Hoot and Holler over V^{3}PN Configuration Example

This document provides a configuration example that illustrates a basic multicast-based voice application over a Cisco Virtual Private Network (VPN).

Contents

Introduction

This document provides a configuration example for Cisco Voice and Video over VPN (V^{3}PN). The voice application used in this example is Hoot and Holler, which is typically used in trading floor financial institutions for communications to branch offices. The configuration scenario emphasizes implementation of the quality of service (QoS) and VPN capabilities; the configuration has the following characteristics:

- All traffic between two client branch sites and headquarters passes through a VPN of IPSec-encrypted tunnels.
- This implementation of Cisco V^{3}PN features the use of Protocol Independent Multicast (PIM) in Sparse Mode and Auto-RP. The routing protocol used to transport traffic is Open Shortest Path First (OSPF).
- The techniques used include Internet Key Exchange/Dead Peer Detection (IKE/DPD), split tunneling, and group policy on the server with Domain Name System (DNS) information, Windows Information Name Service (WINS) information, domain name, and an IP address pool for clients.
- Headquarters uses a Cisco 3800 series router with an ATM interface.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- One branch uses a Cisco 2800 series router and employs a serial interface, while another branch with a Cisco 2800 Series router uses a Symmetrical High-Speed Digital Subscriber Line (SHDSL) interface.
- The various **show** commands demonstrate configurations for the Internet Security Association Key Management Protocol (ISAKMP) and IP Security (IPSec) security associations (SA) on the concentrator, as well as status on the clients.

Prerequisites

The following sections provide information important to understand this configuration example. Read these sections before you continue with the configuration example:

Requirements

There are no specific requirements for this document.

Components Used

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

- At Headquarters, a Cisco 3845 router with a Cisco CallManager cluster, with ATM access to the Internet
- At Branch 1, a Cisco 2801 router with a WIC-SHDSL-V2 interface card installed, and with DSL access to the Internet
- At Branch 2, a Cisco 2811 router with a serial interface connection to the Internet
- Cisco IOS Release 12.3(11)T or later releases
- Advanced Enterprise Services feature set

The information presented in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with the following hardware and software:

- Cisco 2800 series routers
- Cisco 3800 series routers
- For Cisco 2800 series routers, Cisco IOS Release 12.3(8)T4 or later releases. For Cisco 3800 series routers, Cisco IOS Release 12.3(11)T and later releases.

Conventions

For information on document conventions, see the *Cisco Technical Tips Conventions*.

Configure

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

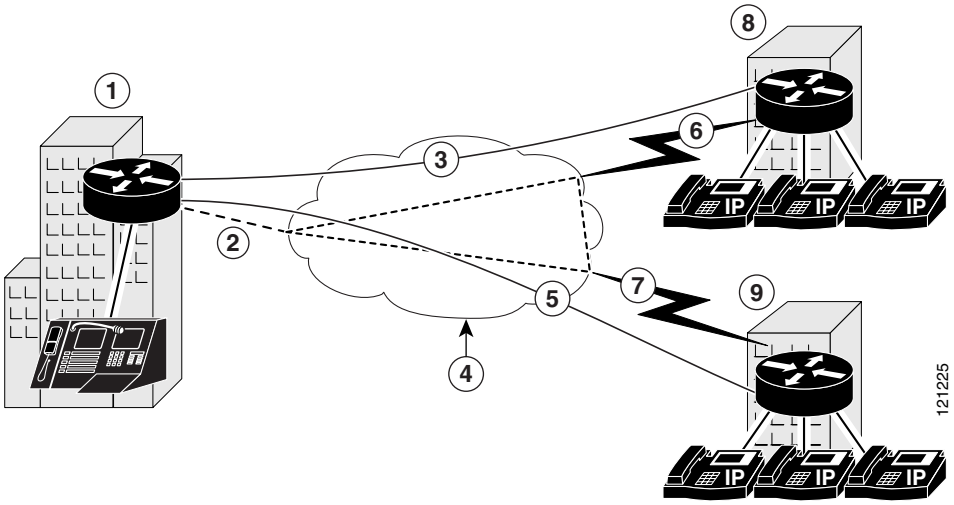
Note For additional information on the commands used in this document, use the Cisco IOS Command Lookup tool. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

Configuration Tips

- Make sure that the tunnels work before you apply the crypto maps.
- Apply IPSec crypto maps to both the tunnel interface and the physical interface.

Network Diagram

This document uses the network setup shown in the diagram below.



Following are the callout terms and definitions for the diagram, identified by number:

1	Headquarters location	**6**	DSL link from the Branch 1 router to the Internet
2	ATM link from the Headquarters router to the Internet	**7**	Serial link from the Branch 2 router to the Internet
3	VPN tunnel through the Internet to Branch 1	**8**	Branch 1 location
4	The Internet, as represented by the cloud	**9**	Branch 2 location
5	VPN tunnel through the Internet to Branch 2		

The Headquarters location (callout 1) uses a Cisco 3845 router with these characteristics:

- ATM access to the Internet
- Operating in a Cisco CallManager cluster
- Public IP address: 10.32.152.26
- Private IP address pool: 192.168.1.0/24

The Branch 1 location (callout 8) uses a Cisco 2801 router with these characteristics:

- DSL access to the Internet
- WIC-SHDSL-V2 interface card installed
- Public IP address: 10.32.153.32
- Private IP address pool: 192.168.2.0/24

The Branch 2 location (callout 9) uses a Cisco 2811 router with these characteristics:

- Serial access to the Internet
- Public IP address: 10.32.150.46/30
- Private IP address pool: 192.168.3.0/24

Configurations

This document uses the following configurations:

- Headquarters Office Configuration (Cisco 3845 Router), page 4
- Branch 1 Router Configuration (Cisco 2801 Router), page 9
- Branch 2 Router Configuration (Cisco 2811 Router), page 14

