Small Branch—DSL with ISDN Backup

Some customer networks are characterized by large numbers of remote branch offices or locations that have relatively low bandwidth requirements, such as fast food restaurants, home/auto insurance agent offices, the hospitality/hotel industry, and banking. A high priority for these organizations is to reduce the monthly expenditure for each individual location; saving $50 USD a month in WAN connectivity costs for a deployment of 3,000 branch offices totals an annual savings of $1.8 million USD.

Enterprises are transitioning to DSL from traditional Frame Relay deployments to reduce monthly expenses and to increase available bandwidth. However, repair mean time for DSL-deployed locations may be 48 hours or more, and an outage of this duration may be unacceptable. This chapter describes a design that uses broadband DSL service with ISDN backup with encryption on both the primary and backup link.

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

- Low recurring costs for WAN access
- Dial backup support required for branch availability
- No multiprotocol or IP multicast requirements
- A highly scalable, redundant, and cost effective head-end IPSec termination
- Encryption required for broadband and backup link

This chapter includes the following sections:

- Solution Characteristics
- Topology
- Failover/Recovery Time
- V3PN QoS Service Policy for Basic Rate ISDN
- Performance Results
- Implementation and Configuration
- Cisco IOS Versions Tested
- Caveats
- Debugging
- Summary
Solution Characteristics

This section describes the characteristics of the DSL with ISDN backup solution, and includes the following topics:

- Traffic Encapsulated in IPSec
- Redundant IPSec Head-ends
- IPSec Peering
- GRE Tunnel Controls Dial Backup
- Digital Certificates and Dynamic Crypto Maps
- Reverse Route Injection
- Remote IP Routing—Floating Static and Specific Routes
- Head-end IP Routing Requirements

Traffic Encapsulated in IPSec

IPSec is used for confidentiality, authentication, and data integrity. The assumption is that GRE tunnels are not required for transporting multiprotocol or IP multicast data. Using an IPSec-only configuration with no GRE and no routing protocol permits more remote sites to be connected to a pair of head-end VPN routers than is the case when GRE and a routing protocol are configured between the remote and head-end routers. Avoiding the overhead of the GRE headers conserves WAN bandwidth both at the branch and at the head-end locations.

Redundant IPSec Head-ends

This design uses multiple IPSec head-end peers defined in the remote routers. IKE keepalive/Dead Peer Detection (DPD) are configured to switch to a surviving peer in the event of an IPSec head-end failure. The IPSec VPN High Availability Enhancements feature, which uses Hot Standby Router Protocol (HSRP) and IPSec, can also be used on the head-end IPSec routers. As a design goal, the dial backup should not be triggered in the event of a head-end IPSec failure. The surviving IPSec peer is configured to recover the IPSec tunnel to avoid unnecessary dial backup initiations. This saves any per-minute ISDN charges and enhances network stability.

IPSec Peering

The remote routers use the same head-end IPSec peers for both the primary and backup IPSec security associations. These head-end peers are identified by different IP addresses in the primary crypto map and the backup crypto map. This allows including static routes in the remote router configuration to block IKE packets from reaching the backup head-end peers when the primary path connectivity is restored. The backup IPSec security associations (SAs) are deleted as is the Reverse Route Injection (RRI) static route in the head-end for the backup path.
**GRE Tunnel Controls Dial Backup**

This design uses a GRE tunnel between each branch router, and one or more head-end routers dedicated to terminating GRE tunnels. The GRE tunnel in this design controls the function of the Basic Rate ISDN interface for dial backup in the event of a WAN/Internet failure. The GRE interface is configured with **backup interface BRI0**. If GRE keepalives are missed because of a WAN failure, the tunnel interface goes down and the BRI0 interface is brought up. The GRE tunnel does not carry any end-user network traffic, but is used strictly for sensing the loss of the primary path.

GRE keepalives are configured on the GRE interface; however, no IP addresses need to be allocated to the GRE tunnel. The branch router GRE tunnel interface is sourced off the inside Ethernet interface. In the examples described in this chapter, a Cisco 1712 router is used and the inside interface is defined as a VLAN interface, because the Cisco 1712 includes a built-in switch. The branch router GRE tunnel destination is a router on the head-end LAN dedicated solely for tunnel termination.

