CHAPTER 30

Troubleshooting the IPsec VPN SPA

This chapter describes techniques that you can use to troubleshoot the operation of your IPsec VPN SPAs in a Catalyst 6500 Series switch.

It includes the following sections:

Note For detailed information on Cisco IOS IPsec cryptographic operations and policies, refer to the *Cisco IOS Security Configuration Guide, Release 12.2* and *Cisco IOS Security Command Reference, Release 12.2*.

For more information about the commands used in this chapter, see the *Catalyst 6500 Series Cisco IOS Command Reference, Release 12.2SX* publication. Also refer to the related Cisco IOS Release 12.2 software command reference and master index publications. For more information about accessing these publications, see the "Related Documentation" section on page xlv.

General Troubleshooting Information

This section describes general information for troubleshooting the IPsec VPN SPA and the Cisco 7600 SSC-400 SIP. It includes the following sections:

Interpreting Console Error Messages

The Catalyst 6500 Series switch can generate error messages and other system messages to inform the operator of events that might require attention. These messages can be displayed on the console, or sent to a logging host using the System Logging (Syslog) protocol or Simple Network Management Protocol (SNMP).

System error messages are organized in the documentation according to the particular system facility that produces the messages. The IPsec VPN SPA and Cisco 7600 SSC-400 SIP use the following facility names in error messages:

- IPsec VPN SPA—SPA_IPSEC_2G (also VPNSPA)
- Cisco 7600 SSC-400—CAT6000_SSC (also C7600_SSC400)

To view the explanations and recommended actions for Catalyst 6500 Series switch error messages, including messages related to service modules, refer to the following documents:

- *Cisco IOS Release 12.2SX System Message Guide* at this URL:

  http://www.cisco.com/en/US/docs/ios/12_2sx/system/messages/122sxsms.html
- *System Messages for 12.2S* (for error messages in Release 12.2S) at this URL:

  http://www.cisco.com/en/US/docs/ios/system/messages/guide/consol_smg.html

Using debug Commands

For information about **debug** commands specific to the Cisco IOS software release 12.2SX, see the *Cisco IOS Master Command List, Release 12.2SX* at this URL:

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support personnel. We recommend that you use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

For information about available crypto conditional debugging commands, see the "Using Crypto Conditional Debug" section on page 30-27.

For more information about other **debug** commands that can be used on a Catalyst 6500 Series switch, see the *Cisco IOS Debug Command Reference, Release 12.2* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/122debug.html

Using show Commands

You can use several **show** commands to monitor and troubleshoot the IPsec VPN SPA on the Catalyst 6500 Series switch.

For more information about **show** commands to verify and monitor the IPsec VPN SPA, see the "Displaying IPsec VPN SPA Configuration Information" section on page 30-6 and the *Catalyst 6500 Series Cisco IOS Command Reference, Release 12.2SX*.

For more information about security-related **show** commands, see the *Cisco IOS Security Command Reference*.

Monitoring the IPsec VPN SPA

This section describes commands that can be used to display information about the IPsec VPN SPA hardware and configuration. It consists of the following subsections:

Displaying IPsec VPN SPA Hardware and System Information

To display hardware and system information, use the following commands:

- **show diagbus, show module, show crypto eli**—See the "Displaying Information About IPsec VPN SPA Ports" section on page 30-3.
- **show crypto engine accelerator statistic slot**—See the "Displaying Platform and Network Interface Controller Statistics for the IPsec VPN SPA" section on page 30-4.
- **show hw-module slot fpd**—See the "Displaying Information About Hardware Revision Levels" section on page 30-6.

Displaying Information About IPsec VPN SPA Ports

To display information about the type of SPAs that are installed in the switch, use the **show diagbus** command.

The following example shows output from the **show diagbus** command on a Catalyst 6500 Series switch with an IPsec VPN SPA installed in subslot 1 of a Cisco 7600 SSC-400 that is installed in slot 5:

```
Router# show diagbus

Slot 5: Logical_index 10
        2-subslot Services SPA Carrier-400 controller
        Board is analyzed ipc ready
        HW rev 0.3, board revision A01
        Serial Number: abc Part number: 73-6348-01

        Slot database information:
        Flags: 0x2004   Insertion time: 0x3DB5F4BC (4d20h ago)

        Controller Memory Size:
                248 MBytes CPU Memory
                8 MBytes Packet Memory
                256 MBytes Total on Board SDRAM
        IOS (tm) cwlc Software (smsc-DWDBG-M), Experimental Version 12.2(20050623:231413)

        SPA Information:
        subslot 5/1: SPA-IPSEC-2G (0x3D7), status: ok
```

For information about the **show module** and **show crypto eli** commands, see the "Displaying the SPA Hardware Type" section on page 20-20.

Displaying Platform and Network Interface Controller Statistics for the IPsec VPN SPA

To display platform statistics and optionally display network interface controller statistics, use the **show crypto engine accelerator statistic slot** command.

Note The **show crypto engine accelerator statistic** command is supported in Cisco IOS Release 12.2(33)SXH and later releases.

