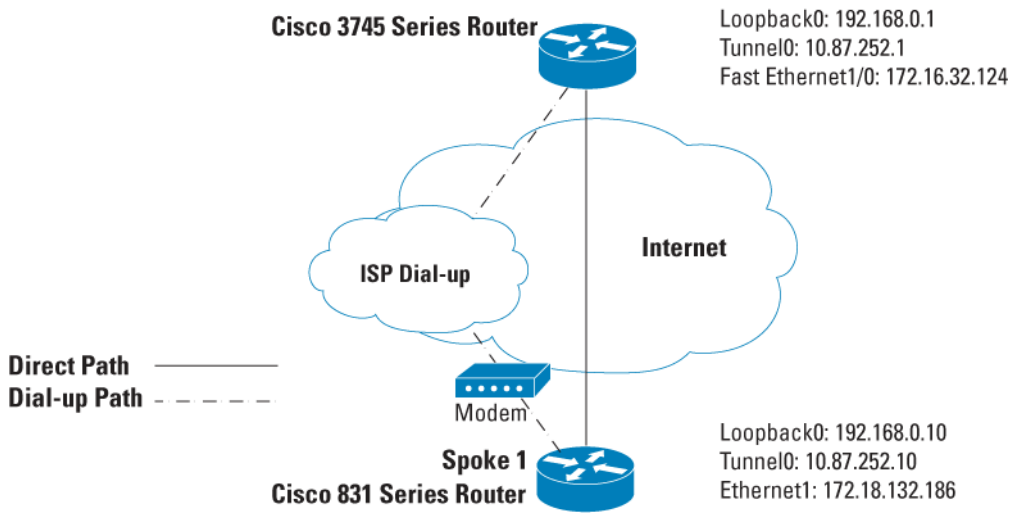
WHITE PAPER

CONFIGURING DIAL BACKUP WITH DYNAMIC MULTIPOINT VPN USING RELIABLE STATIC ROUTING

OVERVIEW

This document provides a sample configuration for configuring Dial backup on a Dynamic Multipoint spoke router in a Dynamic Multipoint VPN (DMVPN) Hub-and-spoke network. The DMVPN solution is used to build large Cisco IOS® IP Security (IPsec) VPNs. DMVPN combines generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP). Dial backup enables the spoke router to try alternative path to reach the hub router, when the direct primary path to the hub router fails. This configuration relies on Dial back up, Reliable Static Routing Backup Using Object Tracking, and Policy Based Routing. This sample configuration shows how to enable the failover over a dial-up modem, when the primary path to the hub router fails and how to recover from the backup path, when the primary path is recovered.

Figure 1. Network Diagram



DMVPN BENEFITS

Simplification of IPsec VPN Configuration

Adding or removing a spoke does not require configuration changes on the hub router. The configuration on all the spokes is identical, except for the site specific addresses. The same configuration template can be used at all the spoke routers.

Support for Dynamically Addressed Spoke Routers

To configure the hub router using point-to-point GRE and IPsec hub-and-spoke VPN networks, the physical interface IP address of the spoke routers must be known, because IP address must be configured as the GRE tunnel destination address. This feature allows spoke routers to have dynamic physical interface IP addresses (common for cable and DSL connections). When the spoke router comes online it sends registration packets to the hub router. Current physical interface IP address of this spoke is located within these registration packets.

Support for Enterprise Class Remote Sites

Using DMVPN provides support for routing protocols to the remote sites. Using routing protocols to remote sites enables dynamic propagation of routing information and optimized route selection. Also, remote sites can utilize multicast traffic for supporting multimedia, video, and distant learning applications.

This network is using hub to spoke configuration topology. This configuration is using an alternate DMVPN configuration, which does not use the new tunnel protection configuration.

