Large Branch—Frame Relay/Broadband Load Sharing and Backup

This chapter describes a design targeted at a large retail customer deployment with an existing Frame Relay network to each store location. Within the store, Internet kiosks (web kiosks) allow a customer to use the online catalog and website of the retailer. This design is also applicable to providing wireless Internet access points within the retail location.

Each store location has one or more VLANs. The store uses dedicated VLANs to support point-of-sale applications and credit card authorization. Other VLANs are for kiosk or public access points. The documented configuration shows only one VLAN, but others can be easily implemented with different Hot Standby Router Protocol (HSRP) groups and active/standby routers.

This customer is interested in supplementing the bandwidth to each store with a broadband WAN because of the low cost and high bandwidth. The broadband WAN is used as a backup mechanism for the existing Frame Relay network and also as the primary path for customer Internet traffic. The Frame Relay network remains because it is viewed as more reliable than the Internet broadband WAN for point-of-sale applications at the store. The QoS policy implemented on the Frame Relay and broadband WAN network reflects this business requirement.

This chapter includes the following sections:

- Solution Characteristics
- Topology
- Failover/Recovery Time
- Implementation
- Verification
- Configuration
- Show Commands
- Cisco IOS Versions Tested
- Caveats
- Summary
Solution Characteristics

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

- Interest in using broadband as a lower cost alternative to traditional WAN media
- Desire to use alternate technologies for primary and backup path
- Encryption for both the existing Frame Relay and the broadband link, or only for the broadband link

**Note**

Gateway Load Balancing Protocol (GLBP) is documented as included in the Cisco 2600 12.2(15)T images; however, c2600-ik9o3s3-mz.122-15.T9 does not include GLBP support. The Cisco 1712 router used in testing did include GLBP support in the 12.3(7)T (c1700-k9o3sy7-mz.123-7.T) image. Because the Cisco 2600 series is commonly deployed in the solution topology, and some customers may need to encrypt packets on the Frame Relay WAN link, GLBP was not included as part of this solution.

Topology

Figure 9-1 shows the topology described in this section:

**Figure 9-1 Large Branch Frame Relay/Broadband Load Sharing and Backup**

IPSec and generic routing encapsulation (GRE) tunnels are terminated on both remote routers: the Frame Relay router and the broadband router. Because the backup and load sharing function does not depend on anything other than HSRP-tracked interfaces and routing protocol metrics, the design concepts can be adapted to work with an unencrypted Frame Relay network or an encrypted link on the Frame Relay network.

If the Frame Relay network is not encrypted and GRE tunnels are not used, using the same routing protocol on both WAN topologies simplifies the design and implementation.
Failover/Recovery Time

The failover and recovery time for this configuration depends on the hello and hold time implemented by the customer for HSRP, GRE keepalive, and the routing protocol used within the GRE tunnel. In this example, EIGRP is used.

The HSRP default hello time is 3 seconds and the hold time is 10 seconds. For EIGRP, the default hello time is 5 seconds and the hold time is 15 seconds. The GRE keepalives are typically set at 10 seconds with retries at 3 or a hold time of 30 seconds.

These values are acceptable to most customer deployments; however, they can be changed as required.

Implementation

This section explains how the router configurations implement load sharing and backup over the Frame Relay and broadband connection. The GRE tunnels are encrypted. The complete configuration files are shown in a following section, but here the focus is on the interface delay and bandwidth configuration for the GRE and LAN interfaces of the remote routers.

This section includes the following topics:

- GRE Tunnels
- Summary Route Advertised
- Bandwidth and Delay
- Branch EIGRP and Addressing
- Summary Advertisement Traverses the LAN
- Head-end to Branch Considerations
- Head-end to Branch Load Sharing Example

GRE Tunnels

In Figure 9-2, two GRE tunnels are defined from each remote router to a head-end GRE/IPSec peer. This configuration provides maximum availability because the site maintains connectivity in the event that one remote router and one head-end router are out of service at the same time.
Figure 9-2  Frame Relay/Broadband-GRE Tunnels

The WAN cloud depictions are removed from the topology in Figure 9-3 to reduce the complexity of the drawing. Tunnel names and IP addresses have been added.

Figure 9-3  Frame Relay/Broadband-Tunnel Interface Names

The GRE interface numbers on the branch and head-end routers are the same on both ends; Tunnel 1 on remote router 2600-18 connects to Tunnel 1 on head-end router 2600-22. This nomenclature facilitates troubleshooting. The IP addresses for the tunnel interfaces are allocated out of the address space for the remote location. In this example, each remote is allocated an address on a /22 network boundary. The tunnel addressing is allocated from that address space. The loopback interfaces are allocated from that address space and are the inside VLANs. In this example, the inside VLAN is address 10.0.68.0/25.
Summary Route Advertised

The head-end routers advertise a summary route to the head-end address space, as shown in Figure 9-4.

