For this lab section, refer to Figure 26-6 on page 927 of the book.

Step 1

```
interface FastEthernet0/0
ip address dhcp
speed auto
 no cdp enable
!
R8#sho interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 00b0.6463.d5c0 (bia
00b0.6463.d5c0)
  Internet address is 65.25.160.24/20 ← DHCP IP Address
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/14073/0 (size/max/drops/flushes); Total
output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 112000 bits/sec, 29 packets/sec
  5 minute output rate 50000 bits/sec, 20 packets/sec
     34930811 packets input, 3686681612 bytes
     Received 12076196 broadcasts, 0 runts, 0 giants, 0
throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     25276212 packets output, 3207017383 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Step 2

```
hostname R1
!
logging queue-limit 100
enable secret 5 $1$1xxK$LWh42sY9aO17mvAuehLPM.
!
ip subnet-zero
no ip domain-lookup
!
!
crypto isakmp policy 1
 authentication pre-share
 crypto isakmp key ccie address 0.0.0.0 0.0.0.0
!
!
```

```
crypto ipsec transform-set tr-ted esp-des esp-md5-hmac
!
crypto dynamic-map ted-map 10
 set transform-set tr-ted
 match address 111
!
!
crypto map ted 10 ipsec-isakmp dynamic ted-map discover
!
!
!
!
interface Loopback1
 description OSPF Loopback
 ip address 1.1.1.1 255.255.255.255
!
interface Loopback10
 description BGP Loopback
 ip address 1.1.1.11 255.255.255.255
!
interface Loopback11
 ip address 11.11.11.11 255.255.255.0
!
interface Loopback12
 description Same IP Address as R2
 ip address 121.121.121.121 255.255.255.0
!
!
!
interface Serial0
 ip address 150.100.31.1 255.255.255.240
 ip nat outside
 encapsulation frame-relay
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 7 094F471A1A0A
 ip ospf network point-to-point
 ip ospf hello-interval 65
 traffic-shape rate 512000 12800 12800 1000
 traffic-shape adaptive 32000
 frame-relay map ip 150.100.31.3 101 broadcast
 frame-relay interface-dlci 101
 frame-relay lmi-type ansi
 crypto map ted
!
!
router ospf 123
 router-id 1.1.1.1
 log-adjacency-changes
 area 0 authentication message-digest
 redistribute static subnets
 network 1.1.1.1 0.0.0.0 area 0
 network 11.11.11.0 0.0.0.255 area 0
 network 150.100.31.0 0.0.0.15 area 0
 network 172.18.1.1 0.0.0.0 area 0
 distribute-list 2 in Serial0
 distribute-list 1 in
!
```

```
ip nat inside source static network 121.121.121.121
172.18.1.1 /32 no-alias
ip classless
ip route 172.18.1.1 255.255.255.255 Null0
ip http server
!
access-list 1 deny   5.5.5.55
access-list 1 permit any
access-list 2 deny   6.6.6.6
access-list 2 permit any

access-list 111 permit ip 11.11.11.0 0.0.0.255 12.12.12.0
0.0.0.255 log
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
line vty 0 4
 logging synchronous
 login
!
end

R1#

R2#sho run
Building configuration...

Current configuration : 2658 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R2
!
logging queue-limit 100
enable secret 5 $1$OiDj$4.39veJ97UQ7La4nOLLiC0
!
ip subnet-zero
no ip domain-lookup
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key ccie address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set tr-ted esp-des esp-md5-hmac
!
crypto dynamic-map ted-map 10
 set transform-set tr-ted
 match address 111
!
!
```

```
crypto map ted 10 ipsec-isakmp dynamic ted-map discover
!
!
!
!
interface Loopback2
 description OSPF Loopback
 ip address 2.2.2.2 255.255.255.255
!
interface Loopback12
 ip address 12.12.12.12 255.255.255.0
!
interface Loopback22
 description BGP Loopback
 ip address 2.2.2.22 255.255.255.255
!
interface Loopback121
 description Same IP Address AS R1
 ip address 121.121.121.121 255.255.255.0
 ip nat inside
!
interface Serial0
 ip address 150.100.32.2 255.255.255.224
 ip access-group 100 in
 ip nat outside
 encapsulation frame-relay
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 7 045802150C2E
 ip ospf network point-to-point
 ip ospf hello-interval 65
 ip ospf priority 0
 frame-relay map ip 150.100.32.3 202 broadcast
 frame-relay interface-dlci 202
 crypto map ted
!
router ospf 123
 router-id 2.2.2.2
 log-adjacency-changes
 area 0 authentication message-digest
 area 2 nssa
 redistribute static subnets
 network 2.2.2.2 0.0.0.0 area 0
 network 12.12.12.0 0.0.0.255 area 0
 network 150.100.32.0 0.0.0.31 area 0
!
router bgp 2
bgp log-neighbor-changes
 bgp confederation identifier 1234
 bgp confederation peers 1 3
 network 2.2.2.22 mask 255.255.255.255
 neighbor 150.100.32.3 remote-as 3
 neighbor 150.100.32.3 description R3
!
ip nat inside source static network 121.121.121.121
172.19.1.1 /32 no-alias
ip classless
ip route 172.19.1.1 255.255.255.255 Null0
ip http server
```