Prerequisites

The sample configuration is based on the following assumptions:

- Public IP address of the hub (this configuration is using 172.16.32.124)
- IP address of the IPsec tunnel on the hub (this configuration is using 192.168.0.1)
- IP address of the IPsec tunnel on the local spoke (this configuration is using 192.168.0.10)
- A static IP address on the wan interface of the spoke
- The Routing protocol to be used with the hub router (this configuration is using Open Shortest Path First (OSPF))
- An assigned pre-shared key that will be used on the hub and all the spokes
- Dial-up account to an Internet service provider (ISP) to provide an alternate path to the hub router

Limitations

- This guide describes the spoke router for hub and spoke DMVPN configurations only.
- Full security audit on the router configuration is not covered. It is recommended to run Security Audit in the wizard mode to lock down and secure the router.
- An initial router configuration step is not covered in the steps. The full configuration is shown in the next section.
- This network is using hub to spoke configuration topology. Traffic from a spoke to another spoke is required to pass via the hub first.
- This configuration is using the alternate DMVPN configuration, which uses a crypto map on the physical interface rather then the new tunnel protection configuration.

Prepare to Begin

Before beginning the configurations, make sure that:

- The spoke router can reach the DMVPN hub directly over the internet, and the DMVPN hub is configured and operational
- The spoke router can reach the DMVPN hub via the dial-up modem and the ISP

Components Used

The sample configuration uses the following Cisco IOS Software releases and Cisco hardware:

- Cisco IOS Software Release 12.3(8)T1 and Cisco 831 Series Router (Cisco 831-K9O3SY6-M Series Router)
- Cisco IOS Software Release 12.3(10) and Cisco 3700 Series Multiservice Access Router (Cisco 3745-IK9O3S-M Series Router)

Figure 1 illustrates the network for the sample configuration.

The information presented in this document was obtained from devices in a specific lab environment. All of the devices started with a cleared (default) configuration. In a live network, it is imperative to understand the potential impact of any command before implementing it.

The idea is to use Internet Control Message Protocol (ICMP) pings to track the reachability of the Hub via the Spokes primary interface. It is

assumed that the spoke router must use different source addresses for tunnel packets going out of the primary interface and for tunnel packets going out of the backup interface. Cisco uses a tunnel mode IPsec and loopback interface as the GRE tunnel source, this allows the local IPsec peer address to dynamically match the outbound (primary or backup) interface address. Only DMVPN hub and spoke networks will be supported.

This sample configuration also used the following software features:

- **DMVPN Configuration with Crypto Map**—This DMVPN configuration uses traditional "crypto map" command instead of the new "tunnel protection" command. This configuration method is required on both hub and spoke routers.
- **Reliable Static Routing Backup Using Object Tracking**—The Reliable Static Routing Backup Using Object Tracking feature introduces the ability for Cisco IOS Software to use Internet Control Message Protocol (ICMP) pings to identify when an IPsec VPN hub become unreachable and allows the initiation of a backup connection from any alternative path with a floating static path. For the complete documentation, check out the Reliable Static Routing Backup Using Object Tracking link in the related information section of this document.
- **Policy Based Routing**—The policy based routing is only required when the reliable static Routing is required to track the IP address of the DMVPN hub router. If tracking of different IP address, such as a secondary IP address on the DMVPN hub, is possible, then a host static route can be used instead of PBR.

  The Policy based routing is needed on the spoke router only. It is used to direct local ICMP packets, sent only from the spoke router to the hub router, to go through the WAN interface, even during the failover. These packets are sent by the Reliable Static Routing Backup Using Object Tracking feature to determine the reachability via the direct Internet path. Following are the configuration used for the Policy Based Routing:

```
interface Ethernet1
   ip address 172.18.132.186 255.255.255.248
!
ip local policy route-map MY_LOCAL_POLICY
!
ip route 172.16.32.124 255.255.255.255 172.18.132.185 track 123
!
access-list 101 permit icmp host 172.18.132.186 host 172.16.32.124
!
route-map MY_LOCAL_POLICY permit 10
   match ip address 101
   set interface Ethernet1
   set ip next-hop 217.181.132.185
```

Dial Backup

Dial backup enables the establishment of an alternative path using the auxiliary port of the spoke router. Cisco 831 Series Router with a virtual aux port configuration is used in this case. For complete information on virtual aux port, check the Virtual auxiliary port Feature documentation.

