CHAPTER 6

Small Branch—Load Sharing on Dual Broadband Links

This solution describes a configuration for load sharing between dual broadband links for a small branch office deployment. It includes the following sections:

Customers frequently want to use both broadband connections when both are available while using the surviving link should one fail. Historically, customers deployed GRE tunnels and ran a routing protocol within the GRE tunnel to detect a link failure. However, deploying both load sharing and redundancy for an IPSec-only configuration can be accomplished using multiple instances of the Reliable Static Routing Backup Using Object Tracking feature along with the appropriate corresponding static routes.

This solution takes advantage of CEF/fast switching load sharing across two equal cost paths for the head-end-to-branch path to the remote subnet. From the perspective of the branch router, the load sharing is accomplished by defining specific routes to the corporate address space over the two broadband connections.

The example in this chapter does not show a split tunnel configuration, but the static routes included in the remote router configuration (**ip route 128.0.0.0 128.0.0.0 …**) are applicable regardless of whether split tunneling is configured or whether the remote router gains Internet access through the enterprise core. This route forwards packets for the upper "half" of the Internet address space out the DSL ISP connection and the lower "half" of the Internet address space is reached via the cable ISP, because the cable ISP is providing a default route using DHCP. In a split tunnel configuration, the packets destined for the Internet have their source IP address changed to the outside global address by Network Address Translation (NAT)/Port Network Address Translation (PNAT).

Note The global address is the IP address assigned to a host on the outside network by the owner of the host. The address is allocated from a globally routable address or network space.

Because this address space is obtained or allocated by the respective ISP, the return path of the flow is symmetrical.

The configuration can be easily adapted to use two DSL links terminated on a pair of DSL WAN Interface Card (WIC) interfaces, or a deployment that uses a pair of DSL routers provided by the ISP for broadband connectivity where the remote IPSec route of the enterprise customer obtains its default route and outside IP address using DHCP.

Topology

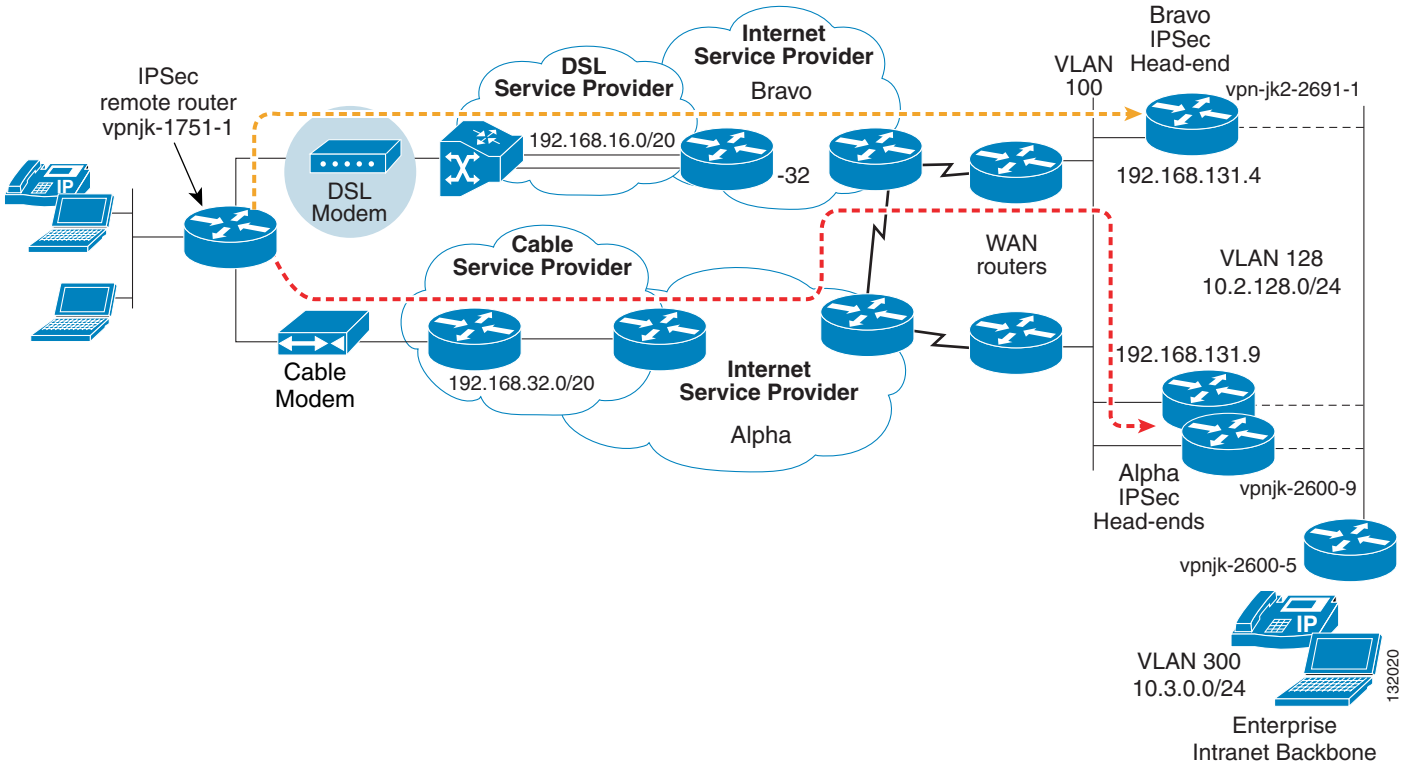
This section describes two WAN topologies. The first shows the use of cable and DSL. The cable connection learns an IP address using DHCP and the DSL connection obtains an address using PPPoE from the respective service providers. The second topology example shows the remote IPSec router learning an IP address using DHCP for both ISP links.