```
!
access-list 100 permit tcp any any eq bgp
access-list 100 permit ip any 224.0.0.0 0.255.255.255
access-list 100 permit icmp any any echo
access-list 100 permit icmp any any echo-reply
access-list 100 permit ospf any any
access-list 100 permit tcp any any eq www
access-list 100 permit esp any any log
access-list 100 permit udp any any eq isakmp log
access-list 111 permit ip 12.12.12.0 0.0.0.255 11.11.11.0
0.0.0.255 log
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
line vty 0 4
 logging synchronous
 login
!
end
```

```
R2#ping
Protocol [ip]:
Target IP address: 11.11.11.11
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 12.12.12.12
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2
seconds:
Packet sent with a source address of 12.12.12.12

01:40:02: IPSEC(tunnel discover request): ,
  (key eng. msg.) INBOUND local= 12.12.12.12, remote=
11.11.11.11,
    local_proxy= 12.12.12.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 150.100.32.2/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004
dest=Serial0:150.100.32.3 .
01:40:02: %SEC-6-IPACCESSLOGP: list 100 permitted udp
150.100.31.1(500) -> 150.100.32.2(500), 1 packet
01:40:03: CryptoEngine0: delete connection 3
01:40:04: CryptoEngine0: generate alg parameter
01:40:05: CRYPTO_ENGINE: Dh phase 1 status: 0
```

```
01:40:05: CRYPTO_ENGINE: Dh phase 1 status: 0..
01:40:07: CryptoEngine0: generate alg parameter
01:40:09: CryptoEngine0: create ISAKMP SKEYID for conn id 4
01:40:09: CryptoEngine0: generate hmac context for conn id
4.
01:40:09: CryptoEngine0: generate hmac context for conn id 4
01:40:09: CryptoEngine0: clear dh number for conn id 1
01:40:09: IPSEC(key_engine): got a queue event...
01:40:09: IPSEC(spi_response): getting spi 523853408 for SA
        from 150.100.32.2    to 150.100.31.1    for prot 3
01:40:09: CryptoEngine0: generate hmac context for conn id 4
01:40:10: CryptoEngine0: generate hmac context for conn id 4
01:40:10: validate proposal 0
01:40:10: IPSEC(validate_proposal_request): proposal part
#1,
  (key eng. msg.) INBOUND local= 150.100.32.2, remote=
150.100.31.1,
    local_proxy= 12.12.12.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 11.11.11.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
01:40:10: validate proposal request 0
01:40:10: CryptoEngine0: generate hmac context for conn id 4
01:40:10: ipsec allocate flow 0
01:40:10: ipsec allocate flow 0
01:40:10: IPSEC(key_engine): got a queue event...
01:40:10: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 150.100.32.2, remote=
150.100.31.1,
    local_proxy= 12.12.12.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 11.11.11.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x1F395E60(523853408), conn_id= 2000, keysize= 0,
flags= 0x4
01:40:10: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 150.100.32.2, remote=
150.100.31.1,
    local_proxy= 12.12.12.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 11.11.11.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x952FF04C(2502946892), conn_id= 2001, keysize= 0,
flags= 0xC
01:40:10: IPSEC(create_sa): sa created,
  (sa) sa_dest= 150.100.32.2, sa_prot= 50,
    sa_spi= 0x1F395E60(523853408),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
a): sa created,(create_s.
  (sa) sa_dest= 150.100.31.1, sa_prot= 50,
    sa_spi= 0x952FF04C(2502946892),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
                                                      Success
rate is 0 percent (0/5)
R2#
01:40:16: %SEC-6-IPACCESSLOGDP: list 111 permitted icmp
12.12.12.12 -> 11.11.11.11 (8/0), 10 packets
```

```
R2#
```

```
R2#ping
Protocol [ip]:
Target IP address: 11.11.11.11
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 12.12.12.12
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2
seconds:
Packet sent with a source address of 12.12.12.12
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
184/187/192 ms
R2#
01:41:10: %SEC-6-IPACCESSLOGNP: list 100 permitted 50
150.100.31.1 -> 150.100.32.2, 1 packet
```

```
R2#sho crypto isakmp sa
dst             src             state          conn-id
slot
150.100.31.1    150.100.32.2    QM_IDLE              4
0
```

```
R2#sho crypto ipsec sa

interface: Serial0
    Crypto map tag: ted, local addr. 150.100.32.2

   local  ident (addr/mask/prot/port):
(12.12.12.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
(11.11.11.0/255.255.255.0/0/0)
   current_peer: 150.100.31.1
     PERMIT, flags={}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 150.100.32.2, remote crypto
endpt.: 150.100.31.1
     path mtu 1500, media mtu 1500
     current outbound spi: 952FF04C
```

```
     inbound esp sas:
      spi: 0x1F395E60(523853408)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: ted
        sa timing: remaining key lifetime (k/sec):
(4607999/3446)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x952FF04C(2502946892)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: ted
        sa timing: remaining key lifetime (k/sec):
(4607999/3446)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