CONFIGURATION OF THE SPOKE ROUTER

Following are the configurations on the spoke router:

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

```
!
hostname c831-27
!
boot-start-marker
boot-end-marker
!
logging buffered 32000 debugging
enable password 7 02150056
!
aaa new-model
!
!
aaa authentication login default none
aaa authentication ppp default local
aaa session-id common
ip subnet-zero
!
!
ip dhcp excluded-address 10.80.1.1
!
ip dhcp pool TEST
   network 10.80.1.0 255.255.255.0
   default-router 10.80.1.1
!
!
ip host hub 172.16.32.124
ip cef
ip ips po max-events 100
no ftp-server write-enable
chat-script dial ABORT ERROR ABORT BUSY "" "ATDT\T" TIMEOUT 60 CONNECT
!
track 123 rtr 1 reachability
!
crypto isakmp policy 10
   hash md5
   authentication pre-share
crypto isakmp key 7578 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
crypto ipsec transform-set LAB-TRANSFORM esp-des esp-md5-hmac
!
crypto map LABMAP 10 ipsec-isakmp
   set peer 172.16.32.124
```

```
   set transform-set LAB-TRANSFORM
   match address 100
!
!
interface Tunnel0
   bandwidth 1000
   ip address 10.87.252.10 255.255.252.0
   no ip redirects
   ip mtu 1400
   ip nhrp authentication cisco
   ip nhrp map 10.87.252.1 192.168.0.1
   ip nhrp network-id 100000
   ip nhrp nhs 10.87.252.1
   ip tcp adjust-mss 1360
   delay 1000
   tunnel source Loopback0
   tunnel destination 192.168.0.1
   tunnel key 100000
!
interface Loopback0
   ip address 192.168.0.10 255.255.255.255
!
interface Ethernet0
   ip address 10.80.1.1 255.255.255.0
   ip virtual-reassembly
   no cdp enable
   hold-queue 32 in
   hold-queue 100 out
!
interface Ethernet1
   ip address 172.18.132.186 255.255.255.248
   ip route-cache flow
   duplex auto
   crypto map LABMAP
!
interface Async1
   bandwidth 56
   ip address negotiated
   encapsulation ppp
   no ip mroute-cache
   dialer in-band
   dialer idle-timeout 300
   dialer fast-idle 10800
```

```
   dialer enable-timeout 6
   dialer wait-for-carrier-time 75
   dialer string 60340
   dialer hold-queue 100 timeout 75
   dialer-group 1
   async default routing
   async dynamic address
   async dynamic routing
   async mode dedicated
   no fair-queue
   ppp authentication pap callin
   ppp pap sent-username lab password 0 lab
   crypto map LABMAP
!
router ospf 100
   log-adjacency-changes
   passive-interface Ethernet1
   network 10.87.252.0 0.0.1.255 area 0
   network 10.80.1.0 0.0.0.255 area 0
!
ip local policy route-map MY_LOCAL_POLICY
ip classless
!
ip route 172.16.32.124 255.255.255.255 172.18.132.185 track 123
ip route 0.0.0.0 0.0.0.0 172.18.132.185
ip route 172.16.32.124 255.255.255.255 Async1 200
ip route 192.168.0.1 255.255.255.255 172.16.32.124
!
! The IP route for the tunnel destination needs to follow the route for
! IPsec remote peer, so in this case we set the IP next-hop on the tunnel
! destination route to be the IPsec peer address. So by fact of recursive
! route lookup in the routing table the tunnel destination route will follow
! the IPsec remote peer route.
!
ip http server
ip http authentication local
no ip http secure-server
ip http path flash:dir
!
!
access-list 100 permit gre host 192.168.0.10 host 192.168.0.1
access-list 101 permit icmp host 172.18.132.186 host 172.16.32.124
access-list 102 permit ip any any
```

```
dialer-list 1 protocol ip list 102
route-map MY_LOCAL_POLICY permit 10
   match ip address 101
   set interface Ethernet1
   set ip next-hop 217.181.132.185
!
!
control-plane
!
rtr 1
!
   type echo protocol ipIcmpEcho 172.16.32.124 source-ipaddr 172.18.132.186
! Explicitly set the IP ICMP source address otherwise the rtr ICMP code will
! use an incorrect source address when switching back the IPsec peer address
! route from using the Async to using Ethernet1, because these ICMP packets
! are policy routed
!
   timeout 1000
   threshold 40
   frequency 3
rtr schedule 1 life forever start-time now
!
line con 0
   exec-timeout 0 0
   modem enable
   transport preferred all
   transport output all
   stopbits 1
line aux 0
   exec-timeout 0 0
   script dialer dial
   modem InOut
   modem autoconfigure discovery
   transport preferred all
   transport input all
   transport output all
   speed 19200
   flowcontrol hardware
line vty 0 4
   access-class 23 in
   exec-timeout 0 0
   password 7 01100F1758040506324F41
   transport preferred all
```

```
   transport input all
   transport output all
!
end
```

