V3PN: Redundancy and Load Sharing Design Guide

OL-7102-01
Version 1.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

V3PN: Redundancy and Load Sharing Design Guide

CONTENTS

CHAPTER 1 **V3PN: Redundancy and Load-Sharing Introduction** 1

Introduction 2

Solution Overview 2

Small Branch Deployments 2

Large Branch Deployments 3

General Deployment and V3PN Redundancy Issues 3

CHAPTER 2 **Small Branch—DSL with ISDN Backup** 1

Solution Characteristics 2

Traffic Encapsulated in IPSec 2

Redundant IPSec Head-ends 2

IPSec Peering 2

GRE Tunnel Controls Dial Backup 3

Digital Certificates and Dynamic Crypto Maps 3

Reverse Route Injection 3

Remote IP Routing—Floating Static and Specific Routes 4

Head-end IP Routing Requirements 4

Topology 4

Failover/Recovery Time 6

V3PN QoS Service Policy for Basic Rate ISDN 6

Performance Results 7

Implementation and Configuration 8

Remote GRE Tunnel Interface 8

Head-end GRE Router 9

IPSec Head-end Routers 10

Remote Router 13

Show Commands 16

Cisco IOS Versions Tested 19

Caveats 19

Debugging 20

Summary 20

CHAPTER 3 Small Branch—Cable with DSL Backup 1

Solution Characteristics 2

Topology 2

Failover/Recovery Time 3

Temporary Failure with Service Restoration 4

Failure of Primary Path—Recovery over Backup Path 5

Routing Topology Following Network Recovery 6

V3PN QoS Service Policy 8

Performance Results 8

Implementation and Configuration 9

Remote Router SAA and Tracking Configuration 9

Head-end SAA Target 10

IPSec Head-end Routers 11

Backup IPSec Peer 11

Primary IPSec Peers 13

Remote Router 16

Show Commands 20

Cisco IOS Versions Tested 20

Summary 21

CHAPTER 4 Small Branch—DSL with Async Backup 1

Solution Characteristics 1

Topology 2

Failover/Recovery Time 3

V3PN QoS Service Policy 4

Performance Results 4

Implementation and Configuration 5

Remote Router SAA and Tracking 5

Head-end SAA Target Router 6

IPSec Head-end Routers 6

Remote Router—Cisco 1711 6

Debugging 11

Cisco IOS Versions Tested 13

Summary 13

CHAPTER 5 Small Branch—Dial Backup to Cisco VPN 3000 Concentrator 1

Topology 1

Failover/Recovery Time 2

Caveats 3

EZVPN—Tunnel Goes to SS_OPEN State on Re-establishing Connection 3

RRI Fails to Insert the Appropriate Static Route 5

V3PN QoS Service Policy 5

Performance Results 5

Implementation and Configuration 6

Enterprise Intranet Backbone Router(s) 7

IPSec Primary and SAA Target Router 8

Primary WAN Router 9

Remote IPSec (1712) Router 11

Cisco VPN 3000 Concentrator Configuration 15

Interfaces 15

Groups 15

Users 19

Policy Management/Traffic Management /SAs 21

System/Tunneling Protocols/IPSec/IKE 22

Cisco IOS Versions Tested 23

Summary 23

CHAPTER 6 Small Branch—Load Sharing on Dual Broadband Links 1

Topology 2

Cable (DHCP) and DSL (PPPoE) 2

Load Sharing Behind Two Broadband Routers 3

Failover/Recovery Time 4

V3PN QoS Service Policy 5

Implementation and Configuration 5

Remote 1751 Router (DHCP and PPPoE) 5

Remote 1751 Router (DHCP and DHCP) 10

Alpha IPSec Head-end 10

Bravo IPSec Head-end 12

Enterprise Intranet Router 14

Show Commands 15

Enterprise Intranet Router 15

Remote 1751 Router (DHCP and PPPoE Configuration) 16

Fail Alpha ISP Network 18

Fail Bravo ISP Network 18

Remote 1751 Router (DHCP and DHCP Configuration) 19

Fail Alpha ISP Network 20

Fail Bravo ISP Network 21

Cisco IOS Versions Tested 22

Caveats 22

CEF Issue 22

Fast Switching Issue 23

Summary 25

CHAPTER 7 Small Branch—Wireless Broadband Deployment 1

Solution Characteristics 1

Advantages 1

Disadvantages 2

Topology 2

Single WAN Interface 3

Multi-WAN Interface 3

Failover/Recovery Time 4

Performance Results 5

Average Jitter Comparison 5

Voice Loss 7

Average Latency 8

Mission Critical Response Time 8

Wireless Broadband Hardware Components 9

Wireless Broadband Modem 9

Yagi Antenna and Cables 9

Cisco 1711 and Cabling 10

Yagi Antenna Aiming 10

Mobility Manager 11

Verification 12

Configuration 13

Multi-WAN Cisco 1711 Router 13

Single WAN Remote Router 19

EZPVN Head-end Server 23

Primary IPSec Head-end 25

Secondary IPSec Head-end 27

Cisco IOS Versions Tested 28

Caveats 29

EZVPN 29

DHCP Server 29

Summary 30

CHAPTER 8 **Small Branch—Dual Hub/Dual DMVPN 1**

Solution Characteristics 1

Topology 2

Failover/Recovery Time 3

V3PN QoS Service Policy 4

DMVPN (GRE Transport Mode) ESP 3DES/SHA 5

DMVPN (GRE Transport Mode) ESP 3DES/SHA with NAT-T 6

Sample V3PN Relevant QoS Configuration 8

TCP Maximum Segment Size 8

IP MTU of Tunnel interfaces 9

Class-map Configuration 11

Weighted fair-queue Configured on Ethernet Interfaces 12

Service Assurance Agent (SAA) VoIP UDP Operation 13

Routing 16

Access Control 18

Performance Testing 20

Original and Revised Configurations 21

Impact of NAT-T 21

Test Topology 22

Implementation and Configuration 23

Remote Branch Router 23

Primary Head-end Router 27

Cisco IOS Versions Tested 30

Summary 30

CHAPTER 9 **Large Branch—Frame Relay/Broadband Load Sharing and Backup 1**

Solution Characteristics 2

Topology 2

Failover/Recovery Time 3

Implementation 3

GRE Tunnels 3

Summary Route Advertised 5

Bandwidth and Delay 6

Delay 6

Bandwidth 6

Branch EIGRP and Addressing 8

Summary Advertisement Traverses the LAN 9

Head-end to Branch Considerations 11

Head-end to Branch Load Sharing Example 12

Verification 14

Load Sharing 14

CEF and NetFlow 15

Backup Paths During Component Failures 16

Configuration 17

IPSec Head-end Routers 17

2600-22 Router 17

2600-23 Router 19

Branch Cisco 1712 Router 21

Branch Cisco 2600 Router 24

Head-end Campus Router 27

Show Commands 27

Cisco IOS Versions Tested 28

Caveats 28

Summary 28

CHAPTER 10 Large Branch—Multilink PPP 1

Topology 1

Traffic Profile 2

V3PN QoS Service Policy 5

Implementation and Configuration 7

Remote Router 7

Head-end Router 10

Show Commands 14

Cisco IOS Versions Tested 16

Caveats 16

Drops In Class VIDEO-CONFERENCING 16

Incorrect Packet Classification 17

Summary 17

CHAPTER 11 Large Branch—Inverse Multiplexing over ATM (IMA) 1

Topology 1

Implementation and Configuration 2

Head-end Router 2

Remote Router 3

Performance 4

Summary 4

APPENDIX A Lab Topology 1

APPENDIX B References and Reading 1

Documents 1

Request For Comment Papers 1

Websites 2

Enterprise Solutions Engineering (ESE) 2

APPENDIX C Acronyms and Definitions 1

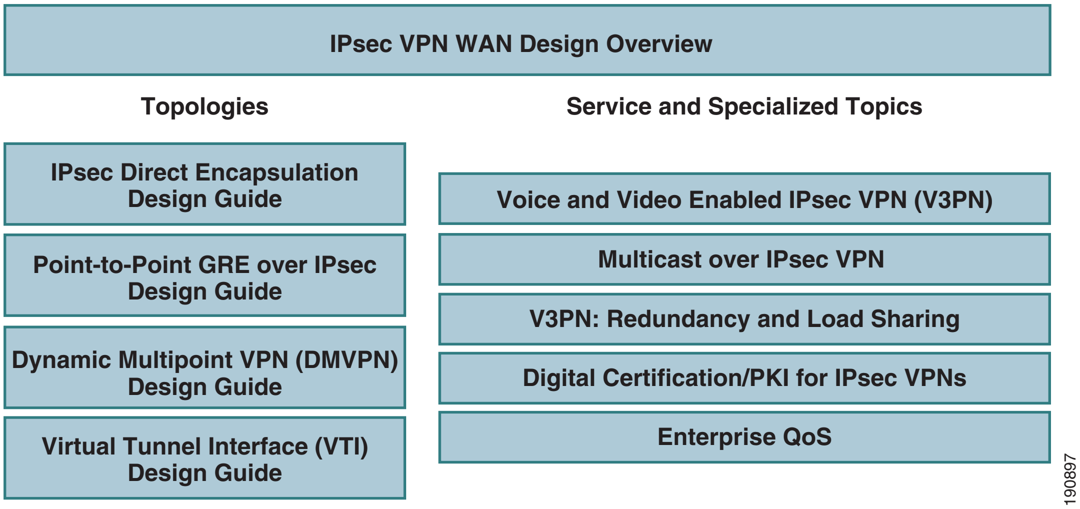
CHAPTER 1

V3PN: Redundancy and Load-Sharing Introduction

This design guide defines the comprehensive functional components required to build an enterprise virtual private network (VPN) solution that can transport IP telephony and video. This design guide identifies the individual hardware requirements and their interconnections, software features, management needs, and partner dependencies, to enable customers to deploy, manage, and maintain an enterprise VPN solution.

This design overview is part of a series of design guides, each based on different technologies for the IPsec VPN WAN architecture. (See Figure 1.) Each technology uses IPsec as the underlying transport mechanism for each VPN.

Figure 1 IPsec VPN WAN Design Guides


IPsec VPN WAN Design Overview
Topologies
Service and Specialized Topics
IPsec Direct Encapsulation Design Guide
Point-to-Point GRE over IPsec Design Guide
Dynamic Multipoint VPN (DMVPN) Design Guide
Virtual Tunnel Interface (VTI) Design Guide
Voice and Video Enabled IPsec VPN (V3PN)
Multicast over IPsec VPN
V3PN: Redundancy and Load Sharing
Digital Certification/PKI for IPsec VPNs
Enterprise QoS
190897

This chapter includes the following sections:

- Introduction
- Solution Overview
- General Deployment and V3PN Redundancy Issues

Introduction

This design and implementation guide extends the Cisco Architecture for Voice, Video, and Integrated Data (AVVID) by enabling applications such as voice and video to be extended to emerging WAN media. Previous VPN design guides have focused on Internet T1, Frame Relay, and the broadband offerings of DSL and cable.

This design guide builds on the following series of design guides:

- *Voice and Video Enabled IPSec VPN (V3PN) SRND***Doc No:** EDCS-220772
- *Business Ready Teleworker SRND* **Doc No:** EDCS-267136

Note These guides are available at http://www.cisco.com/go/srnd**.**

The pressure to reduce recurring WAN expenses has led to increasing customer acceptance of emerging WAN media, along with the need to provide design guidance for implementation of broadband as a backup technology to traditional WAN media. Additionally, customers are implementing broadband circuits as the primary WAN media and look to traditional dial solutions to provide backup to the broadband circuit.

Situations in which a single T1 bandwidth is not sufficient but a T3 is more bandwidth and more costly than required encourage the implementation of multiple T1 circuits. In these instances, customers often struggle with the best means of providing load sharing when the visibility to individual data flows are hidden within an IPSec tunnel.

This guide provides guidance for designs in which new broadband offerings are used in conjunction with traditional WAN media. The focus remains enabling quality of service (QoS) to support voice; however, some deployments may not offer sufficient bandwidth to provide voice support on all interfaces. These issues are articulated in this guide.

Many of these designs apply in environments where QoS is enabled to support point-of-sale or financial transactions in place of voice.

Solution Overview

This solution is delineated in two main components:

- Small Branch Deployments
- Large Branch Deployments

Small Branch Deployments

This design guide describes seven models within the small branch deployment category. The first example shows a customer implementation of triggering dial backup by using a generic routing encapsulation (GRE) tunnel and enabling keepalives within the tunnel to verify connectivity and to trigger dial backup upon loss of connectivity. The GRE tunnel in this example does not encapsulate end-user data traffic; the tunnels only purpose is to verify connectivity. This implementation does not require any new features because the GRE Tunnel Keepalive feature was released in Cisco IOS Release 12.2(8)T. There is no requirement to run a routing protocol or to configure IP addressing for the GRE tunnel.

Several of the small branch deployment models make use of the Reliable Static Routing Backup Using Object Tracking feature introduced in Cisco IOS Release 12.3(2)XE for implementing dial backup on the Cisco 1700 Series routers.

Use of the **ip dhcp-client default-router distance** command is the key to using a primary interface that obtains its IP address via DHCP. This feature is listed as a DDTs resolved in 12.3(2)XC.An example is shown using cable as the primary interface with DSL as the backup interface, but could also be used as a configuration guide if Async or Basic Rate Interface (BRI) is used in place of the backup DSL interface. Both Async and BRI configurations are shown in the sample deployments.

The wireless broadband deployment model shows a Cisco 1711 configured with three WAN interfaces: the wireless broadband interface, an interface to a DSL router, and an Async dial-up interface. You can connect any of the three interfaces to the router to establish connectivity, or you can connect them all for high availability.

From an IPSec authentication standpoint, use of digital certificates, EZVPN, and initiating and responding to Internet Key Exchange (IKE) aggressive mode with pre-shared keys are illustrated. Some of these features were incorporated in Cisco IOS 12.2(15)T (**crypto isakmp profile** and **crypto keyring**), and responding to IKE aggressive mode is a Cisco IOS 12.3 feature.

One small branch deployment model uses a Cisco IOS IPSec head end for the primary connectivity and a Cisco VPN 3080 Concentrator for the dial backup connectivity.

Large Branch Deployments

The following three large branch deployments are described:

- Frame Relay with broadband load sharing and backup
- Multilink point-to-point protocol (MLPPP)
- Inverse multiplexing over ATM (IMA)

There were no surprises with Multilink PPP or IMA: these chapters and the test results are included and tested as a verification of capability. However, a video conference traffic stream was added in one of the tests because one rationale for bandwidth greater than a single T1/E1 is to include video conferencing to a remote location.

The chapter on Frame Relay with broadband load sharing and backup is most applicable for retail store locations that are currently using a traditional Frame Relay network, but want to take advantage of low cost broadband connections to supplement the existing bandwidth and provide an always available backup path. There will be an increasing migration from Frame Relay to broadband, and this method can also be used as a transition phase that minimizes the risk of a wholesale cutover from one technology to another.

General Deployment and V3PN Redundancy Issues

Each chapter in this guide depicts a specific deployment model, and can be used as a self-contained entity, in that the relevant configuration examples for both the remote and head-end routers are illustrated where practical.

However, these deployment models can also be mixed and matched. For example, the chapter showing the use of GRE tunnels to verify connectivity uses DSL as the primary path with Basic Rate ISDN as the back-up connection could draw configuration examples for Async as backup and be a perfectly acceptable design.

The following general assumptions are made:

- DSL examples show the use of PPP over Ethernet (PPPoE) with the PPPoE session terminating on the IPSec router. If in customer deployments of DSL, PPPoE is not used or is terminated on a service provider or separate router, the IPSec router obtains its outside IP address via DHCP from the upstream router. In this case, the DSL connection is similar to the outside interface configuration used for cable.
- For broadband examples, the IP address of the remote router is dynamically assigned. As such, the head-end IPSec routers implement dynamic crypto maps.
- Some form of QoS is applied to support voice or mission-critical applications. Although voice is not always a requirement for small branch deployments, mission-critical applications such as credit card authorizations or other point-of-sale applications benefit from QoS where practical.
- If voice cannot be provisioned because of lack of bandwidth, for example with Async backup, some means of blocking voice is implemented on the router. The goal is to allow voice calls where possible but never to provide a call appearance but not a reasonable expectation of acceptable voice quality.
- IPSec encryption is implemented not only for user data traffic but also for control plane traffic such as GRE keepalives or Service Assurance Agent (SAA) probes. Digital certificate and RADIUS servers are also accessed through an IPSec tunnel from the remote routers to the head end; there should be no need to expose these servers to the Internet without protection from some firewall and intrusion detection system (IDS) scheme.
- It should be expected and practical to implement multiple head-end devices, WAN and IPSec routers or concentrators to provide redundancy at the central site. A single link or device failure should not cause an unrecoverable outage.

This guide provides reasonably complete configuration examples, but assumes the reader is familiar with other V3PN design guides and best practices of network security.

Each chapter describes a particular deployment model and is intended to be a complete review of the concepts and configurations required to implement the design.

CHAPTER 2

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.

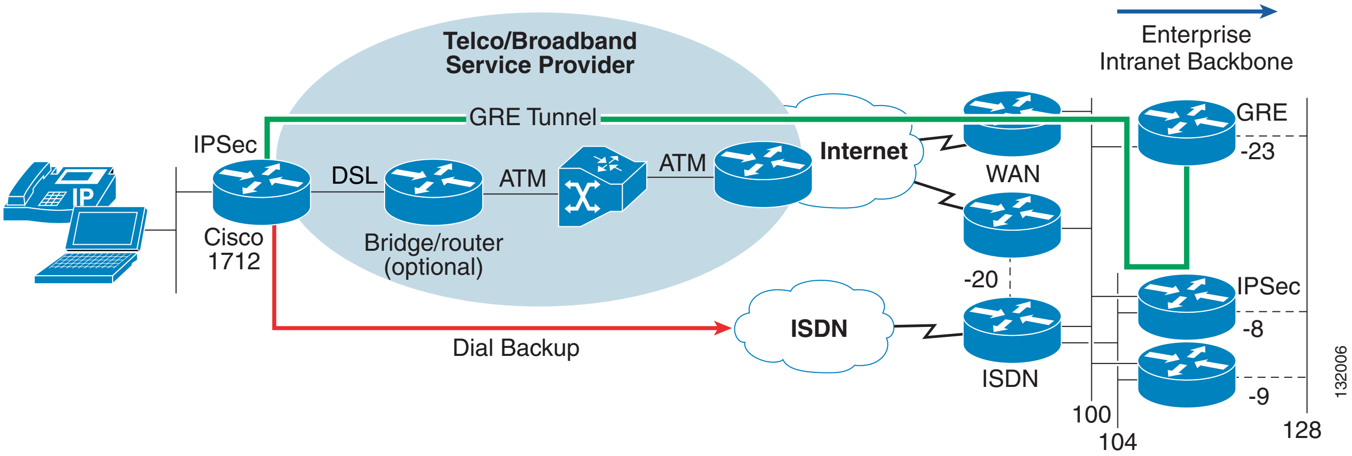
Head-end IP Routing Requirements

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.

Figure 2-1 Topology for DSL with ISDN Backup



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#

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 ESE branch traffic profile (for details see *http://wwwin-eng.cisco.com/Eng/ESE/VPN/Design/V3PNDesignGuide.doc*) was used over the backup path with one G.729 voice call active.The goal of this testing is to determine encrypted voice performance with multilink PPP and LFI configured on the BRI interface.

Note Performance results for the primary path are similar to those presented in the *Business Ready Teleworker SRND***,** which is available at http://www.cisco.com/go/srnd. The Cisco 1712 router has not been included in the above guidesbut will be in future updates. 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

	Call Leg	Chariot Voice Drops %	Chariot RFC 1889 Jitter	Chariot One-way Delay
Cisco 1712 router	Branch -> Head	0%	10.7 ms	39 ms
	Head -> Branch	0.04%	11.4 ms	39 ms

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.

Note The examples do not show the use of Network Address Translation (NAT), inbound access lists or firewall feature set. Examples of these and other security features can be seen in the *Business Ready Teleworker SRND*, which is available at http://www.cisco.com/go/srnd.

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.

```
!
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:

```
!
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.

```
vpnjk-2600-23>sh ip route 10.0.68.0 255.255.255.0 longer-prefixes
…
     10.0.0.0/8 is variably subnetted, 16 subnets, 8 masks
D EX    10.0.68.0/25
           [170/10258432] via 192.168.131.8, 00:00:01, FastEthernet0/1.100
D EX    10.0.68.0/24
           [170/10258432] via 192.168.131.8, 00:01:03, FastEthernet0/1.100
```

Because IP routing decisions are always made on the longest prefix match, the /25 route to network 10.0.68.0 is followed rather than the /24 route. Recall that VLAN 100 is the primary VLAN and VLAN 104 is the backup VLAN. Interface FastEthernet0/1.100 is in VLAN 100 and FastEthernet0/1.104 is in VLAN 104. The sub-interface number equates to the VLAN number in these examples.

```
vpnjk-2600-8#sh ip route 10.0.68.0 255.255.192.0 longer-prefixes


Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 10 subnets, 6 masks
D       10.0.64.0/18
           [90/3014400] via 192.168.131.3, 00:26:39, FastEthernet0/1.100
           [90/3014400] via 192.168.131.2, 00:26:39, FastEthernet0/1.100
           [90/3014400] via 192.168.131.70, 00:26:39, FastEthernet0/1.104
S       10.0.68.0/25 [1/0] via 0.0.0.0, FastEthernet0/1.100
S       10.0.68.0/24 [1/0] via 0.0.0.0, FastEthernet0/1.104
```

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:

```
!
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 6122A4EC000000000021
!
!
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-transparency udp-encaps
!
!                          # Both crypto maps will reference this template
!
crypto dynamic-map DYNO-TEMPLATE 10
 description dynamic crypto map
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
 reverse-route
 qos pre-classify
!
!
!                           # DYNO-MAP on VLAN 100 is the primary crypto
crypto map DYNO-MAP local-address FastEthernet0/1.100
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
!                          # BRI-MAP on VLAN 104 is the backup crypto
!
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 192.168.131.8 255.255.255.224
 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 610BE2E400000000001F
 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 6109335700000000003A
 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
!
!                      # 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
 tx-ring-limit 1
 tx-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
 ppp multilink links minimum 2           # Both B Channels will be brought up immediately
 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
!
ip route 0.0.0.0 0.0.0.0 Dialer1 240
!
!                # This route will force the IKE and IPSec packets to peers
!                # 192.168.131.8 and 192.168.131.9 out Dialer1 interface.
!                # 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
```

```
     192.168.17.0/32 is subnetted, 2 subnets
C       192.168.17.1 is directly connected, Dialer1
C       192.168.17.4 is directly connected, Dialer1
S*   0.0.0.0/0 is directly connected, Dialer1
```

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.

```
vpn-jk2-1712-1#sh int tu 900
Tunnel900 is up, line protocol is up
  Hardware is Tunnel
  Description: tunnel to vpn-jk-2600-23
  Backup interface BRI0, failure delay 0 sec, secondary disable delay 0 sec,
```

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

```
vpn-jk2-1712-1#sh int tu 900
Tunnel900 is up, line protocol is down
  Hardware is Tunnel
  Description: tunnel to vpn-jk-2600-23
  Backup interface BRI0, failure delay 0 sec, secondary disable delay 0 sec,
```

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

```
vpn-jk2-1712-1#sh ip route | begin Gateway
Gateway of last resort is 10.0.128.2 to network 0.0.0.0

     192.168.131.0/24 is variably subnetted, 3 subnets, 2 masks
S       192.168.131.68/31 [1/0] via 10.0.128.2
S       192.168.131.8/31 is directly connected, Dialer1
S       192.168.131.23/32 is directly connected, Dialer1
     10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C       10.0.68.0/25 is directly connected, Vlan1
C       10.0.128.2/32 is directly connected, BRI0
C       10.0.128.0/30 is directly connected, BRI0
     192.168.17.0/32 is subnetted, 2 subnets
C       192.168.17.1 is directly connected, Dialer1
C       192.168.17.4 is directly connected, Dialer1
S*   0.0.0.0/0 [1/0] via 10.0.128.2
```

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.

```
vpn-jk2-1712-1#show cry eng conn act

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
 164 BRI0            10.0.128.1      set    HMAC_SHA+3DES_56_C        0        0
 167 Dialer1         192.168.17.4    alloc  NONE                      0        0
 168 Dialer1         192.168.17.4    alloc  NONE                      0        0
 200 BRI0            10.0.128.1      set    HMAC_SHA+3DES_56_C        0       18
 201 BRI0            10.0.128.1      set    HMAC_SHA+3DES_56_C       12        0

vpn-jk2-1712-1#sh cry isa sa
```

```
dst             src             state          conn-id slot
192.168.131.9   192.168.17.4    MM_NO_STATE        167    0 (deleted)
192.168.131.68  10.0.128.1      QM_IDLE            164    0
192.168.131.8   192.168.17.4    MM_NO_STATE        168    0
```

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
```

```
   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.

```
vpnjk-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:

```
vpnjk-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.

```
vpnjk-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.

```
vpnjk-2600-8#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
```

```
Internet  10.0.68.2              0   Incomplete      ARPA
Internet  10.0.68.1              0   Incomplete      ARPA
```

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.

CHAPTER 3

Small Branch—Cable with DSL Backup

This chapter includes the following sections:

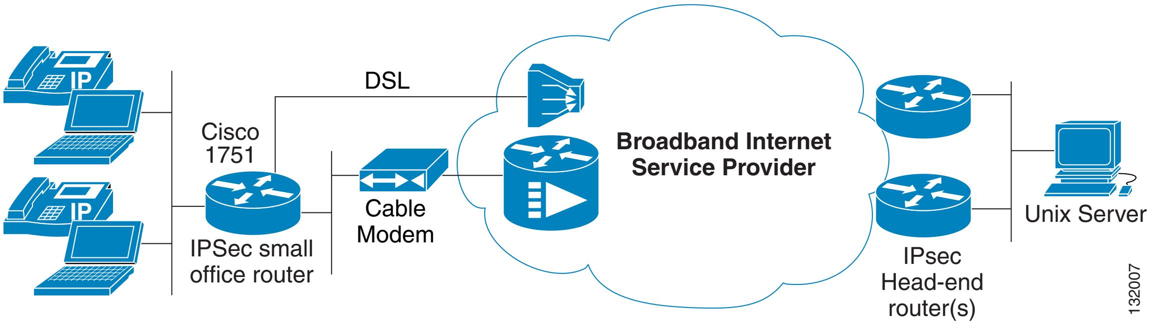
- Solution Characteristics
- Topology
- Failover/Recovery Time
- V3PN QoS Service Policy
- Performance Results
- Implementation and Configuration
- Cisco IOS Versions Tested
- Summary

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

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

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

Figure 3-1 DSL with Cable Backup Topology



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

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

Solution Characteristics

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

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

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

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

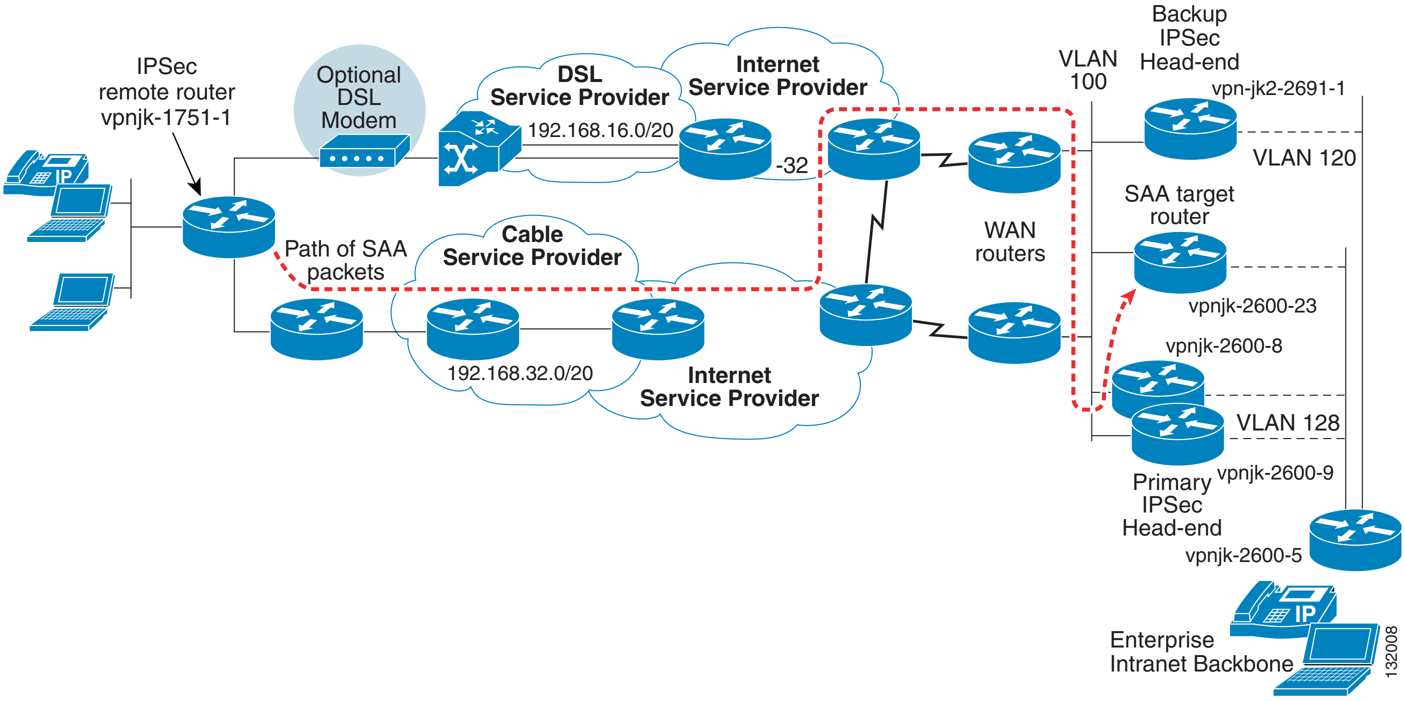
If the pings/probes fail, the static route for the primary path is removed from the routing table, allowing a static route with a higher administrative distance to be inserted into the routing table as an alternate default route. The pings/probes continue to be attempted over the primary interface. If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

Topology

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

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

Figure 3-2 Test Topology—Cable with DSL Backup



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

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

Failover/Recovery Time

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

This section includes the following topics:

- Temporary Failure with Service Restoration
- Failure of Primary Path—Recovery over Backup Path
- Routing Topology Following Network Recovery

Temporary Failure with Service Restoration

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

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

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

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

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

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

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

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

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

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

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

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

```
Dec 19 13:27:41.754 est: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than
(2000)msecs (0/0),process = Crypto IKMP.
-Traceback= 802971E8 80294574 8129E55C 81295D6C 81294760 81294304 812906D0 812635A8
812869FC 81263EC4 8125F278 8125D9F0 8127F120 81 [1]

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

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

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

[1] The CPU HOG messages are an anomaly with the release tested. This is likely because of CSCec05368-Certificate validation has poor performance.

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

Failure of Primary Path—Recovery over Backup Path

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Routing Topology Following Network Recovery

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

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

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

```
traceroute 10.2.128.5

Type escape sequence to abort.
Tracing the route to 10.2.128.5

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

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

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

```
vpnjk-2600-5#show ip eigrp topology all-links   | begin 10.0.68.0
P 10.0.68.0/25, 1 successors, FD is 6925056, serno 1710
        via 10.2.128.9 (6925056/6922496), FastEthernet0/1.128
        via 10.2.120.4 (10258432/10255872), FastEthernet0/1.120
        via 10.2.124.23 (6927616/6925056), FastEthernet0/1.124
```

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

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

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

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

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

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

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

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

V3PN QoS Service Policy

The Qos Service Policy in this solution is taken from the *Business Ready Teleworker SRND* available at http://www.cisco.com/go/srnd.

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

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

```
policy-map Shaper-DSL
 class class-default
```

```
  shape average 182400 1824
  service-policy V3PN-Small_Branch
policy-map Shaper-cable
 class class-default
  shape average 364800 3648
  service-policy V3PN-Small_Branch
!
!
interface Ethernet0/0
 description to DSL MODEM
 bandwidth 256
 no ip address
 service-policy output Shaper-DSL
 …
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Ethernet1/0
 description To CABLE MODEM
 bandwidth 384
 ip dhcp client route track 123
 ip address dhcp
 service-policy output Shaper-cable
 …
```

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

Performance Results

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

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

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

Performance results for voice and data on either the primary or backup path are similar to what is presented in the *Business Ready Teleworker SRND* (http://www.cisco.com/go/srnd)**.** This guide has performance data for both one and two concurrent G.729 voice calls.

Implementation and Configuration

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

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

Note The examples do not show the use of NAT, inbound access lists, or the firewall feature set. Examples of these and other security features can be seen in the *Business Ready Teleworker SRND* at the following URL: http://www.cisco.com/go/srnd.

This section includes the following topics:

- Remote Router SAA and Tracking Configuration
- Head-end SAA Target
- IPSec Head-end Routers
- Remote Router
- Show Commands

Remote Router SAA and Tracking Configuration

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

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

```
ip dhcp-client default-router distance 239
!
track 123 rtr 23 reachability
 delay down 60 up 5
!
interface Ethernet1/0
 description To CABLE MODEM
 bandwidth 384
 ip dhcp client route track 123
 ip address dhcp
!
ip route 0.0.0.0 0.0.0.0 Dialer1 240 name Backup_Path
!
ip route 192.168.131.4 255.255.255.255 Dialer1 name Backup_Peer
!
ip route 192.168.131.23 255.255.255.255 dhcp      # SAA Target Router
ip route 192.168.131.8 255.255.255.254 dhcp       # Primary IPSec Head-ends
!
rtr 23
```

```
 type udpEcho dest-ipaddr 192.168.131.23 dest-port 57005 source-ipaddr 10.0.68.5
source-port 48879
 tos 192
 timeout 1000
 owner TRACK123
 tag Object Tracking
 frequency 20
 lives-of-history-kept 1
 buckets-of-history-kept 10
 filter-for-history failures
rtr schedule 23 start-time now life forever
!
```

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

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

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

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

Head-end SAA Target

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

```
rtr responder
```

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

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

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

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

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Vi1            192.168.131.23  Local          10.0.68.5       11 C0  10       1
DEAD /0  0                     BEEF /0  0     0.0.0.0              44      0.0
```

```
Vi1            192.168.131.8   Local          192.168.17.3    32 00  10       3
B92C /0  0                     C0FA /0  0     0.0.0.0                96     1.6
Vi1            192.168.131.23  Local          10.0.68.5       11 C0  10       1
07AF /0  0                     BEEF /0  0     0.0.0.0                36     0.0
```

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

IPSec Head-end Routers

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

Backup IPSec Peer

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

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname vpn-jk-2691-1
!
boot-start-marker
boot system flash c2691-ik9o3s-mz.123-5
boot system flash c2691-ik9o3s-mz.122-13.T10
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 [removed]
!
memory-size iomem 15
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host ect-msca 172.26.179.237
ip host harry 172.26.176.10
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 crl optional
 auto-enroll 70
!
crypto ca certificate chain ect-msca
 certificate 5D7B2D4300000000003C
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A
!
crypto keyring Backup_Sites
```

```
  pre-shared-key hostname Store77.ese.cisco.com  key 00-02-8A-9B-05-33
!
crypto isakmp policy 1
 encr 3des
 group 2
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
crypto isakmp profile AGGRESSIVE
   description Profile to test Initiating Aggressive Mode
   keyring Backup_Sites
   self-identity fqdn
   match identity host domain ese.cisco.com
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
!
crypto dynamic-map DYNO-TEMPLATE 10
 description dynamic crypto map
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
 reverse-route
 qos pre-classify
!
!
crypto map DYNO-MAP local-address FastEthernet0/1.100
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
!
!
interface FastEthernet0/1
 description dot1q
 no ip address
 ip route-cache flow
 duplex auto
 speed auto
!
interface FastEthernet0/1.100
 description Outside Interface
 encapsulation dot1Q 100
 ip address 192.168.131.4 255.255.255.224
 crypto map DYNO-MAP
!
interface FastEthernet0/1.120
 description Inside Interface
 encapsulation dot1Q 120
 ip address 10.2.120.4 255.255.255.0
!
!                 The bandwidth value of 256 in the metric command is important!
!                 Described previously when illustrating failover.
!
router eigrp 100
 redistribute static metric 256 1000 255 1 1500 route-map IPSEC_Subnets
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 no auto-summary
!
no ip http server
no ip http secure-server
ip classless
```

```
!
!
access-list 68 permit 10.0.64.0 0.0.63.255
access-list 68 deny   any
!
route-map IPSEC_Subnets permit 10
 match ip address 68
!
rtr responder
!
ntp server 192.168.130.1
!
end
```

Primary IPSec Peers

The following is the configuration for primary IPSec peers:

```
!   System image file is "flash:c2600-ik9o3s-mz.122-11.T5"
version 12.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname vpnjk-2600-8
!
logging buffered 4096 debugging
enable password 7 [removed]
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host harry 172.26.176.10
ip host ect-msca 172.26.179.237
!
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 auto-enroll 70
crypto ca certificate chain ect-msca
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A nvram:ect-mscaCA.cer
 certificate 6122A4EC000000000021 nvram:ect-msca.cer
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
!
crypto dynamic-map DYNO-TEMPLATE 10
 description dynamic crypto map
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
 reverse-route
 qos pre-classify
!
!
crypto map DYNO-MAP local-address FastEthernet0/1.100
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
!
interface FastEthernet0/1
 description dot1q
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.100
 description Outside Interface
 encapsulation dot1Q 100
 ip address 192.168.131.8 255.255.255.224
 crypto map DYNO-MAP
!
interface FastEthernet0/1.128
 description Inside Interface
 encapsulation dot1Q 128
 ip address 10.2.128.8 255.255.255.0
!
!                           Bandwidth value for backup IPSec peer is 256
!
router eigrp 100
 redistribute static metric 384 1000 255 1 1500 route-map IPSEC_Subnets
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 no auto-summary
 no eigrp log-neighbor-changes
!
ip default-gateway 172.26.156.1
ip classless
no ip http server
!
!
access-list 68 permit 10.0.68.0 0.0.0.255
access-list 68 deny   any
!
route-map IPSEC_Subnets permit 10
 match ip address 68
!
!
ntp server 192.168.130.1
!
end
===================================================================================

!   System image file is "flash:c2600-ik9o3s-mz.122-11.T5"
version 12.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname vpnjk-2600-9
!
logging buffered 4096 debugging
enable password 7 1511021F0725
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host harry 172.26.176.10
ip host ect-msca 172.26.179.237
!
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 auto-enroll 70
crypto ca certificate chain ect-msca
 certificate 610BE2E400000000001F nvram:ect-msca.cer
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A nvram:ect-mscaCA.cer
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
!
crypto dynamic-map DYNO-TEMPLATE 10
 description dynamic crypto map
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
 reverse-route
 qos pre-classify
!
!
crypto map DYNO-MAP local-address FastEthernet0/1.100
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
!
interface FastEthernet0/1
 description dot1q
 no ip address
 ip route-cache flow
 duplex auto
 speed auto
!
interface FastEthernet0/1.100
 description Outside Interface
 encapsulation dot1Q 100
 ip address 192.168.131.9 255.255.255.224
 crypto map DYNO-MAP
!
interface FastEthernet0/1.128
 description Inside Interface
 encapsulation dot1Q 128
 ip address 10.2.128.9 255.255.255.0
!
!                           Bandwidth value for backup IPSec peer is 256
!
router eigrp 100
 redistribute static metric 384 1000 255 1 1500 route-map IPSEC_Subnets
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
no ip http server
!
!
access-list 68 permit 10.0.68.0 0.0.0.255
!
route-map IPSEC_Subnets permit 10
 match ip address 68
!
ntp server 192.168.130.1
!
end
```

Remote Router

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

```
!           System image file is "flash:vpn/images/c1700-k9o3sy7-mz.123-2.XE"
version 12.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname vpnjk-1751-1
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 [removed]
!
memory-size iomem 25
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!
!
!
ip telnet source-interface FastEthernet0/0
no ip domain lookup
ip domain name ese.cisco.com
ip host harry 172.26.176.10
ip host ect-msca 172.26.179.237
ip cef
ip audit notify log
ip audit po max-events 100
ip dhcp-client default-router distance 239
!
track 123 rtr 23 reachability
 delay down 60 up 5
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir
!
```

```
!              Certificates will be used for authentication for the primary path
!              and IKE Aggressive mode will be used for the backup path
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 revocation-check none
!
!
crypto ca certificate chain ect-msca
 certificate 610C436F00000000002C
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A
!
!
crypto isakmp policy 1
 encr 3des
 group 2
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
!
crypto isakmp peer address 192.168.131.4
 set aggressive-mode password 00-02-8A-9B-05-33
 set aggressive-mode client-endpoint fqdn Store77.ese.cisco.com
crypto isakmp profile AGGRESSIVE
   description Profile to test Initiating Aggressive Mode
   self-identity fqdn
   match identity host domain ese.cisco.com
   initiate mode aggressive
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
no crypto ipsec nat-transparency udp-encaps
!
crypto map PRIMARY_LINK 1 ipsec-isakmp
 description Crypto Map for Primary Path
 set peer 192.168.131.9
 set peer 192.168.131.8
 set transform-set 3DES_SHA_TUNNEL
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
crypto map BACKUP_LINK 1 ipsec-isakmp
 description Crypto Map for Backup Path
 set peer 192.168.131.4
 set transform-set 3DES_SHA_TUNNEL
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
!
!
class-map match-all VOICE
 match ip dscp ef
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match access-group name IKE
```

```
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21
!
!
policy-map V3PN-Small_Branch
description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 128
 class TRANSACTIONAL-DATA
  bandwidth percent 22
 class class-default
  fair-queue
  random-detect
policy-map Shaper-DSL
 class class-default
  shape average 182400 1824
  service-policy V3PN-Small_Branch
policy-map Shaper-cable
 class class-default
  shape average 364800 3648
  service-policy V3PN-Small_Branch
!
!
!
interface Ethernet0/0
 description to DSL MODEM
 bandwidth 256
 no ip address
 service-policy output Shaper-DSL
 load-interval 30
 half-duplex
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface FastEthernet0/0
 description Inside
 ip address 10.0.68.5 255.255.255.128
 no ip proxy-arp
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 speed auto
!
interface Ethernet1/0
 description To CABLE MODEM
 bandwidth 384
 ip dhcp client route track 123
 ip address dhcp
 service-policy output Shaper-cable
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 half-duplex
 crypto map PRIMARY_LINK
!
interface Dialer1
 description Outside
 bandwidth 256
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication pap callin
 ppp chap refuse
 ppp pap sent-username cisco789@cisco.com password 0 foo
 ppp ipcp dns request
 ppp ipcp wins request
 crypto map BACKUP_LINK
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 240 name Backup_Path
ip route 192.168.131.4 255.255.255.255 Dialer1 name Backup_Peer
ip route 192.168.131.23 255.255.255.255 dhcp
ip route 192.168.131.8 255.255.255.254 dhcp
no ip http server
no ip http secure-server
!
!
!
ip access-list extended CRYPTO_MAP_ACL
 permit ip 10.0.68.0 0.0.0.127 any
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
dialer-list 1 protocol ip permit
!
!
control-plane
!
rtr responder
rtr 23
 type udpEcho dest-ipaddr 192.168.131.23 dest-port 57005 source-ipaddr 10.0.68.5
 tos 192
 timeout 1000
 owner TRACK123
 tag Object Tracking
 frequency 20
 lives-of-history-kept 1
 buckets-of-history-kept 10
 filter-for-history failures
rtr schedule 23 start-time now life forever
!
ntp server 192.168.130.1
!
end
```

Show Commands

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

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

These can be displayed on the remote router as follows:

```
vpnjk-1751-1#show rtr history  23  full
```

```
Entry number: 23
Life index: 1
Bucket index: 67
Sample time: 14:08:56.369 est Fri Dec 19 2003
RTT (milliseconds): 0
Response return code: No connection

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

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

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

Cisco IOS Versions Tested

The following code versions were used during testing:

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

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

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

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

Summary

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

CHAPTER 4

Small Branch—DSL with Async Backup

This section describes the use of DSL with Async backup, and includes the following sections:

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

Solution Characteristics

This design incorporates techniques described in the previous two chapters but now further reduces the costs associated with the backup link. With Basic Rate ISDN as the backup link, it is possible to transport encrypted voice traffic across the backup link. However, installing a Basic Rate ISDN line has installation costs and ongoing monthly charges as well as possible per-minute charges when the link is active.