This section includes the following topics:

Cable (DHCP) and DSL (PPPoE)

Figure 6-1 shows the use of a cable and DSL service provider that in turn connects to two Tier-1 ISPs at the head-end location. The enterprise head-end WAN routers connect to each ISP to increase availability; however, in this example the SAA probe packets and data traffic flow through the primary ISP (Alpha) unless that WAN link fails, in which case the WAN router to the secondary ISP (Bravo) is used. Load sharing across the head-end WAN links to and from the ISP is a Border Gateway Protocol (BGP) configuration covered in the various documents on load sharing with BGP.

Figure 6-1 Load Sharing—Dual Broadband Links



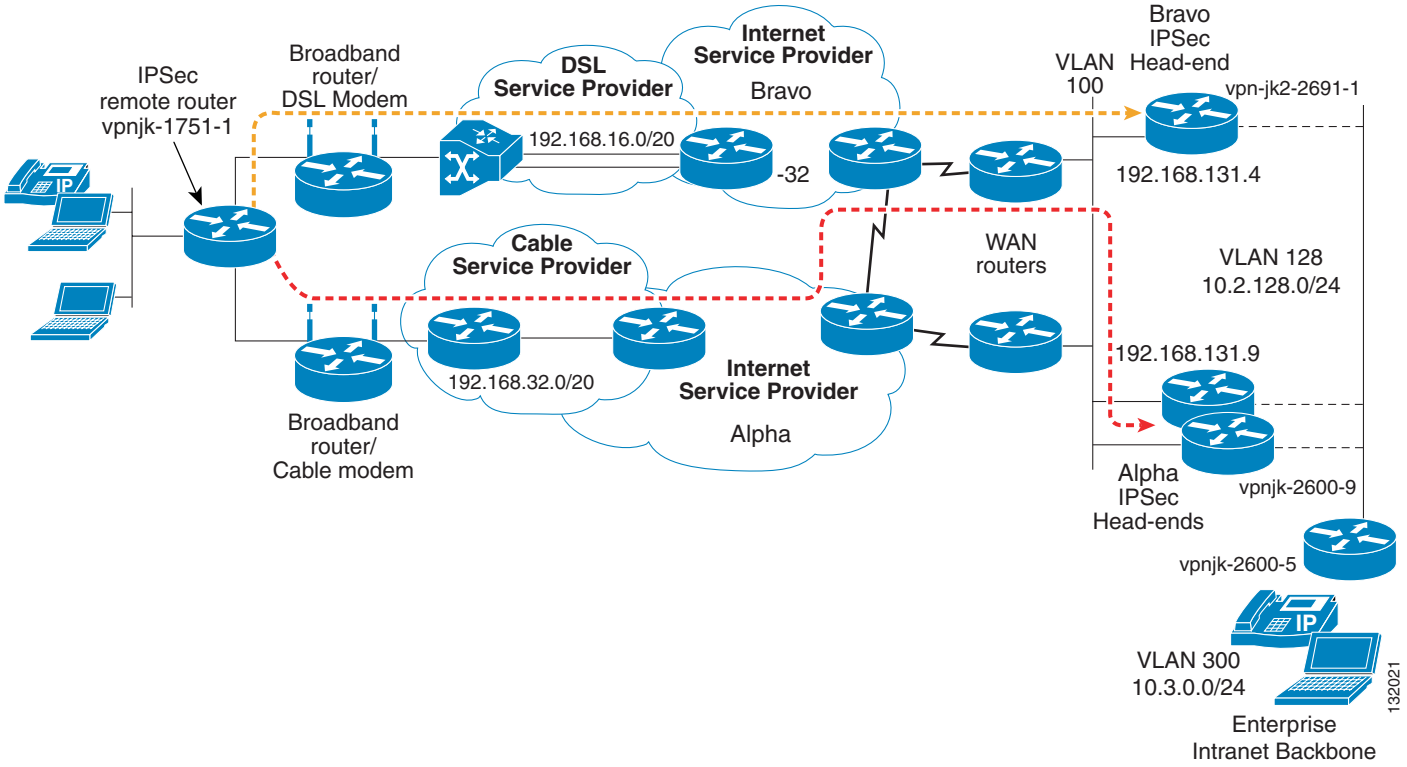
Load sharing between the two IPSec tunnels terminated between the remote router (vpnjk-1751-1), the Alpha IPSec head-end (vpnjk-2600-9), and the Bravo IPSec head-end (vpn-jk2-2691-1) is a function of the routing protocol configuration running on VLAN 128. In this example, the Alpha and Bravo IPSec head-end each redistribute the remote subnet learned by the dynamic crypto map into EIGRP with the same metric. Because of this, the enterprise intranet backbone router(s) see the remote subnet as two equal cost paths and inject both into the routing table. Because there are two paths in the routing table, load sharing is a function of the switching path of the enterprise intranet backbone router(s): Cisco Express Forwarding (CEF), fast, or process switching.

Load Sharing Behind Two Broadband Routers

Broadband service providers may deploy and manage their own customer premises equipment (CPE) router, and hand off an Ethernet interface with either a static IP network or a DHCP server function to provide the enterprise customer IPSec router with an IP address. In this situation, the previous topology of a PPPoE session terminated on a dialer interface and an Ethernet interface with DHCP enabled changes to one in which both upstream links are Ethernet with DHCP supplying the outside IP address and default route.