The following example shows output from the **show crypto engine accelerator statistic** command on a Catalyst 6500 Series switch with an IPsec VPN SPA in subslot 0 of a Cisco 7600 SSC-400 that is installed in slot 1. The output displays platform statistics for the IPsec VPN SPA and also displays the network interface controller statistics.

```
Router# show crypto engine accelerator statistic slot 1/0 detail

VPN module in slot 1/0


Decryption Side Data Path Statistics
====================================
Packets RX..............: 454260
Packets TX..............: 452480

IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 452470
AH Packets..............: 0
ESP Packets.............: 452470
GRE Decapsulations.......: 0
NAT-T Decapsulations.....: 0
Clear....................: 8
ICMP.....................: 0

Packets Drop.............: 193
Authentication Errors....: 0
Decryption Errors........: 0
Replay Check Failed......: 0
Policy Check Failed......: 0
Illegal CLear Packet.....: 0
GRE Errors...............: 0
SPD Errors...............: 0
HA Standby Drop..........: 0

Hard Life Drop...........: 0
Invalid SA...............: 191
SPI No Match.............: 0
Destination No Match.....: 0
Protocol No Match........: 0

Reassembly Frag RX.......: 0
IPSec Fragments..........: 0
IPSec Reasm Done.........: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop...........: 0
Fragments Drop...........: 0
```

```
Decryption Side Controller Statistics

====================================
Frames RX.................: 756088
Bytes RX..................: 63535848
Mcast/Bcast Frames RX....: 2341
RX Less 128Bytes.........: 756025
RX Less 512Bytes.........: 58
RX Less 1KBytes..........: 2
RX Less 9KBytes..........: 3
RX Frames Drop...........: 0

Frames TX.................: 452365
Bytes TX..................: 38001544
Mcast/Bcast Frames TX....: 9
TX Less 128Bytes.........: 452343
TX Less 512Bytes.........: 22
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0


Encryption Side Data Path Statistics
====================================
Packets RX................: 756344
Packets TX................: 753880
IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 753869
GRE Encapsulations.......: 0
NAT-T Encapsulations.....: 0
LAF prefragmented........: 0

Fragmented................: 0
Clear.....................: 753904
ICMP......................: 0

Packets Drop..............: 123
IKE/TED Drop..............: 27
Authentication Errors....: 0
Encryption Errors........: 0
HA Standby Drop..........: 0

Hard Life Drop............: 0
Invalid SA................: 191

Reassembly Frag RX.......: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop...........: 0
Fragments Drop...........: 0


Encryption Side Controller Statistics
====================================
Frames RX.................: 454065
Bytes RX..................: 6168274/
Mcast/Bcast Frames RX....: 1586
RX Less 128Bytes.........: 1562
RX Less 512Bytes.........: 452503
RX Less 1KBytes..........: 0
RX Less 9KBytes..........: 0
RX Frames Drop...........: 0

Frames TX.................: 753558
```

```
Bytes TX..................: 100977246
Mcast/Bcast Frames TX....: 2
TX Less 128Bytes.........: 3
TX Less 512Bytes.........: 753555
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0

Router#
```

Displaying Information About Hardware Revision Levels

To display information about the hardware revision of the Cisco 7600 SSC-400 and the IPsec VPN SPA as well as the version of the field-programmable devices (FPDs) that are on the carrier card and the SPA, use the **show hw-module slot fpd** command. Cisco technical engineers might need this information to debug or troubleshoot problems with a SPA installation.

The following example shows output from the **show hw-module slot** command on a Catalyst 6500 Series switch with an IPsec VPN SPA installed in subslot 0 of a Cisco 7600 SSC-400 that is installed in slot 6:

```
Router# show hw-module slot 2 fpd

==== ====================== ====== ============================================
                             H/W   Field Programmable   Current   Min. Required
Slot Card Type               Ver.  Device: "ID-Name"    Version      Version
==== ====================== ====== ================== =========== ==============
   2 7600-SSC-400              0.5 1-I/O FPGA             1.0         1.0
---- ---------------------- ------ ------------------ ----------- --------------
 2/0 SPA-IPSEC-2G              0.3 1-PROM                 1.1         1.1
==== ====================== ====== ============================================
```

Displaying IPsec VPN SPA Configuration Information

To display information about the IPsec VPN SPA configuration, use the following commands:

- **show crypto vlan**—See the "Displaying Information About Access and Routed Ports That Are Connected" section on page 30-7, "Displaying the VPN Running State" section on page 30-8, and "Displaying Information About IP Multicast Over a GRE Tunnel" section on page 30-23.
- **show interfaces trunk**—See the "Displaying Information About the VLANs Allowed by a Trunk Port" section on page 30-7.
- **show crypto isakmp policy**—See the "Displaying Information About IKE Policies" section on page 30-8.
- **show crypto ipsec transform-set**—See the "Displaying Information About IPsec Transform Sets" section on page 30-9.
- **show crypto map**—See the "Displaying Information About Crypto Maps" section on page 30-9.
- **show crypto isakmp sa**—See the "Displaying Information About SAs at a Peer" section on page 30-11.
- **show crypto isakmp ha standby**—See the "Displaying HSRP Information" section on page 30-11.
- **show crypto ipsec ha**—See the "Displaying HSRP Information" section on page 30-11.
- **show crypto ipsec sa**—See the "Displaying Information About IPsec Security Associations" section on page 30-9 and the "Displaying HSRP Information" section on page 30-11.
- **show crypto ipsec sa standby**—See the "Displaying HSRP Information" section on page 30-11.
- **show ssp client**—See the "Displaying SSP Information" section on page 30-14.