In this example, the GRE head-end router resides on the same subnet as the IPSec head-ends. It can be a “router on a stick” because no data traffic flows through the GRE head-end. The only network traffic of the GRE head-end router is the GRE keepalive packets it generates. In the configuration example described in this chapter, the keepalive hello interval is shown at 20 seconds with three retries. Because the remote router is configured with two IPSec peers and IKE keepalives, the GRE hello and dead interval should be high enough to allow a head-end IPSec router to fail and the remote routers to establish new IPSec SAs to the surviving IPSec head-end before the GRE dead interval expires.

**Digital Certificates and Dynamic Crypto Maps**

For both the primary and backup connections, digital certificates and dynamic crypto maps are used on the IPSec head-end routers. There is no requirement for a fixed IP address at the branch router. Business DSL can be purchased with either dynamic or static IP addressing. The dynamic IP addressing option is less expensive and helps to reduce recurring monthly costs. The configuration examples illustrate the use of PPP over Ethernet (PPPoE). IKE keepalive/DPD are configured on both the head-end and branch routers.

**Reverse Route Injection**

RRI is used on the IPSec head-end routers. The remote router advertises a more specific subnet for the primary WAN connection than is advertised for the backup connection.

---

**Note**

When using dynamic crypto maps, the access list referenced by the remote crypto map is created dynamically on the head-end IPSec router with the source and destination references swapped. The RRI logic inserts a static route into the routing table with the mask configured on the remote router.

IP route selection is always based on the longest prefix match in the routing table. By configuring a more specific access control list (ACL) in the crypto map for the primary interface than is used for the backup interface, packets destined for the remote location prefer the most specific route and avoid the backup IPSec tunnel if both the backup and primary IPSec tunnels are active.

Note that the inside interface of the remote Cisco 1712 router is configured with a /25 mask, the primary crypto map is configured with a /25 mask, and the backup crypto map is configured with a /24 mask. This configuration follows the concept of longest prefix match and allows the primary path to be preferred when both dynamic crypto maps are active on the head-end IPSec routers.
interface Vlan1
  description Inside Interface
  ip address 10.0.68.1 255.255.255.128
!
  ip access-list extended BRI_CRYPTO_MAP_ACL
    permit ip 10.0.68.0 0.0.0.255 any
!
  ip access-list extended CRYPTO_MAP_ACL
    permit ip 10.0.68.0 0.0.0.127 any

The head-end IPSec routers use distinct dynamic crypto map entries and addresses for the primary path and the backup path. The use of different IP addresses for the primary and backup peers (even though they terminate on the same router) allows the remote router to configure specific static IP routes to control the backup function. To conserve physical interfaces on the head-end routers, IEEE 802.1Q trunks are configured and the head-end IPSec routers use multiple logical sub-interfaces on one physical interface.

Remote IP Routing—Floating Static and Specific Routes

On the remote router, floating static default routes (0.0.0.0/0.0.0.0) are configured to route packets either out the primary interface (PPPoE uses a dialer interface) or the Basic Rate ISDN interface. A specific route to the IPSec head-end addresses referenced in the remote crypto map is configured for the primary (Dialer/FastEthernet) path. A host route for the GRE head-end address is configured for the primary (Dialer/FastEthernet) path.

A second specific route to the backup head-end IPSec peer addresses is configured that references the BRI interface. A floating static route to the backup head-end IPSec peer addresses is configured to the Null 0 interface. When the primary path is restored following a failure, the GRE interface shuts down the BRI interface, and the floating static route to the Null 0 interface is inserted into the routing table. The IKE packets of the remote router for the backup peers are routed to the Null 0 interface. Because IKE packets are effectively blocked between the head-end and remote router, the IPSec SAs associated with the dial backup interface are deleted.

Head-end IP Routing Requirements

At the head-end or central site, the enterprise WAN/ISP routers and ISDN head-end router(s) must advertise routes for both the remote subnet and the public or outside interface. In the case of the ISDN interface, this IP address can be an RFC 1918 private IP address; it need not be a public routable IP address. The IP address assigned to the remote router using PPPoE is an Internet routable IP address.

Topology

The topology of this solution is shown in Figure 2-1.
The remote router is a Cisco 1712, which is shown connecting to the Internet through its FastEthernet 0 interface to an external DSL modem. The PPPoE session terminates on the 1712. The outside FastEthernet 0 interface has a QoS service policy applied using hierarchical class-based weighted fair queueing (CBWFQ). A shaper provides the congestion feedback and queues within the shaped rate. The service policy for the Basic Rate ISDN interface is tailored for the lower bandwidth and Layer 2 overhead.