**Figure 9-4**  **Frame Relay/Broadband—Summary Advertisement**

In this example, an advertisement to 10.0.0.0/8 is used. One or more networks or a default network can be advertised. If a default network is advertised, the broadband router requires specific routes to its GRE/IPSec peers pointing out the outside/broadband interface. For example, the 1712-1 router configuration in the configuration samples has a default route to the PPPoE (Dialer) interface as shown:

```
ip route 0.0.0.0 0.0.0.0 Dialer1 239 name Broadband
```

The GRE and IPSec peer statements refer to 192.168.131.22 and 192.168.131.23.

```
vpn-jk2-1712-1#show run | inc set peer|tunnel dest
set peer 192.168.131.22
set peer 192.168.131.23
tunnel destination 192.168.131.22
tunnel destination 192.168.131.23
```

The configuration needs to be changed to eliminate the default route and to include the host specific (host routes or /32 routes) to the head-end peers, as follows:

```
no ip route 0.0.0.0 0.0.0.0 Dialer1 239 name Broadband
ip route 192.168.131.22 255.255.255.255 Dialer1 239 name Broadband22
ip route 192.168.131.23 255.255.255.255 Dialer1 239 name Broadband23
```

If the configuration is using Dynamic Host Configuration Protocol (DHCP) rather than PPP over Ethernet (PPPoE) to obtain the outside IP address, the host specific route references the DHCP keyword instead, as follows:

```
ip route 192.168.131.22 255.255.255.255 dhcp
ip route 192.168.131.23 255.255.255.255 dhcp
```
Bandwidth and Delay

EIGRP uses bandwidth and delay in calculating route metrics. The next two inserts highlight key facts that are helpful in understanding the concept and configuration in this section.

Delay

EIGRP calculates delay as the cumulative delay; you add up the delay from all the routers that learned the network advertisement.

The delay value is based on the input interface of the receiving router, not the output interface of the sending router. There is no requirement that the values match, but best practice is to make them match unless you have a specific reason not to do so.

Units are the following:
- `show ip eigrp topology` gives you delay in microseconds (usec)
- `show interface` commands displays in microsecond units
- `default-metric` command; delay metric is in 10 microsecond units
- `delay interface` command specified in 10 microsecond units

One rule of thumb is that whatever you type is multiplied by 10 when displayed by the router.

Bandwidth

EIGRP uses the minimum bandwidth for all the links to a network. Like delay, this is derived from the input interface. Because the default value is 9 kbps for a tunnel interface and this topology is always using tunnel interfaces, the bandwidth value does not really come into play.

The default and modified values for bandwidth and delay on the remote routers are examined. Figure 9-5 highlights these values.

**Figure 9-5** Frame Relay/Broadband-Delay/Bandwidth Values
The values chosen are selected so that the HSRP active router, in this example 2600-18, calculates a route for network advertisements learned via Tunnel 1 with the same metric as an advertisement for the same network from router 1712-1 over the inside LAN interface.

From the perspective of the 2600-18 router, an advertisement for 10.0.0.0/8 has an EIGRP metric of 297244416. This value is derived from a minimum bandwidth value of 9 kbps and a total delay value of 500,000. The total delay in microseconds is determined by adding the values from the `show interface` command. In this example, the Tunnel 0 interface on 1712-1 has a delay of 499,900 microseconds and the FastEthernet 0/1.204 of the 2600-18 router has a delay of 100 microseconds.

Following is a Perl program to facilitate this calculation. This program calculates the EIGRP metric and derives the same value as a Cisco IOS router. It is executed with a minimum bandwidth of 9 kbps and sums the two delays of 499,900 and 100 microseconds:

```
D:\>perl eigrp.pl 9 499900 100
297244416
```

```
# eigrp.pl
# Usage: eigrp.pl Minimum_bandwidth_in_Kbit Total_delay_in_microseconds
#        eigrp.pl 10000 1280
# or
#        eigrp.pl 10000 1000 200 80
# Author: cisco789@cisco.com CCIE 1846
# Version 1.0  25 July 2000
#
# The path with the smallest metric is the best path.
#$minBW  = $ARGV[0];
#$sumDLY = 0;
#foreach $i (1 .. $#ARGV) {
#  # Delay
#  #$sumDLY = $sumDLY + $ARGV[$i];
#}
# We are expecting delay input in microseconds, (as from the interface
# or default-metric command) not tenths of microseconds.
#$sumDLY = $sumDLY / 10;
# Bandwidth
#$iBW = 10000000 / $minBW;
#$iBW = sprintf('%9d',$iBW);
#$EIGRPmetric = ($iBW + $sumDLY) * 256;
# print "$EIGRPmetric";
exit;
#
# Notes:
# Cisco routers do not perform floating point math, so at each stage
# in the calculation, you will need to round down to the
# nearest integer (whole number) to calculate the metrics the
```
Branch EIGRP and Addressing

Figure 9-6 shows the EIGRP configuration in use by the branch routers.

The addressing scheme has allocated a /22 network for the remote site. The loopback interfaces for the two remote routers are allocated from that address block as well as all VLANs in use.

To prevent recursive routing issues, distribution lists are configured on the remote routers, so only the VLAN interface(s) are advertised to the head-end routers. If the loopback interface address is included in the advertisement to the head-end, the tunnel is changed to “down” by Cisco IOS to avoid recursive routing issues.
Note

If you choose to use this technique, it is important in this design to specify the **out Tunnel** and include a distribute list for each tunnel interface that resides on this router. If the more generic form of **distribute-list VLAN_ONLY out** is used and the interface is not specified, the two remote routers do not advertise the 10.0.0.0/8 network to each other over the inside LAN interface. This prevents the intended load sharing from working. The HSRP active router must receive an advertisement for the head-end network(s) from both the EIGRP neighbors on its tunnel interfaces as well as from the HSRP standby router over the inside LAN interface.

The above EIGRP and IP addressing is shown because many traditional Frame Relay deployments allocated their WAN, VLAN, and loopback interfaces from a contiguous address block allocated to each remote location. This design is intended to introduce broadband as a backup and also load sharing into an existing deployment.

