

# Configuring High Availability Features for Site-to-Site IPsec VPNs

Document ID: 17826

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Configure

- Network Diagram
- Configurations

### How Does It Work?

#### Normal Circumstance (Before Failover)

- After HSRP and IPsec Failover
- After the Original HSRP Primary Router Recovers from an Outage

#### Related Information

## Introduction

This document describes the new, high-availability features for site-to-site IPsec VPN networks. Hot Standby Router Protocol (HSRP) is often used to track routers' interface status to achieve failover between routers. However, because no internal correlation exists between IPsec and HSRP, HSRP does not track the state of IPsec security associations (SAs) and IPsec requires schemes in order to synchronize with HSRP failover when it occurs. These are some highlights of the schemes used to provide a closer coupling between IPsec and HSRP:

- Internet Key Exchange (IKE) keepalive is used to allow IPsec to detect HSRP failover in time.
- The crypto map applied on a specific router interface is linked with the HSRP group already configured on that interface to make IPsec aware of HSRP setup. This also allows IPsec to use the HSRP virtual IP address as the Internet Security Association and Key Management Protocol (ISAKMP) identity of the HSRP routers.
- The reverse route injection (RRI) feature is used to allow dynamic routing information updates during the HSRP and IPsec failover.

**Note:** This Document describes how to use Hot Standby Router Protocol (HSRP) with VPN. HSRP is also used to track failed ISP links. In order to configure redundant ISP links on routers, refer to Analyzing IP Service Levels Using the ICMP Echo Operation. Here the source device is the router and the destination device is the ISP device.

## Prerequisites

### Requirements

There are no specific prerequisites for this document.

## Components Used

The information in this document is based on these software and hardware versions:

- Cisco 7200 Series Routers
- Cisco IOS® Software Release 12.3(7)T1, c7200-a3jk9s-mz.123-7.T1

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

## Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

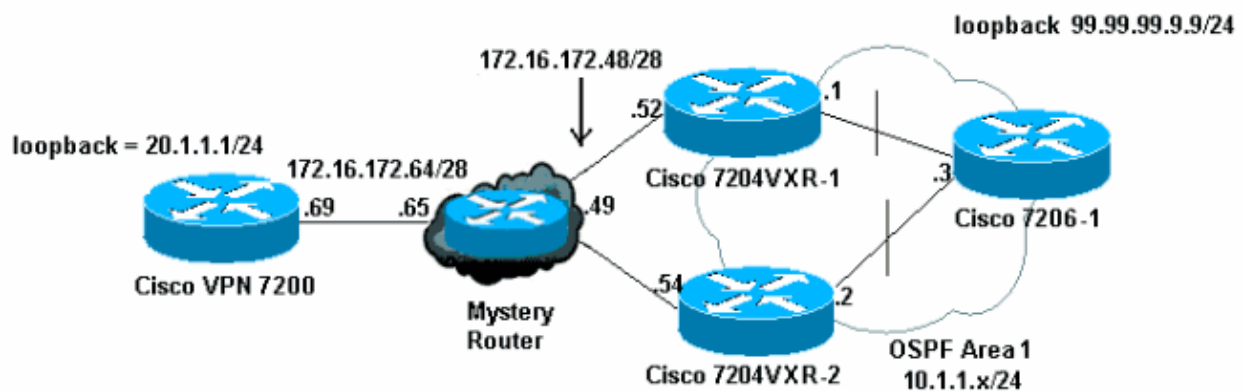
## Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

## Network Diagram

This document uses this network setup:



## Configurations

This document uses these configurations:

- Cisco VPN 7200 Configuration
- Cisco 7204VXR-1 Configuration
- Cisco 7204VXR-2 Configuration
- Cisco 7206-1 Configuration