The head-end ISP/WAN routers and ISDN head-end routers simply provide connectivity for the IPSec and GRE head-end routers. The ISDN head-end and IPSec head-end routers share a common VLAN, shown as VLAN 104. The interfaces in VLAN 104 on the IPSec head-end routers are the IP addresses referenced in the crypto map on the remote router ISDN interface. Consider VLAN 104 as being the dial backup encryption. Encryption under normal operations occurs on VLAN 100. Note that the ISP/WAN routers and the GRE head-end are not required to be configured for VLAN 104. VLAN 100 provides connectivity for all head-end routers.

The GRE tunnel is shown terminating on the remote 1712 router and on the GRE head-end router. The GRE tunnel passes through the IPSec head-end.

The crypto map entry on the 1712 is a "permit ip 10.0.68.0 0.0.0.127 any". GRE packets will match this access list, in addition to other IP packets. You do not need to specifically use the permit GRE command, and you should in fact not configure this, because the RRI logic on the head-end router expects an IP entry in the access list.

The GRE head-end router follows the RRI injected route advertised by either the primary or backup IPSec head-end router. When encrypted by the IPSec head-end, the GRE tunnel is encapsulated in the IPSec tunnel. The GRE tunnel is never established over the dial backup path. This is prevented by the host route for the GRE endpoint out the dialer interface of the remote router. Recall that a dialer interface never goes down, even if the PPPoE session is down, so the host route always remains in the routing table. For the GRE interface to be in an UP/UP state, the GRE packets need to be exchanged over the primary path. Once the GRE interface is UP/UP, the BRI interface on the remote router is physically brought down.
Failover/Recovery Time

With GRE keepalive values of 20 seconds and three retries, and an IKE keepalive value of 10 seconds with the default of 2 seconds between retries, the time to identify loss of the primary path and recover over the encrypted ISDN interface is approximately 70 seconds. To demonstrate this, a traceroute was run to verify the path, a ping from the remote subnet to a head-end device was initiated, and a link in the ISP core was administratively shut down.

```
vpnjk-2600-2#traceroute 10.2.128.5
Type escape sequence to abort.
Tracing the route to 10.2.128.5

  1 10.0.68.1 0 msec 0 msec 0 msec
  2 192.168.131.8 12 msec 12 msec 12 msec # Primary IPSec Peer address
  3 10.2.128.5 16 msec * 12 msec
```

```
vpnjk-2600-2#ping 10.2.128.5 timeout 5 repeat 2000
Type escape sequence to abort.
Sending 2000, 100-byte ICMP Echos to 10.2.128.5, timeout is 5 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[repletion removed]
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (1986/2000), round-trip min/avg/max = 20/41/456 ms
```

```
vpnjk-2600-2#traceroute 10.2.128.5
Type escape sequence to abort.
Tracing the route to 10.2.128.5

  1 10.0.68.1 0 msec 4 msec 0 msec
  2 192.168.131.68 32 msec 28 msec 28 msec # Backup IPSec Peer address
  3 10.2.128.5 32 msec * 28 msec
```

In the above example, the GRE keepalive value of 20 seconds with three retries contributes to the largest portion of the failover time.

---

**Note**

This is a proof of concept failover test; failover with thousands of peers may vary in duration.

During recovery to the primary link, packet loss is minimal, with packet loss for only a few seconds. The GRE tunnel keepalives must be flowing across the primary IPSec peers before the ISDN interface is placed back in standby mode and shut down.

**V3PN QoS Service Policy for Basic Rate ISDN**

The QoS service policy applied to the BRI interface differs slightly from the primary interface because of the limited bandwidth available on the backup interface. On the primary interface in this example, the uplink is 256 kbps and the backup interface is two 64 kbps ISDN B channels.
Both B channels are brought up immediately upon activation of the backup link with the `ppp multilink links minimum 2` command. You can also use the `dialer load-threshold 1 either` command, but this may not activate the second link as quickly as specifying the minimum links using the PPP multilink command.

The size of the encrypted voice packet, assuming a G.729 codec, is 112 bytes when specifying Triple Data Encryption Standard (3DES) and Secure Hash Algorithm (SHA) in the IPSec transform set. IPSec tunnel mode is required in this configuration.