Step 3 – Step 6

```
hostname R3
!
logging queue-limit 100
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
no ip domain-lookup
!
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 2000
crypto isakmp key ccie address 4.4.4.4
crypto isakmp key ccie address 6.6.6.6
crypto isakmp key ccie address 8.8.8.8
!
!
crypto ipsec transform-set trvpn esp-des esp-sha-hmac
 mode transport
!
crypto map vpn local-address loopback 3
!
crypto map vpn 10 ipsec-isakmp
 set peer 4.4.4.4
 set transform-set trvpn
```

```
 match address 111
crypto map vpn 20 ipsec-isakmp
 set peer 6.6.6.6
 set transform-set trvpn
 match address 112
crypto map vpn 30 ipsec-isakmp
 set peer 8.8.8.8
 set transform-set trvpn
 match address 113
!
!
!
!
interface Loopback3
 description OSPF Loopback
 ip address 3.3.3.3 255.255.255.255
!
interface Loopback10
 ip address 3.3.3.13 255.255.255.255
!
interface Loopback11
 ip address 3.3.3.23 255.255.255.255
!
interface Loopback13
 description Loopback for VPN full mesh
 ip address 13.13.13.13 255.255.255.0
!
interface Loopback33
 description BGP Loopback
 ip address 3.3.3.33 255.255.255.255
!
interface Tunnel4
 description Basic GRE Crypto to R4
 ip address 192.168.34.1 255.255.255.0
 tunnel source 3.3.3.3
 tunnel destination 4.4.4.4
 crypto map vpn
!
interface Tunnel6
 description Basic GRE Crypto to R6
 ip address 192.168.36.1 255.255.255.0
 tunnel source 3.3.3.3
 tunnel destination 6.6.6.6
 crypto map vpn
!
interface Tunnel8
 description Basic GRE Crypto to R8
 ip address 192.168.38.1 255.255.255.0
 tunnel source 3.3.3.3
 tunnel destination 8.8.8.8
 crypto map vpn
!
interface Ethernet0
 ip address 130.100.1.3 255.255.255.0
!
interface Serial0
 no ip address
 encapsulation frame-relay
```

```
 no fair-queue
 clockrate 64000
 frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
 ip address 150.100.31.3 255.255.255.240
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 cisco
 ip ospf hello-interval 65
 ip ospf priority 0
 traffic-shape rate 64000 8000 8000 1000
 traffic-shape adaptive 32000
 frame-relay interface-dlci 301
!
interface Serial0.2 point-to-point
 ip address 150.100.32.3 255.255.255.224
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 cisco
 ip ospf hello-interval 65
 ip ospf priority 0
 frame-relay interface-dlci 302
 crypto map vpn
!
interface Serial0.3 point-to-point
 ip address 150.100.33.3 255.255.255.248
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 cisco
 ip ospf hello-interval 65
 ip ospf priority 0
 frame-relay interface-dlci 304
 crypto map vpn
!
!
router eigrp 100
 network 13.0.0.0
 network 192.168.34.0
 network 192.168.36.0
 network 192.168.38.0
 maximum-paths 1
 no auto-summary
!
router ospf 123
 router-id 3.3.3.3
 log-adjacency-changes
 area 0 authentication message-digest
 redistribute connected subnets route-map redist
 network 3.3.3.3 0.0.0.0 area 0
 network 150.100.31.0 0.0.0.15 area 0
 network 150.100.32.0 0.0.0.31 area 0
 network 150.100.33.0 0.0.0.7 area 0
!
router rip
 version 1
 redistribute ospf 123 metric 1
 network 130.100.0.0
!
router bgp 3
 no synchronization
```

```
 bgp router-id 3.3.3.3
bgp log-neighbor-changes
 bgp confederation identifier 1234
 bgp confederation peers 1 2
 network 3.3.3.33 mask 255.255.255.255
 neighbor 10.1.1.9 remote-as 9
 neighbor 10.1.1.9 ebgp-multihop 2
 neighbor 10.1.1.9 next-hop-self
 neighbor 150.100.31.1 remote-as 1
 neighbor 150.100.31.1 next-hop-self
 neighbor 150.100.32.2 remote-as 2
 neighbor 150.100.32.2 next-hop-self
 neighbor 150.100.33.4 remote-as 456
 neighbor 150.100.33.4 next-hop-self
 no auto-summary
!
ip classless
ip route 10.1.1.0 255.255.255.0 130.100.1.1
ip http server
!
access-list 1 permit 3.3.3.13
access-list 1 permit 3.3.3.23
access-list 1 permit 130.100.1.0 log
access-list 100 permit tcp any any eq bgp
access-list 100 permit ospf any any
access-list 100 permit tcp any host 130.100.1.13 eq www
access-list 100 permit ip any 224.0.0.0 0.255.255.255
access-list 100 permit tcp 192.168.1.0 0.0.0.255 host
130.100.1.13 eq 443
access-list 100 permit tcp 192.168.1.0 0.0.0.255 host
130.100.1.13 eq ftp
access-list 100 permit tcp 192.168.1.0 0.0.0.255 host
130.100.1.13 eq ftp-data
access-list 100 permit icmp any any echo-reply log
access-list 100 permit icmp any any echo log
access-list 111 permit ip 13.13.13.0 0.0.0.255 14.14.14.0
0.0.0.255
access-list 112 permit ip 13.13.13.0 0.0.0.255 16.16.16.0
0.0.0.255
access-list 113 permit ip 13.13.13.0 0.0.0.255 18.18.18.0
0.0.0.255
route-map redist permit 10
 match ip address 1
!
tftp-server flash:c2500-ik8os-l.122-16.bin
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
line vty 0 4
 logging synchronous
 login
!
end
```

```
R3#sho crypto map
```

```
Crypto Map "vpn" 10 ipsec-isakmp
        Peer = 4.4.4.4
        Extended IP access list 111
