```
Target : 00:1a:1e:08:42:7e

show vpn status

vpn primary external ip            :xx.xx.xx.xx
vpn primary tunnel ip              :0.0.0.0
vpn backup  external ip            :0.0.0.0
vpn backup  tunnel ip              :0.0.0.0
vpn current used external ip       :xx.xx.xx.xx
vpn current remote tunnel ip       :0.0.0.0
vpn current ap's tunnel ip         :0.0.0.0
vpn is preempt status              :False
vpn hold down period               :600
vpn status                         :down

vpn primary external ip            :xx.xx.xx.xx
vpn primary tunnel ip              :0.0.0.0
vpn backup  external ip            :0.0.0.0
vpn backup  tunnel ip              :0.0.0.0
vpn current used external ip       : xx.xx.xx.xx
vpn current remote tunnel ip       :0.0.0.0
vpn current ap's tunnel ip         :0.0.0.0
vpn is preempt status              :False
vpn hold down period               :600
vpn status                         :down
end of show vpn status
============================================================

show upgrade info

Image Upgrade Progress
----------------------
Mac                IP Adress    AP Class  Status    Image Info  Error Detail
---                ---------    --------  ------    ----------  ------------
00:1a:1e:08:42:7e  172.16.1.97  Orion     image-ok  image file  none
end of show upgrade info
============================================================

show log upgrade
----------Download log start----------
download log not available
----------Download log end------------
Download status: incomplete
----------Upgrade log start----------
upgrade log not available
----------Upgrade log end------------
Upgrade status: upgrade status not available
end of show log upgrade
============================================================

show log rapper

 spi={e49abd9f3c52b140 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to xx.xx.xx.xx [4500] (1.0)
(pid:3506)  time:2012-09-20 13:31:59
```

```
#RECV 337 bytes from xx.xx.xx.xx [4500] (1.0)
(pid:3506)  time:2012-09-20 13:31:59

 spi={e49abd9f3c52b140 df6f66366c935ae5} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   NAT_D (peer/NAT): 12 c3 e8 e9 17 5d 70 60 a3 97 4b 76 52 49 0c bc
29 eb 6a 80
   Notify: NAT_DETECTION_DESTINATION_IP
   NAT_D (us/NAT): 65 6e 3b b4 56 58 10 77 f3 61 29 38 b7 37 ad e8
10 7d f6 42
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i 5b 9f c3 33 61 89 b6 fc 72 74 19 15 36 4c 5c b1
48 13 44 64
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={e49abd9f3c52b140 df6f66366c935ae5} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to xx.xx.xx.xx [4500] (3.0)
(pid:3506)  time:2012-09-20 13:32:02

Sending last fragment, size = 432


#RECV 80 bytes from xx.xx.xx.xx [4500] (3.0)
(pid:3506)  time:2012-09-20 13:32:02

 spi={e49abd9f3c52b140 df6f66366c935ae5} np=E{N}
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=9f0f4300)
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0

IKE_SA [v2 I] (id=0x9078f0c4) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952

Switching output streamget_ike_version: Use IKE Version 2
```

```
papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:3537)  time:2012-09-20 13:32:02
 seconds.
Before getting Certs
TPM enabled
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1580
Decode PEM Key length :0
testHostKeys : status 0

testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BF0002873::00:1a:1e:08:42:7e}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ac100161
IKE_EXAMPLE: Socket created on 172.16.1.97[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
(pid:3537)  time:2012-09-20 13:32:02
 SA_INIT dest= xx.xx.xx.xx
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): 78 db 7a 33 79 6b ba 64 a4 29 8a 86 02 ae 40 92
34 55 0e 30
   NAT_D (peer): 88 c9 0d 02 30 68 fd 39 6d fd bf 58 38 c3 fc 54
```

```
8a 1f 1e 42
 spi={6b19ba186d5692b3 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to xx.xx.xx.xx [4500] (0.0)
(pid:3537)  time:2012-09-20 13:32:02

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0x86a6b563...