**Note**
Although TRANSPORT mode is specified first in the crypto map, TUNNEL mode will be negotiated. Use the `show crypto ipsec sa inc in use settings` command to make sure that tunnel mode is in use.

The priority or Low Latency Queue (LLQ) needs to be provisioned for 112 bytes at 50 packets per second (pps) with 8 bits per byte or 44,800 kbps. Assuming 6 bytes for Layer 2 Multilink PPP (MLPPP) overhead, 48 kbps is provisioned for the priority queue. The burst size is increased from the default of 1200 bytes to 2400 bytes to eliminate voice drops observed during performance testing. Use of G.711 codec is not recommended because it requires approximately 104,800 bits per second (bps).

On a Basic Rate ISDN interface, Cisco IOS Software assumes that only 64 kbps is available, even though the interface provides 128 kbps with both B channels active. The QoS service policy shown in the following configurations allocates less than the 64 kbps; however, the `max-reserved-bandwidth 100` statement needs to be configured on the BRI 0 interface.

To view the counters of the service policy attached to the BRI interface, display the associated virtual-access interface, as in the following example:

```
show policy-map interface virtual-access
```

The virtual-access interfaces are created dynamically and the interface number can be displayed with the `show ip interface brief` command.

The `tx-ring-limit 1` and `ppp multilink fragment delay 10` commands are included in the BRI interface configuration to reduce voice delay and jitter in the performance test.

## Performance Results

The goal of this testing is to determine encrypted voice performance with multilink PPP and LFI configured on the BRI interface.

**Note**
The Cisco 1712 router has not been included in the above guides. The component of this design that has not been tested is the encryption of voice and data traffic over the backup path, the Basic Rate ISDN link.

The performance results are shown in Table 2-1.

### Table 2-1  Cisco 1712 V3PN over Basic Rate ISDN

<table>
<thead>
<tr>
<th>Call Leg</th>
<th>Chariot Voice Drops %</th>
<th>Chariot RFC 1889 Jitter</th>
<th>Chariot One-way Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 1712 router</td>
<td>Branch -&gt; Head</td>
<td>0%</td>
<td>10.7 ms</td>
</tr>
<tr>
<td></td>
<td>Head -&gt; Branch</td>
<td>0.04%</td>
<td>11.4 ms</td>
</tr>
</tbody>
</table>
These results do not include any service provider simulated delay in the ISDN network. These test results are as good or better than would be expected for voice over the primary path, based on previous test results. There is no reason to believe voice quality would not be acceptable when the backup link is active.

Implementation and Configuration

This section illustrates the key configuration components. In the following examples, the following 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:

- Remote GRE Tunnel Interface
- Head-end GRE Router
- IPSec Head-end Routers
- Remote Router
- Show Commands

Remote GRE Tunnel Interface

The relevant portions of this configuration are bolded and italicized. There is no IP address assigned to the tunnel interface. The backup interface command causes the ISDN interface to be brought up if the tunnel keepalives are missed. The keepalive hello interval is set to 20 seconds with a dead interval of 60 seconds (20 seconds * 3 retries). The source of the tunnel interface is the inside or VLAN1 interface. The destination IP address is 192.168.131.23, which is the GRE head-end router, and a host route is configured forcing packets for this IP address out the dialer or primary interface.

```plaintext
! hostname vpn-jk2-1712-1
!
interface Tunnel900
description tunnel to vpn-jk-2600-23
no ip address
backup interface BRI0
keepalive 20 3
tunnel source Vlan1
tunnel destination 192.168.131.23
!
interface Vlan1
ip address 10.0.68.1 255.255.255.128
!
ip route 192.168.131.23 255.255.255.255 Dialer1
!
```
Head-end GRE Router