Headquarters Office Configuration (Cisco 3845 Router)

```
HUB-R1# show running-config

Building configuration...

Current configuration : 9385 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
service password-encryption
!
hostname HUB-R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$t8oN$hXmGodPh8ZM/ka6k/9aO51
!
username cisco secret 5 $1$cfjP$kKpBWe3pfKXfpK0RIqX/E.
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate slot 3
no network-clock-participate slot 4
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate wic 3
no network-clock-participate aim 0
no network-clock-participate aim 1
aaa new-model
!
!
! ENABLE AAA AND USE LOCAL AUTHENTICATION FOR VPN CONNECTIONS
!
aaa authentication login USERLIST local
aaa session-id common
ip subnet-zero
ip cef
!
! CREATE DHCP POOL FOR INTERNAL CLIENTS ON VLAN 10
!
ip dhcp excluded-address 192.168.1.1
!
ip dhcp pool LOCAL
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
!
!
no ip domain lookup
ip domain name cisco.com
! ENABLE MULTICAST ROUTING
ip multicast-routing
ip ids po max-events 100
no ftp-server write-enable
voice-card 0
 no dspfarm
!
!
!
voice class permanent 1
 signal timing oos timeout 65535
 signal keepalive disabled
 signal sequence oos no-action
!
!
controller T1 0/2/0
 framing sf
 linecode ami
!
controller T1 0/2/1
 framing sf
 linecode ami
```

```
! CLASSIFY DIFFERENT QOS TRAFFIC, SETTING IP PRECEDENCE AND DSCP
!
class-map match-all data
 match ip precedence 2
class-map match-all control-traffic
 match ip dscp af31
class-map match-all video
 match ip precedence 4
class-map match-all voice
 match ip dscp ef
!
!
! ALLOCATE AVAILABLE BANDWIDTH FOR EACH QOS CLASSIFICATION, DEPENDING ON EXPECTED NEED
! FOR EXAMPLE, DSCP VALUE EF (CLASS VOICE) WILL BE GIVEN 35% OF THE BANDWIDTH
!
policy-map LLQ
 class control-traffic
  bandwidth percent 5
 class voice
  priority percent 35
 class video
  bandwidth percent 15
 class data
  bandwidth percent 20
 class class-default
  fair-queue
!
!
! SET THE IKE POLICY TO USE 3DES
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
!SPECIFY THAT ISAKMP CLIENTS (SPOKE ROUTERS) WILL NOT NEED TO USE XAUTH (USERNAME AND
PASSWORD) WHEN CONNECTING
!
crypto isakmp key cisco address 10.32.150.46 no-xauth
crypto isakmp key cisco address 10.32.153.34 no-xauth
!
!
crypto ipsec transform-set TRANSFORM_1 esp-3des esp-sha-hmac
!
! DEFINE THE REMOTE SPOKES, THEIR IP ADDRESSES AND ANY POLICIES THAT NEED TO BE
IMPLEMENTED
crypto map INT_CM 1 ipsec-isakmp
 description === Peer device = Branch-2 ===
 set peer 10.32.150.46
 set security-association lifetime kilobytes 530000000
 set security-association lifetime seconds 14400
 set transform-set TRANSFORM_1
 match address IPSEC_ACL_1
crypto map INT_CM 2 ipsec-isakmp
 description === Peer device = Branch-1 ===
 set peer 10.32.153.34
 set security-association lifetime kilobytes 530000000
 set security-association lifetime seconds 14400
 set transform-set TRANSFORM_1
 match address IPSEC_ACL_2
!
!
!
```

```
! CREATE TUNNELS TO THE SPOKE ROUTERS. THE MTU IS LOWERED TO ALLOW THE GRE AND IP-SEC
HEADER
! PIM SD IS ENABLED SO AS TO ALLOW MULTICAST, AND THE TUNNEL SOURCE AND DESTINATION ARE
SPECIFIED
!
interface Tunnel0
 description === Peer device = Branch-2 ===
 bandwidth 10000
 ip unnumbered Vlan10
 ip mtu 1420
 ip pim sparse-dense-mode
 qos pre-classify
 tunnel source ATM1/0
 tunnel destination 10.32.150.46
 crypto map INT_CM
!
interface Tunnel1
 description === Peer device = Branch-1 ===
 bandwidth 10000
 ip unnumbered Vlan10
 ip mtu 1420
 ip pim sparse-dense-mode
 qos pre-classify
 tunnel source ATM1/0
 tunnel destination 10.32.153.34
 crypto map INT_CM
!
! THIS LOOPBACK INTERFACE ACTS AS THE MULTICAST RP
!
interface Loopback100
 ip address 192.168.4.1 255.255.255.255
 ip pim sparse-dense-mode
!
! THIS VIF INTERFACE IS USED AS THE MULTICAST SOURCE FOR THE VOICE ENDPOINT
interface Vif1
 ip address 192.168.6.1 255.255.255.0
 ip pim sparse-dense-mode
!
! NOT USED
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
! NOT USED
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
! INTERFACE CONNECTING TO THE PUBLIC NETWORK IN OUR SCENARIO
! ATM PVC 10/100 IS USED IN THIS EXAMPLE. THE PREVIOUSLY DEFINED LLQ QOS POLICY IS USED
HERE
interface ATM1/0
 description === Public interface ===
 bandwidth 155000
```

```
 ip address 10.32.152.26 255.255.255.252
 ip ospf network point-to-point
 no atm ilmi-keepalive
 crypto map INT_CM
 pvc 10/100
  protocol ip 10.32.152.25 broadcast
  vbr-rt 100000 100000
  service-policy output LLQ
 !
! PLACE ALL SWITCHPORT INTERFACES INTO VLAN 10
!
interface FastEthernet4/0
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/1
 switchport access vlan 10
 no ip address
!
! ... REDUNDANT FAST ETHERNET CONFIGURATION OMITTED.
!
interface FastEthernet4/15
 switchport access vlan 10
 no ip address
!
interface GigabitEthernet4/0
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
! INTERFACE FOR CONNECTING INTERNAL HOSTS.
!
interface Vlan10
 description === Private interface ===
 ip address 192.168.1.1 255.255.255.0
 ip pim sparse-dense-mode
!
! ENABLE ROUTING FOR ALL RELEVANT NETWORKS (INTERNAL USER SUBNET, LOOPBACK FOR RP AND VIF
FOR VOICE)
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.4.1 0.0.0.0 area 0
 network 192.168.6.0 0.0.0.255 area 0
!
! DEFINE STATIC ROUTES SO THAT THE REMOTE NETWORKS STAY IN THE ROUTING TABLE, EVEN IF
CONNECTION IS LOST
! THIS PREVENTS ROUTING TABLE FLAPS
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.32.152.25
ip route 192.168.2.0 255.255.255.0 Null0 249
ip route 192.168.3.0 255.255.255.0 Null0 249
!
ip http server
no ip http secure-server
!
! CONFIGURE AUTOMATIC DISCOVERY OF GROUP-TO-RENDEZVOUS POINT (AUTO-RP)
!
ip pim send-rp-announce Loopback100 scope 5
ip pim send-rp-discovery Loopback100 scope 5
```

```
! SPECIFY TRAFFIC TO BE ENCRYPTED (HERE IT'S ALL GRE TRAFFIC)
!
ip access-list extended IPSEC_ACL_1
 permit gre host 10.32.152.26 host 10.32.150.46
ip access-list extended IPSEC_ACL_2
 permit gre host 10.32.152.26 host 10.32.153.34
!
!
control-plane
!
!CONFIGURE THE VOICE PORT AND LINK IT TO DIAL-PEER 100. THIS CONNECTION IS PERMANENT. THE
VOICE-CLASS WAS DEFINED EARLIER IN THE CONFIGURATION, AND ESTABLISHES AN 'ALWAYS ON'
CONNECTION
!
voice-port 0/1/0
 voice-class permanent 1
 timeouts call-disconnect 3
 connection trunk 100
!
voice-port 0/1/1
!
!
!
!THIS DIAL-PEER CONNECTS THE VOICE PORT TO MULTICAST GROUP 239.168.1.100. g711 CODEC (64k)
IS USED, AND VAD IS ENABLED
!
dial-peer voice 100 voip
 destination-pattern 100
 session protocol multicast
 session target ipv4:239.168.1.100:19890
 codec g711ulaw
 vad aggressive
!
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login authentication USERLIST
!
end
!
```

Branch 1 Router Configuration (Cisco 2801 Router)

```
Branch-1# show running-config

Building configuration...

Current configuration : 6300 bytes
!
! Last configuration change at 03:11:55 UTC Sat Apr 17 2004
! NVRAM config last updated at 02:03:50 UTC Sat Apr 17 2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
!
```

```
hostname Branch-1
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 informational
enable secret 5 $1$b7.Q$Y2x1UXyRifSStbkR/YyrP.
!
username cisco password 7 0519050B234D5C0617
memory-size iomem 20
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate wic 3
no network-clock-participate wic 4
no network-clock-participate wic 5
no network-clock-participate wic 6
no network-clock-participate wic 7
no network-clock-participate wic 8
no network-clock-participate aim 0
no network-clock-participate aim 1
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
aaa new-model
!
!
aaa authentication login USERLIST local
aaa session-id common
ip subnet-zero
ip cef
!
!
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool LOCAL
   network 192.168.2.0 255.255.255.0
   default-router 192.168.2.1
!
!
no ip domain lookup
ip domain name cisco.com
ip multicast-routing
ip sap cache-timeout 30
ip ssh time-out 30
ip ids po max-events 100
no ftp-server write-enable
voice-card 0
!
!
no virtual-template subinterface
!
!
!
voice class permanent 1
 signal timing oos timeout 65535
 signal keepalive disabled
 signal sequence oos no-action
!
!
!
controller T1 3/0
 framing sf
 linecode ami
```

```
controller T1 3/1
 framing sf
 linecode ami
!
! CLASSIFY DIFFERENT QOS TRAFFIC, SETTING IP PRECEDENCE AND DSCP
!
class-map match-all data
 match ip precedence 2
class-map match-all control-traffic
 match ip dscp af31
class-map match-all video
 match ip precedence 4
class-map match-all voice
 match ip dscp ef
!
! ALLOCATE AVAILABLE BANDWIDTH FOR EACH QOS CLASSIFICATION, DEPENDING ON EXPECTED NEED
! FOR EXAMPLE, DSCP VALUE EF (CLASS VOICE) WILL BE GIVEN 35% OF THE BANDWIDTH
!
policy-map LLQ
 class control-traffic
  bandwidth percent 5
 class voice
  priority percent 35
 class video
  bandwidth percent 15
 class data
  bandwidth percent 20
 class class-default
  fair-queue
!
!
! SET THE IKE POLICY TO USE 3DES
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco address 10.32.152.26 no-xauth
!
!
crypto ipsec transform-set TRANSFORM_1 esp-3des esp-sha-hmac
!
! SPECIFY REMOTE PEER
!
crypto map INT_CM 1 ipsec-isakmp
 description === Peer device = HUB-R1 ===
 set peer 10.32.152.26
 set security-association lifetime kilobytes 530000000
 set security-association lifetime seconds 14400
 set transform-set TRANSFORM_1
 match address IPSEC_ACL_1
!
!
! CREATE TUNNEL TO THE HUB ROUTERS. THE MTU IS LOWERED TO ALLOW THE GRE AND IPSEC HEADER
! PIM SD IS ENABLED SO AS TO ALLOW MULTICAST, AND THE TUNNEL SOURCE AND DESTINATION ARE
SPECIFIED
!
!
interface Tunnel0
 description === Peer device = HUB-R1 ===
 bandwidth 10000
 ip unnumbered FastEthernet0/0
 ip mtu 1420
 ip pim sparse-dense-mode
```

```
 qos pre-classify
 tunnel source 10.32.153.34
 tunnel destination 10.32.152.26
 crypto map INT_CM
!
! VIF INTERFACE FOR MULTICAST SOURCE ADDRESS (USED FOR VOICE MULTICAST)
!
interface Vif1
 ip address 192.168.7.1 255.255.255.0
 ip pim sparse-dense-mode
!
interface FastEthernet0/0
 description === Private interface ===
 ip address 192.168.2.1 255.255.255.0
 ip pim sparse-dense-mode
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
! DSL INTERFACE CONNECTING TO THE PUBLIC NETWORK IN OUR SCENARIO
! ATM PVC 8/35 IS USED IN THIS EXAMPLE.
!
interface ATM2/0
 no ip address
 no atm ilmi-keepalive
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
 pvc 0/35
  encapsulation aal5snap
 !
 pvc 8/35
  vbr-nrt 2000 1000
  encapsulation aal5mux ppp Virtual-Template1
 !
!
interface FastEthernet4/0
 no ip address
!
interface FastEthernet4/1
 no ip address
!
interface FastEthernet4/2
 no ip address
!
interface FastEthernet4/3
 no ip address
!
! LOGICAL INTERFACE FOR DSL LINK. THE PREVIOUSLY DEFINED LLQ QOS POLICY IS USED HERE
! PPP MULTILINK IS ENABLED SO INTERFACE CAN SUPPORT QOS
!
interface Virtual-Template1
 description === Public interface ===
 ip address 10.32.153.34 255.255.255.252
 service-policy output LLQ
 ppp multilink
 ppp multilink fragment delay 8
 ppp multilink interleave
 crypto map INT_CM
```

```
interface Vlan1
 no ip address
!
router ospf 1
 log-adjacency-changes
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.32.153.33
ip route 192.168.1.0 255.255.255.0 Null0 249
!
ip http server
no ip http secure-server
!
! SPECIFY TRAFFIC TO BE ENCRYPTED (HERE IT'S ALL GRE TRAFFIC)
!
ip access-list extended IPSEC_ACL_1
 permit gre host 10.32.153.34 host 10.32.152.26
!
!
!
control-plane
!
!
!
! CONFIGURE THE VOICE PORT AND LINK IT TO DIAL-PEER 100. THIS CONNECTION IS PERMANENT. THE
VOICE-CLASS WAS DEFINED EARLIER IN
! THE CONFIGURATION, AND ESTABLISHES AN 'ALWAYS ON' CONNECTION
!
voice-port 1/0
 voice-class permanent 1
 timeouts call-disconnect 3
 connection trunk 100
!
voice-port 1/1
!
voice-port 1/2
!
voice-port 1/3
!
!
!THIS DIAL-PEER CONNECTS THE VOICE PORT TO MULTICAST GROUP 239.168.1.100. g711 CODEC (64k)
IS USED, AND VAD IS ENABLED
!
dial-peer voice 100 voip
 destination-pattern 100
 session protocol multicast
 session target ipv4:239.168.1.100:19890
 codec g711ulaw
 vad aggressive
!
!
!
line con 0
line aux 0
line vty 0 4
 login authentication USERLIST
!
end
```

