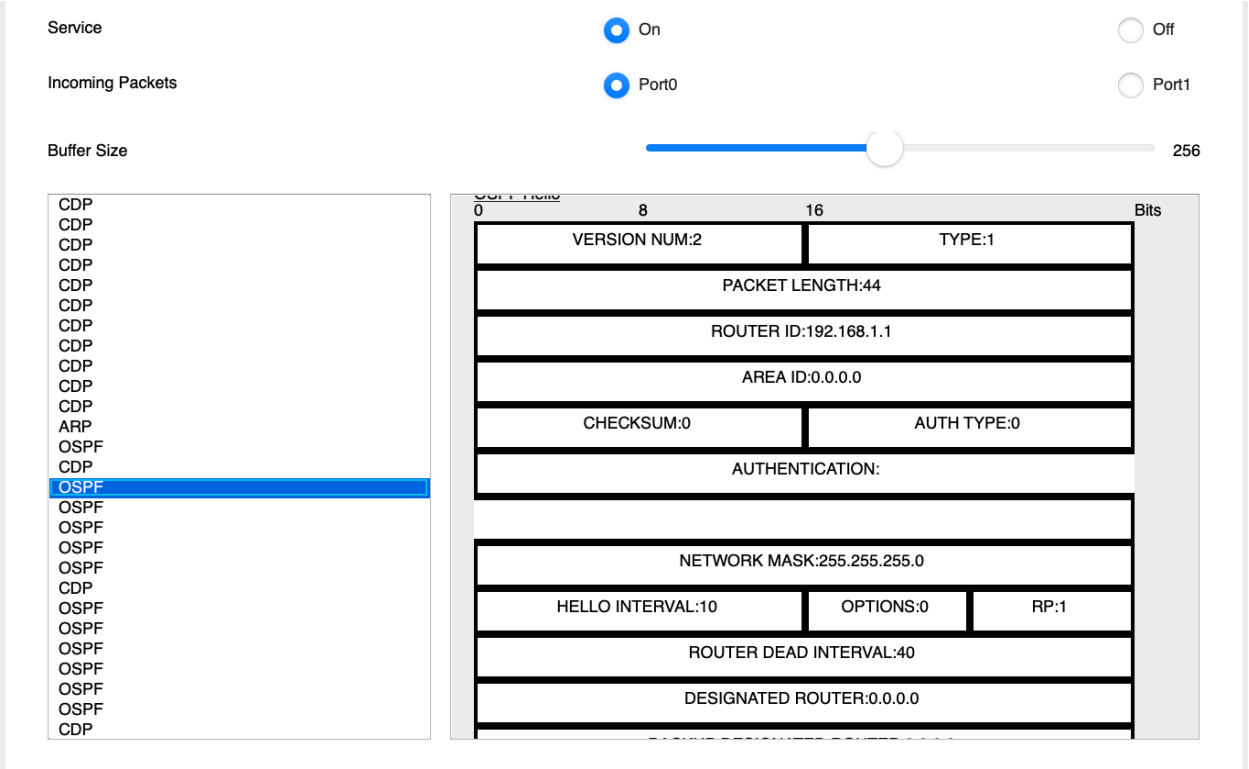
```
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.1 0.0.0.255 area 0
Router(config-router)#exit
```