papi:8423

#RECV 60 bytes from xx.xx.xx.xx [4500] (0.0)
(pid:3537)  time:2012-09-20 13:32:02

 spi={6b19ba186d5692b3 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
   Notify: COOKIE
 spi={6b19ba186d5692b3 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to xx.xx.xx.xx[4500] (0.0)
(pid:3537)  time:2012-09-20 13:32:02


#RECV 337 bytes from xx.xx.xx.xx [4500] (0.0)
(pid:3537)  time:2012-09-20 13:32:02

 spi={6b19ba186d5692b3 8dc68bbb5333d29e} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   NAT_D (peer/NAT): f0 e6 01 65 ce f7 2c b2 f4 8b 20 96 d1 69 1b 63
df 5f da 04
   Notify: NAT_DETECTION_DESTINATION_IP
   NAT_D (us/NAT): c5 06 45 50 dc 49 19 a9 1b 9d 5e c4 2b 1a 4a 7f
38 00 14 b4
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i 08 dc 07 af 81 a3 eb 03 e6 f1 ca d4 06 95 fa 57
7a 92 ca 67
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={6b19ba186d5692b3 8dc68bbb5333d29e} np=E{IDi}
```

```
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to xx.xx.xx.xx[4500] (2.0)
(pid:3537)  time:2012-09-20 13:32:05

Sending last fragment, size = 432


#RECV 80 bytes from xx.xx.xx.xx [4500] (3.0)
(pid:3537)  time:2012-09-20 13:32:05

 spi={6b19ba186d5692b3 8dc68bbb5333d29e} np=E{N}
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=de6e7900)
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0

IKE_SA [v2 I] (id=0x86a6b563) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952

Switching output streamget_ike_version: Use IKE Version 2

papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:3569)  time:2012-09-20 13:32:05
 seconds.
Before getting Certs
TPM enabled
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1580
Decode PEM Key length :0
testHostKeys : status 0

testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
```

```
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BF0002873::00:1a:1e:08:42:7e}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ac100161
IKE_EXAMPLE: Socket created on 172.16.1.97[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
(pid:3569)  time:2012-09-20 13:32:05
 SA_INIT dest= xx.xx.xx.xx
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): fc 4d 59 d1 c3 a6 c9 1f b3 98 74 9f 79 09 38 89
d8 80 f2 53
   NAT_D (peer): 31 9e f7 85 c6 ad 77 75 f2 ca 36 c5 4e 64 d6 b9
cb 75 fc 65
 spi={07f19630b7bd03fe 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to xx.xx.xx.xx [4500] (0.0)
(pid:3569)  time:2012-09-20 13:32:05

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0xe52526b0...
papi:8423

#RECV 60 bytes from xx.xx.xx.xx [4500] (0.0)
(pid:3569)  time:2012-09-20 13:32:05

 spi={07f19630b7bd03fe 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
   Notify: COOKIE
 spi={07f19630b7bd03fe 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to xx.xx.xx.xx [4500] (0.0)
(pid:3569)  time:2012-09-20 13:32:05


#RECV 337 bytes from xx.xx.xx.xx [4500] (0.0)
(pid:3569)  time:2012-09-20 13:32:05

 spi={07f19630b7bd03fe 80462bf07dfe6679} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
```

```
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   NAT_D (peer/NAT): 9d ac 77 94 03 ba cd 44 34 99 66 92 52 81 50 f8
b2 bd 0b ce
   Notify: NAT_DETECTION_DESTINATION_IP
   NAT_D (us/NAT): bd e5 0c 72 f3 3c f8 29 c4 18 24 e9 fe 33 8a 16
0a 2b d4 56
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i 47 7f d8 f9 83 07 78 9d aa be 28 27 fd 2b b2 d8
6e dd 83 94
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={07f19630b7bd03fe 80462bf07dfe6679} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to xx.xx.xx.xx [4500] (2.0)
(pid:3569)  time:2012-09-20 13:32:08

Sending last fragment, size = 432


#RECV 80 bytes from xx.xx.xx.xx [4500] (3.0)
(pid:3569)  time:2012-09-20 13:32:08

 spi={07f19630b7bd03fe 80462bf07dfe6679} np=E{N}
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=b8796c00)
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0

IKE_SA [v2 I] (id=0xe52526b0) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952

Switching output streamget_ike_version: Use IKE Version 2

papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:3602)  time:2012-09-20 13:32:08
 seconds.
Before getting Certs
TPM enabled
```

```
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1580
Decode PEM Key length :0
testHostKeys : status 0

testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BF0002873::00:1a:1e:08:42:7e}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ac100161
IKE_EXAMPLE: Socket created on 172.16.1.97[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
(pid:3602)  time:2012-09-20 13:32:08
 SA_INIT dest=xx.xx.xx.xx
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): ad 42 18 49 c8 0d 33 52 70 a0 fe 37 97 92 9b 7e
dc 01 09 e0
   NAT_D (peer): ca dc 60 b1 15 aa 54 0b 1c 9b 1d 6f c5 de 5b 79
97 32 9f 5e
 spi={15c74e4a15924a3c 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to xx.xx.xx.xx[4500] (0.0)
(pid:3602)  time:2012-09-20 13:32:08

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0xbb77804a...