VERIFYING THE RESULTS

Normal Operation

This section provides information that can be used to confirm that configuration is working properly.

```
c831-27#sh ip nhrp
10.87.252.1/32 via 10.87.252.1, Tunnel0 created 1w4d, never expire
   Type: static, Flags: authoritative
   NBMA address: 192.168.0.1

c831-27#sh cry sess
Crypto session current status

Interface: Ethernet1
Session status: UP-ACTIVE
Peer: 172.16.32.124/500
   IKE SA: local 172.18.132.186/500 remote 172.16.32.124/500 Active
   IPSEC FLOW: permit 47 host 192.168.0.10 host 192.168.0.1
        Active SAs: 2, origin: crypto map

c831-27#sh dialer

As1—dialer type = IN-BAND ASYNC NO-PARITY
Idle timer (300 secs), Fast idle timer (10800 secs)
Wait for carrier (75 secs), Re-enable (6 secs)
Dialer state is idle

Dial String      Successes   Failures    Last DNIS   Last status
60340                 1679         19    00:29:09       successful   Default
c831-27#
c831-27#show ip route track-table
   ip route 172.16.32.124 255.255.255.255 172.16.28.185 track 123 state is [up]
c831-27#
c831-27#sh int tunnel 0
Tunnel0 is up, line protocol is up
    Hardware is Tunnel
    Internet address is 10.87.252.10/22
    MTU 1514 bytes, BW 1000 Kbit, DLY 10000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
```

```
    Encapsulation TUNNEL, loopback not set
    Keepalive not set
    Tunnel source 192.168.0.10 (Loopback0), destination 192.168.0.1
    Tunnel protocol/transport GRE/IP, key 0x186A0, sequencing disabled
    Tunnel TTL 255
    Checksumming of packets disabled,  fast tunneling enabled
    Tunnel transmit bandwidth 8000 (kbps)
    Tunnel receive bandwidth 8000 (kbps)
    Last input 00:00:04, output 00:00:06, output hang never
    Last clearing of “show interface” counters 6d02h
    Input queue: 0/75/6023/0 (size/max/drops/flushes); Total output drops: 1639
    Queueing strategy: fifo
    Output queue: 0/0 (size/max)
    5 minute input rate 5000 bits/sec, 5 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
      801270 packets input, 91832605 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      316526 packets output, 39386483 bytes, 0 underruns
      0 output errors, 0 collisions, 0 interface resets
      0 output buffer failures, 0 output buffers swapped out
c831-27#
c831-27#sh int asyn 1
Async1 is up (spoofing), line protocol is up (spoofing)
    Hardware is Async Serial
    Internet address will be negotiated using IPCP
    MTU 1500 bytes, BW 56 Kbit, DLY 100000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation PPP, LCP Closed, loopback not set
    Keepalive not set
    DTR is pulsed for 5 seconds on reset
    Last input 00:31:17, output 00:31:33, output hang never
    Last clearing of “show interface” counters 6d02h
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo
    Output queue: 0/10 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
      707530 packets input, 118223126 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
      65 input errors, 65 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      237830 packets output, 42472287 bytes, 0 underruns
      0 output errors, 0 collisions, 121 interface resets
```

```
       0 output buffer failures, 0 output buffers swapped out
       0 carrier transitions
c831-27#
c831-27#sh 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 172.16.28.185 to network 0.0.0.0
       172.16.0.0/32 is subnetted, 1 subnets
S         172.16.32.124 [1/0] via 172.16.28.185
       10.32.0.0/24 is subnetted, 1 subnets
O         10.32.12.0 [110/101] via 10.87.252.1, 00:33:13, Tunnel0
       10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C         10.80.1.0/24 is directly connected, Ethernet0
S         10.0.149.0/24 [1/0] via 172.16.28.185
C         10.87.252.0/22 is directly connected, Tunnel0
       192.168.0.0/32 is subnetted, 2 subnets
C         192.168.0.10 is directly connected, Loopback0
S         192.168.0.1 [1/0] via 172.16.32.124
       172.16.28.0/29 is subnetted, 1 subnets
C         172.16.28.184 is directly connected, Ethernet1
S*   0.0.0.0/0 [1/0] via 172.16.28.185
c831-27#
```