A less costly alternative is to use the plain "old telephone service" (POTS) line that is necessary for provisioning the Asymmetric Digital Subscriber Line (ADSL) service to the branch. Rather than implement an access server at the enterprise head-end location, this design uses the access server of the ISP. This is a further cost reduction to the enterprise. Some ISPs provide access to their dial network at no additional cost as part of a DSL subscription. In some cases, 20 hours per month are provided with DSL service. In other cases, there may be a small fee (less than $10 USD a month) to include dial-up with the DSL plan. Alternatively, dial-up services can be ordered from a different service provider than the ISP providing the DSL service. If single-line DSL (SDSL) service is used (SDSL has no baseband POTS line), a separate POTS line can be installed.

There are two primary disadvantages associated with the cost savings of this design:

- Encrypted voice cannot be transported to the enterprise head-end over the Async interface because the bandwidth is insufficient.
- Local loop cable cut will likely take out both the ADSL and POTS line.

However, the integrated WIC-1AM of the Cisco 1711 includes two RJ11 ports: one for the line and the second for the analog phone handset. The analog line can be used for calls when the dial backup is not active.

Both the primary and backup links use PPP encapsulation and the IP address is dynamically (negotiated) assigned by the ISP. For the broadband path, this is through PPPoE; for the Async path, this is through PPP.

Topology

The topology consists of a Cisco 1711 router at the remote branch location, connected to a DSL bridge on the FastEthernet 0 interface. The POTS line for the ADSL service is separated using a DSL filter/splitter and connected to the Async 1 interface.

The ISP that provides DSL service also includes 20 hours of dial access per month at no additional charge. The same username and password for access to the DSL network is used for the dial backup. At the head-end location, a pair of IPSec routers are shown in the configuration files; one for the primary path and the second for the backup path. As in previous sections, a pair of IPSec head-end routers can be configured for both the primary and backup path and two separate addresses can be assigned.

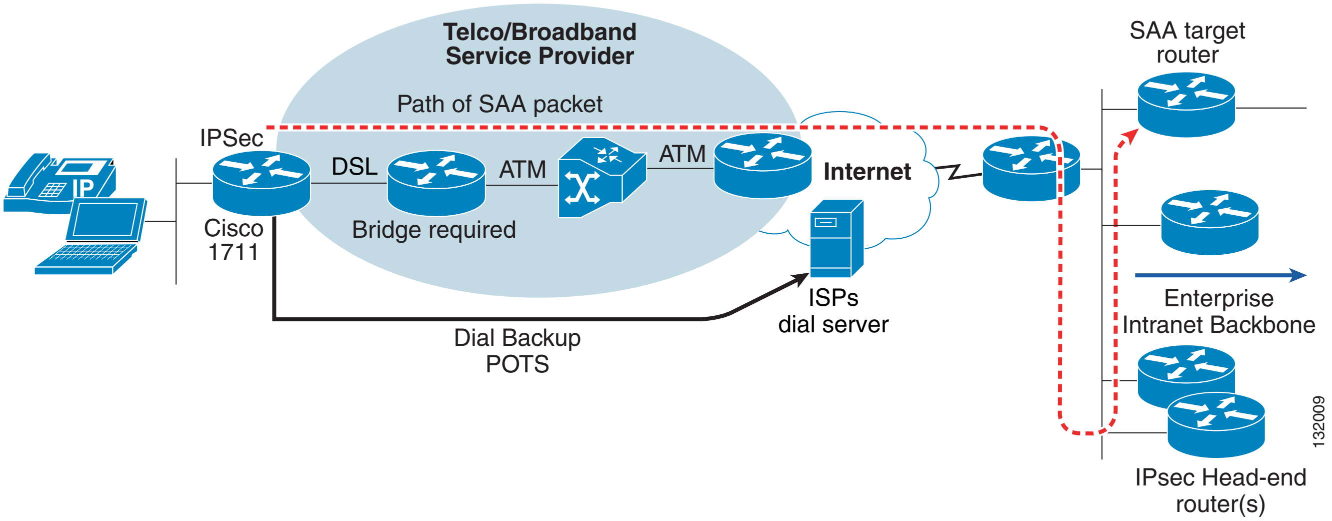
An SAA target router is used at the head-end location.

Note This design uses the Cisco IOS feature, Reliable Static Routing Backup Using Object Tracking, to verify connectivity with SAA probes originating from the inside Ethernet LAN address of the remote router.

The SAA packets traverse the IPSec tunnel. If the tunnel is down and the SAA target is unreachable, dial backup is triggered. Because this design uses SAA to generate ICMP packets, the IP host can be used in place of the SAA target router. It is important that this device remains in service because a failure of the target device causes all branches to attempt a dial backup even though the IPSec tunnel remains available.

Figure 4-1 shows the devices used in this solution.

Figure 4-1 Small Branch DSL with Async Backup



The SAA packets are permitted to reach the head-end only via the DSL interface. This is controlled by a static host route. The backup crypto map advertises a /28 prefix to the head-end IPSec router and the primary IPSec router advertises the /29 prefix that is configured on the inside VLAN 1 interface. This ensures that the return path of the SAA packets uses the IPSec tunnel over the DSL interface if it is active.

Failover/Recovery Time

The following sample configuration uses 60-second track down delay, a polling frequency of 15 seconds for the SAA ICMP probe, and an IKE keepalive value of 10 seconds. To test the dial backup, the DSL cable was removed from the DSL modem. In this display, **debug track** is enabled. With these configuration options, connectivity is restored in approximately two minutes from the initial failure.

```
vpn-jk2-1711-1#show clock
15:17:07.189 est Thu Jan 8 2004            <-  Cable was removed at this time
vpn-jk2-1711-1#
Jan  8 15:17:11.577 est: Track: 21 Down change delayed for 60 secs
Jan  8 15:17:28.293 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
xx.xxx.223.24:500       Id: rtp5-esevpn-gw4.cisco.com
Jan  8 15:17:56.465 est: %DIALER-6-UNBIND: Interface Vi1 unbound from profile Di1
Jan  8 15:17:56.485 est: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to down
Jan  8 15:17:57.465 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to down
Jan  8 15:18:11.577 est: Track: 21 Down change delay expired
Jan  8 15:18:11.577 est: Track: 21 Change #14 rtr 1021, state Up->Down
Jan  8 15:18:57.902 est: %LINK-3-UPDOWN: Interface Async1, changed state to up
Jan  8 15:18:58.906 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed
state to up
Jan  8 15:19:04.710 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
xx.xxx.223.25:500       Id: rtp5-esevpn-gw5.cisco.com
vpn-jk2-1711-1#show clock
15:19:11.954 est Thu Jan 8 2004            <- Connectivity restored via Async interface
```

During transition from the backup Async to primary DSL connection, the recovery is transparent to data applications. Following is an example of a continuous ping running from the PC behind the Cisco 1711 as the DSL cable was inserted back into the DSL modem. The transition from Async to DSL can be identified because the round trip time (RTT) of the ICMP packets decreases substantially from approximately 200ms to 90ms.

```
Reply from 172.26.129.252: bytes=32 time=231ms TTL=247
Reply from 172.26.129.252: bytes=32 time=160ms TTL=247
Reply from 172.26.129.252: bytes=32 time=200ms TTL=247   <- last ping on Async
Reply from 172.26.129.252: bytes=32 time=90ms TTL=247    <- first ping on DSL
Reply from 172.26.129.252: bytes=32 time=100ms TTL=247
Reply from 172.26.129.252: bytes=32 time=111ms TTL=247
Reply from 172.26.129.252: bytes=32 time=90ms TTL=247
Reply from 172.26.129.252: bytes=32 time=90ms TTL=247
Reply from 172.26.129.252: bytes=32 time=90ms TTL=247
Reply from 172.26.129.252: bytes=32 time=90ms TTL=247
Reply from 172.26.129.252: bytes=32 time=90ms TTL=247
Reply from 172.26.129.252: bytes=32 time=90ms TTL=247
```

The LCD display on the IP Phone changes to normal state after recovery because the phone is able to register with the Cisco CallManager over DSL.

V3PN QoS Service Policy

The QoS configuration for the DSL interface is the same as has been previously described in the *Business Ready Teleworker SRND* (http://www.cisco.com/go/srnd).

However, the Async connection does not provide sufficient bandwidth to place a usable encrypted voice call. During testing, encrypted G.711 calls were placed over the Async connection. The latency across the Async connection is typically over 230 ms round trip and packet loss of the voice call was generally 50 percent of the G.711 voice stream. The goal is then to render the Cisco 7960 IP Phone unusable during dial backup. If measures are not taken, the phone registers with its call manager over the Async connection, and the phone display appears normal. However, if a call is successfully dialed, the voice quality is too poor to be usable.

The assumption then is that the primary DSL interface can service one voice call, but no calls can be supported when in dial backup mode.

Because the Context-Based Access Control (CBAC) of the Cisco IOS Firewall is configured on the remote router, applying a static ACL entry to block the Skinny Client Control Protocol (SCCP) packets is ineffective. The IP phone originating a TCP connection to the call manager causes CBAC to insert a temporary ACL entry, permitting the IP phone to register. Additionally, it is preferable to implement a method of blocking voice that does not require configuring specific call manager IP addresses.

To block the IP phone from communicating with the call manager, an input QoS service policy is configured, borrowing the voice and call-setup classes defined for applying uplink QoS on the primary interface. A policer is configured for each class, dropping packets if they either conform or exceed an arbitrary data rate. The data rate configured is immaterial, because packets are dropped if they are above or below the rate. In the following example, the lowest (8000 bps) configurable value was selected.

The service policy is applied on the input Async interface as follows:

```
!
policy-map ASYNC_IN
description Allows us to block voice on the Async
 class VOICE
   police 8000 conform-action drop  exceed-action drop
 class CALL-SETUP
   police 8000 conform-action drop  exceed-action drop

interface Async1
 bandwidth 24
 ip address negotiated
 ip access-group INPUT_ACL in
 service-policy input ASYNC_IN
```

The same input ACL applied to the primary interface is also applied to the backup interface because both interfaces connect to the Internet.

Performance Results

No specific QoS policy was applied to the output Async1 interface except for the default value of weighted fair queueing. Because encrypted voice was not attempted on the backup interface because of bandwidth constraints, no performance tests were run. During the time the dial backup was active, the workstation was able to send and receive text email, view web pages, and so on. Note from the previous section on failover and recovery time, the latency of the Async interface is higher than the broadband connection. The effective bandwidth of the dial backup link is approximately 24 kbps in these tests.

A specific QoS service policy can be applied on the output to the Async interface to guarantee bandwidth to mission-critical or transactional applications. However, weighted fair queueing may be sufficient for these low-volume applications.

Implementation and Configuration

This section describes the key configuration components, and includes the following topics:

- Remote Router SAA and Tracking
- Head-end SAA Target Router
- IPSec Head-end Routers
- Remote Router—Cisco 1711

In the following examples, the addressing conventions are used:

- All subnets of 10.0.0.0 addressing represent *enterprise internal* address space.
- All subnets of 172.16.0.0 addressing represent *enterprise internal* address space.
- All subnets of xx.xxx.223.0 addressing represent *Internet routable* address space.

Remote Router SAA and Tracking

The IP address of the head-end SAA target router is 10.81.0.26. The inside LAN interface address remote Cisco 1711 router is 10.81.7.241. Sourcing the ICMP packets off this interface encrypts the ICMP packets in the IPSec tunnel. The IPSec tunnel must be active before the ICMP connectivity can be restored and data traffic can begin using the IPSec tunnel.

```
!
track 21 rtr 1021
 delay down 60 up 5

ip route 0.0.0.0 0.0.0.0 Dialer1 239 track 21     <- Primary Interface
ip route 0.0.0.0 0.0.0.0 Async1 240               <- Backup Interface

ip route 10.81.0.26 255.255.255.255 Dialer1       <- Force SAA ICMP out Primary Interface

ip route xx.xxx.223.24 255.255.255.255 Dialer1    <- Primary IPSec Peer
ip route xx.xxx.223.25 255.255.255.255 Async1     <- Backup IPSec Peer

rtr 1021
 type echo protocol ipIcmpEcho 10.81.0.26 source-ipaddr 10.81.7.241
 tos 192
 timeout 1000
 owner TRACK 21
 frequency 15
 lives-of-history-kept 1
 buckets-of-history-kept 20
 filter-for-history failures
rtr schedule 1021 start-time now life forever
!
```

Head-end SAA Target Router

Because the SAA configuration uses ICMP in this example, no SAA configuration is required on the head-end target router. In fact, you can use any IP host that reliably responds to ICMP (echo-request) pings.

IPSec Head-end Routers

The configuration of the IPSec head-end router is documented in the Appendix of *Business Ready Teleworker SRND* (http://www.cisco.com/go/srnd)**.** This design was tested by using actual ISPs and production head-end IPSec routers deployed within Cisco.

Remote Router—Cisco 1711

The following is the configuration of the remote router:

```
!
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname vpn-jk2-1711-1
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 [removed]
!
username [removed] privilege 15 secret 5 [removed]
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!
!
ip dhcp pool Client
   import all
   network 10.81.7.240 255.255.255.248
   default-router 10.81.7.241
   dns-server 64.102.6.247 171.68.226.120
   domain-name cisco.com
   option 150 ip 64.102.2.93
   netbios-name-server 171.68.235.228 171.68.235.229
!
!
ip telnet source-interface Vlan1
ip tftp source-interface Vlan1
ip ftp source-interface Vlan1
no ip domain lookup
ip domain name cisco.com
ip host harry 172.26.129.252
ip host rtp5-esevpn-ca 10.81.0.18
ip name-server 64.102.6.247
ip name-server 207.69.188.185
ip cef
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip audit notify log
ip audit po max-events 100
ip ssh source-interface Vlan1
!
track 21 rtr 1021
 delay down 60 up 5
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir
chat-script MODEM "" "atdt\T" TIMEOUT 60 CONNECT \c
!
!
crypto ca trustpoint ese-vpn-cert
 enrollment mode ra
 enrollment url http://10.81.0.18:80/certsrv/mscep/mscep.dll
 revocation-check none
 source interface Vlan1
 auto-enroll 70
!
!
crypto ca certificate chain ese-vpn-cert
 certificate 2ABC84E400000000002A
 certificate ca 36092145BAA631BF4763493E714CD857
!
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set REPLAY esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto map RTP 1 ipsec-isakmp
 description RTP Enterprise Class Teleworker
 set peer xx.xxx.223.24
 set transform-set REPLAY
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
crypto map ASYNC_BACKUP 1 ipsec-isakmp
 description For ASYNC backup interface
 set peer xx.xxx.223.25
 set transform-set REPLAY
 match address CRYPTO_MAP_ACL_BACKUP
 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 ASYNC_IN
description Allows us to block voice on the Async
 class VOICE
   police 8000 conform-action drop  exceed-action drop
 class CALL-SETUP
   police 8000 conform-action drop  exceed-action drop
policy-map V3PN-teleworker
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 class-default
  fair-queue
  random-detect
policy-map Shaper
 class class-default
  shape average 182400 1824
  service-policy V3PN-teleworker
!
!
!
interface FastEthernet0
 description Outside
 no ip address
 service-policy output Shaper
 duplex auto
 speed auto
 pppoe enable
 pppoe-client dial-pool-number 1
 no cdp enable
!
interface FastEthernet1
 no ip address
 vlan-id dot1q 1
  exit-vlan-config
 !
!
interface FastEthernet2
 no ip address
 vlan-id dot1q 1
  exit-vlan-config
 !
!
interface FastEthernet3
 no ip address
 vlan-id dot1q 1
  exit-vlan-config
 !
!
interface FastEthernet4
 no ip address
 vlan-id dot1q 1
  exit-vlan-config
 !
!
interface Vlan1
 description Inside
 ip address 10.81.7.241 255.255.255.248
 ip inspect CBAC in
 ip route-cache flow
 ip tcp adjust-mss 542
 hold-queue 40 out
!
interface Async1
 description EarthLink Dialup Service V34/LAPM/V42B/24000:TX/26400:RX
 bandwidth 24
 ip address negotiated
 ip access-group INPUT_ACL in
 service-policy input ASYNC_IN
 encapsulation ppp
 ip route-cache flow
 load-interval 30
 dialer in-band
 dialer string 6550070
 dialer-group 21
 async mode dedicated
 ppp authentication pap callin
 ppp pap sent-username [removed]@mindspring.com password 7 [removed]
 crypto map ASYNC_BACKUP
!
interface Dialer1
 description Outside
 bandwidth 256
 ip address negotiated
 ip access-group INPUT_ACL in
 ip mtu 1492
 encapsulation ppp
 ip route-cache flow
 dialer pool 1
 no cdp enable
 ppp authentication pap callin
 ppp chap refuse
 ppp pap sent-username [removed]@mindspring.com password 7 [removed]
 ppp ipcp dns request accept
 crypto map RTP
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 239 track 21
ip route 0.0.0.0 0.0.0.0 Async1 240
ip route 10.81.0.26 255.255.255.255 Dialer1
ip route xx.xxx.223.24 255.255.255.255 Dialer1
ip route xx.xxx.223.25 255.255.255.255 Async1
no ip http server
no ip http secure-server
ip flow-export version 5
!
!
!
ip access-list extended CRYPTO_MAP_ACL
 permit ip 10.81.7.240 0.0.0.7 any
ip access-list extended CRYPTO_MAP_ACL_BACKUP
 permit ip 10.81.7.240 0.0.0.15 any
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
ip access-list extended INPUT_ACL
 remark Allow IKE and ESP from the RTP headends
 permit udp xx.xxx.223.16 0.0.0.15 any eq isakmp
 permit udp xx.xxx.223.16 0.0.0.15 eq isakmp any
 permit esp xx.xxx.223.16 0.0.0.15 any
 remark Cisco Corporate Subnets (not complete)
 permit ip 161.44.0.0 0.0.255.255 10.81.7.240 0.0.0.7
 permit ip 171.68.0.0 0.3.255.255 10.81.7.240 0.0.0.7
 permit ip 172.16.0.0 0.15.255.255 10.81.7.240 0.0.0.7
 permit ip 192.168.0.0 0.0.255.255 10.81.7.240 0.0.0.7
 permit ip 128.107.0.0 0.0.255.255 10.81.7.240 0.0.0.7
 permit ip 64.100.0.0 0.3.255.255 10.81.7.240 0.0.0.7
 permit ip 64.104.0.0 0.0.255.255 10.81.7.240 0.0.0.7
 permit ip 10.0.0.0 0.255.255.255 10.81.7.240 0.0.0.7
 permit udp any any eq bootpc
 remark NTP ACLs
 permit udp 192.5.41.40 0.0.0.1 eq ntp any
 permit udp host 216.210.169.40 eq ntp any
 remark SSH from RTP Ridge
 permit tcp xx.xxx.87.0 0.0.0.255 any eq 22
 permit icmp any any
 deny   ip any any
logging source-interface Vlan1
access-list 88 remark cisco123@cisco.com IP Solutions Center rtp7-esevpn-isc
access-list 88 permit 64.102.18.178
access-list 88 remark ------------ RTP Lab Subnet ---------
access-list 88 remark cisco456@cisco.com
access-list 88 permit 172.18.86.64 0.0.0.63
access-list 88 deny   any log
access-list 121 remark Define Interesting Traffic
access-list 121 permit ip any any
dialer-list 21 protocol ip list 121
snmp-server community [removed] RW 88
snmp-server trap-source Vlan1
snmp-server location  Home Office
snmp-server contact cisco789@cisco.com
snmp-server enable traps tty
!
!
control-plane
!
rtr responder
rtr 12
 type echo protocol ipIcmpEcho 172.26.129.252 source-ipaddr 10.81.7.241
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 start-time now life forever
rtr 1021
 type echo protocol ipIcmpEcho 10.81.0.26 source-ipaddr 10.81.7.241
 tos 192
 timeout 1000
 owner TRACK 21
 frequency 15
 lives-of-history-kept 1
 buckets-of-history-kept 20
 filter-for-history failures
rtr schedule 1021 start-time now life forever
banner motd ^C
   C i s c o S y s t e m s
     ||               ||
     ||               ||       Cisco Systems, Inc.
    ||||             ||||      IT-Transport
 .:|||||||:.......:|||||||:..
  US, Asia & Americas support:    + 1 408 526 8888
 EMEA support:                   + 31 020 342 3888
  UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in disciplinary action.
^C
!
```

```
line con 0
 exec-timeout 60 0
 login local
 stopbits 1
line 1
 script dialer MODEM
 modem InOut
 modem autoconfigure discovery
 transport input all
 transport output pad udptn telnet rlogin ssh
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
 stopbits 1
line vty 0 4
 login local
 transport input ssh
!
exception memory minimum 786432
ntp clock-period 17179960
ntp server 192.5.41.41
ntp server 192.5.41.40
ntp server 216.210.169.40
ntp server 10.81.254.202 source Vlan1
!
end
```

Debugging

The Async line must reference a chat script. Chat scripts are text sent to the modem to provide initialization, configuration, and dialing commands. The **chat-script MODEM** is called by the **script dialer MODEM** command configured under line 1.

```
chat-script MODEM "" "atdt\T" TIMEOUT 60 CONNECT \c

…
interface Async1
…
dialer string 6550070

…
line 1
 script dialer MODEM
 modem InOut
 modem autoconfigure discovery
 transport input all
 transport output pad udptn telnet rlogin ssh
 stopbits 1
 speed 115200
 flowcontrol hardware
```

Note that the phone number to dial is 6550070, which is specified under the Async 1 interface configuration. When **debug chat** is enabled, you can see this string substituted for the **\T** command in the chat script. The following shows a successful dial attempt with debugging enabled:

```
Jan  8 16:52:35.289 est: CHAT1: Attempting async line dialer script
Jan  8 16:52:35.289 est: CHAT1: Dialing using Modem script: MODEM & System scrip
```

```
t: none
Jan  8 16:52:35.289 est: CHAT1: process started
Jan  8 16:52:35.293 est: CHAT1: Asserting DTR
Jan  8 16:52:35.293 est: CHAT1: Chat script MODEM started
Jan  8 16:52:35.293 est: CHAT1: Sending string: atdt\T<6550070>
Jan  8 16:52:35.293 est: CHAT1: Expecting string: CONNECT
Jan  8 16:52:55.597 est: CHAT1: Completed match for expect: CONNECT
Jan  8 16:52:55.601 est: CHAT1: Sending string: \c
Jan  8 16:52:55.601 est: CHAT1: Chat script MODEM finished, status = Success
```

It is also useful to use a reverse Telnet to the Async line to manually send the Hayes AT commands to the modem to initiate dialing and login during implementation to verify connectivity to the dial-up service of the ISP. The following example uses the internal WIC-1AM modem on the Cisco 1711:

```
vpn-jk2-1711-1#telnet 10.81.7.241 2001
Trying 10.81.7.241, 2001 ... Open

   C i s c o S y s t e m s
     ||                ||
     ||                ||      Cisco Systems, Inc.
    ||||             ||||      IT-Transport
 .:|||||||:.......:|||||||:..
  US, Asia & Americas support:    + 1 408 526 8888
 EMEA support:                   + 31 020 342 3888
  UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in disciplinary action.

ath OK
atdt6550070 CONNECT 115200/V34/LAPM/V42B/24000:TX/26400:RX
EarthLink Dialup Service
```

After you receive the login prompt, you can interactively enter the username and password or interrupt the modem with the **+++** command and issue the **ATH** command to hang up the call. A **control + shift + 6 x** command reverts back to exec mode where the line can be cleared.

```
acn01.nc-greensbo1 login: +++
OK
ath OK

CTL SHIFT 6 x

vpn-jk2-1711-1#clear line 1
[confirm]y [OK]
vpn-jk2-1711-1#
Resuming connection 1 to 10.81.7.241 ... ]

[Connection to 10.81.7.241 closed by foreign host]Deleting login session
```

Note For more information on chat scripts, see *Creating and Using Modem Chat Scripts* at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca6f5.html

Cisco IOS Versions Tested

The following code versions were used during testing:

- IPSec head-ends—c3725-ik9o3s-mz.122-15.T9
- Cisco 1711—c1700-k9o3sy7-mz.123-2.XE
- SAA target—c2600-adventerprisek9-mz.123-4.T

The IPSec head-end routers were Cisco 3725s with an AIM hardware VPN module. This testing was not intended to scale test head-end performance capabilities. In a customer deployment, IPSec head-ends with suitable performance characteristics aligned with the number of remote routers is advised.

The testing was completed using the DSL connection and dial-up account of the author. There is a Cisco 1760 V3PN bundle (product number: CISCO1760-V3PN/K9) that can be used instead of the Cisco 1711.

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

Note During testing, voice quality issues led to filing DDTs: CSCed61266— QoS Service Policy not matching pkts on PPPoE interface.

Summary

The Object Tracking feature of Cisco IOS provides a means to deploy both DSL and Async modems to the same remote location for increased availability. Because this feature uses SAA, a network manager can use its protocols and applications in addition to ICMP for verifying connectivity. One advantage to this configuration is its scalability; a primary and backup IPSec head-end can be configured independently to the SAA head-end router, and additional SAA head-ends can be added as required. If ICMP is used as the SAA probe protocol, any IP host can be used at the head-end.

The use of a dial-up account associated with the ISP DSL account of the site is a very cost effective means of providing higher availability for low bandwidth transactions such as ATM machines and point-of-sale terminals while using a central call processing model for an IP phone over the primary broadband connection.

CHAPTER 5

Small Branch—Dial Backup to Cisco VPN 3000 Concentrator

This design was proposed to meet the requirements for a national catalog retail business that has approximately 60 retail stores in addition to the direct mail and Internet web business model. The retailer has an existing Cisco VPN 3000 Concentrator that supports remote access software clients, and wants to use that device as an IPSec head end to serve as a crypto peer for dial backup if the primary path over the Internet fails. The application supported is primarily point-of-sale transactions.

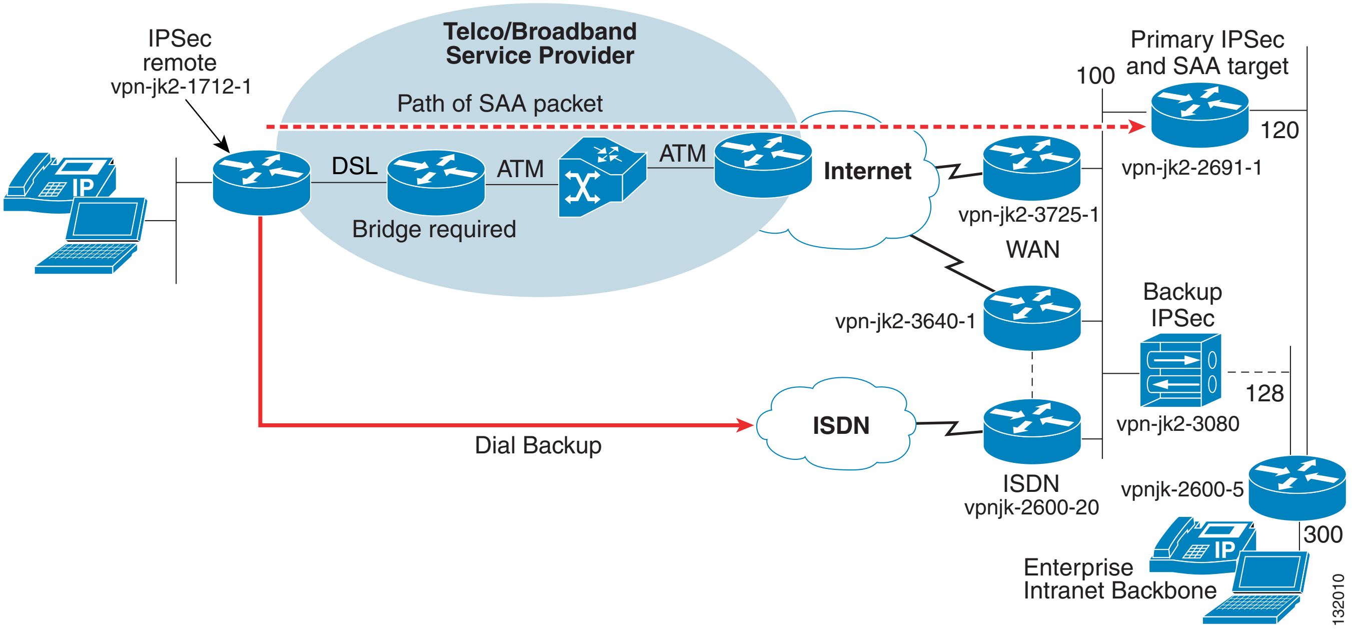
This chapter contains the following sections:

- Topology
- Failover/Recovery Time
- Caveats
- V3PN QoS Service Policy
- Performance Results
- Implementation and Configuration
- Cisco IOS Versions Tested
- Summary

Topology

The topology in Figure 5-1 shows the use of a Cisco 1712 router that includes a Basic Rate ISDN interface; however, the design can be adapted to use a Cisco 1711 and to dial either the access server of an Internet Service Provider or an access server provisioned by the enterprise.

Figure 5-1 Topology Dial Backup to Cisco VPN 3000



The design shows the use of one Cisco IOS head-end IPSec peer that is also the SAA target device for the Reliable Static Routing Backup Using Object Tracking feature in Cisco IOS Software.

The enterprise intranet backbone router is configured to route packets to the remote subnets using the IPSec primary router if the Reverse Route Injection (RRI) network advertisements appear in its routing table; otherwise, the packets are routed to the Cisco VPN 3000 Concentrator.

The VPN 3000 Concentrator is configured with a default route to the ISDN WAN router; however, for higher availability, a customer deployment might use a Hot Standby Router Protocol (HSRP) address shared between a pair of WAN routers, or enable OSPF or RIP on the outside interface and participate in a dynamic routing protocol with the various WAN routers.

Failover/Recovery Time

Failover and recovery times are similar to the results described in two earlier chapters: Small Branch—DSL with ISDN Backup and Small Branch—Cable with DSL Backup.

There is a difference in configuration between the ISDN backup in the previous section and this configuration. As previously described, the Basic Rate ISDN interface is a backup interface for a tunnel interface, and the interface up/down state is keyed off the tunnel interface state. In this configuration, a **dialer idle-timeout** is configured as well as **dialer-list** that excludes IKE packets as interesting traffic.

```
access-list 100 remark DIALER LIST, IKE traffic should not be interesting
access-list 100 deny   icmp any any
access-list 100 deny   udp any eq isakmp any eq isakmp
access-list 100 permit ip any any
dialer-list 2 protocol ip list 100
```

Note For more information regarding dialer interfaces, see the *Cisco IOS Dial Technologies Configuration Guide* at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080393bf3.html.

Caveats

This section describes the caveats associated with this design, and includes the following topics:

- EZVPN—Tunnel Goes to SS_OPEN State on Re-establishing Connection
- RRI Fails to Insert the Appropriate Static Route

EZVPN—Tunnel Goes to SS_OPEN State on Re-establishing Connection

It appears in some instances that the Cisco 1712 is exposed to the following condition: CSCin53097 CSCin53097 (EZVPN—tunnel goes to SS_OPEN state on re-establishing connection). The following is a successful and unsuccessful initiation of the EZVPN tunnel to the VPN Concentrator. To force the primary path down, an ISP link failure was simulated.

This is a successful dial backup and tunnel establishment.

```
vpn-jk2-1712-1#debug track
Jan 21 16:07:47.717 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.4:500       Id: vpn-jk-2691-1.ese.ciscom
Jan 21 16:07:51.289 est: Track: 123 Down change delayed for 60 secs
vpn-jk2-1712-1#
Jan 21 16:08:51.301 est: Track: 123 Down change delay expired
Jan 21 16:08:51.301 est: Track: 123 Change #50 rtr 233, reachability Up->Down
vpn-jk2-1712-1#
Jan 21 16:08:59.489 est: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
Jan 21 16:08:59.625 est: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Jan 21 16:09:00.545 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed
state to up
Jan 21 16:09:00.641 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
Jan 21 16:09:02.229 est: %LINK-3-UPDOWN: Interface BRI0:2, changed state to up
Jan 21 16:09:02.229 est: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 9191234567
vpnjk-2600-20
Jan 21 16:09:03.289 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed
state to up
Jan 21 16:09:03.297 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
192.168.131.30:500       Id: 192.168.131.30
Jan 21 16:09:08.229 est: %ISDN-6-CONNECT: Interface BRI0:2 is now connected to 9191234567
vpnjk-2600-20
vpn-jk2-1712-1#
vpn-jk2-1712-1#show cry ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : VPN3080
Inside interface list: Vlan1,
Outside interface: BRI0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Primary: 172.26.176.10
```

```
This is an example of the state stuck in SS_OPEN. Manually clearing the EZVPN client will
circumvent the problem.


vpn-jk2-1712-1#
Jan 21 16:14:25.043 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.4:500       Id: vpn-jk-2691-1.ese.ciscom
Jan 21 16:14:31.424 est: Track: 123 Down change delayed for 60 secs
Jan 21 16:15:31.424 est: Track: 123 Down change delay expired
Jan 21 16:15:31.424 est: Track: 123 Change #52 rtr 233, reachability Up->Down
Jan 21 16:15:32.936 est: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
Jan 21 16:15:33.072 est: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Jan 21 16:15:33.152 est: %CRYPTO-4-IKMP_NO_SA: IKE message from 192.168.131.30  has no SA
and is not an initialization offer
Jan 21 16:15:33.992 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed
state to up
Jan 21 16:15:34.088 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
Jan 21 16:15:36.244 est: %LINK-3-UPDOWN: Interface BRI0:2, changed state to up
Jan 21 16:15:36.248 est: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 9191234567
vpnjk-2600-20
Jan 21 16:15:37.300 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed
state to up
vpn-jk2-1712-1#
Jan 21 16:15:42.248 est: %ISDN-6-CONNECT: Interface BRI0:2 is now connected to 9191234567
vpnjk-2600-20A pre-shared key for address!

vpn-jk2-1712-1#
Jan 21 16:15:45.044 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.30:500       Id: 192.168.131.30
vpn-jk2-1712-1#
vpn-jk2-1712-1#show cry ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : VPN3080
Inside interface list: Vlan1,
Outside interface: BRI0
Current State: SS_OPEN
Last Event: SOCKET_READY
DNS Primary: 172.26.176.10
vpn-jk2-1712-1#
Jan 21 16:16:33.160 est: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to down
Jan 21 16:16:33.256 est: %ISDN-6-DISCONNECT: Interface BRI0:1  disconnected from
9191234567 vpnjk-2600-20, call lasted 60 seconds
Jan 21 16:16:33.256 est: %LINK-3-UPDOWN: Interface BRI0:1, changed state to down
Jan 21 16:16:33.332 est: %ISDN-6-DISCONNECT: Interface BRI0:2  disconnected from
9191234567 vpnjk-2600-20, call lasted 57 seconds
Jan 21 16:16:33.332 est: %LINK-3-UPDOWN: Interface BRI0:2, changed state to down
Jan 21 16:16:34.100 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed
state to down
Jan 21 16:16:34.100 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed
state to down
Jan 21 16:16:34.160 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to down
vpn-jk2-1712-1#
Jan 21 16:16:37.932 est: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
Jan 21 16:16:38.064 est: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Jan 21 16:16:38.988 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed
state to up
Jan 21 16:16:39.080 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
Jan 21 16:16:40.244 est: %LINK-3-UPDOWN: Interface BRI0:2, changed state to up
Jan 21 16:16:40.248 est: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 9191234567 
vpnjk-2600-20
Jan 21 16:16:41.304 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed 
state to up
vpn-jk2-1712-1#clear crypto ipsec  client ezvpn VPN3080
vpn-jk2-1712-1#
Jan 21 16:16:46.249 est: %ISDN-6-CONNECT: Interface BRI0:2 is now connected to 9191234567 
vpnjk-2600-20
Jan 21 16:16:49.029 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer 
192.168.131.30:500       Id: 192.168.131.30
vpn-jk2-1712-1#show cry ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : VPN3080
Inside interface list: Vlan1,
Outside interface: BRI0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Primary: 172.26.176.10
vpn-jk2-1712-1#
```

```
vpn-jk2-1712-1#show cry eng conn act

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
  22 Dialer1         192.168.17.3    alloc  NONE                      0        0
  23 BRI0            10.0.128.1      set    HMAC_MD5+3DES_56_C        0        0
  24 Dialer1         192.168.17.3    alloc  NONE                      0        0
 200 BRI0            10.0.128.1      set    HMAC_MD5+3DES_56_C        0        9
 201 BRI0            10.0.128.1      set    HMAC_MD5+3DES_56_C       16        0
```

RRI Fails to Insert the Appropriate Static Route

CSDed69116 refers to the following occurrence: RRI fails to insert the appropriate static route into the routing table.In the test topology, without a default route in the routing table of the vpnjk2-2691-1 route (the primary IPSec head-end route), RRI fails to insert the appropriate static route into the routing table. CSCed69116 was filed to address this issue. This was using Cisco IOS version 12.3(5). This defect is documented in CSCed69116.

V3PN QoS Service Policy

The V3PN QoS service policy in this configuration is similar to the other chapters in this guide.

Performance Results

Performance results for the Cisco IOS and VPN concentrator head-ends are shown in Table 5-1.

Table 5-1 IPSEC/DPD/RRI Performance

	Spokes	Bi-Directional Traffic (Mbps)	Bi-Directional Traffic (Kpps)	CPU Utilization %	Stopping Point
Cisco 3745 (AIM-II)	120	22.5	14.5	80	CPU
Cisco PIX 535 (VAC+)	500	167	84	89	CPU
Cisco 3080 (SEP/SEP-E)	138	38.8/39.4	19.6/19.6	80/52	CPU
Cisco 7200 NPE-400 (VAM1)	1040	71.7	31.7	88	CPU
Cisco 7200 NPE-G1 (2xVAM1)	1040	106.7	48.1	81	CPU
Cisco 7200 NPE-G1 (2xVAM2)	1040	108.7	48.7	77	CPU
Cisco Catalyst 6500 (VPNSM)	1040	1029.3	488.7	N/A	VPNSM

These test results are from an IPSec/DPD/RRI test bed configuration using a voice and data traffic mix from the ESE branch traffic profile.For more details refer to the following internal website: http://wwwin-eng.cisco.com/Eng/ESE/VPN/Design/V3PNDesignGuide.doc).

In a deployment where the VPN 3080 is acting as a backup head end to provide connectivity for point-of-sale terminals or cash machines over an Async interface with no voice traffic, these are very conservative performance numbers.

If the 3080 also supports VPN access by remote users with a VPN software client in addition to functioning as a backup IPSec head end for remote locations, the performance characteristics vary.

Note The Cisco PIX OS earlier than Version 7 does not switch a packet in and out the same interface in the tested release of the code.

Implementation and Configuration

This section describes the implementation and configuration of the Dial Backup to Cisco VPN 3000 Concentrator solution. It includes the following topics:

- Enterprise Intranet Backbone Router(s)
- IPSec Primary and SAA Target Router
- Primary WAN Router
- Remote IPSec (1712) Router
- Cisco VPN 3000 Concentrator Configuration

Enterprise Intranet Backbone Router(s)

The enterprise intranet backbone router is designated as vpnjk-2600-5 in Figure 5-1. A large enterprise customer may have one or more routers that connect their extranet to the intranet. The function of this router is to route packets for the remote subnets to the appropriate IPSec head-end device, either the Cisco IOS head-end or the VPN concentrator. If an active IPSec tunnel is available on the Cisco IOS head end, this is the primary or preferred path. If no IPSec tunnel is available for the remote subnet, route the packets to the VPN concentrator.