Router 2

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.1 0.0.0.255 area 0
Router(config-router)#exit
```

No Authentication capture on sniffer

We can see that we got the capture of OSPF with the Auth Type 0 which is authentication null.



Plaintext Authentication

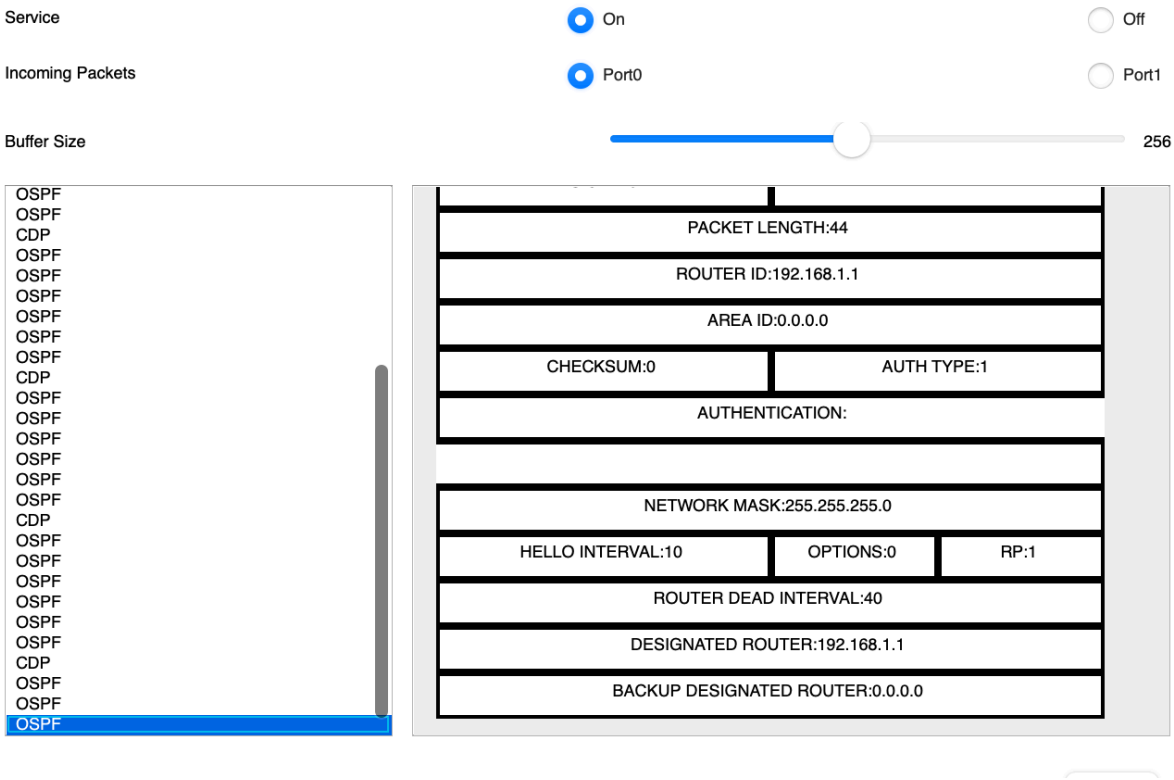
- For each router set the ospf and enable the area authentication.
- For specific interface initialize the plaintext authentication key which is plain text in this case.

  For Router 1

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#area 0 authentication
Router(config-router)#
Router(config-router)#exit
Router(config)#int g0/0
Router(config-if)#ip ospf authentication-key netsec
Router(config-if)#exit
```

For Router 2

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#area 0 authentication
Router(config-router)#
Router(config-router)#exit
Router(config)#int g0/0
Router(config-if)#ip ospf authentication-key netsec
Router(config-if)#exit
```



We can see the auth type 1 abovewhich is plaintext authentication

MD5 Authentication

- For MD5 authentication we will enable message-digest on the area configuration of the ospf first.
- Then we will set the message-digest key value and password which will become the MD5 hash.
- We have to set this configuration on both the routers.

Router 1 configuration

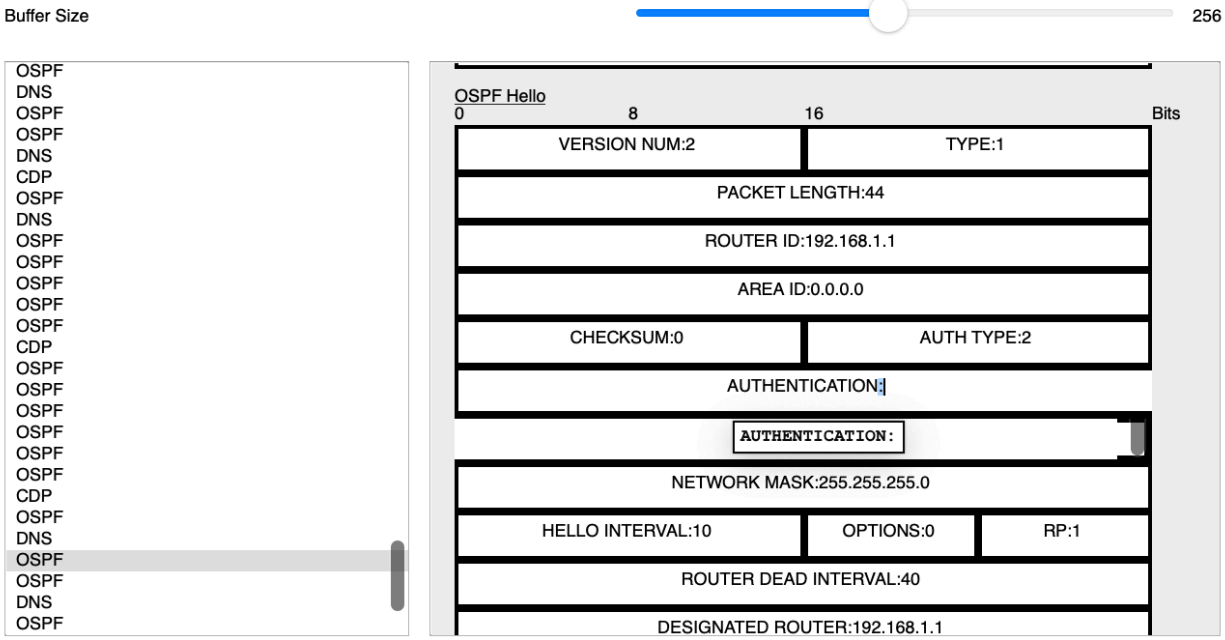
```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#area 0 authentication message-digest
Router(config-router)#
Router(config-router)#
Router(config-router)#exit
Router(config)#int g0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip ospf message-digest-key 1 md5 check
Router(config-if)#exit
```

Router 2 Configuration

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#area 0 authentication message-digest
Router(config-router)#exit
Router(config)#int g0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#ip ospf message-digest-key 1 md5 check
Router(config-if)#exit
```