            access-list 111 permit ip 13.13.13.0 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" 20 ipsec-isakmp
        Peer = 6.6.6.6
        Extended IP access list 112
            access-list 112 permit ip 13.13.13.0 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" 30 ipsec-isakmp
        Peer = 8.8.8.8
        Extended IP access list 113
            access-list 113 permit ip 13.13.13.0 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, }
        Interfaces using crypto map vpn:
                Serial0.2
                Serial0.3
                Tunnel4
                Tunnel6
                Tunnel8
```

```
R3# sho ip route eigrp
D    192.168.46.0/24 [90/310044416] via 192.168.34.2,
01:45:45, Tunnel4
     16.0.0.0/24 is subnetted, 1 subnets
D       16.16.16.16 [90/297372416] via 192.168.36.2,
01:45:45, Tunnel6
     18.0.0.0/24 is subnetted, 1 subnets
D       18.18.18.18 [90/297372416] via 192.168.38.2,
01:45:43, Tunnel8
D    192.168.68.0/24 [90/310044416] via 192.168.36.2,
01:45:46, Tunnel6
     14.0.0.0/24 is subnetted, 1 subnets
D       14.14.14.14 [90/297372416] via 192.168.34.2,
01:45:45, Tunnel4
D    192.168.48.0/24 [90/310044416] via 192.168.34.2,
01:45:46, Tunnel4
```

```
R3#ping
```

```
Protocol [ip]:
Target IP address: 14.14.14.14
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 13.13.13.13
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.14.14.14, timeout is 2
seconds:
Packet sent with a source address of 13.13.13.13
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
128/128/128 ms
```

```
R3#ping
Protocol [ip]:
Target IP address: 16.16.16.16
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 13.13.13.13
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 16.16.16.16, timeout is 2
seconds:
Packet sent with a source address of 13.13.13.13
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
164/165/168 ms
```

```
R3#ping
Protocol [ip]:
Target IP address: 18.18.18.1
*Mar  1 03:41:25.783: %SEC-6-IPACCESSLOGDP: list 111
permitted icmp 13.13.13.13 -> 16.16.16.16 (8/0), 5 packets
18.18.18.18
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 13.13.13.13
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
```

```
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 18.18.18.18, timeout is 2
seconds:
Packet sent with a source address of 13.13.13.13
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
168/169/172 ms
```

```
R3#sho crypto isa sa
dst             src             state          conn-id
slot
8.8.8.8         3.3.3.3         QM_IDLE              3
0
6.6.6.6         3.3.3.3         QM_IDLE              2
0
4.4.4.4         3.3.3.3         QM_IDLE            1       0
```

```
hostname R4
!
logging queue-limit 100
!
ip subnet-zero
no ip domain-lookup
!
!
key chain ccie
 key 6727
  key-string 7 03520C5951
!
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 6.6.6.6
crypto isakmp key ccie address 8.8.8.8
!
!
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 6.6.6.6
 set transform-set trvpn
 match address 112
crypto map vpn 30 ipsec-isakmp
 set peer 8.8.8.8
 set transform-set trvpn
```

```
 match address 113
!
!
!
!
interface Loopback4
 description OSPF Loopback
 ip address 4.4.4.4 255.255.255.255
!
interface Loopback14
 description Loopback for VPN full mesh
 ip address 14.14.14.14 255.255.255.0
!
interface Loopback44
 description BGP Loopback
 ip address 4.4.4.44 255.255.255.255
!
interface Tunnel3
 description Basic GRE Crypto to R3
 ip address 192.168.34.2 255.255.255.0
 tunnel source 4.4.4.4
 tunnel destination 3.3.3.3
 crypto map vpn
!
interface Tunnel6
 description Basic GRE Crypto to R6
 ip address 192.168.46.1 255.255.255.0
 tunnel source 4.4.4.4
 tunnel destination 6.6.6.6
 crypto map vpn
!
interface Tunnel8
 description Basic GRE Crypto to R8
 ip address 192.168.48.1 255.255.255.0
 tunnel source 4.4.4.4
 tunnel destination 8.8.8.8
 crypto map vpn
!
interface Ethernet0
 ip address 140.100.47.4 255.255.255.192
 ip rip send version 2
 ip rip receive version 2
 ip rip authentication mode md5
 ip rip authentication key-chain ccie
 crypto map vpn
!
interface Serial0
 ip address 150.100.33.4 255.255.255.248
 ip rip send version 2
 ip rip receive version 2
 encapsulation frame-relay
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 7 104D000A0618
 ip ospf network point-to-point
 ip ospf hello-interval 65
 ip ospf priority 0
 frame-relay map ip 150.100.33.3 404 broadcast
 frame-relay interface-dlci 404
```

```
 frame-relay lmi-type ansi
 crypto map vpn
!
interface Serial1
 ip address 140.100.45.4 255.255.255.192
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 7 1511021F0725
 ip ospf network point-to-point
 clockrate 2000000
 crypto map vpn
!
router eigrp 100
 network 14.0.0.0
 network 192.168.24.0
 network 192.168.34.0
