CHAPTER 3

# Small Branch—Cable with DSL Backup

This chapter includes the following sections:

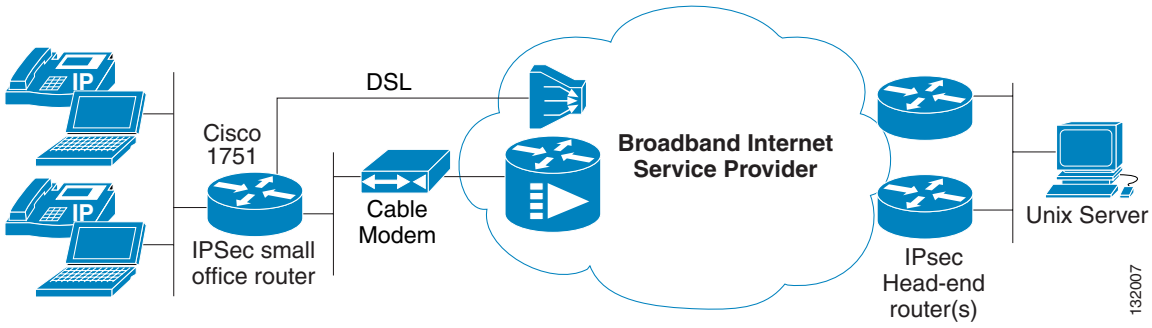


As enterprise customers begin to deploy IP telephony using broadband as the access media to the small office environment, backup links are required to minimize service disruption. In existing Frame Relay deployments, ISDN was the preferred choice as a dial backup mechanism because it offered sufficient bandwidth, was relatively cost effective, and offered a different technology as the underlying media.

Using different technologies for the primary and backup links isolates the enterprise from the catastrophic failure of one technology taking down both the primary and backup links. Examples of this are the notable Frame Relay failures that were manifest in the total collapse of these networks in the late 1990s. The enterprises that were least impacted by these service outages were those that used ISDN as their backup mechanism. The human and software errors that caused the Frame Relay failures did not impact the ISDN network.

Applying this concept of using alternate technologies to provide backup to the small office, the natural conclusion is to deploy both DSL and cable, as shown in Figure 3-1.

***Figure 3-1 DSL with Cable Backup Topology***



A small office is likely to have at least one or more “plain old telephone service” (POTS) lines anyway, and enabling one for DSL service adds approximately $50 USD a month. A cable-provided Internet service costs approximately $50 USD a month in addition to a basic cable service if required. A side benefit is cable TV in the employee lounge. Using the Raleigh-Durham, North Carolina market as an example, the small office has available to it a 256-kbps uplink via DSL and 384-kbps uplink via cable for approximately $100 USD a month.

A degree of ISP separation is also present in addition to the alternate technologies of DSL and cable at the local loop. It is likely that the DSL and cable providers connect to different Tier 2 ISPs that in turn likely connect to multiple Tier 1 ISPs. If the head-end Internet connection uses multiple Tier 1 ISPs, the branch offices are isolated to some extent from service disruptions within a particular ISP. Alternately, the enterprise can consider connecting directly to either the IP network of the cable or DSL provider, or to the Tier 2 ISP servicing the broadband provider.

# Solution Characteristics

This deployment scenario is applicable to small branch offices that have the following connectivity characteristics:

- Low recurring costs for WAN access
- Desire to use alternate technologies for primary and backup path
- No multiprotocol or IP multicast requirements
- A highly-scalable, redundant, and cost effective head-end IPSec termination
- Encryption required for both primary and backup link

The Reliable Static Routing Backup Using Object Tracking feature is used to trigger a backup connection (in these examples using a cable modem) to be initiated by the remote customer premises equipment (CPE) in scenarios where only static routes are used. Both cable and DSL deployments rely on static routes to reach the service provider as a next hop address.

This feature allows a target to be identified and pinged or probed using Cisco Service Assurance Agent (SAA) over the primary interface. In this example, it is a Cisco IOS router at the head-end location that is reachable only through the IPSec tunnel.