This topology is shown in Figure 6-2.

Figure 6-2 Load Sharing—Dual DHCP Broadband Links



In this topology, DSL links terminate the PPPoE session either on the broadband DSL router or on a separate broadband router, such as a Linksys EtherFast® Cable/DSL Router (BEFSR11). Similarly to cable deployments, the DHCP address is either supplied by the cable head-end router or a Linksys BEFSR11 or equivalent.

Failover/Recovery Time

This design implements two IPSec tunnels that are both up and active during normal operations. Both IPSec tunnels are used to transmit and receive data based on the routing configuration of the floating and tracked static routes on the remote router and the redistribution of the RRI-injected routes at the head-end location.

As such, failover and recovery time is a function of the SAA probe frequency, the track delay configuration, the IKE keepalive and DPD values, and the routing protocol updates at the head-end location.

The failover and recovery times are similar to the other designs documented in previous chapters of this guide.

V3PN QoS Service Policy

There are no specific changes to the QoS features of this configuration. However, because the design affords an opportunity to specify a preferred path based on destination IP address, it is beneficial to route voice packets to the link that has the greatest uplink bandwidth under normal conditions when both links are available. Recall that for voice, serialization delay can be an issue for links less than 768 kbps. In this illustration, the cable service provider is offering a 384 kbps uplink and the DSL uplink is 256 kbps.

Assuming that the enterprise IP phones and voice gateways are on the 10.0.0.0/8 address space, routing voice out the uplink with the higher bandwidth may be preferred.

```
ip route 10.0.0.0 255.0.0.0 0.0.0.0 name via_ISP_Alpha track 123
```

To offload packets for the upper "half" of the Internet address space out the DSL connection (the slower of the two links in this example), this static route is configured on the remote router.

```
ip route 128.0.0.0 128.0.0.0 Dialer1 name via_ISP_Bravo track 11
```

Destinations not matched by either of these two routes follow the default route injected into the routing table using DHCP. This route in the example is learned from the cable ISP.

The return path of the voice packets depends on the metrics of the redistributed static route injected by the IPSec RRI configuration in the head-end crypto maps.

It is important that the QoS service policies are appropriately configured for different link speeds. Note that the shaper values shown in the configuration reflect values appropriate for the uplink speed and Layer 2 (cable/DOCSIS or DSL/ATM-PPPoE-AAL5) overhead.

Implementation and Configuration

This section describes the implementation and configuration for the load sharing on dual broadband links solution, and includes the following topics:

Remote 1751 Router (DHCP and PPPoE)

The following configuration is for the remote Cisco 1751 router with DHCP and PPPoE:

```
version 12.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
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
no ip cef          # See caveats section, CEF must be disabled
ip audit notify log
ip audit po max-events 100
ip dhcp-client default-router distance 239
!
!   Track 11 (decimal 11 is 0xB, B for Bravo) will track the ISP Bravo path
!
track 11 rtr 11 reachability
 delay down 60 up 5
!
!   Track 123 will track the ISP Alpha path
!
track 123 rtr 23 reachability
 delay down 60 up 5
!
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir
!
!
!   For the ISP Alpha IPSec peer (192.168.131.9) using Certificates for authentication
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
!
!   For the ISP Bravo IPSec peer (102.168.131.4) using Aggressive mode pre-shared keys
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
!
!   These crypto maps are identical except for the peer's IP address
!
crypto map ISP_Alpha 1 ipsec-isakmp
 description ISP Alpha Connection
 set peer 192.168.131.9
 set transform-set 3DES_SHA_TUNNEL
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
crypto map ISP_Bravo 1 ipsec-isakmp
 description ISP Bravo connection
 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 Ethernet1/0
 description To CABLE MODEM
 bandwidth 384
 ip dhcp client route track 123
 ip address dhcp
 service-policy output Shaper-cable
 no ip route-cache#           See caveats section, Fast Switching must be disabled
 ip tcp adjust-mss 542
 load-interval 30
 half-duplex
 crypto map ISP_Alpha
!
interface Dialer1
 description Outside
 bandwidth 256
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 no ip route-cache#           See caveats section, Fast Switching must be disabled
 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 [removed]
 ppp ipcp dns request
 ppp ipcp wins request
 crypto map ISP_Bravo
!
ip classless
!
!   This route sends traffic for the upper half of the IPV4
!   address space out the Dialer interface
!
ip route 128.0.0.0 128.0.0.0 Dialer1 name via_ISP_Bravo track 11
!
!   This route sends the 10.0.0.0 network (Enterprise's internal
!   address space in this example out the Cable interface
!
ip route 10.0.0.0 255.0.0.0 0.0.0.0 name via_ISP_Alpha track 123
!
!   Gateway of last resort if default learned via DHCP is unavailable
!
ip route 0.0.0.0 0.0.0.0 Dialer1 240 name Last_resort
!
!   Host route forcing Bravo IPSec head-end out Dialer Interface
!
ip route 192.168.131.4 255.255.255.255 Dialer1 name via_ISP_Bravo
!
```

```
!   Route 192.168.131.8 and 192.168.131.9 to the DHCP learned gateway address
!
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
!
!   There are two SAA probes configured, one uses ICMP (ping) the other UDP echo.
!   Both source off the inside IP address, and the destination is their respective
!   IPSec head-end routers. There is one probe for each path to the IPSec head-end
!   routers.
!
rtr responder
!
rtr 11
 type echo protocol ipIcmpEcho 192.168.131.4 source-ipaddr 10.0.68.5
 tos 192
 timeout 500
 tag For_ISP_Bravo_path
 frequency 15
rtr schedule 11 start-time now life forever
!
rtr 23
 type udpEcho dest-ipaddr 192.168.131.9 dest-port 57005 source-ipaddr 10.0.68.5
source-port 48879
 tos 192
 timeout 1000
 owner TRACK123
 tag For_ISP_Alpha_path
 frequency 20
 lives-of-history-kept 1
 buckets-of-history-kept 10
 filter-for-history failures
rtr schedule 23 start-time now life forever
!
line con 0
 exec-timeout 60 0
line aux 0
line vty 0 4
 password [removed]
 login
!
ntp server 192.168.130.1
!
end
```