### Cisco VPN 7200 Configuration

```
vpn7200#show run
Building configuration...
```

```
Current configuration : 1854 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname vpn7200
!
!
ip subnet-zero
ip cef

!--- Defines ISAKMP policy and IKE pre-shared key for
!--- IKE authentication. Note that 172.16.172.53 is the
!--- HSRP virtual IP address of the remote HSRP routers.

crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 172.16.172.53

!--- IKE keepalive to detect the IPsec liveness of the remote
!--- VPN router. When HSRP failover happens, IKE keepalive
!--- will detect the HSRP router switchover.

crypto isakmp keepalive 10
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac

!--- Defines crypto map. Note that the peer address is the
!--- HSRP virtual IP address of the remote HSRP routers.

crypto map vpn 10 ipsec-isakmp
set peer 172.16.172.53
set transform-set myset
match address 101
!
interface Loopback0
ip address 20.1.1.1 255.255.255.255
!
interface FastEthernet0/0
ip address 10.48.66.66 255.255.254.0
duplex full
speed 100
!
interface FastEthernet0/1
ip address 172.16.172.69 255.255.255.240
duplex full
speed 100
crypto map vpn
!
ip classless
ip route 10.1.1.0 255.255.255.0 172.16.172.65
ip route 99.99.99.99 255.255.255.255 172.16.172.65
ip route 172.16.172.48 255.255.255.240 172.16.172.65
no ip http server
!
access-list 101 permit ip 20.1.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 101 permit ip 20.1.1.0 0.0.0.255 host 99.99.99.99
!
line con 0
exec-timeout 0 0
line aux 0
```

```
line vty 0 4
login
!
end
```

### Cisco 7204VXR-1 Configuration

```
7204VXR-1#show run
Building configuration...

Current configuration : 1754 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 7204VXR-1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
!
ip cef!

!--- Defines ISAKMP policy.

crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 172.16.172.69
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac

!--- Defines crypto map. Note that "reverse-route"
!--- turns on the RRI feature.

crypto map vpn 10 ipsec-isakmp
set peer 172.16.172.69
set transform-set myset
match address 101
reverse-route
!
!

!--- Define HSRP under the interface. HSRP will track the
!--- internal interface as well. HSRP group name must be
!--- defined here and will be used for IPSec configuration.
!--- The "redundancy" keyword in the crypto map command
!--- specifies the HSRP group to which IPSec will couple.
!--- In normal circumstances, this router will be the HSRP
!--- primary router since it has higher priority than the
!--- other HSRP router.

interface FastEthernet0/0
ip address 172.16.172.52 255.255.255.240
```

```
duplex full
speed 100
standby 1 ip 172.16.172.53
standby 1 priority 200
standby 1 preempt
standby 1 name VPNHA
standby 1 track FastEthernet0/1 150
crypto map vpn redundancy VPNHA
!
interface FastEthernet0/1
ip address 10.1.1.1 255.255.255.0
duplex full
speed 100
!
interface ATM1/0
no ip address
shutdown
no atm ilmi-keepalive
!
interface FastEthernet3/0
no ip address
shutdown
duplex half
!
interface ATM6/0
no ip address
shutdown
no atm ilmi-keepalive

!---- Define dynamic routing protocol and re-distribute static
!---- route. This enables dynamic routing information update
!---- during the HSRP/IPSec failover. All the "VPN routes"
!---- that are injected in the routing table by RRI as static
!---- routes will be redistributed to internal networks.

!
router ospf 1
log-adjacency-changes
redistribute static subnets
network 10.1.1.0 0.0.0.255 area 0
!
ip classless
ip route 172.16.172.64 255.255.255.240 172.16.172.49
no ip http server
no ip http secure-server
!
!

!---- Defines VPN traffic. The destination IP subnet will be
!---- injected into the routing table as static routes by RRI.

access-list 101 permit ip 10.1.1.0 0.0.0.255 20.1.1.0 0.0.0.255
access-list 101 permit ip host 99.99.99.99 20.1.1.0 0.0.0.255
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
!
!
!
end
```