papi:8423
```

```
#RECV 60 bytes from xx.xx.xx.xx[4500] (0.0)
(pid:3602)  time:2012-09-20 13:32:08

 spi={15c74e4a15924a3c 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
   Notify: COOKIE
 spi={15c74e4a15924a3c 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to xx.xx.xx.xx[4500] (0.0)
(pid:3602)  time:2012-09-20 13:32:08


#RECV 337 bytes from xx.xx.xx.xx[4500] (0.0)
(pid:3602)  time:2012-09-20 13:32:09

 spi={15c74e4a15924a3c 3354a9c67fb39898} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   NAT_D (peer/NAT): 78 18 83 fb 31 8c 04 87 38 57 9d dc a9 7d 60 48
24 d7 b3 91
   Notify: NAT_DETECTION_DESTINATION_IP
   NAT_D (us/NAT): 29 ae ad 05 8a 4b bf e9 af 63 0d e6 54 32 e4 97
ee 29 aa 50
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i c8 1d 56 9d 7e 1e 43 e0 44 e0 32 c2 8e 59 5e fc
d3 66 d3 84
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={15c74e4a15924a3c 3354a9c67fb39898} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to xx.xx.xx.xx[4500] (3.0)
(pid:3602)  time:2012-09-20 13:32:11

Sending last fragment, size = 432


#RECV 80 bytes from xx.xx.xx.xx[4500] (3.0)
(pid:3602)  time:2012-09-20 13:32:11

 spi={15c74e4a15924a3c 3354a9c67fb39898} np=E{N}
```

```
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=8c0b3f00)
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0

IKE_SA [v2 I] (id=0xbb77804a) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952

Switching output streamget_ike_version: Use IKE Version 2

papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:3644)  time:2012-09-20 13:32:12
 seconds.
Before getting Certs
TPM enabled
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1580
Decode PEM Key length :0
testHostKeys : status 0

testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BF0002873::00:1a:1e:08:42:7e}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ac100161
```

```
IKE_EXAMPLE: Socket created on 172.16.1.97[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
(pid:3644)  time:2012-09-20 13:32:12
 SA_INIT dest=xx.xx.xx.xx
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): d8 fc 36 c9 5e 38 de c3 ef 49 b5 83 72 04 36 ab
0c df 4c 56
   NAT_D (peer): ab 5e 76 99 f1 7c 04 a3 d9 15 bc 2b a6 68 74 c7
1f e4 a6 71
 spi={fbf11f4b156960c4 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to xx.xx.xx.xx[4500] (0.0)
(pid:3644)  time:2012-09-20 13:32:12

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0xaa89e254...
papi:8423

#RECV 60 bytes from xx.xx.xx.xx[4500] (0.0)
(pid:3644)  time:2012-09-20 13:32:12

 spi={fbf11f4b156960c4 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
   Notify: COOKIE
 spi={fbf11f4b156960c4 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to xx.xx.xx.xx[4500] (0.0)
(pid:3644)  time:2012-09-20 13:32:12


#RECV 337 bytes from xx.xx.xx.xx[4500] (1.0)
(pid:3644)  time:2012-09-20 13:32:12

 spi={fbf11f4b156960c4 4ffdf767ab773822} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   NAT_D (peer/NAT): 47 5f 77 49 4a 3f fe ce 10 2b 25 93 a7 e3 0b 1d
97 89 bc fe
   Notify: NAT_DETECTION_DESTINATION_IP
   NAT_D (us/NAT): 8b 5b 8d 43 c7 38 62 33 75 30 94 1d 1b 92 30 ea
98 5b dc 73
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
```

```
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i f5 8a 41 f2 dd 8b e3 e8 a7 ea 78 ce 9c 90 b8 6b
20 7b f7 ca
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={fbf11f4b156960c4 4ffdf767ab773822} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to xx.xx.xx.xx[4500] (3.0)
(pid:3644)  time:2012-09-20 13:32:14

Sending last fragment, size = 432


#RECV 80 bytes from xx.xx.xx.xx[4500] (3.0)
(pid:3644)  time:2012-09-20 13:32:15

 spi={fbf11f4b156960c4 4ffdf767ab773822} np=E{N}
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=7a3d6c00)
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0

IKE_SA [v2 I] (id=0xaa89e254) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952

Switching output streamget_ike_version: Use IKE Version 2

papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:3663)  time:2012-09-20 13:32:15
 seconds.