 network 192.168.46.0
 network 192.168.48.0
 maximum-paths 1
 no auto-summary
!
router ospf 123
 router-id 4.4.4.4
 log-adjacency-changes detail
 area 0 authentication message-digest
 area 45 authentication message-digest
 area 45 virtual-link 5.5.5.5 authentication message-digest
 area 45 virtual-link 5.5.5.5 message-digest-key 5 md5 7
0822455D0A16
 redistribute rip subnets route-map red_rip_ospf
 network 4.4.4.4 0.0.0.0 area 0
 network 140.100.45.0 0.0.0.63 area 45
 network 150.100.33.0 0.0.0.7 area 0
!
router rip
 version 2
 redistribute ospf 123 metric 1
 network 4.0.0.0
 network 140.100.0.0
 default-information originate
 no auto-summary
!
router bgp 456
 no synchronization
 bgp router-id 4.4.4.4
 bgp cluster-id 67372076
 bgp log-neighbor-changes
 network 4.4.4.44 mask 255.255.255.255
 network 140.100.47.0 mask 255.255.255.192
 aggregate-address 209.112.0.0 255.255.0.0 summary-only
 neighbor 140.100.45.5 remote-as 456
 neighbor 140.100.45.5 next-hop-self
 neighbor 140.100.47.7 remote-as 1560
 neighbor 140.100.47.7 description R7_BB2
 neighbor 140.100.47.7 password 7 1511021F0725
 neighbor 140.100.47.7 remove-private-AS
 neighbor 150.100.33.3 remote-as 1234
 no auto-summary
!
```

```
ip default-gateway 150.100.3.3
ip classless
ip http server
!
access-list 44 permit 67.67.67.0 log
access-list 44 permit 140.100.9.0 log
access-list 111 permit ip 14.14.14.0 0.0.0.255 13.13.13.0
0.0.0.255
access-list 112 permit ip 14.14.14.0 0.0.0.255 16.16.16.0
0.0.0.255
access-list 113 permit ip 14.14.14.0 0.0.0.255 18.18.18.0
0.0.0.255
route-map red_rip_ospf permit 10
 match ip address 44
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 privilege level 15
 logging synchronous
 no login
!
end
```

```
R4#sho ip route eigrp
     16.0.0.0/24 is subnetted, 1 subnets
D       16.16.16.16 [90/297372416] via 192.168.46.2,
01:51:53, Tunnel6
     18.0.0.0/24 is subnetted, 1 subnets
D       18.18.18.18 [90/297372416] via 192.168.48.2,
01:51:51, Tunnel8
D    192.168.38.0/24 [90/310044416] via 192.168.34.1,
01:51:53, Tunnel3
D    192.168.36.0/24 [90/310044416] via 192.168.46.2,
01:51:53, Tunnel6
D    192.168.68.0/24 [90/310044416] via 192.168.46.2,
01:51:53, Tunnel6
     13.0.0.0/24 is subnetted, 1 subnets
D       13.13.13.13 [90/297372416] via 192.168.34.1,
01:51:53, Tunnel3
```

```
R4#sho crypto map
Crypto Map "vpn" 10 ipsec-isakmp
        Peer = 3.3.3.3
        Extended IP access list 111
            access-list 111 permit ip 14.14.14.0 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 = 6.6.6.6
        Extended IP access list 112
            access-list 112 permit ip 14.14.14.0 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" 30 ipsec-isakmp
        Peer = 8.8.8.8
        Extended IP access list 113
            access-list 113 permit ip 14.14.14.0 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, }
        Interfaces using crypto map vpn:
                Ethernet0
                Serial0
                Serial1
                Tunnel3
                Tunnel6
                Tunnel8
```

```
R4#ping
Protocol [ip]:
Target IP address: 13.13.13.13
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 14.14.14.14
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 13.13.13.13, timeout is 2
seconds:
Packet sent with a source address of 14.14.14.14
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
128/136/168 ms
```

```
R4#ping
Protocol [ip]:
Target IP address: 16.16.16.16
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
```

```
Extended commands [n]: y
Source address or interface: 14.14.14.14
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 16.16.16.16, timeout is 2
seconds:
Packet sent with a source address of 14.14.14.14
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
72/72/76 ms
```

```
R4#ping
Protocol [ip]:
Target IP address: 18.18.18.18
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 14.14.14.14
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 18.18.18.18, timeout is 2
seconds:
Packet sent with a source address of 14.14.14.14
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
72/76/80 ms
r4#
```

```
R4#sho crypto isakmp sa
dst             src             state          conn-id
slot
8.8.8.8         4.4.4.4         QM_IDLE              1
0
3.3.3.3         4.4.4.4         QM_IDLE              2
0
6.6.6.6         4.4.4.4         QM_IDLE              4
0
```

```
hostname R6
!
logging queue-limit 100
aaa new-model
aaa authentication login default group tacacs+
aaa authentication login no_login enable local line none
aaa authentication enable default group tacacs+
aaa authentication ppp default local
```

```
aaa authorization config-commands
aaa authorization exec default group tacacs+ if-
authenticated
aaa authorization commands 3 default group tacacs+