Remote 1751 Router (DHCP and DHCP)

To implement a configuration with two DHCP interfaces, the remote 1751 router configuration changes slightly from the previous example. The dialer interface is eliminated and changes are made to the static routes in the configuration. The static routes shown in the configuration are all that is required, because a default route is learned on both outside interfaces.

```
interface Ethernet0/0
 description to DSL MODEM / Router
 bandwidth 256
 ip dhcp client route track 11
 ip address dhcp
 service-policy output Shaper-DSL
 no ip route-cache
 load-interval 30
 half-duplex
 crypto map ISP_Bravo
!
!   The Bravo IPSec head-end next hop address with be the DHCP learned gateway
!   on Ethernet 0/0
!
ip route 192.168.131.4 255.255.255.255 Ethernet0/0 dhcp
!
!   The Alpha IPSec head-end next hop address will be the DHCP learned gateway
!   on Ethernet 1/0
!
ip route 192.168.131.9 255.255.255.255 Ethernet1/0 dhcp
!
end
```

Alpha IPSec Head-end

The following is the Alpha IPSec head-end configuration:

```
!
! 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 [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 ect-msca 172.26.179.237
ip host harry 172.26.176.10
!
ip audit notify log
ip audit po max-events 100
```

```
!
!   This head-end is using Certificates and a dynamic crypto map
!
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 610BE2E400000000001F 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
 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
!
!   Compare the metric of this head-end with the Bravo IPSec head-end
!       they should be the same if you want the Enterprise Intranet Router to
!   see two equal cost paths for the remote subnets.
!
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
 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
!
!   This router must respond to SAA probes from the remote routers.
!
rtr responder
!
line con 0
 exec-timeout 120 0
 password [removed]
line aux 0
line vty 0 4
 password [removed]
 login
!
ntp server 192.168.130.1
!
end
```

Bravo IPSec Head-end

The following is the Bravo IPSec head-end configuration:

```
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-end-marker
!
logging buffered 65536 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
!
!
ip cef
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
!
!   This router has a Certificate configured, but is not being used
!   in this example
!
```

```
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 FastEthernet0/1.128
 description Inside Interface
 encapsulation dot1Q 128
 ip address 10.2.128.4 255.255.255.0
!
!
```

```
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 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
!
!
!   This router must respond to SAA probes from the remote routers.
!
rtr responder
!
line con 0
 exec-timeout 120 0
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 login
 transport preferred all
 transport input all
 transport output all
!
ntp server 192.168.130.1
!
end
```

Enterprise Intranet Router

The following is the enterprise intranet router configuration:

```
! System image file is "flash:c2600-ik9o3s-mz.123-3"
version 12.3
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service tcp-small-servers
!
hostname vpnjk-2600-5
!
boot-start-marker
boot-end-marker
!
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
ip cef
!
```

```
!
interface FastEthernet0/1
 description dot1q
 no ip address
 ip route-cache flow
 load-interval 30
 duplex auto
 speed auto
!
interface FastEthernet0/1.128
 encapsulation dot1Q 128
 ip address 10.2.128.5 255.255.255.0
!
interface FastEthernet0/1.300
 encapsulation dot1Q 300
 ip address 10.3.0.5 255.255.255.0
!
router eigrp 100
 network 10.0.0.0
 no auto-summary
 no eigrp log-neighbor-warnings
!
no ip http server
no ip http secure-server
rtr responder
!
line con 0
 exec-timeout 300 0
 password [removed]
 login
line aux 0
line vty 0 4
 password [removed]
 login
!
ntp server 192.168.130.1
!
end
```

Show Commands

This section describes the results of the **show** command, and includes the following sections:

- Enterprise Intranet Router
- Remote 1751 Router (DHCP and PPPoE Configuration)
- Remote 1751 Router (DHCP and DHCP Configuration)