Branch 2 Router Configuration (Cisco 2811 Router)

```
Branch-2# show running-config
Building configuration...

Current configuration : 5041 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Branch-2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$9BB/$KP4mHUWzUxzpDEPg5s7ow/
!
username cisco password 7 10481A170C07
memory-size iomem 25
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
aaa new-model
!
!
aaa authentication login USERLIST local
aaa session-id common
ip subnet-zero
ip cef
!
!
ip dhcp excluded-address 192.168.3.1
!
ip dhcp pool LOCAL
   network 192.168.3.0 255.255.255.0
   default-router 192.168.3.1
!
!
no ip domain lookup
ip domain name cisco.com
ip multicast-routing
ip audit notify log
ip audit po max-events 100
!
no ftp-server write-enable
voice-card 0
 no dspfarm
!
!
!
voice class permanent 1
 signal timing oos timeout 65535
 signal keepalive disabled
 signal sequence oos no-action
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
```

```
crypto isakmp key cisco address 10.32.152.26 no-xauth
!
!
crypto ipsec transform-set TRANSFORM_1 esp-3des esp-sha-hmac
!
crypto map INT_CM 1 ipsec-isakmp
 description === Peer device = HUB-R1 ===
 set peer 10.32.152.26
 set security-association lifetime kilobytes 530000000
 set security-association lifetime seconds 14400
 set transform-set TRANSFORM_1
 match address IPSEC_ACL_1
!
!
!
class-map match-all data
 match ip precedence 2
class-map match-all control-traffic
 match ip dscp af31
class-map match-all video
 match ip precedence 4
class-map match-all voice
 match ip dscp ef
!
!
policy-map LLQ
 class control-traffic
  bandwidth percent 5
 class voice
  priority percent 35
 class video
  bandwidth percent 15
 class data
  bandwidth percent 20
 class class-default
  fair-queue
!
!
!
interface Tunnel0
 description === Peer device = HUB-R1 ===
 bandwidth 10000
 ip unnumbered FastEthernet0/0
 ip mtu 1420
 ip pim sparse-dense-mode
 qos pre-classify
 tunnel source Serial0/0/0
 tunnel destination 10.32.152.26
 crypto map INT_CM
!
interface Vif1
 ip address 192.168.5.1 255.255.255.0
 ip pim sparse-dense-mode
!
interface FastEthernet0/0
 description === Private interface ===
 ip address 192.168.3.1 255.255.255.0
 ip pim sparse-dense-mode
 duplex auto
 speed auto
 no keepalive
!
!
!
```

```
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface FastEthernet0/3/0
 no ip address
 shutdown
!
interface FastEthernet0/3/1
 no ip address
 shutdown
!
interface FastEthernet0/3/2
 no ip address
 shutdown
!
interface FastEthernet0/3/3
 no ip address
 shutdown
!
interface Serial0/0/0
 description === Public interface ===
 ip address 10.32.150.46 255.255.255.252
 service-policy output LLQ
 crypto map INT_CM
!
interface Vlan1
 no ip address
!
router ospf 1
 log-adjacency-changes
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.5.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.32.150.45
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip http server
no ip http secure-server
!
ip access-list extended IPSEC_ACL_1
 permit gre host 10.32.150.46 host 10.32.152.26
!
!
!
control-plane
!
!
voice-port 0/1/0
 voice-class permanent 1
 timeouts call-disconnect 3
 connection trunk 100
!
voice-port 0/1/1
!
!
!
dial-peer cor custom
!
!
```

```
dial-peer voice 100 voip
 destination-pattern 100
 session protocol multicast
 session target ipv4:239.168.1.100:19890
 codec g711ulaw
 vad aggressive
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password 7 0002000E0D4B
 login authentication USERLIST
!
!
end
```

Verify

This section provides information you can use to confirm your configuration is working properly. The verification process includes two parts:

- Verify Headquarters Connectivity, page 17
- Verify Remote Location Connectivity, page 27

Verify Headquarters Connectivity

This section provides instructions for verifying that your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of **show** command output.

In summary:

- **show crypto isakmp sa**—Shows whether the remote routers have successfully connected.
- **show crypto ipsec sa**—Shows information about each IPSec SA.
- **show ip ospf neighbor**—Shows whether the router has Open Shortest Path First (OSPF) neighbors.
- **show ip route**—Shows whether the remote networks and multicast subnets are accessible (assess routing table).
- **show ip pim neighbor**—After a routing table is verified, shows whether a valid Protocol Independent Multicast (PIM) neighbor exists.
- **show ip pim rp map**—Shows whether the rendezvous point (RP) (in this instance, the router) is being correctly learned.
- **show ip mroute active**—Shows whether any active multicast streams exist (in this case, voice streams).
- **show voice trunk-conditioning supervisory**—Shows whether the voice port connection is up.
- **show voip rtp connections**—Presents sources and destination of a RTP voice stream.

- **show voice call summary**—Shows information about a call (such as the codec being used or the state of the phone).
- **show class-map**—Displays the QoS marking scheme (such as voice traffic that is marked up). This defines it as a V^3PN implementation.
- **show policy-map interface atm 1/0 output**—Shows how traffic has been queued on the ATM interface. Note that different queues have different packet counts because traffic is assigned on the basis of differentiated services code point (DCSP) and IP precedence values.
- **show crypto engine brief**—Shows the VPN engine currently being run.

Representative output from each of these commands is presented in the verification summaries that follow.

Note Relevant display output is highlighted in **bold** text as appropriate.

The following is an output example for the **show crypto isakmp sa** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show crypto isakmp sa

