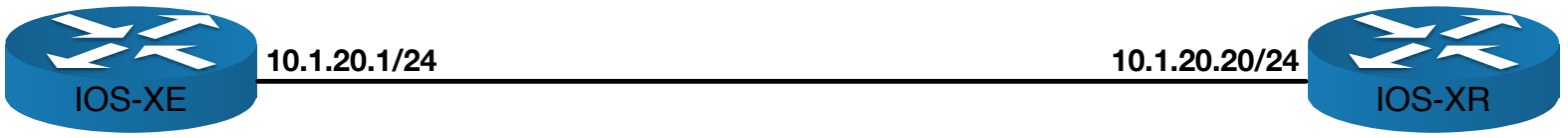
OSPFv2 MD5
Clear Text




```
router ospf 100
 router-id 1.1.1.1
 passive-interface Loopback0
!
interface GigabitEthernet1.120
 encapsulation dot1Q 120
 ip address 10.1.20.1 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key PA55W0RD
 ip ospf 100 area 0
end
```

```
router ospf 100
 router-id 20.20.20.20
 address-family ipv4 unicast
 area 0
  interface Loopback0
   passive enable
  !
  interface GigabitEthernet0/0/0/0.120
   authentication
   authentication key PA55W0RD
  !
 !
```

```
R1#show ip ospf 1 interface Gi1.120
GigabitEthernet1.120 is up, line protocol is up
  Internet Address 10.1.20.1/24, Interface ID 14, Area 0
  Attached via Interface Enable
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 20.20.20.20, Interface address 10.1.20.20
  Backup Designated router (ID) 1.1.1.1, Interface address 10.1.20.1
  Flush timer for old DR LSA due in 00:01:40
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Can be protected by per-prefix Loop-Free FastReroute
  Can be used for per-prefix Loop-Free FastReroute repair paths
  Not Protected by per-prefix TI-LFA
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 5 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 20.20.20.20  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Simple password authentication enabled
```

OSPFv2 MD5 Authentication

```
router ospf 100
 router-id 1.1.1.1
 area 0 authentication message-digest*
 passive-interface Loopback0
!
interface GigabitEthernet1.120
 encapsulation dot1Q 120
 ip address 10.1.20.1 255.255.255.0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 PA55W0RD
 ip ospf 100 area 0
end
```

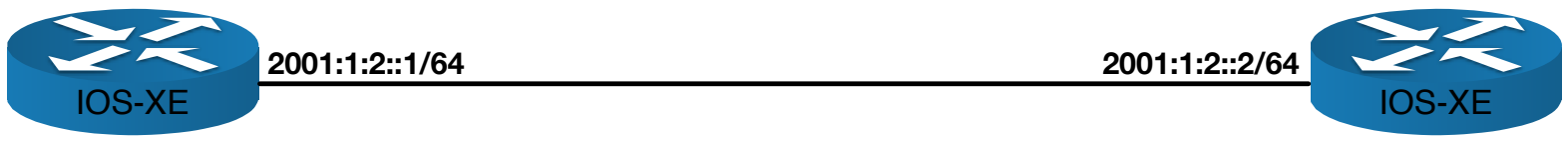
*Area command necessitates that authentication be configured for any neighborships in this area.

```
router ospf 100
 router-id 20.20.20.20
 address-family ipv4 unicast
 area 0
  authentication message-digest*
  interface Loopback0
   passive enable
  !
  interface GigabitEthernet0/0/0/0.120
   authentication message-digest
   message-digest-key 1 md5 encrypted 12302B42222A3F37
  !
 !
```

```
R1#show ip ospf 1 interface Gi1.120
GigabitEthernet1.120 is up, line protocol is up
  Internet Address 10.1.20.1/24, Interface ID 14, Area 0
  Attached via Interface Enable
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 20.20.20.20, Interface address 10.1.20.20
  Backup Designated router (ID) 1.1.1.1, Interface address 10.1.20.1
  Flush timer for old DR LSA due in 00:02:55
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Can be protected by per-prefix Loop-Free FastReroute
  Can be used for per-prefix Loop-Free FastReroute repair paths
  Not Protected by per-prefix TI-LFA
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 5 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 20.20.20.20  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
    Youngest key id is 1
```

OSPFv3 IPSec using Authentication Header

OSPFv3 IPsec ESP Encryption and Authentication is not supported in regular IOS until software release 12.4(9)T




```
router ospfv3 1
 router-id 1.1.1.1
 log-adjacency-changes detail
 area 0 authentication ipsec spi 500 sha1 <<40_HEX_CHARS>>*
 !
 address-family ipv6 unicast
  passive-interface Loopback0
 exit-address-family
!
interface GigabitEthernet1
 ipv6 address 2001:1:2::2/64
 ospfv3 1 ipv6 area 0
end
```