A more simplistic configuration is to allocate the loopback interface that serves as the GRE tunnel source for the remote routers from an address block not allocated to the remote location. For example, assuming that this location has been allocated 10.0.68.0/22 addressing, the Loopback 0 interface for this site can be 10.0.252.1 /32 and 10.0.252.2 / 32 for the next site.

The advantage in this lies in the elimination of the distribution list commands on the remote routers. The network statement under router EIGRP 1068 can be changed from the following:

```
   network 10.0.0.0
```

to the following:

```
   network 10.0.68.0 0.0.3.255
```

The IPSec/GRE head-end routers, deploying dynamic crypto maps in a GRE configuration, can simply have a summary route for the following:

```
   ip route 10.0.252.0 255.255.252.0 ...
```

This results in all the GRE tunnel destination addresses being routed out the interface with the dynamic crypto map applied.

Remember the simple rule to eliminate recursive routing errors with GRE interfaces: **do not advertise a route through the tunnel that will include the tunnel endpoint.** If you find it necessary to do so, you must have a more specific network advertisement to the tunnel endpoint that is not through the tunnel interface itself.

Also, for network management purposes, a second loopback address (Loopback 1) can be allocated from the /22 address block of the site.

**Summary Advertisement Traverses the LAN**

The goal in this design is to advertise the 10.0.0.0/8 network between both branch routers on their inside or LAN interface with a metric that allows two equal cost paths to this network to be inserted into the routing table of the HSRP active router.

Both branch routers receive a network advertisement for 10.0.0.0/8 on each of their tunnel interfaces, and they also advertise this across their inside VLAN/FastEthernet interface to each other, as shown in Figure 9-7.
Figure 9-7  Frame Relay/Broadband—10.0.0.0/8 Advertisement

Router 2600-18, the HSRP active router, has two routes in its routing table to network 10.0.0.0:

VPNjk-2600-18# show ip route 10.0.0.0 255.0.0.0
Routing entry for 10.0.0.0/8
Known via "eigrp 1068", distance 90, metric 297246976, type internal
Redistributing via eigrp 1068
Last update from 10.0.68.138 on Tunnel1, 20:01:07 ago
Routing Descriptor Blocks:
  10.0.68.1, from 10.0.68.1, 20:01:07 ago, via FastEthernet0/1.204
    Route metric is 297246976, traffic share count is 1
    Total delay is 500100 microseconds, minimum bandwidth is 9 Kbit
    Reliability 255/255, minimum MTU 1468 bytes
    Loading 1/255, Hops 2
10.0.68.138, from 10.0.68.138, 20:01:07 ago, via Tunnel1
    Route metric is 297246976, traffic share count is 1
    Total delay is 500100 microseconds, minimum bandwidth is 9 Kbit
    Reliability 255/255, minimum MTU 1476 bytes
    Loading 1/255, Hops 1

These two equal cost paths are used to load share packets by Cisco Express Forwarding (CEF) per source, per destination load sharing, or by fast switching per destination. Per packet load sharing can be accomplished by process switching or CEF per packet; however, this is not recommended because of the increased likelihood of incurring out-of-order packets in this topology. The two WANs may have dramatically different latency characteristics.

VPNjk-2600-18# show ip eigrp topology 10.0.0.0 255.0.0.0
IP-EIGRP (AS 1068): Topology entry for 10.0.0.0/8
State is Passive, Query origin flag is 1, 2 Successor(s), FD is 297246976
Routing Descriptor Blocks:
10.0.68.138 (Tunnel1), from 10.0.68.138, Send flag is 0x0
  Composite metric is (297246976/28160), Route is Internal
  Vector metric:
    Minimum bandwidth is 9 Kbit
    Total delay is 500100 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1476
    Hop count is 1
10.0.68.1 (FastEthernet0/1.204), from 10.0.68.1, Send flag is 0x0
  Composite metric is (297246976/297244416), Route is Internal
  Vector metric:
Minimum bandwidth is 9 Kbit
Total delay is 500100 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1468
Hop count is 2

10.0.68.142 (Tunnel901), from 10.0.68.142, Send flag is 0x0
Composite metric is (297249536/28160), Route is Internal

Vector metric:
Minimum bandwidth is 9 Kbit
Total delay is 500200 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1476
Hop count is 1

vpnjk-2600-18#

**Note**
The first composite metric number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised.

### Head-end to Branch Considerations

As a best practice, the bandwidth and delay values on an interface should match for all devices sharing the interface. For example, the 1712-1 VLAN interface has a different default value for delay than the 2600-18 FastEthernet0/1.204. To compensate, the VLAN interface is changed.

Because in this configuration the values for delay on the remote router tunnel interface are changed from the default values to provide load sharing through the tunnel interfaces over the Frame Relay and broadband links, the best practice is to make the delay values on the head-end routers (2600-22 and 2600-23) match the remote router values. Generally, the values of both ends of a link or interface should match.

Assuming that on the head-end campus routers 2600-22 and 2600-23 are advertising the remote subnet 10.0.68.0/25 to campus router 2600-5 via EIGRP, the return path for all packets is through router 2600-22 and its Tunnel 0 interface, assuming no router or link failures at the time. This is shown in Figure 9-8.
This is not necessarily a bad practice. The Frame Relay link on router 2600-18 has a Committed Information Rate (CIR) of 512 kbps/512 kbps and a port speed of 1 Mbps, and the broadband link is 768 kbps/3 Mbps. The broadband path can provide substantially more bandwidth.