The configuration of the head-end GRE router is simple. For each remote router, configure a tunnel interface with the source address of 192.168.131.23 and a destination IP address that corresponds with the inside LAN (or VLAN) interface of the remote router. That address is 10.0.68.1 in this example:

```plaintext
! hostname vpnjk-2600-23
!
! interface Tunnel900
description Tunnel to vpn-jk2-1712-1
   no ip address
   keepalive 20 3
   tunnel source 192.168.131.23
   tunnel destination 10.0.68.1
!
 interface FastEthernet0/1.100
description vlan 100
 encapsulation dot1Q 100
 ip address 192.168.131.23 255.255.255.224
!
!
These displays illustrate the route advertisement from the GRE head-end (vpnjk-2600-23) router and the advertising IPSec head-end (vpnjk-2600-8) router. The GRE head-end router sees an advertisement for the remote network, both from 192.168.131.8 (vpnjk-2600-8). Both /24 and /25 masks are advertised, because the IPSec tunnels for the primary and backup are active.
The following display was taken when the backup link was active and the primary path had just been restored, but the dynamic crypto map entry of the backup link had not yet been removed from the head-end.

```

```
Because of the longest prefix match rule, the keepalive packets of the GRE tunnel keepalive always prefer the primary path if it is active. If the primary path is not active, the GRE packets from the head to branch location are sent over the ISDN interface, but recall that the remote router has a host route for the GRE head-end address to the dialer interface. Because the dialer interface never goes down, the keepalives are never returned to the head-end over the ISDN interface. This forces the GRE tunnel to use only the primary path for two-way communications.

**IPSec Head-end Routers**

The head-end IPSec configuration is very similar to what has been described in various V3PN design guides. The only major difference is the use of two separate dynamic crypto maps on two separate interfaces: the primary on VLAN 100 and the backup on VLAN 104. Using two separate crypto map instances provides the remote router separate IP addresses to reference on the primary and backup crypto maps, which in turn allows a floating route to be used in the remote router to force the IKE packets for the backup crypto map to be dumped into the Null interface when the ISDN interface is shut down.

See the specific notes in the following configuration:

```plaintext
hostname vpnjk-2600-8
!
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
  certificate 6122A4EC0000000000000021
!
crypto isakmp policy 1
  encr 3des
  group 2
  crypto isakmp keepalive 10
  # Note the IKE keepalive value compared to the GRE keepalive
!
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-transport udp-encaps
!
!
crypto dynamic-map DYNO-TEMPLATE 10
  description dynamic crypto map
  set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
  reverse-route
  qos pre-classify
  !

  # Both crypto maps will reference this template
!

crypto map DYNO-MAP local-address FastEthernet0/1.100

crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
!
  # DYNO-MAP on VLAN 100 is the primary crypto

crypto map BRI-MAP local-address FastEthernet0/1.104

crypto map BRI-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!```

```plaintext
  # BRI-MAP on VLAN 104 is the backup crypto
```
interface FastEthernet0/1.100
  encapsulation dot1Q 100
  ip address 192.168.131.8 255.255.255.224
  crypto map DYNO-MAP

interface FastEthernet0/1.104
  encapsulation dot1Q 104
  ip address 192.168.131.68 255.255.255.224
  crypto map BRI-MAP

# VLAN 128 is the path to the core corporate network

interface FastEthernet0/1.128
  encapsulation dot1Q 128
  ip address 10.2.128.8 255.255.255.0

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

# Access-list 68 is used to limit what is being redistributed into EIGRP. For the purposes of this illustration, we are only allowing one remote network /24 to be redistributed. In reality you want to list a network and mask to cover all remote networks.

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
end

The second IPSec head-end, this configuration is similar to the first head-end configuration.

hostname vpnjk-2600-9

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 610BE2E40000000000001F
  certificate ca 113346B52ACEE8B04ABD5A5C3FED139A

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
no crypto ipsec nat-transparency udp-encaps
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

crypto map BRI-MAP local-address FastEthernet0/1.104
crypto map BRI-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE

interface FastEthernet0/1.100
  encapsulation dot1Q 100
  ip address 192.168.131.9 255.255.255.224
  crypto map DYNO-MAP

interface FastEthernet0/1.104
  encapsulation dot1Q 104
  ip address 192.168.131.69 255.255.255.224
  crypto map BRI-MAP

interface FastEthernet0/1.128
  encapsulation dot1Q 128
  ip address 10.2.128.9 255.255.255.0