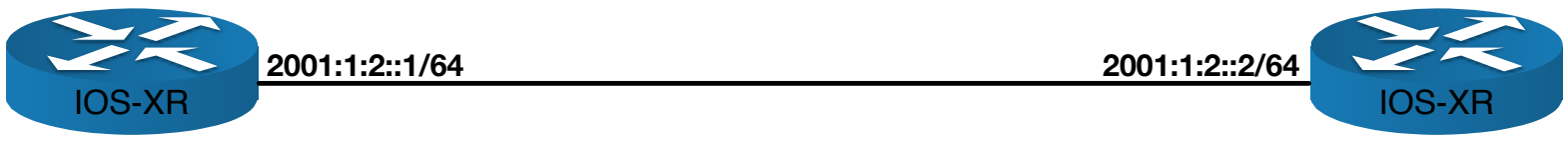
```
router ospfv3 1
 router-id 2.2.2.2
 log-adjacency-changes detail
 !
 address-family ipv6 unicast
  passive-interface Loopback0
 exit-address-family
!
interface GigabitEthernet1
 ipv6 address 2001:1:2::2/64
 ospfv3 authentication ipsec spi 500 sha1 <<40_HEX_CHARS>>
 ospfv3 1 ipv6 area 0
end
```

*Area command necessitates that authentication be configured for any neighborships in this area.

```
R1#show crypto ipsec sa

interface: GigabitEthernet1
    Crypto map tag: GigabitEthernet1-OSPF-MAP, local addr FE80::5200:FF:FE03:0

   IPsecv6 policy name: OSPFv3-500

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (FE80::/10/89/0)
   remote ident (addr/mask/prot/port): (::/0/89/0)
   current_peer FF02::5 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 185, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 185, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: FE80::5200:FF:FE03:0,
     remote crypto endpt.: FF02::5
     plaintext mtu 1412, path mtu 1436, ipv6 mtu 1436, ipv6 mtu idb GigabitEthernet1
     current outbound spi: 0x1F4(500)
     PFS (Y/N): N, DH group: none

     inbound esp sas:

     inbound ah sas:
      spi: 0x1F4(500)
        transform: ah-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2013, flow_id: CSR:13, sibling_flags FFFFFFFF80000019, crypto map: GigabitEthernet1-OSPF-MAP
        sa timing: remaining key lifetime (sec): 0
        Kilobyte Volume Rekey has been disabled
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:
      spi: 0x1F4(500)
        transform: ah-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2014, flow_id: CSR:14, sibling_flags FFFFFFFF80000019, crypto map: GigabitEthernet1-OSPF-MAP
        sa timing: remaining key lifetime (sec): 0
        Kilobyte Volume Rekey has been disabled
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     outbound pcp sas:
```

OSPFv3 IPSec using ESP Encryption and Authentication Header

OSPFv3 on XR only supports IPv6, so this example shows IPv6 only.




```
router ospfv3 1
 router-id 1.1.1.1
 log adjacency changes detail
 area 0
   encryption ipsec spi 500 esp aes 256 <<64_HEX_CHARS>
      authentication sha1 password <<40_HEX_CHARS>> *
  interface Loopback0
   passive
  !
  interface GigabitEthernet0/0/0/1
  !
 !
!
```

```
router ospfv3 1
 router-id 2.2.2.2
 log adjacency changes detail
 area 0
  interface Loopback0
   passive
  !
  interface GigabitEthernet0/0/0/1
   encryption ipsec spi 500 esp aes 256 <<64_HEX_CHARS>
      authentication sha1 password <<40_HEX_CHARS>>
  !
 !
!
```

*Area command necessitates that authentication be configured for any neighborships in this area.

```
RP/0/0/CPU0:XR1#show crypto ipsec sa
Sun Apr 12 20:24:38.735 UTC

SA id:          2
Node id:        0/0/CPU0
SA Type:        MANUAL
SA State:       UP
Ref Count:      2
outbound esp sas:
        spi: 0x1F4(500)
        transform: esp-256-aes esp-sha-hmac
        in use settings = Transport
        no sa timing
        sa DPD disabled
        sa anti-replay (HW accel): Disable, window 0
inbound esp sas:
        spi: 0x1F2(500)
        transform: esp-256-aes esp-sha-hmac
        in use settings = Transport
        no sa timing
        sa DPD disabled
        sa anti-replay (HW accel): Disable, window 0
RP/0/0/CPU0:XR1#
```