- **show ssp packet**—See the "Displaying SSP Information" section on page 30-14.
- **show ssp peers**—See the "Displaying SSP Information" section on page 30-14.
- **show ssp redundancy**—See the "Displaying SSP Information" section on page 30-14.
- **show redundancy linecard-grou**p—See the "Displaying Information About a BFG Configuration" section on page 30-15.
- **show crypto ace redundancy**—See the "Displaying Information About a BFG Configuration" section on page 30-15.
- **show crypto key mypubkey rsa**—See the "Displaying Information About RSA Public Keys" section on page 30-15.
- **show crypto key pubkey-chain rsa**—See the "Displaying Information About RSA Public Keys" section on page 30-15.
- **show crypto pki certificates**—See the "Displaying Information About Certificates" section on page 30-16.
- **show crypto pki trustpoints**—See the "Displaying Information About Trustpoints" section on page 30-17.
- **show ip nhrp**—See the "Displaying Information About the NHRP Cache" section on page 30-18.
- **show crypto session**—See the "Displaying Information About Crypto Sessions" section on page 30-18.
- **show interfaces tunnel**—See the "Displaying Tunnel Interface Information" section on page 30-19.

For a detailed description of the information displayed by the **show** commands, refer to the "IP Security and Encryption" chapter of the *Cisco IOS Security Command Reference*.

Displaying Information About Access and Routed Ports That Are Connected

To verify that an access or routed port is connected, use the **show crypto vlan** command. The following is sample output from the command:

```
Router# show crypto vlan

Interface VLAN 2 on IPSec Service Module port GigabitEthernet2/0/1 connected to VLAN 502
with crypto map set mymap1


Router# show crypto vlan

Interface VLAN 2 on IPSec Service Module port GigabitEthernet2/0/1 connected to Gi2/8 with
crypto map set mymap2
```

Displaying Information About the VLANs Allowed by a Trunk Port

To display information about the VLANs allowed by a trunk port, use the **show interfaces trunk** command. The following is sample output from the command:

```
Router# show interfaces trunk

Port                Mode         Encapsulation  Status        Native vlan
Gi2/0/1             on           802.1q         trunking      1
Gi2/0/2             on           802.1q         trunking      1

Port                Vlans allowed on trunk
```

```
Gi2/0/1             2
Gi2/0/2             502

Port                Vlans allowed and active in management domain
Gi2/0/1             2
Gi2/0/2             502

Port                Vlans in spanning tree forwarding state and not pruned
Gi2/0/1             2
Gi2/0/2             502
```

Displaying the VPN Running State

To display the VPN running state, use the **show crypto vlan** command. The following is sample output from the command:

In the following example, the interface VLAN belongs to the IPsec VPN SPA inside port:

```
Router# show crypto vlan

Interface VLAN 2 on IPSec Service Module port GigabitEthernet2/0/1 connected to Fa8/3
```

In the following example, VLAN 2 is the interface VLAN and VLAN 2022 is the hidden VLAN:

```
Router# show crypto vlan

Interface VLAN 2 on IPSec Service Module port GigabitEthernet2/0/1 connected to VLAN 2022
with crypto map set mymap2
```

In the following example, either the interface VLAN is missing on the IPsec VPN SPA inside port, the IPsec VPN SPA is removed from the chassis, or the IPsec VPN SPA was moved to a different subslot:

```
Router# show crypto vlan

  Interface VLAN 2 connected to VLAN 3 (no IPSec Service Module attached)
```

Displaying Information About IKE Policies

To display information about IKE policies, use the **show crypto isakmp policy** command. The following is sample output from the command:

```
Router# show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

Note If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed in the **show crypto isakmp policy** command output:

```
WARNING:encryption hardware does not support the configured encryption method for ISAKMP
policy value
```

Displaying Information About IPsec Transform Sets

To display information about transform set configurations, use the **show crypto ipsec transform-set** command. The following is sample output from the command:

```
Router# show crypto ipsec transform-set

Transform set combined-des-md5: {esp-des esp-md5-hmac}
will negotiate = {Tunnel,},
Transform set t1: {esp-des esp-md5-hmac}
will negotiate = {Tunnel,},
Transform set t100: {ah-sha-hmac}
will negotiate = {Transport,},
```

Note If a user enters an IPsec transform that the hardware (the IPsec peer) does not support, a warning message will be displayed in the **show crypto ipsec transform-set** command output:

```
WARNING:encryption hardware does not support transform.
```

Displaying Information About Crypto Maps

To display information about crypto map configurations, use the **show crypto map** command. The following is sample output from the command:

```
Router# show crypto map

Crypto Map "test" 10 ipsec-isakmp
        Peer = 11.1.0.1
        Extended IP access list 101
            access-list 101 permit ip host 1.0.0.1 host 2.0.0.1
        Current peer: 11.1.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                tset:  { esp-3des  } ,
        }
        Interfaces using crypto map test:
                Vlan2
 using crypto engine SPA-IPSEC-2G[2/0]
```

Displaying Information About IPsec Security Associations

To display information about IPsec security associations, use the **show crypto ipsec sa** command.

Note When you first enter the **show crypto ipsec sa** command, the packet counters will not show the correct values. Subsequent instances of the command will display the correct values.

The following is sample output from the command:

```
Router# show crypto ipsec sa

interface: Ethernet0

    Crypto map tag: router-alice, local addr. 172.21.114.123
    local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0

    local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
    path mtu 1500, media mtu 1500
    current outbound spi: 20890A6F

    inbound esp sas:
    spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 26, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y

    inbound ah sas:

    outbound esp sas:
    spi: 0x20890A6F(545852015)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 27, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:

interface: Tunnel0

    Crypto map tag: router-alice, local addr. 172.21.114.123
    local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
    local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
    path mtu 1500, media mtu 1500
    current outbound spi: 20890A6F

    inbound esp sas:
    spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
```

```
    slot: 0, conn id: 26, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:

outbound esp sas:
spi: 0x20890A6F(545852015)
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 27, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:
```

Displaying Information About SAs at a Peer

To display information about all current IKE SAs at a peer, use the **show crypto isakmp sa** command. The following is sample output from the command:

```
Router# show crypto isakmp sa
dst             src             state          conn-id slot status
11.0.0.1        21.0.0.1        QM_IDLE          68002 ACTIVE
21.0.0.1        11.0.0.1        QM_IDLE          68003 ACTIVE
10.0.0.1        11.0.0.1        QM_IDLE          68001 ACTIVE
```

Displaying HSRP Information

To display information about HSRP configurations, use the **show crypto isakmp ha standby**, **show crypto ipsec ha**, **show ipsec sa**, and **show crypto ipsec sa standby** commands.

Enter the **show crypto isakmp ha standby** command to view your ISAKMP standby or active SAs. The following is sample output from the command:

```
Router# show crypto isakmp ha standby

dst             src             state       I-Cookie           R-Cookie

172.16.31.100   20.3.113.1      QM_IDLE     796885F3 62C3295E  FFAFBACD

EED41AFF

172.16.31.100   20.2.148.1      QM_IDLE     5B78D70F 3D80ED01  FFA03C6D

09FC50BE

172.16.31.100   20.4.124.1      QM_IDLE     B077D0A1 0C8EB3A0  FF5B152C

D233A1E0

172.16.31.100   20.3.88.1       QM_IDLE     55A9F85E 48CC14DE  FF20F9AE

DE37B913

172.16.31.100   20.1.95.1       QM_IDLE     3881DE75 3CF384AE  FF192CAB
```

Enter the **show crypto ipsec ha** command to view your IPsec high availability (HA) manager state. The following is sample output from the command:

```
Router# show crypto ipsec ha

Interface           VIP                SAs   IPSec HA State

FastEthernet0/0     172.16.31.100     1800   Active since 13:00:16 EDT Tue Oct 1 2002
```

Enter the **show crypto ipsec sa** command to view HA status of the IPsec SA (standby or active). The following is sample output from the command:

```
Router# show crypto ipsec sa

interface: FastEthernet0/0

    Crypto map tag: mymap, local addr. 172.168.3.100
    local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (5.6.0.0/255.255.0.0/0/0)
    current_peer: 172.168.3.1
    PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 172.168.3.100, remote crypto endpt.: 172.168.3.1
    path mtu 1500, media mtu 1500
    current outbound spi: 132ED6AB

    inbound esp sas:
    spi: 0xD8C8635F(3637011295)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

    inbound ah sas:
    spi: 0xAAF10A60(2867923552)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

    inbound pcp sas:

    outbound esp sas:
    spi: 0x132ED6AB(321836715)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

    outbound ah sas:
    spi: 0x1951D78(26549624)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
```

```
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

    outbound pcp sas:
```

Enter the **show crypto ipsec sa standby** command to view your standby SAs. The following is sample output from the command:

```
Router# show crypto ipsec sa standby

interface: FastEthernet0/0
    Crypto map tag: mymap, local addr. 172.168.3.100
    local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (5.6.0.0/255.255.0.0/0/0)
    current_peer: 172.168.3.1
    PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 172.168.3.100, remote crypto endpt.: 172.168.3.1
    path mtu 1500, media mtu 1500
    current outbound spi: 132ED6AB

    inbound esp sas:
    spi: 0xD8C8635F(3637011295)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

    inbound ah sas:
    spi: 0xAAF10A60(2867923552)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

    inbound pcp sas:

    outbound esp sas:
    spi: 0x132ED6AB(321836715)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

    outbound ah sas:
    spi: 0x1951D78(26549624)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
```

```
        replay detection support: Y
        HA Status: STANDBY

    outbound pcp sas:
```

Displaying SSP Information

To display information about an SSP configuration, use the **show ssp client**, **show ssp packet**, **show ssp peers**, and **show ssp redundancy** commands.

Enter the **show ssp client** command to display the domain of interpretation (DOI), name, running version and available version of each client that is registered with SSP. The following is sample output from the command:

```
Router# show ssp client

SSP Client Information

    DOI   Client Name                       Version   Running Ver

      1   IPSec HA Manager                   1.0       1.0

      2   IKE HA Manager                     1.0       1.0
```

Enter the **show ssp packet** command to display the byte count and packet count for the current socket, the creation time of the socket, the server port number, and the port number used for SSP communication. The following is sample output from the command:

```
Router# show ssp packet

SSP packet Information

    Socket creation time: 01:01:06

    Local port: 3249      Server port: 3249

    Packets Sent = 38559, Bytes Sent = 2285020

    Packets Received = 910, Bytes Received = 61472
```

Enter the **show ssp peers** command to display the IP address of the remote peer, the interface used, and the connection state. The following is sample output from the command:

```
Router# show ssp peers

SSP Peer Information

    IP Address      Connection State   Local Interface

    40.0.0.1        Connected          FastEthernet0/1
```

Enter the **show ssp redundancy** command to display the current SSP state, the HSRP group name, interface used, and the elapsed time since last state change. The following is sample output from the command:

```
Router# show ssp redundancy

SSP Redundancy Information

  Device has been ACTIVE for 02:55:34
```

```
Virtual IP      Redundancy Name             Interface

172.16.31.100   KNIGHTSOFNI                 FastEthernet0/0
```

Displaying Information About a BFG Configuration

To display information about a BFG configuration, use the **show redundancy linecard-group** and **show crypto ace redundancy** commands. The following is sample output from the commands:

```
Router# show redundancy linecard-group 1

Line Card Redundancy Group:1 Mode:feature-card
Class:load-sharing
Cards:
Slot:3 Subslot:0
Slot:5 Subslot:0

Router# show crypto ace redundancy
---------------------------------------
LC Redundancy Group ID            :1
Pending Configuration Transactions:0
Current State                     :OPERATIONAL
Number of blades in the group     :2
Slots
---------------------------------------
Slot:3 Subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 22 times
Initialization Timer not running
Slot:5 Subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 24 times
Initialization Timer not running
```

Displaying Information About RSA Public Keys

To display information the RSA public keys configured for your switch, use the **show crypto key mypubkey rsa** command. The following is sample output from the command:

```
Router# show crypto key mypubkey rsa

% Key pair was generated at: 06:07:50 UTC Jan 13 1996

Key name: myrouter.example.com

 Usage: Encryption Key

 Key Data:

  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
```

```
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB

  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

To display a list of all the RSA public keys stored on your switch (including the public keys of peers that have sent your switch their certificates during peer authentication for IPsec), or to display details of a particular RSA public key stored on your switch, use the **show crypto key pubkey-chain rsa** command. The following is sample output from the command:

```
Router# show crypto key pubkey-chain rsa

Codes: M - Manually Configured, C - Extracted from certificate

Code  Usage        IP-address     Name

M     Signature    10.0.0.1       myrouter.example.com

M     Encryption   10.0.0.1       myrouter.example.com

C     Signature    172.16.0.1     routerA.example.com

C     Encryption   172.16.0.1     routerA.example.com

C     General      192.168.10.3   routerB.domain1.com
```

Displaying Information About Certificates

To display information about your certificate, the certificate of the CA, and any RA certificates, use the **show crypto pki certificates** command. The following is sample output from the command:

```
Router# show crypto pki certificates

CA Certificate

Status: Available
    Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
    Certificate Usage: Signature

    Issuer:
        CN = new-user
        OU = pki new-user
        O = cisco
        L = santa cruz2
        ST = CA
        C = US
        EA = user@example.com

    Subject:
        CN = new-user
        OU = pki new-user
        O = cisco
        L = santa cruz2
        ST = CA
        C = US
        EA = user@example.com

    CRL Distribution Point:
        http://new-user.example.com/CertEnroll/new-user.crl

    Validity Date:
        start date: 14:19:29 PST Oct 31 2002
```

```
        end date: 14:27:27 PST Oct 31 2017

    Associated Trustpoints: MS

Certificate

Status: Available
    Certificate Serial Number: 193E28D20000000009F7
    Certificate Usage: Signature

    Issuer:
        CN = new-user
        OU = pki new-user
        O = cisco
        L = santa cruz2
        ST = CA
        C = US
        EA = user@example.com

    Subject:
        Name: User1.Example.Com

    CRL Distribution Point:
        http://new-user.example.com/CertEnroll/new-user.crl

    Validity Date:
        start date: 12:40:14 PST Feb 26 2003
        end   date: 12:50:14 PST Mar 5 2003
        renew date: 16:00:00 PST Dec 31 1969

    Associated Trustpoints: MS
```

Displaying Information About Trustpoints

To display the trustpoints that are configured in the switch, use the **show crypto pki trustpoints** command. The following is sample output from the command:

```
Router# show crypto pki trustpoints

Trustpoint bo:

    Subject Name:

    CN = ACSWireless Certificate Manager

     O = cisco.com

     C = US

          Serial Number:01

    Certificate configured.

    CEP URL:http://ACSWireless

    CRL query url:ldap://ACSWireless
```

Displaying Information About the NHRP Cache

To display information about the Next Hop Resolution Protocol (NHRP) cache, use the **show ip nhrp** and the **show crypto sockets** commands. The following is sample output from the commands:

```
Router# show ip nhrp

10.10.1.75/32 via 10.10.1.75, Tunnel5 created 00:32:11, expire 00:01:46

  Type: dynamic, Flags: authoritative unique registered

  NBMA address: 172.16.175.75

10.10.1.76/32 via 10.10.1.76, Tunnel5 created 00:26:41, expire 00:01:37

  Type: dynamic, Flags: authoritative unique registered

  NBMA address: 172.16.175.76

10.10.1.77/32 via 10.10.1.77, Tunnel5 created 00:31:26, expire 00:01:33

  Type: dynamic, Flags: authoritative unique registered

  NBMA address: 172.17.63.20

Router# show crypto sockets

Number of Crypto Socket connections 1

   Tu0 Peers (local/remote): 9.1.1.1/11.1.1.1
       Local Ident  (addr/mask/port/prot): (9.1.1.1/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (11.1.1.1/255.255.255.255/0/47)
       IPSec Profile: "MyIpsecProf"
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "MyIpsecProf" Map-name: "Tunnel0-head-0"

Router#
```

Displaying Information About Crypto Sessions

To display status information for active crypto sessions, use the **show crypto session** command. The output will include the following:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by which the IPsec SAs are created
- IPsec SAs serving the flows of a session

