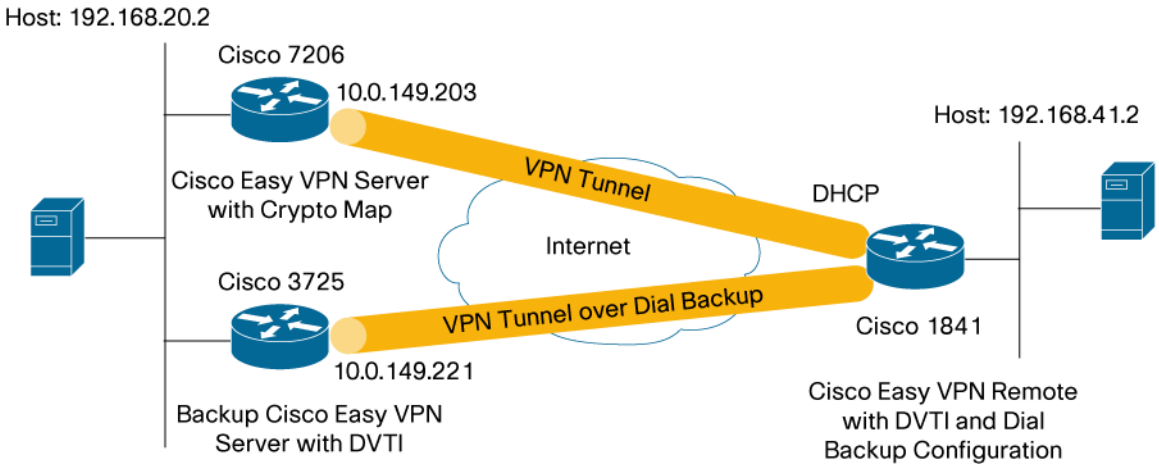
Overview

Configuring Enhanced Easy VPN with Dial Backup

This document provides a sample configuration for Cisco® Enhanced Easy VPN Remote connecting to a primary Easy VPN server with crypto map configuration, and connecting to an enhanced Easy VPN server with dial backup when the primary VPN server fails. This enhanced Easy VPN configuration uses Dynamic Virtual Tunnel Interface (DVTI).

Figure 1. Network Diagram



CISCO ENHANCED EASY VPN WITH DVTI

Cisco Enhanced Easy VPN is a new method for configuring Easy VPN using DVTIs. It can be used on both the Easy VPN Server and Easy VPN Remote routers. It relies on Virtual Tunnel Interface (VTI) to create a virtual access interface for every new Easy VPN tunnel. The configuration of the virtual access interface is cloned from a virtual template configuration. The cloned configuration includes the IP Security (IPSec) configuration and any Cisco IOS® Software feature configured on the virtual template interface, such as quality of service (QoS), NetFlow, or access control lists (ACLs).

With Cisco Enhanced Easy VPN, users can provide highly secure connectivity for remote-access VPNs. Enhanced Easy VPN can be combined with Cisco AVVID (Architecture for Voice, Video and Integrated Data) to deliver converged voice, video, and data over IP networks.

BENEFITS

- **Simplifies Management**—Customers can use the Cisco IOS virtual template to clone, on demand, new virtual access interfaces for IPSec. This simplifies VPN configuration complexity, which translates into reduced costs. In addition, existing management applications now can monitor separate interfaces for different sites.
- **Provides a Routable Interface**—Cisco IOS IPSec DVTIs support all types of IP routing protocols. Customers can use these capabilities to connect larger office environments, such as branch offices.
- **Improves Scaling**—IPSec DVTIs use single security associations per site to cover different types of traffic, thus enabling improved scaling.
- **Offers Flexibility in Defining Features**—An IPSec DVTI is an encapsulation within its own interface. This offers flexibility of defining features for clear-text traffic on IPSec VTIs, and features for encrypted traffic on physical interfaces.