Enterprise Intranet Router

Note the **redistribute** command on the IPSec routers; the minimum bandwidth is specified as 384 kbps for both paths to the remote router. If these are both broadband links, which are commonly asymmetrical speeds, the downlink bandwidth may actually be much higher.

```
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 10.2.128.4 on FastEthernet0/1.128, 5d00h ago
  Routing Descriptor Blocks:
  * 10.2.128.4, from 10.2.128.4, 5d00h 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
    10.2.128.9, from 10.2.128.9, 5d00h 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

vpnjk-2600-5#show ip cef 10.0.68.0 255.255.255.128 internal
10.0.68.0/25, version 1795, epoch 0, per-destination sharing
0 packets, 0 bytes
  Flow: AS 0, mask 25
  via 10.2.128.4, FastEthernet0/1.128, 0 dependencies # Bravo IPSec head-end
    traffic share 1
    next hop 10.2.128.4, FastEthernet0/1.128
    valid adjacency
  via 10.2.128.9, FastEthernet0/1.128, 0 dependencies # Alpha IPSec head-end
    traffic share 1
    next hop 10.2.128.9, FastEthernet0/1.128
    valid adjacency

  0 packets, 0 bytes switched through the prefix
  tmstats: external 0 packets, 0 bytes
           internal 0 packets, 0 bytes
  Load distribution: 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 (refcount 1)

  Hash  OK  Interface                 Address         Packets
  1     Y   FastEthernet0/1.128       10.2.128.4            0
  2     Y   FastEthernet0/1.128       10.2.128.9            0
  3     Y   FastEthernet0/1.128       10.2.128.4            0
  4     Y   FastEthernet0/1.128       10.2.128.9            0
  5     Y   FastEthernet0/1.128       10.2.128.4            0
  6     Y   FastEthernet0/1.128       10.2.128.9            0
  7     Y   FastEthernet0/1.128       10.2.128.4            0
  8     Y   FastEthernet0/1.128       10.2.128.9            0
  9     Y   FastEthernet0/1.128       10.2.128.4            0
  10    Y   FastEthernet0/1.128       10.2.128.9            0
  11    Y   FastEthernet0/1.128       10.2.128.4            0
  12    Y   FastEthernet0/1.128       10.2.128.9            0
  13    Y   FastEthernet0/1.128       10.2.128.4            0
  14    Y   FastEthernet0/1.128       10.2.128.9            0
  15    Y   FastEthernet0/1.128       10.2.128.4            0
  16    Y   FastEthernet0/1.128       10.2.128.9            0
```

Remote 1751 Router (DHCP and PPPoE Configuration)

To demonstrate the load sharing from the perspective of the remote router, the lab topology generates test traffic using a traffic generator node (TGN) on the Ethernet network of the remote Cisco 1751.

Five streams are generated, two to a destination network of 10.2.128.5. The remaining three streams are destined for 191.255.0.1. The goal is to see traffic for 10.2.128.5 switched out the Alpha ISP (cable) and the other three streams out the Beta ISP, which is DSL.

```
vpnjk-2(TGN:ON,Fa0/1:5/5)#sh ip
```

```
Summary of IP traffic streams on FastEthernet0/1
  ts#     tos  len   id frag ttl protocol chksm source          destination
    1 TCP  48  552 0000 0000  60     6     6E86 10.0.68.2       191.255.0.1
    2 UDP  00  328 0000 0000  60    17     6FA3 10.0.68.2       191.255.0.1
    3 UDP  B8   60 0000 0000  60    17     A5F0 10.0.68.2       10.2.128.5
    4 TCP  68   80 0000 0000  60     6     A637 10.0.68.2       10.2.128.5
    5 UDP  88  628 0000 0000  60    17     6DEF 10.0.68.2       191.255.0.1


vpnjk-2(TGN:ON,Fa0/1:5/5)#show rate

The rates are since the last rate change during traffic generation.

Summary of traffic stream rates on FastEthernet0/1
                                                        measured
  ts# template state repeat   interval/rate        interval/rate   packets_sent
    1 TCP        on     1                10 pps            9.999        1880073
    2 UDP        on     1                10 pps            9.999        2108424
    3 UDP        on     1                50 pps           49.999        5935746
    4 TCP        on     1                10 pps            9.999        1129352
    5 UDP        on     1                10 pps            9.999         291878
Totals for FastEthernet0/1                               89.999       11345473
```

To verify the routing, show the routes for the target networks.

```
vpnjk-1751-1#show ip route 191.255.0.1
Routing entry for 128.0.0.0/1, supernet
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Dialer1
      Route metric is 0, traffic share count is 1


vpnjk-1751-1#show ip route 10.0.0.0
Routing entry for 10.0.0.0/8, 2 known subnets
  Attached (1 connections)
  Variably subnetted with 2 masks

S       10.0.0.0/8 [1/0] via 0.0.0.0
C       10.0.68.0/25 is directly connected, FastEthernet0/0

vpnjk-1751-1#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 239, metric 0, candidate default path
  Routing Descriptor Blocks:
  * 192.168.33.1
      Route metric is 0, traffic share count is 1
```

In total, the TGN is generating 90 pps; 30 pps for the DSL provider and 60 pps for the cable provider.

```
vpnjk-1751-1#show interfaces virtual-access 1 | inc rate
  Queueing strategy: fifo
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 139000 bits/sec, 30 packets/sec

vpnjk-1751-1#show interfaces ethernet 1/0 | inc rate
  Queueing strategy: fifo
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 62000 bits/sec, 60 packets/sec
```

Fail Alpha ISP Network

Now simulate a failure in the Alpha ISP network. The remote 1751 crypto tunnel goes down and subsequently the SAA probes to the tracked object through that tunnel fail.

```
vpnjk-1751-1#
Mar  9 16:50:07.216 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.9:500       Id: vpnjk-2600-9.ese.cisco.com
Mar  9 16:50:23.340 est: Track: 123 Down change delayed for 60 secs
Mar  9 16:51:23.341 est: Track: 123 Down change delay expired
Mar  9 16:51:23.341 est: Track: 123 Change #8 rtr 23, reachability Up->Down
```

