For this lab section, refer to Figure 26-5 on page 922 of the book.

Step 1

```
R8

interface Dialer10
 ip address 172.22.85.1 255.255.255.0
 encapsulation ppp
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 7 0822455D0A16
 ip ospf cost 65535
 dialer in-band
 dialer idle-timeout 60
 dialer enable-timeout 5
 dialer hold-queue 20
 dialer aaa
 dialer-group 1
 no peer default ip address
 no cdp enable
 ppp callback accept
 ppp authentication chap callin
 crypto map vpn
```

```
R8R8#sho crypto map
Crypto Map "vpn" 10 ipsec-isakmp
        Peer = 6.6.6.6
        Extended IP access list 111
            access-list 111 permit ip 18.18.18.0 0.0.0.255
16.16.16.0 0.0.0.255
        Current peer: 6.6.6.6
        Security association lifetime: 4608000
kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                trvpn,
        }

Crypto Map "vpn" 20 ipsec-isakmp
        Peer = 4.4.4.4
        Extended IP access list 112
            access-list 112 permit ip 18.18.18.0 0.0.0.255
14.14.14.0 0.0.0.255
        Current peer: 4.4.4.4
        Security association lifetime: 4608000
kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                trvpn,
        }

Crypto Map "vpn" 30 ipsec-isakmp
        Peer = 3.3.3.3
        Extended IP access list 113
            access-list 113 permit ip 18.18.18.0 0.0.0.255
13.13.13.0 0.0.0.255
```

```
        Current peer: 3.3.3.3
        Security association lifetime: 4608000
kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                trvpn,
        }
        Interfaces using crypto map vpn:
                Tunnel1
                Tunnel3
                Tunnel4
                Tunnel6
                Dialer10
```

```
1w4d: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to
up
1w4d: BR0/0:1 PPP: Using dialer call direction
1w4d: BR0/0:1 PPP: Treating connection as a callin
1w4d: BR0/0:1 PPP: Phase is ESTABLISHING, Passive Open
1w4d: BR0/0:1 LCP: State is Listen
1w4d: BR0/0:1 LCP: TIMEout: State Listen
1w4d: BR0/0:1 PPP: Authorization required
1w4d: BR0/0:1 LCP: O CONFREQ [Listen] id 82 len 15
1w4d: BR0/0:1 LCP:    AuthProto CHAP (0x0305C22305)
1w4d: BR0/0:1 LCP:    MagicNumber 0xEB79A1D5
(0x0506EB79A1D5)
1w4d: BR0/0:1 LCP: I CONFACK [REQsent] id 82 len 15
1w4d: BR0/0:1 LCP:    AuthProto CHAP (0x0305C22305)
1w4d: BR0/0:1 LCP:    MagicNumber 0xEB79A1D5
(0x0506EB79A1D5)
1w4d: BR0/0:1 LCP: I CONFREQ [ACKrcvd] id 15 len 18
1w4d: BR0/0:1 LCP:    AuthProto CHAP (0x0305C22305)
1w4d: BR0/0:1 LCP:    MagicNumber 0xB06EF32D
(0x0506B06EF32D)
1w4d: BR0/0:1 LCP:    Callback 0  (0x0D0300)
1w4d: BR0/0:1 LCP: O CONFACK [ACKrcvd] id 15 len 18
1w4d: BR0/0:1 LCP:    AuthProto CHAP (0x0305C22305)
1w4d: BR0/0:1 LCP:    MagicNumber 0xB06EF32D
(0x0506B06EF32D)
1w4d: BR0/0:1 LCP:    Callback 0  (0x0D0300)
1w4d: BR0/0:1 LCP: State is Open
1w4d: BR0/0:1 PPP: Phase is AUTHENTICATING, by both
1w4d: BR0/0:1 CHAP: O CHALLENGE id 154 len 23 from "R8"
1w4d: BR0/0:1 CHAP: I CHALLENGE id 3 len 23 from "R6"
1w4d: BR0/0:1 CHAP: Waiting for Peer to authenticate first
1w4d: BR0/0:1 CHAP: I RESPONSE id 154 len 23 from "R6"
1w4d: BR0/0:1 PPP: Phase is FORWARDING, Attempting Forward
1w4d: BR0/0:1 PPP: Phase is AUTHENTICATING, Unauthenticated
User
1w4d: BR0/0:1 PPP: Sent CHAP LOGIN Request
1w4d: BR0/0:1 PPP: Received LOGIN Response PASS
1w4d: BR0/0:1 PPP: Phase is FORWARDING, Attempting Forward
1w4d: BR0/0:1 PPP: Phase is AUTHENTICATING, Authenticated
User