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CONFIGURATION SUMMARY

This spoke router uses reliable static routing to discover when the primary Cisco Easy VPN Server fails. Reliable static routing uses the IP SLA monitor feature to monitor a remote destination. The reliable static routing does polling of the Easy VPN server availability every 10 seconds. When connectivity to the primary server fails, the reliable static routes are removed from the routing table and Easy VPN replaces the active crypto map with the backup crypto map. This enables a floating static route to become active and initiate a crypto session over the backup path. The floating static route causes the traffic to be encrypted by the backup path and to be forwarded out the dialup interface.

During the primary network path failure, the IP SLA monitor continues to monitor the primary server availability. When the IP SLA monitor detects that the primary Easy VPN Server is reachable, it will reinstall the reliable static route in the routing table, replacing the floating static route, and will reactivate the primary crypto map. While traffic is being forwarded to the primary server, the backup path becomes idle, causing the dialup to time out and bring down the backup interface.

The traffic is forwarded to or from the IPSec tunnel interface by virtue of the IP routing table lookup. Routes are dynamically learned during Internet Key Exchange (IKE) Mode configuration exchange and inserted into the routing table pointing to the virtual access interface.

This configuration allows for split tunneling. With split tunneling, remote users can send traffic destined to the Internet directly without going onto the IPSec tunnel.

The remote router is using dynamic IP addresses, a typical configuration for DSL and cable connectivity. The remote router is also using Network Extension Mode. In this mode, the remote subnet is visible to the hub network. This enables the support of devices such as voice over IP (VoIP) phones located at the remote site. This configuration can be used for User Mode as well.

This configuration shows two types of Easy VPN tunnels: a traditional Easy VPN tunnel using the primary path and an Enhanced Easy VPN tunnel with DVTI using the backup path. The two different types of tunnels were used for the purpose of demonstration only; both tunnels can be of the same type. With a traditional Easy VPN tunnel, one or more IPSec security associations are created for each IPSec tunnel (depending on the server configuration); each IPSec security association allows a specific source and destination IP address on the IPSec tunnel. With Enhanced Easy VPN, only one IPSec security association is created for each IPSec tunnel with any source to any destination IP addresses.

For more information about the IPSec DVTI feature, see “IPSec Virtual Tunnel Interface” (a link is provided in the Related Information section of this document).

LIMITATIONS

This guide provides a sample of Easy VPN configuration with DVTI configuration only.

- This guide does not cover a full security audit on the router. It is recommended that users run a Cisco Router and Security Device Manager (SDM) security audit in Wizard Mode to secure the router.
- An initial router configuration step is not shown in the steps. The full configuration is shown in the following section.
- This configuration guide enables split tunneling. Split tunneling is enabled on the hub by the ACL command under the crypto isakmp client configuration mode. To disable the split tunneling on the remote, remove the ACL command from the Easy VPN Server.
- The spoke is configured with Port Address Translation (PAT) to provide connectivity over the Internet. The spoke configuration requires Cisco IOS Software Release 12.4(4)T to work.
- This configuration uses Network Extension Mode. For details on configuring User Mode, please review documentation for Cisco Easy VPN Remote or Server.
- This configuration does not include multicast.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

COMPONENTS USED

The sample configuration uses the following releases of the software and hardware:

- Cisco IOS Software Release 12.4(4)T
- Cisco 1841, 3725, and 7206 routers

Figure 1 illustrates a sample network configuration.