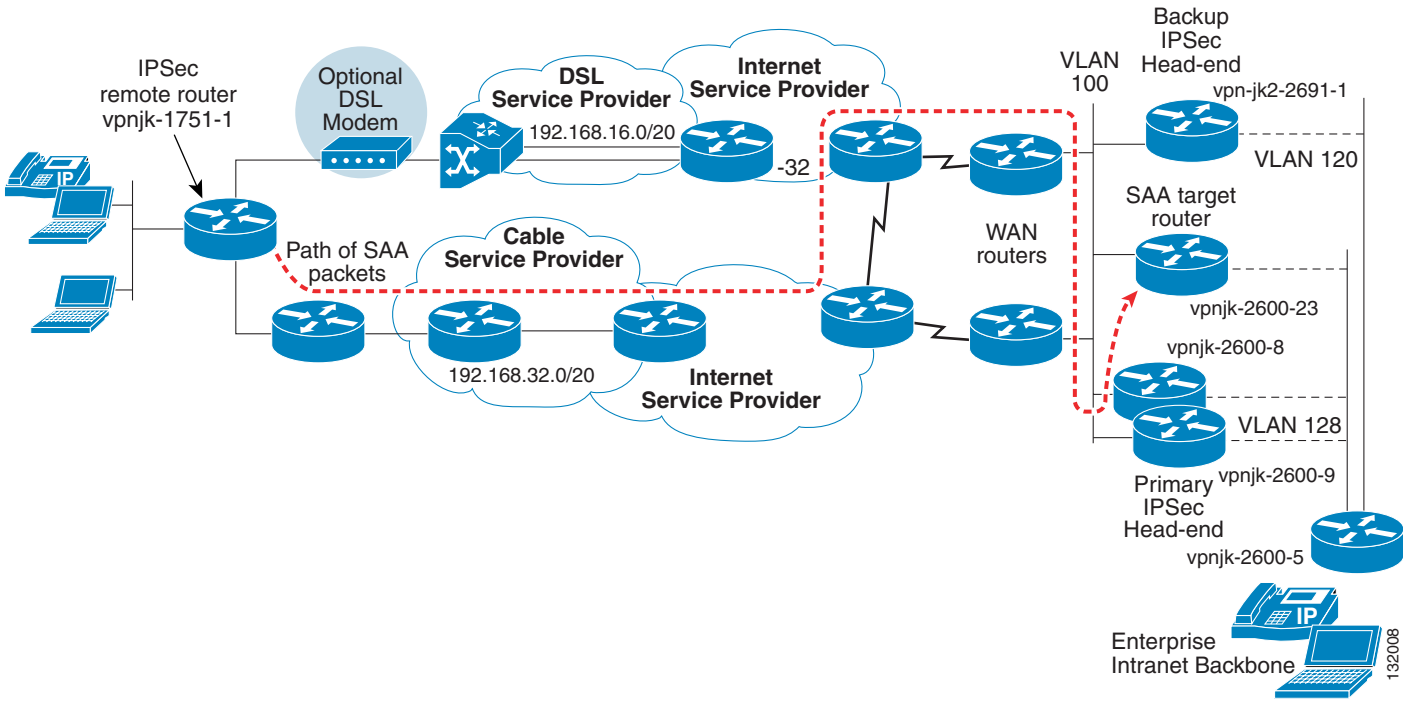
If the pings/probes fail, the static route for the primary path is removed from the routing table, allowing a static route with a higher administrative distance to be inserted into the routing table as an alternate default route. The pings/probes continue to be attempted over the primary interface. If they are successful again, the connection is re-established over the primary interface.

# Topology

The topology shown in Figure 3-2 is used as an example. The routers are named as follows:

- IPSec primary head-end routers—vpnjk-2600-8 and vpnjk-2600-9
- IPSec backup path head-end router—vpn-jk2-2691
- Head-end SAA target router—vpnjk-2600-23
- Remote router—vpnjk-1751-1

*Figure 3-2 Test Topology—Cable with DSL Backup*




This design uses the Cisco IOS feature, Reliable Static Routing Backup Using Object Tracking, to verify connectivity with SAA probes originating from the inside Ethernet LAN address of the remote router through the IPSec tunnel that traverses the DSL provider to the IPSec head-end routers. The SAA probe packets are encrypted and forwarded to the head-end SAA target router. The probe responses follow the return path and the SAA control plane follows the same path as the probe packets.

This configuration provides a backup path over the DSL service provider if the primary path over the cable service provider fails. Connectivity failures of the SAA probes trigger the use of the backup path.

# Failover/Recovery Time

This section shows examples of a temporary failure that causes packet loss but recovers before the backup path is activated. The second example illustrates a failure of the primary path of sufficient duration to trigger the use of the backup link.

This section includes the following topics:

# Temporary Failure with Service Restoration

An issue associated with on-demand backup links is how to avoid triggering use of the backup path for very short connectivity failures through the primary path. With a keepalive protocol, the network administrator is generally able to configure a keepalive interval and a dead interval. The dead interval effectively controls how many consecutive keepalives are missed before declaring the primary path down.

With the Reliable Static Routing Backup Using Object Tracking feature, the dead interval is controlled by the **delay down** command within the **track** statement and the hello interval is configured by the **frequency** command within the **rtr** statement. As an illustration, these values are set at 60 and 20 seconds respectively. The IKE keepalive value is 10 seconds with a default of 2 seconds between retries following initial failure.

The following captured commands show the sequence of events and time for a simulated brief link flap for the connection between the network of the broadband service provider network and their ISP.