dst             src             state          conn-id slot
10.32.152.26    10.32.153.34    QM_IDLE             29    0
10.32.152.26    10.32.150.46    QM_IDLE             31    0
```

The following is an output example for the **show crypto ipsec sa** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: INT_CM, local addr. 10.32.152.26

   protected vrf:
   local  ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.32.153.34/255.255.255.255/47/0)
   current_peer: 10.32.153.34:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 174918, #pkts encrypt: 174918, #pkts digest: 174918
    #pkts decaps: 126855, #pkts decrypt: 126855, #pkts verify: 126855
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 66, #recv errors 0

     local crypto endpt.: 10.32.152.26, remote crypto endpt.: 10.32.153.34
     path mtu 1420, media mtu 1420
     current outbound spi: 69111392

     inbound esp sas:
      spi: 0xD5823DEF(3582082543)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5213, flow_id: 93, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508969241/10148)
        ike_cookies: DE2C7D5A FB6197B3 795753FB 41D07F6D
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
```

```
inbound pcp sas:

     outbound esp sas:
      spi: 0x69111392(1762726802)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5214, flow_id: 94, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508968340/10147)
        ike_cookies: DE2C7D5A FB6197B3 795753FB 41D07F6D
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

   protected vrf:
   local  ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.32.150.46/255.255.255.255/47/0)
   current_peer: 10.32.150.46:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 168329, #pkts encrypt: 168329, #pkts digest: 168329
    #pkts decaps: 127676, #pkts decrypt: 127676, #pkts verify: 127676
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 5, #recv errors 0

     local crypto endpt.: 10.32.152.26, remote crypto endpt.: 10.32.150.46
     path mtu 1420, media mtu 1420
     current outbound spi: D3C362F0

     inbound esp sas:
      spi: 0x4589EBE8(1166666728)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5219, flow_id: 99, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (528510577/14207)
        ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
        IV size: 8 bytes
        replay detection support: Y
      spi: 0xC172073D(3245475645)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5221, flow_id: 101, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (522107198/14206)
        ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x2A87D473(713544819)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5220, flow_id: 100, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (528510577/14205)
```

```
        ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
        IV size: 8 bytes
        replay detection support: Y
      spi: 0xD3C362F0(3552797424)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5222, flow_id: 102, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (522107166/14204)
        ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
        IV size: 8 bytes
        replay detection support: Y

    outbound ah sas:

    outbound pcp sas:

interface: Tunnel1
    Crypto map tag: INT_CM, local addr. 10.32.152.26

   protected vrf:
   local  ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.32.153.34/255.255.255.255/47/0)
   current_peer: 10.32.153.34:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 171877, #pkts encrypt: 171877, #pkts digest: 171877
    #pkts decaps: 123829, #pkts decrypt: 123829, #pkts verify: 123829
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 66, #recv errors 0

     local crypto endpt.: 10.32.152.26, remote crypto endpt.: 10.32.153.34
     path mtu 1420, media mtu 1420
     current outbound spi: 69111392

     inbound esp sas:
      spi: 0xD5823DEF(3582082543)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5213, flow_id: 93, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508970067/10208)
        ike_cookies: DE2C7D5A FB6197B3 795753FB 41D07F6D
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x69111392(1762726802)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5214, flow_id: 94, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508969170/10207)
        ike_cookies: DE2C7D5A FB6197B3 795753FB 41D07F6D
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
```

```
  outbound pcp sas:

protected vrf:
local  ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.32.150.46/255.255.255.255/47/0)
current_peer: 10.32.150.46:500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 165228, #pkts encrypt: 165228, #pkts digest: 165228
 #pkts decaps: 124592, #pkts decrypt: 124592, #pkts verify: 124592
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 5, #recv errors 0

  local crypto endpt.: 10.32.152.26, remote crypto endpt.: 10.32.150.46
  path mtu 1420, media mtu 1420
  current outbound spi: D3C362F0

  inbound esp sas:
   spi: 0x4589EBE8(1166666728)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 5219, flow_id: 99, crypto map: INT_CM
     crypto engine type: Hardware, engine_id: 2
     sa timing: remaining key lifetime (k/sec): (528510577/14267)
     ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
     IV size: 8 bytes
     replay detection support: Y
   spi: 0xC172073D(3245475645)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 5221, flow_id: 101, crypto map: INT_CM
     crypto engine type: Hardware, engine_id: 2
     sa timing: remaining key lifetime (k/sec): (522108046/14267)
     ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
     IV size: 8 bytes
     replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x2A87D473(713544819)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 5220, flow_id: 100, crypto map: INT_CM
     crypto engine type: Hardware, engine_id: 2
     sa timing: remaining key lifetime (k/sec): (528510577/14266)
     ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
     IV size: 8 bytes
     replay detection support: Y
   spi: 0xD3C362F0(3552797424)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 5222, flow_id: 102, crypto map: INT_CM
     crypto engine type: Hardware, engine_id: 2
     sa timing: remaining key lifetime (k/sec): (522108025/14266)
     ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
     IV size: 8 bytes
     replay detection support: Y

  outbound ah sas:
```

```
     outbound pcp sas:


interface: ATM1/0
    Crypto map tag: INT_CM, local addr. 10.32.152.26

   protected vrf:
   local  ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.32.153.34/255.255.255.255/47/0)
   current_peer: 10.32.153.34:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 172131, #pkts encrypt: 172131, #pkts digest: 172131
    #pkts decaps: 124081, #pkts decrypt: 124081, #pkts verify: 124081
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 66, #recv errors 0

     local crypto endpt.: 10.32.152.26, remote crypto endpt.: 10.32.153.34
     path mtu 1420, media mtu 1420
     current outbound spi: 69111392

     inbound esp sas:
      spi: 0xD5823DEF(3582082543)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5213, flow_id: 93, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508969984/10202)
        ike_cookies: DE2C7D5A FB6197B3 795753FB 41D07F6D
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x69111392(1762726802)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5214, flow_id: 94, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508969108/10202)
        ike_cookies: DE2C7D5A FB6197B3 795753FB 41D07F6D
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

   protected vrf:
   local  ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.32.150.46/255.255.255.255/47/0)
   current_peer: 10.32.150.46:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 165491, #pkts encrypt: 165491, #pkts digest: 165491
    #pkts decaps: 124855, #pkts decrypt: 124855, #pkts verify: 124855
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 5, #recv errors 0
```

```
local crypto endpt.: 10.32.152.26, remote crypto endpt.: 10.32.150.46
path mtu 1420, media mtu 1420
current outbound spi: D3C362F0

inbound esp sas:
 spi: 0x4589EBE8(1166666728)
   transform: esp-3des esp-sha-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 5219, flow_id: 99, crypto map: INT_CM
   crypto engine type: Hardware, engine_id: 2
   sa timing: remaining key lifetime (k/sec): (528510577/14263)
   ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
   IV size: 8 bytes
   replay detection support: Y
 spi: 0xC172073D(3245475645)
   transform: esp-3des esp-sha-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 5221, flow_id: 101, crypto map: INT_CM
   crypto engine type: Hardware, engine_id: 2
   sa timing: remaining key lifetime (k/sec): (522107974/14262)
   ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
   IV size: 8 bytes
   replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x2A87D473(713544819)
   transform: esp-3des esp-sha-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 5220, flow_id: 100, crypto map: INT_CM
   crypto engine type: Hardware, engine_id: 2
   sa timing: remaining key lifetime (k/sec): (528510577/14262)
   ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
   IV size: 8 bytes
   replay detection support: Y
 spi: 0xD3C362F0(3552797424)
   transform: esp-3des esp-sha-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 5222, flow_id: 102, crypto map: INT_CM
   crypto engine type: Hardware, engine_id: 2
   sa timing: remaining key lifetime (k/sec): (522107953/14261)
   ike_cookies: 59F8CBF0 5B2E8553 7D356DD4 F5DE05AD
   IV size: 8 bytes
   replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

The following is an output example for the **show ip ospf neighbors** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.7.1       0   FULL/  -        00:00:39    192.168.2.1     Tunnel1
192.168.5.1       0   FULL/  -        00:00:36    192.168.3.1     Tunnel0
```

The following is an output example for the **show ip route** command, performed using the configuration on the Headquarters router:

```
HUB-R1# 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 10.32.152.25 to network 0.0.0.0

     192.168.4.0/32 is subnetted, 1 subnets
C       192.168.4.1 is directly connected, Loopback100
O    192.168.5.0/24 [110/11] via 192.168.3.1, 00:12:48, Tunnel0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.32.152.24/30 is directly connected, ATM1/0
C    192.168.6.0/24 is directly connected, Vif1
O    192.168.7.0/24 [110/11] via 192.168.2.1, 00:12:48, Tunnel1
C    192.168.1.0/24 is directly connected, Vlan10
O    192.168.2.0/24 [110/11] via 192.168.2.1, 00:12:50, Tunnel1
O    192.168.3.0/24 [110/11] via 192.168.3.1, 00:12:50, Tunnel0
S*   0.0.0.0/0 [1/0] via 10.32.152.25
```

The following is an output example for the **show ip pim neighbors** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show ip pim neighbor

PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
192.168.3.1       Tunnel0                  00:13:52/00:01:40 v2    1 / S
192.168.2.1       Tunnel1                  00:13:44/00:01:18 v2    1 / S
```

The following is an output example for the **show ip pim rp map** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show ip pim rp map

PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent (Loopback100)

Group(s) 224.0.0.0/4
  RP 192.168.4.1 (?), v2v1
    Info source: 192.168.4.1 (?), elected via Auto-RP
         Uptime: 2d02h, expires: 00:02:25
```

The following is an output example for the **show ip mroute active** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 239.168.1.100, (?)
   Source: 192.168.5.2 (?)
     Rate: 0 pps/0 kbps(1sec), 0 kbps(last 0 secs), 2 kbps(life avg)
   Source: 192.168.7.2 (?)
     Rate: 0 pps/0 kbps(1sec), 80 kbps(last 40 secs), 2 kbps(life avg)
```

The following is an output example for the **show voice trunk-conditioning supervisory** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show voice trunk-conditioning supervisory

SLOW SCAN
0/1/0 : state : TRUNK_SC_CONNECT, voice : on, signal : on ,master
        status: trunk connected
        sequence oos : no-action
        pattern :
        timing : idle = 0, restart = 0, standby = 0, timeout = 65535
        supp_all = 0, supp_voice = 0, keep_alive = 0
        timer: oos_ais_timer = 0, timer = 0
```

The following is an output example for the **show voip rtp connections** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   16      15         20380    19890  192.168.6.2     239.168.1.100
Found 1 active RTP connections
```

The following is an output example for the **show voice call summary** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show voice call summary

PORT           CODEC    VAD VTSP STATE            VPM STATE
============== ======== === ==================== ======================
0/1/0          g711ulaw  y  S_CONNECT            S_TRUNKED
0/1/1          -         -  -                    FXSLS_ONHOOK
```

The following is an output example for the **show class-map** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show class-map

 Class Map match-all control-traffic (id 1)
   Match ip  dscp af31

 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all video (id 3)
   Match ip  precedence 4