The following is sample output from the command:

```
Router# show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication
```

```
Interface: Ethernet1/0
Session status: UP-NO-IKE
Peer: 10.2.80.179/500 fvrf: (none) ivrf: (none)
Desc: My-manual-keyed-peer
Phase1_id: 10.2.80.179
IPSEC FLOW: permit ip host 10.2.80.190 host 10.2.80.179
Active SAs: 4, origin: manual-keyed crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Interface: Ethernet1/2
Session status: DOWN
Peer: 10.1.1.1/500 fvrf: (none) ivrf: (none)
Desc: SJC24-2-VPN-Gateway
Phase1_id: 10.1.1.1
IPSEC FLOW: permit ip host 10.2.2.3 host 10.2.2.2
Active SAs: 0, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
IPSEC FLOW: permit ip 10.2.0.0/255.255.0.0 10.4.0.0/255.255.0.0
Active SAs: 0, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Interface: Serial2/0.17
Session status: UP-ACTIVE
Peer: 10.1.1.5/500 fvrf: (none) ivrf: (none)
Desc: (none)
Phase1_id: 10.1.1.5
IKE SA: local 10.1.1.5/500 remote 10.1.1.5/500 Active
Capabilities:(none) connid:1 lifetime:00:59:51
IPSEC FLOW: permit ip host 10.1.1.5 host 10.1.2.5
Active SAs: 2, origin: dynamic crypto map
Inbound: #pkts dec'ed 4 drop 0 life (KB/Sec) 20085/171
Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 20086/171
```

Displaying Tunnel Interface Information

To display tunnel interface information, use the **show interfaces tunnel** command. The following is sample output from the command:

```
Router# show interfaces tunnel 1

Tunnel4 is up, line protocol is down
Hardware is Routing Tunnel
Internet address is 10.1.1.1/24
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
Encapsulation TUNNEL, loopback not set
Keepalive set (10 sec)
Tunnel source 9.2.2.1, destination 6.6.6.2
Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
Tunnel TOS 0xF, Tunnel TTL 128
Checksumming of packets disabled, fast tunneling enabled
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy, fifo
Output queue 0/0, 1 drops; input queue 0/75, 0 drops
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets, 0 restarts
```

Table 30-1 describes significant fields shown in the display.

Table 30-1 show interfaces tunnel Field Descriptions

Field	Description
Tunnel is {up | down}	Interface is currently active and inserted into ring (up) or inactive and not inserted (down).
line protocol is {up | down | administratively down}	Shows line protocol up if a valid route is available to the tunnel destination. Shows line protocol down if no route is available, or if the route would be recursive.
Hardware	Specifies the hardware type.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method is always TUNNEL for tunnels.
loopback	Indicates whether loopback is set or not.
Keepalive	Indicates whether keepalives are set or not.
Tunnel source	IP address used as the source address for the tunnel packets.
destination	IP address of the tunnel destination.
Tunnel protocol	Tunnel transport protocol (the protocol the tunnel is using). This is based on the **tunnel mode** command, which defaults to GRE.
key	(Optional) ID key for the tunnel interface.
sequencing	(Optional) Indicates whether the tunnel interface drops datagrams that arrive out of order.
Last input	Number of hours, minutes, and seconds (or never) since the last packet was successfully received by an interface and processed locally on the switch. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds (or never) since the last packet was successfully transmitted by an interface.

Table 30-1 show interfaces tunnel Field Descriptions (continued)

Field	Description
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are displayed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. Three asterisks (***) indicate the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Output queue, drops Input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
30 second input rate, 30 second output rate	Average number of bits and packets transmitted per second in the last 30 seconds. The 30-second input and output rates should be used only as an approximation of traffic per second during a given 30-second period. These rates are exponentially weighted averages with a time constant of 30 seconds. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.

Table 30-1 show interfaces tunnel Field Descriptions (continued)

Field	Description
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end switch's receiver can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.

Table 30-1 show interfaces tunnel Field Descriptions (continued)

Field	Description
collisions	Number of messages retransmitted because of an Ethernet collision. This usually is the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). Some collisions are normal. However, if your collision rate climbs to around 4 or 5 percent, you should consider verifying that there is no faulty equipment on the segment and moving some existing stations to a new segment. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been reset. The interface may be reset by the administrator or automatically when an internal error occurs.
restarts	Number of times that the controller was restarted because of errors.

Displaying Information About IP Multicast Over a GRE Tunnel

To display information about an IP multicast over a GRE tunnel configuration, enter the **show crypto vlan** and **show ip mroute** commands.

Enter the **show crypto vlan** command to check that the tunnel has been taken over by the IPsec VPN SPA. The following is sample output from the command:

```
Router# show crypto vlan

Interface VLAN 100 on IPSec Service Module port Gi7/0/1 connected to Po1 with crypto map
set map_t3
Tunnel15 is accelerated via IPSec SM in subslot 7/0
```

Enter the **show ip mroute** command and look for the H flag to check that the IP multicast traffic is hardware-switched. The following is sample output from the command:

```
Router# show ip mroute 230.1.1.5

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 230.1.1.5), 01:23:45/00:03:16, RP 15.15.1.1, flags: SJC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Tunnel15, Forward/Sparse-Dense, 00:25:47/00:03:16
```

```
(120.1.0.3, 230.1.1.5), 01:23:46/00:03:25, flags: T
Incoming interface: GigabitEthernet8/1, RPF nbr 0.0.0.0, RPF-MFD
Outgoing interface list:
Tunnel15, Forward/Sparse-Dense, 00:25:47/00:03:16, H
```

Troubleshooting Specific Problems on the IPsec VPN SPA

This section provides additional information about troubleshooting specific problems related to the IPsec VPN SPA. It includes the following subsections:

Clearing IPsec Security Associations

You can clear (and reinitialize) IPsec security associations by using the **clear crypto sa** command.

Using the **clear crypto sa** command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the SA database. For more information, refer to the **clear crypto sa** command in the *Cisco IOS Security Command Reference*, *Release 12.2*.