However, if the Frame Relay network generally provides access to the remote location at port speed and if the broadband network is aDSL at 256 kbps/1.4 Mbps, it is better to at least load share or to prefer the Frame Relay network. DSL is typically provisioned over ATM, which has substantially more Layer 2 overhead than Frame Relay.

**Head-end to Branch Load Sharing Example**

To accomplish this as per the example, configure the delay value on 2600-23 Tunnel 901 with a delay value of 49990. This causes the campus router 2600-5 to insert two equal cost routes into its routing table for remote network 10.0.68.0/25.

```
vpnjk-2600-23#show ip route 10.0.68.0
Routing entry for 10.0.68.0/25
Known via "eigrp 1068", distance 90, metric 297246976, type internal
Redistributing via eigrp 1068
Last update from 10.2.124.22 on FastEthernet0/1.124, 00:52:47 ago
Routing Descriptor Blocks:
* 10.2.124.22, from 10.2.124.22, 00:52:47 ago, via FastEthernet0/1.124
  Route metric is 297246976, traffic share count is 1
  Total delay is 500100 microseconds, minimum bandwidth is 9 Kbit
  Reliability 255/255, minimum MTU 1476 bytes
  Loading 1/255, Hops 2
```

Now on router 2600-23, the delay value on Tunnel 901 is changed to advertise an equal cost path to router 2600-5.

```
vpnjk-2600-23#config t
Enter configuration commands, one per line.  End with CNTL/Z.
vpnjk-2600-23(config)#interface tunnel 901
vpnjk-2600-23(config-if)#delay 49990
```
vpnjk-2600-23(config-if)#end

vpnjk-2600-5#show ip route 10.0.68.0
Routing entry for 10.0.68.0/25
  Known via "eigrp 1068", distance 90, metric 297246976, type internal
  Redistributing via eigrp 1068
  Last update from 10.2.124.23 on FastEthernet0/1.124, 00:00:07 ago
  Routing Descriptor Blocks:
    * 10.2.124.22, from 10.2.124.22, 00:00:07 ago, via FastEthernet0/1.124
      Route metric is 297246976, traffic share count is 1
      Total delay is 500100 microseconds, minimum bandwidth is 9 Kbit
      Reliability 255/255, minimum MTU 1476 bytes
      Loading 1/255, Hops 2
    10.2.124.23, from 10.2.124.23, 00:00:07 ago, via FastEthernet0/1.124
      Route metric is 297246976, traffic share count is 1
      Total delay is 500100 microseconds, minimum bandwidth is 9 Kbit
      Reliability 255/255, minimum MTU 1476 bytes
      Loading 1/255, Hops 2

Now both WAN paths are used for the return path, as shown in Figure 9-9:

Figure 9-9 Frame Relay/Broadband—Downstream Option 2

Note that although Tunnel 0 and Tunnel 1 terminate on different branch routers, they both terminate on
the same head-end router; that is, 2600-22. While load-sharing across WAN links, a single head-end
router is decrypting all traffic from this branch.

This is not necessarily bad, because a good design implements sufficient crypto capacity to service all
remote branches on one surviving head-end. However, on the next branch, the network manager should
use delay values on the 900 series tunnel interfaces (902 and 903 perhaps) to prefer them over tunnel
interfaces 2 and 3. This spreads the load more equally across all head-end routers.
Verification

This section describes two methods of verification, and includes the following topics:

- Load Sharing
- CEF and NetFlow
- Backup Paths During Component Failures

Load Sharing

To demonstrate the load sharing, an IP traffic stream is generated with a traffic generation IOS router to simulate three traffic streams (ts#) from a single source IP address to three separate destination IP addresses.

<table>
<thead>
<tr>
<th>ts#</th>
<th>tos</th>
<th>len</th>
<th>protocol</th>
<th>source</th>
<th>destination</th>
<th>rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>B8</td>
<td>60</td>
<td>17</td>
<td>10.0.68.2</td>
<td>10.2.124.5</td>
<td>50 pps</td>
</tr>
<tr>
<td>2</td>
<td>B8</td>
<td>60</td>
<td>17</td>
<td>10.0.68.2</td>
<td>10.2.124.9</td>
<td>50 pps</td>
</tr>
<tr>
<td>3</td>
<td>B8</td>
<td>60</td>
<td>17</td>
<td>10.0.68.2</td>
<td>10.2.124.16</td>
<td>10 pps</td>
</tr>
</tbody>
</table>

The degree of load sharing, or the balance of packets between the two uplinks, depends on the number of hosts on the LAN and the number of flows. With one file transfer as the only traffic on the network between two hosts, only a single path is used; however, in this topology, per packet load sharing is not recommended because the likelihood of out-of-order packets is very likely given the dissimilar WAN links in the topology.

Figure 9-10 shows how the 110 packets per second (pps) were split between the two uplinks: 50 pps on the Frame Relay network and 60 pps on the broadband network.

The following list is a summary of the show interface commands issued to the routers under test.