Operation During Initiating the Backup Path

This section provides information on the messages during initiating the back up path. The debug dialer was enabled on the router.

```
c831-27#
*Mar 25 23:15:16.867: As1 DDR: place call
*Mar 25 23:15:16.867: As1 DDR: Dialing cause ip (s=172.16.28.187, d=172.18.132.186)
*Mar 25 23:15:16.867: As1 DDR: Attempting to dial 60340
*Mar 25 23:15:16.867: CHAT1: Attempting async line dialer script
*Mar 25 23:15:16.867: CHAT1: Dialing using Modem script: dial & System script: none
*Mar 25 23:15:16.871: CHAT1: process started
*Mar 25 23:15:16.871: CHAT1: Asserting DTR
*Mar 25 23:15:16.871: CHAT1: Chat script dial started
*Mar 25 23:15:34.803: CHAT1: Chat script dial finished, status = Success
*Mar 25 23:15:36.803: %LINK-3-UPDOWN: Interface Async1, changed state to up
*Mar 25 23:15:36.803: As1 DDR: Dialer statechange to up
*Mar 25 23:15:36.803: As1 DDR: Dialer call has been placed
*Mar 25 23:15:37.595: As1 DDR: dialer protocol up
*Mar 25 23:15:37.595: As1 DDR: Call connected, 1 packets unqueued, 1 transmitted, 0 discarded
*Mar 25 23:15:37.803: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to up
*Mar 25 23:15:48.023: %OSPF-5-ADJCHG: Process 100, Nbr 192.168.0.1 on Tunnel0 from FULL to DOWN,
Neighbor Down: Dead timer expired
*Mar 25 23:15:49.383: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP.Peer 172.16.32.124:500       Id:
172.16.32.124
*Mar 25 23:16:10.419: %OSPF-5-ADJCHG: Process 100, Nbr 192.168.0.1 on Tunnel0 from LOADING
to FULL, Loading Done
c831-27#
```