aaa authorization network default local
aaa authorization auth-proxy default group tacacs+
aaa authorization configuration default group tacacs+
aaa accounting send stop-record authentication failure
aaa accounting delay-start
aaa accounting nested
aaa accounting update newinfo periodic 5
aaa accounting auth-proxy default start-stop group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa accounting resource default start-stop group tacacs+!
username R8 password 0 cisco
ip subnet-zero
!
!
no ip domain-lookup
!

!
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 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
 standby 1 ip 130.100.26.1
 standby 1 preempt
 standby 1 authentication ccie
 standby 1 track Serial0/0
 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
 no ip redirects
 no ip proxy-arp
 ip nat outside
 no ip route-cache same-interface
 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
!
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 cluster-id 2355385857
 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
!
ip nat inside source list 1 interface Serial0/0 overload
ip nat inside source static tcp 130.100.26.10 80
140.100.56.6 80 extendable no-alias
```

```
ip nat inside source static tcp 130.100.26.12 21
140.100.56.6 21 extendable no-alias
ip nat inside source static tcp 130.100.26.12 20
140.100.56.6 20 extendable no-alias
ip nat inside source static tcp 130.100.26.6 23 140.100.56.6
23 extendable no-alias
ip classless
ip route 192.168.1.0 255.255.255.0 130.100.26.2
ip route 192.168.1.1 255.255.255.255 130.100.26.2
ip http server
!
!
ip access-list standard no_ospf_route
 deny   130.100.26.0 0.0.0.255
 permit any
!
ip access-list extended ccie
 permit icmp any any
 permit udp any any eq isakmp
 permit esp any any
 permit eigrp any any
 permit ospf any any
 permit tcp any any eq bgp
 permit tcp any eq bgp any
 permit gre any any
 permit tcp any any established
 permit tcp any any eq bgp log
 permit eigrp any any log
 permit esp any any log
 permit tcp any any eq telnet

 deny   ip any any
 permit tcp any any eq www log
 deny   tcp any host 130.100.26.6 established
 permit tcp any host 10.0.0.1
 permit tcp any host 130.100.26.6
ip access-list extended time_acl
 deny   tcp any any eq www log time-range weekdays
 permit udp any any time-range weekends
 permit gre any any log
 permit ospf any any log
 permit icmp any any log
 permit tcp any any eq bgp log
 permit tcp any any eq telnet log
 permit esp any any log
 permit ahp any any log
 permit ip any any log
logging 130.100.26.8
access-list 1 permit 130.100.26.0 0.0.0.255 log
access-list 2 permit 8.8.8.88
access-list 3 deny   130.100.26.0 0.0.0.255 log
access-list 3 permit any log
access-list 11 permit 130.100.26.0 log
access-list 12 permit any log
access-list 67 permit 150.100.32.2
access-list 67 permit 150.100.31.1
access-list 111 permit ip 16.16.16.0 0.0.0.255 13.13.13.0
0.0.0.255 log
```

```
access-list 112 permit ip 16.16.16.0 0.0.0.255 18.18.18.0
0.0.0.255 log
access-list 113 permit ip 16.16.16.0 0.0.0.255 14.14.14.0
0.0.0.255 log
access-list 120 permit icmp any any
access-list 121 permit tcp any any eq 443
dialer-list 1 protocol ip permit
dialer-list 5 protocol ip permit
no cdp run
route-map net_130 permit 10
 match ip address 11
!
route-map redist deny 10
!
route-map red permit 10
 match ip address 1
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 access-class 67 in
 privilege level 15
 autocommand  telnet 5.5.5.5
!
time-range weekdays
 periodic weekdays 8:00 to 18:00
!
time-range weekends
 periodic weekend 18:00 to 20:00
!
end
```

```
R6#sho ip route eigrp
     18.0.0.0/24 is subnetted, 1 subnets
D       18.18.18.18 [90/297372416] via 192.168.68.2,
01:58:27, Tunnel8
D    192.168.38.0/24 [90/310044416] via 192.168.36.1,
01:58:27, Tunnel3
D    192.168.34.0/24 [90/310044416] via 192.168.46.1,
01:58:26, Tunnel4
     13.0.0.0/24 is subnetted, 1 subnets
D       13.13.13.13 [90/297372416] via 192.168.36.1,
01:58:26, Tunnel3
     14.0.0.0/24 is subnetted, 1 subnets
D       14.14.14.14 [90/297372416] via 192.168.46.1,
01:58:26, Tunnel4
D    192.168.48.0/24 [90/310044416] via 192.168.46.1,
01:58:27, Tunnel4
```

```
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
                Tunnel0
                Tunnel3
                Tunnel4
                Tunnel8
```

```
R6#ping
Protocol [ip]:
Target IP address: 13.13.13.13
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 16.16.16.16
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 13.13.13.13, timeout is 2
seconds:
Packet sent with a source address of 16.16.16.16
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
164/168/172 ms
```

```
R6#ping
Protocol [ip]:
Target IP address: 14.14.14.14
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 16.16.16.16