Router 1712:

- Vlan1
  - Vlan1 is up, line protocol is up
– MTU 1500 bytes, BW 100000 Kb, DLY 100 usec
– 30 second input rate 36000 bits per second (bps), **61 pps** (routing protocol, NTP, and other management traffic as well as the load interval account for slight variations in the packet rates)
– 30 second output rate 1000 bps, 2 pps

• Tunnel 0
  – Tunnel 0 is up, line protocol is up
  – MTU 1514 bytes, BW 9 kbps, DLY 499900 usec,
  – 30 second input rate 0 bps, 0 pps
  – 30 second output rate 40000 bps, **60 pps**

• Tunnel 900
  – No test traffic routed out this interface

Router 2600-18:

• FastEthernet0/1
  – FastEthernet0/1 is up, line protocol is up
  – MTU 1500 bytes, BW 100000 kbps, DLY 100 usec,
  – 5 minute input rate 74000 bps, **119 pps**
  – 5 minute output rate 37000 bps, **60 pps**

• Tunnel 1
  – Tunnel1 is up, line protocol is up
  – MTU 1514 bytes, BW 9 kbps, DLY 500000 usec,
  – 30 second input rate 0 bps, 0 pps
  – 30 second output rate 33000 bps, **50 pps**

• Tunnel 901
  – No test traffic routed out this interface

**CEF and NetFlow**

Another means of verifying the packet flow is to issue these commands on router 2600-18 and to look at the NetFlow representation of the destination of the traffic as well as the CEF exact-route option. (See Figure 9-11.)
The NetFlow display shows that two of the flows are being sent back over the FastEthernet interface to the 1712 router supporting the broadband connection.

```plaintext
vpnjk-2600-18#show ip cache flow | beg SrcIf
SrcIf       SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/1.204     10.0.68.2     Fa0/1.204     10.2.124.16    11 7FD9 7FDA  6652
Fa0/1.204     10.0.68.2     Tu1          10.2.124.5     11 7FD9 7FDA    33K
Fa0/1.204     10.0.68.2     Fa0/1.204     10.2.124.9     11 7FD9 7FDA    33K
Fa0/1.204     10.0.68.1       Null          224.0.0.10      58 0000 0000   291

vpnjk-2600-18#show ip cef exact-route 10.0.68.2 10.2.124.5
10.0.68.2       -> 10.2.124.5     : Tunnel1 (next hop 10.0.68.138)

vpnjk-2600-18#show ip cef exact-route 10.0.68.2 10.2.124.9
10.0.68.2       -> 10.2.124.9     : FastEthernet0/1.204 (next hop 10.0.68.1)

vpnjk-2600-18#show ip cef exact-route 10.0.68.2 10.2.124.16
10.0.68.2       -> 10.2.124.16    : FastEthernet0/1.204 (next hop 10.0.68.1)
```

**Note**

The **CEF exact-route** command does not require traffic to be flowing to display the exact route. In fact, this command was used to verify which IP addresses to configure for the destination addresses on the traffic streams to generate this illustration.

**Backup Paths During Component Failures**

During the following component failures, the remote site maintains connectivity as described in Table 9-1.
This section describes the configuration of the components of the Frame Relay/broadband load sharing and backup solution, and includes the following topics:

- IPSec Head-end Routers
- Branch Cisco 1712 Router
- Branch Cisco 2600 Router
- Head-end Campus Router

### IPSec Head-end Routers

This section includes the configuration for the IPSec head-end routers.

#### 2600-22 Router

This is the first head-end router configuration:

```
! System image file is "flash:c2600-1k9o3s3-mz.122-15.T9"
version 12.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname vpnjk-2600-22
!
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
ip cef
!
```

### Table 9-1 Failure Scenarios and Backup Connectivity

<table>
<thead>
<tr>
<th>Failure Scenario</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec/GRE head-end router 2600-22 fails or is out of service</td>
<td>Remote router 1712-1 becomes the HSRP active router and uses Tunnel 900 (broadband WAN link) for all traffic.</td>
</tr>
<tr>
<td>IPSec/GRE head-end router 2600-23 fails or is out of service</td>
<td>No change—2600-18 continues as HSRP active router and Tunnels 1 and 0 (broadband and Frame Relay links) are still used.</td>
</tr>
<tr>
<td>Frame Relay network fails—total failure of both PVCs</td>
<td>Remote router 1712-1 becomes the HSRP active router and uses Tunnel 0 (broadband WAN link) for all traffic; 2600-18 can be accessed via its LAN interface.</td>
</tr>
<tr>
<td>Broadband network fails</td>
<td>Remote router 2600-18 is active HSRP router and Tunnel 1 (Frame Relay) is used for all traffic; 1712-1 can be accessed via its LAN interface.</td>
</tr>
</tbody>
</table>
Configuration