Operation Through the Backup Path

Following is the status of the configuration, working properly through the failover path:

```
c831-27#sh ip nhrp
10.87.252.1/32 via 10.87.252.1, Tunnel0 created 1w4d, never expire
     Type: static, Flags: authoritative
     NBMA address: 192.168.0.1
c831-27#sh cry sess
Crypto session current status

Interface: Ethernet1
Session status: UP-ACTIVE
Peer: 172.16.32.124/500
     IKE SA: local 172.18.132.186/500 remote 172.16.32.124/500 Active
     IPSEC FLOW: permit 47 host 192.168.0.10 host 192.168.0.1
          Active SAs: 2, origin: crypto map
```

```
Interface: Async1
Session status: UP-ACTIVE
Peer: 172.16.32.124/500
     IKE SA: local 172.21.0.29/500 remote 172.16.32.124/500 Active
     IPSEC FLOW: permit 47 host 192.168.0.10 host 192.168.0.1
          Active SAs: 2, origin: crypto map

c831-27#sh dialer

As1—dialer type = IN-BAND ASYNC NO-PARITY
Idle timer (300 secs), Fast idle timer (10800 secs)
Wait for carrier (75 secs), Re-enable (6 secs)
Dialer state is data link layer up
Dial reason: ip (s=172.16.28.187, d=172.18.132.186)
Time until disconnect 290 secs
Current call connected 00:04:59
Connected to 60340

Dial String      Successes    Failures   Last DNIS     Last status
60340               1680         19       00:04:59       successful   Default

c831-27#sh ip route track-table
   ip route 172.16.32.124 255.255.255.255 172.16.28.185 track 123 state is [down]
c831-27#sh int tunnel 0
Tunnel0 is up, line protocol is up
     Hardware is Tunnel
     Internet address is 10.87.252.10/22
     MTU 1514 bytes, BW 1000 Kbit, DLY 10000 usec,
       reliability 255/255, txload 1/255, rxload 1/255
     Encapsulation TUNNEL, loopback not set
     Keepalive not set
     Tunnel source 192.168.0.10 (Loopback0), destination 192.168.0.1
     Tunnel protocol/transport GRE/IP, key 0x186A0, sequencing disabled
     Tunnel TTL 255
     Checksumming of packets disabled,  fast tunneling enabled
     Tunnel transmit bandwidth 8000 (kbps)
     Tunnel receive bandwidth 8000 (kbps)
     Last input 00:00:03, output 00:00:05, output hang never
     Last clearing of “show interface” counters 6d02h
     Input queue: 0/75/6864/0 (size/max/drops/flushes); Total output drops: 1643
     Queueing strategy: fifo
     Output queue: 0/0 (size/max)
     5 minute input rate 0 bits/sec, 0 packets/sec
     5 minute output rate 0 bits/sec, 0 packets/sec
```

```
       803485 packets input, 92073897 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       316685 packets output, 39402455 bytes, 0 underruns
       0 output errors, 0 collisions, 0 interface resets
       0 output buffer failures, 0 output buffers swapped out

c831-27#sh int asyn 1
Async1 is up, line protocol is up
     Hardware is Async Serial
     Internet address is 172.21.0.29/32
     MTU 1500 bytes, BW 56 Kbit, DLY 100000 usec,
       reliability 255/255, txload 1/255, rxload 9/255
     Encapsulation PPP, LCP Open
     Open: IPCP, loopback not set
     Keepalive not set
     DTR is pulsed for 5 seconds on reset
     Time to interface disconnect: idle 00:04:54
     Last input 00:00:04, output 00:00:05, output hang never
     Last clearing of “show interface” counters 6d02h
     Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0
     Queueing strategy: fifo
     Output queue: 0/10 (size/max)
     5 minute input rate 2000 bits/sec, 1 packets/sec
     5 minute output rate 0 bits/sec, 0 packets/sec
       707927 packets input, 118286572 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
       65 input errors, 65 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       237903 packets output, 42483142 bytes, 0 underruns
       0 output errors, 0 collisions, 121 interface resets
       0 output buffer failures, 0 output buffers swapped out
       0 carrier transitions

c831-27#sh 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 172.16.28.185 to network 0.0.0.0
```

```
       172.16.0.0/32 is subnetted, 1 subnets
S       172.16.32.124 is directly connected, Async1
       172.21.0.0/32 is subnetted, 2 subnets
C       172.21.0.29 is directly connected, Async1
C       172.21.0.11 is directly connected, Async1
       10.32.0.0/24 is subnetted, 1 subnets
O       10.32.12.0 [110/101] via 10.87.252.1, 00:05:36, Tunnel0
       10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.80.1.0/24 is directly connected, Ethernet0
S       10.0.149.0/24 [1/0] via 172.16.28.185
C       10.87.252.0/22 is directly connected, Tunnel0
       192.168.0.0/32 is subnetted, 2 subnets
C       192.168.0.10 is directly connected, Loopback0
S       192.168.0.1 [1/0] via 172.16.32.124
       172.16.28.0/29 is subnetted, 1 subnets
C       172.16.28.184 is directly connected, Ethernet1
S*   0.0.0.0/0 [1/0] via 172.16.28.185
c831-27#
```