This router is an EIGRP neighbor with the Cisco IOS IPSec head-end router, and it learns external routes of the specific remote subnets using EIGRP. In this example, the network prefix is /25. There is a static route to a /18 prefix that represents the address space of all the remote subnets. If the more specific /25 route does not exist, the /18 route is followed, connecting to the VPN 3000 Concentrator.

```
!
hostname vpnjk-2600-5
!
interface FastEthernet0/1
 description dot1q
 no ip address
 ip route-cache flow
!
interface FastEthernet0/1.120
 encapsulation dot1Q 120  This VLAN connects to the IOS IPSec Head-end - 2691
 ip address 10.2.120.5 255.255.255.0
!
interface FastEthernet0/1.128
 encapsulation dot1Q 128  This VLAN connects to the VPN Concentrator - 3080
 ip address 10.2.128.5 255.255.255.0
!
interface FastEthernet0/1.300
 encapsulation dot1Q 300  This VLAN connects to the Enterprise Intranet Backbone
 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
!
ip route 10.0.64.0 255.255.192.0 10.2.128.30 name VPN3080
!
end

vpnjk-2600-5#sh ip route 10.0.68.0
Routing entry for 10.0.64.0/18                 Primary path down.
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 10.2.128.30
      Route metric is 0, traffic share count is 1

vpnjk-2600-5#sh ip route 10.0.68.0
Routing entry for 10.0.68.0/25                Primary path available
  Known via "eigrp 100", distance 170, metric 10258432, type external
  Redistributing via eigrp 100
  Last update from 10.2.120.4 on FastEthernet0/1.120, 00:00:35 ago
  Routing Descriptor Blocks:
  * 10.2.120.4, from 10.2.120.4, 00:00:35 ago, via FastEthernet0/1.120
      Route metric is 10258432, traffic share count is 1
      Total delay is 10100 microseconds, minimum bandwidth is 256 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

```
Note: There is a /25 route for each remote subnet active over the primary path. The /18
prefix will always be in the routing table.

vpnjk-2600-5#show ip route
…
S       10.0.64.0/18 [1/0] via 10.2.128.30
D EX    10.0.68.0/25
           [170/10258432] via 10.2.120.4, 00:09:36, FastEthernet0/1.120
```

IPSec Primary and SAA Target Router

In other chapters of this guide, the head-end SAA target router and the IPSec head-end routers are separate routers. In this example, both functions are implemented on one router. When there is only one IPSec head-end router, it is practical to use its IP address as the SAA target. If the IPSec tunnel is down, the SAA address is down. When the design has multiple primary peers, it may be advantageous to use a separate SAA target router. A disadvantage to this design is that if the SAA target router is down and the IPSec peers are functional, the backup mechanism is activated when it is not really needed.

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname vpn-jk-2691-1
!
boot system flash c2691-ik9o3s-mz.122-13.T10
logging buffered 4096 debugging
enable secret 5 [removed]
!
memory-size iomem 15
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
no ip cef                              # CEF was disabled, see caveats
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host harry 172.26.176.10
ip host ect-msca 172.26.179.237
!
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 crl optional
 auto-enroll 70
crypto ca certificate chain ect-msca
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A
 certificate 5D7B2D4300000000003C
!
!
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
!
interface FastEthernet0/1.100
 description Outside Interface
 encapsulation dot1Q 100
 ip address 192.168.131.4 255.255.255.224       # crypto peer and SAA target address
 crypto map DYNO-MAP
!
interface FastEthernet0/1.120
 description Inside Interface                   # EIGRP neighbor on this interface to
 encapsulation dot1Q 120                        # vpnjk-2600-5 Enterprise Intranet
 ip address 10.2.120.4 255.255.255.0            # Backbone Router
!
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
!
ip classless
ip http server
!
!
access-list 68 permit 10.0.64.0 0.0.63.255      # Allow redistribution of
access-list 68 deny   any                       # subnets of 10.0.64.0 /18
!
route-map IPSEC_Subnets permit 10
 match ip address 68
!
rtr responder                                   # To respond to SAA requests
!
end
```

Primary WAN Router

This section shows the configuration of the primary enterprise WAN router. There is a issue in the RRI code that presents a problem if there is no default route in the routing table of the IPSec head-end router. To circumvent this issue[1], this WAN router is configured to advertise a 0/0 route into EIGRP 100 so that the IPSec head-end router learns a default route. In the event this router is down or out-of-service, the secondary WAN router should be similarly configured.

[1] CSCed69116 was filed against this issue.

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname vpn-jk2-3725-1
!
boot-start-marker
boot system flash c3725-ik9o3s-mz.123-3
boot-end-marker
!
memory-size iomem 15
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!
ip cef
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
interface Loopback0
 ip address 192.168.130.1 255.255.255.255
!
!
interface FastEthernet0/1
 description dot1q
 no ip address
!
interface FastEthernet0/1.100
 description vlan 100
 encapsulation dot1Q 100
 ip address 192.168.131.1 255.255.255.224
 no ip proxy-arp
!
interface FastEthernet0/1.102
 description vlan 102
 encapsulation dot1Q 102
 ip address 192.168.131.33 255.255.255.224
 no ip proxy-arp
!
!
interface ATM2/0
description WAN Link to the Internet (AS 65001)
 no ip address
 no atm ilmi-keepalive
!
interface ATM2/0.235 point-to-point
 ip address 192.168.129.6 255.255.255.252
 pvc peer235 2/35
  vbr-nrt 1000 1000
  encapsulation aal5snap
 !
!
router eigrp 100
 redistribute static metric 100 1000 255 1 1500 route-map QuadZero
 redistribute bgp 65030 metric 100 1000 255 1 1500
 network 192.168.130.0 0.0.1.255
 no auto-summary
```

```
!
router bgp 65030
 no synchronization
 bgp log-neighbor-changes
 network 192.168.130.0 mask 255.255.254.0
 network 192.168.230.0 mask 255.255.254.0
 neighbor 192.168.129.5 remote-as 65001
 neighbor 192.168.130.2 remote-as 65030
 neighbor 192.168.130.2 update-source Loopback0
 no auto-summary
!
no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Null0 240            # Redistributed into EIGRP 100 for IPSec HE
ip route 192.168.130.0 255.255.254.0 Null0    # Provides ‘nailed up’ networks for BGP
ip route 192.168.230.0 255.255.254.0 Null0    # Provides ‘nailed up’ networks for BGP
!
!
access-list 10 permit 0.0.0.0
!
route-map QuadZero permit 10                  # Redistribute the 0/0 route to EIGRP
 match ip address 10
!
ntp source Loopback0
ntp master
ntp server 172.26.176.10 source FastEthernet0/0
!
end
```

Remote IPSec (1712) Router

This is the configuration of the remote Cisco 1712 router.

```
!             System image file is "flash:c1700-k9o3sy7-mz.123-2.XE"
version 12.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone

service password-encryption
!
hostname vpn-jk2-1712-1
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 [removed]
!
username vpnjk-2600-20 password 7 [removed]
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
ip domain name ese.cisco.com
ip host harry 172.26.176.10
ip host ect-msca 172.26.179.237
ip name-server 172.26.176.10
ip cef
ip audit notify log
ip audit po max-events 100
!
track 123 rtr 233 reachability
 delay down 60 up 5
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir
isdn switch-type basic-5ess
!
!
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 5DA1A8EE00000000003D
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A
!
!
crypto isakmp policy 20
 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 ipsec client ezvpn VPN3080
 connect auto
 group SOHO key point_of_sale
 mode network-extension
 peer 192.168.131.30
 username site100 password  cisco123
!
!
crypto map IOS_2691 10 ipsec-isakmp
 description used for testing ezvpn for dial backup
 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
!
!
policy-map V3PN-WAN-EDGE-ISDN
description Note LLQ for PPP/ISDN G.729=56K
```

```
 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, G.711=128K
 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 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
 tx-ring-limit 1
 tx-queue-limit 1
 dialer idle-timeout 60
 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 9194442222
 dialer hold-queue 5
 dialer-group 2
 isdn switch-type basic-5ess
 ppp authentication chap
 ppp multilink
 ppp multilink fragment delay 10
 ppp multilink links minimum 2
 crypto ipsec client ezvpn VPN3080
!
interface FastEthernet0
 description Outside to DSL Modem
 bandwidth 256
 no ip address
 service-policy output Shaper
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface FastEthernet1
 no ip address
 vlan-id dot1q 1
  exit-vlan-config
 !
!
!
interface Vlan1
```

```
 description Inside
 ip address 10.0.68.1 255.255.255.128
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 crypto ipsec client ezvpn VPN3080 inside
!
!
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 7 [removed]
 ppp ipcp dns request
 ppp ipcp wins request
 crypto map IOS_2691
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 239 name primary_path track 123
ip route 0.0.0.0 0.0.0.0 10.0.128.2 240 name BRI_peer_20
ip route 10.0.128.2 255.255.255.255 BRI0
!
ip route 192.168.131.4 255.255.255.255 Dialer1 name To2691_head-end
ip route 192.168.131.30 255.255.255.255 10.0.128.2 name To3080_head-end
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
!
access-list 100 remark DIALER LIST, IKE traffic should not be interesting
access-list 100 deny   icmp any any
access-list 100 deny   udp any eq isakmp any eq isakmp
access-list 100 permit ip any any
dialer-list 2 protocol ip list 100
!
rtr responder
!                     RTR 12 simply generates traffic to simulate background 'noise'
rtr 12
 type echo protocol ipIcmpEcho 10.2.128.5 source-ipaddr 10.0.68.1
 frequency 10
rtr schedule 12 start-time now life forever
!                     RTR 233 is associated with the object tracking
rtr 233
type udpEcho dest-ipaddr 192.168.131.4 dest-port 57005 source-ipaddr 10.0.68.1 source-port
48879
 tos 192
 owner TRACK123
 tag Object Tracking
 frequency 20
 lives-of-history-kept 1
 buckets-of-history-kept 10
 filter-for-history failures
rtr schedule 233 start-time now life forever
!
```

```
!                    Aliases to aid in troubleshooting
alias exec xa crypto ipsec client ezvpn xauth
alias exec ca sh cry eng conn act
alias exec cc crypto ipsec client ezvpn connect VPN3080
alias exec cz clear crypto ipsec  client ezvpn VPN3080
alias exec sz show cry ipsec client ezvpn
!
ntp server 192.168.130.1
!
end
```

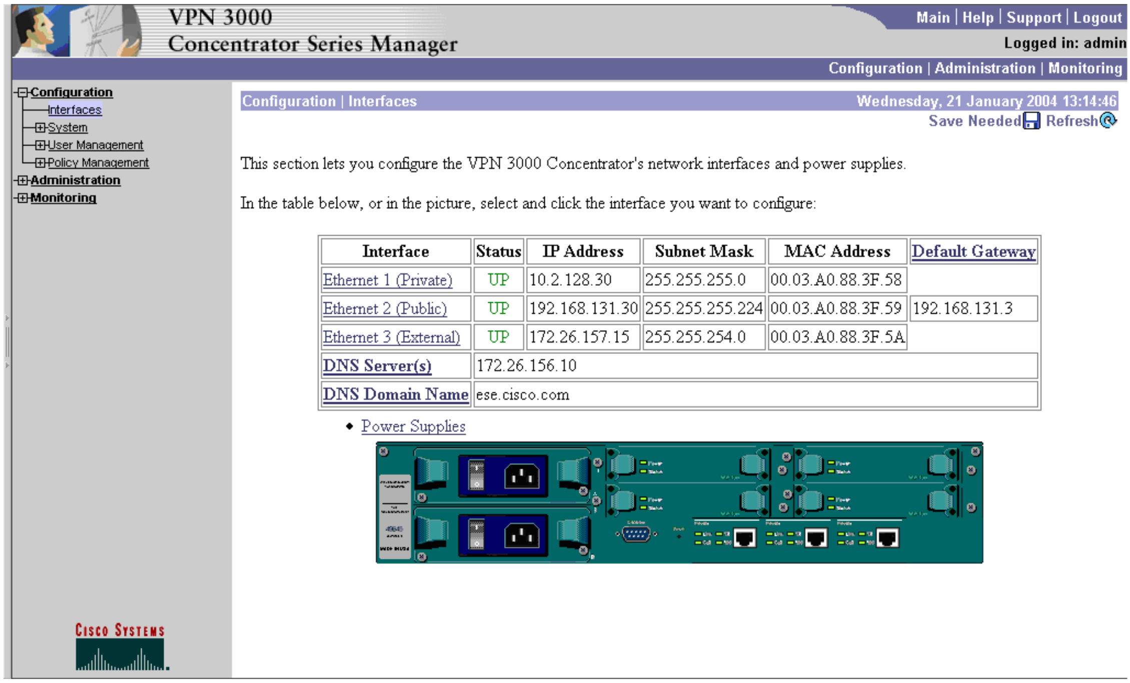
Cisco VPN 3000 Concentrator Configuration

The Cisco VPN 3000 Concentrator is configured with a default route (gateway) of 192.168.131.3, which is the head-end ISDN WAN router. The inside or private address is on the same subnet as the enterprise intranet router. The external address is a lab flashnet address for management.

Interfaces

Figure 5-2 shows the VPN 3000 configuration interface.

Figure 5-2 VPN 3000 Configuration Interface


VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Administration
Monitoring
Configuration | Interfaces
Wednesday, 21 January 2004 13:14:46
Save Needed
Refresh
Power Supplies
Cisco Systems
132011

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	10.2.128.30	255.255.255.0	00.03.A0.88.3F.58	
Ethernet 2 (Public)	UP	192.168.131.30	255.255.255.224	00.03.A0.88.3F.59	192.168.131.3
Ethernet 3 (External)	UP	172.26.157.15	255.255.254.0	00.03.A0.88.3F.5A	
DNS Server(s)	172.26.156.10				
DNS Domain Name	ese.cisco.com				

Groups

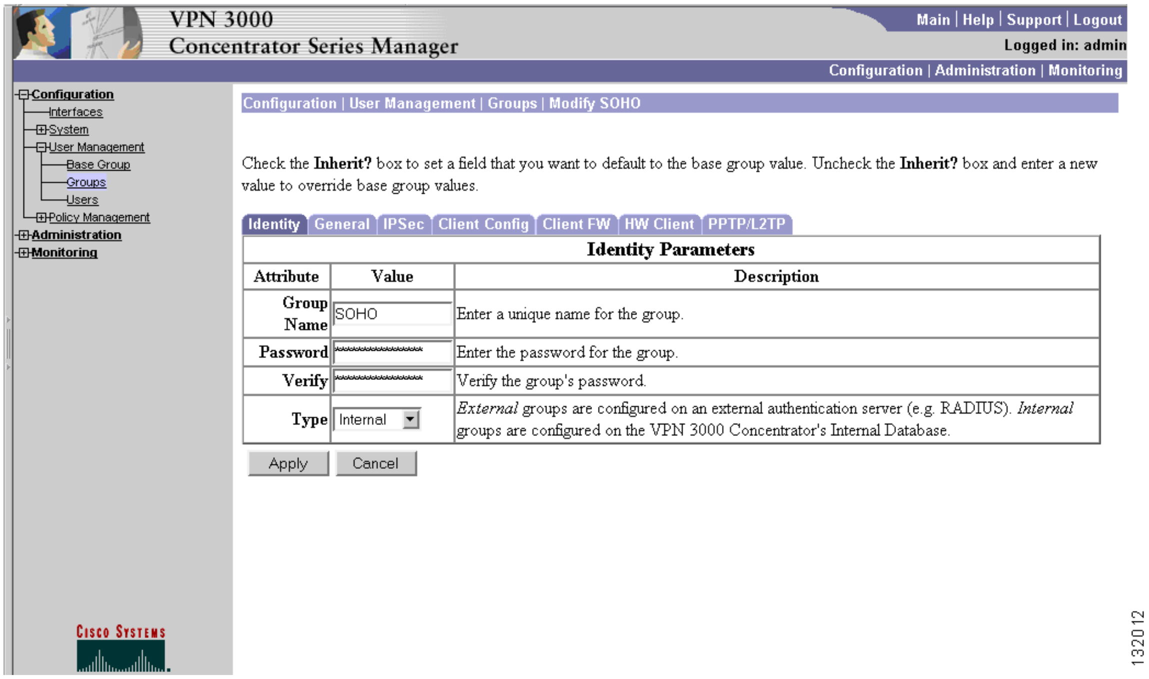
This section describes the configuration of the groups.

Identity

The group configuration of the remote router is defined on the window shown in Figure 5-3.

```
crypto ipsec client ezvpn VPN3080
 connect auto
 group SOHO key point_of_sale
 mode network-extension
 peer 192.168.131.30
 username site100 password  cisco123
```

Figure 5-3   VPN 3000 Group Identity


VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Administration
Monitoring
Configuration | User Management | Groups | Modify SOHO
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP
Apply
Cancel
Cisco Systems
132012

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters

Attribute	Value	Description
Group Name	SOHO	Enter a unique name for the group.
Password	****************	Enter the password for the group.
Verify	****************	Verify the group's password.
Type	Internal	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

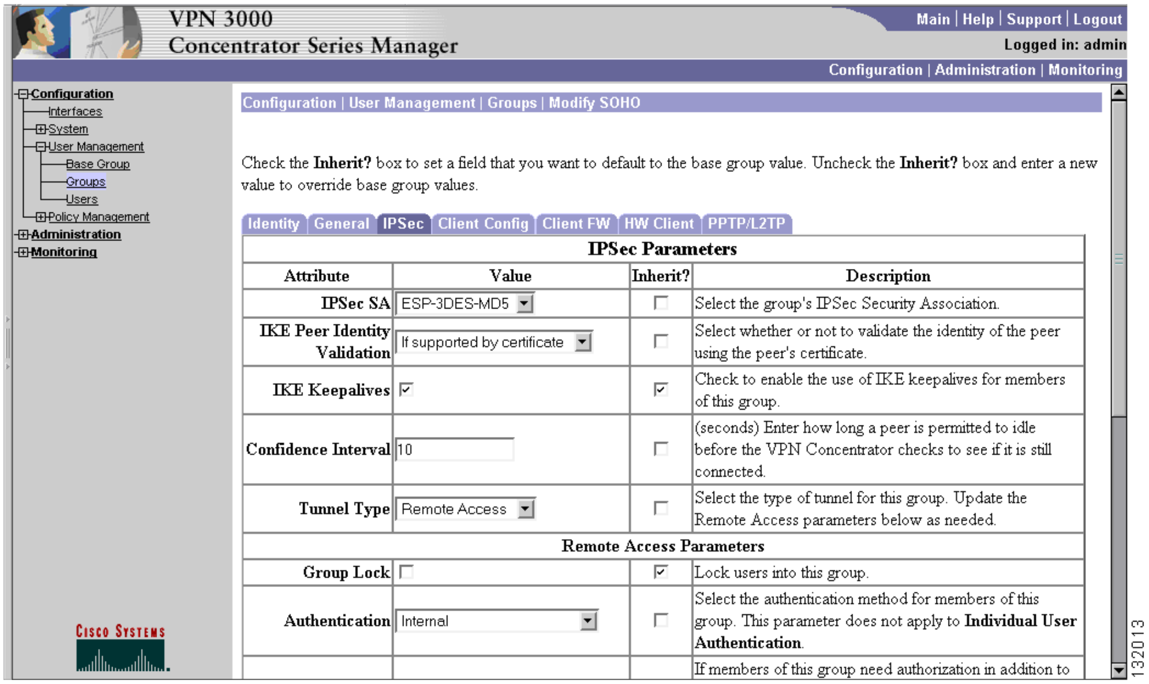
IPSec

IKE keepalives are enabled for this group, and the confidence interval (dead interval) is configured at 10 seconds rather than the default of 5 minutes.

A tunnel type of remote access should be configured.

Figure 5-4 shows the IPSec configuration window.

Figure 5-4 VPN 3000 IPSec



Configuration | User Management | Groups | Modify SOHO

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

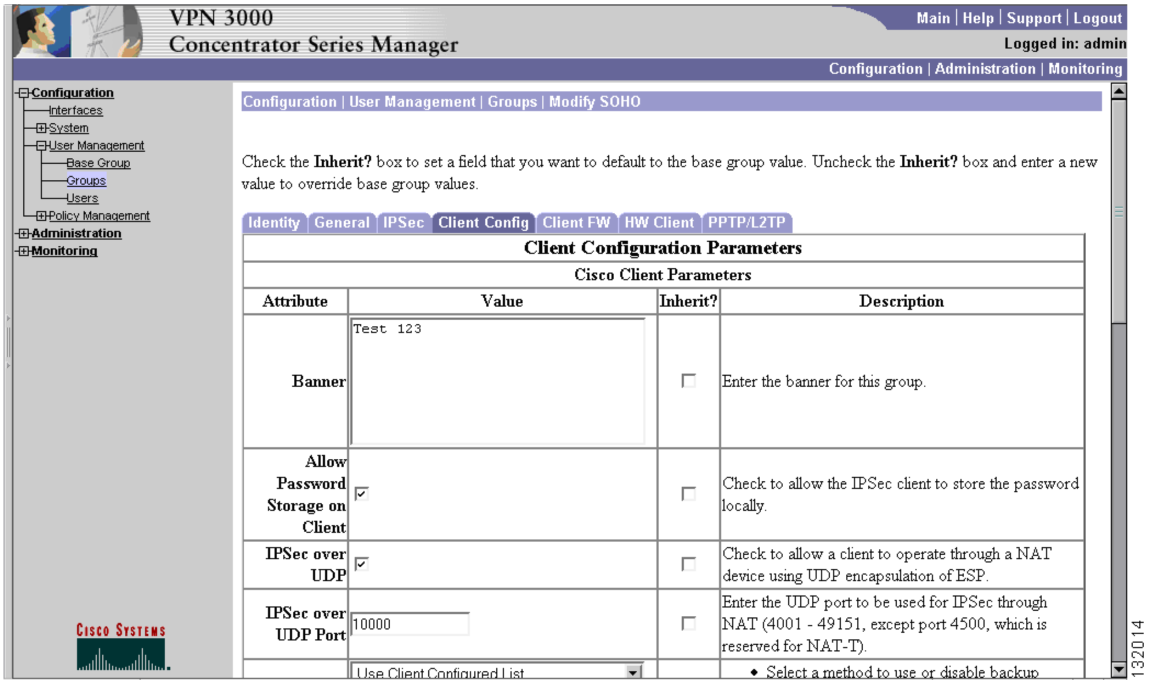
IPSec Parameters			
Attribute	**Value**	**Inherit?**	**Description**
IPSec SA	ESP-3DES-MD5	□	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	□	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	10	□	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
Tunnel Type	Remote Access	□	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	□	☑	Lock users into this group.
Authentication	Internal	□	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
			If members of this group need authorization in addition to

Client Configuration

The IPSec client is permitted to store the password locally. The remote router is disabling NAT-T, so IPSec over UDP is not negotiated because both ends are not configured for NAT-T.

Figure 5-5 shows the VPN 3000 Client Configuration window.

Figure 5-5 VPN 3000 Client Configuration



Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Client Configuration Parameters

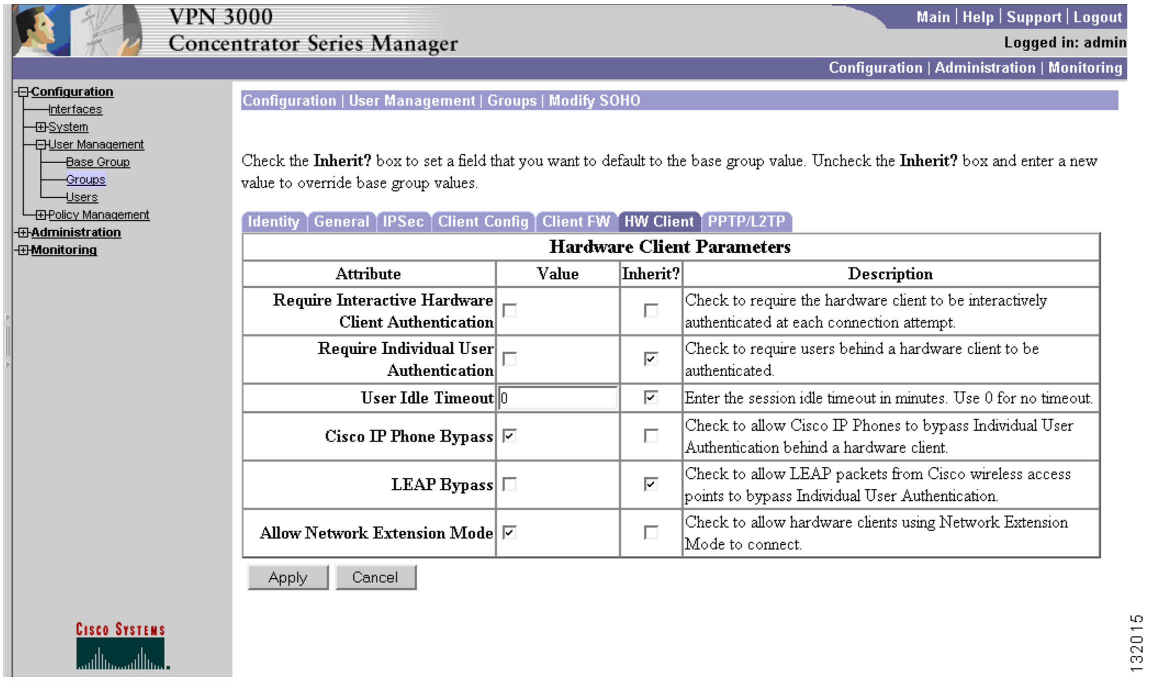
Cisco Client Parameters

Attribute	Value	Inherit?	Description
Banner	Test 123	□	Enter the banner for this group.
Allow Password Storage on Client	☑	□	Check to allow the IPSec client to store the password locally.
IPSec over UDP	☑	□	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPSec over UDP Port	10000	□	Enter the UDP port to be used for IPSec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
	Use Client Configured List		• Select a method to use or disable backup

Hardware Configuration

Network Extension Mode is permitted, as shown in Figure 5-6.

Figure 5-6 VPN 3000 Hardware Configuration



Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Hardware Client Parameters			
Attribute	**Value**	**Inherit?**	**Description**
Require Interactive Hardware Client Authentication	□	□	Check to require the hardware client to be interactively authenticated at each connection attempt.
Require Individual User Authentication	□	☑	Check to require users behind a hardware client to be authenticated.
User Idle Timeout	0	☑	Enter the session idle timeout in minutes. Use 0 for no timeout.
Cisco IP Phone Bypass	☑	□	Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware client.
LEAP Bypass	□	☑	Check to allow LEAP packets from Cisco wireless access points to bypass Individual User Authentication.
Allow Network Extension Mode	☑	□	Check to allow hardware clients using Network Extension Mode to connect.

Users

This section describes the configuration of the users.

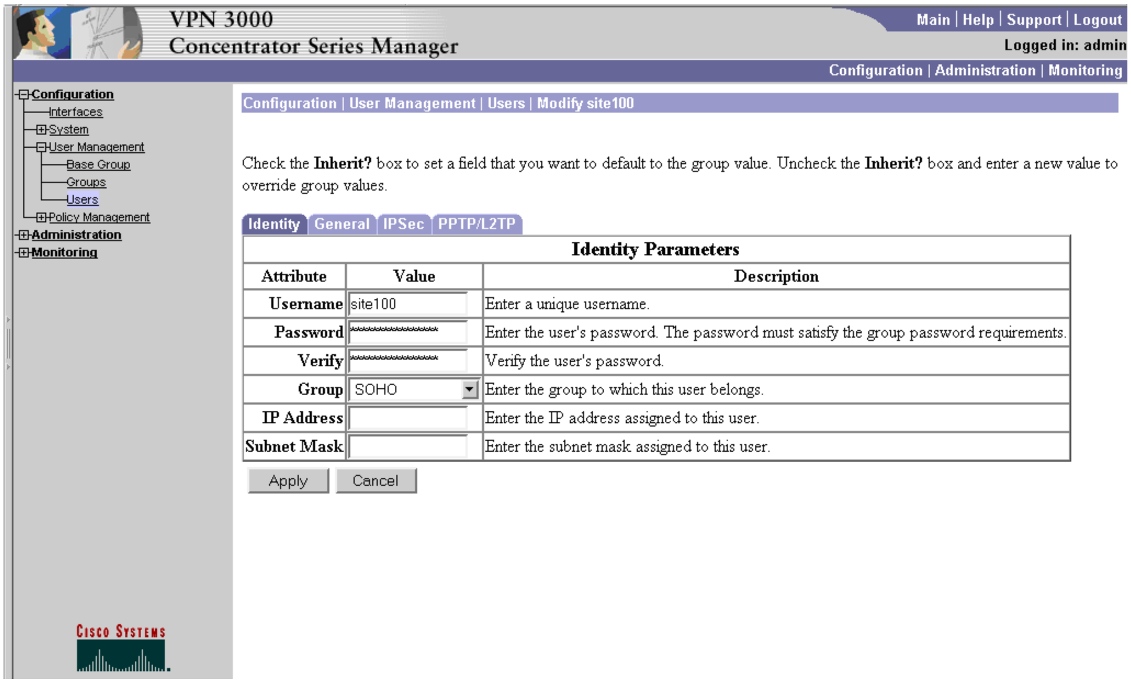
Identity

The username for this location is defined as *site100*. Each location has a unique username.

```
crypto ipsec client ezvpn VPN3080
 connect auto
 group SOHO key point_of_sale
 mode network-extension
 peer 192.168.131.30
 username site100 password  cisco123
```

Figure 5-7 shows the Identity Parameters configuration window.

Figure 5-7 VPN 3000 User Identity



Configuration | User Management | Users | Modify site100

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity Parameters

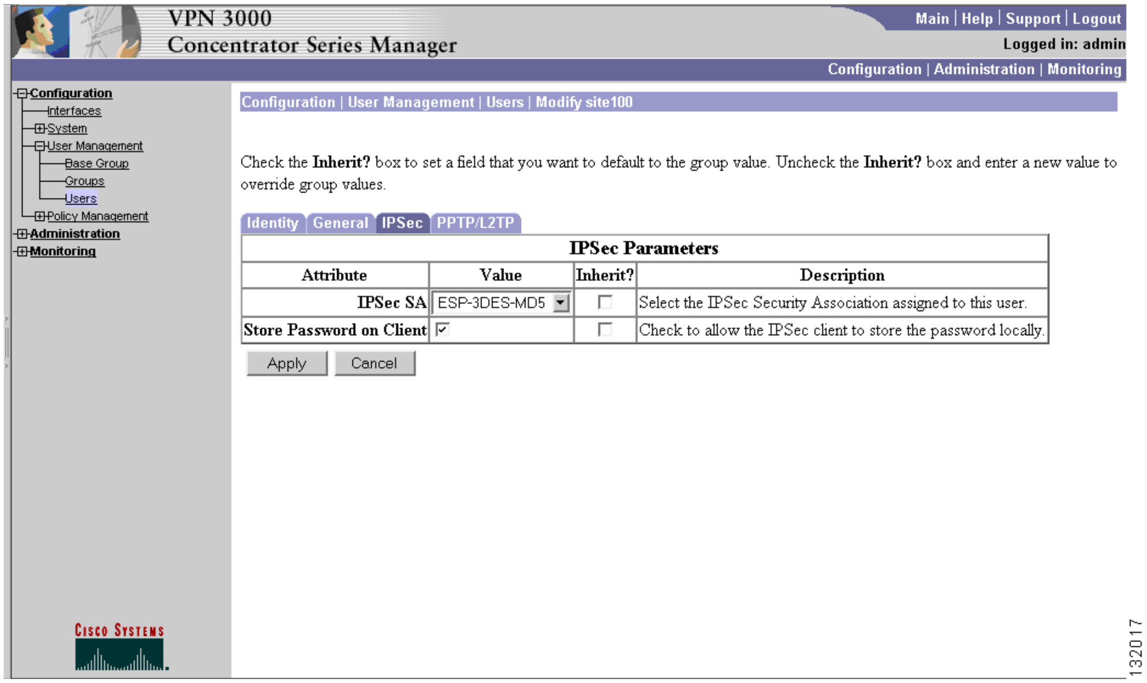
Attribute	Value	Description
Username	site100	Enter a unique username.
Password	****************	Enter the user's password. The password must satisfy the group password requirements.
Verify	****************	Verify the user's password.
Group	SOHO	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

IPSec

The IPSec client is permitted to store the password locally.

Figure 5-8 shows the IPSec Parameters window.

Figure 5-8 VPN 3000 IPSec



Configuration | User Management | Users | Modify site100

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

IPSec Parameters

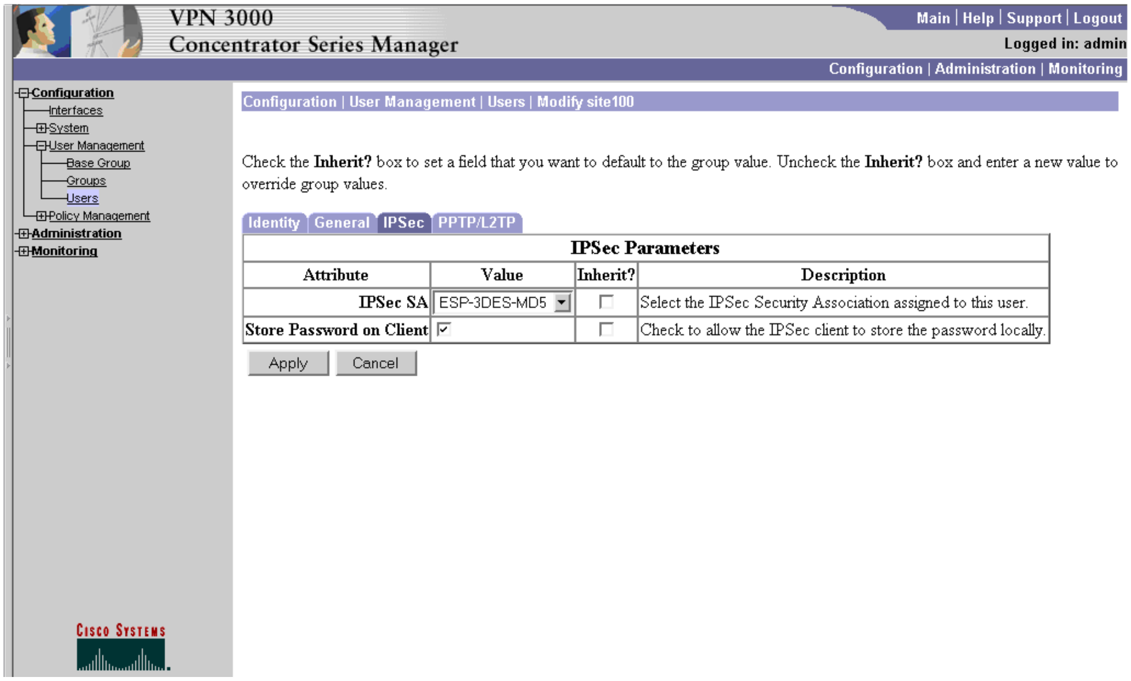
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	□	Select the IPSec Security Association assigned to this user.
Store Password on Client	☑	□	Check to allow the IPSec client to store the password locally.

Policy Management/Traffic Management /SAs

The transform set is defined as follows: tunnel mode, 3DES, and MD5 with default lifetimes.

Figure 5-9 shows the Policy Management window.

Figure 5-9 VPN 3000 Policy Management



Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

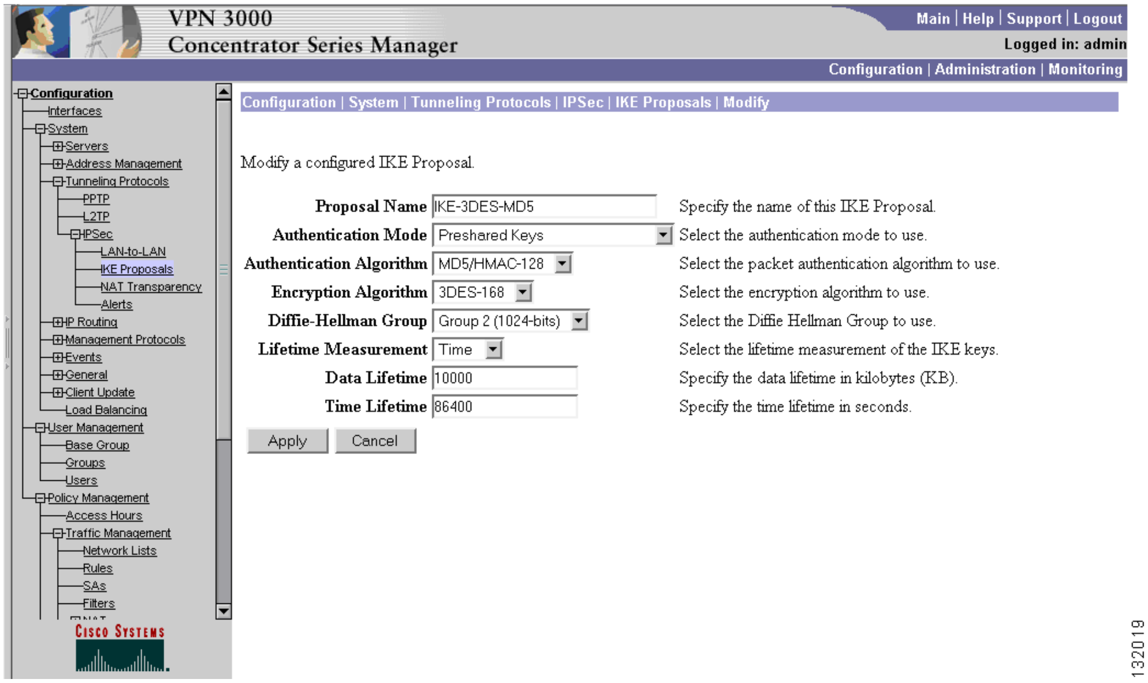
IPSec Parameters			
Attribute	**Value**	**Inherit?**	**Description**
IPSec SA	ESP-3DES-MD5	□	Select the IPSec Security Association assigned to this user.
Store Password on Client	☑	□	Check to allow the IPSec client to store the password locally.

System/Tunneling Protocols/IPSec/IKE

The IKE proposal is defined. Encryption strength is 3DES, hash is MD5, and Diffie-Hellman value is Group 2. The default lifetimes are also configured.

Figure 5-10 shows the Tunneling Protocols window.

Figure 5-10 VPN 3000 Tunneling Protocols



Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify

Modify a configured IKE Proposal.

Proposal Name	IKE-3DES-MD5	Specify the name of this IKE Proposal.
Authentication Mode	Preshared Keys	Select the authentication mode to use.
Authentication Algorithm	MD5/HMAC-128	Select the packet authentication algorithm to use.
Encryption Algorithm	3DES-168	Select the encryption algorithm to use.
Diffie-Hellman Group	Group 2 (1024-bits)	Select the Diffie Hellman Group to use.
Lifetime Measurement	Time	Select the lifetime measurement of the IKE keys.
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime	86400	Specify the time lifetime in seconds.

Cisco IOS Versions Tested

The following code versions were used during testing.

- IPSec head-ends—c2691-ik9o3s-mz.122-13.T10
- Cisco 1712—c1700-k9o3sy7-mz.123-2.XE
- IPSec concentrator—vpn3000-4.0.4.A-k9

The IPSec head-end router was a Cisco 2691 with an AIM hardware VPN module. The Cisco VPN 3000 Concentrator was a Cisco 3080 running Version 4.0.4.A.

This testing was not intended to scale test head-end performance capabilities. In a customer deployment, using IPSec head-ends with suitable performance characteristics aligned with the number of remote routers is advised.

Summary

This design applies to a small-to-medium-sized business with an existing remote access solution using a Cisco VPN 3000 Concentrator that wants to leverage this device to provide backup coverage. This chapter described the head-end routing configuration to demonstrate how you can use a combination of dynamic and static routing to route packets to the appropriate head-end device. The example in this section described the use of Basic Rate ISDN for the dial-backup links, but Async dial-up to an ISP can also be used.

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:

- Topology
- Failover/Recovery Time
- V3PN QoS Service Policy
- Implementation and Configuration
- Show Commands
- Cisco IOS Versions Tested
- Caveats
- Summary

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.

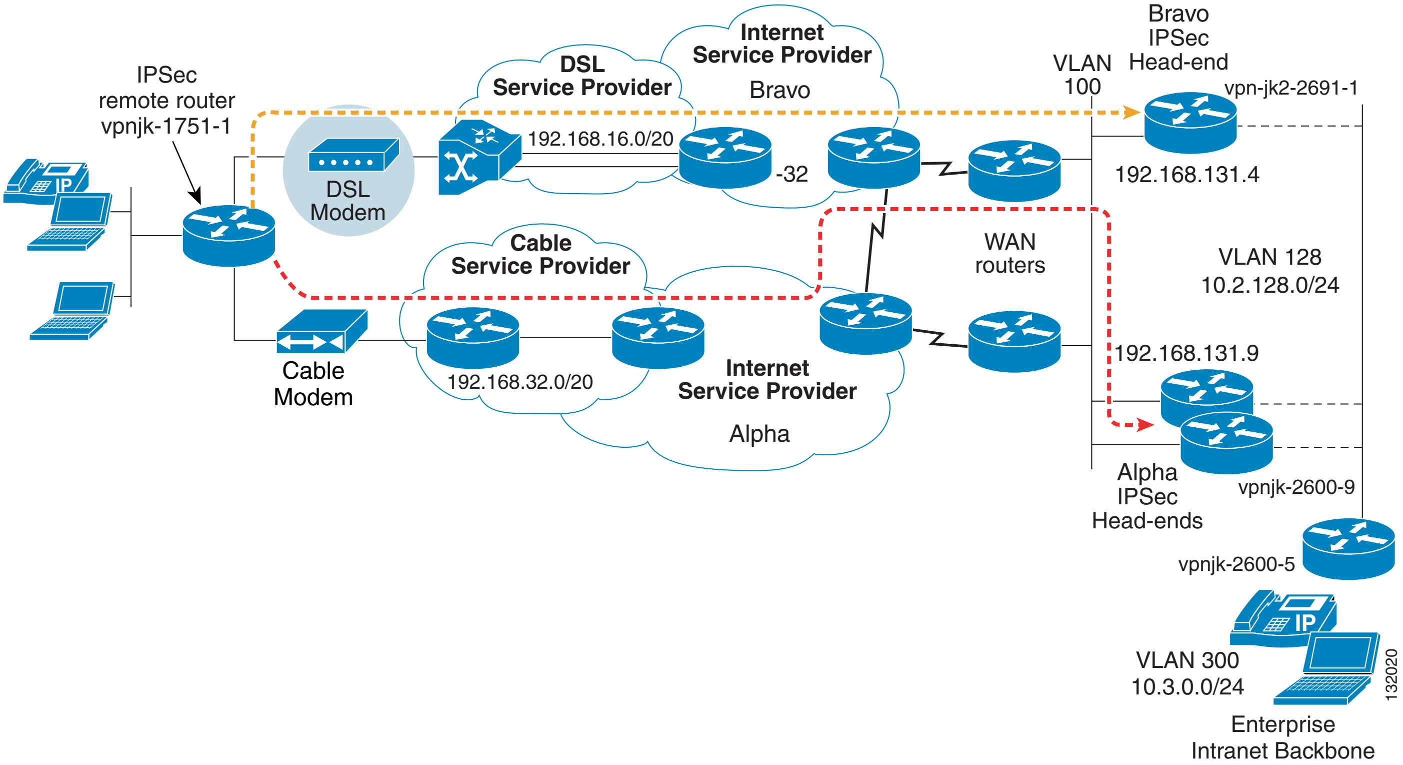
This section includes the following topics:

- Cable (DHCP) and DSL (PPPoE)
- Load Sharing Behind Two Broadband Routers

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



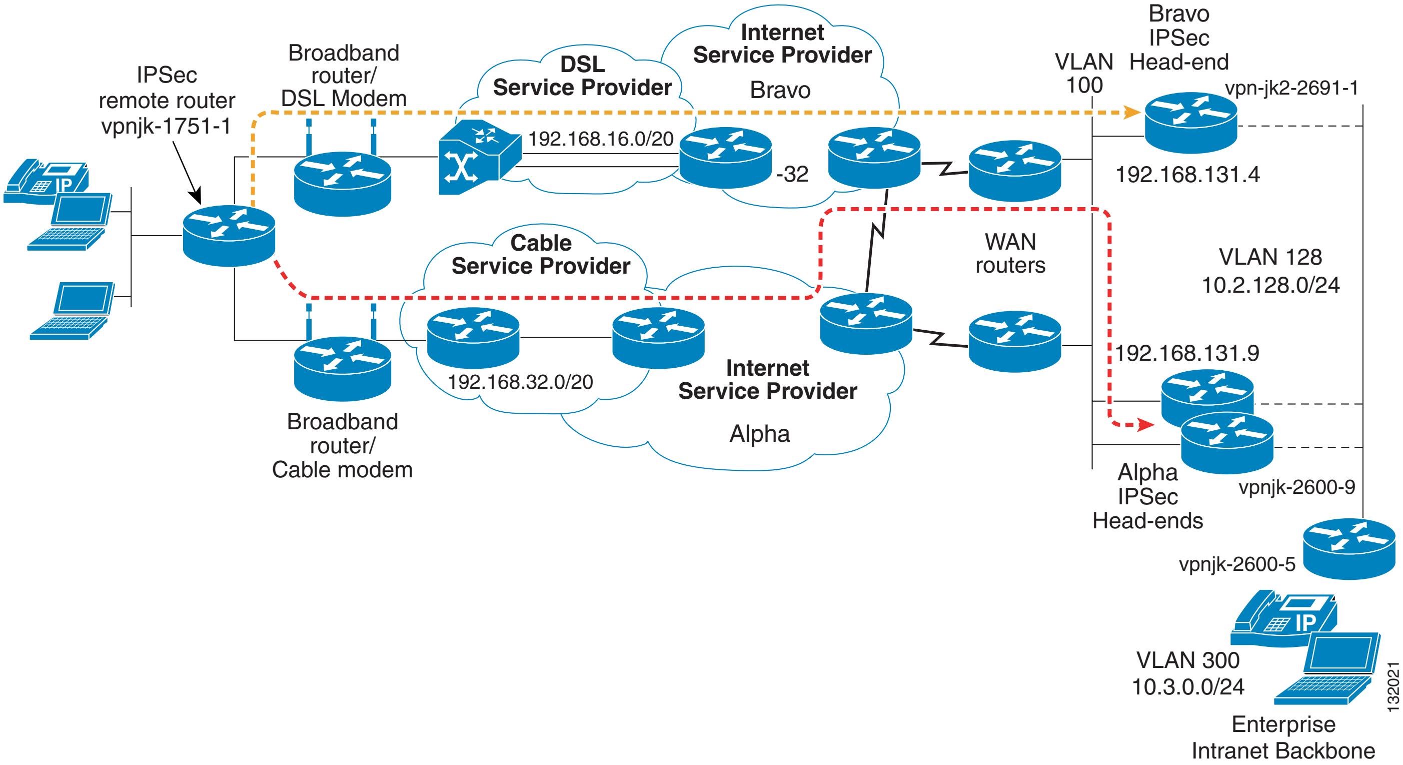
Load sharing between the two IPSec tunnels terminated between the remote router (vpnjk-1751-1), the Alpha IPSec head-end (vpnjk-2600-9), and the Bravo IPSec head-end (vpn-jk2-2691-1) is a function of the routing protocol configuration running on VLAN 128. In this example, the Alpha and Bravo IPSec head-end 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)
- Remote 1751 Router (DHCP and DHCP)
- Bravo IPSec Head-end
- Enterprise Intranet Router

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 5D7B2D430000000000003C
 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
```

This issue is believed related to CSCed29811—static recursive route pointing at default route not cef switched. For this reason, CEF switching can not be used.