 Class Map match-all voice (id 2)
   Match ip  dscp ef
```

The following is an output example for the **show policy-map interface atm 1/0 output** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show policy-map interface atm 1/0 output

 ATM1/0: VC 10/100 -

  Service-policy output: LLQ

    Class-map: control-traffic (match-all)
      180010 packets, 43922248 bytes
      5 minute offered rate 1000 bps, drop rate 0 bps
```

```
    Match: ip dscp af31
    Queueing
      Output Queue: Conversation 265
      Bandwidth 5 (%)
      Bandwidth 5000 (kbps) Max Threshold 64 (packets)
      (pkts matched/bytes matched) 89887/21932300
      (depth/total drops/no-buffer drops) 0/0/0

  Class-map: voice (match-all)
    6485132 packets, 1893649352 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip dscp ef
    Queueing
      Strict Priority
      Output Queue: Conversation 264
      Bandwidth 35 (%)
      Bandwidth 35000 (kbps) Burst 875000 (Bytes)
      (pkts matched/bytes matched) 147/42924
      (total drops/bytes drops) 48/14016

  Class-map: video (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 4
    Queueing
      Output Queue: Conversation 266
      Bandwidth 15 (%)
      Bandwidth 15000 (kbps) Max Threshold 64 (packets)
      (pkts matched/bytes matched) 0/0
      (depth/total drops/no-buffer drops) 0/0/0

  Class-map: data (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 2
    Queueing
      Output Queue: Conversation 267
      Bandwidth 20 (%)
      Bandwidth 20000 (kbps) Max Threshold 64 (packets)
      (pkts matched/bytes matched) 0/0
      (depth/total drops/no-buffer drops) 0/0/0

  Class-map: class-default (match-any)
    97836 packets, 15410572 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
    Queueing
      Flow Based Fair Queueing
      Maximum Number of Hashed Queues 256
      (total queued/total drops/no-buffer drops) 0/0/0
```

The following is an output example for the **show crypto engine brief** command, performed using the configuration on the Headquarters router:

```
HUB-R1# show crypto engine brief

      crypto engine name:  Virtual Private Network (VPN) Module
      crypto engine type:  hardware
                   State:  Enabled
            Product Name:  Onboard-VPN
              FW Version:  01100200
            Time running:  479742 seconds
             Compression:  Yes
                     DES:  Yes
```

```
                3 DES:  Yes
              AES CBC:  Yes (128,192,256)
             AES CNTR:  No
Maximum buffer length:  4096
     Maximum DH index:  0500
     Maximum SA index:  0500
   Maximum Flow index:  1000
Maximum RSA key size:  2048


  crypto engine name:  Cisco VPN Software Implementation
   crypto engine type:  software
        serial number:  77C943AD
  crypto engine state:  installed
crypto engine in slot:  N/A
```

Verify Remote Location Connectivity

This section provides instructions for verifying that your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of **show** command output.

In general, the **show** commands that are used to verify remote location connectivity are the same as the commands used for the Headquarters router. See the "Verify Headquarters Connectivity" section on page 17 for summaries of the **show** commands that are common to both Headquarters and branch verification. The following commands are used for the remote locations only:

- **show policy-map interface virtual-access 4 output**—Shows how traffic has been queued on the DSL interface (Branch 1). Note that different queues have different packet counts because traffic is assigned on the basis of DCSP and IP precedence values.
- **show policy-map interface serial 0/0/0 output**—Shows how traffic has been queued on the serial interface (Branch 2). Note that different queues have different packet counts because traffic is assigned on the basis of DCSP and IP precedence values.

Representative output for each of these commands is presented in the verification summaries that follow.

Note Relevant display output is highlighted in **bold** text.

Example output is split into two sections:

- Verifying Branch 1 Router, page 27
- Verifying Branch 2 Router, page 34

Verifying Branch 1 Router

The following is an output example for the **show crypto isakmp sa** command, performed using the configuration on the Branch 1 router (DSL):

```
Branch-1# show crypto isakmp sa

dst             src             state          conn-id slot
10.32.152.26    10.32.153.34    QM_IDLE              4    0
```

The following is an output example for the **show crypto ipsec sa** command, performed using the configuration on the Branch 1 router:

```
Branch-1# show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: INT_CM, local addr. 10.32.153.34

   protected vrf:
   local  ident (addr/mask/prot/port): (10.32.153.34/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
   current_peer: 10.32.152.26:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 78341, #pkts encrypt: 78341, #pkts digest: 78341
    #pkts decaps: 118387, #pkts decrypt: 118387, #pkts verify: 118387
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 11, #recv errors 0

     local crypto endpt.: 10.32.153.34, remote crypto endpt.: 10.32.152.26
     path mtu 1420, media mtu 1420
     current outbound spi: D5823DEF

     inbound esp sas:
      spi: 0x69111392(1762726802)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5151, flow_id: 31, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508937407/10703)
        ike_cookies: 795753FB 41D07F6D DE2C7D5A FB6197B3
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xD5823DEF(3582082543)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5152, flow_id: 32, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508938275/10702)
        ike_cookies: 795753FB 41D07F6D DE2C7D5A FB6197B3
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:


interface: Virtual-Template1
    Crypto map tag: INT_CM, local addr. 10.32.153.34

   protected vrf:
   local  ident (addr/mask/prot/port): (10.32.153.34/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
   current_peer: 10.32.152.26:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 78380, #pkts encrypt: 78380, #pkts digest: 78380
```

```
     #pkts decaps: 118426, #pkts decrypt: 118426, #pkts verify: 118426
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 11, #recv errors 0

      local crypto endpt.: 10.32.153.34, remote crypto endpt.: 10.32.152.26
      path mtu 1420, media mtu 1420
      current outbound spi: D5823DEF

      inbound esp sas:
       spi: 0x69111392(1762726802)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 5151, flow_id: 31, crypto map: INT_CM
         crypto engine type: Hardware, engine_id: 2
         sa timing: remaining key lifetime (k/sec): (508937393/10702)
         ike_cookies: 795753FB 41D07F6D DE2C7D5A FB6197B3
         IV size: 8 bytes
         replay detection support: Y

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xD5823DEF(3582082543)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 5152, flow_id: 32, crypto map: INT_CM
         crypto engine type: Hardware, engine_id: 2
         sa timing: remaining key lifetime (k/sec): (508938237/10700)
         ike_cookies: 795753FB 41D07F6D DE2C7D5A FB6197B3
         IV size: 8 bytes
         replay detection support: Y

      outbound ah sas:

      outbound pcp sas:


interface: Virtual-Access3
    Crypto map tag: INT_CM, local addr. 10.32.153.34

   protected vrf:
   local  ident (addr/mask/prot/port): (10.32.153.34/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
   current_peer: 10.32.152.26:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 78508, #pkts encrypt: 78508, #pkts digest: 78508
    #pkts decaps: 118555, #pkts decrypt: 118555, #pkts verify: 118555
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 11, #recv errors 0

     local crypto endpt.: 10.32.153.34, remote crypto endpt.: 10.32.152.26
     path mtu 1420, media mtu 1420
     current outbound spi: D5823DEF

     inbound esp sas:
      spi: 0x69111392(1762726802)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
```

```
        slot: 0, conn id: 5151, flow_id: 31, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508937361/10700)
        ike_cookies: 795753FB 41D07F6D DE2C7D5A FB6197B3
        IV size: 8 bytes
        replay detection support: Y

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xD5823DEF(3582082543)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5152, flow_id: 32, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508938204/10697)
        ike_cookies: 795753FB 41D07F6D DE2C7D5A FB6197B3
        IV size: 8 bytes
        replay detection support: Y

      outbound ah sas:

      outbound pcp sas:


interface: Virtual-Access4
    Crypto map tag: INT_CM, local addr. 10.32.153.34

   protected vrf:
   local  ident (addr/mask/prot/port): (10.32.153.34/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
   current_peer: 10.32.152.26:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 78628, #pkts encrypt: 78628, #pkts digest: 78628
    #pkts decaps: 118675, #pkts decrypt: 118675, #pkts verify: 118675
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 11, #recv errors 0

     local crypto endpt.: 10.32.153.34, remote crypto endpt.: 10.32.152.26
     path mtu 1420, media mtu 1420
     current outbound spi: D5823DEF

     inbound esp sas:
      spi: 0x69111392(1762726802)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5151, flow_id: 31, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508937328/10697)
        ike_cookies: 795753FB 41D07F6D DE2C7D5A FB6197B3
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xD5823DEF(3582082543)
        transform: esp-3des esp-sha-hmac ,
```

```
        in use settings ={Tunnel, }
        slot: 0, conn id: 5152, flow_id: 32, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508938172/10695)
        ike_cookies: 795753FB 41D07F6D DE2C7D5A FB6197B3
        IV size: 8 bytes
        replay detection support: Y

    outbound ah sas:

    outbound pcp sas:
```

The following is an output example for the **show ip ospf neighbor** command, performed using the configuration on the Branch 1 router:

```
Branch-1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1       0   FULL/  -        00:00:35    192.168.1.1     Tunnel0
```

The following is an output example from the **show ip route** command, performed using the configuration on the Branch 1 router:

```
Branch-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 10.32.153.33 to network 0.0.0.0

     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/11] via 192.168.1.1, 00:33:28, Tunnel0
O    192.168.5.0/24 [110/21] via 192.168.1.1, 00:33:28, Tunnel0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.32.153.33/32 is directly connected, Virtual-Access4
C       10.32.153.32/30 is directly connected, Virtual-Access3
                        is directly connected, Virtual-Access4
O    192.168.6.0/24 [110/11] via 192.168.1.1, 00:33:28, Tunnel0
C    192.168.7.0/24 is directly connected, Vif1
O    192.168.1.0/24 [110/11] via 192.168.1.1, 00:33:28, Tunnel0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
O    192.168.3.0/24 [110/21] via 192.168.1.1, 00:33:28, Tunnel0
S*   0.0.0.0/0 [1/0] via 10.32.153.33
```