Hub Router Configurations

```
Current configuration : 6965 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service sequence-numbers
!
hostname c3745-20
!
boot-start-marker
boot system flash c3745-ik9o3s-mz.123-10.bin
boot-end-marker
!
logging buffered 51200 warnings
!
username sdm privilege 15 password 0 sdm
no network-clock-participate slot 1
no aaa new-model
ip subnet-zero
no ip source-route
```

```
!
!
ip cef
!
!
crypto isakmp policy 1
   encr 3des
   authentication pre-share
   group 2
!
crypto isakmp policy 10
   hash md5
   authentication pre-share
crypto isakmp key 7578 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
crypto ipsec transform-set LAB-TRANSFORM esp-des esp-md5-hmac
!
crypto dynamic-map DYNMAP 10
   set transform-set LAB-TRANSFORM
!
!
crypto map LABMAP 10 ipsec-isakmp dynamic DYNMAP
!
!
!
!
interface Loopback0
   ip address 192.168.0.1 255.255.255.255
   !
interface Tunnel0
   bandwidth 1000
   ip address 10.87.252.1 255.255.252.0
   no ip redirects
   ip mtu 1400
   ip nhrp authentication cisco
   ip nhrp map multicast dynamic
   ip nhrp network-id 100000
   ip nhrp holdtime 360
   ip tcp adjust-mss 1360
   delay 1000
   tunnel source Loopback0
   tunnel mode gre multipoint
```

```
   tunnel key 100000
!
interface FastEthernet0/1
   description $FW_INSIDE$
   ip address 10.32.12.4 255.255.255.0
!
interface FastEthernet1/0
   description $FW_OUTSIDE$
   ip address 172.16.32.124 255.255.255.0
   ip access-group 152 in
   ip verify unicast reverse-path
   no ip redirects
   no ip unreachables
   no ip proxy-arp
   ip route-cache flow
   speed auto
   full-duplex
   crypto map LABMAP
!
router ospf 100
   log-adjacency-changes
   redistribute static subnets route-map VPN-OUT
   network 10.87.252.0 0.0.1.255 area 0
   network 10.0.0.0 0.255.255.255 area 0
   network 172.0.0.0 0.255.255.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.32.1
end
```

ISP Router Configuration

```
!hostname ISP
!
logging buffered 51200 warnings
username lab password 0 lab
!
aaa new-model
aaa authentication login default local
aaa authorization network AUTH_LIST local
aaa authorization network I123 local
aaa session-id common
ip subnet-zero
!
```

```
ip domain name yourdomain.com
ip name-server 172.19.192.254
ip cef
!
!
interface FastEthernet0/0
   description $ETH-LAN$$ETH-SW-LAUNCH$
   ip address 172.19.193.20 255.255.255.0
   ip accounting output-packets
   ip route-cache flow
   speed 100
   full-duplex
!
interface Async5
   bandwidth 56
   ip address 172.21.0.11 255.255.0.0
   encapsulation ppp
   ip route-cache flow
   no ip mroute-cache
   dialer in-band
   dialer idle-timeout 300
   dialer fast-idle 10800
   dialer enable-timeout 20
   dialer wait-for-carrier-time 75
   dialer map ip 172.21.1.1 name test-1600 broadcast 6662400
   dialer hold-queue 100 timeout 75
   dialer-group 1
   async default routing
   async dynamic address
   async dynamic routing
   async mode dedicated
   peer default ip address pool p140
   no fair-queue
   ppp authentication pap callin
!
ip local pool p140 172.21.0.20 172.21.0.30
ip route 0.0.0.0 0.0.0.0 172.19.193.1
access-list 102 permit ip any any
dialer-list 1 protocol ip list 102
!
!
line aux 0
   exec-timeout 0 0
```

```
   modem InOut
   modem autoconfigure discovery
   transport input all
   transport output all
   autoselect ppp
   speed 19200
   flowcontrol hardware
end
```

RELATED INFORMATION

- IPsec Support Page
- An Introduction to IP Security (IPsec) Encryption
- Cisco IOS Easy VPN Client Feature
- Cisco IOS Easy VPN Server
- Reliable Static Routing Backup Using Object Tracking: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5413/products_feature_guide09186a00801d862d.html
- Virtual Auxliliary Port Feature and Configuration of DSL Settings: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d12.html#1061935
- Configuring IPsec Network Security
- Configuring Internet Key Exchange Security Protocol
- Command Lookup Tool (registered customers only)
- Technical Support—Cisco Systems

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

204153.1_ETMG_AE_12.04
Printed in the USA