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

REMOTE ROUTER CONFIGURATION

```
version 12.4
!
hostname C1841-41
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name yourdomain.com
ip name-server 30.30.30.10
ip name-server 30.30.30.11
ip ssh version 1
ip sla 1
 icmp-echo 10.0.149.203 source-interface FastEthernet0/1
 timeout 10000
 threshold 1000
 frequency 11
ip sla schedule 1 life forever start-time now
!
chat-script Dialout ABORT ERROR ABORT BUSY “”  “AT” OK “ATDT \T” TIMEOUT 45 CONN
modemcap entry modem:MSC=&FS0=8
!
username cisco password 0 cisco
!
track 123 rtr 1 reachability
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
!
crypto isakmp keepalive 10
!
crypto ipsec client ezvpn bup
 connect auto
 group cisco key cisco
 local-address Async0/0/0
 mode network-extension
 peer 10.0.149.221
 virtual-interface 1
 xauth userid mode interactive
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 local-address FastEthernet0/1
 backup bup track 123
 mode network-extension
 peer 10.0.149.203
 virtual-interface 1
 xauth userid mode interactive
!
!
interface FastEthernet0/0
 ip address 192.168.41.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 ip route-cache flow
 speed 100
 full-duplex
 crypto ipsec client ezvpn bup inside
 crypto ipsec client ezvpn ez inside
!
interface FastEthernet0/1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 ip route-cache flow
 speed 100
 full-duplex
 crypto ipsec client ezvpn ez
!
interface FastEthernet0/1/0
!
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface Virtual-Template1 type tunnel
 ip unnumbered FastEthernet0/0
 tunnel mode ipsec ipv4
!
interface Vlan1
 no ip address
!
interface Async0/0/0
 bandwidth 56
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer in-band
 dialer fast-idle 10800
 dialer enable-timeout 20
 dialer wait-for-carrier-time 75
 dialer string 60341
 dialer hold-queue 100 timeout 75
 dialer-group 1
 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 ipsec client ezvpn bup
 routing dynamic
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.149.203 track 123
ip route 0.0.0.0 0.0.0.0 Async0/0/0 240 permanent
ip route 10.0.149.221 255.255.255.255 Async0/0/0
ip route 10.0.149.203 255.255.255.255 dhcp
!
!
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
ip http server
no ip http secure-server
!
dialer-list 1 protocol ip permit
!
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
 exec-timeout 0 0
 modem InOut
 modem autoconfigure type modem
 transport input all
 transport output all
 stopbits 1
 speed 1200
 flowcontrol hardware
line 0/0/0
 exec-timeout 0 0
 modem InOut
 modem autoconfigure discovery
 transport input all
 transport output all
 stopbits 1
 speed 115200
 flowcontrol hardware
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password lab
 login local
 transport input telnet ssh
!
End
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

STATUS DURING NORMAL OPERATION

```
C1841-41#show crypto session detail
Crypto session current status

Code: C—IKE Configuration mode, D—Dead Peer Detection
K—Keepalives, N—NAT-traversal, X—IKE Extended Authentication

Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 10.0.149.203 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.0.149.203
      Desc: (none)
  IKE SA: local 10.0.35.4/500 remote 10.0.149.203/500 Active
          Capabilities:CD connid:1010 lifetime:23:58:32
  IPSEC FLOW: permit ip 192.168.41.0/255.255.255.0 192.168.20.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 85 drop 0 life (KB/Sec) 4457034/3504
        Outbound: #pkts enc'ed 85 drop 0 life (KB/Sec) 4457034/3504
  IPSEC FLOW: permit ip 192.168.41.0/255.255.255.0 192.168.71.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4528189/3504
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4528189/3504

C1841-41#show ip route
Codes: C—connected, S—static, R—RIP, M—mobile, B—BGP
       D—EIGRP, EX—EIGRP external, O—OSPF, IA—OSPF inter area
       N1—OSPF NSSA external type 1, N2—OSPF NSSA external type 2
       E1—OSPF external type 1, E2—OSPF external type 2
       i—IS-IS, su—IS-IS summary, L1—IS-IS level-1, L2—IS-IS level-2
       ia—IS-IS inter area, *—candidate default, U—per-user static route
       o—ODR, P—periodic downloaded static route