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—IPSec packets fast switched on wrong interface with recursive route**.** 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.

CHAPTER 7

Small Branch—Wireless Broadband Deployment

This chapter describes the use of wireless broadband service offerings for small office and home office (SOHO) deployments, including the documentation of the performance characteristics of encrypted voice over IP (VoIP) (Enterprise Class Teleworker)and the configuration of the remote router to use the services as either a primary or backup WAN.

This chapter includes the following sections:

- Solution Characteristics
- Topology
- Failover/Recovery Time
- Performance Results
- Wireless Broadband Hardware Components
- Verification
- Configuration
- Cisco IOS Versions Tested
- Caveats
- Summary

Solution Characteristics

This section describes the characteristics of the small branch wireless broadband deployment solution, and includes the following topics:

- Advantages
- Disadvantages

Advantages

DSL deployments require the phone line to be less than 2.5 miles from the central office of the carrier. To use cable, the residence must be serviced by a cable provider. Both these cases require physical wires, either twisted pair or coaxial cable. A primary advantage of wireless broadband is mobility; the ability to connect to the Internet without using a physical circuit.

Broadband wireless is ideal for a SOHO deployment when cable or DSL are not available, or when the lead time to install is inconvenient, as in the banking and hospitality sectors. Banks are commonly co-located in supermarkets or high traffic areas, so the network manager of the bank must provide connectivity for a cash machine or branch office with short lead times. Hotels need basic connectivity at new locations to handle reservations and credit card transactions. Delays in circuit installation can mean lost business.

Wireless broadband is also advantageous to an enterprise customer as a backup or alternative means of connectivity. As an example, this chapter describes a configuration using a Cisco 1711 router with three WAN interfaces: DSL, wireless broadband, and Async dial-up. If the DSL circuit fails, the wireless broadband is the preferred path. If both DSL and wireless broadband fail, the router creates an encrypted tunnel using dial backup.

Disadvantages

One disadvantage of wireless broadband is the lack of coverage guarantee at all times and all locations within the service area. For example, one location tested by Cisco and described in this chapter was between two antenna towers, with each tower less that two miles from the residence. Signal strength to one of the tower locations was limited by terrain and buildings, and was impaired by foliage for the other.

Note The wireless broadband service provider offers the following caveat: “Wireless broadband coverage is impacted by, among other things, terrain, weather, antenna location, system modification, foliage, and man-made structures (such as buildings), and can therefore not be predicted precisely at all times.”

The wireless modem management software has a signal quality and strength scale of 0–4. Signal quality is a more important indicator than signal strength. Using either the built-in antenna or an external reverse polarity Yagi antenna (purchased separately), testing revealed that quality and strength are in the range of 1–2 on a scale of 0–4.

The wireless broadband service tested offered impressive average latency, meeting or exceeding cable or DSL performance. The packet loss rate and jitter are generally much higher. For most data applications, this is not noticeable. In testing, a Linksys web server (camera) is accessed using the wireless broadband service and the images are of acceptable quality.

Packet loss and jitter can impact the quality of VoIP, and the test results indicated that the voice quality ranged from very good to very poor. Test results are provided later in this chapter.

Topology

This section describes the following two topologies:

- Single WAN Interface
- Multi-WAN Interface

The single WAN interface topology uses the wireless broadband as the only WAN interface. The multi-WAN interface uses the wireless broadband network as an alternate path to the primary DSL network. The single WAN configuration is used for VoIP performance testing. The standard Chariot teleworker traffic profile is used. Chariot endpoints are located at the employee residence and Cisco lab. The test results use the Internet and are representative of a typical deployment and configuration.

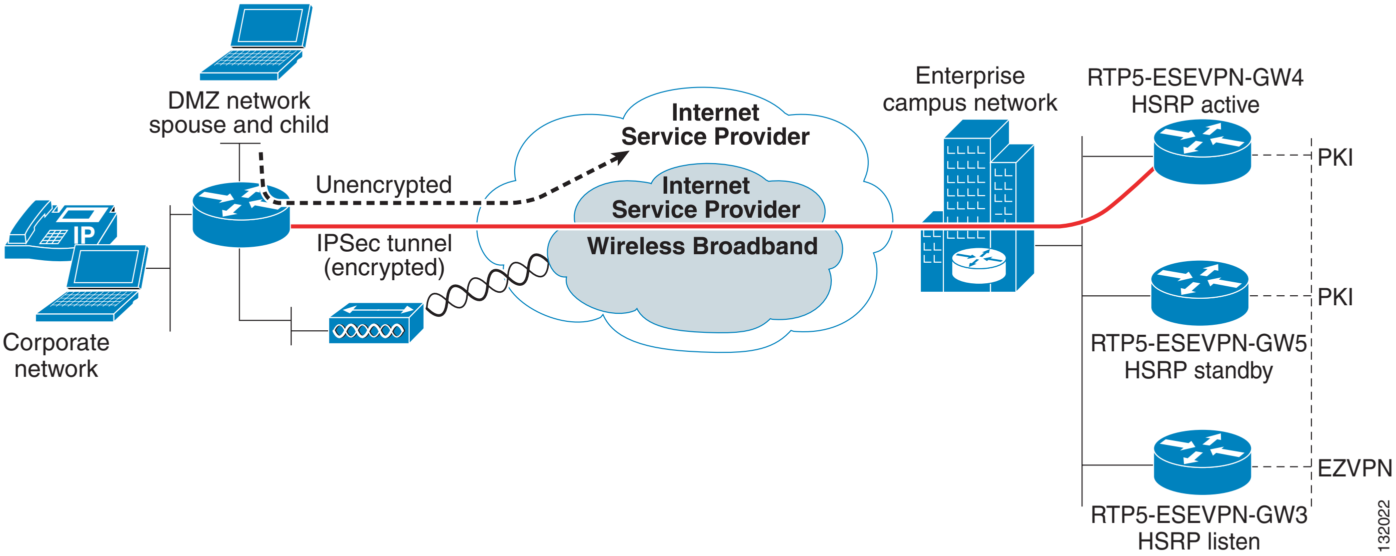
For the multi-WAN configuration, a Linksys web camera was the client/host used to answer pings and to generate network traffic for testing and demonstration.

Note The Linksys web camera was not deployed or in use during the VoIP testing.

Single WAN Interface

The single WAN interface topology is shown in Figure 7-1:

Figure 7-1 Wireless Broadband—Single WAN



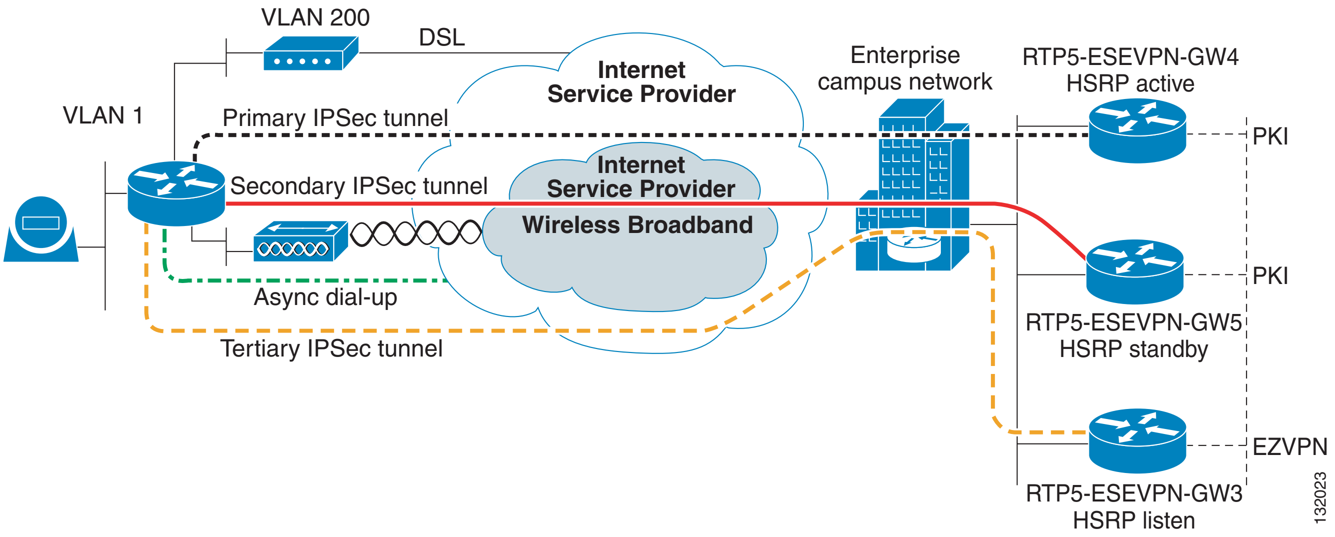
The single WAN topology is used for the VoIP performance testing. Only one IPSec peer is defined in the remote router, and failover and recovery was not a test objective.

Two inside VLANs were defined to implement a physical split tunnel configuration. During the performance testing, no spouse and child traffic was included in the profile.

Multi-WAN Interface

The multi-WAN interface is shown in Figure 7-2:

Figure 7-2 Wireless Broadband—Multi-WAN



The multi-WAN topology takes advantage of key features of the Cisco 1711 router. The Async interface is configured as dial backup to a head-end Cisco 7200 EZVPN server. The Fast Ethernet 0 interface is configured to obtain an IP address from the wireless broadband modem using DHCP. The crypto map on this interface uses RSA keys and a Public-Key Infrastructure (PKI) and Certificate Authority (CA) for authentication. The primary outside interface is defined as a VLAN (200) to the switch module of the Cisco 1711. This interface connects to a DSL router and uses a static IP address. DHCP cannot be used to obtain addresses for a VLAN interface. Authentication also uses RSA keys and a PKI/CA.

A Linksys web camera is attached to the inside or VLAN 1 interface and is used to verify connectivity and to generate sample network traffic. Both the DSL and wireless broadband links have active IPSec tunnels and can pass traffic. The Service Assurance Agent (SAA) probes are generating ICMP packets periodically through their respective tunnels. The Async interface dials the access server of the ISPs only in the event that both the DSL and wireless broadband links are down.

Failover/Recovery Time

The Cisco IOS Reliable Static Routing Backup Using Object Tracking feature was used to monitor and control the backup interface function. How quickly a secondary or tertiary interface is brought online is a function of the configured “down” value of the **track** command. In testing, the following parameters were used:

```
track 200 rtr 200
 delay down 60 up 5
```

Recovery from a path failure takes at least 60 seconds with these values. They are, however, configurable.

Note Enabling **debug track** can provide a visual indication of the quality of the wireless broadband link. Assuming the delay down is configured at 60 and the frequency of the SAA object is 15 seconds, four consecutive SAA packets must be lost for the tracked route to be removed from the routing table. As probes are lost, the debug track provides a log message indicating this. If subsequent probes are lost or are successful, this is also logged by debug track. During periods of high packet loss, the number of logged messages increases accordingly.

Performance Results

The wireless broadband service tested is the wireless broadband service in the Research Triangle Park, North Carolina, USA area.

The test locations are Cisco employee residences in the Raleigh-Durham, North Carolina area using the same IPSec equipment and infrastructure supporting teleworkers over cable and DSL.

These tests results are from a Cisco 1711 router deployed at the employee residence. Cable service provider -Cable–Business Class Service 3 Mbps/768 kbps is used as a reference. The uplink (or branch-to-head-end leg) is shaped to 600 kbps.

Also installed is the wireless broadband (Platinum Class) shaped 256 kbps up and unlimited down. The antenna tower is less than two miles from the residence. Two tests were run; a best case and a worst case. The best case uses the external Yagi antenna.

The signal strength is 3 of 4 and the signal quality is 4 of 4, on the 0–4 scale, as displayed by the Mobility Manager software, not the external LEDs.

The worst case used the supplied antenna (sometimes called a “popsicle-stick” antenna) shown on the product literature photo of the modem in Wireless Broadband Modem, page 7-9. In testing, the signal strength with this antenna is 0 to 1 and signal quality is 0 to 2. The modem is inside the residence.

There are two goal lines on the following performance results charts:

- Lab goal—Value in lab testing that the performance characteristic should not exceed in a lab environment with no appreciable impact because of WAN. Jitter target is less than 8 ms and the latency target is less than 50 ms. Voice packet loss is to be less than 1/2 of one percent.
- Internet goal—Higher than the lab goal values because there is some ISP-associated loss, latency, and jitter. These target values are jitter at less than 20 ms, latency at less than 100 ms, and voice packet loss at less than 1 percent.

Note The ITU value is 150 ms or less. Latency even up to 250 ms can be acceptable. Latency was not an issue in any of these tests.

These tests are conducted at a first adopter stage in the wireless broadband service. There is little or no contention for bandwidth by other subscribers. Results can vary based on a variety of factors, including environmental or terrain interference. The same holds true for the cable tests; results are influenced by contention from other subscribers as well as varying degrees of Internet backbone and enterprise campus traffic.

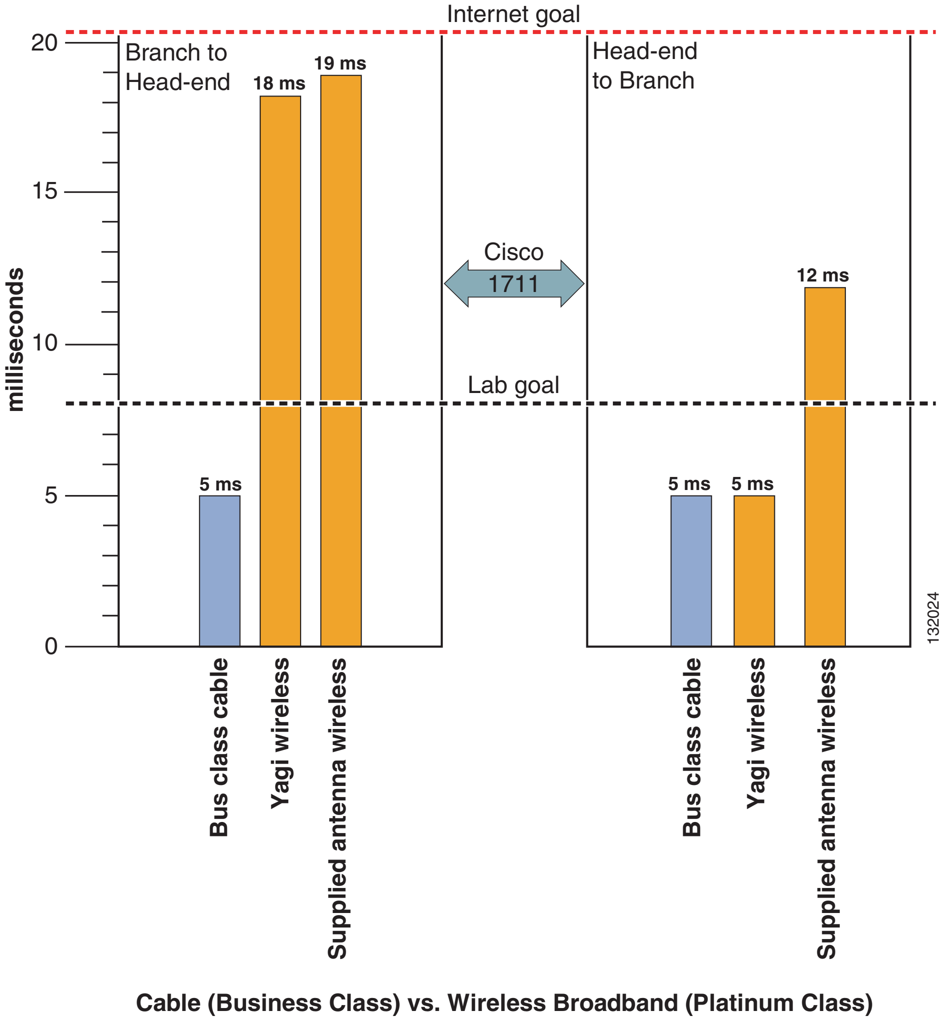
These test results are intended to represent what a typical user may encounter.

Note For best results, an external antenna is recommended.

Average Jitter Comparison

The average jitter between cable and wireless broadband is compared in Figure 7-3:

Figure 7-3 Average Jitter



The uplink, or branch-to-head-end jitter values are substantially higher than the baseline using cable. However, the router on the cable connection was using hierarchical class-based weighted fair queuing (CBWFQ) and shaped at 600 kbps on the uplink, and the wireless broadband link is shaped at 256 kbps.

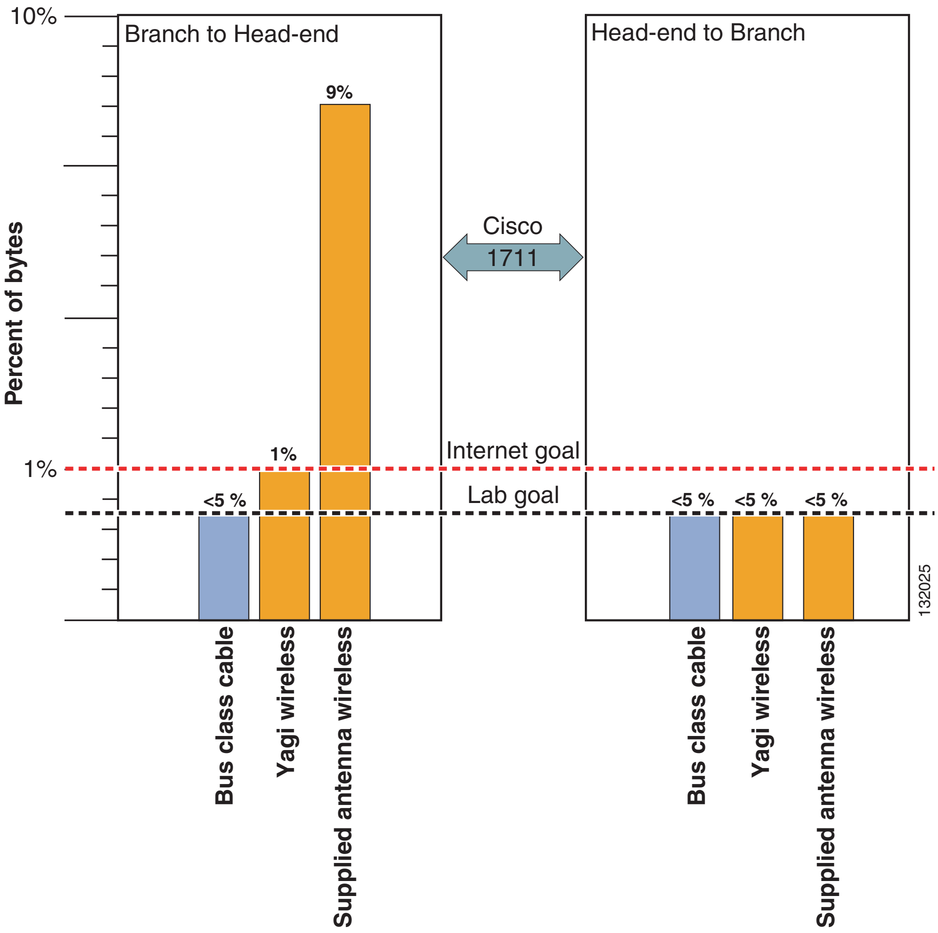
Both the cable and wireless broadband link have no service provider guarantee for uplink speed. The values advertised are for burst or maximum uplink speed. In this environment, both the cable and wireless broadband links are tested with VoIP and also with a TCP-based throughput utility and a shaped value is selected that can be conservatively expected to be available most of the time. The goal is not to overrun a modem or head-end infrastructure and drop packets indiscriminately. Packets should be intelligently queued within a shaped rate by the remote router.

To add to the objective data, actual VoIP calls are placed using the wireless broadband to subjectively verify that the voice quality is good.

Voice Loss

The voice loss is compared between cable and wireless broadband in Figure 7-4:

Figure 7-4 *Voice Loss*



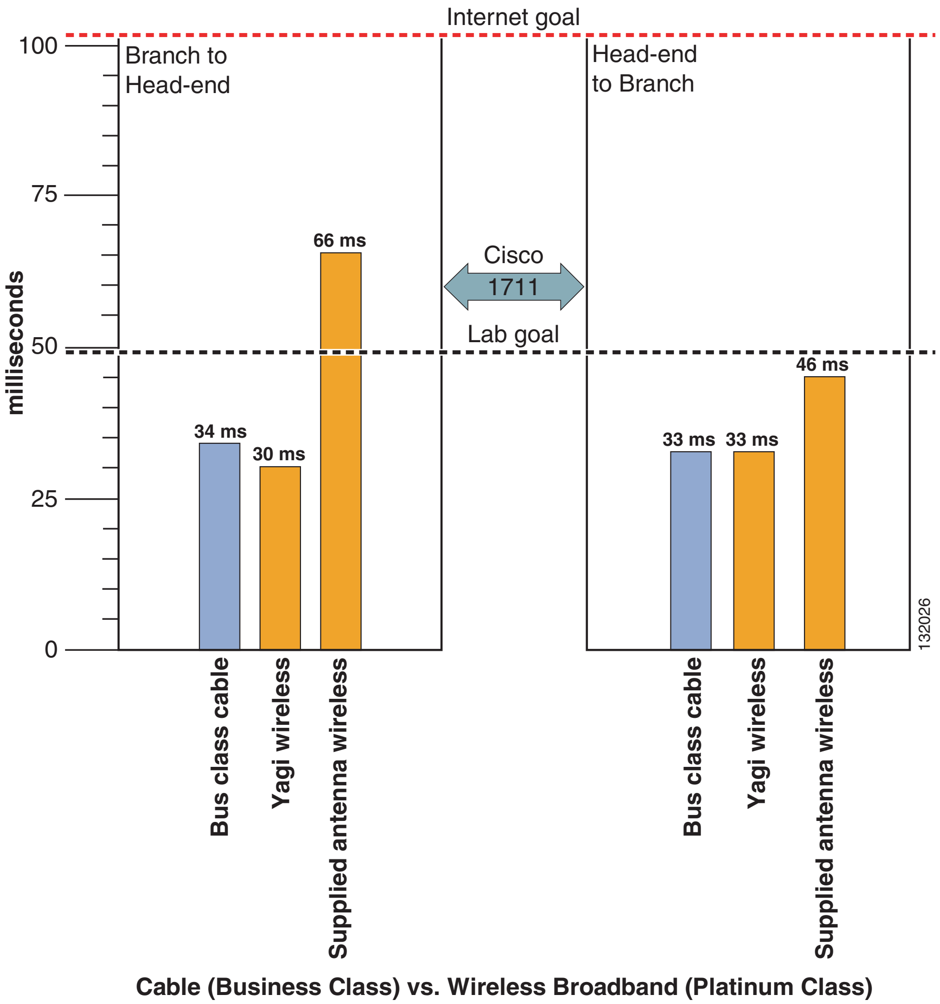
The percent of bytes lost for the G.729 voice stream is acceptable for cable and wireless broadband using the Yagi antenna. Voice loss using the supplied antenna exceeds the target threshold. Nine percent loss for voice is excessive. Nine percent loss is high even for data-only applications.

Note Voice codecs can manage single packet loss with concealment algorithms. If consecutive packets are lost, it is noticeable to the listener.

Average Latency

The average latency is compared between cable and wireless broadband in Figure 7-5:

Figure 7-5 Latency



The average latency is very good in all configurations. These values are equivalent to what is typically seen in broadband deployments.

Mission Critical Response Time

The Chariot traffic profile also includes data that is marked with Differentiated Services Code Point (DSCP) value of AF21. While many of the tests include a transactional data class allocated a minimum bandwidth of 22 percent, the wireless broadband tests did not include a separate class. Therefore, these packets are in the class default class . The Yagi and supplied antenna tests report .2 seconds and .5 seconds for mission critical response time. The cable value is .1 second. All are reasonably good values.

Wireless Broadband Hardware Components

This section describes the hardware components of the wireless broadband solution, and includes the following topics:

- Wireless Broadband Modem
- Yagi Antenna and Cables
- Cisco 1711 and Cabling
- Yagi Antenna Aiming
- Mobility Manager

Wireless Broadband Modem

The MT-1000 wireless broadband modem (see Figure 7-6) is tested using the included antenna as well as an external Yagi antenna. The plastic side panel of the MT-100 needed to be removed to securely connect the cables for the external antenna.

Figure 7-6 MT-1000 Wireless Broadband Modem

Note The Ethernet interface is a 10/100 interface but was tested with Cisco 1711s and not tested with the Cisco 831. The Cisco 831 Ethernet 1 (outside) interface is a 10 Mbps interface and is not a 100 Mbps FastEthernet interface.

Yagi Antenna and Cables

The information of the external antenna is as follows:

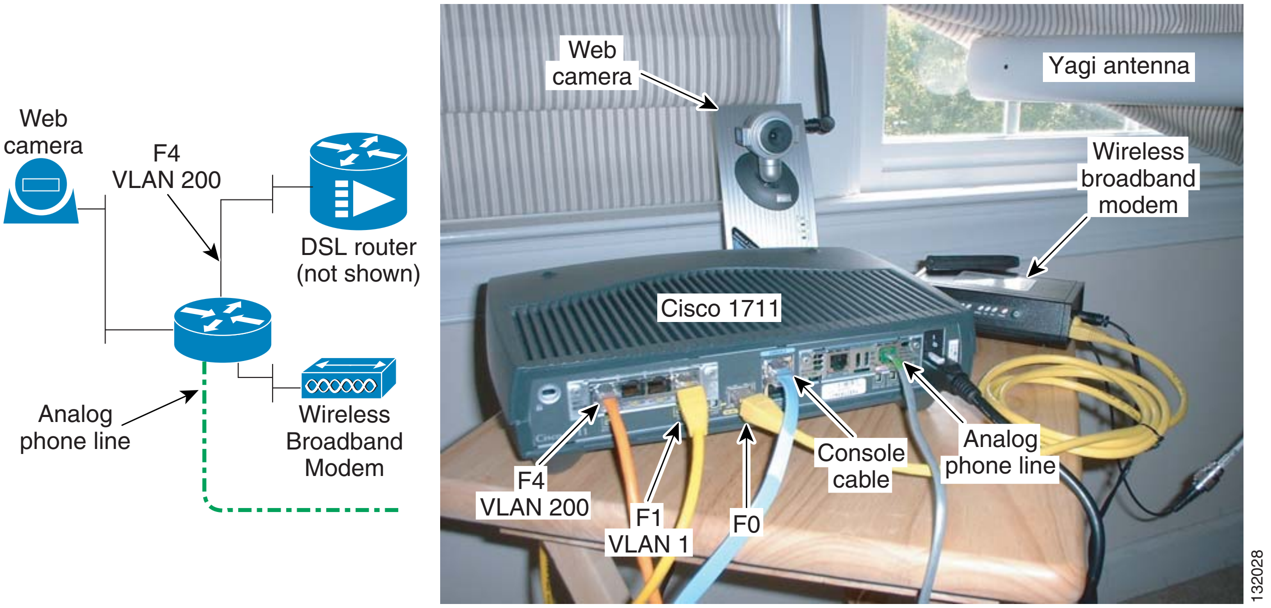
- HyperGain® HG1910Y
  High Performance 1850-1970 MHz 10 dBi Radome Enclosed Yagi Antenna
- Standard Connector—Yagi N-female
- Part Number—HG1910Y-NF
- Wireless LAN Radio Pigtails—RP-MMCX Type to N-female 19 in. (LMR/WBC100 cable) part number CA-PHCABLE2

An N-male to N-male connector is required between the standard Yagi N-female connector and the N-female pigtail cable that attaches to the MT-1000. Cable length depends on the distance between the Yagi antenna and the MT-1000.

Cisco 1711 and Cabling

Figure 7-7 shows the remote Cisco 1711 router with the physical cabling and connections.

Figure 7-7 Cisco 1711 and Cabling



The F4 (interface Fa4) switch port is configured as VLAN 200 and is connected to a Cisco 837 DSL router (not shown). The F1 (interface Fa1) switch port is configured as VLAN 1 and is connected to the Linksys Web Camera. The F0 (interface Fa0) port is connected to the wireless broadband modem. The analog phone line is connected to the DSL splitter.

Yagi Antenna Aiming

These instructions on aiming the antenna assume that the consumer or an installer knows the location of the nearest antennas.

Yagi antenna are directional antenna and must be aimed at the radio tower for best signal strength and quality. In testing, a vendor contact provided a map marked with the two nearest tower locations and the residence location.

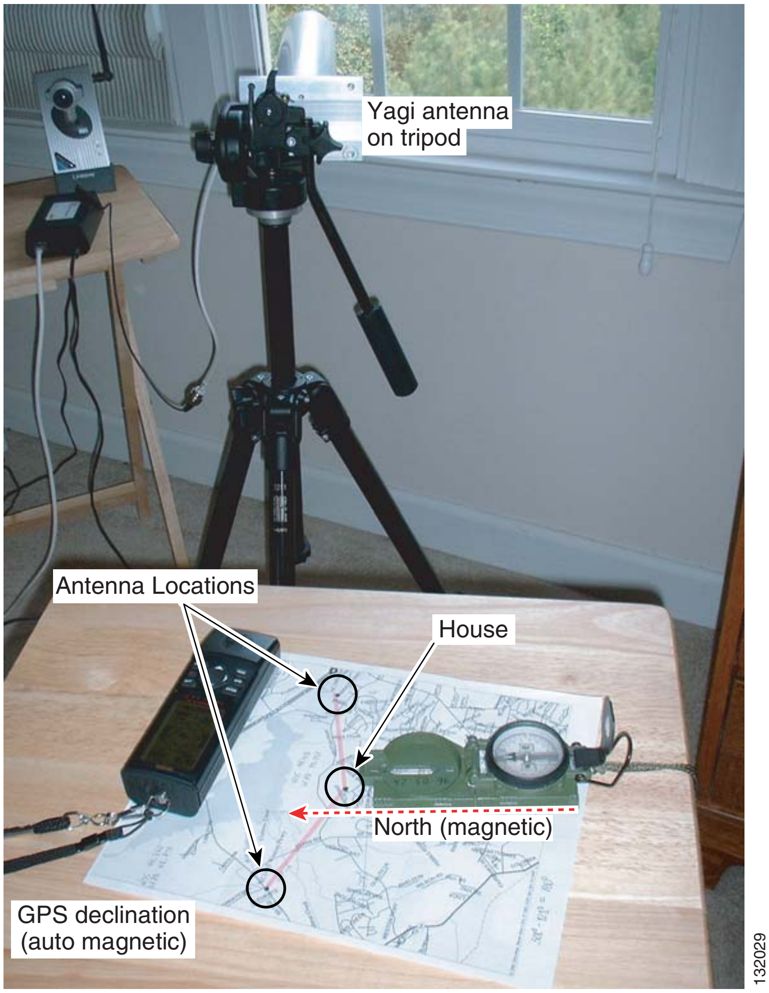
The map did not contain a reference line for either true or magnetic north. A global positioning system (GPS) receiver and the coordinates for the residence are available. By driving to one of the antenna locations and marking its location, the GOTO function on the GPS is used to determine the degrees azimuth. These two values should have a difference of 180 degrees. A GPS receiver when at rest provides no bearing information, but it does indicate the azimuth you must travel to reach the desired location.

To orient the map, the compass base is aligned between the two known points, and the map and compass are rotated until the index line (which is parallel with the base) is over the desired number of degrees. While the map remains in this position, orient the compass base so that the stationary index line is aligned with north, or 0 degrees, and draw a reference line using the compass base as a straight-edge. This puts a magnetic north reference line on the map assuming the number of degrees between the two known positions can be obtained by a GPS set to magnetic declination. Most GPS units can be set to true north or magnetic north with either auto or manual declination.

With the map remaining facing North, the compass base can be aligned between the Yagi antenna location and the second tower. The number of degrees indicated by the index mark is the azimuth the antenna must face (80 degrees in this test). The azimuth between the residence and the first tower is 301 degrees and from the tower to the house is 121 degrees. These values must be 180 degrees different to be correct.

Figure 7-8 shows the Yagi antenna pointed approximately 80 degrees to the second tower with the compass and map.

Figure 7-8 Aiming the Yagi



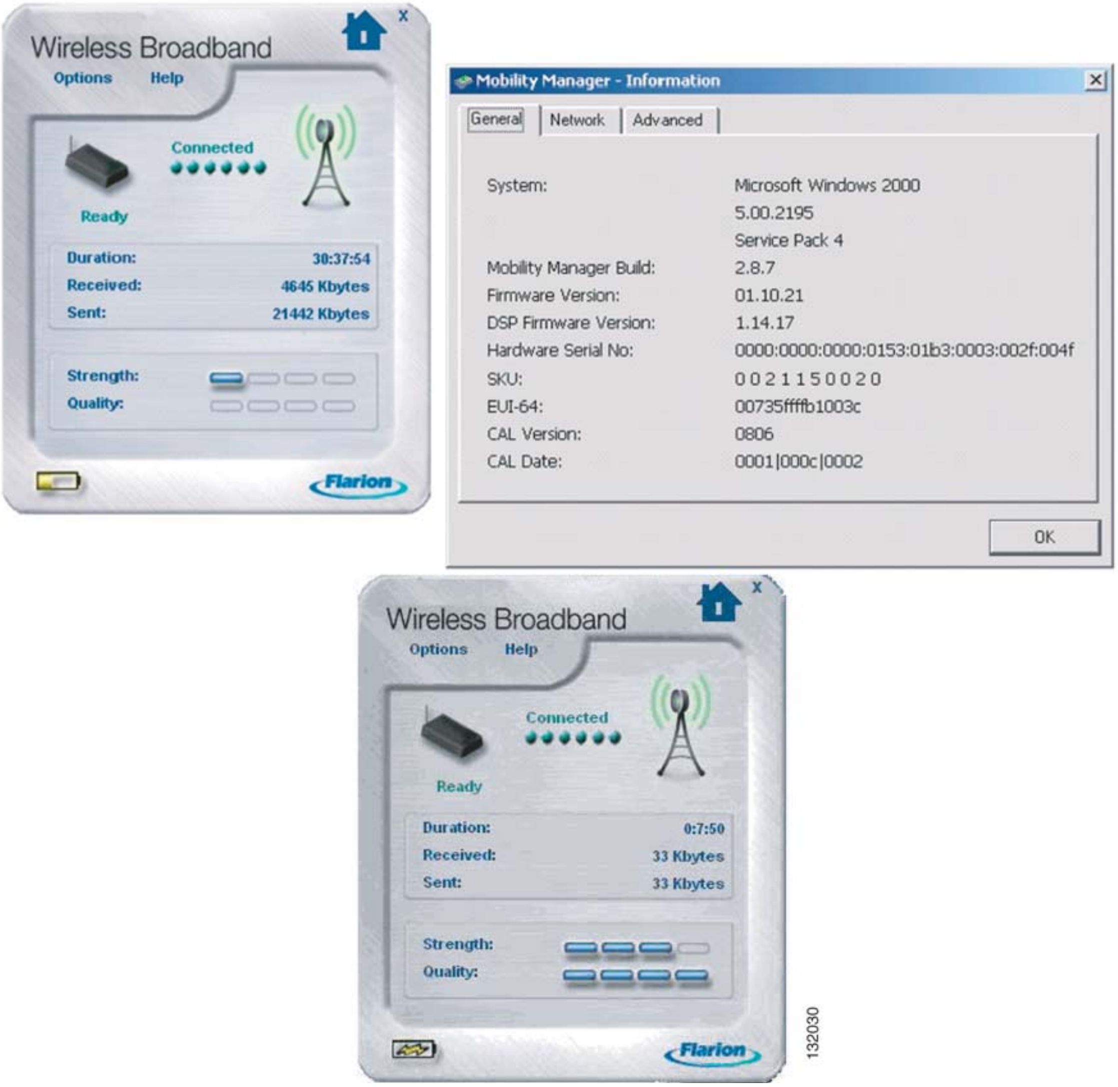
Ideally, the Yagi is attached outside the structure. It saves time by first testing on a tripod or temporary support before permanently mounting.

Mobility Manager

The wireless broadband service includes Mobility Manager software. This software is installed on a PC, and the PC Ethernet interface and the wireless broadband modem are connected with a straight-through Ethernet CAT5 cable. Signal strength and quality are displayed on their own four-point scale to fine-tune the Yagi antenna.

You can also use the software to upload firmware updates to the modem and to determine its status. You should also use this software to verify the connection before connecting to a router. Because the modem contains its own DHCP server, there is no problem moving the cable between a PC and the router interface configured as a DHCP client. Samples of best and worst case signal strength and quality are shown in Figure 7-9:

Figure 7-9 ***Mobility Manager***



Duration: 30:37:54
Received: 4645 Kbytes
Sent: 21442 Kbytes
Strength:
Quality:

Mobility Manager - Information

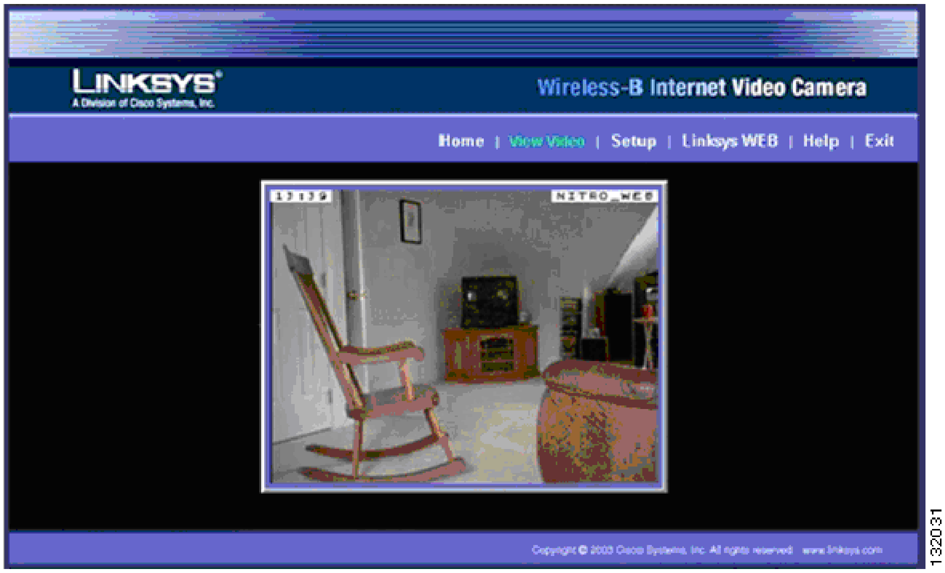
System:	Microsoft Windows 2000 5.00.2195 Service Pack 4
Mobility Manager Build:	2.8.7
Firmware Version:	01.10.21
DSP Firmware Version:	1.14.17
Hardware Serial No:	0000:0000:0000:0153:01b3:0003:002f:004f
SKU:	0021150020
EUI-64:	00735ffffb1003c
CAL Version:	0806
CAL Date:	0001|000c|0002

Duration: 0:7:50
Received: 33 Kbytes
Sent: 33 Kbytes
Strength:
Quality:

Verification

For usability with visual and audible confirmation, live voice calls are placed over the wireless broadband link and a Linksys web camera is viewed. The performance charts for the Chariot test scripts are described in the performance section. Figure 7-10 shows a screen print of the image from the camera.

Figure 7-10 Video Image over Wireless Broadband


LINKSYS®
A Division of Cisco Systems, Inc.
Wireless-B Internet Video Camera
Home | View Video | Setup | Linksys WEB | Help | Exit
13:19
NITRO_WEB
132031

Copyright © 2003 Cisco Systems, Inc. All rights reserved. www.linksys.com

In the multi-WAN configuration, the DSL and wireless broadband links are failed, forcing the Cisco 1711 into a dial-up mode. From a head-end campus, the IP address of the web camera is the target of a ping during the failure scenarios to verify that IKE Keepalive/DPD/RRI is removing routes from the routing table and also from EIGRP advertisements between the three IPSec head-end routers.

Note The three IPSec head-end routers exchange routes using the 192.168.82.0 network.