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.14.14.14, timeout is 2
seconds:
Packet sent with a source address of 16.16.16.16
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
72/74/80 ms
```

```
R6#ping
Protocol [ip]:
Target IP address: 18.18.18.18
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 16.16.16.16
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 18.18.18.18, timeout is 2
seconds:
Packet sent with a source address of 16.16.16.16

Mar 11 15:50:41.508: %SEC-6-IPACCESSLOGDP: list 111
permitted icmp 16.16.16.16 -> 18.18.18.18 (8/0), 1
packet.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
12/13/16 ms
```

```
R6#sho crypto isakmp sa
dst             src             state          conn-id
slot
```

```
6.6.6.6         3.3.3.3         QM_IDLE                 2
0
6.6.6.6         8.8.8.8         QM_IDLE                 1
0
6.6.6.6         4.4.4.4         QM_IDLE                 3
0
```

```
hostname R8
!
logging queue-limit 100
enable password 7 05080F1C2243
!
username cisco privilege 15 password 7 02050D480809
clock timezone PST -8
clock summer-time PDT recurring
aaa new-model
!
!
aaa authentication login default local
aaa authentication ppp default group tacacs+
aaa authorization network default group tacacs+
aaa accounting nested
aaa accounting network default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
ip subnet-zero
!
!
ip ftp source-interface FastEthernet0/0
ip ftp username admin
ip ftp password 7 060506324F41
ip domain name cisco.com
ip name-server 24.160.227.25
!
ip inspect audit-trail
ip inspect max-incomplete low 300
ip inspect max-incomplete high 950
ip inspect dns-timeout 50
ip inspect tcp idle-time 130
ip inspect tcp max-incomplete host 132 block-time 15
ip inspect name r8_cbac tcp
ip inspect name r8_cbac http java-list 2 alert on audit-
trail on
ip audit notify log
ip audit po max-events 100
!
!
!
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 4.4.4.4
crypto isakmp key ccie address 6.6.6.6
!
!
```

```
crypto ipsec transform-set trvpn esp-des esp-sha-hmac
 mode transport
!
crypto map vpn 10 ipsec-isakmp
 set peer 6.6.6.6
 set transform-set trvpn
 match address 111
crypto map vpn 20 ipsec-isakmp
 set peer 4.4.4.4
 set transform-set trvpn
 match address 112
crypto map vpn 30 ipsec-isakmp
 set peer 3.3.3.3
 set transform-set trvpn
 match address 113
!
isdn switch-type basic-ni
!
!
key chain ccie
 key 1
  key-string 7 0307580203
!
!
interface Loopback8
 description OSPF Loopback
 ip address 8.8.8.8 255.255.255.255
 ip broadcast-address 8.8.8.8
!
interface Loopback18
 description Loopback for VPN full mesh
 ip address 18.18.18.18 255.255.255.255
!
interface Loopback88
 description BGP Loopback
 ip address 8.8.8.88 255.255.255.255
!
!
interface Tunnel1
 description GRE Tunnel to R6
 ip address 192.168.2.1 255.255.255.0
 ip broadcast-address 192.168.2.255
 ip ospf authentication message-digest
 ip ospf message-digest-key 5 md5 7 045802150C2E
 tunnel source 192.168.1.1
 tunnel destination 130.100.26.6
 crypto map vpn
!
interface Tunnel3
 description Basic GRE Crypto to R3
 ip address 192.168.38.2 255.255.255.0
 tunnel source 8.8.8.8
 tunnel destination 3.3.3.3
 crypto map vpn
!
interface Tunnel4
 description Basic GRE Crypto to R4
 ip address 192.168.48.2 255.255.255.0
```

```
 tunnel source 8.8.8.8
 tunnel destination 4.4.4.4
 crypto map vpn
!
interface Tunnel6
 description Basic GRE Crypto to R6
 ip address 192.168.68.2 255.255.255.0
 tunnel source 8.8.8.8
 tunnel destination 6.6.6.6
 crypto map vpn
!
interface FastEthernet0/0
 description NAT to Internet
 ip address dhcp
 ip nat outside
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
 ntp disable
 no cdp enable
!
interface BRI0/0
 no ip address
 encapsulation ppp
 ip ospf cost 100
 dialer rotary-group 10
 dialer-group 1
 isdn switch-type basic-ni
 isdn spid1 8881 8888
 isdn spid2 8882 8888
 no cdp enable
 ppp authentication chap
!
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
 no cdp enable
!
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
```

```
!
router eigrp 100
 network 18.0.0.0
 network 192.168.38.0
 network 192.168.48.0
 network 192.168.68.0
 maximum-paths 1
 no auto-summary
!
router ospf 123
 router-id 8.8.8.8
 log-adjacency-changes detail
 area 86 authentication message-digest
 network 8.8.8.8 0.0.0.0 area 86
 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 10 in
!
router rip
 version 1
 network 192.168.1.0
 network 199.199.199.0
 no auto-summary
!
router bgp 65000
 no synchronization
 bgp router-id 8.8.8.8
 bgp log-neighbor-changes
 network 8.8.8.88 mask 255.255.255.255
 redistribute connected route-map loop
 neighbor 6.6.6.6 remote-as 456
 neighbor 6.6.6.6 ebgp-multihop 2
 neighbor 6.6.6.6 update-source Loopback8
 no auto-summary
!
ip local pool Internet 192.168.1.10 192.168.1.20
