OSPF Authentication

OSPFv2 — for IPv4 only

Cleartext authentication

```
R1(config)#interface Gi0/0
R1(config-if)#ip ospf authentication
R1(config-if)#ip ospf authentication-key P4SSW0RD
```

MD5 or SHA cryptographic hash

```
R1(config)#interface Gi0/0
R1(config-if)#ip ospf authentication message-digest
R1(config-if)#ip ospf message-digest-key 1 md5 P4SSW0RD
```

```
R1(config)#router ospf 10
R1(config-router)#area 0 authentication message-digest
R1(config-router)#exit
R1(config)#interface Gi0/0
R1(config-if)#ip ospf message-digest-key 1 md5 P4SSW0RD
```

```
R1(config)#key chain EXAMPLE-KEYCHAIN
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string P4SSW0RD
R1(config-keychain-key)#cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)#exit
R1(config-keychain)#exit
R1(config)#interface Gi0/0
R1(config-if)# ip ospf authentication key-chain EXAMPLE-KEYCHAIN
```

Three different configuration options can be used to apply OSPFv2 authentication with MD5/SHA hash. It is important that the key number value matches on neighboring OSPF routers because the hash is created based on the key number and the authentication password combined.

OSPFv2 Authentication Types

No authentication	Null (0)
Cleartext password	Simple password (1)
Message digest	Cryptographic (2)

OSPFv3 — for IPv6 and IPv4

IPSec Authentication Header with MD5 or SHA

```
R1(config)#interface Gi0/0
R1(config-if)#ipv6 ospf authentication ipsec spi 256 md5 ABCDEF123456789ABCDEF123456789AB
```

```
R1(config)#interface Gi0/0
R1(config-if)#ospfv3 authentication ipsec spi 256 sha1 ABCDEF123456789ABCDEF123456789ABCDEF1234
```

OSPFv3 supports IPSec Authentication Header with the MD5 or the SHA cryptographic hash. The traditional (old-style) or the new-style OSPFv3 configuration can be applied.

Authentication Trailer with MD5/SHA (no IPSec) for Hello or DBD

```
R1(config)#key chain EXAMPLE-KEYCHAIN
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string P4SSW0RD
R1(config-keychain-key)#cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)#exit
R1(config-keychain)#exit
R1(config)#interface Gi0/0
R1(config-if)#ospfv3 authentication key-chain EXAMPLE-KEYCHAIN
R1(config-if)#end
R1#show ospfv3 neighbor detail | sec Options
    Options is 0x000413 in Hello (V6-Bit, E-Bit, R-Bit, AT-Bit)
    Options is 0x000013 in DBD (V6-Bit, E-Bit, R-Bit)
```

```
R1(config)#key chain EXAMPLE-KEYCHAIN
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string P4SSW0RD
R1(config-keychain-key)#cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)#exit
R1(config-keychain)#exit
R1(config)#router ospfv3 10
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#area 0 authentication key-chain EXAMPLE-KEYCHAIN
R1(config-router-af)#exit
R1(config-router)#exit
R1(config)#interface Gi1
R1(config-if)#ospfv3 authentication key-chain EXAMPLE-KEYCHAIN
R1(config-if)#end
R1#show ospfv3 neighbor detail | sec Options
    Options is 0x000413 in Hello (V6-Bit, E-Bit, R-Bit, AT-Bit)
    Options is 0x000413 in DBD (V6-Bit, E-Bit, R-Bit, AT-Bit)
```

Authentication Trailer can be configured for the OSPFv3 Hello packets and for Database Description (DBD) packets. The ”AT-bit” indicates the use of OSPFv3 Authentication Trailer.