Following the failure, the DHCP-learned default route is removed from the routing table and the floating static to 0.0.0.0 through the dialer interface is used instead.

```
vpnjk-1751-1#show ip route | beg Gate
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.26.0.0/32 is subnetted, 2 subnets
S       172.26.176.10 [1/0] via 172.26.156.1, FastEthernet0/0
S       172.26.179.237 [1/0] via 172.26.156.1, FastEthernet0/0
     192.168.131.0/24 is variably subnetted, 2 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
     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 is directly connected, Dialer1
S    128.0.0.0/1 is directly connected, Dialer1
```

Observe the interface counters; there are 90 pps being sent out the DSL Virtual-Access 1 interface but only 83 pps or 181,000 bps out the PPPoE-enabled Ethernet 0/0 interface. The QoS service policy on this interface is dropping packets because the shaped rate of this interface is 184,200.

```
vpnjk-1751-1#show int | inc output rate|is up
Ethernet0/0 is up, line protocol is up
  30 second output rate 181000 bits/sec, 83 packets/sec
FastEthernet0/0 is up, line protocol is up
  30 second output rate 1000 bits/sec, 2 packets/sec
Ethernet1/0 is up, line protocol is up
  30 second output rate 0 bits/sec, 0 packets/sec
Virtual-Access1 is up, line protocol is up
  5 minute output rate 205000 bits/sec, 90 packets/sec
Dialer1 is up, line protocol is up (spoofing)
  30 second output rate 0 bits/sec, 0 packets/sec
Virtual-Access1 is up, line protocol is up
  5 minute output rate 205000 bits/sec, 90 packets/sec
```

This example shows a proper re-routing over the surviving DSL interface with QoS managing the available bandwidth.

Fail Bravo ISP Network

Now simulate a failure of the other ISP network.

```
vpnjk-1751-1#
Mar 10 10:33:39.825 est: Track: 11 Down change delayed for 60 secs
vpnjk-1751-1#
Mar 10 10:33:59.905 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.4:500       Id: vpn-jk-2691-1.ese.cisco.com
Mar 10 10:34:39.824 est: Track: 11 Down change delay expired
Mar 10 10:34:39.824 est: Track: 11 Change #2 rtr 11, reachability Up->Down
vpnjk-1751-1#
```

Observe the routing table and the interface counters:

```
vpnjk-1751-1#show ip route | beg Gate
Gateway of last resort is 192.168.33.1 to network 0.0.0.0

     172.26.0.0/32 is subnetted, 2 subnets
S       172.26.176.10 [1/0] via 172.26.156.1, FastEthernet0/0
S       172.26.179.237 [1/0] via 172.26.156.1, FastEthernet0/0
     192.168.131.0/24 is variably subnetted, 2 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
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       10.0.0.0/8 [1/0] via 0.0.0.0
C       10.0.68.0/25 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

vpnjk-1751-1#show int | inc output rate|is up
Ethernet0/0 is up, line protocol is up
  30 second output rate 0 bits/sec, 0 packets/sec
FastEthernet0/0 is up, line protocol is up
  30 second output rate 1000 bits/sec, 2 packets/sec
Ethernet1/0 is up, line protocol is up
  30 second output rate 200000 bits/sec, 90 packets/sec
Virtual-Access1 is up, line protocol is up
  5 minute output rate 0 bits/sec, 0 packets/sec
Dialer1 is up, line protocol is up (spoofing)
  30 second output rate 0 bits/sec, 0 packets/sec
Virtual-Access1 is up, line protocol is up
  5 minute output rate 0 bits/sec, 0 packets/sec
vpnjk-1751-1#
```

This confirms that all traffic is using the surviving link.

Remote 1751 Router (DHCP and DHCP Configuration)

This configuration requires disabling CEF and fast switching, as documented in the Caveats section. With the same traffic profile as demonstrated previously, when both links are up, there is an equal distribution across both uplinks. Process switching load shares per packet, and this configuration relies on both default routes learned by DHCP on separate interfaces to be in the routing table with an administrative distance of 239 (equal costs).

On each outside DHCP interface, the default route learned using DHCP is being tracked **(ip dhcp client route track …).**

```
vpnjk-1751-1#sh rtr operational-state | inc return code|Entry
Entry number: 11
```

```
Latest operation return code: OK# SAA probe for ISP Bravo is successful
Entry number: 23
Latest operation return code: OK# SAA probe for ISP Alpha is successful
```

Because both probes are successful, both default routes are in the routing table.

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

     192.168.131.0/32 is subnetted, 2 subnets
S       192.168.131.9 [1/0] via 192.168.33.1
S       192.168.131.4 [1/0] via 192.168.18.1
     10.0.0.0/25 is subnetted, 1 subnets
C       10.0.68.0 is directly connected, FastEthernet0/0
C    192.168.18.0/24 is directly connected, Ethernet0/0
C    192.168.33.0/24 is directly connected, Ethernet1/0
S*   0.0.0.0/0 [239/0] via 192.168.33.1
                [239/0] via 192.168.18.1

vpnjk-1751-1#show interfaces | inc up|rate
Ethernet0/0 is up, line protocol is up
  Half-duplex, 10BaseT
  Queueing strategy: fifo
  30 second input rate 2000 bits/sec, 2 packets/sec
  30 second output rate 99000 bits/sec, 45 packets/sec# Half packets output E0/0
FastEthernet0/0 is up, line protocol is up
  Full-duplex, 100Mb/s, 100BaseTX/FX
  Queueing strategy: fifo
  30 second input rate 161000 bits/sec, 90 packets/sec
  30 second output rate 1000 bits/sec, 1 packets/sec
Ethernet1/0 is up, line protocol is up
  Half-duplex, 10BaseT
  Queueing strategy: fifo
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 99000 bits/sec, 45 packets/sec# Half packets output E1/0
```

Fail Alpha ISP Network

Now fail a component of the Alpha ISP network and observe the results:

```
Mar 11 14:49:19.825 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.9:500       Id: vpnjk-2600-9.ese.cisco.com
Mar 11 14:49:24.345 est: Track: 123 Down change delayed for 60 secs
Mar 11 14:50:24.344 est: Track: 123 Down change delay expired
Mar 11 14:50:24.344 est: Track: 123 Change #2 rtr 23, reachability Up->Down
vpnjk-1751-1#
vpnjk-1751-1#show ip route | beg Gate
Gateway of last resort is 192.168.18.1 to network 0.0.0.0


     192.168.131.0/32 is subnetted, 2 subnets
S       192.168.131.9 [1/0] via 192.168.33.1
S       192.168.131.4 [1/0] via 192.168.18.1
     10.0.0.0/25 is subnetted, 1 subnets
C       10.0.68.0 is directly connected, FastEthernet0/0
C    192.168.18.0/24 is directly connected, Ethernet0/0
C    192.168.33.0/24 is directly connected, Ethernet1/0
S*   0.0.0.0/0 [239/0] via 192.168.18.1
```

Observing the above, only the surviving default route remains in the routing table and no packets are sent out the Alpha (Ethernet 1/0) interface. Note that only 84 pps are sent out the Beta (Ethernet0/0) interface because of lack of bandwidth for the available load.

```
vpnjk-1751-1#show interface | inc up|rate
Ethernet0/0 is up, line protocol is up
  Half-duplex, 10BaseT
  Queueing strategy: fifo
  30 second input rate 1000 bits/sec, 2 packets/sec
  30 second output rate 179000 bits/sec, 84 packets/sec
FastEthernet0/0 is up, line protocol is up
  Full-duplex, 100Mb/s, 100BaseTX/FX
  Queueing strategy: fifo
  30 second input rate 161000 bits/sec, 90 packets/sec
  30 second output rate 1000 bits/sec, 2 packets/sec
Ethernet1/0 is up, line protocol is up
  Half-duplex, 10BaseT
  Queueing strategy: fifo
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
```

Connectivity is maintained; however, the QoS policy manages the available bandwidth so that voice and other critical applications are guaranteed their minimum bandwidth.

Fail Bravo ISP Network

Now fail the Bravo ISP network and verify the primary interface is used for all traffic.

```
Mar 11 14:43:04.343 est: Track: 11 Down change delayed for 60 secs
Mar 11 14:43:13.443 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.4:500       Id: vpn-jk-2691-1.ese.cisco.com
Mar 11 14:44:04.342 est: Track: 11 Down change delay expired
Mar 11 14:44:04.342 est: Track: 11 Change #4 rtr 11, reachability Up->Down
vpnjk-1751-1#
vpnjk-1751-1#show ip route | begin Gate
Gateway of last resort is 192.168.33.1 to network 0.0.0.0

     192.168.131.0/32 is subnetted, 2 subnets
S       192.168.131.9 [1/0] via 192.168.33.1
S       192.168.131.4 [1/0] via 192.168.18.1
     10.0.0.0/25 is subnetted, 1 subnets
C       10.0.68.0 is directly connected, FastEthernet0/0
C    192.168.18.0/24 is directly connected, Ethernet0/0
C    192.168.33.0/24 is directly connected, Ethernet1/0
S*   0.0.0.0/0 [239/0] via 192.168.33.1
```

In the following display, it is apparent that no packets are sent out the E0/0 or Bravo ISP interface, while all 90 pps are forwarded out the Alpha ISP interface.

```
vpnjk-1751-1#show interface | inc up|rate
Ethernet0/0 is up, line protocol is up
  Half-duplex, 10BaseT
  Queueing strategy: fifo
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
FastEthernet0/0 is up, line protocol is up
  Full-duplex, 100Mb/s, 100BaseTX/FX
  Queueing strategy: fifo
  30 second input rate 161000 bits/sec, 90 packets/sec
```