## Cisco 7204VXR-2 Configuration

```
7204VXR-2#show run
Building configuration...

Current configuration : 2493 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 7204VXR-2
!
boot-start-marker
boot system flash disk1:c7200-a3jk9s-mz.123-7.T1
boot-end-marker
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
ip host rund 10.48.92.61
!
!
ip cef
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 172.16.172.69
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 172.16.172.69
set transform-set myset
match address 101
reverse-route
!

!--- During normal operational conditions this router
!--- will be the standby router.

interface FastEthernet0/0
ip address 172.16.172.54 255.255.255.240
ip directed-broadcast
duplex full
standby 1 ip 172.16.172.53
standby 1 preempt
standby 1 name VPNHA
standby 1 track FastEthernet1/0
crypto map vpn redundancy VPNHA
!
interface FastEthernet1/0
ip address 10.1.1.2 255.255.255.0
ip directed-broadcast
duplex full
!
interface FastEthernet3/0
ip address 10.48.67.182 255.255.254.0
ip directed-broadcast
shutdown
```

```

duplex full
!
router ospf 1
log-adjacency-changes
redistribute static subnets
network 10.1.1.0 0.0.0.255 area 0
!
ip classless

ip route 172.16.172.64 255.255.255.240 172.16.172.49
no ip http server
no ip http secure-server
!
!
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 20.1.1.0 0.0.0.255
access-list 101 permit ip host 99.99.99.99 20.1.1.0 0.0.0.255
!
line con 0
exec-timeout 0 0
transport preferred all
transport output all
stopbits 1
line aux 0
transport preferred all
transport output all
stopbits 1
line vty 0 4
login
transport preferred all
transport input all
transport output all
!
!
!
end

```

### Cisco 7206-1 Configuration

```

7206-1#show run
Building configuration...

Current configuration : 1551 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname 7206-1
!
ip subnet-zero
no ip source-route
ip cef
!
interface Loopback0
ip address 99.99.99.99 255.255.255.255
!
interface FastEthernet0/0
shutdown
duplex full
speed 100
!

```

```

!--- Define dynamic routing protocol. All the "VPN routes"
!--- will be learned and updated dynamically from upstream HSRP
!--- routers using the dynamic routing protocols.

interface FastEthernet0/1
ip address 10.1.1.3 255.255.255.0
duplex full
speed 100
!
router ospf 1
log-adjacency-changes
passive-interface Loopback0
network 10.1.1.0 0.0.0.255 area 0
network 99.99.99.99 0.0.0.0 area 0
!
ip classless
no ip http server
!
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end

```

## How Does It Work?

This example demonstrates how HSRP and IPSec failover work together using the above setup and configuration. Three aspects are highlighted in this case study:

- HSRP failover due to interface failure.
- How IPSec failover happens after HSRP failover. As can be seen, IPSec failover here will be "stateless" failover.
- How the routing information changes caused by the failover are dynamically updated and propagated to internal networks.

**Note:** The test traffic here is Internet Control Message Protocol (ICMP) packets between the loopback IP address of the Cisco 7206-1 (99.99.99.99) and the loopback IP address of the Cisco VPN 7200 (20.1.1.1) and simulates the VPN traffic between the two sites.

## Normal Circumstance (Before Failover)

Before failover, the Cisco 7204VXR-1 is the primary HSRP router and the Cisco VPN 7200 has IPSec SAs with the Cisco 7204VXR-1.

When the crypto map is configured on the interface, the RRI feature injects a VPN route to match the configured IPSec access control list (ACL) and the **set peer** command statement in the crypto map. This route is added to the routing table of the primary HSRP router 7204VXR-1.

The output of the **debug crypto ipsec** command indicates the addition of VPN route 20.1.1/24 to the Routing Information Base (RIB).

```

IPSEC(rte_mgr): VPN Route Added 20.1.1.0 255.255.255.0
via 172.16.172.69 in IP DEFAULT TABLE

```



The routing table on the primary HSRP router yields a static route to 20.1.1/24, which is redistributed by Open Shortest Path First (OSPF) to the secondary HSRP router, 7204VXR-2, and to the internal router, 7206-1.