Chapter 9       Large Branch—Frame Relay/Broadband Load Sharing and Backup

9-18

V3PN: Redundancy and Load Sharing Design Guide

OL-7102-01

!!
crypto keyring GREEN
  pre-shared-key hostname vpnjk-2600-18.ese.cisco.com key nosxlerx
  pre-shared-key hostname vpn-jk2-1712-1.ese.cisco.com key siexrrax
!!
crypto isakmp policy 10
  encr 3des
  group 2
!!
crypto isakmp policy 20
  encr 3des
  authentication pre-share # This config will respond to IKE Aggressive Mode
    group 2
  crypto isakmp keepalive 10
  crypto isakmp profile AGGRESSIVE
    description Profile for IKE Aggressive Mode
      keyring GREEN
      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_TUNNEL
    match address GRE # This is an optional statement, see Caveats section
    !
crypto map DYNO-MAP local-address FastEthernet0/1.100
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!!
interface Tunnel0
  description 1712
  ip address 10.0.68.146 255.255.255.252
  ip summary-address eigrp 1068 10.0.0.0 255.0.0.0 5
delay 49990
  keepalive 10 3
  tunnel source 192.168.131.22
  tunnel destination 10.0.68.129
!!
interface Tunnel1
  description to 2600-18
  ip address 10.0.68.138 255.255.255.252
  ip summary-address eigrp 1068 10.0.0.0 255.0.0.0 5
  keepalive 10 3
  tunnel source 192.168.131.22
  tunnel destination 10.0.68.253
!!
interface FastEthernet0/1
  description dot1q
  no ip address
  ip route-cache flow
duplex auto
  speed auto
!!
interface FastEthernet0/1.100
  encapsulation dot1q 100
  ip address 192.168.131.22 255.255.255.224
  crypto map DYNO-MAP
interface FastEthernet0/1.124
  encapsulation dot1Q 124
  ip address 10.2.124.22 255.255.255.0
  standby ip 10.2.124.99
!
router eigrp 100
  network 10.0.0.0
  network 192.168.130.0 0.0.1.255
  no auto-summary
!
router eigrp 1068  # This AS is used for the Tunnel interfaces
  network 10.0.0.0
  no auto-summary
!
ip classless
!
! If a crypto ACL is used, define one ACL line for each tunnel interface
!
ip access-list extended GRE
  permit gre host 192.168.131.22 host 10.0.68.253
  permit gre host 192.168.131.22 host 10.0.68.129
!
!
rtr responder
alias exec shca show crypto ipsec sa det | inc eer|life
!
ntp server 192.168.130.1
!
end

2600-23 Router

This is the second head-end router configuration:

! System image file is "flash:c2600-ik903s3-mz.122-15.T9"
version 12.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
!
hostname vpnjk-2600-23
!
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
!
!
crypto keyring GREEN
  pre-shared-key hostname vpnjk-2600-18.ese.cisco.com  key nosxlerx
  pre-shared-key hostname vpn-jk2-1712-1.ese.cisco.com  key siexrrax
!
crypto isakmp policy 10
  encr 3des
  authentication pre-share  # This config will respond to IKE Aggressive Mode
group 2
crypto isakmp keepalive 10
crypto isakmp profile AGGRESSIVE
description Profile to test Initiating Aggressive Mode
keyring GREEN
  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
no crypto ipsec nat-transparency udp-encaps

crypto dynamic-map DYNO-TEMPLATE 10
  description dynamic crypto map
  set transform-set 3DES_SHA_TUNNEL
  match address GRE  # This is an optional statement, see Caveats section
qos pre-classify

! crypto map DYNO-MAP local-address FastEthernet0/1.100
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE

interface Tunnel900
  description Tunnel to vpn-jk2-1712-1
  ip address 10.0.68.134 255.255.255.252
  ip summary-address eigrp 1068 10.0.0.0 255.0.0.0 5
  keepalive 10 3
tunnel source 192.168.131.23
tunnel destination 10.0.68.129

interface Tunnel901
  description Tunnel to 2600-18 [over Frame]
  ip address 10.0.68.142 255.255.255.252
  ip summary-address eigrp 1068 10.0.0.0 255.0.0.0 5
delay 50010
  keepalive 10 3
tunnel source 192.168.131.23
tunnel destination 10.0.68.253

interface FastEthernet0/1
  description dot1q
  no ip address
  load-interval 30
duplex auto
speed auto

interface FastEthernet0/1.100
  description vlan 100
  encapsulation dot1Q 100
  ip address 192.168.131.23 255.255.255.224
  crypto map DYNO-MAP

interface FastEthernet0/1.124
  description vlan 124
  encapsulation dot1Q 124
  ip address 10.2.124.23 255.255.255.0
  standby ip 10.2.124.99
  standby priority 110

router eigrp 1068  # This AS is used for the Tunnel interfaces
  network 10.0.0.0
  no auto-summary
router eigrp 100  
   network 10.0.0.0  
   network 192.168.130.0 0.0.1.255  
   no auto-summary  
   no eigrp log-neighbor-warnings  
!  
ip classless  
!  
! If a crypto ACL is used, define one ACL line for each tunnel interface  
!  
ip access-list extended GRE  
   permit gre host 192.168.131.23 host 10.0.68.253  
   permit gre host 192.168.131.23 host 10.0.68.129  
!  
rtr responder  
!  
ntp server 192.168.130.1  
!  
end

Branch Cisco 1712 Router

The following is a configuration sample for the branch Cisco 1712 router.

Note

A complete configuration for this router has not been shown; among other items, a V3PN service policy has not been included in its entirety!

! System image file is "flash:c1700-k9o3sy7-mz.123-7.T"  
version 12.3  
service timestamps debug datetime msec localtime show-timezone  
service timestamps log datetime msec localtime show-timezone  
service password-encryption  
!  
hostname vpn-jk2-1712-1  
!  
clock timezone est -5  
clock summer-time edt recurring  
!  
ip cef  
!  
crypto isakmp policy 10  
   encr 3des  
      authentication pre-share  
# This configuration is initiating IKE Aggressive Mode  
group 2  
!  
crypto isakmp peer address 192.168.131.22  
set aggressive-mode password siexrrax  
set aggressive-mode client-endpoint fqdn vpn-jk2-1712-1.ese.cisco.com  
!  
crypto isakmp peer address 192.168.131.23  
set aggressive-mode password siexrrax  
set aggressive-mode client-endpoint fqdn vpn-jk2-1712-1.ese.cisco.com  
!  
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
mode transport
!
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac

crypto map BROADBAND 10 ipsec-isakmp
  description Crypto MAP
  set peer 192.168.131.22
  set transform-set 3DES_SHA_TUNNEL
  match address GRE_to_22
  qos pre-classify

crypto map BROADBAND 20 ipsec-isakmp
  description Crypto MAP
  set peer 192.168.131.23
  set transform-set 3DES_SHA_TUNNEL
  match address GRE_to_23
  qos pre-classify