1w4d: BR0/0:1 DDR: Remote name for R6
1w4d: BR0/0:1 DDR: Authenticated host R6 with no matching
dialer map
```

```
1w4d: BR0/0:1 PPP: Sent LCP AUTHOR Request
1w4d: BR0/0:1 PPP: Sent IPCP AUTHOR Request
1w4d: BR0/0:1 CHAP: Using hostname from unknown source
1w4d: BR0/0:1 CHAP: Using password from AAA
1w4d: BR0/0:1 CHAP: O RESPONSE id 3 len 23 from "R8"
1w4d: BR0/0:1 LCP: Received AAA AUTHOR Response PASS
1w4d: BR0/0:1 CHAP: I SUCCESS id 3 len 4
1w4d: BR0/0:1 IPCP: Received AAA AUTHOR Response PASS
1w4d: BR0/0:1 CHAP: O SUCCESS id 154 len 4
1w4d: DSES 1A5E0: Session create
1w4d: BR0/0:1 DDR: PPP callback: Callback server starting to
R6 6666
1w4d: BR0/0:1 DDR: disconnecting call
1w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0/0:1, changed state to up
1w4d: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected
to 6666 R6
1w4d: %ISDN-6-DISCONNECT: Interface BRI0/0:1  disconnected
from 6666 R6, call lasted 3 seconds
1w4d: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to
down
1w4d: BR0/0:1 PPP: Sending Acct Event[Down] id[14E]
1w4d: BR0/0:1 PPP: Phase is TERMINATING
1w4d: BR0/0:1 LCP: State is Closed
1w4d: BR0/0:1 PPP: Phase is DOWN
1w4d: BR0/0:1 DDR: disconnecting call
1w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0/0:1, changed state to down
1w4d: DDR: Callback timer expired
1w4d: Di10 DDR: beginning callback to R6 6666
1w4d: BR0/0 DDR: rotor dialout [priority]
1w4d: BR0/0 DDR: Dialing cause ???
1w4d: BR0/0 DDR: Attempting to dial 6666
1w4d: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to
up
1w4d: DDR: Freeing callback to R6 6666
1w4d: DDR: removing callback, 0 packets unqueued and
discarded
1w4d: BR0/0:1 PPP(0000014F): Replacing Acct Session Id from
PPP Callback Author Data
1w4d: BR0/0:1 PPP: Using dialer call direction
1w4d: BR0/0:1 PPP: Treating connection as a callout
1w4d: BR0/0:1 PPP: Phase is ESTABLISHING, Active Open
1w4d: BR0/0:1 PPP: Authorization required
1w4d: BR0/0:1 PPP: No remote authentication for callback
1w4d: BR0/0:1 LCP: O CONFREQ [Closed] id 83 len 10
1w4d: BR0/0:1 LCP:    MagicNumber 0xEB79B65D
(0x0506EB79B65D)
1w4d: BR0/0:1 LCP: I CONFREQ [REQsent] id 16 len 15
1w4d: BR0/0:1 LCP:    AuthProto CHAP (0x0305C22305)
1w4d: BR0/0:1 LCP:    MagicNumber 0xB06F16EB
(0x0506B06F16EB)
1w4d: BR0/0:1 LCP: O CONFACK [REQsent] id 16 len 15
1w4d: BR0/0:1 LCP:    AuthProto CHAP (0x0305C22305)
1w4d: BR0/0:1 LCP:    MagicNumber 0xB06F16EB
(0x0506B06F16EB)
1w4d: BR0/0:1 LCP: TIMEout: State ACKsent
1w4d: BR0/0:1 LCP: O CONFREQ [ACKsent] id 84 len 10
```

```
1w4d: BR0/0:1 LCP:    MagicNumber 0xEB79B65D
(0x0506EB79B65D)
1w4d: BR0/0:1 LCP: I CONFACK [ACKsent] id 84 len 10
1w4d: BR0/0:1 LCP:    MagicNumber 0xEB79B65D
(0x0506EB79B65D)
1w4d: BR0/0:1 LCP: State is Open
1w4d: BR0/0:1 PPP: Phase is AUTHENTICATING, by the peer
1w4d: BR0/0:1 CHAP: I CHALLENGE id 4 len 23 from "R6"
1w4d: BR0/0:1 CHAP: Using hostname from unknown source
1w4d: BR0/0:1 CHAP: Using password from AAA
1w4d: BR0/0:1 CHAP: O RESPONSE id 4 len 23 from "R8"
1w4d: BR0/0:1 CHAP: I SUCCESS id 4 len 4
1w4d: BR0/0:1 PPP: Phase is FORWARDING, Attempting Forward
1w4d: BR0/0:1 PPP: Phase is ESTABLISHING, Finish LCP
1w4d: BR0/0:1 PPP: Phase is UP
1w4d: BR0/0:1 IPCP: O CONFREQ [Closed] id 1 len 10
1w4d: BR0/0:1 IPCP:    Address 172.22.85.1 (0x0306AC165501)
1w4d: BR0/0:1 PPP: Process pending packets
1w4d: BR0/0:1 IPCP: I CONFREQ [REQsent] id 1 len 10
1w4d: BR0/0:1 IPCP:    Address 172.22.85.2 (0x0306AC165502)
