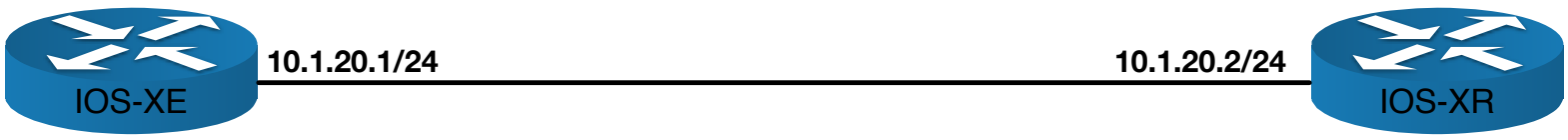
ISIS LSP, CSNP and PSNP Authentication using MD5

IS-IS has two modes of authentication, each of which can specify level 1 or level 2:

> Authenticating Hello Packets (IIHs)
> Authenticating other control packets - LSP, CSNPs and PSNPs.

This page shows the latter. This authentication is based on an additional TLV. Auth failure of LSP, CSNPs and PSNPs will not prevent the neighborship coming up. But they will prevent the LSPs being properly exchanged and this prevents synchronisation.




```
router isis 1
 net 49.0001.0000.0000.0001.00
 authentication mode md5 level-2
 authentication key-chain KEY1 level-2
 metric-style wide
 log-adjacency-changes all
 passive-interface Loopback0
 bfd all-interfaces
 mpls ldp sync
 mpls ldp autoconfig
!
!
interface GigabitEthernet1
 ip address 10.1.20.1 255.255.255.0
 ip router isis 1
 bfd interval 250 min_rx 250 multiplier 3
 isis network point-to-point
end
!
key chain KEY1
 key 1
  key-string PA55W0RD
```

```
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0002.00
 log adjacency changes
 lsp-password hmac-md5 PA55W0RD
 address-family ipv4 unicast
  metric-style wide
  mpls ldp auto-config
 !
 interface Loopback0
  passive
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/0
  bfd minimum-interval 250
  bfd multiplier 3
  bfd fast-detect ipv4
  point-to-point
  address-family ipv4 unicast
   mpls ldp sync level 2
  !
 !
```

There isn't a direct **show** command to verify IS-IS authentication is enabled (except for **show run**), however XR can verify authentication of LSP, PSNP and CSNP packets as follows…

```
RP/0/0/CPU0:XR1#show isis trace only detailed | inc AUTH
Tue Apr 14 20:08:10.982 UTC
Apr 14 12:18:24.813 isis/1/det 0/0/CPU0 t1  CFG_LEVEL_VERIFY_AREA_AUTH L0
Apr 14 12:18:30.193 isis/1/det 0/0/CPU0 t8  UPD_PSNP_SEND_ADD_AUTH L2 Gi0/0/0/0
Apr 14 12:18:30.603 isis/1/det 0/0/CPU0 t8  UPD_CSNP_SEND_ADD_AUTH L2 Gi0/0/0/0
Apr 14 12:18:31.363 isis/1/det 0/0/CPU0 t8  UPD_PSNP_SEND_ADD_AUTH L2 Gi0/0/0/0
Apr 14 12:18:33.282 isis/1/det 0/0/CPU0 t8  UPD_PSNP_SEND_ADD_AUTH L2 Gi0/0/0/0
<<output committed for brevity>>
Apr 14 12:24:59.616 isis/1/det 0/0/CPU0 t8  UPD_PSNP_SEND_ADD_AUTH L2 Gi0/0/0/0
Apr 14 12:25:00.196 isis/1/det 0/0/CPU0 t8  UPD_PSNP_SEND_ADD_AUTH L2 Gi0/0/0/0
Apr 14 12:25:02.106 isis/1/det 0/0/CPU0 t8  UPD_PSNP_SEND_ADD_AUTH L2 Gi0/0/0/0
Apr 14 12:25:07.385 isis/1/det 0/0/CPU0 t8  UPD_LSP_UPDATE_AUTH Upd Type: LSP L2 0000.0000.0019.00-00
Apr 14 12:25:07.485 isis/1/det 0/0/CPU0 t8  UPD_LSP_UPDATE_AUTH Upd Type: LSP L2 0000.0000.0019.00-00
Apr 14 12:25:07.695 isis/1/det 0/0/CPU0 t8  UPD_LSP_UPDATE_AUTH Upd Type: LSP L2 0000.0000.0019.00-00
Apr 14 12:25:08.115 isis/1/det 0/0/CPU0 t8  UPD_LSP_UPDATE_AUTH Upd Type: LSP L2 0000.0000.0019.00-00
```