The next hop for the VPN route 20.1.1/24 injected as a static route into the RIB of router 7204VXR-1 is the IP address of the remote crypto peer. In this case, the next hop for the VPN route 20.1.1/24 is 172.16.172.69. The IP address of the next hop of the VPN route is resolved via a recursive route lookup as shown in this Cisco Express Forwarding table:

```
7204VXR-1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is not set

```
99.0.0.0/32 is subnetted, 1 subnets
O    99.99.99.99 [110/2] via 10.1.1.3, 00:11:21, FastEthernet0/1
20.0.0.0/24 is subnetted, 1 subnets
S    20.1.1.0 [1/0] via 172.16.172.69
172.16.0.0/28 is subnetted, 2 subnets
C    172.16.172.48 is directly connected, FastEthernet0/0
S    172.16.172.64 [1/0] via 172.16.172.49
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.1.0/24 is directly connected, FastEthernet0/1
S    10.48.66.0/23 [1/0] via 10.1.1.2
```

```
7204VXR-1#show ip cef 20.1.1.0 detail
20.1.1.0/24, version 66, epoch 0, cached adjacency 172.16.172.49
0 packets, 0 bytes
via 172.16.172.69, 0 dependencies, recursive
next hop 172.16.172.49, FastEthernet0/0 via 172.16.172.64/28
valid cached adjacency
```

The secondary HSRP router and the internal router 7206-1 learn this VPN route via OSPF/. Network administrators do not need to input the static route manually. More importantly, the routing changes caused by the failover are updated dynamically.

```
7204VXR-2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 10.48.66.1 to network 0.0.0.0

```
99.0.0.0/32 is subnetted, 1 subnets
O    99.99.99.99 [110/2] via 10.1.1.3, 00:29:31, FastEthernet1/0
20.0.0.0/24 is subnetted, 1 subnets
O E2    20.1.1.0 [110/20] via 10.1.1.1, 00:11:06, FastEthernet1/0
172.16.0.0/28 is subnetted, 2 subnets
C    172.16.172.48 is directly connected, FastEthernet0/0
S    172.16.172.64 [1/0] via 172.16.172.49
```

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.1.0/24 is directly connected, FastEthernet1/0
C    10.48.66.0/23 is directly connected, FastEthernet3/0
S*   0.0.0.0/0 [1/0] via 10.48.66.1
```

```
7206-1#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
99.0.0.0/32 is subnetted, 1 subnets
C    99.99.99.99 is directly connected, Loopback0
20.0.0.0/24 is subnetted, 1 subnets
O E2 20.1.1.0 [110/20] via 10.1.1.1, 00:14:01, FastEthernet0/1
172.16.0.0/28 is subnetted, 1 subnets
O E2 172.16.172.64 [110/20] via 10.1.1.1, 00:32:21, FastEthernet0/1
                                     [110/20] via 10.1.1.2, 00:32:21, FastEthernet0/1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.1.0/24 is directly connected, FastEthernet0/1
O E2 10.48.66.0/23 [110/20] via 10.1.1.2, 00:32:22, FastEthernet0/1
```

Router 7204VXR-1 is the primary HSRP router that tracks the internal interface Fa0/1.

```
7204VXR-1#show standby
FastEthernet0/0 - Group 1
State is Active
2 state changes, last state change 03:21:20
Virtual IP address is 172.16.172.53
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.172 secs
Preemption enabled
Active router is local
Standby router is 172.16.172.54,
  priority 100 (expires in 7.220 sec)
Priority 200 (configured 200)
Track interface FastEthernet0/1 state Up decrement 150
IP redundancy name is "VPNHA" (cfgd)
```

You can use the **show track** command to see a list of all objects tracked by HSRP.

```
7204VXR-1#show track
Track 1 (via HSRP)
Interface FastEthernet0/1 line-protocol
Line protocol is Up
1 change, last change 03:18:22
Tracked by:
HSRP FastEthernet0/0 1
```

Router 7204VXR-2 is the standby HSRP router. Under normal operational conditions, this device tracks the internal interface Fa1/0.

```
7204VXR-2#show standby
FastEthernet0/0 - Group 1
State is Standby
```

```

1 state change, last state change 02:22:30
Virtual IP address is 172.16.172.53
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.096 secs
Preemption enabled
Active router is 172.16.172.52,
priority 200 (expires in 7.040 sec)
Standby router is local
Priority 100 (default 100)
Track interface FastEthernet1/0 state Up decrement 10
IP redundancy name is "VPNHA" (cfgd)

```

These IPsec-related **show** commands yield output on the Cisco VPN 7200 router that demonstrates the ISAKMP and IPsec SAs between the Cisco VPN 7200 and the primary HSRP router, the Cisco 7204VXR-1.