Here the ISP link fails at 13:26:28:

```
Dec 19 13:26:28.265 est: %ATM-5-UPDOWN: Interface ATM1/IMA0.1, Changing autovc .
Dec 19 13:26:28.269 est: %BGP-5-ADJCHANGE: neighbor 192.168.129.26 Down Interfap
```

The IKE keepalives identified the failure at 13:26:51 or approximately 23 seconds later. IKE attempts to contact the secondary peer, assuming an IPSec head-end failure.

```
vpnjk-1751-1#
Dec 19 13:26:51.422 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.8:500       Id: vpnjk-2600-8.ese.cisco.com
```

With **debug track**, you can see that the tracking logic has identified a connection failure of the SAA configuration but delays action for 60 seconds. This is 27 seconds from the original link failure.

```
Dec 19 13:26:55.074 est: Track: 123 Down change delayed for 60 secs
```

At this point, the original link failure has recovered; this is one minute from the initial link failure.

```
Dec 19 13:26:53.795 est: %ATM-5-UPDOWN: Interface ATM1/IMA0.1, Changing autovc .
Dec 19 13:27:28.156 est: %BGP-5-ADJCHANGE: neighbor 192.168.129.26 Up
```

At this point, the IPSec tunnel has been re-established; however, the new tunnel is with the secondary IPSec head end, vpnjk-2600-9.ese.cisco.com, and the initial IPSec tunnel was with the primary IPSec head-end, vpnjk-2600-8.ese.cisco.com.

```
Dec 19 13:27:41.754 est: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than
(2000)msecs (0/0),process = Crypto IKMP.
-Traceback= 802971E8 80294574 8129E55C 81295D6C 81294760 81294304 812906D0 812635A8
812869FC 81263EC4 8125F278 8125D9F0 8127F120 81

Dec 19 13:27:42.274 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
192.168.131.9:500       Id: vpnjk-2600-9.ese.cisco.com
```

With connectivity established, the SAA UDP probe was successful and the action was aborted. This event occurred 9 seconds before the 60 second track delay expired.

```
Dec 19 13:27:46.894 est: Track: 123 Down change delay cancelled
```

At this point, all connectivity has been restored. The only change was a swap of the IPSec tunnel from the primary to the secondary head-end during the brief failure. The IKE keepalive values can be increased if needed. However, recall that the SAA probes are encrypted and require the IPSec tunnel to reach the head-end SAA router.

# Failure of Primary Path—Recovery over Backup Path

The following example shows the backup path being activated. First, a failure in the network of the ISP disrupts connectivity.

```
Jan 30 16:37:40.738 est: %BGP-5-ADJCHANGE: neighbor 192.168.129.29 Down Interface flap
Jan 30 16:37:42.733 est: %LINK-5-CHANGED: Interface Serial0/0, changed state to down
```

Approximately 39 seconds from the ISP link failure, the tracking logic has identified the failure.

```
vpnjk-1751-1#
Jan 30 16:37:59.192 est: Track: 123 Down change delayed for 60 secs
Jan 30 16:38:05.776 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.9:500       Id: vpnjk-2600-9.ese.cisco.com
```

One minute later (recall that **delay down 60** is configured), the IP route associated with the track subsystem is removed from the routing table. This is a default route to the dialer interface (the primary path). The secondary path is through a cable modem, and the router obtains a default route using DHCP for the interface to the cable provider.

```
Jan 30 16:38:59.192 est: Track: 123 Down change delay expired
Jan 30 16:38:59.192 est: Track: 123 Change #8 rtr 23, reachability Up->Down
```

The floating static route to the PPPoE dialer interface is now in the routing table. The DHCP learned route is configured with an administrative distance of 239. The floating static is 240.

```
vpnjk-1751-1>show rtr op  23  | inc return code
Latest operation return code: No connection
vpnjk-1751-1>show ip route | inc 0.0.0.0
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/25 is subnetted, 1 subnets
S*   0.0.0.0/0 is directly connected, Dialer1
```

Approximately 96 seconds after the ISP link failure, connectivity has been restored to the backup head-end IPSec peer.

```
Jan 30 16:39:16.084 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
192.168.131.4:500       Id: vpn-jk-2691-1.ese.cisco.com
```

During the failure, a ping was started before the ISP link failure to determine the approximate length of time of the failure, plus or minus 5 seconds. 20 Internet Control Message Protocol (ICMP) packets were lost, or approximately 100 seconds for recovery.

```
vpnjk-2600-2#ping 10.2.128.5 timeout 5 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 10.2.128.5, timeout is 5 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.....................!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!![repetition removed]
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
Success rate is 98 percent (980/1000), round-trip min/avg/max = 8/15/24 ms
```