Configuration

This section describes the configurations for the various components of the wireless broadband solution, and includes the following topics:

- Multi-WAN Cisco 1711 Router
- Single WAN Remote Router
- EZPVN Head-end Server
- Primary IPSec Head-end
- Secondary IPSec Head-end

Multi-WAN Cisco 1711 Router

The configuration for the multi-WAN Cisco 1711 router is as follows:

```
!!
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service tcp-small-servers
```

```
!
hostname vpn-jk2-1711-1
!
boot-start-marker
boot system flash c1700-k9o3sy7-mz.123-2.XF
boot-end-marker
!
logging buffered 2048000 debugging
enable secret 5 $xxxxvvvvvvvvvv
!
username ese_vpn_team privilege 15 secret 5 vvvvvvvvvvvv.
clock timezone est -5
clock summer-time edt recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
!
!
!
!
ip tftp source-interface Vlan1
no ip domain lookup
ip domain name cisco.com
ip host harry 172.26.129.252
ip host rtp5-esevpn-ios-ca 10.81.0.27
ip name-server 207.69.188.185
ip name-server xx.xxx.6.247
ip name-server 171.68.226.120
ip cef
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip audit notify log
ip audit po max-events 100
ip dhcp-client default-router distance 222
!
track 150 rtr 150
 delay down 60 up 5
!
track 200 rtr 200
 delay down 60 up 5
no ftp-server write-enable
chat-script MODEM "" "atdt\T" TIMEOUT 60 CONNECT \c
!
!
crypto ca trustpoint rtp5-esevpn-ios-ca
 enrollment url http://rtp5-esevpn-ios-ca:80
 revocation-check none
 source interface Vlan1
 auto-enroll 70
!
!
crypto ca certificate chain rtp5-esevpn-ios-ca
 certificate 23
  quit
 certificate ca 01
  quit
!
!              Refer to status of CSCef87216
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
!
!
crypto ipsec transform-set TUNNEL_3DES_SHA esp-3des esp-sha-hmac
!
!
!
crypto ipsec client ezvpn RTP5-ESEVPN-GW3
 connect auto
 group EZVPN_Group key [must_match_Group_in_Head-end]
 mode network-extension
 peer xx.xxx.223.24
 username vpn-jk2-1711-1 password [must_match_PW_in_Head-end]
!
!
crypto map RTP5-ESEVPN-GW4 10 ipsec-isakmp
 description IPsec Peer for DSL Link
 set peer xx.xxx.223.24
 set transform-set TUNNEL_3DES_SHA
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
crypto map RTP5-ESEVPN-GW5 10 ipsec-isakmp
 description IPsec Peer for Broadband Wireless
 set peer xx.xxx.223.25
 set transform-set TUNNEL_3DES_SHA
 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
!
!          See policy-map BLOCK_VoIP there will be no VoIP on the backup links
!
policy-map BACKUP-INTERFACES
 class INTERNETWORK-CONTROL
  bandwidth percent 5
  set dscp cs6
 class TRANSACTIONAL-DATA
  bandwidth percent 22
 class class-default
  fair-queue
  random-detect
!
policy-map Shaper-WIRELESS
 class class-default
  shape average 102400# Interval not set to 10ms as no VoIP on this link.
  fair-queue
  random-detect
  service-policy BACKUP-INTERFACES
!
policy-map BLOCK_VoIP
```

```
description Prevent an IP Phone from registering on this link
 class VOICE
   police 8000 conform-action drop  exceed-action drop
 class CALL-SETUP
   police 8000 conform-action drop  exceed-action drop
policy-map V3PN-teleworker
description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
  set dscp cs6
 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-teleworker
!
!
!
interface FastEthernet0
 description Outside to MT-1000 Wireless Broadband MODEM
 ip dhcp client route track 150
 ip address dhcp
 ip access-group INPUT_ACL in
 service-policy input BLOCK_VoIP
 service-policy output Shaper-WIRELESS
 ip route-cache flow
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
 crypto map RTP5-ESEVPN-GW5
!
interface FastEthernet1
 description Inside to WEB Camera
 no ip address
 vlan-id dot1q 1
  exit-vlan-config
 !
!
interface FastEthernet2
 no ip address
 vlan-id dot1q 1
  exit-vlan-config
 !
!
interface FastEthernet3
 no ip address
 vlan-id dot1q 1
  exit-vlan-config
 !
!
interface FastEthernet4
 description Outside to DSL Router
 switchport access vlan 200
 no ip address
!
```

```
interface Vlan1
 description Inside
 ip address 10.81.7.225 255.255.255.248
 ip inspect CBAC in
 ip route-cache flow
 ip tcp adjust-mss 542
 crypto ipsec client ezvpn RTP5-ESEVPN-GW3 inside
!
interface Vlan200
 description Outside to DSL Router
 ip address 192.168.2.211 255.255.255.0
 ip access-group INPUT_ACL in
 service-policy output Shaper-DSL
 ip route-cache flow
 crypto map RTP5-ESEVPN-GW4
!
interface Async1
 description EarthLink Dialup Service V34/LAPM/V42B/24000:TX/26400:RX
 bandwidth 24
 ip address negotiated
 ip access-group INPUT_ACL in
 service-policy input BLOCK_VoIP
 service-policy output BACKUP-INTERFACES
 encapsulation ppp
 ip route-cache flow
 load-interval 30
 dialer in-band
 dialer string 6550070
 dialer-group 21
 async mode dedicated
 ppp authentication pap callin
 ppp pap sent-username xxxxxx@mindspring.com password 7 vvvvvvvvvvvvvvvv
 crypto ipsec client ezvpn RTP5-ESEVPN-GW3
!
ip classless
!
! A default route will be available via DHCP with an administrative distance of 222,
! based on the ip dhcp-client default-router distance 222 command.
!
! The DSL router's IP address is 192.168.2.1
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1 200 name Quad_Zero_via_DSL track 200
ip route 0.0.0.0 0.0.0.0 Async1 240 name DIAL_BACKUP
!
!
! The EZVPN IOS Head-end Server is xx.xxx.223.23
!
ip route xx.xxx.223.23 255.255.255.255 Async1 name DIAL_BACKUP_IPSEC_peer
ip route xx.xxx.223.23 255.255.255.255 Null0 223 name DUMP_when_int_down
!
! The IPSec peer for the DSL link
!
ip route xx.xxx.223.24 255.255.255.255 Vlan200 192.168.2.1 permanent name DSL_router
!
!
!  The IPSec peer for the Wireless Broadband link
!
ip route xx.xxx.223.25 255.255.255.255 FastEthernet0 dhcp 222
ip route xx.xxx.223.25 255.255.255.255 Null0 223 name DUMP_when_int_down
!
!
ip route 172.30.30.128 255.255.255.255 FastEthernet0 dhcp# Host route to Wirless MODEM
!                             # DHCP Server, See Caveats.
no ip http server
no ip http secure-server
ip flow-export version 5
!
!
!
ip access-list extended CRYPTO_MAP_ACL
 permit ip 10.81.7.224 0.0.0.7 any
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
ip access-list extended INPUT_ACL
 remark Allow IKE and ESP from the RTP headends
 permit udp xx.xxx.16 0.0.0.15 any eq isakmp
 permit udp xx.xxx.223.16 0.0.0.15 any eq non500-isakmp
 permit esp xx.xxx.223.16 0.0.0.15 any
 remark Cisco Corporate Subnets (not complete)
 permit ip xxx.44.0.0 0.0.255.255 10.81.7.224 0.0.0.7
 permit ip xxx.68.0.0 0.3.255.255 10.81.7.224 0.0.0.7
 permit ip xxx.16.0.0 0.15.255.255 10.81.7.224 0.0.0.7
 permit ip xxx.168.0.0 0.0.255.255 10.81.7.224 0.0.0.7
 permit ip xxx.107.0.0 0.0.255.255 10.81.7.224 0.0.0.7
 permit ip xx.100.0.0 0.3.255.255 10.81.7.224 0.0.0.7
 permit ip xx.104.0.0 0.0.255.255 10.81.7.224 0.0.0.7
 permit ip xx.0.0.0 0.255.255.255 10.81.7.224 0.0.0.7
 permit udp any any eq bootpc
 remark NTP ACLs
 permit udp 192.5.41.40 0.0.0.1 eq ntp any
 permit udp host 216.210.169.40 eq ntp any
 remark SSH from RTP Ridge
 permit tcp xx.xxx.87.0 0.0.0.255 any eq 22
 permit icmp any any
 deny   ip any any
access-list 121 remark Define Interesting Traffic
access-list 121 permit ip any any
dialer-list 21 protocol ip list 121
!
control-plane
!
rtr responder
rtr 12
 type echo protocol ipIcmpEcho xxx.26.129.252 source-ipaddr 10.81.7.225
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 life forever start-time now
rtr 150
 type echo protocol ipIcmpEcho xx.102.223.25 source-ipaddr 10.81.7.225
 tos 192
 timeout 500
 owner vpn-jk2-1711-1
 tag TRACKING_PROBE_FOR_WIRELESS_BROADBAND
 frequency 15
 lives-of-history-kept 1
 buckets-of-history-kept 20
 filter-for-history failures
rtr schedule 150 life forever start-time now
!
rtr 200
 type echo protocol ipIcmpEcho xx.xxx.223.24 source-ipaddr 10.81.7.225
 tos 192
 timeout 200
 owner vpn-jk2-1711-1
 tag TRACKING_PROBE_FOR_DSL
 frequency 15
 lives-of-history-kept 1
 buckets-of-history-kept 20
 filter-for-history failures
rtr schedule 200 life forever start-time now
!
alias exec vlandata vlan database
!
line con 0
 exec-timeout 60 0
 login local
 stopbits 1
line 1
 script dialer MODEM
 modem InOut
 modem autoconfigure discovery
 transport input all
 transport output pad udptn telnet rlogin ssh
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
 stopbits 1
line vty 0 4
 login local
 transport input ssh
!
exception memory minimum 786432
ntp clock-period 17179979
ntp server 192.5.41.41
ntp server 192.5.41.40
ntp server 216.210.169.40
ntp server 10.81.254.202 source Vlan1
end
```

Single WAN Remote Router

This Cisco 1711 router is configured with a “physical” split tunnel. The spouse and child computers are on the VLAN 2 logical interface and their addresses are available via NAT/pNAT to the Internet unencrypted. All corporate traffic is encrypted and sent to the corporate head-end. During performance testing, no spouse and child traffic is present in the Chariot traffic profile.

```
!
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname steve-vpn-1711
!
boot-start-marker
boot system flash:c1700-k9o3sy7-mz.123-8.T3.bin
boot-end-marker
!
logging buffered 200000 debugging
!
username ese_vpn_team privilege 15 secret 5 xxxx
clock timezone est -5
clock summer-time edt recurring
```

```
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
!
!
ip dhcp excluded-address 192.168.1.1 192.168.1.10
!
ip dhcp pool Client    # Corporate Network Address space, not NAT
   network 10.81.7.168 255.255.255.248
   default-router 10.81.7.169
   dns-server xx.xxx.6.247 171.68.226.120
   domain-name cisco.com
   option 150 ip xx.xxx.2.93
   netbios-name-server 171.68.235.228 171.68.235.229
!
ip dhcp pool SpouseChild# Spouse and Child will be NAT/pNAT'ed
   import all
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
!
!
ip telnet source-interface Vlan1
ip tftp source-interface Vlan1
no ip domain lookup
ip domain name cisco.com
ip host harry 172.26.129.252
ip host rtp5-esevpn-ios-ca 10.81.0.27
ip name-server 207.69.188.185
ip name-server xx.xxx.6.247
ip cef
ip inspect max-incomplete high 1400
ip inspect one-minute high 1400
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip ips po max-events 100
ip ssh source-interface Vlan1
!
!
crypto pki trustpoint rtp5-esevpn-ios-ca
 enrollment url http://rtp5-esevpn-ios-ca:80
 revocation-check none
 source interface Vlan1
 auto-enroll 70
!
!
crypto pki certificate chain rtp5-esevpn-ios-ca
 certificate 16
 certificate ca 01
!
!
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-teleworker
```

```
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 class-default
  fair-queue
  random-detect
policy-map Shaper-wireless
description (real is wireless-Platinum) assume 256kbps up
 class class-default
  shape average 256000 2560 0
  service-policy V3PN-teleworker
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set REPLAY esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto map RTP 1 ipsec-isakmp
 description RTP Enterprise Class Teleworker
 set peer xx.xxx.223.24
 set peer xx.xxx.223.25# A Second peer could be defined
 set security-association lifetime seconds 14400
 set transform-set REPLAY
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
interface FastEthernet0
 description Outside
 bandwidth 256
 ip address dhcp
 ip access-group INPUT_ACL in
 ip access-group INPUT_ACL_out out
 ip nat outside
 ip virtual-reassembly
 service-policy output Shaper-wireless
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
 crypto map RTP
!
interface FastEthernet1
 description SPOUSECHILD-ONLY-VLAN2-ONLY
 switchport access vlan 2
 no ip address
 load-interval 30
!
interface FastEthernet2
 description CORPUSER-ONLY-VLAN1-ONLY
 no ip address
 load-interval 30
!
interface FastEthernet3
 description CORPUSER-ONLY-VLAN1-ONLY
 no ip address
 load-interval 30
```

```
!
interface FastEthernet4
 description TO-AP-VLAN1or2 based off of AP login
 switchport mode trunk
 no ip address
 load-interval 30
 vlan-range dot1q 1 2
  description this port can be VLAN 1 or 2
  exit-vlan-config
 !
!
!  Inside Interface ip tcp adjust-mss 542 was not defined
!
interface Vlan1
 description Inside
 ip address 10.81.7.169 255.255.255.248
 ip inspect CBAC in
 load-interval 30
!
!
!
!  This address space will be NAT/pNAT'ed and is unencrypted to the Internet
!
interface Vlan2
 description SpouseChild lanside
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip inspect CBAC in
 ip virtual-reassembly
 load-interval 30
!
!
interface Async1
 no ip address
 shutdown
!
ip classless
!
!  This address 172.30.30.128 is the DHCP server on the MODEM
!
ip route 172.30.30.128 255.255.255.255 FastEthernet0 65.76.244.213
!
ip nat inside source list pNAT_ACL interface FastEthernet0 overload
!
!
ip access-list extended CRYPTO_MAP_ACL
 permit ip 10.81.7.168 0.0.0.7 any
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
ip access-list extended INPUT_ACL
 remark Allow IKE and ESP from the RTP headends
 permit udp xx.xxx.223.16 0.0.0.15 any eq isakmp
 permit udp xx.xxx.223.16 0.0.0.15 eq isakmp any
 permit esp xx.xxx.223.16 0.0.0.15 any
 remark double ACL check not applicable in this IOS version
 permit udp any any eq bootpc
 remark NTP ACLs
 permit udp 192.5.41.40 0.0.0.1 eq ntp any
 permit udp host 216.210.169.40 eq ntp any
 remark SSH from RTP Ridge
 permit tcp xx.xxx.87.0 0.0.0.255 any eq 22
 permit icmp any any
 deny   ip any any
ip access-list extended INPUT_ACL_out
```

```
 permit esp any any
 permit ip any any
ip access-list extended pNAT_ACL
 permit ip 192.168.1.0 0.0.0.255 any
logging source-interface Vlan1
!
rtr responder
!
ntp server 192.5.41.41
ntp server 192.5.41.40
ntp server 216.210.169.40
ntp server 10.81.254.202 source Vlan1
end
```

EZPVN Head-end Server

The configuration for the EZVPN head-end server is as follows:

```
!
version 12.3
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname rtp5-esevpn-gw3
!
boot-start-marker
boot system disk0:c7200-ik9o3s-mz.123-4.T3
boot-end-marker
!
logging queue-limit 100
logging buffered 100000 debugging
enable secret 5 xxxx
!
username vpn-jk2-1711-1 secret 5 [must_match_PW_in_remote]
clock timezone est -5
clock summer-time edt recurring
aaa new-model
!
!
aaa authentication login default group tacacs+ enable
aaa authentication login RTP_ezvpn_user local
aaa authentication ppp default if-needed group radius
aaa authorization network RTP_ezvpn_group local
aaa session-id common
ip subnet-zero
!
!
ip cef
ip domain name cisco.com
ip host harry.cisco.com 172.26.129.252
ip host rtp5-esevpn-ios-ca 10.81.0.27
ip name-server xx.xxx.6.247
!
!
crypto ca trustpoint rtp5-esevpn-ios-ca
 enrollment url http://rtp5-esevpn-ios-ca:80
 revocation-check crl
 auto-enroll 70
!
!
crypto ca certificate chain rtp5-esevpn-ios-ca
```

```
 certificate 21
 certificate ca 01
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
crypto isakmp client configuration address-pool local dynpool
crypto isakmp xauth timeout 60

!
crypto isakmp client configuration group EZVPN_Group
 key [must_match_Group_in_remote]
 dns xx.xxx.6.247 171.68.226.120
 domain cisco.com
 pool dynpool
 save-password
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
!
crypto dynamic-map DYNOMAP 10
 set transform-set 3DES_SHA_TUNNEL
 reverse-route
!
!
crypto map EZmap local-address Loopback0
crypto map EZmap client authentication list RTP_ezvpn_user
crypto map EZmap isakmp authorization list RTP_ezvpn_group
crypto map EZmap client configuration address respond
crypto map EZmap 10 ipsec-isakmp dynamic DYNOMAP
!
!
!
controller ISA 2/1
!
!
!
interface Loopback0
 description Public address
 ip address xx.xxx.223.23 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet1/0
 description Private
 ip address 10.81.0.23 255.255.255.240
 ip access-group DoS_Input_Queue_Wedge in
 ip route-cache same-interface
 ip route-cache flow
 duplex full
 speed 100
 standby 1 ip 10.81.0.20
 standby 1 priority 90# This router has the least favorable priority.
 standby 1 preempt
 standby 1 authentication eSeVpN
 crypto map EZmap
!
interface FastEthernet1/1
```

```
 description VLAN 101 RTP5-ALPHA-GW1
 ip address 192.168.82.23 255.255.255.0
 ip route-cache flow
 duplex full
 speed 100
!
interface Virtual-Template1
 no ip address
 ppp authentication chap callin
!
router eigrp 64
 redistribute static metric 1000 100 255 1 1500 route-map RRI
 network 192.168.82.0
 no auto-summary
 no eigrp log-neighbor-warnings
!
ip local pool dynpool 10.81.7.241 10.81.7.246
ip classless
ip route 0.0.0.0 0.0.0.0 10.81.0.17
no ip http server
no ip http secure-server
!
!
!
ip access-list extended DoS_Input_Queue_Wedge
 remark http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml
 deny   53 any any
 deny   55 any any
 deny   77 any any
 deny   pim any any
 permit ip any any
ip radius source-interface Loopback0
access-list 1 permit 10.81.7.0 0.0.0.255
access-list 1 deny   any
access-list 1 remark Home user address pool(s)
snmp-server location Creeksize RTP building 5
snmp-server contact cisco789@cisco.com 919-123-4567
snmp-server enable traps tty
!
route-map RRI permit 10
 description Redistribute remote subnets from RRI
 match ip address 1
!
!   # some config items removed
!
end
```

Primary IPSec Head-end

The following is an abbreviated configuration of the primary IPSec head-end router:

```
version 12.3
!
hostname rtp5-esevpn-gw4
!
boot-start-marker
!   System image file is "flash:c3725-adventerprisek9-mz.123-7.11.T"
boot-end-marker
!
ip cef
!
```

```
crypto pki trustpoint rtp5-esevpn-ios-ca
 enrollment url http://rtp5-esevpn-ios-ca:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain rtp5-esevpn-ios-ca
 certificate 15
 certificate ca 01
!
!
!
crypto isakmp policy 10
 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 RTP_DYNO 10
 set security-association lifetime seconds 28800
 set transform-set 3DES_SHA_TUNNEL
 reverse-route
 qos pre-classify
!
!
crypto map RTP local-address Loopback0
crypto map RTP 1 ipsec-isakmp dynamic RTP_DYNO
!
interface Loopback0
 description Public address
 ip address xx.xxx.223.24 255.255.255.255
!
interface FastEthernet0/0
 description VLAN 100 RTP5-Alpha-GW1
 ip address 10.81.0.24 255.255.255.240
 ip access-group DoS_Input_Queue_Wedge in
 no ip redirects
 ip route-cache same-interface
 ip route-cache flow
 load-interval 30
 speed 100
 full-duplex
 standby 1 ip 10.81.0.20
 standby 1 priority 110       # This is the highest or most favored of the three
 standby 1 preempt
 standby 1 authentication eSeVpN
 crypto map RTP
!
interface FastEthernet0/1
 description VLAN 101 RTP5-Alpha-GW1
 ip address 192.168.82.24 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 64
 redistribute static metric 1000 100 255 1 1500 route-map RRI
 network 192.168.82.0
 no auto-summary
 no eigrp log-neighbor-warnings
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.81.0.17
ip route 10.81.7.0 255.255.255.0 Null0
access-list 1 permit 10.81.7.0 0.0.0.255
access-list 1 deny   any log
!
route-map RRI permit 10
 description Redistribute remote subnets from RRI
 match ip address 1
!

end
```

Secondary IPSec Head-end

The following is an abbreviated configuration of the secondary IPSec head-end router:

```
!
hostname rtp5-esevpn-gw5
!
boot-start-marker
boot system flash c3725-advsecurityk9-mz.123-7.11.T
boot-end-marker
!
ip cef
!
!
crypto pki trustpoint rtp5-esevpn-ios-ca
 enrollment url http://rtp5-esevpn-ios-ca:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain rtp5-esevpn-ios-ca
 certificate 04
 certificate ca 01
!
crypto isakmp policy 10
 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 RTP_DYNO 10
 set security-association lifetime seconds 28800
 set transform-set 3DES_SHA_TUNNEL
 reverse-route
 qos pre-classify
!
!
crypto map RTP local-address Loopback0
crypto map RTP 1 ipsec-isakmp dynamic RTP_DYNO
!
!
```

```
interface Loopback0
 description Public address
 ip address xx.xxx.223.25 255.255.255.255
!
interface FastEthernet0/0
 description Private
 ip address 10.81.0.25 255.255.255.240
 ip access-group DoS_Input_Queue_Wedge in
 no ip redirects
 service-policy input INGRESS_POLICY
 ip route-cache same-interface
 ip route-cache flow
 load-interval 30
 speed 100
 full-duplex
 standby 1 ip 10.81.0.20
 standby 1 preempt # Default HSRP priority is 100
 standby 1 authentication eSeVpN
 crypto map RTP
!
interface FastEthernet0/1
 description VLAN 101 RTP5-Alpha-GW1
 ip address 192.168.82.25 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 64
 redistribute static metric 1000 100 255 1 1500 route-map RRI
 network 192.168.82.0
 no auto-summary
 no eigrp log-neighbor-warnings
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.81.0.17
ip route 10.81.7.0 255.255.255.0 Null0
!
access-list 1 permit 10.81.7.0 0.0.0.255
access-list 1 deny   any log
!
route-map RRI permit 10
 description Redistribute remote subnets from RRI
 match ip address 1
!
end
```

Cisco IOS Versions Tested

The following Cisco IOS versions were used in testing:

- vpn-jk2-1711-1—c1700-k9o3sy7-mz.123-2.XF (see Caveats, page 7-29, regarding CSCef87216 (multi-WAN)
- steve-vpn-1711—c1700-k9o3sy7-mz.123-8.T3 (single WAN)
- DSL router—c837-k9o3sy6-mz.123-4.T3
- rtp5-esevpn-gw3—c7200-ik9o3s-mz.123-4.T3
- rtp5-esevpn-gw4—c3725-adventerprisek9-mz.123-7.11.T
- rtp5-esevpn-gw5—c3725-adventerprisek9-mz.123-7.11.T

Caveats

Cisco no longer supports the use, or need for, LAN Access Mobility (LAM), and it was not used in these configurations and tests with the wireless modem.

This section describes the issues encountered during testing, and includes the following sections:

- EZVPN
- DHCP Server

EZVPN

Initially, Cisco IOS version 12.3(8)T4 was installed on the Cisco 1711 router, but because of a software issue, an IKE policy could not be present in the router configuration if EZVPN was also being used as an authentication method.DDTS CSCef87216 was filed accordingly. Cisco IOS version 12.3(2)XF did not exhibit this issue.

DHCP Server

The wireless broadband modem provides a local DHCP server to supply an IP address to the host or router attached. Although the IP address provided for the default gateway and the DHCP client is an Internet routable address, (in this example 65.76.244.214), the IP address of the DHCP server is not. The address of the DHCP server is always 172.30.30.128, as shown in the following display.

```
vpn-jk2-1711-1#show dhcp lease
Temp IP addr: 65.76.244.214  for peer on Interface: FastEthernet0
Temp  sub net mask: 255.0.0.0
   DHCP Lease server: 172.30.30.128, state: 3 Bound
   DHCP transaction id: 2324
   Lease: 60 secs,  Renewal: 30 secs,  Rebind: 52 secs
Temp default-gateway addr: 65.76.244.213
   Next timer fires after: 00:00:27
   Retry count: 0   Client-ID: cisco-000d.bd64.8aa4-Fa0
   Client-ID hex dump: 636973636F2D303030642E626436342E
                       386161342D466130
   Hostname: vpn-jk2-1711-1
```

On a multi-WAN configuration, for the router to use the correct interface to reach the DHCP server address, a static host route is required as shown:

```
ip route  172.30.30.128 255.255.255.255 FastEthernet0 dhcp
```

```
vpn-jk2-1711-1#show ip route 172.30.30.128
Routing entry for 172.30.30.128/32
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 65.76.244.213
      Route metric is 0, traffic share count is 1
```

The assigned address has a short lease time of 60 seconds, meaning that the router or PC must request a renewal every 30 seconds, as shown in the following debug.

```
vpn-jk2-1711-1#debug dhcp
```

```
DHCP client activity debugging is on
vpn-jk2-1711-1#
Oct  1 14:19:56.762 edt: DHCP: SRequest attempt # 1 for entry:
Oct  1 14:19:56.762 edt: DHCP: SRequest - ciaddr: 65.76.244.214
Oct  1 14:19:56.762 edt: DHCP: SRequest placed lease len option: 60
Oct  1 14:19:56.762 edt: DHCP: SRequest: 307 bytes
Oct  1 14:19:56.762 edt: DHCP: SRequest: 307 bytes
Oct  1 14:19:56.766 edt: DHCP: Received a BOOTREP pkt
Oct  1 14:19:56.766 edt: DHCP Client Pooling: ***Allocated IP address: 65.76.244.214
------- every thirty seconds -------------------
Oct  1 14:20:26.766 edt: DHCP: SRequest attempt # 1 for entry:
Oct  1 14:20:26.766 edt: DHCP: SRequest - ciaddr: 65.76.244.214
Oct  1 14:20:26.766 edt: DHCP: SRequest placed lease len option: 60
Oct  1 14:20:26.766 edt: DHCP: SRequest: 307 bytes
Oct  1 14:20:26.766 edt: DHCP: SRequest: 307 bytes
Oct  1 14:20:26.770 edt: DHCP: Received a BOOTREP pkt
Oct  1 14:20:26.770 edt: DHCP Client Pooling: ***Allocated IP address: 65.76.244.214
```

Without the host route to the DHCP lease server, the DHCP request follows the default route to the DSL link. Because the address is an RFC 1918 address, it is not routed over the Internet. The end result is that the DHCP lease is not renewed and the router outside interface flaps continuously.

Summary

Wireless broadband is best suited for its target market of providing mobility to a single PC with either an external or PCMCIA modem. This chapter focused on using an external modem with an attached router. Likely deployment situations are small offices seeking rapid deployment of equipment or multiple WAN interfaces for availability. Voice was also tested to determine the viability of deployments for teleworkers. If sufficient signal strength and quality are available and interference because of environmental or terrain is not an issue, voice quality ranges from good to very good. However, like all wireless media, consistency and availability are often an issue.

CHAPTER 8

Small Branch—Dual Hub/Dual DMVPN

This chapter describes the migration of a single Dynamic Multipoint Virtual Private Network (DMVPN) configuration, which is a router with a single DMVPN configuration connected to one DMVPN hub, with one configured generic routing encapsulation (GRE) tunnel, to a dual DMVPN configuration supporting VoIP.

Note This is a hub-and-spoke deployment; spoke-to-spoke was not tested or rrecommended for VoIP.

The dual hub/dual DMVPN design provides head-end redundancy by configuring two DMVPN clouds on a remote router, with each cloud having a separate IPSec head-end router.

This chapter describes the changes that result from adding VoIP to configuration examples that initially support only data.

Note IP telephony is supported only on a best effort basis, so the configurations that include VoIP are not complete.

This chapter includes the following sections:

- Solution Characteristics
- Topology
- Failover/Recovery Time
- V3PN QoS Service Policy
- Performance Testing
- Test Topology
- Implementation and Configuration
- Cisco IOS Versions Tested
- Summary

Solution Characteristics

This design solution applies in situations where customers require VoIP, and IP multicast applications are supported. The final configuration represents a dual hub and dual DMVPN clouds supporting a VoIP deployment.

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

- Low recurring costs for WAN access
- IP multicast requirements
- VoIP support
- Redundant IPSec/GRE termination at the campus head-end

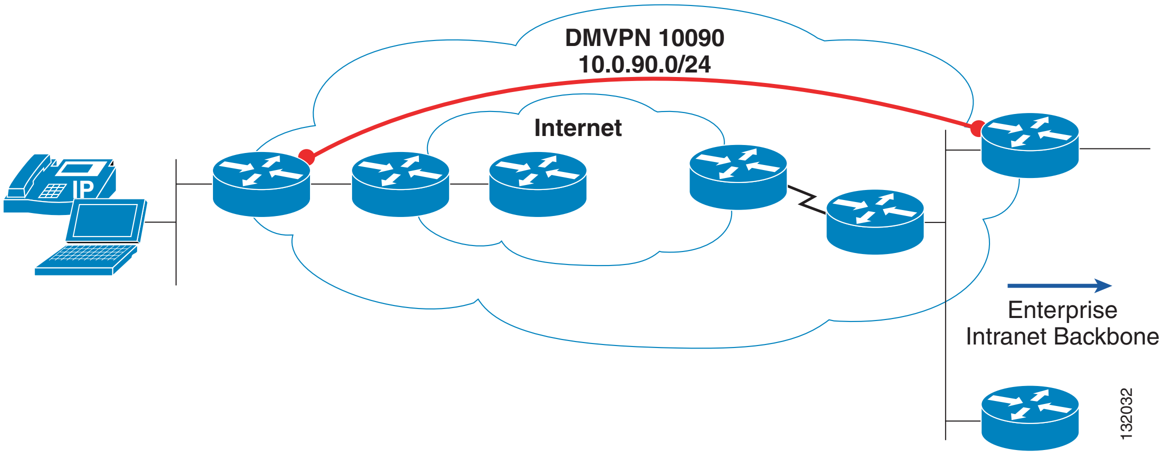
Test results are presented to describe voice quality with and without the recommended changes implemented to enhance the initial configuration of the customer.

This chapter also describes a case study in which the initial customer configuration in tested to validate support for VoIP.

Topology

The initial customer configuration consists of a single DMVPN cloud with a single campus head-end router providing connectivity for the population of teleworkers. This topology is shown in Figure 8-1.

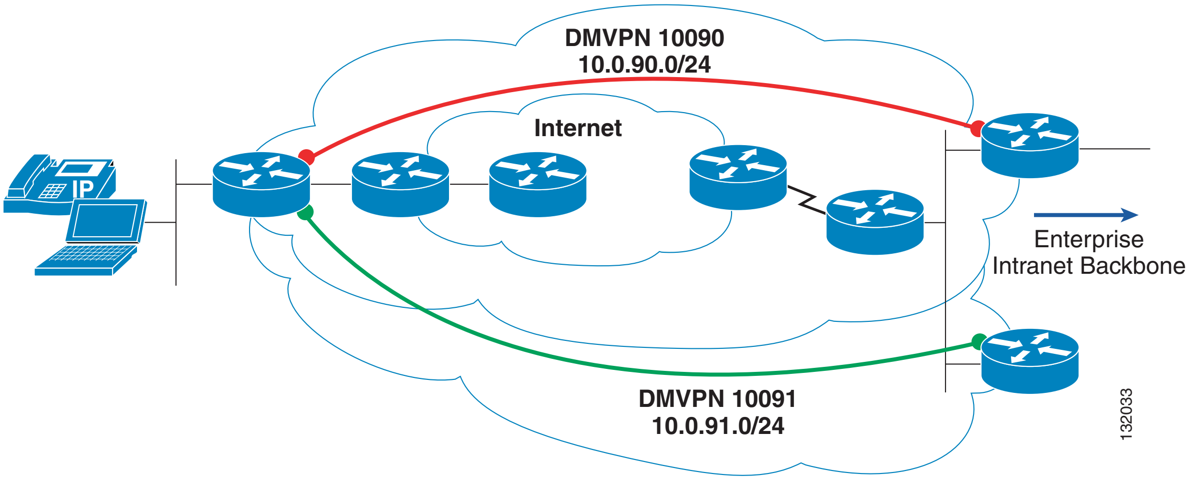
Figure 8-1 Single Hub—Single DMVPN



Because the customer configuration must now support VoIP, a second DMVPN cloud is needed to increase availability for the remote locations. The dual hub/dual DMVPN cloud design is selected over a dual hub/single DMVPN cloud because the topology provides more control of the packet routing between the two head-end peers.

The recommended topology is shown in Figure 8-2:

Figure 8-2 Dual Hub/Dual DMVPN



The dual hub/dual DMVPN topology has the advantage of providing two tunnel interfaces in the remote branch (teleworker) routers. Because the remote routers, or spokes, have a routing protocol neighbor relationship on two separate interfaces, the two paths can be influenced by interface specific values. Depending on the routing protocol in use, you can implement cost, bandwidth, delay, metric offset, or summary advertisements on the individual tunnel interfaces to influence which head-end router is the preferred path. From a manual load sharing perspective, half the population of spoke routers can use DMVPN cloud 10090 as their preferred path with cloud 10091 as the backup. The other half of the spokes can use cloud 10091 as the preferred path and cloud 10090 as backup.

With a distance vector routing protocol such as EIGRP, it is very easy to add a third DMVPN cloud, and to divide the population of spoke routers so that one third prefers the first cloud, one third prefers the second, and the final one third prefers the last cloud. The backup cloud for the spoke is spread across the other clouds and their respective head-end routers.

Failover/Recovery Time

When EIGRP is the routing protocol on the mGRE tunnels, detection of a head-end or path failure by the remote router is based on the configured routing protocol dead interval (interface configuration command **ip hold-time eigrp …**), which by default is 15 seconds. Other protocols, such as RIP, OSPF, and so on, have their own default values and can be configured by the network manager.

One currently-known issue with dual hub/dual DMVPN cloud configurations is that the second Internet Key Exchange (IKE) security association (SA) may be deleted. If the peer associated with the UP-NO-IKE status is reloaded, connectivity is not restored until the IPSec SAs age out, because there is no IKE SA to send keepalive/dead peer detection (DPD) messages.

As a result of this, the second IKE SA must re-key each time the IPSec SA expires. By default, the IKE lifetime is 24 hours and the IPSec lifetime is one hour. From a head-end performance standpoint (CPU consumption), that means 24 times more IKE processing than necessary.For more information on the problem and for a status update or resolution, please refer to CSCeg18278. This defect is identified as CSCed18278-IKE SSA delected in dual hub, dual DMVPN cloud configuration.

V3PN QoS Service Policy

This section includes the following topics:

- DMVPN (GRE Transport Mode) ESP 3DES/SHA
- DMVPN (GRE Transport Mode) ESP 3DES/SHA with NAT-T
- Sample V3PN Relevant QoS Configuration

In various V3PN design guides, QoS service policies are defined to allocate bandwidth based on IPSec-protected GRE and direct IPSec encapsulation respectively.

Note For more information, see the V3PN design guide at the following URL: http://www.cisco.com/en/US/netsol/ns340/ns394/ns430/networking_solutions_package.html

IPSec-protected GRE tunnels are commonly deployed for site-to-site communications, and direct IPSec encapsulation is well-suited for teleworkers.

Note IPSec encapsulation is also known as an IPSec-only deployment (no GRE). Teleworker deployments generally do not need multicast or multiprotocol support and thus do not reap any benefit from GRE encapsulation and its additional overhead.

DMVPN has been heavily marketed to customers, and it is one option for deployments that require IP multicast applications to the teleworker desktop (DMVPN does not support multiprotocol but only IP multicast). Examples of these deployments include video surveillance applications using IP multicast and financial brokerage house applications that are implemented using IP multicast.

In a small office small home (SOHO) deployment, it is common to see the VPN router deployed behind a personal firewall such as a Linksys BEFSR41 EtherFast® Cable/DSL Router. This architecture is deployed at the residence of the teleworker because it allows the teleworker to control the username and password of the PPP over Ethernet (PPPoE) session, simplifies configuration of the enterprise-managed VPN router, and provides a "spouse and child" network over the common broadband connection.

The deployment scenario assumes the following:

- The topology may include a Network Address Translation (NAT)/Port Network Address Translation (pNAT) personal firewall device.
- Both cable and DSL broadband are supported.
- PPPoE is typical on the DSL deployments, and Data Over Cable Service Interface Specifications (DOCSIS) 1.0 is typical for cable.
- The uplink data rates are at or below 768 kbps and as such, voice packets are subject to serialization delay.

Because of these factors, the configuration is optimized for the worst case scenario, which is DSL using PPPoE at an uplink data rate below 768 kbps. The **ip tcp adjust-mss** command is used to minimize the lack of Layer 2 link fragmentation and interleaving.

The goal is to select an optimum value for **ip tcp adjust-mss** that minimizes both the IPSec padding and ATM adaption layer (AAL) 5 padding. The diagrams in the following section show the individual field lengths and their relationship to the underlying ATM cells on a DSL deployment.

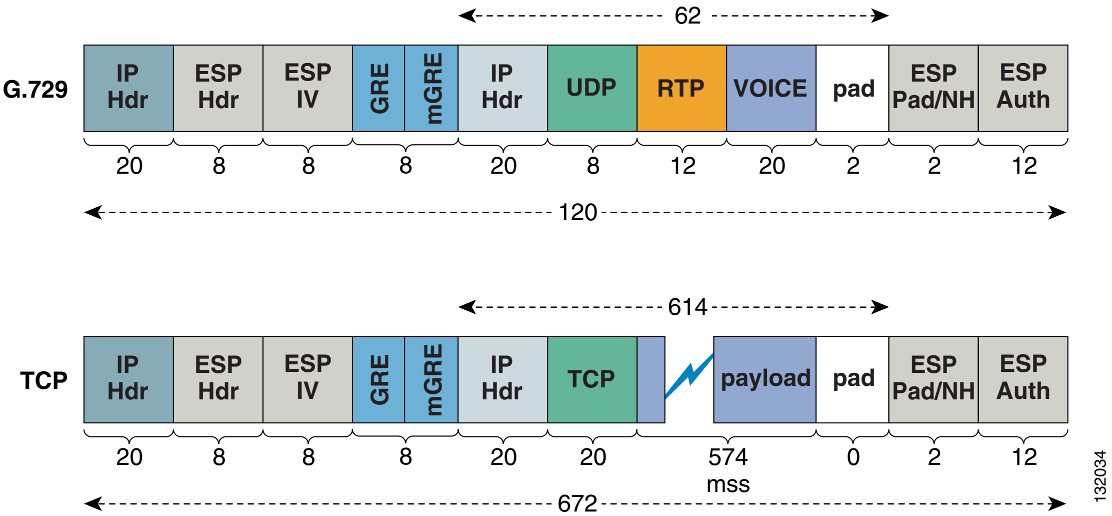
DMVPN (GRE Transport Mode) ESP 3DES/SHA

The following configuration uses a transform set that includes Triple Data Encryption Standard (3DES), Secure Hash Algorithm (SHA), and transport mode for multipoint GRE (mGRE):

```
crypto ipsec transform-set TRANSPORT_3DES_SHA esp-3des esp-sha-hmac
 mode transport
crypto ipsec profile ECT_PROFILE_1
 …
 set transform-set TRANSPORT_3DES_SHA
!
interface Tunnel0
 description DMVPN
 …
 tunnel mode gre multipoint
 …
 tunnel protection ipsec profile ECT_PROFILE_1 shared
```

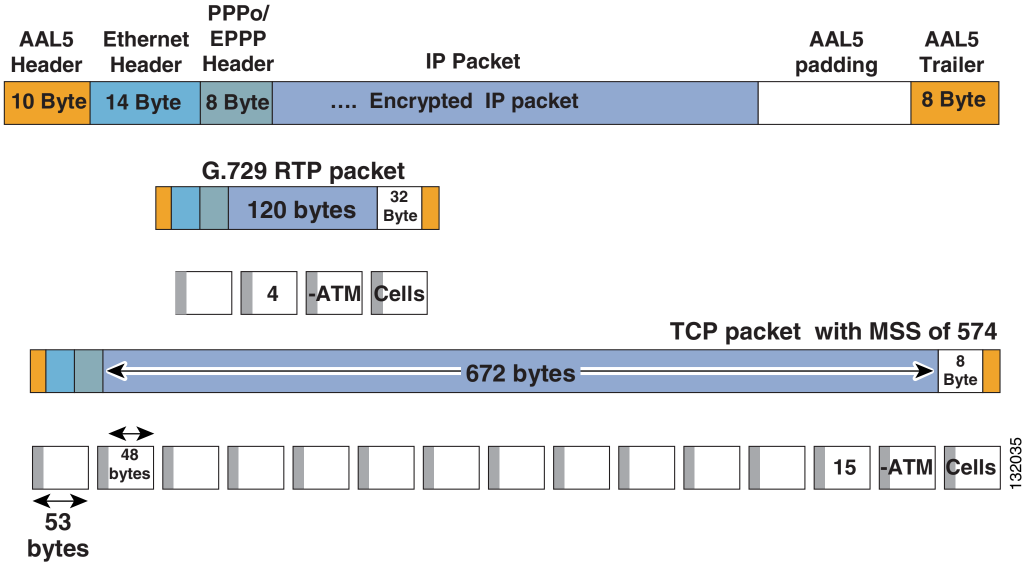
The encrypted mGRE encapsulated packets for both G.729 and a TCP packet are shown in Figure 8-3.

Figure 8-3 Packet Decode—G.729 and TCP



This encrypted IP packet, when encapsulated in PPPoE/AAL5/ATM cells for a DSL deployment, is shown in Figure 8-4.

Figure 8-4 DSL/PPPoE Encapsulation



The result is that a G.729 packet requires four ATM cells, and a TCP packet with a maximum segment size (MSS) of 574 requires 15 ATM cells. There are 8 bytes of AAL5 padding in the last cell. This configuration does not assume Network Address Translation Traversal (NAT-T), but rather the IP header is Extended Services Platform (ESP), protocol "50". NAT-T is optimized so that when no NAT device is detected between the IPSec peers, UDP encapsulation is not used to avoid the additional overhead of the additional UDP header. This configuration shows IKE packets on UDP port 500 and ESP (protocol 50) for the IPSec tunnel.