```

7204VXR-1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption

C-id      Local      Remote      I-VRF  Encr  Hash  Auth  DH  Lifetime  Cap.
1         172.16.172.53  172.16.172.69          des  md5   psk   1   23:49:52  K
Connection-id:Engine-id = 1:1(software)

```

```

7204VXR-1#show crypto ipsec sa
interface: FastEthernet0/0
Crypto map tag: vpn, local addr. 172.16.172.53

protected vrf:
local ident (addr/mask/prot/port): (99.99.99.99/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
current_peer: 172.16.172.69:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.16.172.53, remote crypto endpt.: 172.16.172.69
path mtu 1500, media mtu 1500
current outbound spi: 44E0B22B

inbound esp sas:
spi: 0x5B23F22E(1529082414)
transform: esp-des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4504144/2949)
ike_cookies: B57A9DC9 FA2D627B F70FEDF6 FAAF9E34
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```

spi: 0x44E0B22B(1155576363)  
transform: esp-des esp-md5-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 2001, flow\_id: 2, crypto map: vpn  
crypto engine type: Software, engine\_id: 1  
sa timing: remaining key lifetime (k/sec): (4504145/2949)  
ike\_cookies: B57A9DC9 FA2D627B F70FEDF6 FAAF9E34  
IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcp sas:

vpn7200#show crypto isakmp sa

dst	src	state	conn-id	slot
172.16.172.53	172.16.172.69	QM_IDLE	1	0

7204VXR-2#show crypto ipsec sa

interface: FastEthernet0/1

Crypto map tag: vpn, local addr. 172.16.172.69

local ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)  
remote ident (addr/mask/prot/port): (99.99.99.99/255.255.255.255/0/0)  
current\_peer: 172.16.172.53  
PERMIT, flags={origin\_is\_acl,}  
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10  
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0  
#send errors 5, #recv errors 0

local crypto endpt.: 172.16.172.69, remote crypto endpt.: 172.16.172.53

path mtu 1500, ip mtu 1500

current outbound spi: 5B23F22E

inbound esp sas:

spi: 0x44E0B22B(1155576363)  
transform: esp-des esp-md5-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 2029, flow\_id: 1, crypto map: vpn  
sa timing: remaining key lifetime (k/sec): (4607997/2824)  
IV size: 8 bytes  
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x5B23F22E(1529082414)  
transform: esp-des esp-md5-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 2030, flow\_id: 2, crypto map: vpn  
sa timing: remaining key lifetime (k/sec): (4607998/2824)  
IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcp sas:

## After HSRP and IPSec Failover

The failover was triggered by shutting down Fa0/0 on the Cisco 7204VXR-1. You will see similar behavior if the other interface, Fa0/1, is down because HSRP also tracks the status of this interface.

When the Cisco VPN 7200 receives no response to IKE keepalive packets sent to the primary HSRP router, the router tears down the IPSec SAs.

This **debug crypto isakmp** command output shows how the IKE keepalive detects the outage of the primary router:

```
ISAKMP (0:1): received packet from 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): processing HASH payload. message ID = 1585108592
ISAKMP (0:1): processing NOTIFY ITS_ALIVE protocol 1
spi 0, message ID = 1585108592, sa = 61C3E754
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node -1484552386
ISAKMP (0:1): deleting node 1585108592 error FALSE
    reason "informational (in) state 1"
ISAKMP (0:1): purging node 642343711
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node -523181212
ISAKMP (0:1): purging node -2089541867
ISAKMP (0:1): incrementing error counter on sa: PEERS_ALIVE_TIMER
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node 1671177686
ISAKMP (0:1): incrementing error counter on sa: PEERS_ALIVE_TIMER
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node 1706520344
ISAKMP (0:1): incrementing error counter on sa: PEERS_ALIVE_TIMER
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node 503375209
ISAKMP (0:1): incrementing error counter on sa: PEERS_ALIVE_TIMER
ISAKMP (0:1): sending packet to 172.16.172.53 (I) QM_IDLE
ISAKMP (0:1): purging node 1272270610
ISAKMP (0:1): incrementing error counter on sa: PEERS_ALIVE_TIMER
ISAKMP (0:1): peer not responding!
ISAKMP (0:1): peer does paranoid keepalives.

ISAKMP (0:1): phase 1 going away; let's be paranoid.
ISAKMP (0:1): Bring down phase 2's
ISAKMP (0:1): That phase 1 was the last one of its kind.
    Taking phase 2's with us.
ISAKMP (0:1): peer does paranoid keepalives.

ISAKMP (0:1): deleting SA reason "P1 errcounter exceeded
    (PEERS_ALIVE_TIMER)" state (I)
    QM_IDLE (peer 172.16.172.53) input queue 0
IPSEC(key_engine): got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.16.172.53
IPSEC(delete_sa): deleting SA,
(sa) sa_dest= 172.16.172.69, sa_prot= 50,
sa_spi= 0x44E0B22B(1155576363),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2029
IPSEC(delete_sa): deleting SA,
(sa) sa_dest= 172.16.172.53, sa_prot= 50,
sa_spi= 0x5B23F22E(1529082414),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2030
ISAKMP (0:1): sending packet to 172.16.172.53 (I) MM_NO_STATE
ISAKMP (0:1): purging node -248155233
ISAKMP (0:1): peer does paranoid keepalives.

IPSEC(key_engine): got a queue event...
```

```
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.16.172.53
ISAKMP (0:1): purging node 958118275
```