1w4d: BR0/0:1 AAA/AUTHOR/IPCP: Start.  Her address
172.22.85.2, we want 0.0.0.0
1w4d: BR0/0:1 AAA/AUTHOR/IPCP: Reject 172.22.85.2, using
0.0.0.0
1w4d: BR0/0:1 AAA/AUTHOR/IPCP: Done.  Her address
172.22.85.2, we want 0.0.0.0
1w4d: BR0/0:1 IPCP: O CONFACK [REQsent] id 1 len 10
1w4d: BR0/0:1 IPCP:    Address 172.22.85.2 (0x0306AC165502)
1w4d: BR0/0:1 IPCP: I CONFACK [ACKsent] id 1 len 10
1w4d: BR0/0:1 IPCP:    Address 172.22.85.1 (0x0306AC165501)
1w4d: BR0/0:1 IPCP: State is Open
1w4d: Di10 IPCP: Install route to 172.22.85.2
1w4d: BR0/0:1 IPCP: Add link info for cef entry 172.22.85.2
1w4d: BR0/0:1 DDR: dialer protocol up
1w4d: BR0/0:1: Call connected, 0 packets unqueued, 0
transmitted, 0 discarded
1w4d: %OSPF-5-ADJCHG: Process 123, Nbr 6.6.6.6 on Dialer10
from DOWN to INIT, Received Hello
1w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0/0:1, changed state to up
1w4d: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected
to 6666 unknown
```

```
R8R8#sho 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, 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 65.25.160.1 to network 0.0.0.0
```

```
     17.0.0.0/24 is subnetted, 1 subnets
B       17.1.1.0 [20/0] via 172.22.85.2, 00:00:55
D    192.168.46.0/24 [90/310044416] via 192.168.68.1,
00:00:58, Tunnel6
     16.0.0.0/32 is subnetted, 1 subnets
D       16.16.16.16 [90/297372416] via 192.168.68.1,
00:00:58, Tunnel6
     1.0.0.0/32 is subnetted, 2 subnets
O IA    1.1.1.1 [110/357] via 172.22.85.2, 00:00:47,
Dialer10
B       1.1.1.11 [20/0] via 172.22.85.2, 00:00:55
     2.0.0.0/32 is subnetted, 2 subnets
C       2.2.2.2 is directly connected, Loopback0
B       2.2.2.22 [20/0] via 172.22.85.2, 00:00:55
     18.0.0.0/32 is subnetted, 1 subnets
C       18.18.18.18 is directly connected, Loopback18
     3.0.0.0/32 is subnetted, 4 subnets
O IA    3.3.3.3 [110/293] via 172.22.85.2, 00:00:47,
Dialer10
O E2    3.3.3.13 [110/20] via 172.22.85.2, 00:00:47,
Dialer10
O E2    3.3.3.23 [110/20] via 172.22.85.2, 00:00:47,
Dialer10
B       3.3.3.33 [20/0] via 172.22.85.2, 00:00:56
     4.0.0.0/32 is subnetted, 2 subnets
O IA    4.4.4.4 [110/229] via 172.22.85.2, 00:00:47,
Dialer10
B       4.4.4.44 [20/0] via 172.22.85.2, 00:00:56
     140.100.0.0/16 is variably subnetted, 4 subnets, 2
masks
O IA    140.100.45.0/26 [110/228] via 172.22.85.2, 00:00:47,
Dialer10
B       140.100.47.0/26 [20/0] via 172.22.85.2, 00:00:56
O IA    140.100.56.0/26 [110/164] via 172.22.85.2, 00:00:47,
Dialer10
O E2    140.100.9.0/27 [110/20] via 172.22.85.2, 00:00:47,
Dialer10
     65.0.0.0/20 is subnetted, 1 subnets
C       65.25.160.0 is directly connected, FastEthernet0/0
     5.0.0.0/32 is subnetted, 2 subnets
S       5.5.5.5 [1/0] via 192.168.1.222
B       5.5.5.55 [20/0] via 172.22.85.2, 00:00:56
     156.46.0.0/16 is variably subnetted, 5 subnets, 2 masks
B       156.46.2.0/24 [20/0] via 172.22.85.2, 00:00:56
B       156.46.3.0/24 [20/0] via 172.22.85.2, 00:00:56
B       156.46.1.0/24 [20/0] via 172.22.85.2, 00:00:56
B       156.46.4.0/24 [20/0] via 172.22.85.2, 00:00:56
B       156.46.100.0/22 [20/0] via 172.22.85.2, 00:00:56
     6.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O IA    6.6.6.6/32 [110/101] via 172.22.85.2, 00:00:47,
Dialer10
S       6.6.6.0/24 [1/0] via 192.168.1.222
B       6.6.6.66/32 [20/0] via 172.22.85.2, 00:00:56
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Loopback100
     172.19.0.0/32 is subnetted, 1 subnets
```

```