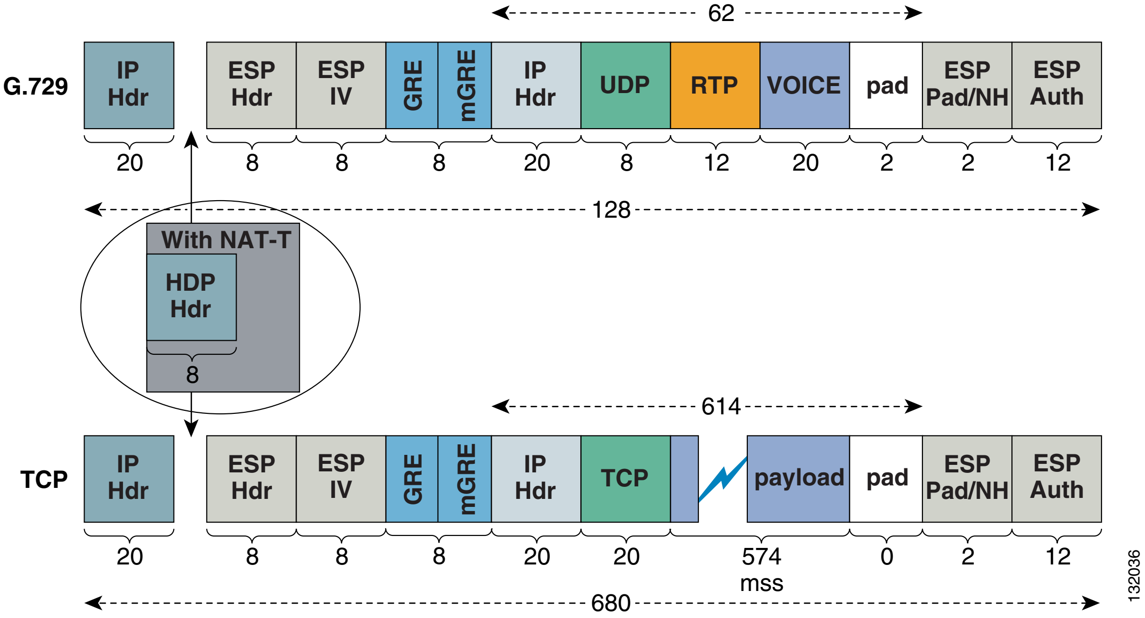
DMVPN (GRE Transport Mode) ESP 3DES/SHA with NAT-T

Based on a configuration using a transform set that includes 3DES, SHA, and transport mode for mGRE using the same configuration from the previous section, assume that a NAT/pNAT device is in the path between the IPSec peers and NAT-T is enabled.

```
crypto ipsec nat-transparency udp-encapsulation
```

The above Cisco IOS configuration command is enabled by default. The encrypted mGRE encapsulated packets for both G.729 and a TCP packet are shown in Figure 8-5.

Figure 8-5 Packet Decode—G.729 and TCP with NAT-T

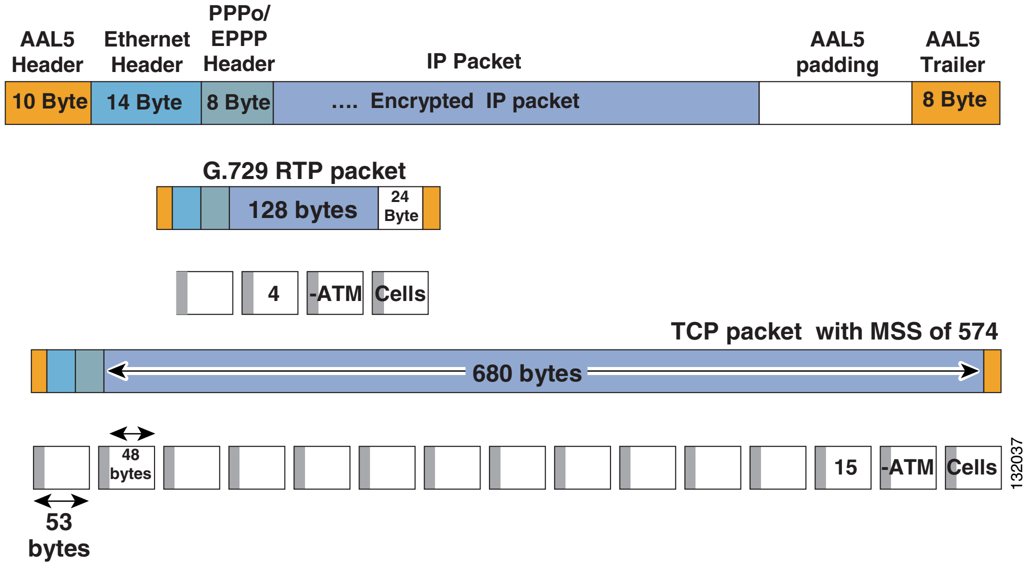


In this example, the TCP packets have a padding of 0 for IPSec. The IP header is UDP with source and destination port 4500. The NAT/pNAT device may change the IP address and port number. Using the **show crypto ipsec sa detail | inc peer** command on the head-end router shows the source port and IP address derived from NAT-T.

Note Because both IKE and ESP packets share the same UDP port number (4500), IKE packets have a Non-ESP marker field consisting of 4 bytes zero filled that aligns with the Service Provider Interface (SPI) field of an ESP packet. Because the SPI cannot be all zeros, this enable the receiver to distinguish between an ESP and IKE packet. As such, the additional overhead of NAT-T is the 8 byte UDP header for ESP packets, and 12 bytes for IKE packets (8 bytes for the UDP header and an additional 4 bytes for the non-ESP Marker).There is also an additional packet, a NAT-keepalive packet, which is a UDP packet, port number 4500, with a single byte field with a value of 0xFF. The receiver ignores these packets; however, they serve to keep the NAT/pNAT device translation table fresh.

These encrypted IP packets, when encapsulated in PPPoE/AAL5/ATM cells for a DSL deployment, are shown in Figure 8-6.

Figure 8-6 DSL/PPPoE Encapsulation with NAT-T



The result is a G.729 packet that requires four ATM cells, and a TCP packet with an MSS of 574 that requires 15 ATM cells. There are zero bytes AAL5 padding in the last cell. The TCP MSS value of 574 is used so that with or without NAT-T negotiated, the TCP packets always require 15 ATM cells. This simplifies the task by generalizing the configuration of the remote router.

Sample V3PN Relevant QoS Configuration

Based on the previous analysis of the customer configuration, this section shows recommended changes to optimize and enhance the configuration.

TCP Maximum Segment Size

Given the previous analysis of the fields in the unencrypted payloads and resulting encryptions and encapsulations, using a TCP MSS size override of 574 on the inside Ethernet and GRE tunnel interface is used in the following configuration:

```
!
interface Ethernet0
 ip address 10.0.94.1 255.255.255.0
 ip route-cache flow
 ip tcp adjust-mss 574
!
interface Tunnel0
 description DMVPN
 ip address 10.0.90.12 255.255.255.0
 …
 ip route-cache flow
 ip tcp adjust-mss 574
```

Note Performance results with this change and the other recommended changes are shown in a subsequent section.

IP MTU of Tunnel interfaces

The customer configuration includes a manually configured tunnel IP maximum transmission unit (MTU) with a value of 1408, as shown:

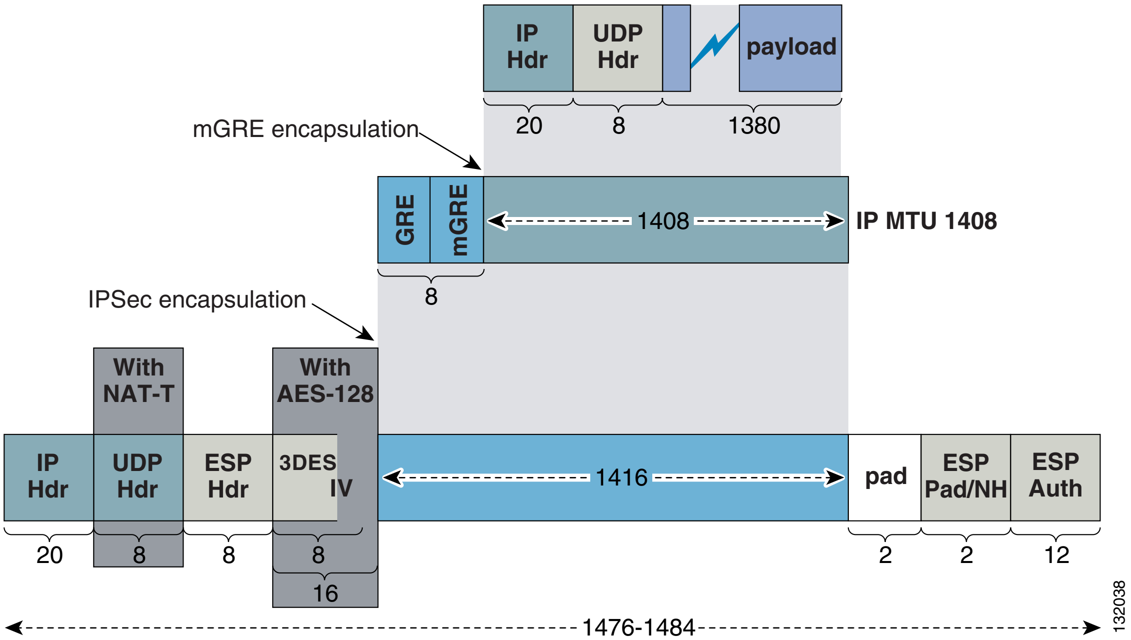
```
interface Tunnel0
…
 ip mtu 1408
```

1408 is an optimal IP MTU value for deployments, whether or not they include PPPoE, NAT-T, 3DES, or Advanced Encryption Standard (AES)-128. In the previous section, the remote router adjusts the MSS value for TCP sessions to and from the remote site. Although this eliminates any fragmentation issues for the majority of the data traffic, there still might be UDP applications that generate some MTU-sized packets. Ideally, these should be fragmented by the router before encryption.

Changing the IP MTU of the tunnel interface effectively forces fragmentation before encryption. Fragmenting after encryption means that the decrypting router must reassemble the fragments before they can be decrypted. This requirement means that the decrypting router must process switch the fragmented packets and allocate a huge buffer in memory to assemble the fragments, which negatively impacts performance, especially if the decrypting router is the head-end crypto aggregation point that decrypts for multiple remote or spoke routers. Fragmenting before encryption forces the receiving workstation to re-assemble the fragments instead.

Given a tunnel interface with an IP MTU of 1408, the largest UDP packet that can be encapsulated without fragmentation is 1380 bytes of payload plus 28 bytes for IP and UDP headers. This encapsulation process is shown in Figure 8-7.

Figure 8-7 mGRE and IPSec Encapsulation



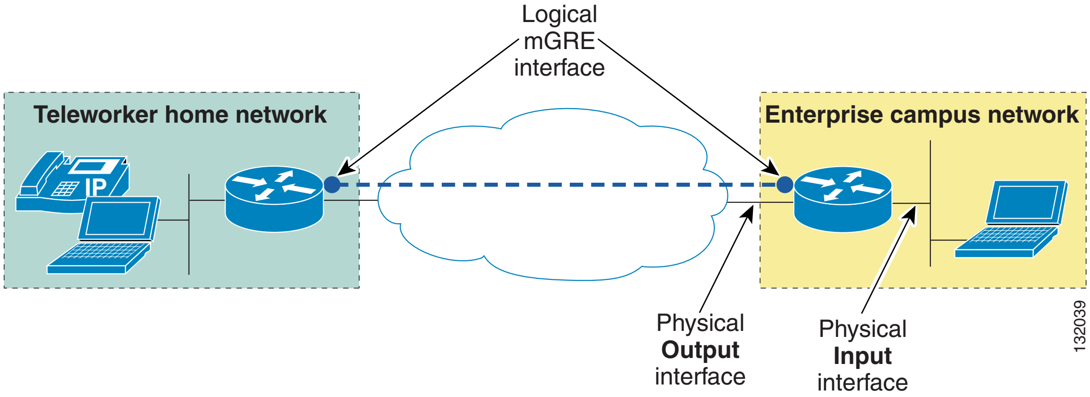
With PPPoE (commonly used with residential DSL offerings), a maximum encrypted packet size of 1492 is preferred because PPPoE includes an 8-byte header.

Note Ethernet has a maximum payload size of 1500 octets. The PPPoE header is six octets and the PPP protocol ID is two octets, so the PPP MTU must not be greater than 1492. For more information, see RFC 2516 at the following URL: http://www.rfc-archive.org/getrfc.php?rfc=2516.

AES-128 has a 16-byte initialization vector (IV) as compared to 8 bytes for 3DES. If the remote router is behind a personal firewall, an additional UDP header is also present. The size of the ESP pad varies depending on the payload size being encrypted and whether the encryption algorithm is 3DES or AES.

There are some rules for identifying fragmentation and determining whether it is pre- or post-encryption. The topology in Figure 8-8 is shown as a reference:

Figure 8-8 Fragmentation Illustration



Assume that the workstation in the enterprise campus network is generating packets to the remote teleworker home network at a constant rate with no other traffic present.

Note A test tool or application that can be configured to generate a UDP packet at a configured size and at a constant rate in packets per second is useful for this illustration.

Fragmentation can be identified by observations on the head-end router.

- Pre-encryption fragmentation—Fragmentation because of the MTU of the mGRE tunnel interface
  - **show ip traffic | include fragmented** shows a steadily increasing counter.
  - **show interface tunnel[n] | include rate** shows an input rate twice the number of packets per second being sent by the workstation.
- Post-encryption fragmentation—Fragmentation because of the MTU of the output interface
  - **show interface tunnel[n] | include rate** shows an input rate equal to the sending rate of the workstation.
  - **show interface [output interface] | include rate** shows an output rate twice the number of packets per second as shown on the tunnel interface.

Thus, given the variety of topologies encountered in the typical teleworker deployment scenarios, the customer choice of IP MTU for the mGRE tunnel interfaces is a good choice.

Class-map Configuration

In this case study, the customer has configured match statements in the class map that were not relevant and redundant. As a best practice, these extraneous entries should be removed.

For example, the initial customer configuration is as follows:

```
class-map match-any ISC_OUT_Cisco-IT_voice_call-setup
 match ip dscp af31
 match ip dscp af32
 match ip dscp cs3
 match ip precedence 3
class-map match-any ISC_OUT_Cisco-IT_voice_voice
 match ip dscp ef
 match ip dscp cs5
 match ip precedence 5
```

Matching on Differentiated Services Code Point (DSCP) value of CS5 and also on IP Precedence of “5” is redundant.

Note Section 4.2 of RFC 2474 describes the use of CS (Class Selector) codepoints to provide backward compatibility matching of IP Precedence values. See RFC 2474 at the following URL: http://www.rfc-archive.org/getrfc.php?rfc=2474

For example, see the following configuration, given this sample class map and an IP phone generating packets for call setup with DSCP value of CS3 or IP Precedence 3:

```
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
  match ip precedence 3

R1#show pol int e 0/0 output | beg CALL-SETUP
        Class-map: CALL-SETUP (match-any)
          5 packets, 306 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af31
            0 packets, 0 bytes
            30 second rate 0 bps
          Match: ip dscp cs3
            5 packets, 306 bytes
            30 second rate 0 bps
          Match: ip precedence 3
            0 packets, 0 bytes
            30 second rate 0 bps
```

From the above display, observe that no packets are matching IP Precedence 3, but rather DSCP value of CS3. The following displays shows the order reversed in the class map:

```
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip precedence 3
  match ip dscp cs3


R1#show pol int e 0/0 output | beg CALL-SETUP
        Class-map: CALL-SETUP (match-any)
          32 packets, 2068 bytes
```

```
30 second offered rate 0 bps, drop rate 0 bps
Match: ip dscp af31
  0 packets, 0 bytes
  30 second rate 0 bps
Match: ip precedence 3
  32 packets, 2068 bytes
  30 second rate 0 bps
Match: ip dscp cs3
  0 packets, 0 bytes
  30 second rate 0 bps
```

In the above configuration, there are no matches on the DSCP value of CS3, but rather the match for IP Precedence 3 selects the packets.

Additionally, the customer call-setup class contains a match for AF32. Because the target configuration is for a remote router supporting an IP phone, there is no expectation that AF32 packets will ever be seen at this point in the topology. The DSCP value of AF32 is generally seen only if the traffic is out of contract and was remarked from AF31 to AF32 by a router.

Note According to RFC 2597 ("Assured Forwarding PHB Group"), AF31 has a lower drop probability than AF32 and the act of remarking from AF31 to AF32 is an indication of congestion within the per-hop behavior (PHB) group. See more information on RFC 2597 at the following URL: http://www.rfc-archive.org/getrfc.php?rfc=2597

Because this configuration is for the router that provides network access for the phone, and the phone either generates AF31 or CS3 for its call-setup traffic, no remarking is possible.

Assuming a Cisco IP phone, **match ip dscp cs5** can also be eliminated, because the firmware of the phone always generates DSCP values of EF for the voice media stream.

The proposed configuration can be reduced to the following:

```
class-map match-any ISC_OUT_Cisco-IT_voice_call-setup
  match ip dscp cs3
  match ip dscp af31


class-map match-all ISC_OUT_Cisco-IT_voice_voice
 match ip dscp ef
```

There now is only one entry for the voice class map, the **match-any** is changed to **match-all**, and the default value is for a one entry class-map.

Weighted fair-queue Configured on Ethernet Interfaces

The customer configuration included **fair-queue** on the outside Ethernet interface, as shown in the following:

```
interface Ethernet1
 description Provisioned by ISC (public interface)
 ip address dhcp
 ip access-group ISC_FIREWALL_outside_inbound_1 in
 service-policy output ISC_OUT_Cisco-IT_voice_TOP
 ip route-cache flow
 duplex auto
 fair-queue
```

It is extremely unlikely that the Ethernet interfaces on these routers will ever experience congestion. Weighted fair queueing (WFQ) is only recommended for interfaces clocked below 2 Mbps. In fact, Cisco 83x and 17xx routers are gated by CPU consumption before 10 Mbps Ethernet interfaces can be congested. The default of FIFO queueing on the Ethernet interfaces is recommended. To remove WFQ from the interface, enter **no fair-queue** while in interface configuration mode.

Service Assurance Agent (SAA) VoIP UDP Operation

The customer configuration includes an SAA VoIP UDP operation feature that was introduced in Cisco IOS Release 12.3(4) and includes Impairment/Calculated Impairment Planning Factor (ICPIF) and Mean Opinion Score (MOS) values. This feature is configured on the remote router configuration as follows:

```
rtr 10
 type jitter dest-ipaddr 10.86.252.2 dest-port 16384 codec g729a
 tag jitter-with-voice-scores
 frequency 180
rtr schedule 10 life forever start-time now
```

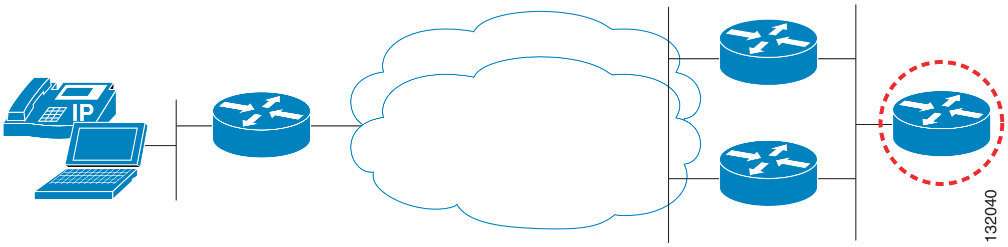
This is a very useful feature for diagnosing voice quality issues for a teleworker. However, some optimization is suggested to reduce the overhead and to optimize the data collection aspect.

Configuring SAA VoIP UDP at the Campus Head-end

The first recommendation is to remove the SAA VoIP UDP operation from the remote router, and instead either deploy a dedicated router or use an existing campus head-end router to initiate the probes. The remote router must then be configured only with **rtr responder** and does not need to be running a Cisco IOS release at or later than 12.3(4)T; only the head-end router has the code dependency for the introduction of the feature.

The campus head-end router shown circled in Figure 8-9 is assumed to have the recommended configuration described later in this section.

Figure 8-9 Campus Head-end SAA VoIP UDP Router



Reducing SAA Bandwidth Requirements

The default number of packets generated by the VoIP UDP operation (type jitter) is 1,000 with an interval of 20 ms between packets, or 50 packets per second. Thus, the default configuration generates 20 seconds worth of simulated voice traffic every 180 seconds or three minutes. Although the head-end router generates the packets initially, the remote router answers these packets on the return path. In the initial customer configuration, the type of service (ToS) byte of the packets of the probes was not set, and these simulated voice packets will be marked best effort, or ToS of 0. Because the goal is to measure the latency and jitter of the simulated voice stream assuming that it is representative of an actual voice call, it is preferred to mark the simulated packets with the same ToS value as an actual voice call.

For this reason, the number of packets are reduced to a more manageable value of 20 packets (**codec-numpackets 20**). The probe runs every 300 seconds or five minutes and marks the simulated voice stream with a ToS of decimal 184 (hex B8) or DSCP EF as would be the case with a real voice stream. The priority or Low Latency Queueing (LLQ) is adjusted to accommodate this additional traffic.

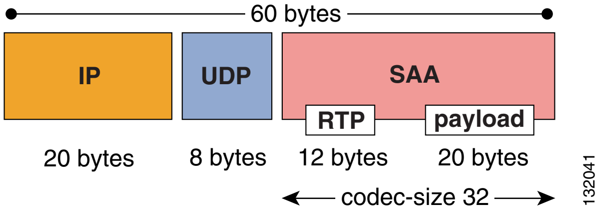
Recommended Probe Configuration

The implemented configuration is as follows:

```
rtr 10
 type jitter dest-ipaddr 10.0.94.1 dest-port 16384 codec g729a codec-numpackets 20
codec-size 32
 tos 184
 timeout 200
 tag JITTER_10.0.94.0
 frequency 300
!
```

The **codec-size** value of 32 is the default value and does not show in the running configuration. It is included here to illustrate that the codec size would be the sum of the RTP header plus the payload, or voice sample. Figure 8-10 shows the fields of the SAA-generated packet:

Figure 8-10 SAA VoIP Codec-size



Assuming a DMVPN or mGRE encapsulation, look at the NetFlow display while the SAA probe is running to verify packet sizes:

```
R1#show ip cache verb flow
...
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active

…
Et1            192.168.131.16  Local          192.168.128.207 2F B8  10      21
0000 /0  0                     0000 /0  0     0.0.0.0              88      0.3

Tu0            10.0.90.16      Local          10.0.94.1       11 B8  10       1
DBA2 /0  0                     07AF /0  0     0.0.0.0              80      0.0


Tu0            10.0.90.16      Local          10.0.94.1       11 B8  10      20
DBA2 /0  0                     4000 /0  0     0.0.0.0              60      0.3
```

The first flow is Protocol (Pr) hex 2F or decimal 47, GRE. The ToS byte from the unencrypted packet is copied to the GRE header and as such, this GRE packet is marked DSCP EF or hex B8. There are 21 packets in this flow: one SAA control packet and the 20 packets simulating voice. The B/Pk shows the average number of bytes per packet, including the IP/GRE headers.

The second line of the display has a destination port address of hex 7AF or decimal 1967. Port 1967 is enabled when **rtr responder** is configured and the remote router is listening on this UDP port. By default, **control enable** is enabled, and it must be enabled for this SAA probe to function properly. This packet is the control plane for the SAA probe.

The third line in the display is the SAA-generated simulated voice packets. There are 20, as specified above. They have a destination UDP (hex 11 or decimal 17) port number of hex 4000 or decimal 16384, as specified in the SAA configuration above. Because all these packets are the same size, the average B/Pk is 60, which is the size of each packet from the packet decode in the previous figure.

SAA Reaction Configuration

To aid in more quickly identifying teleworkers experiencing voice quality issues, reaction-configurations can be defined by using syslog/logging buffer entries to highlight probes that are experiencing jitter and latency that is exceeding or falling below a pre-determined threshold value.

For example, see the following:

```
rtr reaction-configuration 10 react jitterDSAvg threshold-value 8 7 threshold-type
immediate action-type trapOnly
rtr reaction-configuration 10 react rtt threshold-value 150 149 threshold-type immediate
action-type trapOnly
rtr reaction-configuration 10 react jitterSDAvg threshold-value 6 5 threshold-type
immediate action-type trapOnly
rtr reaction-configuration 10 react timeout threshold-type immediate action-type trapOnly
rtr schedule 10 life forever start-time now
!
```

In the above configuration, a log entry is generated if the average jitter from destination to source (teleworker to head-end) rises above 8 ms and again when it falls below 7 ms. The roundtrip time thresholds (RTTs) are 150 ms and 149 ms, and with the jitter from source to destination (head-end to teleworker), the reaction is triggered if the jitter rises above 6 ms and again if it falls below 5 ms.

The head-end to teleworker jitter values are lower that the teleworker to head-end path because most residential broadband services have greater bandwidth from the Internet, and the jitter typically is less in that direction. The values selected vary from deployment to deployment.

Revising the Policy-map for VoIP UDP Operation

To accommodate including the SAA probes being marked DSCP EF, the priority or LLQ size is increased approximately 26 kbps. Assuming DMVPN (mGRE in transport mode) with NAT-T, ESP 3DES, and SHA, these SAA probe packets are 128 bytes in length after encryption. Now add 32 bytes per packet for the AAL5, Ethernet, and PPP/PPPoE header, resulting in 160 bytes per packet, at 8 bits per byte and 50 packets per second (160 * 8 * 50) or 64,000 kbps. The SAA probe is active in .4 seconds, because 20 packets at a 20 ms interval is 400 ms.

```
!
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_DMVPN_Teleworker
description G.729=~64K G.711=~128K Plus 26K for IP SLA (SAA)
```

```
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 154
 class class-default
  fair-queue
  random-detect
policy-map Shaper
 class class-default
  shape average 182400 1824
  service-policy V3PN_DMVPN_Teleworker
!
```

Comparison testing determined the impact of this SAA probe on latency, drops, and jitter of the real voice (RTP) stream. Branch to head-end jitter increases one millisecond, from 9.2 ms to 10.2 ms, and approximately 20 ms are added to the branch to head-end latency. The head-end to branch values were for all practical purposes unchanged. Voice drops are not an issue. However, the release under test was exposed to CSCeg34495 which is a packet classification issue identified as CSCeg34495. It is possible that the performance characteristics would actually be better than described using a Cisco IOS release not exposed to this issue.

Routing

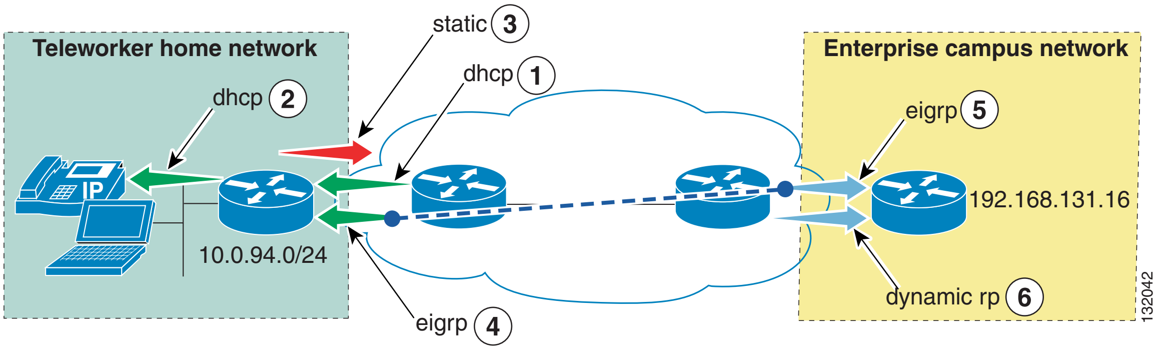
Before discussing access control for this implementation, it is necessary to describe the IP routing configuration. The enterprise security policy specifies that access to Internet services is via the head-end enterprise campus network. This is often referred to as split tunneling not being permitted.

That implies that the remote teleworker PC needs to follow a default route learned via the mGRE tunnel interface rather than from the DHCP server that supplied the outside IP addressing information to the VPN router.

The routing information sources are described and shown in Figure 8-11.

Note References to 192.168.x.x are a placeholder for an Internet-routable address.

Figure 8-11 Routing Information Sources



The following sequence occurs:

1. The teleworker VPN router learns a default gateway from the DHCP server of the ISP.

```
vpn-831#show dhcp lease | inc default-gateway
Temp default-gateway addr: 192.168.128.1

vpn-831#show ip route | inc 192.168.128.1
Gateway of last resort is 192.168.128.1 to network 0.0.0.0
S       192.168.131.16 [1/0] via 192.168.128.1
S*   0.0.0.0/0 [254/0] via 192.168.128.1
```

2. The teleworker VPN router supplies a default gateway and serves IP addressing and other options to the IP phone and workstation using a local DHCP pool.

```
!
ip dhcp pool TELEWORKER
   network 10.0.94.0 255.255.255.0
   default-router 10.0.94.1
   dns-server 10.2.120.253 10.2.120.252
   domain-name ese.cisco.com
   option 150 ip 10.2.120.254
!
```

3. The teleworker VPN router is configured with a static route to the head-end tunnel endpoint. In this example, 192.168.131.16 and 192.168.131.17 are placeholders for the head-end tunnel endpoint addresses. In an actual deployment, they would be Internet-routable addresses.

```
vpn-831#show run | inc ip route

ip route 192.168.131.16 255.255.255.254 dhcp
```

   The above is required because there will be two sources of a default route, one from the Internet and one from the mGRE tunnel. The VPN router must have more specific routes to servers that must be reached outside the VPN tunnel, rather than using the default route learned inside the IP tunnel.

4. The teleworker VPN router learns a default route using the GRE tunnel from the head-end campus router. The default administrative distance for an EIGRP internal/external route is 90/170, and 254 for a DHCP learned route. The default route learned through the GRE tunnel is overridden because it has a lower administrative distance than the default route learned using DHCP.

```
vpn-jk3-2651xm-1#show ip route | inc 0.0.0.0/0
D*EX 0.0.0.0/0 [170/58770176] via 10.0.90.16, 00:00:14, Tunnel0
```

5. The head-end campus router learns an advertisement through the GRE tunnel for the subnet of the remote branch teleworker router.

```
vpn-jk3-2651xm-6#show ip route | inc 10.0.94.0
D       10.0.94.0/24 [90/1817600] via 10.0.90.12, 22:53:07, Tunnel0
```

6. The head-end campus router must learn either from a static default route or more likely from some dynamic routing protocol of the outside Internet routable address of the remote teleworker.

The difference between IPSec-protected GRE and direct IPSec encapsulation is related to determining whether a packet is encrypted. In the case of IPSec-protected GRE tunnels, all packets routed through the tunnel is encrypted, so it is the routing table of the remote router that determines if a packet is encrypted. In direct IPSec encapsulation, any packet that matches the access list specified in the crypto map is encrypted. So routing determines only whether the packet exits an interface with an applied crypto map, not whether it is actually encrypted. This is a subtle but important difference, because it allows the network administrator to use the head-end routing protocol configuration to control the encryption selection process on the remote routers.

Access Control

The initial customer configuration consists of inbound ACLs on the outside physical interface. There are no inbound access lists on the tunnel interface. Also, the configuration includes both Transport layer (TCP and UDP) inspection as well as Application layer inspection.

The initial configuration is as follows:

```
ip inspect name ISC_inside_1 tcp
ip inspect name ISC_inside_1 rtsp
ip inspect name ISC_inside_1 smtp
ip inspect name ISC_inside_1 h323
ip inspect name ISC_inside_1 realaudio
ip inspect name ISC_inside_1 tftp
ip inspect name ISC_inside_1 skinny
ip inspect name ISC_inside_1 ftp
ip inspect name ISC_inside_1 udp
ip inspect name ISC_inside_1 netshow
ip inspect name ISC_inside_1 sip
```

Typically, Transport layer inspection is sufficient for most deployments. With TCP and UDP inspection, the return path packets must match an existing session initiated from the protected (or inside) network. The source and destination IP addresses and port numbers must match in reverse of the session initiated by the inside client.

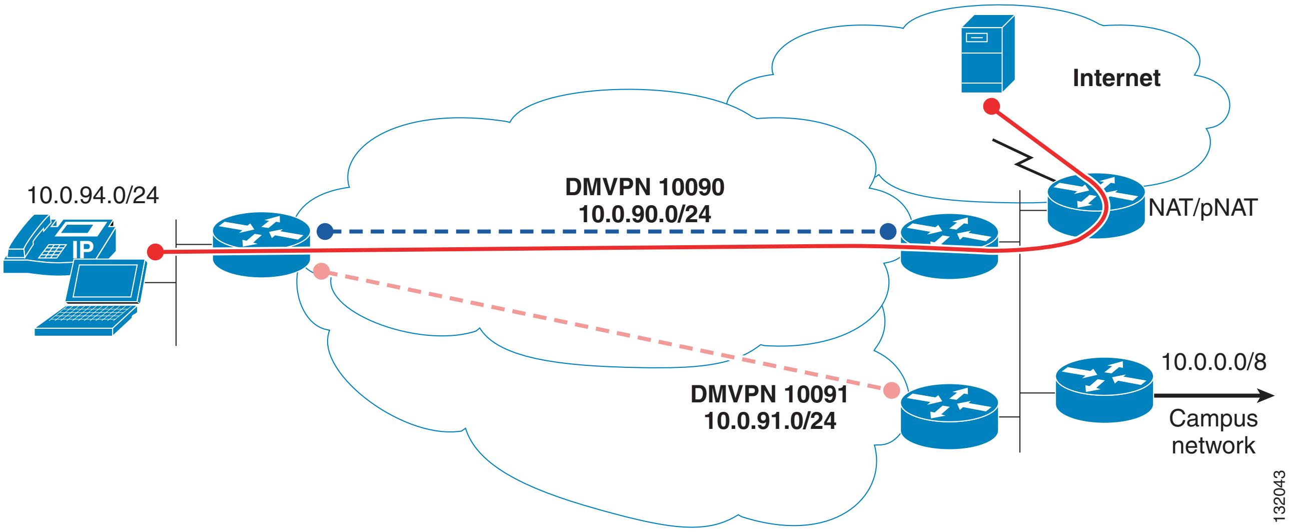
Note For more information, see the following URL (which requires a Cisco password): http://www.cisco.com/en/US/partner/products/sw/secursw/ps1018/products_white_paper09186a0080094658.shtml

Application layer inspection takes precedence over Network layer inspection, and is required if the specific application (such as FTP) uses different port numbers than specified by the session initiator in the return packets.

The customer security policy is such that split tunneling is not permitted. All Internet access for devices on the remote subnet must be through the corporation campus head-end. Because private addressing is in use, the campus head-end location must use NAT/pNAT to determine any Internet access required. The address of the return packets from the Internet server or application is the Internet routable address, and as such, Context-based Access Control (CBAC) must be configured to permit Internet access , but only for TCP, UDP, and FTP initially. Additional Application layer inspection can be added as required.

An example of this topology is represented in Figure 8-12.

Figure 8-12 Access Control Topology Example



The tunnel interfaces have inbound access lists, and CBAC is enabled on the inside Ethernet interface of the remote branch teleworker router. If the inbound access list entry does not specifically permit the packet, the CBAC configuration must have entered a dynamic entry into the access list to permit packets from the enterprise campus head-end to access the remote router subnet.

This layered security approach affords a more stringent posture than what is typically implemented in the enterprise campus network.

The recommended configuration is as follows:

```
!
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
!
interface Tunnel0
…
 ip address 10.0.90.12 255.255.255.0
 ip access-group TUNNEL_INBOUND_ACL in
!
interface Tunnel1
 …
 ip address 10.0.91.12 255.255.255.0
 ip access-group TUNNEL_INBOUND_ACL in
!
interface Ethernet0
 ip address 10.0.94.1 255.255.255.0
 ip inspect CBAC in
 ip route-cache flow
 ip tcp adjust-mss 574
!
interface Ethernet1
 ip address dhcp
 ip access-group INBOUND_ACL in
 service-policy output Shaper
 ip route-cache flow
!
ip access-list extended INBOUND_ACL
 permit udp any eq isakmp any eq isakmp
 permit udp 192.168.131.0 0.0.0.31 eq non500-isakmp any eq non500-isakmp
 permit esp 192.168.131.0 0.0.0.31 any
 permit gre 192.168.131.0 0.0.0.31 any
 permit udp any any eq bootpc
 remark NTP ACLs
 permit udp any eq ntp any eq ntp
 permit icmp any any
 remark SSH
 permit tcp 192.168.131.0 0.0.0.31 any eq 22
 deny   ip any any log
!
ip access-list extended TUNNEL_INBOUND_ACL
 permit ip 10.0.0.0 0.0.0.255 10.0.94.0 0.0.0.255
 permit icmp any any
 permit eigrp any any
 permit igmp any any
 permit pim any any
 deny   ip any any log
!
line vty 0 4
 login local
 transport input ssh
```

Note The log option is useful initially to identify any ports and protocols that are missing from the implementation but are needed for the deployment. After testing, it is recommended to remote this option to spare the overhead of process switching the matches on the entry and the resulting syslog chatter.

Performance Testing

Performance tests were conducted using the customer initial configuration and the enhanced (revised) configuration described in this section. There are also test results using the revised configuration with and without a Linksys BEFSR41 personal firewall between the IPSec peers with NAT-T enabled. Table 8-1 describes these tests.

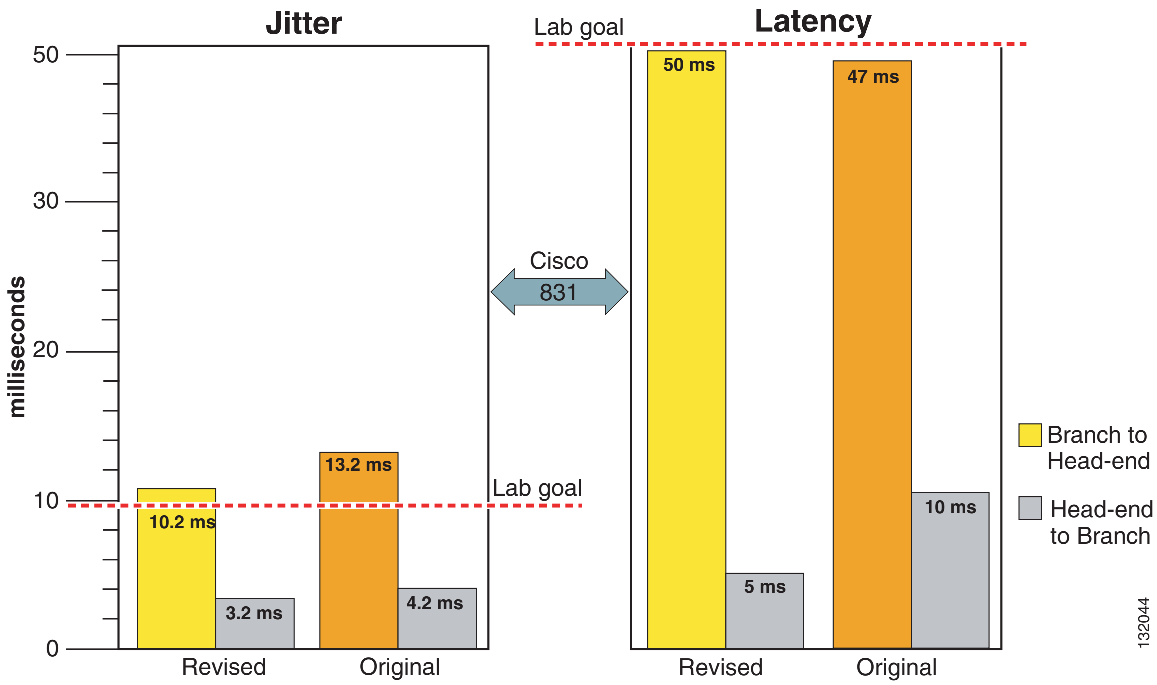
Table 8-1 Performance Test Table

Configuration	Customer Initial Configuration	Revised Configuration
Weighted fair-queue configured on Ethernet interfaces	WFQ enabled	FIFO
Class-map configuration	Extraneous entries	Optimized
TCP MSS	Not configured	574
SAA VoIP UDP Operation—Revised policy-map for VoIP UDP operation	On remote router without ToS marking and at customer configured frequency	Remote router as responder only, optimized, and head-end configured and initiated
Access control	All application layers enabled	UDP, TCP, and FTP only
NAT-T and Linksys Personal Firewall	N/A	With and without using the above configuration changes

Original and Revised Configurations

Figure 8-13 shows the net impact of the revised configuration on VoIP latency and jitter. The difference in voice drops was of no consequence.

Figure 8-13 Original and Revised Configuration Test Results



The ESE lab testbed uses a goal of 50 ms as the average Chariot reported latency and 8–10 ms as the average jitter for acceptable VoIP quality. In a customer deployment, acceptable VoIP quality can be obtained when both latency and jitter are observed at higher values. The lab is a controlled and optimal environment and these somewhat conservative goals are the standard.

In most teleworker environments, the data rates are asymmetrical; both branch router to head-end router and the reverse are reported. In this test, a simulated 256 kbps/1.4 Mbps data rate was assumed. The 831 output interface was shaped at 182,400 bps. Because of the higher downlink data rate, latency and jitter are generally not an issue for this half of the call leg. The downlink values are shown in the diagram but are subdued and behind the uplink or branch to head-end values.

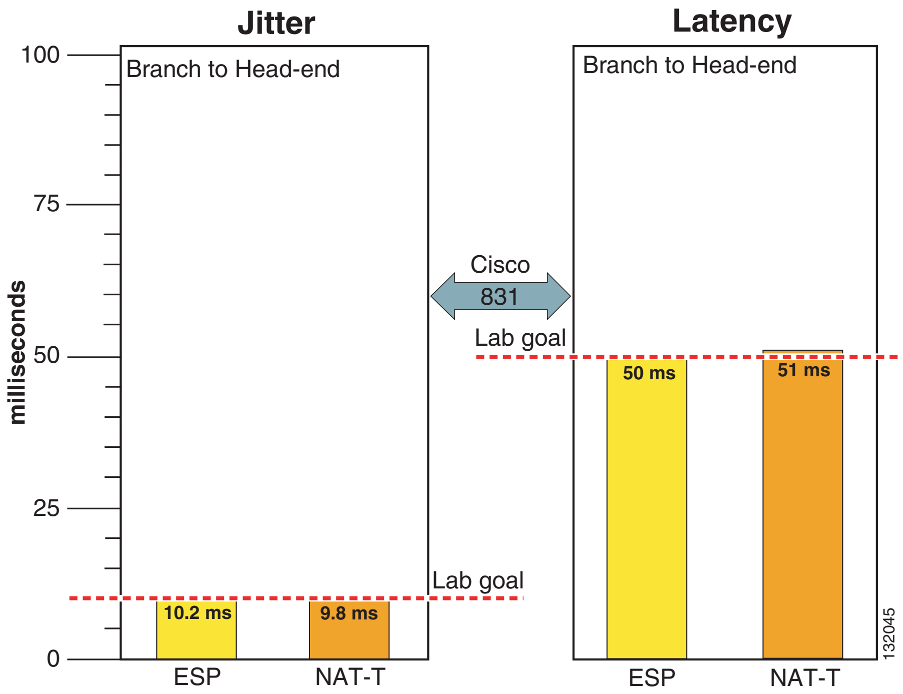
In either configuration, the latency is similar, and near the 50 ms goal.