The following is an output example for the **show ip pim neighbor** command, performed using the configuration on the Branch 1 router:

```
Branch-1# show ip pim neighbor

PIM Neighbor Table
Neighbor          Interface               Uptime/Expires    Ver   DR
Address                                                           Prio/Mode
192.168.1.1       Tunnel0                 00:20:59/00:01:25 v2    1 / S
```

The following is an output example for the **show ip pim rp mapping** command, performed using the configuration on the Branch 1 router:

```
Branch-1# show ip pim rp mapping
```

```
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 192.168.4.1 (?), v2v1
    Info source: 192.168.4.1 (?), elected via Auto-RP
         Uptime: 00:20:28, expires: 00:02:23
```

The following is an output example for the **show ip mroute active** command, performed using the configuration on the Branch 1 router:

```
Branch-1# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 239.168.1.100, (?)
   Source: 192.168.5.2 (?)
     Rate: 0 pps/0 kbps(1sec), 80 kbps(last 10 secs), 7 kbps(life avg)
   Source: 192.168.7.2 (?)
     Rate: 0 pps/0 kbps(1sec), 80 kbps(last 10 secs), 7 kbps(life avg)
```

The following is an output example for the **show voice trunk-conditioning supervisory** command, performed using the configuration on the Branch 1 router:

```
Branch-1# show voice trunk-conditioning supervisory

SLOW SCAN
1/0 : state : TRUNK_SC_CONNECT, voice : on, signal : on ,master
        status: trunk connected
        sequence oos : no-action
        pattern :
        timing : idle = 0, restart = 0, standby = 0, timeout = 65535
        supp_all = 0, supp_voice = 0, keep_alive = 0
        timer: oos_ais_timer = 0, timer = 0
```

The following is an output example for the **show voip rtp connections** command, performed using the configuration on the Branch 1 router:

```
Branch-1# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   4       3          31156    19890  192.168.7.2     239.168.1.100
Found 1 active RTP connections
```

The following is an output example for the **show voice call summary** command, performed using the configuration on the Branch 1 router:

```
Branch-1# show voice call summary

PORT            CODEC    VAD VTSP STATE              VPM STATE
=============== ======== === ===================== ======================
1/0             g711ulaw  y  S_CONNECT              S_TRUNKED
1/1             -         -  -                      FXSLS_ONHOOK
1/2             -         -  -                      FXSLS_ONHOOK
1/3             -         -  -                      FXSLS_ONHOOK
```

The following is an output example for the **show class map** command, performed using the configuration on the Branch 1 router:

```
Branch-1# show class-map

 Class Map match-all control-traffic (id 1)
   Match ip  dscp af31
```

```
 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all video (id 3)
   Match ip  precedence 4

 Class Map match-all voice (id 2)
   Match ip  dscp ef
```

The following is an output example for the **show policy-map interface virtual-access 4 output** command, performed using the configuration on the Branch 1 router:

```
Branch-1 #show policy-map interface virtual-access 4 output

 Virtual-Access4

  Service-policy output: LLQ

    Class-map: control-traffic (match-all)
      45166 packets, 10659176 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af31
      Queueing
        Output Queue: Conversation 265
        Bandwidth 5 (%)
        Bandwidth 50 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: voice (match-all)
      3241999 packets, 920726516 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp ef
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 35 (%)
        Bandwidth 350 (kbps) Burst 8750 (Bytes)
        (pkts matched/bytes matched) 3217794/913852296
        (total drops/bytes drops) 0/0

    Class-map: video (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 4
      Queueing
        Output Queue: Conversation 267
        Bandwidth 15 (%)
        Bandwidth 150 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: data (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 2
      Queueing
        Output Queue: Conversation 266
        Bandwidth 20 (%)
        Bandwidth 200 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
```

```
    41789 packets, 6646861 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
    Queueing
      Flow Based Fair Queueing
      Maximum Number of Hashed Queues 256
      (total queued/total drops/no-buffer drops) 0/0/0
```

The following is an output example for the **show crypto engine brief** command, performed using the configuration on the Branch 1 router:

```
Branch-1# show crypto engine brief

        crypto engine name:  Virtual Private Network (VPN) Module
        crypto engine type:  hardware
                     State:  Enabled
        VPN Module in slot:  0
              Product Name:  AIM-VPN/BPII
         Software Serial #:  55AA
                 Device ID:  0014 - revision 0002
                 Vendor ID:  13A3
              Revision No:  0x00140002
             VSK revision:  0
             Boot version:  255
              DPU version:  0
              HSP version:  2.2(21) (ALPHA)
             Time running:  0 Seconds
              Compression:  Yes
                      DES:  Yes
                   3 DES:  Yes
                  AES CBC:  Yes (128,192,256)
                 AES CNTR:  No
    Maximum buffer length:  4096
         Maximum DH index:  1000
         Maximum SA index:  1000
       Maximum Flow index:  2000
     Maximum RSA key size:  2048


        crypto engine name:  Cisco VPN Software Implementation
        crypto engine type:  software
             serial number:  70107010
      crypto engine state:  installed
    crypto engine in slot:  N/A
```

Verifying Branch 2 Router

The following is an output example for the **show crypto isakmp sa** command, performed using the configuration on the Branch 2 router (serial):

```
Branch-2# show crypto isakmp sa

dst             src             state          conn-id slot
10.32.152.26    10.32.150.46    QM_IDLE              3    0
```

The following is an output example for the **show crypto ipsec sa** command, performed using the configuration on the Branch 2 router:

```
Branch-2# show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: INT_CM, local addr. 10.32.150.46
```

```
   protected vrf:
   local  ident (addr/mask/prot/port): (10.32.150.46/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
   current_peer: 10.32.152.26:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1706, #pkts encrypt: 1706, #pkts digest: 1706
    #pkts decaps: 1715, #pkts decrypt: 1715, #pkts verify: 1715
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 10, #recv errors 0

     local crypto endpt.: 10.32.150.46, remote crypto endpt.: 10.32.152.26
     path mtu 1420, media mtu 1420
     current outbound spi: C172073D

     inbound esp sas:
      spi: 0x2A87D473(713544819)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5151, flow_id: 31, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508372675/14364)
        ike_cookies: 7D356DD4 F5DE05AD 59F8CBF0 5B2E8553
        IV size: 8 bytes
        replay detection support: Y
      spi: 0xD3C362F0(3552797424)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5153, flow_id: 33, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (521045477/14364)
        ike_cookies: 7D356DD4 F5DE05AD 59F8CBF0 5B2E8553
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x4589EBE8(1166666728)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5152, flow_id: 32, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (508372675/14364)
        ike_cookies: 7D356DD4 F5DE05AD 59F8CBF0 5B2E8553
        IV size: 8 bytes
        replay detection support: Y
      spi: 0xC172073D(3245475645)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5154, flow_id: 34, crypto map: INT_CM
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (521045458/14363)
        ike_cookies: 7D356DD4 F5DE05AD 59F8CBF0 5B2E8553
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
interface: Serial0/0/0
```

```
     Crypto map tag: INT_CM, local addr. 10.32.150.46

    protected vrf:
    local  ident (addr/mask/prot/port): (10.32.150.46/255.255.255.255/47/0)
    remote ident (addr/mask/prot/port): (10.32.152.26/255.255.255.255/47/0)
    current_peer: 10.32.152.26:500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 1864, #pkts encrypt: 1864, #pkts digest: 1864
     #pkts decaps: 1874, #pkts decrypt: 1874, #pkts verify: 1874
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 10, #recv errors 0

      local crypto endpt.: 10.32.150.46, remote crypto endpt.: 10.32.152.26
      path mtu 1420, media mtu 1420
      current outbound spi: C172073D

      inbound esp sas:
       spi: 0x2A87D473(713544819)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 5151, flow_id: 31, crypto map: INT_CM
         crypto engine type: Hardware, engine_id: 2
         sa timing: remaining key lifetime (k/sec): (508372675/14361)
         ike_cookies: 7D356DD4 F5DE05AD 59F8CBF0 5B2E8553
         IV size: 8 bytes
         replay detection support: Y
       spi: 0xD3C362F0(3552797424)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 5153, flow_id: 33, crypto map: INT_CM
         crypto engine type: Hardware, engine_id: 2
Branch-2#         sa timing: remaining key lifetime (k/sec): (521045425/14360)
         ike_cookies: 7D356DD4 F5DE05AD 59F8CBF0 5B2E8553
         IV size: 8 bytes
         replay detection support: Y

      inbound ah sas:
      inbound pcp sas:

      outbound esp sas:
       spi: 0x4589EBE8(1166666728)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 5152, flow_id: 32, crypto map: INT_CM
         crypto engine type: Hardware, engine_id: 2
         sa timing: remaining key lifetime (k/sec): (508372675/14360)
         ike_cookies: 7D356DD4 F5DE05AD 59F8CBF0 5B2E8553
         IV size: 8 bytes
         replay detection support: Y
       spi: 0xC172073D(3245475645)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 5154, flow_id: 34, crypto map: INT_CM
         crypto engine type: Hardware, engine_id: 2
         sa timing: remaining key lifetime (k/sec): (521045411/14359)
         ike_cookies: 7D356DD4 F5DE05AD 59F8CBF0 5B2E8553
         IV size: 8 bytes
         replay detection support: Y

      outbound ah sas:
      outbound pcp sas:
```