Sniffer

We can see that we got auth type 2 authentication which is md5



We can see that Message digest is enabled on the ospf interface of the router.

```
Router#show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address
192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:03
  Index 1/1, 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)
  Message digest authentication enabled
    Youngest key id is 1
```

HMAC and SHA 256:

Router 1 configuration:

```
Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.1 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
Router(config)#
Router(config)#key chain sha256
Router(config-keychain)#key 1
Router(config-keychain-key)#?
  accept-lifetime          Set accept lifetime of key
  cryptographic-algorithm  Set cryptographic authentication algorithm
  exit                      Exit from key-chain key configuration mode
  key-string               Set key string
  no                       Negate a command or set its defaults
  send-lifetime            Set send lifetime of key
Router(config-keychain-key)#cryptographic-algorithm ?
  hmac-sha-1    HMAC-SHA-1 authentication algorithm
  hmac-sha-256  HMAC-SHA-256 authentication algorithm
  hmac-sha-384  HMAC-SHA-384 authentication algorithm
  hmac-sha-512  HMAC-SHA-512 authentication algorithm
  md5           MD5 authentication algorithm
Router(config-keychain-key)#cryptographic-algorithm hmac-sha-256
Router(config-keychain-key)#key-string netseclab
Router(config-keychain-key)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0/0
Router(config-if)#ip ospf authentication key-chain sha256
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Router 2 Configuration:

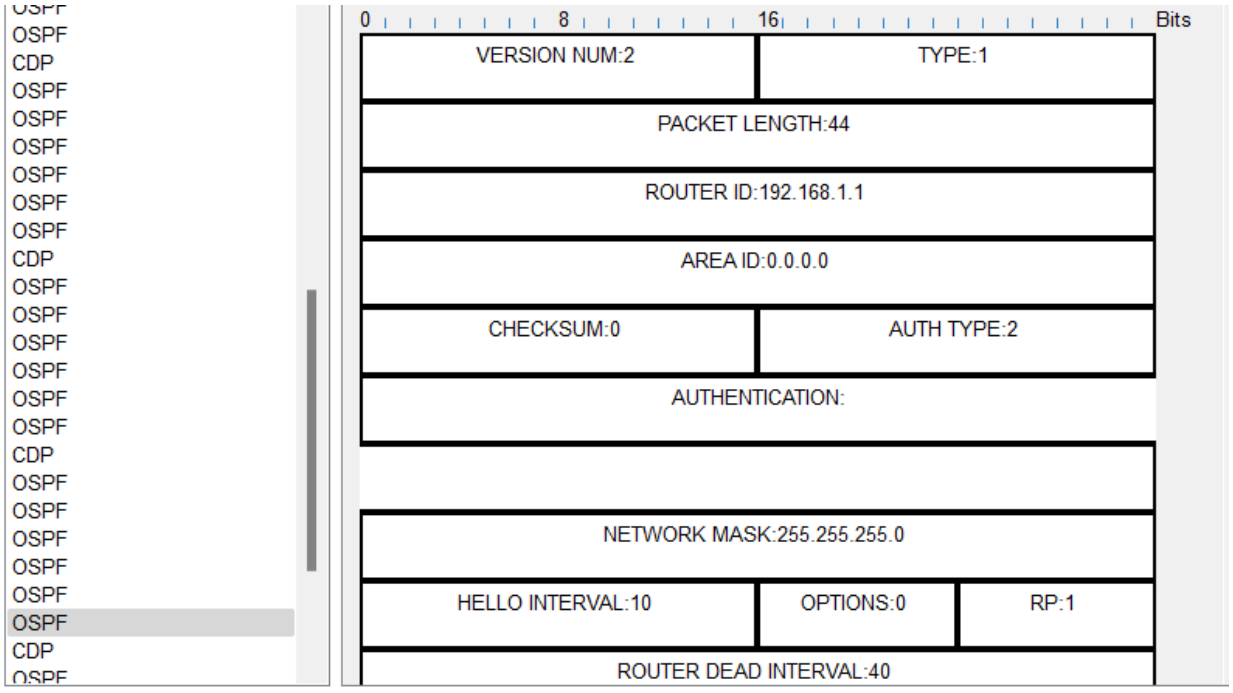
```
Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.1 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
Router(config)#
Router(config)#key chain sha256
Router(config-keychain)#key 1
Router(config-keychain-key)#cryptographic?
cryptographic-algorithm
Router(config-keychain-key)#cryptographic-algorithm hmac-sha-256
Router(config-keychain-key)#key string netseclab
Router(config-keychain-key)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0/1
Router(config-if)#ip ospf authentication key-chain sha256
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