… and IOS may show a log entry as follows…

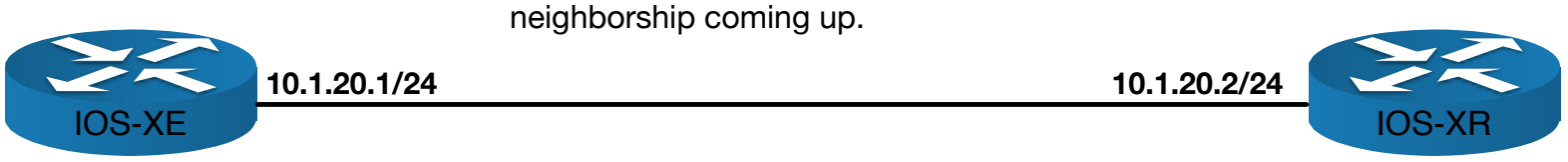
```
%CLNS-4-AUTH_FAIL: ISIS: LSP authentication failed
```

ISIS Hello Authentication using MD5

IS-IS has two modes of authentication, each of which can specify level 1 or level 2:

> Authenticating Hello Packets (IIHs)
> Authenticating other control packets - LSP, CSNPs and PSNPs.

This page shows the former. IIH auth failure of will prevent the neighborship coming up.




```
router isis 1
 net 49.0001.0000.0000.0001.00
 metric-style wide
 log-adjacency-changes all
 passive-interface Loopback0
 bfd all-interfaces
 mpls ldp sync
 mpls ldp autoconfig
!
!
interface GigabitEthernet1
 ip address 10.1.20.1 255.255.255.0
 ip router isis 1
 bfd interval 250 min_rx 250 multiplier 3
 isis network point-to-point
 isis authentication mode md5
 isis authentication key-chain KEY1
end
!
key chain KEY1
 key 1
  key-string PA55W0RD
```

```
router isis 1
 is-type level-2-only
 net 49.0001.0000.0000.0002.00
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide
  mpls ldp auto-config
 !
 interface Loopback0
  passive
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/0
  bfd minimum-interval 250
  bfd multiplier 3
  bfd fast-detect ipv4
  point-to-point
  hello-password hmac-md5 PA55W0RD
  address-family ipv4 unicast
   mpls ldp sync level 2
  !
 !
```

Depending on the XR version, you might be able to enter the **`show isis database detail <lspid>`** command to verify authentication. Look for Auth in the output. Alertnaveiy on XR you can verify authentication of IIH packets as follows…

```
RP/0/0/CPU0:XR1#show isis trace only hello  | in Gi0/0/0/0 | inc AUTH
Tue Apr 14 20:43:07.829 UTC
Apr 14 20:20:32.221 isis/1/hlo 0/0/CPU0 t7  ADJ_SEND_P2P_ADD_AUTH Gi0/0/0/0 L2
Apr 14 20:20:40.921 isis/1/hlo 0/0/CPU0 t7  ADJ_SEND_P2P_ADD_AUTH Gi0/0/0/0 L2
Apr 14 20:20:49.870 isis/1/hlo 0/0/CPU0 t7  ADJ_SEND_P2P_ADD_AUTH Gi0/0/0/0 L2
Apr 14 20:20:58.180 isis/1/hlo 0/0/CPU0 t7  ADJ_SEND_P2P_ADD_AUTH Gi0/0/0/0 L2
Apr 14 20:21:05.809 isis/1/hlo 0/0/CPU0 t7  ADJ_SEND_P2P_ADD_AUTH Gi0/0/0/0 L2
Apr 14 20:21:15.648 isis/1/hlo 0/0/CPU0 t7  ADJ_SEND_P2P_ADD_AUTH Gi0/0/0/0 L2
Apr 14 20:21:25.338 isis/1/hlo 0/0/CPU0 t7  ADJ_SEND_P2P_ADD_AUTH Gi0/0/0/0 L2
Apr 14 20:21:33.447 isis/1/hlo 0/0/CPU0 t7  ADJ_SEND_P2P_ADD_AUTH Gi0/0/0/0 L2
Apr 14 20:21:41.947 isis/1/hlo 0/0/CPU0 t7  ADJ_SEND_P2P_ADD_AUTH Gi0/0/0/0 L2
```

… or XR logging message will show this if a failure occurs:

```
RP/0/0/CPU0:Apr 14 20:20:37.021 : isis[1010]: %ROUTING-ISIS-5-AUTH_FAILURE_DROP :
Dropped P2P IIH from GigabitEthernet0/0/0/0.419 SNPA 5000.0004.0000 due to
authentication TLV not found
```

In IOS if regular adjacency logging is enabled a failure log will look like this.

```
%CLNS-4-AUTH_FAIL: ISIS: Serial IIH authentication failed
```

IOS can also use **`debug isis authentication information`**. A failure will show up as follows…

```
ISIS-AuthInfo (1): No live key, reject the packet
```

…and if auth is succeeding the debug will show the following…

```
ISIS-AuthInfo (1): IIH no change, use the same hmac value
```