The following is an output example for the **show ip ospf neighbor** command, performed using the configuration on the Branch 2 router:

```
Branch-2# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1       0   FULL/  -        00:00:37    192.168.1.1     Tunnel0
```

The following is an output example for the **show ip route** command, performed using the configuration on the Branch 2 router:

```
Branch-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 10.32.150.45 to network 0.0.0.0

     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/11] via 192.168.1.1, 00:31:10, Tunnel0
C    192.168.5.0/24 is directly connected, Vif1
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.32.150.44/30 is directly connected, Serial0/0/0
O    192.168.6.0/24 [110/11] via 192.168.1.1, 00:31:10, Tunnel0
O    192.168.7.0/24 [110/21] via 192.168.1.1, 00:31:10, Tunnel0
O    192.168.1.0/24 [110/11] via 192.168.1.1, 00:31:11, Tunnel0
O    192.168.2.0/24 [110/21] via 192.168.1.1, 00:31:11, Tunnel0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.32.150.45
                is directly connected, Serial0/0/0
```

The following is an output example for the **show ip pim neighbor** command, performed using the configuration on the Branch 2 router:

```
Branch-2# show ip pim neighbor

PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
192.168.1.1       Tunnel0                  00:31:52/00:01:26 v2    1 / S
```

The following is an output example for the **show ip pim rp mapping** command, performed using the configuration on the Branch 2 router:

```
Branch-2# show ip pim rp mapping

PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 192.168.4.1 (?), v2v1
    Info source: 192.168.4.1 (?), elected via Auto-RP
         Uptime: 2d03h, expires: 00:02:47
```

The following is an output example for the **show ip mroute active** command, performed using the configuration on the Branch 2 router:

```
Branch-2# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps
```

```
Group: 239.168.1.100, (?)
   Source: 192.168.5.2 (?)
     Rate: 50 pps/80 kbps(1sec), 80 kbps(last 10 secs), 2 kbps(life avg)
   Source: 192.168.7.2 (?)
     Rate: 50 pps/80 kbps(1sec), 80 kbps(last 30 secs), 2 kbps(life avg)
```

The following is an output example for the **show voice trunk-conditioning supervisory** command, performed using the configuration on the Branch 2 router:

```
Branch-2# show voice trunk-conditioning supervisory

SLOW SCAN
0/1/0 : state : TRUNK_SC_CONNECT, voice : on, signal : on ,master
        status: trunk connected
        sequence oos : no-action
        pattern :
        timing : idle = 0, restart = 0, standby = 0, timeout = 65535
        supp_all = 0, supp_voice = 0, keep_alive = 0
        timer: oos_ais_timer = 0, timer = 0
```

The following is an output example for the **show voip rtp connections** command, performed using the configuration on the Branch 2 router:

```
Branch-2# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   9       8          18618    19890  192.168.5.2     239.168.1.100
Found 1 active RTP connections
```

The following is an output example for the **show voice call summary** command, performed using the configuration on the Branch 2 router:

```
Branch-2# show voice call summary

PORT            CODEC    VAD VTSP STATE             VPM STATE
=============== ======== === ==================== ======================
0/1/0          g711ulaw  y  S_CONNECT             S_TRUNKED
0/1/1          -         -  -                     FXSLS_ONHOOK
```

The following is an output example for the **show policy-map interface serial 0/0/0 output** command, performed using the configuration on the Branch 2 router:

```
Branch-2# show policy-map interface serial 0/0/0 output

 Serial0/0/0

  Service-policy output: LLQ

    Class-map: control-traffic (match-all)
      50099 packets, 11823300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af31
      Queueing
        Output Queue: Conversation 265
        Bandwidth 5 (%)
        Bandwidth 77 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 863/203668
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: voice (match-all)
      3241968 packets, 920715872 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
```

```
    Match: ip dscp ef
    Queueing
      Strict Priority
      Output Queue: Conversation 264
      Bandwidth 35 (%)
      Bandwidth 540 (kbps) Burst 13500 (Bytes)
      (pkts matched/bytes matched) 13/3532
      (total drops/bytes drops) 0/0

  Class-map: video (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 4
    Queueing
      Output Queue: Conversation 266
      Bandwidth 15 (%)
      Bandwidth 231 (kbps) Max Threshold 64 (packets)
      (pkts matched/bytes matched) 0/0
      (depth/total drops/no-buffer drops) 0/0/0

  Class-map: data (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 2
    Queueing
      Output Queue: Conversation 267
      Bandwidth 20 (%)
      Bandwidth 308 (kbps) Max Threshold 64 (packets)
      (pkts matched/bytes matched) 0/0
      (depth/total drops/no-buffer drops) 0/0/0

  Class-map: class-default (match-any)
    75804 packets, 9111740 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
    Queueing
      Flow Based Fair Queueing
      Maximum Number of Hashed Queues 256
      (total queued/total drops/no-buffer drops) 0/0/0
```

The following is an output example for the **show crypto engine brief** command, performed using the configuration on the Branch 2 router:

```
Branch-2# show crypto engine brief

        crypto engine name:  Virtual Private Network (VPN) Module
        crypto engine type:  hardware
                     State:  Enabled
              Product Name:  Onboard-VPN
  NetGX Middleware Version:  v1.2.0
    NetGX Firmware Version:  v2.2.0
              Time running:  414404 seconds
               Compression:  Yes
                       DES:  Yes
                     3 DES:  Yes
                   AES CBC:  Yes (128,192,256)
                  AES CNTR:  No
     Maximum buffer length:  4096
          Maximum DH index:  0300
          Maximum SA index:  0300
        Maximum Flow index:  2400
      Maximum RSA key size:  2048
```

```
      crypto engine name:  Cisco VPN Software Implementation
      crypto engine type:  software
           serial number:  FFFFFFFF
     crypto engine state:  installed
  crypto engine in slot:  N/A
```

Troubleshoot

This section provides information you can use to confirm that your configuration is working properly.

See the following tech notes:

- *IP Security Troubleshooting - Understanding and Using debug Commands*

Troubleshooting Commands

Note Before issuing **debug** commands, please see *Important Information on Debug Commands*.

The following **debug** commands must be running on both IPSec routers (peers). Security associations must be cleared on both peers.

- **debug crypto engine**—Displays information pertaining to the crypto engine, such as when the Cisco IOS software is performing encryption or decryption operations.
- **debug crypto ipsec**—Displays IPSec negotiations of phase 2.
- **debug crypto isakmp**—Displays ISAKMP negotiations of phase 1.
- **debug ip pim auto-rp**—Displays the contents of each PIM packet used in the automatic discovery of group-to-rendezvous point (RP) mapping as well as the actions taken on the address-to-RP mapping database.
- **clear crypto isakmp**—Clears the security associations related to phase 1.
- **clear crypto sa**—Clears the security associations related to phase 2.