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

! access-list 68 permit 10.0.68.0 0.0.0.255

route-map IPSEC_Subnets permit 10
  match ip address 68

end
Remote Router

Following is the configuration for the remote Cisco 1712 router. The relevant portions of the configuration are annotated.

```
! hostname vpn-jk2-1712-1
!
username vpnjk-2600-20 password 0 foo
!
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 6109357000000000003A
    certificate ca 113346b52aceeb04abd5a5c3fed139A
!
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
no crypto ipsec nat-transparency udp-encaps
!
# The primary crypto map is associated with the Dialer interface
# and the peer statements reference VLAN 100 addresses on the head-end.
!
crypto map TEST local-address Dialer1
    crypto map TEST 1 ipsec-isakmp
        description Crypto for normal operations
        set peer 192.168.131.9
            vpn-jk-2600-9 VLAN 100 interface
        set peer 192.168.131.8
            vpn-jk-2600-8 VLAN 100 interface
        set transform-set 3DES_SHA_TUNNEL
        match address CRYPTO_MAP_ACL
        qos pre-classify
!
# The backup crypto map is associated with the BRI0 interface
# and the peer statements reference VLAN 104 addresses on the head-end.
!
crypto map BRI local-address BRI0
    crypto map BRI 1 ipsec-isakmp
        description Crypto when in dial backup mode
        set peer 192.168.131.69
            vpn-jk-2600-9 VLAN 104 interface
        set peer 192.168.131.68
            vpn-jk-2600-8 VLAN 104 interface
        set transform-set 3DES_SHA_TUNNEL
        match address BRI_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
!
policy-map V3PN-WAN-EDGE-ISDN
description Note LLQ for PPP/ISDN G.729=48K
class VOICE
  priority 48 2400
class CALL-SETUP
  bandwidth percent 2
class INTERNETWORK-CONTROL
  bandwidth percent 5
class class-default
  fair-queue
  random-detect
!
policy-map V3PN-teleworker
description Note LLQ for ATM/DSL G.729=64K
class CALL-SETUP
  bandwidth percent 2
class INTERNETWORK-CONTROL
  bandwidth percent 5
class VOICE
  priority 64
class class-default
  fair-queue
  random-detect
policy-map Shaper
class class-default
  shape average 182400 1824
  service-policy V3PN-teleworker
!
!
interface Tunnel900
description tunnel to vpn-jk-2600-23
no ip address
backup interface BRI0
keepalive 20 3
tunnel source Vlan1
tunnel destination 192.168.131.23
!
interface BRI0
bandwidth 128
ip address 10.0.128.1 255.255.255.252
max-reserved-bandwidth 100
service-policy output V3PN-WAN-EDGE-ISDN
encapsulation ppp
no ip mroute-cache
load-interval 30
tax-ring-limit 1
tax-queue-limit 1
dialer idle-timeout 0
dialer wait-for-carrier-time 10
dialer map ip 10.0.128.2 name vpnjk-2600-20 broadcast 9191234567
dialer map ip 10.0.128.2 name vpnjk-2600-20 broadcast 9191234568
dialer hold-queue 5
dialer-group 2
isdn switch-type basic-5ess
ppp authentication chap
ppp multilink
ppp multilink fragment delay 10 # Both B Channels will be brought up immediately
ppp multilink links minimum 2

crypto map BRI
!

interface FastEthernet0
description Outside to DSL Modem
bandwidth 256
no ip address
service-policy output Shaper
load-interval 30
duplex auto
speed auto
pppoe enable
pppoe-client dial-pool-number 1
!

interface FastEthernet1
no ip address
vlan-id dot1q 1
exit-vlan-config
!

interface FastEthernet2
no ip address
!

interface FastEthernet3
no ip address
!

interface FastEthernet4
no ip address
!

interface Dialer1
description Outside
bandwidth 256
ip address negotiated
ip mtu 1492
encapsulation ppp
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 TEST
!

interface Vlan1
description Inside Interface
ip address 10.0.68.1 255.255.255.128
ip route-cache flow
ip tcp adjust-mss 542
load-interval 30
!
ip classless
!

# Two default routers are defined, the route thru the
# BRI interface will only be in the routing table when the
# BRI interface is UP/UP
ip route 0.0.0.0 0.0.0.0 10.0.128.2 name BRI_peer_20
ip route 10.0.128.2 255.255.255.255 BRI0
! # This route will force the IKE and IPSec packets to peers
ip route 0.0.0.0 0.0.0.0 Dialer1 240
! # These are the primary peers on VLAN 100
ip route 192.168.131.8 255.255.255.254 Dialer1
! # This host route forces the GRE tunnel out the primary path only.
! ip route 192.168.131.23 255.255.255.255 Dialer1
! # These routes are for the backup IPSec peers on VLAN 104
! # When the BRI interface is down, the Null0 route will be in the
! # routing table.
! ip route 192.168.131.68 255.255.255.254 10.0.128.2
ip route 192.168.131.68 255.255.255.254 Null0 239
! no ip http server
no ip http secure-server
!
ip access-list extended BRI_CRYPTO_MAP_ACL
  permit ip 10.0.68.0 0.0.0.255 any
!
ip access-list extended CRYPTO_MAP_ACL
  permit ip 10.0.68.0 0.0.0.127 any
!
access-list 100 deny icmp any any
access-list 100 permit ip any any
dialer-list 2 protocol ip list 100
!
ntp server 192.168.130.1
!
end

Show Commands

Under normal operations over the DSL connection, the routing table for the remote 1712 router appears as follows:

vpn-jk2-1712-1#sh ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
  192.168.131.0/24 is variably subnetted, 3 subnets, 2 masks
     S  192.168.131.68/31 is directly connected, Null0
     S  192.168.131.8/31 is directly connected, Dialer1
     S  192.168.131.23/32 is directly connected, Dialer1
  10.0.0.0/25 is subnetted, 1 subnets
     C  10.0.68.0 is directly connected, Vlan1
In the above display, the 192.168.17.0 address space is allocated to the router using PPPoE. The 192.168.131.0 address space represents the Internet routable address space of the head end. Note the VLAN 104 head-end address space; 192.168.131.68/31 is being routed to the Null 0 interface during normal operation. The tunnel interface is UP/UP.

Next a cable cut failure in the DSL service provider to Tier 1 ISP is simulated.

During backup mode, the routing table of the remote Cisco 1712 is as follows:

In this example, there is no loss of connectivity to the DSL service provider; the failure was simulated by shutting down the interface connecting the DSL service provider to the Tier 1 ISP in the test topology. The values that have been added or changed from the normal state example are highlighted.

During dial backup, the remote router has two IPSec SAs (ID=200,201), and an established IKE SA (ID=164) over the BRI path. The router continues to attempt to re-establish connectivity to the head-end IPSec peers over the normal path. Their IKE SAs (ID=167,168) are in the connection table.
On the head-end IPSec router, when the dial backup is active, there is a dynamic crypto map entry over the BRI-MAP but none on the primary path (the DYNO-MAP).