```
  30 second output rate 1000 bits/sec, 2 packets/sec
Ethernet1/0 is up, line protocol is up
  Half-duplex, 10BaseT
  Queueing strategy: fifo
  30 second input rate 2000 bits/sec, 2 packets/sec
  30 second output rate 196000 bits/sec, 90 packets/sec
```

These examples demonstrate that load sharing can be accomplished when both links are available, and that connectivity to the site can be maintained if one link fails.

Cisco IOS Versions Tested

The following versions of Cisco IOS were tested:

- Remote 1751—c1700-k9o3sy7-mz.123-2.XE, c1700-k9o3sy7-mz.123-2.XF
- IPSec head-ends (Bravo)—c2691-ik9o3s-mz.123-5
- IPSec head-ends (Alpha)—c2600-ik9o3s-mz.122-11.T5

Caveats

This section describes the issues that were encountered during testing, and includes the following topics:

- CEF Issue
- Fast Switching Issue

Both CEF and fast switching must be disabled (must process switch) on the remote router for load sharing to function properly when running Cisco IOS Release 12.3(2)XE. In the PPPoE/DHCP configuration using Cisco IOS Release 12.3(2)XF, process switching must also be enabled. Table 6-1 shows the proper switching path for the solution to function in the two configurations on the two Cisco IOS releases tested.

Table 6-1 Switching Path Table

Configuration	12.3(2)XE	12.3(2)XF
DHCP/DHCP	Must process switch	Can CEF or fast switch
PPPoE/DHCP	Must process switch	Must process switch

This design is impacted by these two issues:

- Static recursive route pointing at default route is not CEF switched (CSCed29811)
- IPSec packets are fast switched on wrong interface with recursive route (CSCed95604)

CEF Issue

During testing, it was discovered that CEF must be disabled on the remote router for packets to follow any static routes with the default (0.0.0.0) network as the next hop. This type of route requires a *recursive lookup*, which means that resolving the appropriate output interface for the route to 10.2.128.5 requires also resolving the next hop for the 0.0.0.0/0 network.

In this example, a constant 10 pps is sent to destination IP address of 10.2.128.5. In looking at the routing table, that destination should match the route 10.0.0.0/8, which is a recursive route to the default network learned using DHCP on the Ethernet 1/0 interface.

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


     192.168.131.0/24 is variably subnetted, 2 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
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       10.0.0.0/8 [1/0] via 0.0.0.0
C       10.0.68.0/25 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
S    128.0.0.0/1 is directly connected, Dialer1
```

When CEF is disabled, 10 pps is switched out Ethernet 1/0.

```
vpnjk-1751-1(config)#no ip cef
vpnjk-1751-1(config)#end

vpnjk-1751-1#show int e 1/0 | inc address|rate
  Hardware is PQUICC Ethernet, address is 0004.dd0b.c783 (bia 0004.dd0b.c783)
  Internet address is 192.168.33.12/24
  Queueing strategy: fifo
  30 second input rate 1000 bits/sec, 1 packets/sec
  30 second output rate 10000 bits/sec, 10 packets/sec
```

When CEF is enabled, and you wait at least 30 seconds for the load interval value to show an accurate value, you see that CEF drops the packets and does not switch them to 10.2.128.5.

```
vpnjk-1751-1(config)#ip cef
vpnjk-1751-1(config)#end

vpnjk-1751-1#show int e 1/0 | inc address|rate
  Hardware is PQUICC Ethernet, address is 0004.dd0b.c783 (bia 0004.dd0b.c783)
  Internet address is 192.168.33.12/24
  Queueing strategy: fifo
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
```

Fast Switching Issue

In addition to disabling CEF, fast switching must also be disabled on the remote router for packets to be properly switched over both paths. This issue is related to CSCed95604. Fast switching is enabled on the output interfaces, as shown in the example below:

```
vpnjk-1751-1#show ip int | inc swi|is up
Ethernet0/0 is up, line protocol is up
FastEthernet0/0 is up, line protocol is up
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
```

```
  IP Flow switching is enabled
  IP CEF switching is disabled
  IP Flow switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
Ethernet1/0 is up, line protocol is up
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
Virtual-Access1 is up, line protocol is up
Dialer1 is up, line protocol is up
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disab
```

Note that Ethernet 1/0 has no output packets:

```
vpnjk-1751-1#show int | inc rate|is up
Ethernet0/0 is up, line protocol is up
  Queueing strategy: fifo
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 182000 bits/sec, 84 packets/sec
FastEthernet0/0 is up, line protocol is up
  Queueing strategy: fifo
  30 second input rate 161000 bits/sec, 90 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
Ethernet1/0 is up, line protocol is up
  Queueing strategy: fifo
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
Virtual-Access1 is up, line protocol is up
  Queueing strategy: fifo
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 187000 bits/sec, 90 packets/sec
Dialer1 is up, line protocol is up (spoofing)
  Queueing strategy: weighted fair
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
Virtual-Access1 is up, line protocol is up
  Queueing strategy: fifo
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 187000 bits/sec, 90 packets/sec
vpnjk-1751-1#
```

This is true even though the default route learned using DHCP is in the routing table.

```
vpnjk-1751-1# show ip route | beg Gate
Gateway of last resort is 192.168.33.1 to network 0.0.0.0


     192.168.131.0/24 is variably subnetted, 2 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
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

```
S       10.0.0.0/8 [1/0] via 0.0.0.0
C       10.0.68.0/25 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
S    128.0.0.0/2 is directly connected, Dialer1
```

As shown by the fast cache, the destination prefix of 10.2.128.0/25 has a next hop of 192.168.33.1.

```
vpnjk-1751-1# show ip cache
IP routing cache 5 entries, 1020 bytes
   139 adds, 134 invalidates, 0 refcounts
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 01:21:28 ago

Prefix/Length           Age       Interface       Next Hop
10.2.128.0/25           00:40:26  Ethernet1/0     192.168.33.1
191.255.0.1/32          00:50:48  Dialer1         191.255.0.1
192.168.130.0/24        00:16:18  Ethernet1/0     192.168.33.1
192.168.131.4/32        00:37:26  Dialer1         192.168.131.4
192.168.131.9/32        00:01:39  Ethernet1/0     192.168.33.1
```

Note Note from the previous interface display that no packets are output on Ethernet 1/0. This issue was filed as CSCed95604.

Summary

A natural desire of network managers is to load share on both WAN links if both are operational, and to be able to maintain connectivity on the remaining link should one fail. This design provides that capability without the use of a routing protocol and GRE tunnels. It is particularly suited to the small branch location in retail or customer service industries, with or without QoS enabled to support voice.