The following is an example of output for the **debug crypto isakmp** and **debug crypto ipsec** commands. Relevant display output is shown in bold text, and comments are preceded by an exclamation point and shown in italics.

```
router# debug crypto isakmp
router# debug crypto ipsec

Jul 29 16:06:33.619 PDT: ISAKMP (0:134217730): received packet from 10.32.150.46 dport 500
sport 500 Global (I) MM_SA_SETUP
Jul 29 16:06:33.619 PDT: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Jul 29 16:06:33.619 PDT: ISAKMP:(0:2:SW:1):Old State = IKE_I_MM3  New State = IKE_I_MM4
Jul 29 16:06:33.619 PDT: ISAKMP:(0:2:SW:1): processing KE payload. message ID = 0
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1): processing NONCE payload. message ID = 0
Jul 29 16:06:33.635 PDT: ISAKMP: Looking for a matching key for 10.32.150.46 in default :
success
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1):found peer pre-shared key matching 10.32.150.46
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1):SKEYID state generated
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1): processing vendor id payload
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1): vendor ID is Unity
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1): processing vendor id payload
```

```
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1): vendor ID is DPD
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1): processing vendor id payload
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1): speaking to another IOS box!
Jul 29 16:06:33.635 PDT: ISAKMP:received payload type 20
Jul 29 16:06:33.635 PDT: ISAKMP:received payload type 20
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
Jul 29 16:06:33.635 PDT: ISAKMP:(0:2:SW:1):Old State = IKE_I_MM4  New State = IKE_I_MM4
Jul 29 16:06:33.639 PDT: ISAKMP:(0:2:SW:1):Send initial contact
Jul 29 16:06:33.639 PDT: ISAKMP:(0:2:SW:1):SA is doing pre-shared key authentication using
id type ID_IPV4_ADDR
Jul 29 16:06:33.639 PDT: ISAKMP (0:134217730): ID payload
        next-payload : 8
        type         : 1
        address      : 10.32.152.26
        protocol     : 17
        port         : 500
        length       : 12
Jul 29 16:06:33.639 PDT: ISAKMP:(0:2:SW:1):Total payload length: 12
Jul 29 16:06:33.639 PDT: ISAKMP:(0:2:SW:1): sending packet to 10.32.150.46 my_port 500
peer_port 500 (I) MM_KEY_EXCH
Jul 29 16:06:33.639 PDT: ISAKMP:(0:2:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Jul 29 16:06:33.639 PDT: ISAKMP:(0:2:SW:1):Old State = IKE_I_MM4  New State = IKE_I_MM5
Jul 29 16:06:33.643 PDT: ISAKMP (0:134217730): received packet from 10.32.150.46 dport 500
sport 500 Global (I) MM_KEY_EXCH
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1): processing ID payload. message ID = 0
Jul 29 16:06:33.643 PDT: ISAKMP (0:134217730): ID payload
        next-payload : 8
        type         : 1
        address      : 10.32.150.46
        protocol     : 17
        port         : 500
        length       : 12
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1): processing HASH payload. message ID = 0
! REMOTE PEER IS SHOWN TO BE AUTHENTICATED IN THE NEXT LINE.
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):SA authentication status:
        authenticated
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):SA has been authenticated with 10.32.150.46
Jul 29 16:06:33.643 PDT: ISAKMP: Trying to insert a peer 10.32.152.26/10.32.150.46/500/,
and inserted successfully.
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):Old State = IKE_I_MM5  New State = IKE_I_MM6
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):Old State = IKE_I_MM6  New State = IKE_I_MM6
Jul 29 16:06:33.643 PDT: ISAKMP (0:134217730): received packet from 10.32.150.46 dport 500
sport 500 Global (I) MM_KEY_EXCH
Jul 29 16:06:33.643 PDT: ISAKMP: set new node 2118711810 to QM_IDLE
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1): processing HASH payload. message ID =
2118711810
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1): processing DELETE payload. message ID =
2118711810
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):peer does not do paranoid keepalives.
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):deleting node 2118711810 error FALSE reason
"Informational (in) state 1"
Jul 29 16:06:33.643 PDT: IPSEC(key_engine): got a queue event with 1 kei messages
Jul 29 16:06:33.643 PDT: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
! PHASE 1 IS SHOWN TO BE COMPLETED SUCCESSFULLY IN THE NEXT LINE.
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):Old State = IKE_I_MM6  New State =
IKE_P1_COMPLETE
Jul 29 16:06:33.643 PDT: ISAKMP:(0:2:SW:1):beginning Quick Mode exchange, M-ID of
159862783
```

```
Jul 29 16:06:33.651 PDT: ISAKMP:(0:2:SW:1): sending packet to 10.32.150.46 my_port 500
peer_port 500 (I) QM_IDLE
Jul 29 16:06:33.651 PDT: ISAKMP:(0:2:SW:1):Node 159862783, Input = IKE_MESG_INTERNAL,
IKE_INIT_QM
Jul 29 16:06:33.651 PDT: ISAKMP:(0:2:SW:1):Old State = IKE_QM_READY  New State =
IKE_QM_I_QM1
Jul 29 16:06:33.651 PDT: ISAKMP:(0:2:SW:1):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Jul 29 16:06:33.651 PDT: ISAKMP:(0:2:SW:1):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
Jul 29 16:06:33.923 PDT: ISAKMP (0:134217730): received packet from 10.32.150.46 dport 500
sport 500 Global (I) QM_IDLE
Jul 29 16:06:33.923 PDT: ISAKMP:(0:2:SW:1): processing HASH payload. message ID =
159862783
Jul 29 16:06:33.923 PDT: ISAKMP:(0:2:SW:1): processing SA payload. message ID = 159862783
Jul 29 16:06:33.923 PDT: ISAKMP:(0:2:SW:1):Checking IPSec proposal 1
Jul 29 16:06:33.923 PDT: ISAKMP: transform 1, ESP_3DES
Jul 29 16:06:33.923 PDT: ISAKMP:   attributes in transform:
Jul 29 16:06:33.923 PDT: ISAKMP:      encaps is 1 (Tunnel)
Jul 29 16:06:33.923 PDT: ISAKMP:      SA life type in seconds
Jul 29 16:06:33.923 PDT: ISAKMP:      SA life duration (basic) of 3600
Jul 29 16:06:33.923 PDT: ISAKMP:      SA life type in kilobytes
Jul 29 16:06:33.923 PDT: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
Jul 29 16:06:33.923 PDT: ISAKMP:      authenticator is HMAC-SHA
Jul 29 16:06:33.923 PDT: ISAKMP:      group is 1

! A PROPOSAL IS FOUND THAT IS COMPATIBLE IN THE NEXT LINE.
Jul 29 16:06:33.923 PDT: ISAKMP:(0:2:SW:1):atts are acceptable.
Jul 29 16:06:33.923 PDT: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.32.152.26, remote= 10.32.150.46,
    local_proxy= 10.32.152.26/255.255.255.255/47/0 (type=1),
    remote_proxy= 10.32.150.46/255.255.255.255/47/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x12
Jul 29 16:06:33.923 PDT: Crypto mapdb : proxy_match
        src addr     : 10.32.152.26
        dst addr     : 10.32.150.46
        protocol     : 47
        src port     : 0
        dst port     : 0
Jul 29 16:06:33.923 PDT: ISAKMP:(0:2:SW:1): processing NONCE payload. message ID =
159862783
Jul 29 16:06:33.923 PDT: ISAKMP:(0:2:SW:1): processing KE payload. message ID = 159862783
Jul 29 16:06:33.931 PDT: ISAKMP:(0:2:SW:1): processing ID payload. message ID = 159862783
Jul 29 16:06:33.931 PDT: ISAKMP:(0:2:SW:1): processing ID payload. message ID = 159862783
Jul 29 16:06:33.931 PDT: ISAKMP: Locking peer struct 0x6635AA1C, IPSEC refcount 1 for for
stuff_ke
Jul 29 16:06:33.931 PDT: ISAKMP:(0:2:SW:1): Creating IPSec SAs
Jul 29 16:06:33.931 PDT:         inbound SA from 10.32.150.46 to 10.32.152.26 (f/i)  0/ 0
        (proxy 10.32.150.46 to 10.32.152.26)
Jul 29 16:06:33.931 PDT:         has spi 0x1442EBFC and conn_id 0 and flags 13
Jul 29 16:06:33.931 PDT:         lifetime of 3600 seconds
Jul 29 16:06:33.931 PDT:         lifetime of 4608000 kilobytes
Jul 29 16:06:33.931 PDT:         has client flags 0x0
Jul 29 16:06:33.931 PDT:         outbound SA from 10.32.152.26 to 10.32.150.46 (f/i) 0/0
        (proxy 10.32.152.26 to 10.32.150.46)
Jul 29 16:06:33.931 PDT:         has spi -2093906224 and conn_id 0 and flags 1B
Jul 29 16:06:33.931 PDT:         lifetime of 3600 seconds
Jul 29 16:06:33.931 PDT:         lifetime of 4608000 kilobytes
Jul 29 16:06:33.931 PDT:         has client flags 0x0
Jul 29 16:06:33.931 PDT: ISAKMP:(0:2:SW:1): sending packet to 10.32.150.46 my_port 500
peer_port 500 (I) QM_IDLE
Jul 29 16:06:33.935 PDT: ISAKMP:(0:2:SW:1):deleting node 159862783 error FALSE reason "No
Error"
```

```
Jul 29 16:06:33.935 PDT: ISAKMP:(0:2:SW:1):Node 159862783, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
! PHASE 2 IS SHOWN TO BE COMPLETED SUCCESSFULLY IN THE NEXT LINE.
Jul 29 16:06:33.935 PDT: ISAKMP:(0:2:SW:1):Old State = IKE_QM_I_QM1  New State =
IKE_QM_PHASE2_COMPLETE
Jul 29 16:06:33.935 PDT: IPSEC(key_engine): got a queue event with 2 kei messages
Jul 29 16:06:33.935 PDT: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 10.32.152.26, remote= 10.32.150.46,
    local_proxy= 10.32.152.26/0.0.0.0/47/0 (type=1),
    remote_proxy= 10.32.150.46/0.0.0.0/47/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0x1442EBFC(339930108), conn_id= 0, keysize= 0, flags= 0x13
Jul 29 16:06:33.935 PDT: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 10.32.152.26, remote= 10.32.150.46,
    local_proxy= 10.32.152.26/0.0.0.0/47/0 (type=1),
    remote_proxy= 10.32.150.46/0.0.0.0/47/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0x833186D0(2201061072), conn_id= 0, keysize= 0, flags= 0x1B
Jul 29 16:06:33.935 PDT: Crypto mapdb : proxy_match
        src addr     : 10.32.152.26
        dst addr     : 10.32.150.46
        protocol     : 47
        src port     : 0
        dst port     : 0
Jul 29 16:06:33.935 PDT: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the
same proxies and 101.253.249.204
Jul 29 16:06:33.935 PDT: IPSec: Flow_switching Allocated flow for sibling 80000003
Jul 29 16:06:33.935 PDT: IPSEC(policy_db_add_ident): src 10.32.152.26, dest 10.32.150.46,
dest_port 0
Jul 29 16:06:33.935 PDT: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.32.152.26, sa_proto= 50,
    sa_spi= 0x1442EBFC(339930108),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 4002
Jul 29 16:06:33.935 PDT: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.32.150.46, sa_proto= 50,
    sa_spi= 0x833186D0(2201061072),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 4001
```

Related Information

- *Cisco IOS Quality of Service Configuration Guide, Release 12.3*
- *Cisco IOS Security Configuration Guide*
- *Cisco IOS Voice Command Reference, Release 12.3*
- *Cisco IOS Wide-Area Networking Configuration Guide*
- Cisco Technical Assistance Center