Average jitter for the revised configuration is 10.2 ms and 13.2 ms for the original configuration, or approximately a 22 percent improvement. At higher data rates, this difference would be less as the link speed approaches 768 kbps, and serialization or blocking delay becomes less of an issue.

Impact of NAT-T

NAT-T mode is enabled by default in Cisco IOS routers, and if during the initial IKE exchange on UDP 500, a NAT/pNAT device is detected between the IPSec peers, these peers exchange both IKE and IPSec packets encapsulated in UDP on port 4500. If no NAT/pNAT device exists between the peers, the normal behavior of IKE on UDP 500 and IPSec ESP in protocol “50” is used. A Linksys BEFSR41 EtherFast® Cable/DSL Router with 4-Port Switch is inserted between the IPSec peers and a performance test is run with the revised configuration. (See Figure 8-14.)

Figure 8-14 Impact of NAT-T

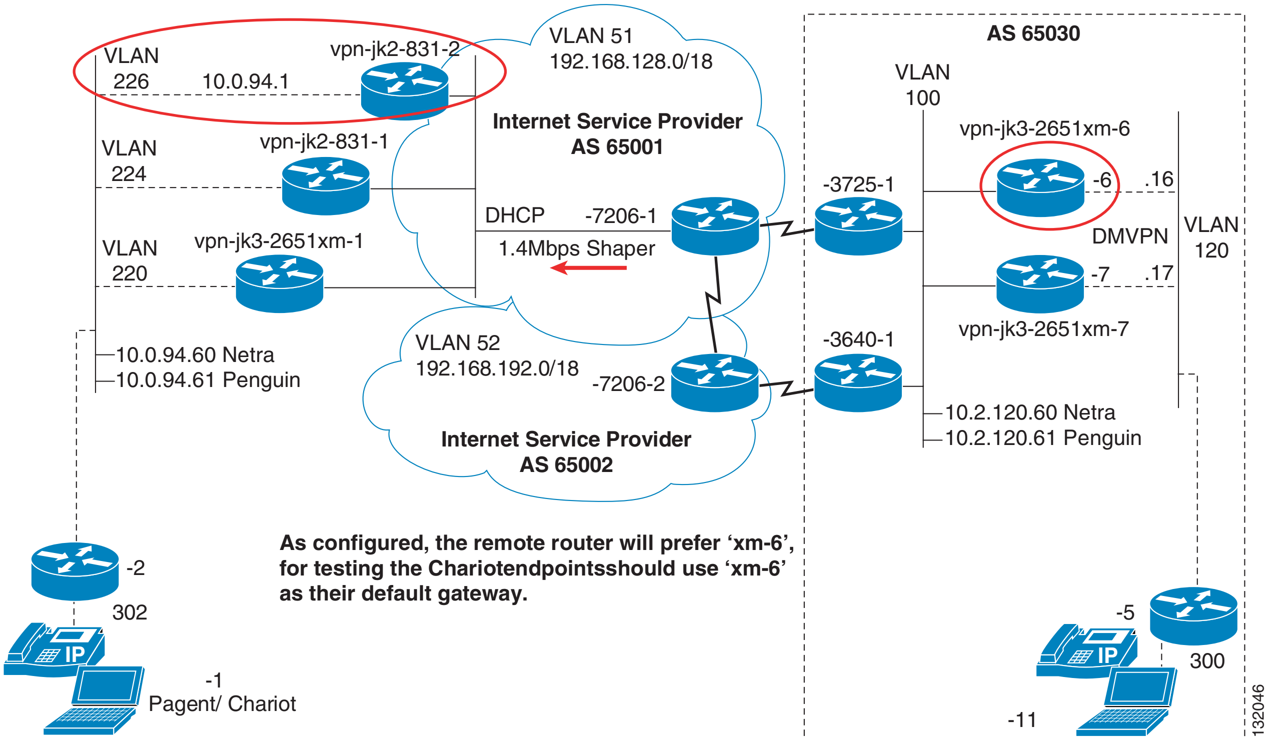


Simply stated, the results were similar enough to indicate that the additional router and the NAT/pNAT translation on the UDP 4500 packets did not impact latency and jitter of the VoIP stream to a measurable degree.

Test Topology

Figure 8-15 shows the topology under test:

Figure 8-15 Test Topology



As configured, the remote router will prefer 'xm-6', for testing the Chariotendpointsshould use 'xm-6' as their default gateway.

Implementation and Configuration

This section describes the configuration of the dual hub/dual DMVPN solution, and includes the following sections:

- Remote Branch Router
- Primary Head-end Router

Remote Branch Router

This is the configuration of the remote branch router:

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname vpn-jk2-831-2
!
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!
```

```
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host JOEL_KING_LAB_ca_server 192.168.131.25
ip cef
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip ips po max-events 100
no ftp-server write-enable
!
crypto pki trustpoint ESE_JK_RACK
 enrollment url http://JOEL_KING_LAB_ca_server:80
 revocation-check none
!
!
crypto pki certificate chain ESE_JK_RACK
 certificate 03
  [removed]
  quit
 certificate ca 01
  [removed]
  quit
!
!
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_DMVPN_Teleworker
description G.729=~64K G.711=~128K Plus 26K for IP SLA (SAA)
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 154
 class class-default
  fair-queue
  random-detect
policy-map Shaper
 class class-default
  shape average 182400 1824
  service-policy V3PN_DMVPN_Teleworker
!
!
!
crypto isakmp policy 10
 encr 3des
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
!
!
crypto ipsec transform-set TRANSPORT_3DES_SHA esp-3des esp-sha-hmac
 mode transport
crypto ipsec transform-set TUNNEL_3DES_SHA esp-3des esp-sha-hmac
!
```

```
crypto ipsec profile ECT_PROFILE_1
 set security-association lifetime kilobytes 530000000
 set security-association lifetime seconds 14400
 set transform-set TRANSPORT_3DES_SHA
!
!
crypto call admission limit ike sa 65536 # Included simply to show it is configurable
!                                        # An 831 has a 20 crypto peer (IKE peer limit)
!                                          but 5-10 peers is a practical limit.
!
interface Tunnel0
 description Tunnel0 - DMVPN
 bandwidth 2000
 ip address 10.0.90.12 255.255.255.0
 ip access-group TUNNEL_INBOUND_ACL in
 no ip redirects
 ip mtu 1408
 ip nhrp map 10.0.90.16 192.168.131.16
 ip nhrp map multicast 192.168.131.16
 ip nhrp network-id 10090
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.90.16
 ip route-cache flow
 ip tcp adjust-mss 574
 ip summary-address eigrp 100 10.0.94.0 255.255.255.0 5
 qos pre-classify
 tunnel source Ethernet1
 tunnel mode gre multipoint
 tunnel key 10090
 tunnel protection ipsec profile ECT_PROFILE_1 shared
!
interface Tunnel1
 description Tunnel1 - DMVPN
 bandwidth 2000
 ip address 10.0.91.12 255.255.255.0
 ip access-group TUNNEL_INBOUND_ACL in
 no ip redirects
 ip mtu 1408
 ip nhrp map 10.0.91.17 192.168.131.17
 ip nhrp map multicast 192.168.131.17
 ip nhrp network-id 10091
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.91.17
 ip route-cache flow
 ip tcp adjust-mss 574
 ip summary-address eigrp 100 10.0.94.0 255.255.255.0 5
 load-interval 30
 qos pre-classify
 tunnel source Ethernet1
 tunnel mode gre multipoint
 tunnel key 10091
 tunnel protection ipsec profile ECT_PROFILE_1 shared
!
interface Ethernet0
 description Ethernet0 - inside
 ip address 10.0.94.1 255.255.255.0
 ip inspect CBAC in
 ip route-cache flow
 ip tcp adjust-mss 574
 load-interval 30
!
interface Ethernet1
 description Ethernet1 - outside
 ip address dhcp
 ip access-group INBOUND_ACL in
 service-policy output Shaper
 ip route-cache flow
 load-interval 30
 duplex auto
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet3
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto
!
router eigrp 100
 network 10.0.0.0
 no auto-summary          # Manual summarization on the interfaces
!
ip classless
ip route 172.26.0.0 255.255.0.0 10.0.94.2
ip route 192.168.131.16 255.255.255.254 dhcp
!
no ip http server
no ip http secure-server
!
!
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
ip access-list extended INBOUND_ACL
 permit udp any eq isakmp any eq isakmp
 permit udp 192.168.131.0 0.0.0.31 eq non500-isakmp any eq non500-isakmp
 permit esp 192.168.131.0 0.0.0.31 any
 permit gre 192.168.131.0 0.0.0.31 any
 permit udp any any eq bootpc
 remark NTP ACLs
 permit udp any eq ntp any eq ntp
 permit icmp any any
 remark SSH
 permit tcp 192.168.131.0 0.0.0.31 any eq 22
 deny   ip any any
ip access-list extended TUNNEL_INBOUND_ACL
 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit icmp any any
 permit eigrp any any
 permit igmp any any
 permit pim any any
 deny   ip any any
snmp-server community private RW
snmp-server community public RO
snmp-server system-shutdown
snmp-server enable traps tty
!
```

```
control-plane
!
call admission limit 99    # Included simply to show it is configurable
call admission load 1 10   # Included simply to show it is configurable
rtr responder
alias exec conact show cry eng conn act
alias exec shintb sh ip int brief
alias exec shacl show access-list
alias exec clacl clear access-list counters
alias exec shisa show crypto isa sa
alias exec stcon ping 10.2.120.16 source 10.0.94.1 repeat 15
!
line con 0
 exec-timeout 120 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 password [removed]
 login
 transport preferred all
 transport input all
 transport output all
!
scheduler max-task-time 5000
!
ntp server 192.168.130.1
end
```

Primary Head-end Router

There are two head-end routers in this configuration, but only one is shown. The second head-end router terminates Tunnel 1 of the branch router.

```
version 12.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname vpn-jk3-2651xm-6
!
!
logging buffered 8192 debugging
!
clock timezone est -5
clock summer-time edt recurring
no network-clock-participate slot 1
no network-clock-participate wic 0
no aaa new-model
ip subnet-zero
ip cef
!
!
ip ips po max-events 100
no ip domain lookup
ip domain name ese.cisco.com
ip host cisco123_LAB_ca_server 192.168.131.25
ip multicast-routing
```

```
no ftp-server write-enable
!
!
crypto pki trustpoint ESE_JK_RACK
 enrollment url http://cisco123_LAB_ca_server:80
 revocation-check crl
!
!
crypto pki certificate chain ESE_JK_RACK
 certificate 04
  [removed]
  quit
 certificate ca 01
  [removed]
  quit
!
crypto isakmp policy 1
 encr 3des
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set TRANSPORT_3DES_SHA esp-3des esp-sha-hmac
 mode transport
crypto ipsec transform-set TUNNEL_3DES_SHA esp-3des esp-sha-hmac
!
crypto ipsec profile ECT_PROFILE_1
 set transform-set TRANSPORT_3DES_SHA TUNNEL_3DES_SHA
!
!
crypto call admission limit ike sa 65536 # Included simply to show it is configurable
!
!
interface Tunnel0
 description DMVPN
 bandwidth 2000
 ip address 10.0.90.16 255.255.255.0
 ip access-group TUNNEL_INBOUND_ACL in
 no ip redirects
 ip mtu 1408
 no ip next-hop-self eigrp 100
 ip pim nbma-mode
 ip pim sparse-dense-mode
 ip multicast rate-limit out 768
 ip nhrp map multicast dynamic
 ip nhrp network-id 10090
 ip nhrp holdtime 600
 ip nhrp server-only
 no ip split-horizon eigrp 100
 load-interval 30
 delay 2000
 tunnel source FastEthernet0/1.100
 tunnel mode gre multipoint
 tunnel key 10090
 tunnel protection ipsec profile ECT_PROFILE_1
!
interface FastEthernet0/0
 description FlashNet156
 ip address 172.26.157.36 255.255.254.0
 load-interval 30
 duplex auto
 speed auto
!
!
interface FastEthernet0/1.100
```

```
 description Outside interface
 encapsulation dot1Q 100
 ip address 192.168.131.16 255.255.255.224   # Address referenced on remote peer
!
interface FastEthernet0/1.120
 description Inside interface
 encapsulation dot1Q 120
 ip address 10.2.120.16 255.255.255.0
!
!
router eigrp 100
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 distribute-list TEN_and_SUBNETS out Tunnel0
 no auto-summary
!
ip classless
ip http server
no ip http secure-server
!
ip access-list standard OFFSET
 permit any
ip access-list standard TEN_ONLY
 permit 10.0.0.0
 remark --- only send 10.0.0.0
ip access-list standard TEN_and_SUBNETS
 permit 10.0.0.0 0.0.255.255
!
ip access-list extended TUNNEL_INBOUND_ACL
 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit icmp any any
 permit eigrp any any
 permit igmp any any
 permit pim any any
 deny   ip any any
!
!
!
control-plane
!
call admission limit 99       # Included simply to show it is configurable
call admission load 1 10      # Included simply to show it is configurable
!
rtr responder
rtr 18
 type jitter dest-ipaddr 10.0.94.1 dest-port 16384 codec g729a codec-numpackets 20
 tos 184
 timeout 200
 tag JITTER_10.0.94.0
 frequency 30
rtr reaction-configuration 18 react jitterDSAvg threshold-value 8 7 threshold-type
immediate action-type trapOnly
rtr reaction-configuration 18 react rtt threshold-value 150 149 threshold-type immediate
action-type trapOnly
rtr reaction-configuration 18 react jitterSDAvg threshold-value 6 5 threshold-type
immediate action-type trapOnly
rtr reaction-configuration 18 react timeout threshold-type immediate action-type trapOnly
rtr schedule 18 life forever start-time now
alias exec conact show cry eng conn act
alias exec shintb sh ip int brief
alias exec shacl show access-list
alias exec clacl clear access-list counters
alias exec shisa show crypto isa sa
!
```

```
line con 0
 exec-timeout 120 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password [removed]
 login
!
ntp server 192.168.130.1
!
end
```

Cisco IOS Versions Tested

The following Cisco IOS versions were used for testing:

- Branch routers—c831-k9o3sy6-mz.123-8.T5
- Head-end routers—c2600-advsecurityk9-mz.123-8.T5

Summary

Although many customers often take the approach of implementing a pilot deployment without head-end redundancy, saying they will address redundancy later, all new installations should plan for and implement multiple head-ends from the beginning. An example of the importance of this approach lies in the fact the testing found and filed the software defect CSCeg18278. With the lead time to debug and obtain a software image incorporating the fix perhaps several months away, early detection of any outstanding issues minimizes their impact on deployment schedules.

The same also applies to implementations that are for data-only today, but VoIP will be added later. This may mean eExtensive re-work of the deployed remote routers configuration may be necessary to accommodate VoIP in the future. With some minor revisions to the customer configuration, VoIP can be planned for and provisioned from the start, rather than later in a hurried manner.

These customer configurations were not dramatically wrong, but a few minor changes would have enhanced the performance of VoIP. As is often the case with networks, there is seldom only one problem and they tend not to cause a total failure of network connectivity. Generally, there are multiple issues that lead to a problem, and constant assessment of the network and its configuration serve to maintain reliability, availability, and good performance.

CHAPTER 9

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:

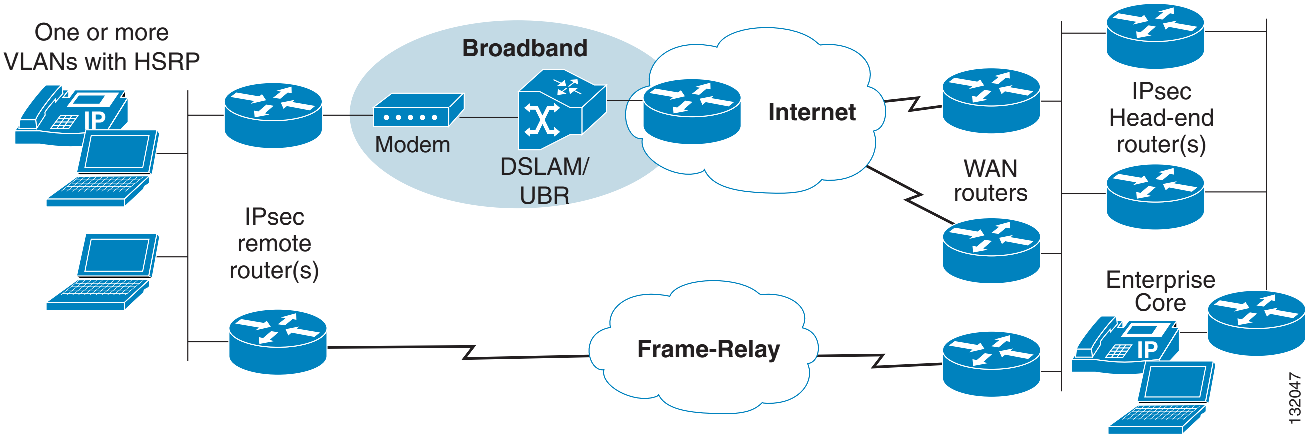
- Interest in using broadband as a lower cost alternative to traditional WAN media
- Desire to use alternate technologies for primary and backup path
- Encryption for both the existing Frame Relay and the broadband link, or only for the broadband link

Note According to CCO and its Feature Navigator, 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.

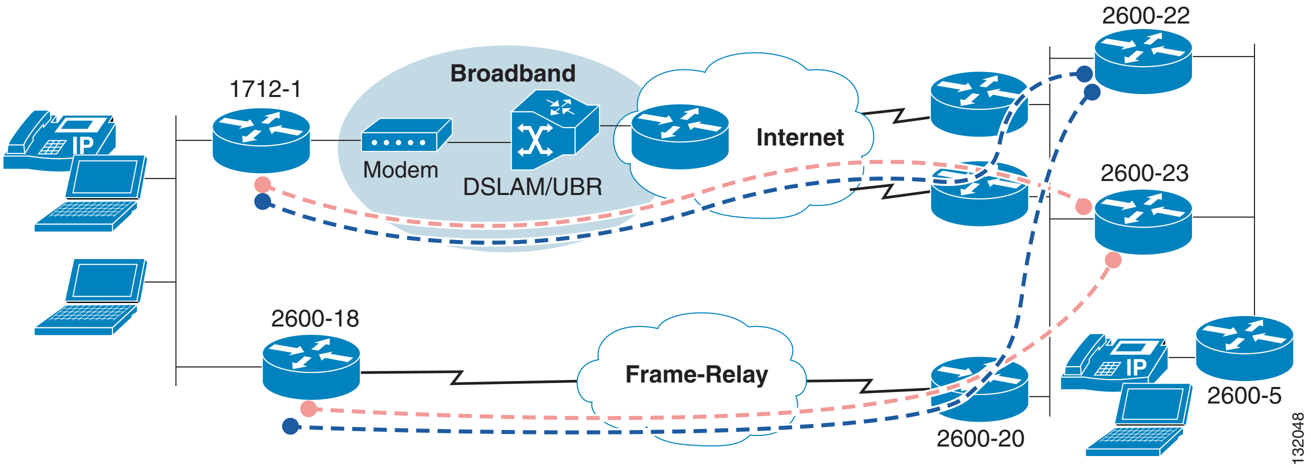
This section includes the following topics:

- 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

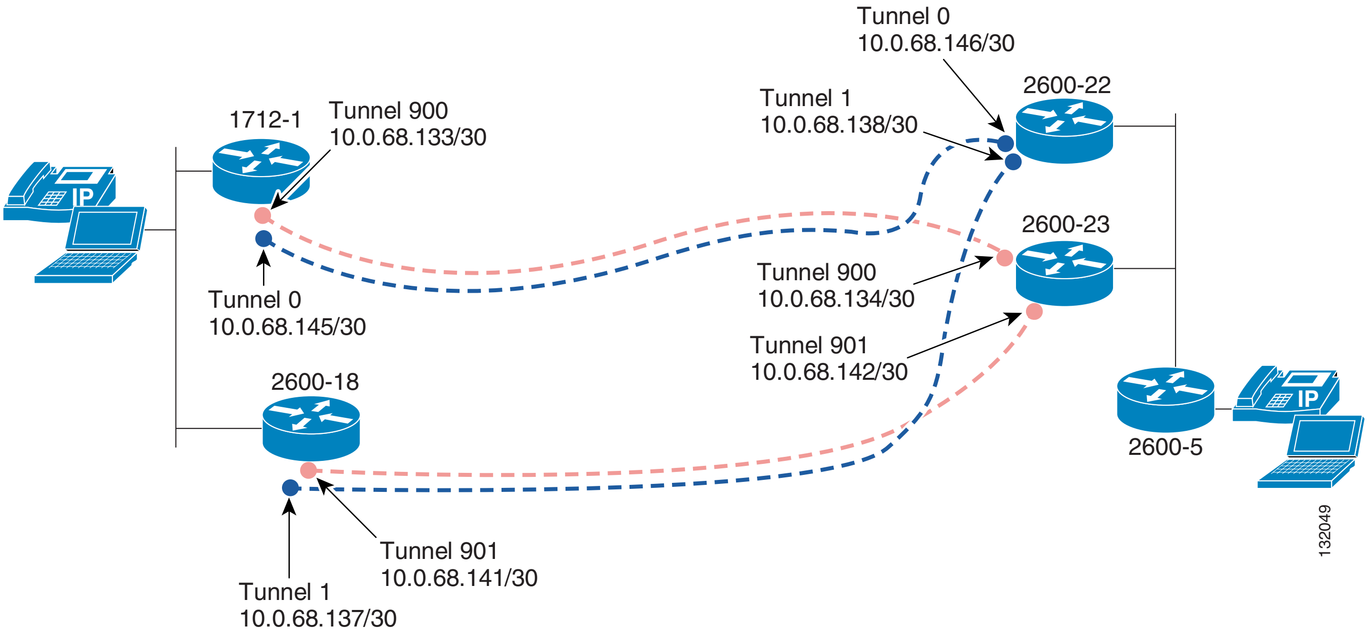
In Figure 9-2, two GRE tunnels are defined from each remote router to a head-end GRE/IPSec peer. This configuration provides maximum availability because the site maintains connectivity in the event that one remote router and one head-end router are out of service at the same time.

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

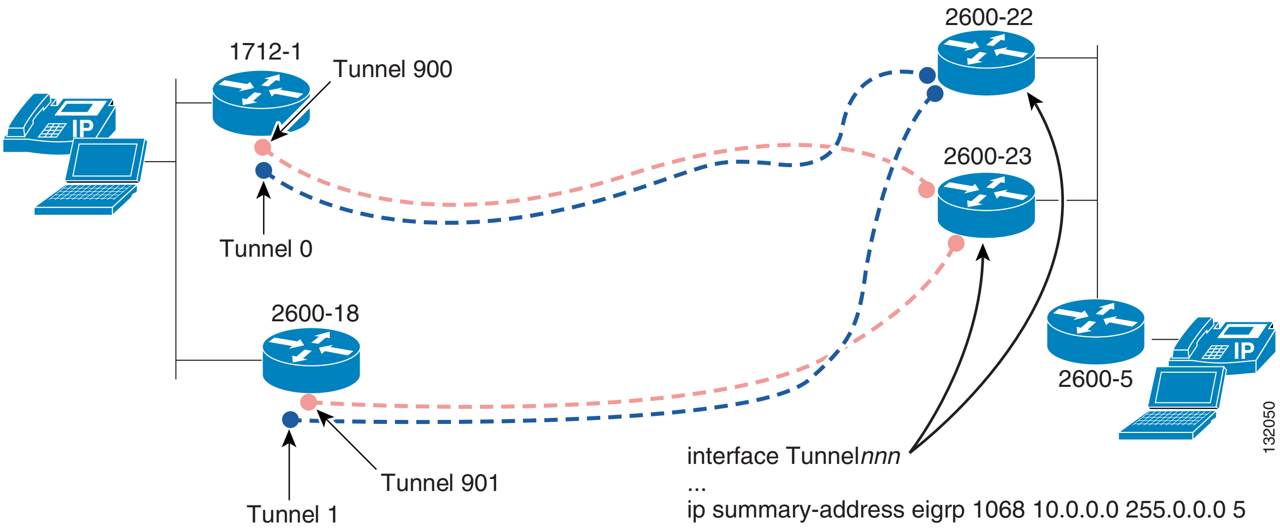


The GRE interface numbers on the branch and head-end routers are the same on both ends; Tunnel 1 on remote router 2600-18 connects to Tunnel 1 on head-end router 2600-22. This nomenclature facilitates troubleshooting. The IP addresses for the tunnel interfaces are allocated out of the address space for 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

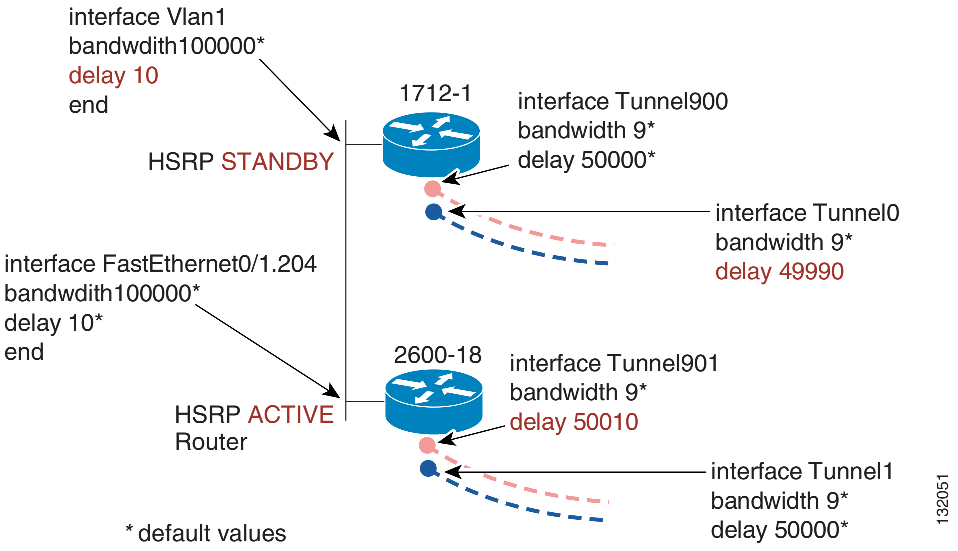
One rule of thumb is that whatever you type is multiplied by 10 when displayed by the router.

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:

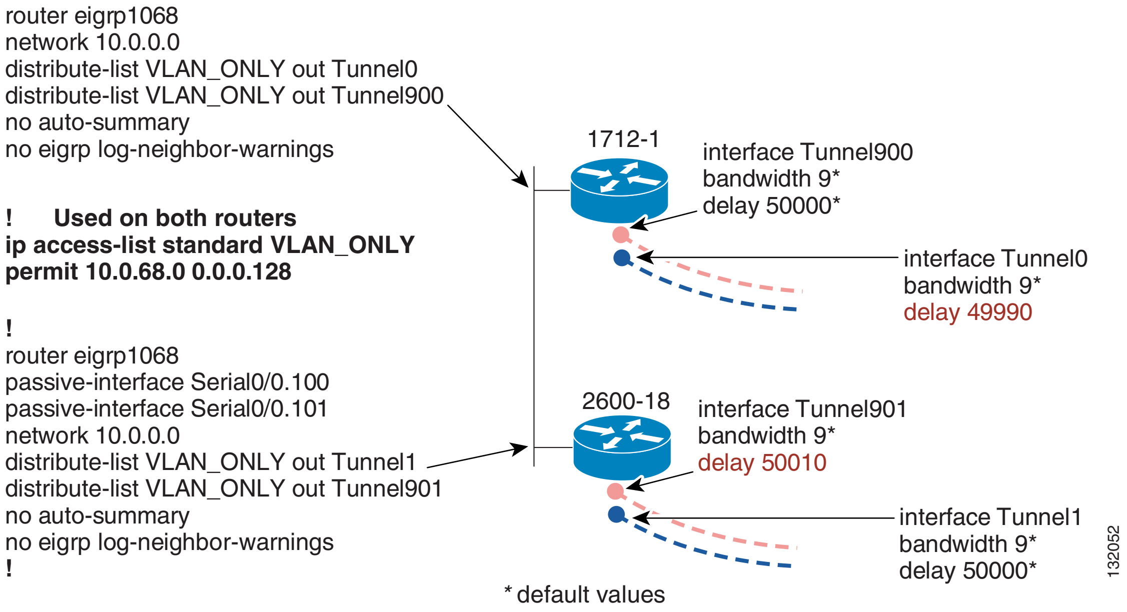
```
D:\>perl eigrp.pl 9 499900 100
297244416

#
#       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
# same as the router
#
```

Branch EIGRP and Addressing

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

Figure 9-6 Frame Relay/Broadband-EIGRP Configuration



```
router eigrp1068
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

!     Used on both routers
ip access-list standard VLAN_ONLY
permit 10.0.68.0 0.0.0.128

!
router eigrp1068
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
!
```

```
interface Tunnel900
bandwidth 9*
delay 50000*
```

```
interface Tunnel0
bandwidth 9*
delay 49990
```

```
interface Tunnel901
bandwidth 9*
delay 50010
```

```
interface Tunnel1
bandwidth 9*
delay 50000*
```

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.

```
1712-1#show run | inc interface|tunnel source|ip address
interface Tunnel0
 ip address 10.0.68.145 255.255.255.252
 tunnel source Loopback0
interface Tunnel900
 ip address 10.0.68.133 255.255.255.252
 tunnel source Loopback0
interface Loopback0
 ip address 10.0.68.129 255.255.255.255
…
interface Vlan1
 ip address 10.0.68.1 255.255.255.128
interface Dialer1
 ip address negotiated
```

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 Tunneln** and include a distribute list for each tunnel interface that resides on this router. If the more generic form of **distribute-list VLAN_ONLYout** 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.

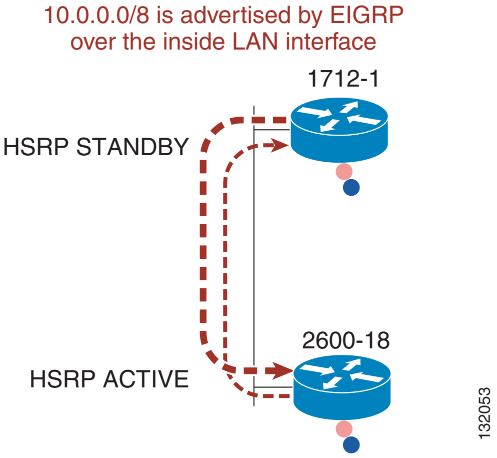
Also, for network management purposes, a second loopback address (Loopback 1) can be allocated from the /22 address block of the site.

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


10.0.0.0/8 is advertised by EIGRP over the inside LAN interface
1712-1
HSRP STANDBY
2600-18
HSRP ACTIVE
132053

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.

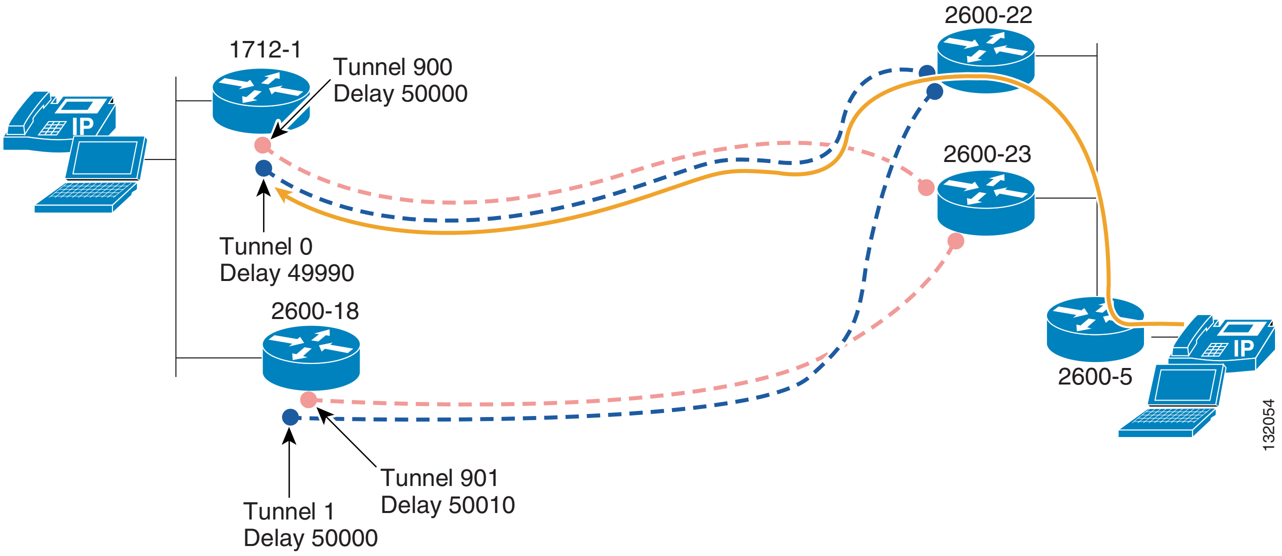
Head-end to Branch Considerations

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.

Figure 9-8 Frame Relay/Broadband—Downstream Option 1



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-2600-5#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 10.2.124.22 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.

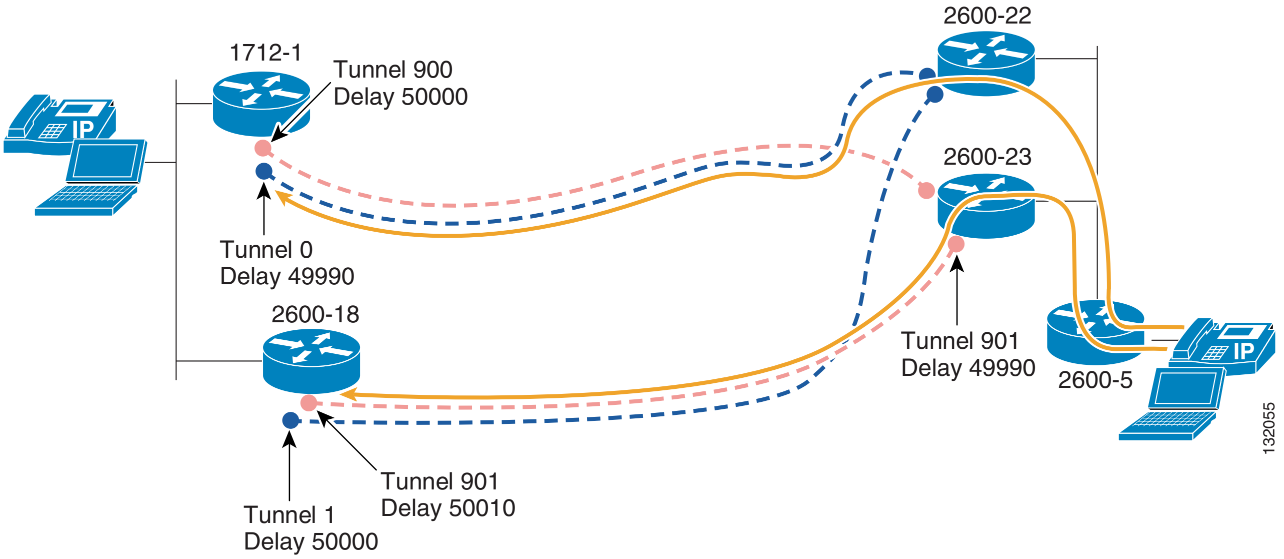
```
vpnjk-2600-23#config t
Enter configuration commands, one per line.  End with CNTL/Z.
vpnjk-2600-23(config)#interface tunnel 901
vpnjk-2600-23(config-if)#delay 49990
```

```
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

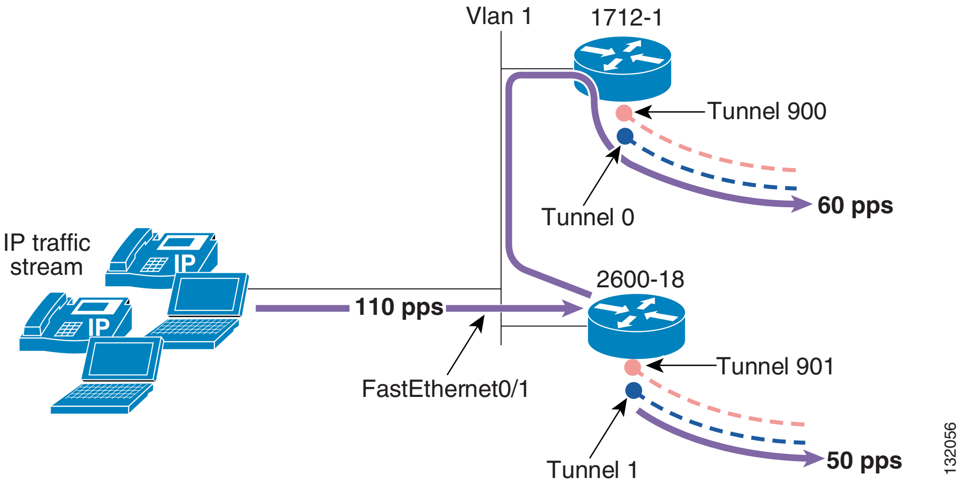
To demonstrate the load sharing, an IP traffic stream is generated with a traffic generation IOS router to simulate three traffic streams *(ts#)* from a single source IP address to three separate destination IP addresses.

```
ts#            tos  len protocol source    destination   rate
    1 UDP  B8   60    17     10.0.68.2  10.2.124.5     50 pps
    2 UDP  B8   60    17     10.0.68.2  10.2.124.9     50 pps
    3 UDP  B8   60    17     10.0.68.2  10.2.124.16   10 pps
```

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.

Figure 9-10 Frame Relay/Broadband—Verification



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

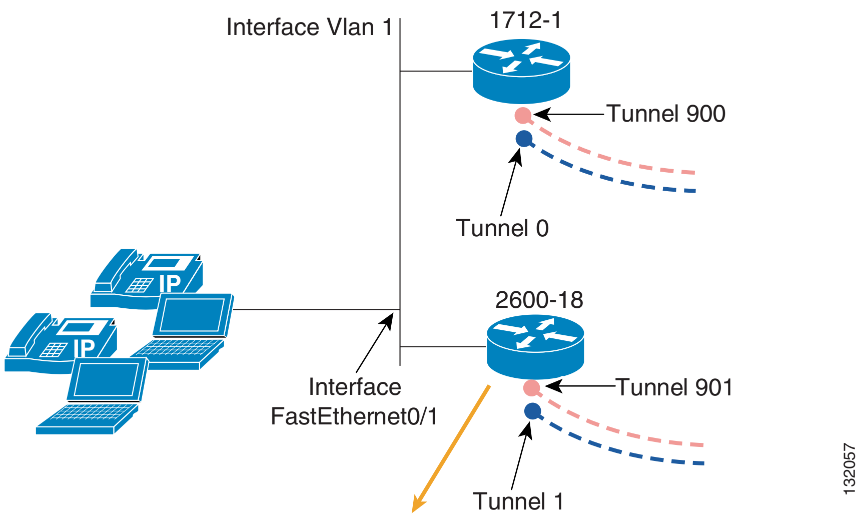
Router 2600-18:

- 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.)

Figure 9-11 Frame Relay/Broadband—CEF/NetFlow Verification



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.

```
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 cache 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.

Table 9-1 Failure Scenarios and Backup Connectivity

Failure Scenario	Result
IPSec/GRE head-end router 2600-22 fails or is out of service	Remote router 1712-1 becomes the HSRP active router and uses Tunnel 900 (broadband WAN link) for all traffic.
IPSec/GRE head-end router 2600-23 fails or is out of service	No change—2600-18 continues as HSRP active router and Tunnels 1 and 0 (broadband and Frame Relay links) are still used.
Frame Relay network fails—total failure of both PVCs	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.
Broadband network fails	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

Configuration

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-ik9o3s3-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
!
```

```
!
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-ik9o3s3-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
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
!
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 10.0.68.129 255.255.255.255
!
!
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 10.0.68.0 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 ipIcmpEcho 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
!
!
 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 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
 qos pre-classify
 keepalive 10 3
 tunnel source Loopback0
 tunnel destination 192.168.131.22
!
interface Tunnel901
 description 2600-23
 ip address 10.0.68.141 255.255.255.252
 load-interval 30
 delay 50010
 qos 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
!                                          Note: One physical interface, two PVCs
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
```

```
!
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
!                                 # decrease 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
 frame-relay mincir 486400
 service-policy output TEST
 frame-relay fragment 640
!

end
```

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.

```
!
hostname vpnjk-2600-5
!
!
interface FastEthernet0/1.124
 encapsulation dot1Q 124
 ip address 10.2.124.5 255.255.255.0
!
!
router eigrp 1068
 network 10.0.0.0
 no auto-summary
!
end
```

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 s ize 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.

CHAPTER 10

Large Branch—Multilink PPP

Large branch offices that require encrypted voice and data are generally limited to nine G.729 calls for a single T1 because 33 percent of the link is targeted for voice and the remainder of the bandwidth is targeted for data. For the enterprise customer who needs more than nine concurrent calls, or must also support video conferencing, using Multilink PPP (MLPPP) and including an additional T1 line rather than upgrading to either a full or fractional DS3 may be desirable from a cost standpoint.

Multilink PPP over leased lines to a head-end location may be the most cost effective option for the medium-to-large branch. The disadvantage with MLPPP is the lack of service provider support. Test results are included in this chapter for 8–15 concurrent voice calls, given a 4:1 to 10:1 Erlang ratio that translates to a WAN topology that can support an office staffed from 32 to 150 people.

Note An *Erlang* is a unit of telecommunications traffic measurement. An Erlang represents the continuous use of one voice path. Erlang traffic measurements (or estimates) can be used to determine how many concurrent voice calls should be provisioned between multiple network locations.