```
vpnjk-2600-8#sh crypto map
Crypto Map: "DYNO-MAP" idb: FastEthernet0/1.100 local address: 192.168.131.8
Crypto Map "DYNO-MAP" 10 ipsec-isakmp
    Dynamic map template tag: DYNO-TEMPLATE
    Interfaces using crypto map DYNO-MAP:
        FastEthernet0/1.100

Crypto Map: "BRI-MAP" idb: FastEthernet0/1.104 local address: 192.168.131.68
Crypto Map "BRI-MAP" 10 ipsec-isakmp
    Dynamic map template tag: DYNO-TEMPLATE
Crypto Map "BRI-MAP" 11 ipsec-isakmp
    Peer = 10.0.128.1
    Extended IP access list
        access-list  permit ip any 10.0.68.0 0.0.0.255
        dynamic (created from dynamic map DYNO-TEMPLATE/10)
    Current peer: 10.0.128.1
    Security association lifetime: 4608000 kilobytes/3600 seconds
    PFS (Y/N): N
    Transform sets={ 3DES_SHA_TRANSPORT, }
    Reverse Route Injection Enabled
    Interfaces using crypto map BRI-MAP:
        FastEthernet0/1.104
```

During the Chariot performance test, the service policy associated with the virtual access interface was displayed for the VOICE class.

```
vpn-jk2-1712-1#show policy-map interface virtual-access 3 out class VOICE
Virtual-Access3
    Service-policy output: V3PN-WAN-EDGE-ISDN
    Class-map: VOICE (match-all)
        0 packets, 0 bytes
        30 second offered rate 0 bps, drop rate 0 bps
        Match: ip dscp ef
        Queueing
            Strict Priority
        Output Queue: Conversation 40
        Bandwidth 48 (kbps) Burst 2400 (Bytes)
        (pkts matched/bytes matched) 20454/2372648
        (total drops/bytes drops) 0/0
```

Note that both B channels are fully used during the Chariot performance test, at 50 pps for voice, which leaves 48–49 pps of data.