We can notice from the below screenshot that Cryptographic sha256 algorithm is enabled successfully.

```
Router#show ip ospf interface g0/0/0

GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1, 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 sha256
```



Step by step guide below.

- For Topology and IP address configuration we will have everything the same.
- We will make changes by the following.
  On the router follow the steps accordingly
- After we give “configure terminal” for any router we have to give the following commands:
    1. key chain sha256 (any name)
    2. Key 1 (any key value, user customizable)
    3. Cryptographic-algorithm hmac-sha-256 (we can configure 512 too)
    4. key-string netseclab (Instead of netsec_lab configure any word)
    5. end.

- For the interface, we have to give the following:
    1. Interface g0/0 (or g0/1)
    2. Ip ospf authentication key-chain sha256 (custom name you configured above)
    3. end

Following these steps we can configure the HMAC and SHA authentication.

OSPF

It is a widely used link-state routing protocol in networking devices. The fullform for OSPF is Open Short Path First. It produces LSA (Link State Advertisement) which will be sent to the routers in their path to acknowledge the link state. OSPF works based on the bandwidth and delay. The best feature of OSPF is its authentication mechanism. It has four different types of authentication actually 3:

- Null (So no authentication)
- Plaintext Authentication
- MD5
- HMAC SHA (Key size may vary depending on your choice 256 or 512)

1. Null is a default setting in OSPF which has no authentication. It is not good for real life scenarios in enterprise or production environments because it makes the routers vulnerable to attacks. So this should be avoided at all times.
2. Plaintext Authentication is better than Null authentication, but still is not a good form of authentication because it may be vulnerable to brute force attacks. If a session is replayed or eavesdropping will showcase the passwords as it travels in LSA as a plaintext.
3. MD5 Authentication is much better than Plaintext as passwords will be hashed before sending the LSA, but for today's standards MD5 has a lot of collisions and its not good in collision resistance. So become more vulnerable if the attacker is more advanced in some cases. So it must be avoided in most cases possible.
4. HMAC SHA Authentication is the best and collision resistant as compared to our today's standards. It is better to use larger key lengths like 512 for future proof and security.

Overall the difference between these authentication types depends on their resistance and ability of their security strength. So using HMAC SHA is preferred for most routers if the data of the organization is very much important.

Reason for OSPF Authentication:

- For preventing the information about the network topology and other network information because OSPF LSA give away a lot of important information.
- To prevent the attacker from connecting his router to the organization and try to attack. Because without verifying his router, he can't do anything, which is a good thing in the first place.
- Also a lot of routing attacks can be mitigated and layer 3 will be secured well.

Gabi's talk in 2011 and 2013 created the awareness of routing protocol attacks and significance of the authentication of OSPF protocol. Also his talk created the awareness of looking into layer 2 and layer 3 as it has a lot of potential for vulnerabilities and attacks.