O E2    172.19.1.1 [110/20] via 172.22.85.2, 00:00:47,
Dialer10
     172.18.0.0/32 is subnetted, 1 subnets
O E2    172.18.1.1 [110/20] via 172.22.85.2, 00:00:47,
Dialer10
     172.22.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.22.85.2/32 is directly connected, Dialer10
C       172.22.85.0/24 is directly connected, Dialer10
     67.0.0.0/24 is subnetted, 1 subnets
O E2    67.67.67.0 [110/20] via 172.22.85.2, 00:00:47,
Dialer10
     37.0.0.0/24 is subnetted, 1 subnets
B       37.1.1.0 [20/0] via 172.22.85.2, 00:00:56
     7.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
B       7.7.7.7/32 [20/0] via 172.22.85.2, 00:00:56
B       7.1.1.0/24 [20/0] via 172.22.85.2, 00:00:56
     8.0.0.0/32 is subnetted, 2 subnets
C       8.8.8.8 is directly connected, Loopback8
C       8.8.8.88 is directly connected, Loopback88
C    192.168.38.0/24 is directly connected, Tunnel3
     9.0.0.0/32 is subnetted, 1 subnets
B       9.9.9.9 [20/0] via 172.22.85.2, 00:00:56
     130.100.0.0/24 is subnetted, 1 subnets
S       130.100.26.0 [1/0] via 192.168.1.222
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial0/0
     27.0.0.0/24 is subnetted, 1 subnets
B       27.1.1.0 [20/0] via 172.22.85.2, 00:00:56
D    192.168.36.0/24 [90/310044416] via 192.168.68.1,
00:00:58, Tunnel6
     11.0.0.0/32 is subnetted, 1 subnets
O IA    11.11.11.11 [110/357] via 172.22.85.2, 00:00:47,
Dialer10
D    192.168.34.0/24 [90/310044416] via 192.168.48.1,
00:00:58, Tunnel4
     12.0.0.0/32 is subnetted, 1 subnets
O IA    12.12.12.12 [110/357] via 172.22.85.2, 00:00:47,
Dialer10
C    192.168.68.0/24 is directly connected, Tunnel6
C    192.168.1.0/24 is directly connected, FastEthernet0/1
     13.0.0.0/32 is subnetted, 1 subnets
D       13.13.13.13 [90/297372416] via 192.168.38.1,
00:00:59, Tunnel3
O    192.168.2.0/24 [110/11211] via 172.22.85.2, 00:00:48,
Dialer10
     14.0.0.0/32 is subnetted, 1 subnets
D       14.14.14.14 [90/297372416] via 192.168.48.1,
00:00:59, Tunnel4
     150.100.0.0/16 is variably subnetted, 3 subnets, 3
masks
O IA    150.100.32.0/27 [110/356] via 172.22.85.2, 00:00:48,
Dialer10
O IA    150.100.33.0/29 [110/292] via 172.22.85.2, 00:00:48,
Dialer10
O IA    150.100.31.0/28 [110/356] via 172.22.85.2, 00:00:48,
Dialer10
C    192.168.48.0/24 is directly connected, Tunnel4
S*   0.0.0.0/0 [254/0] via 65.25.160.1
```

```
B    209.112.0.0/16 [20/0] via 172.22.85.2, 00:00:56
R8#
```

```
R8#sho ip route eigrp
D    192.168.46.0/24 [90/310044416] via 192.168.68.1,
00:01:25, Tunnel6
     16.0.0.0/32 is subnetted, 1 subnets
D       16.16.16.16 [90/297372416] via 192.168.68.1,
00:01:25, Tunnel6
D    192.168.36.0/24 [90/310044416] via 192.168.68.1,
00:01:25, Tunnel6
D    192.168.34.0/24 [90/310044416] via 192.168.48.1,
00:01:25, Tunnel4
     13.0.0.0/32 is subnetted, 1 subnets
D       13.13.13.13 [90/297372416] via 192.168.38.1,
00:01:25, Tunnel3
     14.0.0.0/32 is subnetted, 1 subnets
D       14.14.14.14 [90/297372416] via 192.168.48.1,
00:01:25, Tunnel4
```

```
R8# sho crypto isakmp sa
dst             src             state          conn-id
slot
3.3.3.3         8.8.8.8         QM_IDLE              3
0
6.6.6.6         8.8.8.8         QM_IDLE              2
0
4.4.4.4         8.8.8.8         QM_IDLE            1       0
```

```
hostname R6
!
logging queue-limit 100
aaa new-model
aaa authentication ppp default local
aaa authorization network default local
!
username R8 password 0 cisco
ip subnet-zero
ip cef
!