If you want to also remove the IKE (phase 1) SAs, follow the **clear crypto sa** command with the **clear crypto isa** command. Alternatively, you can use the **clear crypto session** command to achieve the same result as the **clear crypto sa** and the **clear crypto isa** commands. The **clear crypto session** command supports many of the same parameters as the **clear crypto sa** command.

Troubleshooting Trunk Port Configurations

Caution When you configure an Ethernet port as a trunk port, all the VLANs are allowed on the trunk port by default. This default configuration does not work well with the IPsec VPN SPA and causes network loops. To avoid this problem, you must explicitly specify only the desirable VLANs.

For more information on trunk configuration guidelines, review the "Configuring a Trunk Port" section on page 21-15.

To verify which ports are assigned to the VLAN, enter the **show vlan id** *number* command, using the interface VLAN identifier. Following is an example of a trunk port configuration and the output of the **show vlan id** command:

```
Router# show run interface gi 1/3
Building configuration...

Current configuration : 175 bytes
!
interface GigabitEthernet1/3
```

```
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502-504,1002-1005
 switchport mode trunk
 no ip address
end


Router# show crypto vlan

Interface VLAN 2 on IPSec Service Module port Gi7/0/1 connected to VLAN 502 with crypto
map set testtag_1
Interface VLAN 3 on IPSec Service Module port Gi7/0/1 connected to VLAN 503 with crypto
map set testtag_2
Interface VLAN 4 on IPSec Service Module port Gi7/0/1 connected to VLAN 504 with crypto
map set testtag_3

Router# show vlan id 2

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0002                         active    Gi7/0/1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Router# show vlan id 502

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
502  VLAN0502                         active    Gi1/3, Gi7/0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
502  enet  100502     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Router#
```

Troubleshooting IPsec Stateful Failover (VPN High Availability)

If you find that either the active or standby IPsec stateful failover (VPN high availability) processes do not function as expected, you can perform the following checks:

- Use the **show ssp** command to verify the SSP process is running.
- Make sure that both switches share identical IPsec configurations. This is critical. If switches are configured differently, IPsec stateful failover (VPN high availability) will not work.

Note Support for IPsec stateful failover is removed in Cisco IOS Release 12.2SXH. The feature is supported in Cisco IOS Release 12.2SXF.

- Verify that an IPsec connection can be formed with existing maps, transforms, and access lists.
- Configure HSRP on the inside and outside interfaces and make the HSRP groups track one another. Verify this works properly by performing a **shut** command on either of the interfaces, then observe that the HSRP standby switch takes active control from the active switch.
- Verify that SSP peers can see each other by performing a **show ssp peer** command on both the active and standby switches.
- Bind the IKE and IPsec to SSP and send traffic over the tunnels. You can view high availability (HA) messages on the standby switch as both the active and standby switches synchronize.
- HSRP settings may require adjustments depending on the interface employed, such as Fast Ethernet or Gigabit Ethernet.

Checking HSRP Settings

To check HSRP settings, perform this task:

	Command	Purpose
Step 1	`Router# show standby brief`	Ensures that the interfaces are synchronized.
Step 2	`Router# no standby delay timer`	Leaves the delay timers at their default settings
Step 3	`Router# show standby brief`	When the other switch comes online, enter the **show standby brief** command once again. If the output shows an interface on standby, you must set the standby switch's delay timer.

Clearing Dormant SAs on Standby Switches

To clear associated SA entries, perform this task:

	Command	Purpose
Step 1	`Router# clear crypto isakmp ha [standby][resync]`	Clears all dormant (standby) entries from the device. If the **resync** keyword is used, all standby IKE SAs will be removed, and a resynchronization of state will occur.
Step 2	`Router# clear crypto sa ha standby [peer ip address | resync]`	Clears all standby SAs for the device if **peer** is specified.

Enabling Debugging for HA

To enable debugging for HA, perform this task:

	Command	Purpose
Step 1	`Router# debug crypto isakmp ha [detail | fsm | update]`	Enables basic debug messages related to the IKE HA Manager.
Step 2	`Router# debug crypto ipsec ha [detail | fsm | update]`	Enables IPsec HA debugging
Step 3	`Router# debug ssp [fsm | socket | packet | peers | redundancy | config]`	Enables SSP debugging.

Troubleshooting a Blade Failure Group

To enable IPsec VPN SPA debugging for a blade failure group, enter the **debug crypto ace b2b** command:

```
Router# debug crypto ace b2b

ACE B2B Failover debugging is on
```

Troubleshooting IKE Policy and Transform Sets

Any IPsec transforms or IKE encryption methods that the current hardware does not support should be disabled; they are ignored whenever an attempt to negotiate with the peer is made.

If a user enters an IPsec transform or an IKE encryption method that the hardware does not support, a warning message will be generated. These warning messages are also generated at boot time. When an encrypted card is inserted, the current configuration is scanned. If any IPsec transforms or IKE encryption methods are found that are not supported by the hardware, a warning message will be generated.

Using Crypto Conditional Debug

The crypto conditional debug feature provides three command-line interface (CLI) commands that allow you to debug an IP Security (IPsec) tunnel on the basis of predefined crypto conditions such as the peer IP address, connection-ID of a crypto engine, and security parameter index (SPI). By limiting debug messages to specific IPsec operations and reducing the amount of debug output, you can better troubleshoot a switch with a large number of tunnels.

The crypto conditional debug commands (**debug crypto condition**, **debug crypto condition unmatched**, and **show crypto debug-condition**) allow you to specify conditions (filter values) in which to generate and display debug messages related only to the specified conditions.