As service in the ISP network is restored, the SAA probe is again able to reach the head-end SAA target router. The remote router configuration includes a host route to the head-end SAA target router using the DHCP learned next hop router, so the SAA probe must connect over the primary interface. When the primary path is restored, successful probe transactions trigger a tracking change in state from down to up. The tracking configuration delays the transition from down to up for 5 seconds.

```
vpnjk-1751-1>
Jan 30 16:53:14.328 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
192.168.131.9:500       Id: vpnjk-2600-9.ese.cisco.com
Jan 30 16:53:24.196 est: Track: 123 Up change delayed for 5 secs
Jan 30 16:53:29.196 est: Track: 123 Up change delay expired
Jan 30 16:53:29.196 est: Track: 123 Change #9 rtr 23, reachability Down->Up
```

There is no advantage in configuring a long up delay because the IPSec tunnel must be established for the SAA probe to complete. There is little or no appreciable packet loss when changing state from down to up, because both the primary and backup path and IPSec tunnel are connected at the same time. The tracking subsystem is simply adding the default route for the primary or DHCP interface to influence the network traffic of the end user. Following is an example of the default route under normal operations.

```
vpnjk-1751-1>show ip route | begin Gateway
Gateway of last resort is 192.168.33.1 to network 0.0.0.0

     192.168.131.0/24 is variably subnetted, 3 subnets, 2 masks
S       192.168.131.8/31 [1/0] via 192.168.33.1
S       192.168.131.4/32 is directly connected, Dialer1
S       192.168.131.23/32 [1/0] via 192.168.33.1
     10.0.0.0/25 is subnetted, 1 subnets
C       10.0.68.0 is directly connected, FastEthernet0/0
     192.168.17.0/32 is subnetted, 2 subnets
C       192.168.17.1 is directly connected, Dialer1
C       192.168.17.3 is directly connected, Dialer1
C    192.168.33.0/24 is directly connected, Ethernet1/0
S*   0.0.0.0/0 [239/0] via 192.168.33.1
```

# Routing Topology Following Network Recovery

The IPSec IKE and IPSec security associations for the backup interface remain active after the primary interface has been restored. Looking at the routing table of the backup head-end IPSec peer following the link restoration, the RRI injected route remains.

```
vpn-jk-2691-1#sh ip route static
     10.0.0.0/8 is variably subnetted, 12 subnets, 8 masks
S       10.0.68.0/25 [1/0] via 192.168.17.3
```

However, the path over the primary IPSec head-end peer is used from the remote LAN to the enterprise intranet backbone router. In this case, 192.168.131.9 is vpnjk-2600-9.ese.cisco.com.

```
traceroute 10.2.128.5

Type escape sequence to abort.
Tracing the route to 10.2.128.5

  1 10.0.68.5 4 msec 0 msec 4 msec
  2 192.168.131.9 8 msec 8 msec 8 msec
  3 10.2.128.5 8 msec *  8 msec
```

From the head-end perspective, recovery of the primary path induces a metric change, and **debug ip routing** was enabled on the enterprise intranet router during recovery. Note that the route to 10.0.68.0/25 is replaced by one with a lower (better) metric over the primary path.

```
vpnjk-2600-5#
Jan 30 16:53:14 est: RT: del 10.0.68.0/25 via 10.2.120.4, eigrp metric [170/10258432]
Jan 30 16:53:14 est: RT: add 10.0.68.0/25 via 10.2.128.9, eigrp metric [170/6925056]


vpnjk-2600-5#show ip eigrp topology all-links   | begin 10.0.68.0
```

```
P 10.0.68.0/25, 1 successors, FD is 6925056, serno 1710
        via 10.2.128.9 (6925056/6922496), FastEthernet0/1.128
        via 10.2.120.4 (10258432/10255872), FastEthernet0/1.120
        via 10.2.124.23 (6927616/6925056), FastEthernet0/1.124
```

This action is based on the Enhanced Interior Gateway Routing Protocol (EIGRP) configuration of the primary and backup IPSec head-end peers. The backup peer is redistributing the RRI static routes with a bandwidth of 256:

```
vpn-jk-2691-1#sh run b | beg router eigrp
router eigrp 100
 redistribute static metric 256 1000 255 1 1500 route-map IPSEC_Subnets
```

However, the primary peers are redistributing the RRI static routes with a bandwidth of 384 kbps:

```
vpnjk-2600-9#show run brief | begin router eigrp
router eigrp 100
 redistribute static metric 384 1000 255 1 1500 route-map IPSEC_Subnets
```

In this sample configuration, the trained rate of the DSL connection is 256 kbps uplink and the cable connection is simulating a 384 kbps guaranteed rate.