When failover occurs on the Cisco 7204VXR-1 primary HSRP router, the device becomes a standby router. Existing ISAKMP and IPsec SAs are torn down. The Cisco 7204VXR-2 secondary HSRP router becomes active and establishes new IPsec SAs with the Cisco VPN 7200.

Output of the **debug standby events** command shows events related to HSRP.

```
HSRP: Fa0/0 API Software interface going down
HSRP: Fa0/0 API Software interface going down
HSRP: Fa0/0 Interface down
HSRP: Fa0/0 Grp 1 Active: b/HSRP disabled
HSRP: Fa0/0 Grp 1 Active router is unknown, was local
HSRP: Fa0/0 Grp 1 Standby router is unknown, was 172.16.172.54
HSRP: Fa0/0 Grp 1 Active -> Init
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Init
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Active -> Init
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.
Peer 172.16.172.69:500 Id: 172.16.172.69
HSRP: Fa0/0 Grp 1 Redundancy enquiry for VPNHA succeeded
HSRP: Fa0/0 API Add active HSRP addresses to ARP table
%LINK-5-CHANGED: Interface FastEthernet0/0,
changed state to administratively down
HSRP: API Hardware state change
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
```

Because the interface is shut down, the HSRP state changes to "Init".

```
paal#show standby
FastEthernet0/0 - Group 1
State is Init (interface down)
3 state changes, last state change 00:07:29
Virtual IP address is 172.16.172.53
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption enabled
Active router is unknown
Standby router is unknown
Priority 200 (configured 200)
Track interface FastEthernet0/1 state Up decrement 150
IP redundancy name is "VPNHA" (cfgd)
```

Cisco 7204VXR-2 becomes the active HSRP router and changes its state to "Active".

```
HSRP: Fa0/0 Grp 1 Standby: c/Active timer expired (172.16.172.52)
HSRP: Fa0/0 Grp 1 Active router is local, was 172.16.172.52
HSRP: Fa0/0 Grp 1 Standby router is unknown, was local
HSRP: Fa0/0 Grp 1 Standby -> Active (active 0->1, passive 2->1)
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Standby -> Active
```

```
!--- VPN route 20.1.1.0/24 is added to the routing table.
```

```
IPSEC(rte_mgr): VPN Route Added 20.1.1.0 255.255.255.0
via 172.16.172.69 in IP DEFAULT TABLE
```

```
7204VXR-2#show standby
FastEthernet0/0 - Group 1
State is Active
```

```

2 state changes, last state change 00:10:38
Virtual IP address is 172.16.172.53
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.116 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 100 (default 100)
Track interface FastEthernet1/0 state Up decrement 10
IP redundancy name is "VPNHA" (cfgd)

```

With RRI enabled, the VPN routes are updated dynamically during the failover. The static route 20.1.1.0/24 is removed, and Cisco 7204VXR-1 router learns the route from the Cisco 7204VXR-2 router.