!
no ip domain-lookup
ip dhcp excluded-address 130.100.26.6
ip dhcp excluded-address 130.100.26.2
!
ip dhcp pool ccie
   network 130.100.26.0 255.255.255.224
   default-router 130.100.26.6
!
ip inspect audit-trail
ip inspect name ccie tcp
ip inspect name ccie udp
ip inspect name ccie ftp
ip inspect name ccie smtp

ip audit notify nr-director
```

```
ip audit notify log
ip audit po max-events 180
ip audit po remote hostid 123 orgid 6666 rmtaddress
130.100.26.8 localaddress 130.100.26.6 port 45000 preference
1 timeou
t 5 application director
ip audit po local hostid 43 orgid 6666
ip audit signature 1100 disable
ip audit signature 2154 disable
ip audit signature 3100 disable
ip audit name testids info action reset
ip audit name testids attack action reset
ip audit name ids info action reset
ip audit name ids attack action reset
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 2000
crypto isakmp key ccie address 3.3.3.3
crypto isakmp key ccie address 8.8.8.8
crypto isakmp key ccie address 4.4.4.4
!
!
crypto ipsec transform-set trvpn esp-des esp-sha-hmac
 mode transport
!
crypto map vpn 10 ipsec-isakmp
 set peer 3.3.3.3
 set transform-set trvpn
 match address 111
crypto map vpn 20 ipsec-isakmp
 set peer 8.8.8.8
 set transform-set trvpn
 match address 112
crypto map vpn 30 ipsec-isakmp
 set peer 4.4.4.4
 set transform-set trvpn
 match address 113
!
isdn switch-type basic-ni
!
key chain ccie
 key 1
  key-string ccie
call rsvp-sync
!
!
interface Loopback6
 description OSPF Loopback
 ip ospf network point-to-point
 ip address 6.6.6.6 255.255.255.255
!
interface Loopback16
 description Loopback for VPN full mesh
 ip address 16.16.16.16 255.255.255.0
!
interface Loopback66
```

```
 ip address 140.100.86.1 255.255.255.224
!
interface Loopback666
 description BGP Loopback
 ip address 6.6.6.66 255.255.255.255
!
interface Tunnel0
 description To R8 over PIX2
 ip address 192.168.2.2 255.255.255.0

 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 cisco

 tunnel source 130.100.26.6
 tunnel destination 130.100.26.3
 crypto map vpn
!
interface Tunnel3
 description Basic GRE Crypto to R3
 ip address 192.168.36.2 255.255.255.0
 tunnel source 6.6.6.6
 tunnel destination 3.3.3.3
 crypto map vpn
!
interface Tunnel4
 description Basic GRE Crypto to R4
 ip address 192.168.46.2 255.255.255.0
 tunnel source 6.6.6.6
 tunnel destination 4.4.4.4
 crypto map vpn
!
interface Tunnel8
 description Basic GRE Crypto to R8
 ip address 192.168.68.1 255.255.255.0
 tunnel source 6.6.6.6
 tunnel destination 8.8.8.8
 crypto map vpn
!
interface FastEthernet0/0
 ip address 130.100.26.6 255.255.255.224
 no ip proxy-arp
 ip nat inside
 ip rip authentication mode md5
 ip rip authentication key-chain ccie
 ip inspect ccie in
 speed 10
 half-duplex
 no cdp enable

 crypto map vpn
!
interface BRI0/0
 no ip address
 encapsulation ppp
 ip ospf cost 65000
 dialer pool-member 1
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
```

```
 isdn spid1 6661 6666
 isdn spid2 6662 6666
 no cdp enable
 ppp authentication chap
!
interface Serial0/0
 ip address 140.100.56.6 255.255.255.192
 ip access-group ccie in
 ip nat outside
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 cisco
 ip ospf network point-to-point
 no cdp enable
 crypto map vpn
!
interface Dialer1
 ip address 172.22.85.2 255.255.255.0
 encapsulation ppp
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 cisco
 ip ospf cost 65535
 ip ospf demand-circuit
 dialer pool 1
 dialer idle-timeout 60
 dialer string 8888
 dialer hold-queue 20
 dialer-group 1
 no peer default ip address
 no fair-queue
 no cdp enable
 ppp callback request
 ppp authentication chap
 ppp chap hostname R6
 ppp chap password 0 cisco
 crypto map vpn
!