!
!
!
!
!
interface Tunnel0
  description 2600-22
  bandwidth 9 # Default value
  ip address 10.0.68.145 255.255.255.252
  load-interval 30
delay 49990
  qos pre-classify
  keepalive 10 3
  tunnel source Loopback0
  tunnel destination 192.168.131.22

!
!
!
!
interface Tunnel900
  description To 2600-23
  ip address 10.0.68.133 255.255.255.252
  load-interval 30
  qos pre-classify
  keepalive 10 3
  tunnel source Loopback0
  tunnel destination 192.168.131.23
!
!
!
interface Loopback0
  ip address 10.0.68.1 255.255.255.128

!
!
!
interface FastEthernet0
  description Outside to DSL Modem
  bandwidth 256
  no ip address
  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 Vlan1
  description Inside Interface
  ip address 10.0.68.1 255.255.255.128
  no ip proxy-arp
ip route-cache flow
ip tcp adjust-mss 542
load-interval 30
delay 10
standby 68 ip 10.0.68.126
standby 68 priority 81
standby 68 preempt
!
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 foo@cisco.com password 7
ppp ipcp dns request
ppp ipcp wins request
crypto map BROADBAND
!
router eigrp 1068
  network 10.0.0.0
distribute-list VLAN_ONLY out Tunnel0
distribute-list VLAN_ONLY out Tunnel900
  no auto-summary
  no eigrp log-neighbor-warnings
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 239 name Broadband
!
!
ip access-list standard VLAN_ONLY
  permit 10.0.0.0/16 0.0.0.128
!
ip access-list extended GRE_to_22
  permit gre host 10.0.68.129 host 192.168.131.22
ip access-list extended GRE_to_23
  permit gre host 10.0.68.129 host 192.168.131.23
!
control-plane
!
rtr responder
rtr 99
type echo protocol icmpECHO 10.2.124.99 source-ipaddr 10.0.68.1
tos 192
frequency 10
rtr schedule 99 life forever start-time now
!
end
Branch Cisco 2600 Router

This configuration is for the branch Cisco 2600 router:

```
! System image file is "flash:c2600-ik9o3s3-mz.122-15.T9"
!
version 12.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname vpnjk-2600-18
!
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
ip cef
!
!
crypto isakmp policy 10
  encr 3des
  authentication pre-share # This configuration is initiating IKE Aggressive Mode
group 2
!
crypto isakmp policy 20
  encr 3des
group 2
crypto isakmp keepalive 10
!
crypto isakmp peer address 192.168.131.22
  set aggressive-mode password nosxlerx
  set aggressive-mode client-endpoint fqdn vpnjk-2600-18.ese.cisco.com
!
crypto isakmp peer address 192.168.131.23
  set aggressive-mode password nosxlerx
  set aggressive-mode client-endpoint fqdn vpnjk-2600-18.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
no crypto ipsec nat-transparency udp-encaps# There are no NAT devices in this topology
  # so regardless if this is enabled (as in
  # 1712 config) NAT-T will not be used.
!
crypto map FRAME local-address Loopback0
crypto map FRAME 10 ipsec-isakmp
description Crypto MAP
set peer 192.168.131.22
set transform-set 3DES_SHA_TUNNEL
match address GRE_to_22
qos pre-classify
crypto map FRAME 20 ipsec-isakmp
description Crypto MAP
set peer 192.168.131.23
set transform-set 3DES_SHA_TUNNEL
match address GRE_to_23
qos pre-classify
!
!
```
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 TEST
class VOICE
  priority 168
class INTERNETWORK-CONTROL
  bandwidth percent 5
  set dscp cs6
# Here we are setting IKE packets to CS6
class TRANSACTIONAL-DATA
  bandwidth percent 22
  class class-default
  fair-queue
!
!
!
interface Loopback0
  ip address 10.0.68.253 255.255.255.255
!
interface Tunnel1
  description to 2600-22
  bandwidth 9  # This is the default value for a tunnel
  ip address 10.0.68.137 255.255.255.252
  load-interval 30
gos pre-classify
  keepalive 10 3
tunnel source Loopback0
tunnel destination 192.168.131.22
!
interface Tunnel1901
  description 2600-23
  ip address 10.0.68.141 255.255.255.252
  load-interval 30
  delay 50010
gos pre-classify
  keepalive 10 3
tunnel source Loopback0
tunnel destination 192.168.131.23
!
interface Serial0/0
  bandwidth 2000
  no ip address
  encapsulation frame-relay
  load-interval 30
  frame-relay traffic-shaping
  frame-relay lmi-type cisco
!
interface Serial0/0.100 point-to-point
  description to vpn-jk-2600-20
  bandwidth 512
  ip address 10.0.65.1 255.255.255.252
  frame-relay class ts-branch
  frame-relay interface-dlci 100
  class ts-branch
crypto map FRAME