```
vpn-jk2-1712-1#show interfaces bri0 1 2 | inc load|rate
    reliability 255/255, txload 215/255, rxload 215/255
    Queueing strategy: weighted fair [suspended, using FIFO]
    30 second input rate 54000 bits/sec, 98 packets/sec
    30 second output rate 54000 bits/sec, 99 packets/sec
```
Cisco IOS Versions Tested

The following code versions were used during testing.

- IPSec head-ends—c2600-ik9o3s-mz.122-11.T5
- Cisco 1712—c1700-k9o3sy7-mz.122-15.ZL1
- GRE head end—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, Cisco recommends using IPSec head-ends with suitable performance characteristics aligned with the number of remote routers.

An available Cisco 1760 V3PN bundle, (product number: CISCO1760-V3PN/K9) can be used instead of the 1712, if a Basic Rate ISDN WAN interface card (WIC) is installed. The Cisco 1712 supports ISDN S/T, an external Network Termination Unit-1 (NTU-1) is required in some locales, which is available from http:\www.blackbox.com among other sources.

Caveats

Several DPD/RRI issues were encountered during testing.
When running Cisco IOS 12.2(11)T5, the IPSec head-end router inserts the static routes in the routing table with a next hop address of 0.0.0.0 as shown.

vnpjk-2600-8#sh ip route static

    10.0.0.0/8 is variably subnetted, 14 subnets, 7 masks
    S    10.0.68.0/24 [1/0] via 0.0.0.0, FastEthernet0/1.104
    S    10.0.68.0/25 [1/0] via 0.0.0.0, FastEthernet0/1.100

However, the router had no default gateway configured:

vnpjk-2600-8#show ip route | inc Gateway
Gateway of last resort is not set

This router was using Address Resolution Protocol (ARP) to resolve the MAC address for the remote network address. The ISDN head-end router (MAC address 0005.9bbf.1901) replied with a proxy ARP.

vnpjk-2600-8#sh arp | inc 10.0.68.1
Internet 10.0.68.1 1 0005.9bbf.1901 ARPA FastEthernet0/1.100

Proxy ARP was disabled on the ISDN head-end router, while the IPSec head-end continued to use ARP for the address, and the ISDN head-end router no longer replied.
When IP Cisco Express Forwarding (CEF) and proxy ARP were disabled on the ISDN router, RRI functioned properly.

### Debugging

You can enable tunnel keepalive debugging to verify connectivity over the primary path. Cisco recommends enabling this on the remote router rather than the head-end router if a large number of tunnels are terminated on the head-end router, because it generates a console message for each tunnel and each keepalive.

```
vpnjk-2600-23#debug tunnel keepalive
Tunnel keepalive debugging is on
Nov 25 16:10:29 est: Tunnel900: sending keepalive, 10.0.68.1->192.168.131.23 (len=24 ttl=255), counter=1
Nov 25 16:10:29 est: Tunnel900: keepalive received, 10.0.68.1->192.168.131.23 (len=24 ttl=253), resetting counter
Nov 25 16:10:49 est: Tunnel900: sending keepalive, 10.0.68.1->192.168.131.23 (len=24 ttl=255), counter=1
Nov 25 16:10:49 est: Tunnel900: keepalive received, 10.0.68.1->192.168.131.23 (len=24 ttl=253), resetting counter
```

Note the time-to-live (TTL) is 253 for the received keepalive because the keepalive passed through the IPSec tunnel and thus two routers in total.

### Summary

Enterprise customers who currently use Basic Rate ISDN dial backup to provide backup connectivity in the event their Frame Relay link fails will also want to provide similar backup mechanisms as they migrate the primary link from Frame Relay to DSL. Because in many cases the DSL connection is provisioned over the Internet, IPSec encryption may be a requirement for the primary link though it was not required over a private Frame Relay carrier. An added benefit of this design is that there is no additional cost of encrypting the Basic Rate ISDN backup link, because the same head-end routers can be used to encrypt both primary and backup.

Use of the GRE tunnel to trigger dial backup is both a scalable and a reliable means of initiating the backup link. Not encrypting the data traffic in the GRE tunnel saves both WAN bandwidth and offers greater head-end scalability, because no routing protocol is required.