router eigrp 100
 network 16.0.0.0
 network 192.168.36.0
 network 192.168.46.0
 network 192.168.68.0
 maximum-paths 1
 no auto-summary
!
router ospf 123
 router-id 6.6.6.6
 log-adjacency-changes detail
 area 56 authentication message-digest
 area 56 virtual-link 5.5.5.5 authentication message-digest
 area 56 virtual-link 5.5.5.5 message-digest-key 5 md5 cisco
 area 86 authentication message-digest
 network 6.6.6.6 0.0.0.0 area 56
 network 140.100.56.0 0.0.0.63 area 56
 network 172.22.85.0 0.0.0.255 area 86
 network 192.168.2.0 0.0.0.255 area 86
 default-information originate always
 distribute-list 1 out
!
```

```
router rip
 version 2
 network 130.100.0.0
 no auto-summary
!
router bgp 456
 no synchronization
 bgp router-id 6.6.6.6
bgp log-neighbor-changes
 network 6.6.6.66 mask 255.255.255.255
 network 130.100.86.0 mask 255.255.255.224
 neighbor 8.8.8.8 remote-as 65000
 neighbor 8.8.8.8 ebgp-multihop 2
 neighbor 8.8.8.8 update-source Loopback6
 neighbor 140.100.56.5 remote-as 456
 neighbor 140.100.56.5 next-hop-self
 no auto-summary
!
!
!
!
```

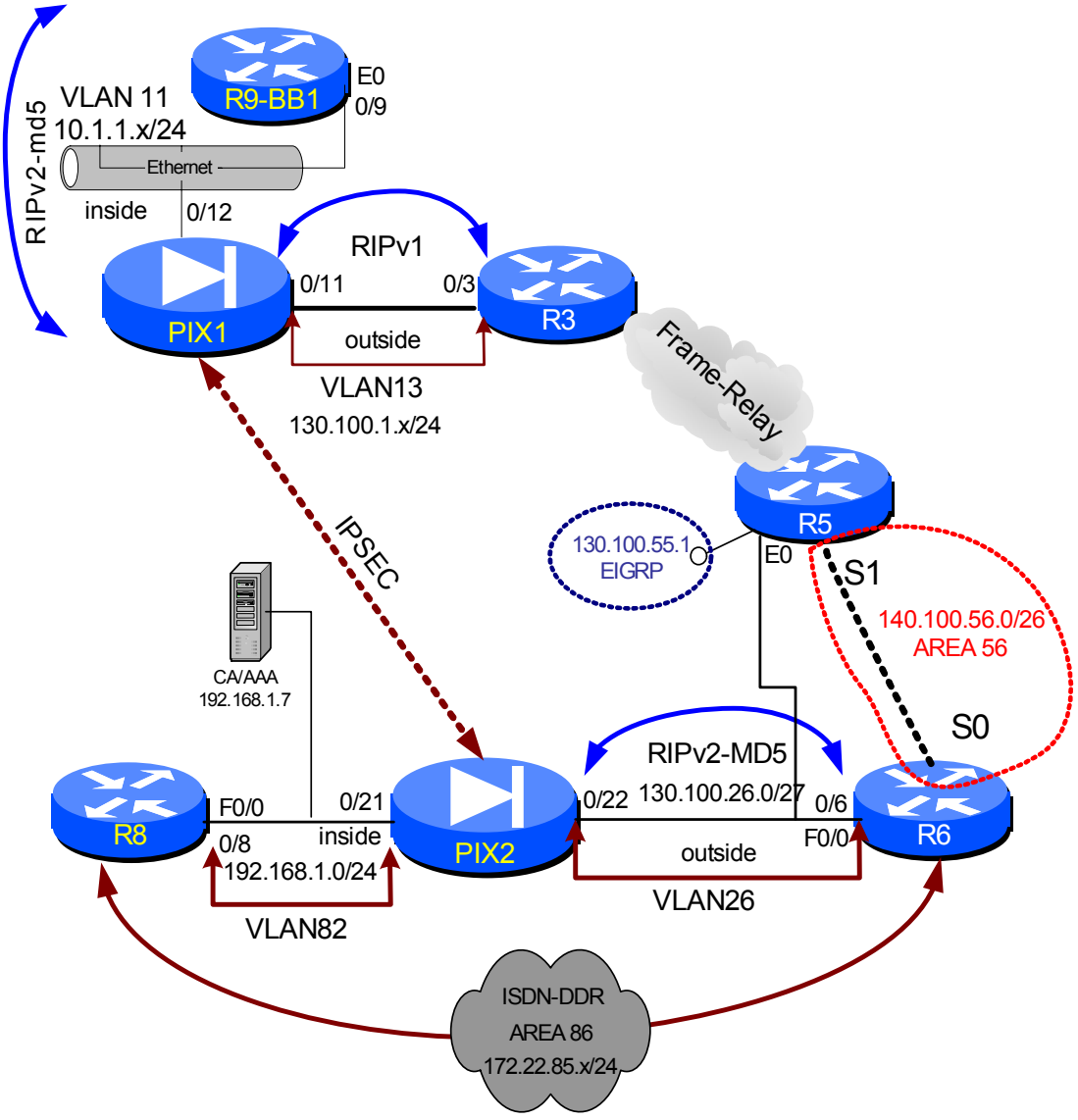
```
R6# sho crypto map
Crypto Map "vpn" 10 ipsec-isakmp
        Peer = 3.3.3.3
        Extended IP access list 111
            access-list 111 permit ip 16.16.16.0 0.0.0.255
13.13.13.0 0.0.0.255
        Current peer: 3.3.3.3
        Security association lifetime: 4608000
kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ trvpn, }

Crypto Map "vpn" 20 ipsec-isakmp
        Peer = 8.8.8.8
        Extended IP access list 112
            access-list 112 permit ip 16.16.16.0 0.0.0.255
18.18.18.0 0.0.0.255
        Current peer: 8.8.8.8
        Security association lifetime: 4608000
kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ trvpn, }

Crypto Map "vpn" 30 ipsec-isakmp
        Peer = 4.4.4.4
        Extended IP access list 113
            access-list 113 permit ip 16.16.16.0 0.0.0.255
14.14.14.0 0.0.0.255