**Note** Many cable providers quote a burst rate and not a guaranteed rate in their marketing literature.

```
vpnjk-2600-5#show ip route 10.0.68.0
Routing entry for 10.0.68.0/25
  Known via "eigrp 100", distance 170, metric 6925056, type external
  Redistributing via eigrp 100
  Last update from 10.2.128.9 on FastEthernet0/1.128, 00:05:05 ago
  Routing Descriptor Blocks:
  * 10.2.128.9, from 10.2.128.9, 00:05:05 ago, via FastEthernet0/1.128
      Route metric is 6925056, traffic share count is 1
      Total delay is 10100 microseconds, minimum bandwidth is 384 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

The above display shows the characteristics of the route when the IPSec tunnel is active on the primary IPSec peer. The minimum bandwidth for the route is 256 kbps when the primary path has failed and the backup IPSec peer has the best route to the remote network.

# V3PN QoS Service Policy

The primary path is cable and the backup path is DSL. These technologies vary in the amount of Layer 2 overhead. The priority or LLQ must be configured for the worst case to use a common child service policy, but the parent service policy, the shaper, can be tuned accordingly.

A shaper for both DSL and cable is configured and applied to the respective Ethernet interface.

```
policy-map Shaper-DSL
 class class-default
  shape average 182400 1824
  service-policy V3PN-Small_Branch
policy-map Shaper-cable
 class class-default
  shape average 364800 3648
  service-policy V3PN-Small_Branch
!
!
interface Ethernet0/0
```

```
 description to DSL MODEM
 bandwidth 256
 no ip address
 service-policy output Shaper-DSL
 …
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Ethernet1/0
 description To CABLE MODEM
 bandwidth 384
 ip dhcp client route track 123
 ip address dhcp
 service-policy output Shaper-cable
 …
```

No other special considerations need be given. A common shaper value using the lower of the two values can be used for both cable and DSL to simplify configuration.

# Performance Results

The SAA target head-end router must be available to respond to SAA probes for the remote routers to make use of their primary path. Cisco recommends that the CPU of the SAA target head-end router ideally be less than 30 percent busy; 30 percent to 60 percent is acceptable. Over 60 percent busy is not recommended.

A Cisco 26xx series router being used as a dedicated SAA target head-end router is estimated to process 20–30 probes per second and to stay within these CPU requirements. The number of remote routers being serviced by the SAA target head-end router depends on the frequency of the SAA probe from each remote router. The configuration example shown here uses a frequency of 20 seconds between probes, which equates to up to 600 remote routers.

**Note** If the SAA probe frequency is configured at a value less than the IKE keepalive frequency, the Dead Peer Detection (DPD) logic generally never sends out IKE keepalive packets, because the SAA probes do not allow the IKE worry interval to expire. However, decreasing the SAA probe frequency means more load on the SAA head-end and more packets that must be encrypted and decrypted by the head-end IPSec routers. The network manager has a great deal of latitude in configuring these various timers.

# Implementation and Configuration

This section describes the key configuration components. In the following examples, these addressing conventions are used:

- All subnets of 10.0.0.0 addressing represent *enterprise internal* address space.
- All subnets of 192.168.0.0 addressing represent *Internet routable* address space.

This section includes the following topics:

- Show Commands

# Remote Router SAA and Tracking Configuration

The configuration of the remote router is relatively simple; a tracking operation must be configured to associate the DHCP learned default route with the SAA configuration. The cable head-end provides an IP address and default gateway using DHCP. For the DSL interface, the IP address is negotiated using PPP. A floating static default route is configured pointing to the dialer interface.

First, the administrative distance of the default route learned using DHCP is 239, which is set with the **ip dhcp-client default-router distance** command. Then the tracked object 123 is defined and associated with SAA (rtr) operation 23. The default route to the DHCP router is associated with track 123, via the **ip dhcp client route track 123** interface command. This route is removed from the routing table if the SAA destination IP address cannot be reached. The floating static route to Dialer 1 with administrative distance of 240 is inserted in its place.

```
ip dhcp-client default-router distance 239
!
track 123 rtr 23 reachability
 delay down 60 up 5
!
interface Ethernet1/0
 description To CABLE MODEM
 bandwidth 384
 ip dhcp client route track 123
 ip address dhcp
!
ip route 0.0.0.0 0.0.0.0 Dialer1 240 name Backup_Path
!
ip route 192.168.131.4 255.255.255.255 Dialer1 name Backup_Peer
!
ip route 192.168.131.23 255.255.255.255 dhcp      # SAA Target Router
ip route 192.168.131.8 255.255.255.254 dhcp       # Primary IPSec Head-ends
!
rtr 23
 type udpEcho dest-ipaddr 192.168.131.23 dest-port 57005 source-ipaddr 10.0.68.5
source-port 48879
 tos 192
 timeout 1000
 owner TRACK123
 tag Object Tracking
 frequency 20
 lives-of-history-kept 1
 buckets-of-history-kept 10
 filter-for-history failures
rtr schedule 23 start-time now life forever
!
```

The SAA configuration shows the use of an UDP echo probe rather than an ICMP probe. ICMP probes are required if the head-end target is not a Cisco router with **rtr responder** configured. Either probe is acceptable, the function of the probe is traverse inside the crypto tunnel to verify the primary path is functional. The UDP source and destination port numbers are arbitrary, decimal 57005 is 0xDEAD in hexadecimal, and decimal 48879 is 0xBEEF. These character strings are easy to identify when looking at port number values shown in hexadecimal.

There is a host route to the SAA target device, 192.168.131.23, using the DHCP learned default gateway as the target. All SAA connection attempts must use the cable or primary interface.

**Note** While the SAA target device address is in the 192.168.0.0/16 address space, which represents Internet routable address space in these illustrations, the SAA probe is encapsulated inside the IPSec tunnel. The next hop address in the static route for 192.168.131.23 is the DHCP learned default gateway. This routes the probe out the cable or primary interface. The source IP address of the SAA probe is the inside LAN interface which is referenced in the crypto map. The SAA probe therefore is encrypted and transmitted inside the IPSec tunnel

Some optional SAA configuration commands are shown in grey/italics that are explained in a subsequent section.

# Head-end SAA Target

To configure the head-end SAA target, include the following in the configuration:

```
rtr responder
```

The SAA control plane listens on UDP port 1967, when the default configuration value of *control enable* is in effect.

```
vpnjk-2600-23#show ip sockets
Proto    Remote      Port      Local        Port  In Out Stat TTY OutputIF
 17 0.0.0.0             0 10.0.253.4         67   0   0 2211   0
 88   --listen--          10.0.253.4        100   0   0    0   0
 17   --listen--          10.0.253.4        123   0   0    1   0
 17 0.0.0.0             0 10.0.253.4       1967   0   0  211   0
```

From the remote router, the SAA control plane as well as the probe packets can be identified using NetFlow if enabled on the appropriate interfaces.

```
vpnjk-1751-1#sh ip cache verb flow | begin SrcIf

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Vi1            192.168.131.23  Local          10.0.68.5       11 C0  10       1
DEAD /0  0                     BEEF /0  0     0.0.0.0                44     0.0
Vi1            192.168.131.8   Local          192.168.17.3    32 00  10       3
B92C /0  0                     C0FA /0  0     0.0.0.0                96     1.6
Vi1            192.168.131.23  Local          10.0.68.5       11 C0  10       1
07AF /0  0                     BEEF /0  0     0.0.0.0                36     0.0
```

The probe packets are 44 bytes (Layer 3) by default. Source port of 0x7AF is decimal 1967. Note that the source port for the control plane and the probe packets are the same value.

# IPSec Head-end Routers

This section describes the configuration of IPSec head-end routers.

## Backup IPSec Peer

This configuration includes a digital certificate; however, for the purposes of this test, the authentication method over the back-up interface is IKE aggressive mode with pre-shared keys. The keys are not stored on a separate RADIUS server, rather on a *keyring* defined on this router.

```
version 12.3
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname vpn-jk-2691-1
!
boot-start-marker
boot system flash c2691-ik9o3s-mz.123-5
boot system flash c2691-ik9o3s-mz.122-13.T10
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 [removed]
!
memory-size iomem 15
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host ect-msca 172.26.179.237
ip host harry 172.26.176.10
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 crl optional
 auto-enroll 70
!
crypto ca certificate chain ect-msca
 certificate 5D7B2D4300000000003C
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A
!
crypto keyring Backup_Sites
  pre-shared-key hostname Store77.ese.cisco.com  key 00-02-8A-9B-05-33
!
crypto isakmp policy 1
 encr 3des
 group 2
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
crypto isakmp profile AGGRESSIVE
   description Profile to test Initiating Aggressive Mode
   keyring Backup_Sites
   self-identity fqdn
   match identity host domain ese.cisco.com
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
!
crypto dynamic-map DYNO-TEMPLATE 10
```

```
 description dynamic crypto map
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
 reverse-route
 qos pre-classify
!
!
crypto map DYNO-MAP local-address FastEthernet0/1.100
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
!
!
interface FastEthernet0/1
 description dot1q
 no ip address
 ip route-cache flow
 duplex auto
 speed auto
!
interface FastEthernet0/1.100
 description Outside Interface
 encapsulation dot1Q 100
 ip address 192.168.131.4 255.255.255.224
 crypto map DYNO-MAP
!
interface FastEthernet0/1.120
 description Inside Interface
 encapsulation dot1Q 120
 ip address 10.2.120.4 255.255.255.0
!
!                 The bandwidth value of 256 in the metric command is important!
!                 Described previously when illustrating failover.
!
router eigrp 100
 redistribute static metric 256 1000 255 1 1500 route-map IPSEC_Subnets
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 no auto-summary
!
no ip http server
no ip http secure-server
ip classless
!
!
access-list 68 permit 10.0.64.0 0.0.63.255
access-list 68 deny   any
!
route-map IPSEC_Subnets permit 10
 match ip address 68
!
rtr responder
!
ntp server 192.168.130.1
!
end
```

## Primary IPSec Peers

The following is the configuration for primary IPSec peers:

```
!   System image file is "flash:c2600-ik9o3s-mz.122-11.T5"
version 12.2
service timestamps debug datetime localtime show-timezone
```

```
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname vpnjk-2600-8
!
logging buffered 4096 debugging
enable password 7 [removed]
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host harry 172.26.176.10
ip host ect-msca 172.26.179.237
!
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 auto-enroll 70
crypto ca certificate chain ect-msca
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A nvram:ect-mscaCA.cer
 certificate 6122A4EC000000000021 nvram:ect-msca.cer
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
!
crypto dynamic-map DYNO-TEMPLATE 10
 description dynamic crypto map
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
 reverse-route
 qos pre-classify
!
!
crypto map DYNO-MAP local-address FastEthernet0/1.100
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
!
interface FastEthernet0/1
 description dot1q
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.100
 description Outside Interface
 encapsulation dot1Q 100
 ip address 192.168.131.8 255.255.255.224
 crypto map DYNO-MAP
!
interface FastEthernet0/1.128
 description Inside Interface
```

```
 encapsulation dot1Q 128
 ip address 10.2.128.8 255.255.255.0
!
!                           Bandwidth value for backup IPSec peer is 256
!
router eigrp 100
 redistribute static metric 384 1000 255 1 1500 route-map IPSEC_Subnets
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 no auto-summary
 no eigrp log-neighbor-changes
!
ip default-gateway 172.26.156.1
ip classless
no ip http server
!
!
access-list 68 permit 10.0.68.0 0.0.0.255
access-list 68 deny   any
!
route-map IPSEC_Subnets permit 10
 match ip address 68
!
!
ntp server 192.168.130.1
!
end
================================================================================

!   System image file is "flash:c2600-ik9o3s-mz.122-11.T5"
version 12.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname vpnjk-2600-9
!
logging buffered 4096 debugging
enable password 7 1511021F0725
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host harry 172.26.176.10
ip host ect-msca 172.26.179.237
!
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 auto-enroll 70
crypto ca certificate chain ect-msca
 certificate 610BE2E400000000001F nvram:ect-msca.cer
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A nvram:ect-mscaCA.cer
!
crypto isakmp policy 1
 encr 3des
 group 2
```

```
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
!
crypto dynamic-map DYNO-TEMPLATE 10
 description dynamic crypto map
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
 reverse-route
 qos pre-classify
!
!
crypto map DYNO-MAP local-address FastEthernet0/1.100
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
!
interface FastEthernet0/1
 description dot1q
 no ip address
 ip route-cache flow
 duplex auto
 speed auto
!
interface FastEthernet0/1.100
 description Outside Interface
 encapsulation dot1Q 100
 ip address 192.168.131.9 255.255.255.224
 crypto map DYNO-MAP
!
interface FastEthernet0/1.128
 description Inside Interface
 encapsulation dot1Q 128
 ip address 10.2.128.9 255.255.255.0
!
!                            Bandwidth value for backup IPSec peer is 256
!
router eigrp 100
 redistribute static metric 384 1000 255 1 1500 route-map IPSEC_Subnets
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
no ip http server
!
!
access-list 68 permit 10.0.68.0 0.0.0.255
!
route-map IPSEC_Subnets permit 10
 match ip address 68
!
ntp server 192.168.130.1
!
end
```

# Remote Router

The following is the configuration for the remote router. See the specific notes in the following configuration:

```
!           System image file is "flash:vpn/images/c1700-k9o3sy7-mz.123-2.XE"
version 12.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname vpnjk-1751-1
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 [removed]
!
memory-size iomem 25
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!
!
!
ip telnet source-interface FastEthernet0/0
no ip domain lookup
ip domain name ese.cisco.com
ip host harry 172.26.176.10
ip host ect-msca 172.26.179.237
ip cef
ip audit notify log
ip audit po max-events 100
ip dhcp-client default-router distance 239
!
track 123 rtr 23 reachability
 delay down 60 up 5
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir
!
!              Certificates will be used for authentication for the primary path
!              and IKE Aggressive mode will be used for the backup path
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 revocation-check none
!
!
crypto ca certificate chain ect-msca
 certificate 610C436F00000000002C
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A
!
!
crypto isakmp policy 1
 encr 3des
 group 2
!
crypto isakmp policy 20
```