The output from the **show ip route** command demonstrates this dynamic update.

```

7204VXR-1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    99.0.0.0/32 is subnetted, 1 subnets
O       99.99.99.99 [110/2] via 10.1.1.3, 02:46:16, FastEthernet0/1
20.0.0.0/24 is subnetted, 1 subnets
O E2    20.1.1.0 [110/20] via 10.1.1.2, 00:08:35, FastEthernet0/1
    172.16.0.0/28 is subnetted, 1 subnets
O E2    172.16.172.64 [110/20] via 10.1.1.2, 00:07:56, FastEthernet0/1
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, FastEthernet0/1
S       10.48.66.0/23 [1/0] via 10.1.1.2

```

The static VPN route is injected into the routing table on the Cisco 7204VXR-2 router.

```

7204VXR-2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    99.0.0.0/32 is subnetted, 1 subnets
O       99.99.99.99 [110/2] via 10.1.1.3, 03:04:18, FastEthernet1/0
20.0.0.0/24 is subnetted, 1 subnets
S       20.1.1.0 [1/0] via 172.16.172.69
    172.16.0.0/28 is subnetted, 2 subnets
C       172.16.172.48 is directly connected, FastEthernet0/0
S       172.16.172.64 [1/0] via 172.16.172.49
    10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet1/0

```

Internal router 7206-1 learns the 20.1.1/24 route to the remote VPN peer from its OSPF neighbor router, 7204VXR-2. These routing changes occur dynamically through the combination of HSRP/RRI and OSPF.

```
7206-1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    99.0.0.0/32 is subnetted, 1 subnets
C       99.99.99.99 is directly connected, Loopback0
    20.0.0.0/24 is subnetted, 1 subnets
O E2    20.1.1.0 [110/20] via 10.1.1.2, 00:13:55, FastEthernet0/1
    172.16.0.0/28 is subnetted, 1 subnets
O E2    172.16.172.64 [110/20] via 10.1.1.2, 00:13:17, FastEthernet0/1
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, FastEthernet0/1
O E2    10.48.66.0/23 [110/20] via 10.1.1.2, 03:06:08, FastEthernet0/1
```

After Cisco 7204VXR-2 becomes the active router during HSRP failover, the VPN traffic between the Cisco 7204VXR-2 and Cisco VPN 7200 router brings up ISAKMP and IPsec SAs.

The output of the **show crypto isakmp sa** and **show crypto ipsec sa** commands on the VPN 7200 router is shown here:

```
7204VXR-2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption

C-id      Local                               Remote                               I-VRF      Encr Hash Auth DH Lifetime
1         172.16.172.53 172.16.172.69                      des md5    psk 1    23:53:47 K
Connection-id:Engine-id = 1:1(software)

7204VXR-2#show crypto ipsec sa

interface: FastEthernet0/0
Crypto map tag: vpn, local addr. 172.16.172.53

protected vrf:
local ident (addr/mask/prot/port): (99.99.99.99/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
current_peer: 172.16.172.69:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.16.172.53, remote crypto endpt.: 172.16.172.69
path mtu 1500, media mtu 1500
current outbound spi: 83827275
```



```

inbound esp sas:
spi: 0x8D70E8A3(2372987043)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4453897/3162)
ike_cookies: 95074F89 3FF73F2B F70FEDF6 5998090C
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x83827275(2206364277)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4453898/3162)
ike_cookies: 95074F89 3FF73F2B F70FEDF6 5998090C
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas: vpn7200#show crypto isa sa
dst          src          state   conn-id slot
172.16.172.53 172.16.172.69 QM_IDLE 1       0

vpn7200#show crypto ipsec sa

interface: FastEthernet0/1
Crypto map tag: vpn, local addr. 172.16.172.69

local ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (99.99.99.99/255.255.255.255/0/0)
current_peer: 172.16.172.53
PERMIT, flags={origin_is_acl,}
#pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
#pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 6, #recv errors 0

local crypto endpt.: 172.16.172.69, remote crypto endpt.: 172.16.172.53
path mtu 1500, ip mtu 1500
current outbound spi: 8D70E8A3

inbound esp sas:
spi: 0x83827275(2206364277)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2029, flow_id: 1, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4607997/3070)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

```

```

outbound esp sas:
spi: 0x8D70E8A3(2372987043)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2030, flow_id: 2, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4607998/3070)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

```

## After the Original HSRP Primary Router Recovers from an Outage

After the service recovers on the Cisco 7204VXR-1 original HSRP primary router, the device resumes position as active router because it has a higher priority and because HSRP preempt is configured.