        Current peer: 4.4.4.4
        Security association lifetime: 4608000
kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ trvpn, }
        Interfaces using crypto map vpn:
                FastEthernet0/0
                Serial0/0
```

```
                    Dialer1
                    Tunnel0
                    Tunnel3
                    Tunnel4
                    Tunnel8

R6#
```



Step 2

```
PIX2(config)# sho run
: Saved
:
```

```
PIX Version 6.2(2)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
hostname PIX2
access-list inside_outbound_nat0_acl permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
access-list outside_cryptomap_20 permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
ip address outside 130.100.26.2 255.255.255.224
ip address inside 192.168.1.222 255.255.255.0
nat (inside) 0 access-list inside_outbound_nat0_acl
access-group outside_access_in in interface outside
route outside 0.0.0.0 0.0.0.0 130.100.26.6 1
route inside 192.168.0.0 255.255.0.0 192.168.1.1 1
sysopt connection permit-ipsec
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto map outside_map 20 ipsec-isakmp
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 130.100.1.1
crypto map outside_map 20 set transform-set ESP-DES-MD5
crypto map outside_map interface outside
isakmp enable outside
isakmp key ******** address 130.100.1.1 netmask 255.255.255.255
no-xauth no-config-mode
isakmp identity address
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 86400
```

```
PIX2(config)# debug crypto ipsec
PIX2(config)# debug crypto isakmp
PIX2(config)# debug crypto engine
```

```
ISAKMP (0): beginning Main Mode exchange

crypto_isakmp_process_block:src:130.100.1.1, dest:130.100.26.2
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id
type ID_IPV4_ADDR
```

```
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:130.100.1.1, dest:130.100.26.2
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!