ip local pool test 172.16.1.10 172.16.1.100
ip local pool default 10.10.10.1 10.10.10.10
ip drp access-group 3
ip drp authentication key-chain ccie
ip drp server
no ip http server
ip http authentication local
no ip http secure-server
ip classless
ip route 5.5.5.0 255.255.255.0 192.168.1.222
ip route 5.5.5.5 255.255.255.255 192.168.1.222
ip route 6.6.6.0 255.255.255.0 192.168.1.222
ip route 10.1.1.0 255.255.255.0 10.1.1.1
ip route 10.1.1.0 255.255.255.0 192.168.1.222
ip route 130.100.26.0 255.255.255.0 192.168.1.222
ip route 140.100.0.0 255.255.0.0 192.168.1.222
ip route 140.100.56.0 255.255.255.0 192.168.1.222
ip tacacs source-interface Loopback8
!
!
!
```

```
ip access-list extended idletime
ip access-list extended inacl
ip access-list extended key-exchange
ip access-list extended protocol
ip access-list extended service
ip access-list extended timeout
!
access-list 1 permit 192.168.1.0 0.0.0.255 log
access-list 1 deny   172.16.1.0 0.0.0.255 log
access-list 2 permit 8.8.8.88
access-list 3 permit 6.6.6.6
access-list 3 permit 192.168.2.1
access-list 5 permit 192.168.1.8 log
access-list 10 deny   0.0.0.0 log
access-list 10 permit any log
access-list 11 permit 192.168.0.0 log
access-list 111 permit ip 18.18.18.0 0.0.0.255 16.16.16.0
0.0.0.255 log
access-list 112 permit ip 18.18.18.0 0.0.0.255 14.14.14.0
0.0.0.255 log
access-list 113 permit ip 18.18.18.0 0.0.0.255 13.13.13.0
0.0.0.255 log
access-list 150 permit gre any any
access-list 150 permit ospf any any
access-list 150 permit tcp any any eq telnet
access-list 150 permit tcp any any eq bgp
access-list 150 permit icmp any any echo-reply
access-list 150 permit icmp any any time-exceeded
access-list 150 permit icmp any any packet-too-big
access-list 150 permit icmp any any traceroute
access-list 150 permit icmp any any unreachable
access-list 150 deny   tcp any any
access-list 150 deny   udp any any
access-list 151 permit tcp host 8.8.8.8 any eq www
dialer-list 1 protocol ip permit
no cdp run
!
route-map loop permit 10
 match ip address 2
!
route-map Loopback permit 10
 match ip address 10
!
tacacs-server host 192.168.1.7
tacacs-server directed-request
tacacs-server key cisco6727
snmp-server manager
radius-server authorization permit missing Service-Type
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
```

```
alias exec sr sho ip route
alias exec DB show ip route
privilege configure level 7 snmp-server
privilege exec level 1 telnet
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
privilege exec level 1 show ip route
privilege exec level 1 show ip
privilege exec level 1 show startup-config
privilege exec level 1 show
!
line con 0
 exec-timeout 0 0
 privilege level 15
 speed 115200
 flowcontrol hardware
line aux 0
 modem InOut
 transport input all
line vty 0 4
transport input telnet ssh
line vty 5 15
 privilege level 15
!
!
end
```

```
R8#sho ip route eigrp
D    192.168.46.0/24 [90/310044416] via 192.168.48.1,
03:01:48, Tunnel4
     16.0.0.0/24 is subnetted, 1 subnets
D       16.16.16.16 [90/297372416] via 192.168.68.1,
03:01:48, Tunnel6
D    192.168.36.0/24 [90/310044416] via 192.168.38.1,
03:01:48, Tunnel3
D    192.168.34.0/24 [90/310044416] via 192.168.38.1,
03:01:48, Tunnel3
     13.0.0.0/24 is subnetted, 1 subnets
D       13.13.13.13 [90/297372416] via 192.168.38.1,
03:01:48, Tunnel3
     14.0.0.0/24 is subnetted, 1 subnets
D       14.14.14.14 [90/297372416] via 192.168.48.1,
03:01:48, Tunnel4
```

```
R8#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
```

```
R8#ping
Protocol [ip]:
Target IP address: 13.13.13.13
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 18.18.18.18
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 13.13.13.13, timeout is 2
seconds:
Packet sent with a source address of 18.18.18.18
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
168/168/172 ms
```

```
R8#ping
```

```
Protocol [ip]:
Target IP address: 14.14.14.14
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 18.18.18.18
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.14.14.14, timeout is 2
seconds:
Packet sent with a source address of 18.18.18.18
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
76/100/192 ms
```

```
R8#ping
Protocol [ip]:
Target IP address: 16.16.16.16
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 18.18.18.18
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 16.16.16.16, timeout is 2
seconds:
Packet sent with a source address of 18.18.18.18
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
12/14/16 ms
```

```
R8#sho crypto isakmp sa
dst             src             state          conn-id
slot
3.3.3.3         8.8.8.8         QM_IDLE              2
0
4.4.4.4         8.8.8.8         QM_IDLE              4
0
6.6.6.6         8.8.8.8         QM_IDLE              3
0
```