Gateway of last resort is 10.0.149.203 to network 0.0.0.0

C    192.168.41.0/24 is directly connected, FastEthernet0/0
S    192.168.20.0/24 [1/0] via 0.0.0.0, Virtual-Access3
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.35.0/24 is directly connected, FastEthernet0/1
S       10.0.149.221/32 is directly connected, Async0/0/0
S       10.0.149.203/32 [1/0] via 10.0.35.216
S    192.168.71.0/24 [1/0] via 0.0.0.0, Virtual-Access3
S*   0.0.0.0/0 [1/0] via 10.0.149.203
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
C1841-41#show dialer

As0/0/0—dialer type = IN-BAND ASYNC NO-PARITY
Idle timer (120 secs), Fast idle timer (10800 secs)
Wait for carrier (75 secs), Re-enable (20 secs)
Dialer state is idle

Dial String      Successes   Failures    Last DNIS   Last status
60341                    3          0    19:30:26       successful   Default

C1841-41#show interfaces virtual-access 3
Virtual-Access3 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of FastEthernet0/1 (10.0.35.4)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x44, loopback not set
  Keepalive not set
  Tunnel source 10.0.35.4 (FastEthernet0/1), destination 10.0.149.203
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of “show interface” counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
     70708 packets input, 4525312 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
     70759 packets output, 4528576 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out

C1841-41#sh int asyn 0/0/0
Async0/0/0 is up (spoofing), line protocol is up (spoofing)
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
  Hardware is GT96K SmartSCM Integrated Modem
  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 19:28:46, output 19:28:46, output hang never
  Last clearing of “show interface” counters 20:06:53
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 65
  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
     2885 packets input, 260171 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
     3101 packets output, 294363 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=up  DTR=up  RTS=up  CTS=up
```

LOGS DURING THE NETWORK FAILURE

```
C1841-41#
*Oct 28 17:47:29.907: %CRYPTO-6-EZVPN_CONNECTION_DOWN: (Client)  User=  Group=ci
sco  Server_public_addr=10.0.149.203
*Oct 28 17:47:48.399: %LINK-3-UPDOWN: Interface Async0/0/0, changed state to up
*Oct 28 17:47:49.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async0/0/0
, changed state to up
*Oct 28 17:47:52.031: %CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=  Group=cisc
o  Server_public_addr=10.0.149.221
```

STATUS DURING THE BACKUP PATH

```
C1841-41#show crypto session detail
Crypto session current status

Code: C—IKE Configuration mode, D—Dead Peer Detection
K—Keepalives, N—NAT-traversal, X—IKE Extended Authentication

Interface: Async0/0/0
Session status: UP-ACTIVE
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
Peer: 10.0.149.221 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.0.149.221
      Desc: (none)
  IKE SA: local 172.21.0.22/500 remote 10.0.149.221/500 Active
          Capabilities:CD connid:1011 lifetime:23:57:08
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 128 drop 0 life (KB/Sec) 4539054/3436
        Outbound: #pkts enc'ed 128 drop 0 life (KB/Sec) 4539054/3436

C1841-41#show ip route
Codes: C—connected, S—static, R—RIP, M—mobile, B—BGP
       D—EIGRP, EX—EIGRP external, O—OSPF, IA—OSPF inter area
       N1—OSPF NSSA external type 1, N2—OSPF NSSA external type 2
       E1—OSPF external type 1, E2—OSPF external type 2
       i—IS-IS, su—IS-IS summary, L1—IS-IS level-1, L2—IS-IS level-2
       ia—IS-IS inter area, *—candidate default, U—per-user static route
       o—ODR, P—periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S    192.168.72.0/24 [1/0] via 0.0.0.0, Virtual-Access2
     172.21.0.0/32 is subnetted, 2 subnets
C       172.21.0.22 is directly connected, Async0/0/0
C       172.21.0.11 is directly connected, Async0/0/0
C    192.168.41.0/24 is directly connected, FastEthernet0/0
S    192.168.20.0/24 [1/0] via 0.0.0.0, Virtual-Access2
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.35.0/24 is directly connected, FastEthernet0/1
S       10.0.149.221/32 is directly connected, Async0/0/0
S       10.0.149.203/32 [1/0] via 10.0.35.216
S*   0.0.0.0/0 is directly connected, Async0/0/0