The **show** and **debug** command output from different routers shows another switchover of HSRP and IPsec. The ISAKMP and IPsec SAs are reestablished automatically, and the routing information changes are updated dynamically.

This sample output shows that router 7204VXR-1 changes its state to "Active".

```

HSRP: Fa0/0 API 172.16.172.52 is not an HSRP address
HSRP: Fa0/0 API MAC address update
HSRP: Fa0/0 API Software interface coming up
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
HSRP: API Hardware state change
HSRP: Fa0/0 API Software interface coming up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
  changed state to up
HSRP: Fa0/0 Interface up
HSRP: Fa0/0 Starting minimum interface delay (1 secs)
HSRP: Fa0/0 Interface min delay expired
HSRP: Fa0/0 Grp 1 Init: a/HSRP enabled
HSRP: Fa0/0 Grp 1 Init -> Listen
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Init -> Backup
HSRP: Fa0/0 Grp 1 Listen: c/Active timer expired (unknown)
HSRP: Fa0/0 Grp 1 Listen -> Speak
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Backup -> Speak
HSRP: Fa0/0 Grp 1 Speak: d/Standby timer expired (unknown)
HSRP: Fa0/0 Grp 1 Standby router is local
HSRP: Fa0/0 Grp 1 Speak -> Standby
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Speak -> Standby
HSRP: Fa0/0 Grp 1 Redundancy enquiry for VPNHA succeeded
HSRP: Fa0/0 Grp 1 Standby: c/Active timer expired (unknown)
HSRP: Fa0/0 Grp 1 Active router is local
HSRP: Fa0/0 Grp 1 Standby router is unknown, was local
HSRP: Fa0/0 Grp 1 Standby -> Active
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Standby -> Active
HSRP: Fa0/0 Grp 1 Active: i/Resign rcvd (100/172.16.172.54)
HSRP: Fa0/0 Grp 1 Redundancy group VPNHA state Active -> Active
HSRP: Fa0/0 Grp 1 Redundancy group VPNHA state Active -> Active
HSRP: Fa0/0 Grp 1 Standby router is 172.16.172.54

```

Router 7204VXR-2 changes its state to "Standby". The VPN route is removed from the routing table.

```

HSRP: Fa0/0 Grp 1 Standby router is 172.16.172.52
HSRP: Fa0/0 Grp 1 Hello in 172.16.172.52 Active pri 200 vIP 172.16.172.53
hel 3000 hol 10000 id 0000.0c07.ac01
HSRP: Fa0/0 Grp 1 Active router is 172.16.172.52, was local

```

```
HSRP: Fa0/0 Grp 1 Standby router is unknown, was 172.16.172.52
HSRP: Fa0/0 Grp 1 Active: g>Hello rcvd from
      higher pri Active router (200/172.16.172.52)
HSRP: Fa0/0 Grp 1 Active -> Speak (active 1->0, passive 0->1)
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Speak
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Active -> Speak
HSRP: Fa0/0 Grp 1 Speak: d/Standby timer expired (unknown)
HSRP: Fa0/0 Grp 1 Standby router is local
HSRP: Fa0/0 Grp 1 Speak -> Standby (active 0, passive 1)
HSRP: Fa0/0 Grp 1 Redundancy "VPNHA" state Speak -> Standby
HSRP: Fa0/0 Grp 1 Redundancy enquiry for VPNHA succeeded
addr 172.16.172.53 name VPNHA state Speak
active 172.16.172.52 standby 172.16.172.54
```

*!--- The VPN route is removed.*

```
IPSEC(rte_mgr): VPN Route Removed 20.1.1.0 255.255.255.0
via 172.16.172.69 in IP DEFAULT TABLE
```

## Related Information

- [IPSec Negotiation/IKE Protocols Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Sep 08, 2004

Document ID: 17826

---