Note: One physical interface, two PVCs
! interface Serial0/0.101 point-to-point
description to vpn-jk2-3640-1
bandwidth 512
ip address 10.0.65.5 255.255.255.252
frame-relay interface-dlci 101
class ts-branch
crypto map FRAME
!
interface FastEthernet0/1
no ip address
ip route-cache flow
duplex auto
speed auto
!
interface FastEthernet0/1.204
description VLAN 204
encapsulation dot1Q 204
ip address 10.0.68.18 255.255.255.128
standby 68 ip 10.0.68.126
standby 68 preempt
standby 68 track Tunnel1 20 # If this interface goes down, HSRP priority will
debase by 20. Note the 1712 has a default priority
! of 81, which is 19 less than this router’s default
! value of 100.
standby 68 track Tunnel901
!
EIGRP is used to learn and advertise routes on the LAN and Tunnels
!
router eigrp 1068
passive-interface Serial0/0.100
passive-interface Serial0/0.101
network 10.0.0.0
distribute-list VLAN_ONLY out Tunnel1
distribute-list VLAN_ONLY out Tunnel901
no auto-summary
no eigrp log-neighbor-warnings
!
RIP is used to learn a route to 192.168.130.0/23, the IPSec/GRE head-ends
So RIP V2 is our WAN (Frame-Relay) routing protocol
router rip
version 2
passive-interface FastEthernet0/1.204
passive-interface Tunnel1
passive-interface Tunnel901
network 10.0.0.0
no auto-summary
!
!
ip access-list standard VLAN_ONLY
permit 10.0.68.0 0.0.0.128
!
ip access-list extended GRE_to_22
permit gre host 10.0.68.253 host 192.168.131.22
ip access-list extended GRE_to_23
permit gre host 10.0.68.253 host 192.168.131.23
ip access-list extended IKE
permit udp any eq isakmp any eq isakmp
!
map-class frame-relay ts-branch
frame-relay cir 486400
frame-relay bc 4864
frame-relay be 0
Head-end Campus Router

This configuration is for the head-end campus router.

Note

This is an abbreviated configuration. The only role for the head-end campus router in this configuration is to demonstrate the ability to load share from campus to remote LAN network. This router and the two IPSec/GRE head-end routers are EIGRP neighbors.

Show Commands

This section contains Cisco IOS show commands as an illustration of Routing Information Protocol Version 2 (RIP V2) configured on the Frame Relay network.

Some customers run RIP on their Frame Relay deployments because of its slower convergence and perhaps less CPU and memory requirements than other protocols. Because of this, RIP V2 is configured on the Frame Relay network so that the remote router can learn how to reach the network address of the GRE and IPSec head-end routers in this configuration.

The Frame Relay router has one physical interface with two permanent virtual circuits (PVCs) to the enterprise head-end routers. Because of this, there are two RIP learned routes in the routing table.

```
vpnjk-2600-18#show ip route rip
R 192.168.130.0/23 [120/1] via 10.0.65.2, 00:00:14, Serial0/0.100
   [120/1] via 10.0.65.6, 00:00:21, Serial0/0.101
```

The above RIP route provides reachability for these destination addresses.

```
vpnjk-2600-18#show run | inc set peer|tunnel destination
set peer 192.168.131.22
set peer 192.168.131.23
tunnel destination 192.168.131.22
tunnel destination 192.168.131.23
```
Cisco IOS Versions Tested

The following Cisco IOS versions were used in the test topology:

- vpnjk-2600-23—c2600-ik9o3s3-mz.122-15.T9
- vpnjk-2600-22—c2600-ik9o3s3-mz.122-15.T9
- vpnjk-2600-18—c2600-ik9o3s3-mz.122-15.T9
- vpn-jk2-1712-1—c1700-k9o3sy7-mz.123-7.T

Caveats

In the IPSec/GRE head-end configuration examples, dynamic crypto maps are used for the head-end routers rather than static crypto maps. This is desirable because it saves head-end configuration lines, and therefore configuration size and complexity. Because the topology runs both a routing protocol and GRE keepalives in the tunnel interfaces, the IPSec tunnels are up and active at all times because of the keepalives, so there is no technical reason that the head-end router must have a static crypto map.

Note

There may be no need to run both a Layer 2 and Layer 3 keepalive when one might suffice. If the Layer 3 keepalives are lost, the EIGRP neighbor goes down; if the GRE keepalives are lost, the tunnel interface goes down. It may be desirable from a network management standpoint to be able to generate a Simple Network Management Protocol (SNMP) trap when the GRE interface goes down.

On the dynamic crypto map, there is no need to specify an access list. When the IPSec tunnel comes up, the remote router supplies the necessary access list and the reverse of it is dynamically entered in the head-end crypto map entry.

As long as the remote peer is up, the GRE keepalives are encrypted and sent to the remote peer. If the remote peer IPSec tunnel is not up, the head-end router sends GRE keepalives toward the Internet, and because there is no crypto map access list statically defined, they are sent out the interface unencrypted. User data traffic is not sent unencrypted, because the tunnel must be up before any user data is sent, but GRE keepalives are sent unencrypted.

Most ISPs and enterprise customers block RFC 1918 addressing from reaching the Internet, and in the configuration described in this chapter, RFC 1918 addresses are used for the tunnel source at the remote router so that these unencrypted GRE packets can be blocked from reaching the Internet.

Even if unencrypted GRE keepalive packets reach an Internet router, it is unlikely to present a serious security exposure; however, be aware of the implications of not specifying an ACL on a dynamic crypto map with GRE tunnels.

Summary

With the increased availability of broadband WAN at price points that are similar to Basic Rate ISDN, enterprise customers will look to this new technology to offer increased bandwidth for both backup and load sharing applications.