ISAKMP (0): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:130.100.1.1, dest:130.100.26.2
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP (0): beginning Quick Mode exchange, M-ID of
100359867:5fb5ebbIPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x48958e19(1217760793) for SA
        from     130.100.1.1 to    130.100.26.2 for prot 3

return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:130.100.1.1/500 Total VPN
Peers:1
VPN Peer: ISAKMP: Peer ip:130.100.1.1/500 Ref cnt incremented to:1
Total VPN Peers:1
crypto_isakmp_process_block:src:130.100.1.1, dest:130.100.26.2
spt:500 dpt:500
crypto_isakmp_process_block:src:130.100.1.1, dest:130.100.26.2
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 100359867

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
```

```
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
proposal part #1,
  (key eng. msg.) dest= 130.100.1.1, src= 130.100.26.2,
    dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 100359867

ISAKMP (0): processing ID payload. message ID = 100359867
ISAKMP (0): processing ID payload. message ID =
100359867map_alloc_entry: allocating entry 1
map_alloc_entry: allocating entry 2

ISAKMP (0): Creating IPSec SAs
        inbound SA from     130.100.1.1 to    130.100.26.2 (proxy
10.1.1.0 to     192.168.1.0)
        has spi 1217760793 and conn_id 1 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from    130.100.26.2 to     130.100.1.1 (proxy
192.168.1.0 to        10.1.1.0)
        has spi 342191396 and conn_id 2 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a
queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 130.100.26.2, src= 130.100.1.1,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x48958e19(1217760793), conn_id= 1, keysize= 0, flags=
0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 130.100.26.2, dest= 130.100.1.1,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x14656d24(342191396), conn_id= 2, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:130.100.1.1/500 Ref cnt incremented to:2
Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:130.100.1.1/500 Ref cnt incremented to:3
Total VPN Peers:1
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:130.100.1.1, dest:130.100.26.2
spt:500 dpt:500
```

```
PIX2(config)# sho crypto isa sa
Total     : 1
Embryonic : 0
        dst               src        state     pending     created
     130.100.1.1     130.100.26.2    QM_IDLE           0           1
```

```
PIX2(config)# sho crypto ipsec sa


interface: outside
    Crypto map tag: outside_map, local addr. 130.100.26.2

   local  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
   current_peer: 130.100.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
    #pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 130.100.26.2, remote crypto endpt.:
130.100.1.1
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 14656d24

     inbound esp sas:
      spi: 0x48958e19(1217760793)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: outside_map
        sa timing: remaining key lifetime (k/sec): (4607999/28579)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:


     inbound pcp sas:


     outbound esp sas:
      spi: 0x14656d24(342191396)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: outside_map
        sa timing: remaining key lifetime (k/sec): (4607999/28579)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:
```

```
    outbound pcp sas:
```

```
PIX2(config)# sho crypto ma

Crypto Map: "outside_map" interfaces: { outside }

Crypto Map "outside_map" 20 ipsec-isakmp
        Peer = 130.100.1.1
        access-list outside_cryptomap_20 turbo-configured; 1
elements
        access-list outside_cryptomap_20 line 1 permit ip
192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0 (hitcnt=6)
        Current peer: 130.100.1.1
        Security association lifetime: 4608000 kilobytes/28800
seconds
        PFS (Y/N): N
        Transform sets={ ESP-DES-MD5, }
pix2(config)#
```

```
PIX1# sho run
: Saved
:
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
hostname PIX1
access-list inside_outbound_nat0_acl permit ip 10.1.1.0
255.255.255.0 192.168.1.0 255.255.255.0
access-list outside_cryptomap_20 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
interface ethernet0 auto
interface ethernet1 auto
ip address outside 130.100.1.1 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
nat (inside) 0 access-list inside_outbound_nat0_acl
static (inside,outside) 10.1.1.9 10.1.1.9 netmask 255.255.255.255
0 0  norandomseq
access-group bgpin in interface outside
route outside 0.0.0.0 0.0.0.0 130.100.1.3 1
route inside 9.9.9.0 255.255.255.0 10.1.1.9 1
sysopt connection permit-ipsec
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto map outside_map 20 ipsec-isakmp
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 130.100.26.2
crypto map outside_map 20 set transform-set ESP-DES-MD5
crypto map outside_map interface outside
isakmp enable outside
isakmp key ******** address 130.100.26.2 netmask 255.255.255.255
no-xauth no-config-mode
isakmp identity address
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
```

```
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 86400
```

```
PIX1# sho crypto isa sa
Total     : 1
Embryonic : 0
        dst             src          state       pending
created
     130.100.1.1     130.100.26.2    QM_IDLE          0           1
```

```
PIX1#sho crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, local addr. 130.100.1.1

   local  ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   current_peer: 130.100.26.2
     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 0, #recv errors 0

     local crypto endpt.: 130.100.1.1, remote crypto endpt.:
130.100.26.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 48958e19

     inbound esp sas:
      spi: 0x14656d24(342191396)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: outside_map
        sa timing: remaining key lifetime (k/sec): (4607999/28300)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:
     inbound pcp sas:

     outbound esp sas:
      spi: 0x48958e19(1217760793)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: outside_map
        sa timing: remaining key lifetime (k/sec): (4607999/28300)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:
```

```
     outbound pcp sas:
```

```
PIX1# sho crypto map

Crypto Map: "outside_map" interfaces: { outside }

Crypto Map "outside_map" 20 ipsec-isakmp
        Peer = 130.100.26.2
        access-list outside_cryptomap_20; 1 elements
        access-list outside_cryptomap_20 permit ip 10.1.1.0
255.255.255.0 192.168.1.0 255.255.255.0 (hitcnt=14)
        Current peer: 130.100.26.2
        Security association lifetime: 4608000 kilobytes/28800
seconds
        PFS (Y/N): N
        Transform sets={ ESP-DES-MD5, }
```

```
R8#ping 10.1.1.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
132/132/136 ms
```