C1841-41#show dialer

As0/0/0—dialer type = IN-BAND ASYNC NO-PARITY
Idle timer (120 secs), Fast idle timer (10800 secs)
Wait for carrier (75 secs), Re-enable (20 secs)
Dialer state is data link layer up
Dial reason: ip (s=192.168.41.2, d=192.168.149.2)
Time until disconnect 119 secs
Current call connected 00:03:43
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
Connected to 60341

Dial String      Successes   Failures    Last DNIS   Last status
60341                    4          0    00:03:43       successful   Default

C1841-41#show interfaces virtual-access 2
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Async0/0/0 (172.21.0.22)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x44, loopback not set
  Keepalive not set
  Tunnel source 172.21.0.22 (Async0/0/0), destination 10.0.149.221
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of “show interface” counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
     1587 packets input, 101748 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
     1589 packets output, 101876 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
C1841-41#show interfaces virtual-access 3
Virtual-Access3 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x44, loopback not set
  Keepalive not set
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
  Tunnel source 10.0.35.4 (FastEthernet0/1), destination 10.0.149.203
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of “show interface” counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  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
     70775 packets input, 4529600 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
     70841 packets output, 4533824 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out

C1841-41#sh interface asyn 0/0/0
Async0/0/0 is up, line protocol is up
  Hardware is GT96K SmartSCM Integrated Modem
  Internet address is 172.21.0.22/32
  MTU 1500 bytes, BW 56 Kbit, DLY 100000 usec,
     reliability 255/255, txload 4/255, rxload 4/255
  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 00:01:59
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of “show interface” counters 20:13:21
  Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 85
  Queueing strategy: fifo
  Output queue: 0/10 (size/max)
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     3494 packets input, 316195 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
     3737 packets output, 354796 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

C1841-41#
```

LOGS DURING THE NETWORK RECOVERY

```
C1841-41#
*Oct 28 17:54:04.906: %CRYPTO-6-EZVPN_CONNECTION_DOWN: (Client)  User=  Group=ci
sco  Server_public_addr=10.0.149.221
*Oct 28 17:54:06.710: %CRYPTO-4-IKMP_NO_SA: IKE message from 10.0.149.203 has no
 SA and is not an initialization offer
*Oct 28 17:54:06.750: %CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=  Group=cisc
o  Server_public_addr=10.0.149.203  NEM_Remote_Subnets=192.168.41.0/255.255.255.
0  192.
*Oct 28 17:56:06.910: %LINK-5-CHANGED: Interface Async0/0/0, changed state to re
set
*Oct 28 17:56:07.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async0/0/0
, changed state to down
*Oct 28 17:56:11.914: %LINK-3-UPDOWN: Interface Async0/0/0, changed state to down
```

HUB 1 ROUTER CONFIGURATION

```
version 12.4
!
hostname c7200-3
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login groupname local
aaa authentication login default local
aaa authorization network default local
aaa authorization network groupname local
!
aaa session-id common
!
resource policy
!
ip subnet-zero
ip cef
!
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
ip domain list yourdomain.com
ip domain list .
ip domain name cisco.com
ip name-server 171.1.1.1
ip name-server 171.1.1.2
!
username cisco password 0 cisco
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration group cisco
 key cisco
 dns 30.30.30.10 30.30.30.11
 wins 30.30.30.12 30.30.30.13
 domain cisco.com
 pool dynpool
 acl 150
!
!
crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
crypto map dynmap isakmp authorization list default
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!
interface Loopback1
 ip address 192.168.71.2 255.255.255.0
!
interface FastEthernet0/0
 no ip address
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
 shutdown
 duplex half
!
interface Ethernet3/0
 ip address 10.0.149.203 255.255.255.0
 duplex full
 crypto map dynmap
!
interface Ethernet3/1
 ip address 192.168.20.203 255.255.255.0
 duplex full
 standby 0 ip 192.168.20.1
!
router eigrp 1
 redistribute static
 network 192.168.20.0
 no auto-summary
!
ip local pool dynpool 30.30.30.20 30.30.30.30
ip classless
ip route 0.0.0.0 255.255.255.255 Ethernet3/0
!
access-list 150 permit ip 192.168.20.0 0.0.0.255 any log-input
access-list 150 permit ip 192.168.71.0 0.0.0.255 any log-input
!
!
!
!
control-plane
!
end
```

HUB 2 ROUTER CONFIGURATION