Before getting Certs
TPM enabled
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1580
Decode PEM Key length :0
```

```
testHostKeys : status 0

testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BF0002873::00:1a:1e:08:42:7e}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ac100161
IKE_EXAMPLE: Socket created on 172.16.1.97[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
(pid:3663)  time:2012-09-20 13:32:15
 SA_INIT dest=xx.xx.xx.xx
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): 22 bf 7d 25 6f b5 c6 0b 0c 9c 38 6d a0 ca fa 01
4b a6 ec 3c
   NAT_D (peer): 5e ee 1d 6d 12 24 7f d4 24 33 51 2c ff c9 df 64
33 9a 3c 27
 spi={f6bdc5ad4f590ff7 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to xx.xx.xx.xx[4500] (0.0)
(pid:3663)  time:2012-09-20 13:32:15

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0x80f7362d...
papi:8423

#RECV 60 bytes from xx.xx.xx.xx[4500] (1.0)
(pid:3663)  time:2012-09-20 13:32:15

 spi={f6bdc5ad4f590ff7 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
   Notify: COOKIE
 spi={f6bdc5ad4f590ff7 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to xx.xx.xx.xx[4500] (1.0)
(pid:3663)  time:2012-09-20 13:32:15
```

```
#RECV 337 bytes from xx.xx.xx.xx[4500] (1.0)
(pid:3663)  time:2012-09-20 13:32:15

 spi={f6bdc5ad4f590ff7 9cd04cd63896afcf} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   NAT_D (peer/NAT): 38 a3 b3 5c 5e 24 89 b4 2a 9a 1c ab 82 48 7d c3
f6 3e a4 54
   Notify: NAT_DETECTION_DESTINATION_IP
   NAT_D (us/NAT): 1a ce 5d 73 43 cd 1a bf 15 fb 7d 4a c8 c6 08 be
6e a6 17 5d
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i b2 2a d5 f1 e7 3d 4f 24 e1 a7 fb fc df 5a 79 ca
7e 1f d3 de
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={f6bdc5ad4f590ff7 9cd04cd63896afcf} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to xx.xx.xx.xx[4500] (3.0)
(pid:3663)  time:2012-09-20 13:32:18

Sending last fragment, size = 432


#RECV 80 bytes from xx.xx.xx.xx[4500] (3.0)
(pid:3663)  time:2012-09-20 13:32:18

 spi={f6bdc5ad4f590ff7 9cd04cd63896afcf} np=E{N}
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=63eed800)
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0

IKE_SA [v2 I] (id=0x80f7362d) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952
```

```
Switching output streamget_ike_version: Use IKE Version 2

papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:3699)  time:2012-09-20 13:32:18
 seconds.
Before getting Certs
TPM enabled
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1580
Decode PEM Key length :0
testHostKeys : status 0

testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BF0002873::00:1a:1e:08:42:7e}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ac100161
IKE_EXAMPLE: Socket created on 172.16.1.97[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
(pid:3699)  time:2012-09-20 13:32:18
 SA_INIT dest=xx.xx.xx.xx
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): e2 af 3c e1 ee d7 d4 04 27 59 3f 88 79 72 da cb
cf 0c ae c0
```

```
   NAT_D (peer): 20 bc 18 af 37 1a c2 93 5a ec f3 3f 9e b7 29 49
86 86 58 b2
 spi={7a6fb38dfaae6a17 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to xx.xx.xx.xx[4500] (0.0)
(pid:3699)  time:2012-09-20 13:32:18

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0xb6e1a523...
papi:8423

#RECV 60 bytes from xx.xx.xx.xx[4500] (0.0)
(pid:3699)  time:2012-09-20 13:32:18

 spi={7a6fb38dfaae6a17 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
   Notify: COOKIE
 spi={7a6fb38dfaae6a17 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to xx.xx.xx.xx[4500] (0.0)
(pid:3699)  time:2012-09-20 13:32:18


#RECV 337 bytes from xx.xx.xx.xx[4500] (0.0)
(pid:3699)  time:2012-09-20 13:32:18

 spi={7a6fb38dfaae6a17 03cbcb27a9877219} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   NAT_D (peer/NAT): ad fd bd ba 97 59 a1 ea a0 62 c3 96 3f d0 a7 57
83 53 08 67
   Notify: NAT_DETECTION_DESTINATION_IP
   NAT_D (us/NAT): 62 d8 a2 32 8b 5a 55 50 d9 29 dc 29 bd a7 8a 37
38 9b 9d f7
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i 6b a9 15 03 d1 c5 f1 ec e0 c5 ff 05 43 87 88 70
c3 1b 66 a5
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
```

```
 spi={7a6fb38dfaae6a17 03cbcb27a9877219} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to xx.xx.xx.xx[4500] (2.0)
(pid:3699)  time:2012-09-20 13:32:21

Sending last fragment, size = 432


end of show log rapper
=======================================================
```