```
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
!
crypto isakmp peer address 192.168.131.4
 set aggressive-mode password 00-02-8A-9B-05-33
 set aggressive-mode client-endpoint fqdn Store77.ese.cisco.com
crypto isakmp profile AGGRESSIVE
   description Profile to test Initiating Aggressive Mode
   self-identity fqdn
   match identity host domain ese.cisco.com
   initiate mode aggressive
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
no crypto ipsec nat-transparency udp-encaps
!
crypto map PRIMARY_LINK 1 ipsec-isakmp
 description Crypto Map for Primary Path
 set peer 192.168.131.9
 set peer 192.168.131.8
 set transform-set 3DES_SHA_TUNNEL
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
crypto map BACKUP_LINK 1 ipsec-isakmp
 description Crypto Map for Backup Path
 set peer 192.168.131.4
 set transform-set 3DES_SHA_TUNNEL
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
!
!
class-map match-all VOICE
 match ip dscp ef
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match access-group name IKE
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21
!
!
policy-map V3PN-Small_Branch
description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 128
 class TRANSACTIONAL-DATA
  bandwidth percent 22
 class class-default
  fair-queue
  random-detect
policy-map Shaper-DSL
 class class-default
```

```
  shape average 182400 1824
  service-policy V3PN-Small_Branch
policy-map Shaper-cable
 class class-default
  shape average 364800 3648
  service-policy V3PN-Small_Branch
!
!
!
interface Ethernet0/0
 description to DSL MODEM
 bandwidth 256
 no ip address
 service-policy output Shaper-DSL
 load-interval 30
 half-duplex
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface FastEthernet0/0
 description Inside
 ip address 10.0.68.5 255.255.255.128
 no ip proxy-arp
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 speed auto
!
interface Ethernet1/0
 description To CABLE MODEM
 bandwidth 384
 ip dhcp client route track 123
 ip address dhcp
 service-policy output Shaper-cable
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 half-duplex
 crypto map PRIMARY_LINK
!
interface Dialer1
 description Outside
 bandwidth 256
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication pap callin
 ppp chap refuse
 ppp pap sent-username cisco789@cisco.com password 0 foo
 ppp ipcp dns request
 ppp ipcp wins request
 crypto map BACKUP_LINK
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 240 name Backup_Path
ip route 192.168.131.4 255.255.255.255 Dialer1 name Backup_Peer
ip route 192.168.131.23 255.255.255.255 dhcp
ip route 192.168.131.8 255.255.255.254 dhcp
```

```
no ip http server
no ip http secure-server
!
!
!
ip access-list extended CRYPTO_MAP_ACL
 permit ip 10.0.68.0 0.0.0.127 any
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
dialer-list 1 protocol ip permit
!
!
control-plane
!
rtr responder
rtr 23
 type udpEcho dest-ipaddr 192.168.131.23 dest-port 57005 source-ipaddr 10.0.68.5
 tos 192
 timeout 1000
 owner TRACK123
 tag Object Tracking
 frequency 20
 lives-of-history-kept 1
 buckets-of-history-kept 10
 filter-for-history failures
rtr schedule 23 start-time now life forever
!
ntp server 192.168.130.1
!
end
```

# Show Commands

The following optional SAA configuration statements provide for maintaining a history of the last ten failed connection attempts:

```
 lives-of-history-kept 1
 buckets-of-history-kept 10
 filter-for-history failures
```

These can be displayed on the remote router as follows:

```
vpnjk-1751-1#show rtr history  23  full
Entry number: 23
Life index: 1
Bucket index: 67
Sample time: 14:08:56.369 est Fri Dec 19 2003
RTT (milliseconds): 0
Response return code: No connection

Life index: 1
Bucket index: 68
Sample time: 14:09:16.366 est Fri Dec 19 2003
RTT (milliseconds): 0
Response return code: No connection

Life index: 1
Bucket index: 69
Sample time: 14:09:36.367 est Fri Dec 19 2003
RTT (milliseconds): 0
Response return code: No connection
```

The time stamps in the display help to identify when network connectivity failures occurred. Use Network Time Protocol (NTP) to maintain accurate time on the remote routers.

# Cisco IOS Versions Tested

The following code versions were used during testing:

- Primary IPSec head-ends—c2600-ik9o3s-mz.122-11.T5
- Backup IPSec head-ends—c2691-ik9o3s-mz.123-5
- Cisco 1751—c1700-k9o3sy7-mz.123-2.XE
- SAA target—c2600-ik9o3s3-mz.123-3

The IPSec head-end routers were Cisco 2651s with an Advanced Integration Module (AIM) hardware VPN module. This testing was not intended to scale test head-end performance capabilities. In a customer deployment, using IPSec head-ends with suitable performance characteristics aligned with the number of remote routers is advised.

An available Cisco1760 V3PN bundle (product number: CISCO1760-V3PN/K9) can be used instead of the Cisco 1751.

Reliable Static Routing Backup Using Object Tracking was first introduced in Cisco IOS version 12.3(2)XE.

# Summary

The Object Tracking feature of Cisco IOS Software provides a means to deploy both DSL and cable modems to the same remote location for increased availability. Because this feature uses SAA, a network manager can use its protocols and applications in addition to ICMP for verifying connectivity. One advantage to this configuration is its scalability; you can configure a primary and backup IPSec head-end independently from the SAA head-end router, and you can add additional SAA head-ends as required.