```
version 12.4
!
hostname c3725-21
!
!
!
aaa new-model
!
!
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
aaa authentication login default local
aaa authorization network default local
!
aaa session-id common
!
resource policy
!
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
ip domain name cisco.com
ip name-server 172.19.192.254
ip name-server 171.69.11.48
ip ssh version 1
!
username cisco password 0 cisco
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
 key cisco
 dns 6.0.0.2
 wins 7.0.0.1
 domain cisco.com
 pool dpool
 acl 101
crypto isakmp profile vi
   match identity group cisco
   isakmp authorization list default
   client configuration address respond
   virtual-template 1
!
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
!
!
interface Loopback8
 ip address 8.8.8.8 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.0.149.221 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.20.21 255.255.255.0
 duplex auto
 speed 100
!
interface Virtual-Template1 type tunnel
 ip unnumbered FastEthernet0/0
 tunnel source FastEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
 service-policy output FOO
!
router eigrp 1
 network 192.168.1.0
 network 192.168.20.0
 no auto-summary
!
ip local pool dpool 5.0.0.1 5.0.0.3
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.149.207
!
ip http server
ip http authentication local
no ip http secure-server
!
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
access-list 101 permit ip 192.168.20.0 0.0.0.255 any log-input
!
!
End
```

DIAL HUB

```
version 12.4
!
hostname c2851-27
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
ip domain name cisco.com
!
!
modemcap entry modem:MSC=&FS0=8
username lab password 0 lab
!
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
!
interface GigabitEthernet0/0
 ip address 10.23.2.1 255.255.255.0
 duplex auto
 speed auto
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
 crypto map test_cryptomap
!
interface GigabitEthernet0/1
 ip address 10.0.149.227 255.255.255.0
 duplex full
 speed 100
!
interface Async1
 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 3600
 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 dynamic address
 async dynamic routing
 async mode dedicated
 peer default ip address pool p140
 no fair-queue
 ppp authentication pap callin
 routing dynamic
!
interface Group-Async0
 physical-layer async
 no ip address
 no group-range
!
ip local pool p140 172.21.0.20 172.21.0.30
ip classless
ip route 2.2.2.2 255.255.255.255 10.23.2.2
ip route 3.3.3.3 255.255.255.255 10.23.2.3
ip route 7.7.7.7 255.255.255.255 10.0.149.207
ip route 8.8.8.8 255.255.255.255 10.0.149.207
!
ip http server
no ip http secure-server
```

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

```
!
access-list 102 permit ip any any
access-list 170 permit ip host 1.1.1.1 host 3.3.3.3 log
dialer-list 1 protocol ip list 102
!
!
control-plane
!
!
alias configure sh do show
alias exec po ping 3.3.3.3 sour 1.1.1.1
!
line con 0
 exec-timeout 0 0
line aux 0
 exec-timeout 0 0
 modem InOut
 transport input all
 transport output all
 autoselect ppp
 speed 115200
 flowcontrol hardware
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

RELATED INFORMATION

- IPSec Support Page
- Cisco Easy VPN Remote
- Cisco Easy VPN Server
- IPSec Virtual Tunnel Interface
- Configuring IPSec Network Security
- Configuring IKE Security Protocol
- Command Lookup Tool (registered customers only)
- Technical Support—Cisco Systems

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

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 Website 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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

205233.CA_ETMG_KS_11.05

Printed in the USA

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.