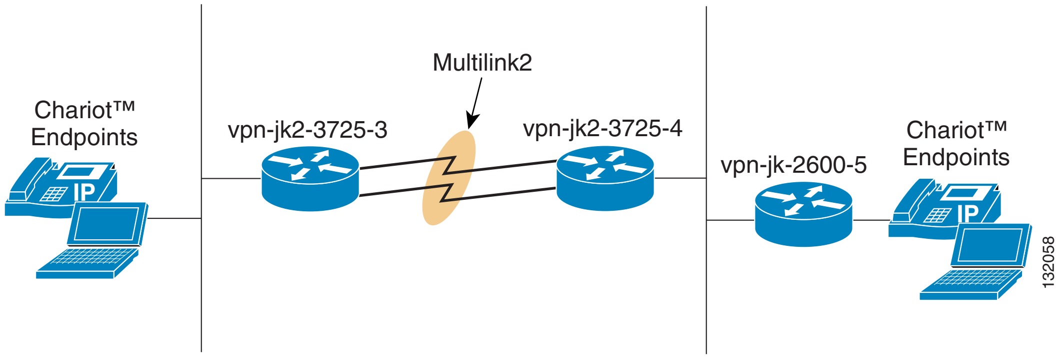
This chapter includes the following sections:

- Topology
- Traffic Profile
- V3PN QoS Service Policy
- Implementation and Configuration
- Show Commands
- Cisco IOS Versions Tested
- Caveats
- Summary

Topology

The topology under test, as shown in Figure 10-1, contains two Cisco 3725 routers with two serial interfaces (WIC-2T) clocked internally.

Figure 10-1 Large Branch—Multilink PPP



The **clockrate 1300000** command is used on one router serial interface to provide clocking for the lab testing. A rate of 1.536 M or 1.544 M is not supported by Cisco IOS for this interface type when clocked internally.

In testing, it is assumed that a branch of this size requires a separate router to increase the availability of the site. In other words, it was not assumed the second T1 was for availability, but rather as a capacity requirement.

Traffic Profile

The traffic profile in these tests include the typical ESE Enterprise Mix (**EMIX**) -G.729 voice calls, transactional data (TN3270 and HTTP), and best effort including HTTP, SMTP, DNS, and FTP.

Simulated Video Conferencing is also included. As part of the standard Chariot tests, an H.261 NetMeeting video conference stream is included and was modified for these tests. The H.261 video coding standard was designed for data rates that are multiples of 64 kbps, and is sometimes called “p x 64 kbps” (p is in the range 1–30). This video codec was designed for ISDN lines, which add capacity in increments of 64 kbps.

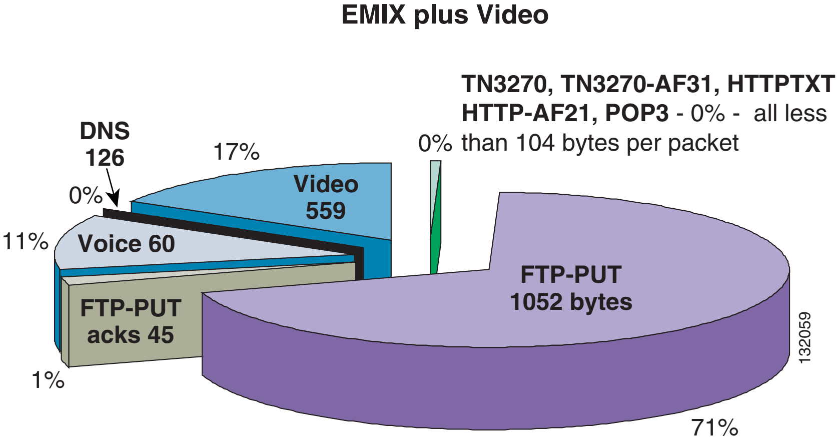
The default Chariot test has a buffer size of 522 bytes. The Layer 3 size of these UDP packets as reported by NetFlow is approximately 559 bytes, the difference being the IP, UDP, and Chariot headers included in the Layer 3 size of the packet. Note that this 559-byte packet does not include GRE, crypto, or PPP encapsulation headers. When using IPSec transport mode, the packet is 626 bytes or 650 bytes per packet using IPSec tunnel mode.

The Chariot target data rate is configured at 256 kbps, which equates to a video data stream of approximately 58 pps. The Chariot file size for this video stream is 2,088,000 bytes. In the caveats section, the testing ramifications of this file size are explored in more detail.

Shown in Figure 10-2 is a representation of the traffic flow used in these tests. The branch to head-end flows are shown. The head-end to branch flows are similar in percentages. The average packet size is shown for the respective categories.

Note The Cisco 6729 IP Phone was used for voice and NetMeeting for video only (no audio).

Figure 10-2 Traffic Profile—Branch to Head-end



Note that in this traffic profile, the QoS service policy is provisioned for voice and video in percentages of link bandwidth:

```
  class VOICE
   priority percent 18

  class VIDEO-CONFERENCING
   priority percent 15
```

The Call Admission Control parameters for this test limit the number of concurrent voice calls to less than 18 percent of the available bandwidth, and the data rate of the video stream is sufficient for the allocated bandwidth. In the test results documented in this chapter, the number of concurrent G.729 voice calls is eight. At approximately 56 kbps per call, the priority queue should have at least 448 kbps (56 * 8).

```
vpn-jk2-3725-4#show policy-map interface multilink 2 out class VOICE
 Multilink2
  Service-policy output: V3PN_Branch

    Class-map: VOICE (match-all)
      96040 packets, 8450920 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp ef
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 18 (%)
        Bandwidth 468 (kbps) Burst 11700 (Bytes)
        (pkts matched/bytes matched) 96041/13445040
        (total drops/bytes drops) 0/0
```

Calculating an adequate size of the priority (LLQ) queue for encrypted video is not as straightforward as for voice. Where voice packets are a fixed size, video packets can vary in size. As such, the crypto overhead as a percentage of the unencrypted video packet varies based on the size of the packet. Smaller packets have a higher percentage of crypto overhead than do large packets.

The rule of thumb for provisioning the video LLQ requirements is to add 20 percent to the configured video data rate. Table 10-1 illustrates the crypto overhead associated with the packet size distribution of a typical video stream.

Table 10-1 V3PN—Video Provisioning

Packet size distribution (bytes)[1]	% of Packets[2]	Assuming video packet of N bytes	IPSec tunnel mode and GRE byte increase	Percent increase
1025–1518	37%	1025	1104	8%
513–1024	20%	513	592	15%[3]
257–512	8%	257	336	31%
129–256	34%	129	208	61%

[1] Rule of Thumb: Video LLQ provisioned at rate plus 20%

[2] Rule of Thumb: Video LLQ provisioned at rate plus 20%

[3] Assuming an average packet size between 500–600 bytes

The Chariot video stream simulated a 256 kbps video stream. Given that the average packet size in that stream falls between 500 to 600 bytes, the crypto overhead can be assumed to be approximately 15 percent. Adding 15 percent crypto overhead to the video stream and then adding 20 percent to accommodate video bursts, you should allocate at least 353 kbps. In testing, the recommended 15 percent bandwidth allocation for the 2.6 M link is 390 kbps, which is sufficient for the 256 kbps video stream.

```
vpn-jk2-3725-4# show policy-map interface multilink 2 out class VIDEO-CONFERENCING
 Multilink2

  Service-policy output: V3PN_Branch

    Class-map: VIDEO-CONFERENCING (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af41
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 15 (%)
        Bandwidth 390 (kbps) Burst 9750 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0
```

In testing, this proved to be an acceptable allocation for the video stream. Note that both the VOICE and VIDEO-CONFERENCING display show the same Output Queue Conversation number of 264. There is only one Strict Priority queue. Although voice and video are provisioned separately, they share the same queue. For this reason, interactive video conferencing is not recommended on link speeds that have serialization (blocking) delay issues; namely, links below 768 kbps.

V3PN QoS Service Policy

The configuration was coded with an absolute **bandwidth 2600** and **ppp multilink links minimum 2,** assuming that a backup router and pair of T1s would be deployed.

Be advised, however, that the bandwidth of the multilink interface is derived from the sum of the bandwidth of the active member links, and the QoS service policy calculates the actual bandwidth by multiplying the configured percentages by the derived multilink interface bandwidth. The given voice is shown as 33 percent of 2,600,000, or 858 kbps.

```
vpn-jk2-3725-4#show policy int multilink 2 | inc Class-map|Bandwidth
    Class-map: CALL-SETUP (match-any)
        Bandwidth 2 (%)
        Bandwidth 52 (kbps) Max Threshold 64 (packets)
    Class-map: INTERNETWORK-CONTROL (match-any)
        Bandwidth 5 (%)
        Bandwidth 130 (kbps) Max Threshold 64 (packets)
    Class-map: VOICE (match-all)
        Bandwidth 33 (%)
        Bandwidth 858 (kbps) Burst 21450 (Bytes)
    Class-map: TRANSACTIONAL-DATA (match-all)
        Bandwidth 22 (%)
        Bandwidth 572 (kbps) Max Threshold 64 (packets)
    Class-map: class-default (match-any)
```

The bandwidth values above are calculated from the derived multilink bandwidth:

```
vpn-jk2-3725-4#show int multilink 2 | inc BW
  MTU 1500 bytes, BW 2600 Kbit, DLY 100000 usec,
```

The multilink bandwidth is derived from the member links, which in this case are two serial interfaces:

```
vpn-jk2-3725-4#show interface serial 1/0 | inc BW
  MTU 1500 bytes, BW 1300 Kbit, DLY 20000 usec,
vpn-jk2-3725-4#show interface serial 1/1 | inc BW
  MTU 1500 bytes, BW 1300 Kbit, DLY 20000 usec,
```

If the second T1 is installed for availability rather than capacity, it is better to specify the voice and video bandwidth of the LLQ in absolute kbps values rather than a percentage.

For testing, three QoS service polices were tested. The legend on the chart lists them as default WRED, Tuned WRED, and Voice + Video Tuned WRED**.** These test iterations and their policy map configurations are shown in Table 10-2:

Table 10-2 QoS Service Policy Testing

Test Iteration	Policy Map

Default WRED	policy-map V3PN_Branch
	  class CALL-SETUP
	   bandwidth percent 2
	  class INTERNETWORK-CONTROL
	   bandwidth percent 5
	  class VOICE
	   priority percent 33
	  class TRANSACTIONAL-DATA
	   bandwidth percent 22
	  class class-default
	   fair-queue
	   random-detect

Tuned WRED	policy-map V3PN_Branch
	  class CALL-SETUP
	   bandwidth percent 2
	  class INTERNETWORK-CONTROL
	   bandwidth percent 5
	  class VOICE
	   priority percent 33
	  class TRANSACTIONAL-DATA
	   bandwidth percent 22
	  class class-default
	   fair-queue
	   random-detect dscp-based
	   random-detect dscp 0 4 10 10

Voice + Video Tuned WRED	policy-map V3PN_Branch
	  class CALL-SETUP
	   bandwidth percent 2
	  class INTERNETWORK-CONTROL
	   bandwidth percent 5
	  class VOICE
	   priority percent 18
	  class TRANSACTIONAL-DATA
	   bandwidth percent 22
	  class VIDEO-CONFERENCING
	   priority percent 15
	  class class-default
	   fair-queue
	   random-detect dscp-based
	   random-detect dscp 0 4 10 10

The rationale for testing the tuned Weighted Random Early Detection (WRED) was to apply the concept originally tested in the *Voice and Video Enabled IPSec VPN (V3PN) Design Guide,* (http://wwwin-eng.cisco.com/Eng/ESE/VPN/Design/V3PNDesignGuide.doc) where IPSec anti-replay drops were reduced by decreasing the queue-limit in the individual bandwidth classes from a default of 64 packets to much lower values.

Note See the *Voice and Video Enabled IPSec VPN (V3PN) Design Guide* at the following URL: http://www.cisco.com/en/US/netsol/ns340/ns394/ns430/networking_solutions_package.html

Because the **queue-limit** command is not germane with WRED enabled, the minimum and maximum thresholds for the best effort traffic in class default. The command format is the following:

```
random-detect dscp dscpvalue min-threshold max-threshold [mark-probability-denominator]
```

As can be seen in Table 10-2, the min-threshold was set at 4 packets, max-threshold was set at 10 packets, and the default of .1 or 10 percent was not changed.

With WRED enabled but using default values, no drops were encountered on the output service policy, with the min-threshold at 4 and max-threshold at 10. In general, the anti-replay drops decreased slightly and output interface queue drops were registered.

However, it is important to note that anti-replay drops on all tests, using Multilink PPP or Inverse Multiplexing over ATM (IMA) were always less than 1 percent of packets decrypted given these link speeds of 2.6–3 M. In these tests, the priority or LLQ does not exceed 33 percent of the link.

Table 10-3 shows the relevant performance metrics:

Table 10-3 Performance Metrics

Cisco 3725 Multilink PPP 2 links 2.6 Mbps total	Voice milliseconds[1]		Number data		CPU
	Jitter (goal <8)	Latency (goal< 50)	G.729 Calls	Mbps in/out	
Default WRED	2.4	7.9	15	2.4 M	28%
Tuned WRED	2.5	6.3	15	2.5 M	28%
Voice + Video Tuned WRED	2.3	6.7	8	3.4 M[2]	21%

[1] Branch to Head and Head to Branch values are averaged

[2] Video included in data Mbps values

In all three tests, voice jitter and latency was well below the testing goal of 8 ms and 50 ms respectively. Voice lost is not shown, but was approaching 0 percent in all tests.

The hardware encryption acceleration module was an AIM-VPN/EPII VPN Hardware Module. The router had 248832K/13312K bytes of memory.

Implementation and Configuration

This section describes the configuration for the components of the Multilink PPP solution, and includes the following sections:

- Remote Router
- Head-end Router

Remote Router

Following is the remote router configuration:

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

```
hostname vpn-jk2-3725-3
!
boot-start-marker
boot system flash:c3725-ik9o3s-mz.123-6
boot-end-marker
!
enable secret 5 [removed]
!
clock timezone est -5
clock summer-time edt recurring
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
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 po max-events 100
no ftp-server write-enable
!
!
class-map match-all VOICE
  match ip dscp ef
class-map match-all VIDEO-CONFERENCING
  match ip dscp af41
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_Branch
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class VOICE
   priority percent 18        # See previous section for changes between test iterations
  class TRANSACTIONAL-DATA
   bandwidth percent 22
  class VIDEO-CONFERENCING
   priority percent 15
  class class-default
   fair-queue
   random-detect dscp-based
   random-detect dscp 0   4     10    10
!
!
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
!
crypto isakmp peer address 192.168.255.3
 set aggressive-mode password 77-80-69_24.1_WW-748
 set aggressive-mode client-endpoint fqdn Store_223.ese.cisco.com
crypto isakmp profile AGGRESSIVE
   description _
   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
no crypto ipsec nat-transparency udp-encaps
!
crypto map PRIMARY_LINK 1 ipsec-isakmp
 description Crypto Map for Primary Path
 set peer 192.168.255.3
 set transform-set 3DES_SHA_TUNNEL
 match address GRE_MAP_ACL
 qos pre-classify
!
interface Loopback0
 description lo0
 ip address 10.0.80.254 255.255.255.255
!
interface Multilink2
 description Multilink2
 bandwidth 2600                      # See V3PN Service Policy Section
 ip address 192.168.193.18 255.255.255.252
 service-policy output V3PN_Branch
 ip route-cache flow
 load-interval 30
 ppp multilink
 ppp multilink slippage msec 26
 ppp multilink links minimum 2
 ppp multilink group 2
 crypto map PRIMARY_LINK
!
interface Tunnel0
 description Tunnel0                 # Note no crypto map on Tunnel interface
 ip address 10.0.80.250 255.255.255.252
 qos pre-classify
 keepalive 10 3                      # No routing protocol configured,
!                                    # rather GRE keepalive
 tunnel source Loopback0
 tunnel destination 192.168.255.3
!
interface FastEthernet0/1
 description FastEthernet0/1
 no ip address
 ip route-cache flow
 load-interval 30
 duplex auto
 speed auto
!
interface FastEthernet0/1.212
 description FastEthernet0/1.212
 encapsulation dot1Q 212
 ip address 10.0.80.1 255.255.255.128
!
interface Serial1/0
```

```
 description Serial1/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 2
!
interface Serial1/1
 description Serial1/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 2
!
ip http server
no ip http secure-server
ip classless
!      No routing protocol configured on this router.
ip route 0.0.0.0 0.0.0.0 Multilink2 249
ip route 10.3.0.0 255.255.255.128 Tunnel0 237
!
ip access-list extended CRYPTO_MAP_ACL
 permit ip 10.0.80.0 0.0.0.127 any
ip access-list extended GRE_MAP_ACL
 permit gre host 10.0.80.254 host 192.168.255.3
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
!
snmp-server community private RW
snmp-server community public RO
snmp-server system-shutdown
snmp-server enable traps tty
!
!
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
 password 7 [removed]
 login
 transport preferred all
 transport input all
 transport output all
!
ntp source FastEthernet0/1.212
!
end
```

Head-end Router

Following is the head-end router configuration:

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname vpn-jk2-3725-4
```

```
!
boot-start-marker
boot system flash:c3725-ik9o3s-mz.123-6
boot-end-marker
!
enable secret 5 [removed]
!
clock timezone est -5
clock summer-time edt recurring
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
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 po max-events 100
no ftp-server write-enable
!
!
class-map match-all VOICE
  match ip dscp ef
class-map match-all VIDEO-CONFERENCING
  match ip dscp af41
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_Branch        # See comments in remote router’s policy-map configuration
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class VOICE
   priority percent 18
  class TRANSACTIONAL-DATA
   bandwidth percent 22
  class VIDEO-CONFERENCING
   priority percent 15
  class class-default
   fair-queue
   random-detect dscp-based
   random-detect dscp 0   4     10    10
!
!
crypto keyring Purple_Stores
  pre-shared-key hostname Store_223.ese.cisco.com  key 77-80-69_24.1_WW-748
!
crypto isakmp policy 20
```

```
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
crypto isakmp profile AGGRESSIVE
   description _
   keyring Purple_Stores
   self-identity fqdn
   match identity host domain ese.cisco.com
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto dynamic-map DYNO-TEMPLATE 10   # Dynamic Crypto Maps with GRE and IKE Aggressive
 description dynamic crypto map       # mode in this configuration
 set transform-set 3DES_SHA_TUNNEL
 qos pre-classify
!
!
crypto map DYNO-MAP local-address Loopback0
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
!
!
interface Loopback0
 description lo0
 ip address 192.168.255.3 255.255.255.255
!
interface Multilink2
 description Multilink2
 bandwidth 2600
 ip address 192.168.193.17 255.255.255.252
 service-policy output V3PN_Branch
 ip route-cache flow
 load-interval 30
 ppp multilink
 ppp multilink slippage msec 26
 ppp multilink links minimum 2
 ppp multilink group 2
 crypto map DYNO-MAP
!
interface Tunnel0
 description Tunnel0
 ip address 10.0.80.249 255.255.255.252
 qos pre-classify
 keepalive 10 3
 tunnel source Loopback0
 tunnel destination 10.0.80.254
!
interface FastEthernet1/0
 description dot1q
 no ip address
 ip route-cache flow
 load-interval 30
 duplex auto
 speed auto
!
interface FastEthernet1/0.128
 encapsulation dot1Q 128
 ip address 10.2.128.3 255.255.255.0
!
interface Serial1/0
 description Serial1/0
 no ip address
 encapsulation ppp
 clockrate 1300000
 ppp multilink
 ppp multilink group 2
!
interface Serial1/1
 description Serial1/1
 no ip address
 encapsulation ppp
 clockrate 1300000
 ppp multilink
 ppp multilink group 2
!
router eigrp 100
 redistribute static metric 2600 1000 255 1 1500 route-map PERMIT_80
 network 10.0.0.0
!       # We should have included a passive interface command
!       # because we are not expecting to form a neighbor relationship
!       # across the GRE tunnel
 distribute-list 10 in FastEthernet1/0.128
 no auto-summary
 no eigrp log-neighbor-warnings
!
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Multilink2 249
ip route 10.0.80.0 255.255.255.128 Tunnel0 237
!
!
!
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
access-list 10 permit 10.3.0.0
access-list 10 deny   any
access-list 80 permit 10.0.80.0
!
route-map PERMIT_80 permit 10
 description To only allow 10.0.80.0/24
 match ip address 80
!
snmp-server community private RW
snmp-server community public RO
snmp-server system-shutdown
snmp-server enable traps tty
!
!
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
 password 7 [removed]
 login
 transport preferred all
 transport input all
 transport output all
!
ntp server 192.168.130.1
!
```

```
end
```

Show Commands

According to the interface counters, the interface is running in the 80–84 percent utilization range with a load interval of 30 seconds.

```
Multilink2 is up, line protocol is up
  Hardware is multilink group interface
  Description: Multilink2
  Internet address is 192.168.193.18/30
  MTU 1500 bytes, BW 2600 Kbit, DLY 100000 usec,
     reliability 255/255, txload 207/255, rxload 214/255
  Encapsulation PPP, LCP Open, multilink Open
  Open: CDPCP, IPCP, loopback not set
  DTR is pulsed for 2 seconds on reset
  Last input 00:00:07, output never, output hang never
  Last clearing of "show interface" counters 00:02:25
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1570
  Queueing strategy: weighted fair
  Output queue: 6/1000/64/1570 (size/max total/threshold/drops)
     Conversations  1/4/256 (active/max active/max total)
     Reserved Conversations 3/3 (allocated/max allocated)
     Available Bandwidth 338 kilobits/sec
  30 second input rate 2185000 bits/sec, 683 packets/sec
  30 second output rate 2111000 bits/sec, 682 packets/sec
     99861 packets input, 39534594 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     100101 packets output, 39145904 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions


show policy int
 Multilink2

  Service-policy output: V3PN_Branch

    Class-map: CALL-SETUP (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af31
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: ip dscp cs3
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
        Output Queue: Conversation 265
        Bandwidth 2 (%)
        Bandwidth 52 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: INTERNETWORK-CONTROL (match-any)
      76 packets, 7664 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp cs6
        76 packets, 7664 bytes
        30 second rate 0 bps
      Match: access-group name IKE
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
        Output Queue: Conversation 266
        Bandwidth 5 (%)
        Bandwidth 130 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 15/1256
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: VOICE (match-all)
      58160 packets, 5118080 bytes
      30 second offered rate 282000 bps, drop rate 0 bps
      Match: ip dscp ef
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 18 (%)
        Bandwidth 468 (kbps) Burst 11700 (Bytes)
        (pkts matched/bytes matched) 58152/8141280
        (total drops/bytes drops) 0/0

    Class-map: TRANSACTIONAL-DATA (match-all)
      278 packets, 162904 bytes
      30 second offered rate 10000 bps, drop rate 0 bps
      Match: ip dscp af21
      Queueing
        Output Queue: Conversation 267
        Bandwidth 22 (%)
        Bandwidth 572 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 278/178472
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: VIDEO-CONFERENCING (match-all) # See Caveats in this section!
      8746 packets, 5133902 bytes
      30 second offered rate 252000 bps, drop rate 9000 bps
      Match: ip dscp af41
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 15 (%)
        Bandwidth 390 (kbps) Burst 9750 (Bytes)
        (pkts matched/bytes matched) 8746/5632424
        (total drops/bytes drops) 630/405720

    Class-map: class-default (match-any)
      34005 packets, 24847658 bytes
      30 second offered rate 1404000 bps, drop rate 51000 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 256
        (total queued/total drops/no-buffer drops) 2/962/0
         exponential weight: 9

   dscp    Transmitted      Random drop      Tail drop    Minimum Maximum  Mark
           pkts/bytes       pkts/bytes       pkts/bytes    thresh  thresh  prob
   af11       0/0              0/0              0/0           32      40  1/10
   af12       0/0              0/0              0/0           28      40  1/10
   af13       0/0              0/0              0/0           24      40  1/10
   af21       0/0              0/0              0/0           32      40  1/10
   af22       0/0              0/0              0/0           28      40  1/10
```

```
   af23     0/0              0/0             0/0             24      40  1/10
   af31     0/0              0/0             0/0             32      40  1/10
   af32     0/0              0/0             0/0             28      40  1/10
   af33     0/0              0/0             0/0             24      40  1/10
   af41     0/0              0/0             0/0             32      40  1/10
   af42     0/0              0/0             0/0             28      40  1/10
   af43     0/0              0/0             0/0             24      40  1/10
    cs1     0/0              0/0             0/0             22      40  1/10
    cs2     0/0              0/0             0/0             24      40  1/10
    cs3     0/0              0/0             0/0             26      40  1/10
    cs4     0/0              0/0             0/0             28      40  1/10
    cs5     0/0              0/0             0/0             30      40  1/10
    cs6    23/2912           0/0             0/0             32      40  1/10
    cs7     0/0              0/0             0/0             34      40  1/10
     ef     0/0              0/0             0/0             36      40  1/10
   rsvp     0/0              0/0             0/0             36      40  1/10
default   33049/25916882   963/825988        0/0              4      10  1/10
```

See caveats following this section.

Cisco IOS Versions Tested

The following Cisco IOS version was tested: Cisco 3725—c3725-ik9o3s-mz.123-6

Caveats

This section describes the caveats to the Multilink PPP solution, and includes the following topics:

- Drops In Class VIDEO-CONFERENCING
- Incorrect Packet Classification

Drops In Class VIDEO-CONFERENCING

In Show Commands, page 10-14, packet loss in the video class was observed during performance testing. Upon further analysis and testing, it was determined that the drops resulted from a testing anomaly and not a Cisco IOS or configuration issue. Recall from the previous discussion on the Chariot video test stream that the size of the stream was configured at 2,088,000 bytes. At the 256 kbps data rate, this simulates a video conference that has a duration of approximately one minute. Chariot then restarts the simulated video stream and then again the second stream lasts approximately one minute. This sequence of events continues for the duration of the test. For a ten minute test, there might be 9–10 individual video streams during the test.

The packet loss experienced occurred at the end of the Chariot stream. In most cases, for the duration of the test, the video packet loss ranged from 3–7 percent. After this behavior was determined, the size of the Chariot video stream was increased to simulate a video conference that would last the duration of the test. In this mode, the video packet loss was negligible. The packet loss goal for an interactive video conference is less than 1 percent.

```
vpn-jk2-3725-4#sh pol int mu 2 output class VIDEO-CONFERENCING
 Multilink2

  Service-policy output: V3PN_Branch
```

```
Class-map: VIDEO-CONFERENCING (match-all)
  19163 packets, 11245772 bytes
  30 second offered rate 252000 bps, drop rate 1000 bps
  Match: ip dscp af41
  Queueing
    Strict Priority
    Output Queue: Conversation 264
    Bandwidth 15 (%)
    Bandwidth 390 (kbps) Burst 9750 (Bytes)
    (pkts matched/bytes matched) 19168/12338456
    (total drops/bytes drops) 16/10304
```

The 16 packets dropped in this test all occurred in the last few seconds of the video stream when the session was closing, so this loss behavior is thus marked against the test tool and is not an issue with Cisco IOS or configuration.

Incorrect Packet Classification

In Show Commands, page 10-14, the QoS service policy includes a class for INTERNETWORK-CONTROL that includes a match for a Differentiated Services Code Point (DSCP) value of CS6. Note that in the same display under class class-default, the WRED display indicates there are matches for CS6. This is a classification issue because these packets are in class default and not in the bandwidth class INTERNETWORK-CONTROL. These classification issues may be related to sCSCed61266, CSCea77121, or CSCdz62381.

Summary

This chapter includes performance results and configuration examples for features that have not been tested by ESE to date. These include interactive video conferencing in the traffic profile and the use of Multilink PPP for data rates above E1 but less than T3. WRED has also been included in class default, where the initial V3PN site-to-site testing used a fair queue configuration. Tuning the WRED parameters was also tested. Although various router hardware platforms were not exhaustively tested (only the Cisco 3725 was tested), the viability of encrypted voice and video was demonstrated. Also, note that the incidence of anti-replay drops in a higher data rate multilink configuration exhibits similar characteristics to the sub-E1/T1 rates previously tested.

CHAPTER 11

Large Branch—Inverse Multiplexing over ATM (IMA)

This configuration is similar to Chapter 10, "Large Branch—Multilink PPP." This chapter substitutes the previous solution of Multilink PPP (over two serial T1 links) with Inverse Multiplexing over ATM (IMA) using a bundle of two ATM circuits, and shows only the relevant configuration portions and performance results.

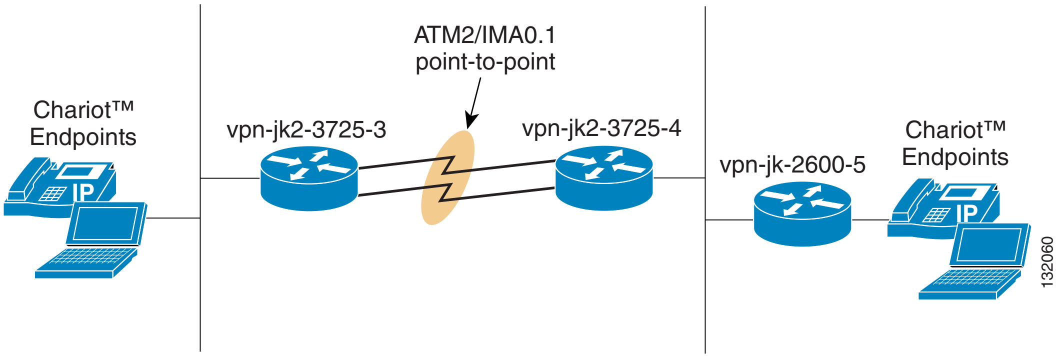
This chapter includes the following sections:

- Topology
- Implementation and Configuration
- Performance
- Summary

Topology

The topology is identical to the previous section with the exception of replacing the Multilink PPP configured dual serial links with IMA adapters. (See Figure 11-1.)

Figure 11-1 Large Branch—ATM (IMA)



Implementation and Configuration

This section describes the configuration of the components of the inverse multiplexing over ATM (ATA) solution.

Head-end Router

Following is the head-end router configuration:

```
!
hostname vpn-jk2-3725-4
!
interface ATM2/0
 description ATM2/0
 no ip address
 no atm ilmi-keepalive
 ima-group 0
 clock source internal
 no scrambling-payload
!
interface ATM2/1
 description ATM2/1
 no ip address
 no atm ilmi-keepalive
 ima-group 0
 clock source internal
 no scrambling-payload
!
interface ATM2/2
 no ip address
 shutdown
 no atm ilmi-keepalive
 clock source internal
 no scrambling-payload
!
interface ATM2/3
 no ip address
 shutdown
 no atm ilmi-keepalive
 clock source internal
 no scrambling-payload
!
interface ATM2/IMA0
 description ATM2/IMA0
 no ip address
 ip route-cache flow
 load-interval 30
 no atm ilmi-keepalive
 ima active-links-minimum 2
 ima clock-mode common 0
 ima differential-delay-maximum 26       # Default value is 25ms, 26 used so it will
!                                        # show in the configuration
interface ATM2/IMA0.1 point-to-point
 description ATM2/IMA0.1
 bandwidth 3072
 ip address 192.168.193.13 255.255.255.252
 crypto map DYNO-MAP                  # Same dynamic crypto map/tunnel interface as MLPPP
 pvc YELLOW 0/100
  vbr-nrt 3072 3072                   # Highest value supported.
  oam-pvc manage
  oam retry 5 5 5
  service-policy output V3PN_Branch          # Same as MLPPP
 !
!
ip route 0.0.0.0 0.0.0.0 ATM2/IMA0.1 250
ip route 10.0.80.0 255.255.255.128 Tunnel0 237
...
end
```

Remote Router

Following is the remote router configuration:

```
!
hostname vpn-jk2-3725-3
!
interface ATM2/0
 description ATM2/0
 no ip address
 no atm ilmi-keepalive
 ima-group 0
 no scrambling-payload
!
interface ATM2/1
 description ATM2/1
 no ip address
 no atm ilmi-keepalive
 ima-group 0
 no scrambling-payload
!
interface ATM2/2
 no ip address
 shutdown
 no atm ilmi-keepalive
 no scrambling-payload
!
interface ATM2/3
 no ip address
 shutdown
 no atm ilmi-keepalive
 no scrambling-payload
!
interface ATM2/IMA0
 description ATM2/IMA0
 no ip address
 ip route-cache flow
 load-interval 30
 no atm ilmi-keepalive
 ima active-links-minimum 2
 ima clock-mode common 0
 ima differential-delay-maximum 26
!
interface ATM2/IMA0.1 point-to-point
 description ATM2/IMA0.1
 bandwidth 3072
 ip address 192.168.193.14 255.255.255.252
 crypto map PRIMARY_LINK
 pvc YELLOW 0/100
  vbr-nrt 3072 3072
  oam-pvc manage
  oam retry 5 5 5
  service-policy output V3PN_Branch
 !
!
ip route 0.0.0.0 0.0.0.0 ATM2/IMA0.1 250
ip route 10.3.0.0 255.255.255.128 Tunnel0 237
end
```

Performance

The performance results shown in Table 11-1 were produced using similar traffic profiles and QoS policies as described in Chapter 10, “Large Branch—Multilink PPP.”

Table 11-1 3725 ATM IMA Performance

Cisco 3725 ATM/ATA 2 links 3072 Kbps total	Voice milliseconds		Number data		CPU
	Jitter (goal <8)	Latency)goal< 50)	G.729 Calls	Mbps in/out	
Default WRED	5.4	16.7	15	2.9M	22%
Tuned WRED	5.3	14.1	15	2.9M	23%
Voice + Video Tuned WRED	4.7	14.4	9	3.9M	19%

Because the amount of raw bandwidth was slightly higher in the IMA configuration, one additional voice call was added in the IMA voice and video test. The Chariot test for the IMA testing included proportionally more flows of the same applications as well.

In the PVC configuration for the IMA subinterface, the vbr-nrt parameter was configured at the highest configurable value, 3072 kbps, while the Multilink PPP interfaces were clocked individually at 1,300,000. This difference accounts for the slightly higher throughput of data in the test results. However recall that the ATM cell tax is appreciable higher than the overhead associated with Multilink PPP, so that the gain in bandwidth is offset to some extent.

It should be noted that although the voice latency in these tests was well within the goal of being less than 50 ms, it was higher than the Multilink PPP values. However overall CPU averaged lower.

Summary

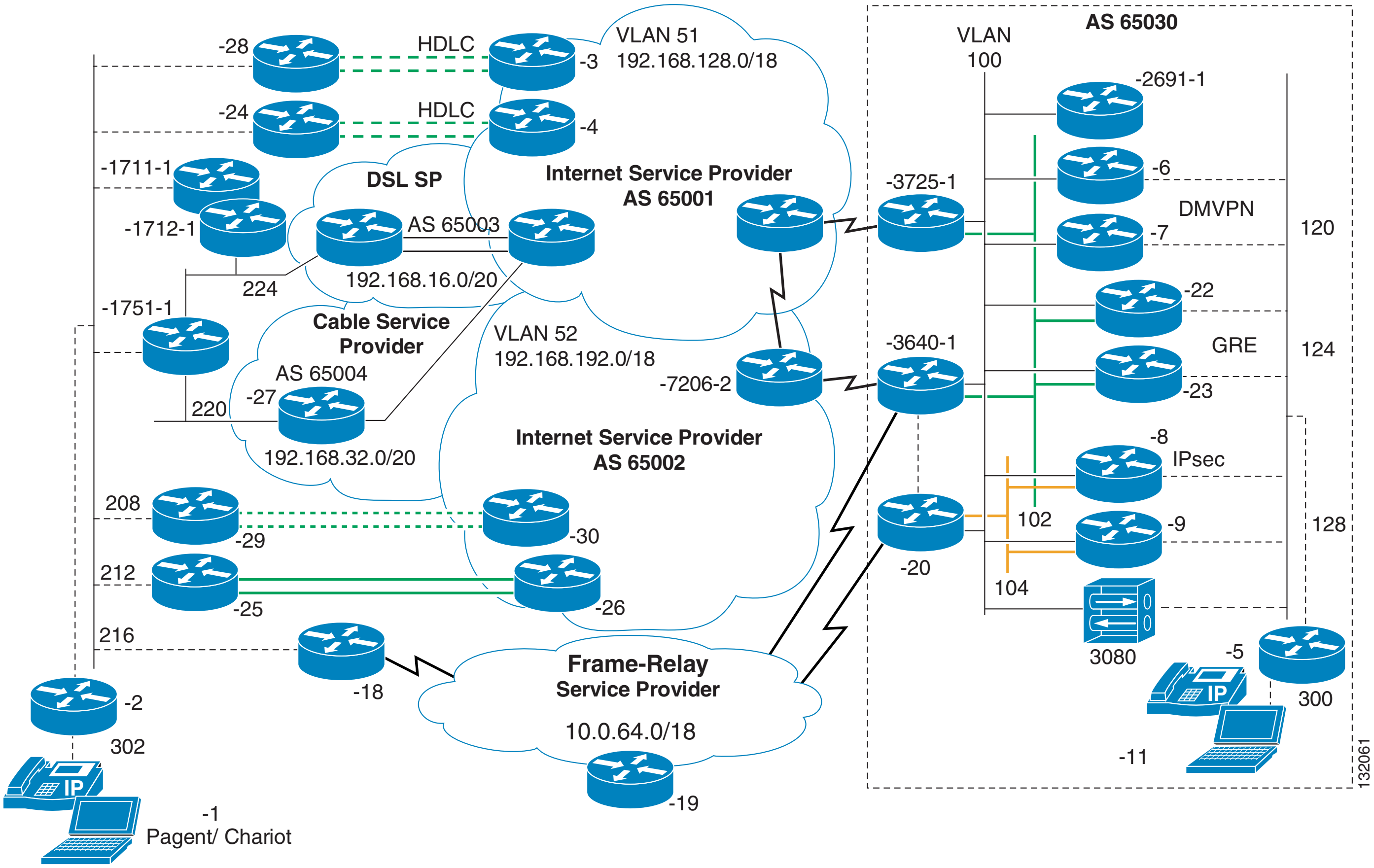
These performance results along with the Multilink PPP results demonstrate the viability of V3PN with data rates above E1.

APPENDIX A

Lab Topology

Figure A-1shows the lab topology used as the basis for this design guide.

Figure A-1 Lab Topology



APPENDIX B

References and Reading

This section includes references to resources for more information.

Documents

For best-practice information on designing and implementing enterprise IP Security (IPSec) virtual private networks (VPNs), see "SAFE VPN: IPSec Virtual Private Networks in Depth" at the following URL:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2d.shtml

- AVVID QoS Quick Reference Guide—EDCS-118535

Request For Comment Papers

- RFC897—The TCP Maximum Segment Size and Related Topics
- RFC1191—Path MTU Discovery
- RFC1889—RTP: A Transport Protocol for Real-Time Applications
- RFC2516—Transmitting PPP Over Ethernet
- RFC2401—Security Architecture for the Internet Protocol
- RFC2402—IP Authentication Header
- RFC2403—The Use of HMAC-MD5-96 within ESP and AH
- RFC2404—The Use of HMAC-SHA-1-96 within ESP and AH
- RFC2405—The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC2406—IP Encapsulating Security Payload (ESP)
- RFC2407—The Internet IP Security Domain of Interpretation for ISAKMP
- RFC2408—Internet and Key Management Protocol (ISAKMP)
- RFC2409—The Internet Key Exchange (IKE)
- RFC2410—The NULL Encryption Algorithm and Its Use With IPsec
- RFC2411—IP Security Document Roadmap
- RFC2412—The OAKLEY Key Determination Protocol

Websites

Enterprise Solutions Engineering (ESE)

- Enterprise Solutions Engineering (ESE)—http://wwwin.cisco.com/ent/ese/
- Cisco AVVID Common Infrastructure—http://wwwin.cisco.com/ent/ese/cani/campus/
- Cisco AVVID VPN Solution—http://wwwin.cisco.com/ent/ese/cani/vpn/
- Cisco AVVID IP Telephony Solution—http://wwwin.cisco.com/ent/ese/solutions/voice/
- Cisco AVVID Wireless LAN Solution—http://wwwin.cisco.com/ent/ese/cani/wireless/
- Enterprise VPNs—http://www.cisco.com/go/evpn
- Cisco SAFE Blueprint—http://www.cisco.com/go/safe
- Cisco Network Security—http://www.cisco.com/go/security
- Cisco AVVID Partner Program—http://www.cisco.com/go/securityassociates
- Cisco VPN Product Documentation—http://www.cisco.com/univercd/cc/td/doc/product/vpn/
- Download VPN Software from CCO—http://www.cisco.com/kobayashi/sw-center/sw-vpn.shtml
- Improving Security on Cisco Routers—http://www.cisco.com/warp/public/707/21.html
- Essential IOS Features Every ISP Should Consider—http://www.cisco.com/warp/public/707/EssentialIOSfeatures_pdf.zip
- Increasing Security on IP Networks—http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_package.html
- Security and VPN Support Resources—http://www.cisco.com/en/us/partner/hw/vpndevc/tsd_products_support_category_home.html
- IPSec Negotiation/IKE Protocols—http://www.cisco.com/en/US/tech/tk583/tk372/tsd_technology_support_protocol_home.html
- Networking Professionals Connection—http://forums.cisco.com
- NetFlow—http://www.cisco.com/go/netflow

APPENDIX C

Acronyms and Definitions

Term	Definition
3DES	Triple Data Encryption Standard
ACL	Access control list
AES	Advanced Encryption Standard
AH	Authentication header
AIM	Advanced Integration Module
ATM	Asynchronous Transfer Mode
AVVID	Architecture for Voice, Video, and Integrated Data
CA	Certificate authority
CAC	Call Admission Control
CANI	Cisco AVVID Network Infrastructure
CAR	Committed access rate
CBWFQ	Class Based Weighted Fair Queuing
CEF	Cisco Express Forwarding
CPE	Customer premises equipment
cRTP	Compressed Real-Time Protocol
DES	Data Encryption Standard
DLSw	Data link switching
DMZ	De-militarized zone
DNS	Domain Name Service
DSL	Digital Subscriber Line
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Protocol
FIFO	First in first out
FR	Frame Relay
FRTS	Frame Relay Traffic Shaping
FTP	File Transfer Protocol
GRE	Generic route encapsulation

Term	Definition
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IP	Internet Protocol
IPMc	IP Multicast
IPSec	IP Security
IP GRE	See GRE
ISA	Integrated Service Adapter
ISM	Integrated Service Module
ISP	Internet Service Provider
Layer 2	OSI reference model Link layer
Layer 3	OSI reference model Network layer
Layer 4	OSI reference model Transport Layer
LFI	Link Fragmentation and Interleaving
LLQ	Low Latency Queuing
L2TP	Layer 2 Tunneling Protocol
MDRR	Modified Deficit Round Robin
MLPPP	Multi-link Point-to-point Protocol
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NetFlow	Cisco IOS component, collects and exports traffic statistics
OSPF	Open Shortest Path First
PAT	Port Address Translation
PBR	Policy-Based Routing
PE	Premises equipment
PPTP	Point-to-Point Tunneling Protocol
PVC	Permanent virtual circuit
QoS	Quality of service
RTP	Real-Time Protocol
SA	Security association
SHA-1	Secure Hash Algorithm One
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOHO	Small office/home office
SRST	Survivable Remote Site Telephony
TCP	Transmission Control Protocol
TED	Tunnel Endpoint Discovery

Term	Definition
ToS	Type of service
UDP	User Datagram Protocol
VAD	Voice Activity Detection
VoIP	Voice over IP
V^{3}PN	Voice and Video Enabled IPSec VPN
VAM	VPN Acceleration Module
VPN	Virtual private network
WAN	Wide area network
WRED	Weighted Random Early Detection