Table 30-2 lists the supported condition types.

Table 30-2 Supported Condition Types for Crypto Conditional Debug Commands

Condition Type (Keyword)	Description
connid	An integer between 1 and 32766. Relevant debug messages will be shown if the current IPsec operation uses this value as the connection-ID to interface with the crypto engine.
flowid	An integer between 1 and 32766. Relevant debug messages will be shown if the current IPsec operation uses this value as the flow-ID to interface with the crypto engine.
fvrf	The name string of a virtual private network (VPN) routing and forwarding (VRF) instance. Relevant debug messages will be shown if the current IPsec operation uses this VRF instance as its front-door VRF (FVRF).
ivrf	The name string of a VRF instance. Relevant debug messages will be shown if the current IPsec operation uses this VRF instance as its inside VRF (IVRF).
peer group	A Unity group name string. Relevant debug messages will be shown if the peer is using this group name as its identity.
peer hostname	A fully qualified domain name (FQDN) string. Relevant debug messages will be shown if the peer is using this string as its identity.
peer ipv4	A single IP address. Relevant debug messages will be shown if the current IPsec operation is related to the IP address of this peer.
peer subnet	A subnet and a subnet mask that specify a range of peer IP addresses. Relevant debug messages will be shown if the IP address of the current IPsec peer falls into the specified subnet range.
peer username	A username string. Relevant debug messages will be shown if the peer is using this username as its identity.
spi	A 32-bit unsigned integer. Relevant debug messages will be shown if the current IPsec operation uses this value as the SPI.

Note If **connid**, **flowid**, or **spi** is used as a debug condition, the debug messages for a related IPsec flow are generated. An IPsec flow has two connection-IDs, flow-IDs, and SPI values—one inbound and one outbound. Either one of the two connection-IDs, flow-IDs, and SPI values can be used as the debug condition that triggers debug messages for the IPsec flow.

Crypto Conditional Debug Configuration Guidelines and Restrictions

When configuring crypto conditional debug, follow these guidelines and restrictions:

- This feature does not support debug message filtering for hardware crypto engines.
- Although conditional debugging is useful for troubleshooting peer-specific or functionality-related Internet Key Exchange (IKE) and IPsec problems, conditional debugging may not be able to define and check large numbers of debug conditions.
- Because extra space is needed to store the debug condition values, additional processing overhead is added to the CPU and memory usage is increased. Thus, enabling crypto conditional debugging on a switch with heavy traffic should be used with caution.
- Your switch will perform conditional debugging only after at least one of the global crypto debug commands (**debug crypto isakmp**, **debug crypto ipsec**, or **debug crypto engine**) has been enabled. This requirement helps to ensure that the performance of the switch will not be impacted when conditional debugging is not being used.

Enabling Crypto Conditional Debug Filtering

To enable crypto conditional debug filtering, perform the following tasks:

	Command	Purpose
Step 1	`Router# enable`	Enables privileged EXEC mode.
Step 2	`Router# debug crypto condition [connid integer engine-id integer] [flowid integer engine-id integer] [fvrf string] [ivrf string] [peer [group string] [hostname string] [ipv4 ipaddress] [subnet subnet mask] [username string]] [spi integer] [reset]`	Defines conditional debug filters. See Table 30-2 for descriptions of values.
Step 3	`Router# show crypto debug-condition {[peer] [connid] [spi] [fvrf] [ivrf] [unmatched]}`	Displays crypto debug conditions that have already been enabled in the switch.
Step 4	`Router# debug crypto isakmp`	Enables global IKE debugging.
Step 5	`Router# debug crypto ipsec`	Enables global IPsec debugging.
Step 6	`Router# debug crypto engine`	Enables global crypto engine debugging.
Step 7	`Router# debug crypto condition unmatched [isakmp | ipsec | engine]`	(Optional) Displays debug conditional crypto messages when no context information is available to check against debug conditions. If none of the optional keywords are specified, all crypto-related information will be shown.

Disabling Crypto Conditional Debugging

Before you disable crypto conditional debugging, you must first disable any crypto global debug CLIs that you have issued. You can then disable crypto conditional debugging. To disable crypto conditional debugging, enter the following command:

```
Router# debug crypto condition reset
```

Enabling Crypto Error Debug Messages

Enabling the **debug crypto error** command displays only error-related debug messages, which allows you to easily determine why a crypto operation, such as an IKE negotiation, has failed within your system. To enable crypto error debug messages, enter the following command from privileged EXEC mode:

```
Router# debug crypto {isakmp | ipsec | engine} error
```

Note When enabling this command, ensure that global crypto debug commands are not enabled; otherwise, the global commands will override any possible error-related debug messages.

For complete configuration information for crypto conditional debug support, refer to this URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_dbcry.html

Preparing for Online Insertion and Removal of a SPA

The Catalyst 6500 Series switch supports online insertion and removal (OIR) of the SSC, in addition to each of the SPAs. You can remove an SSC with its SPAs still intact, or you can remove a SPA independently from the SSC, leaving the SSC installed in the switch.

An SSC can remain installed in the switch with one SPA remaining active while you remove another SPA from one of the SSC subslots. If you are not planning to immediately replace a SPA into the SSC, then be sure to install a blank filler plate in the subslot. The SSC should always be fully installed with either functional SPAs or blank filler plates.

For more information about activating and deactivating SPAs in preparation for OIR, see the “Preparing for Online Insertion and Removal of SIPs and SPAs” topic in the “Troubleshooting the SIPs and SSC” chapter in this guide.