Virtual Tunnel Interface (VTI) Design Guide

This design guide is written for systems engineers and support engineers to provide guidelines and best practices for deploying virtual tunnel interfaces (VTIs).

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. It identifies the individual hardware requirements and their interconnections, software features, management needs, and partner dependencies. This helps a customer deploy a manageable and maintainable enterprise VPN solution. It is assumed that the reader has a basic understanding of IP Security (IPsec).

This design guide is part of an ongoing series that addresses VPN solutions, using the latest VPN technologies from Cisco, and based on practical, tested designs.

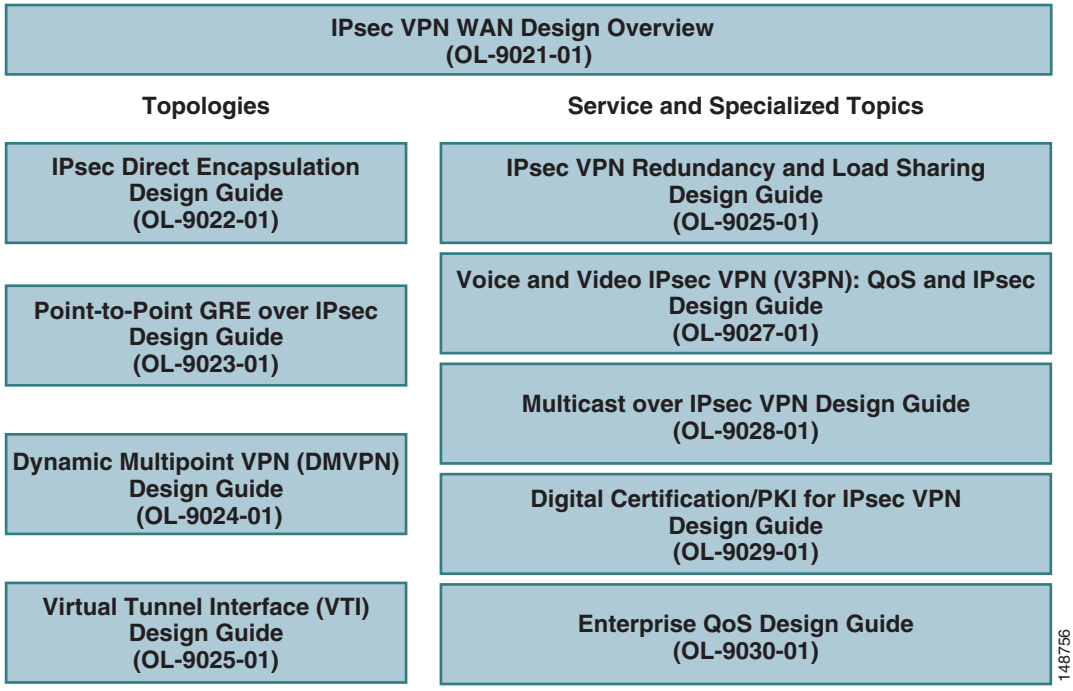
Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The IPsec VPN wide area network (WAN) architecture is described in multiple design guides based on the type of technology used, as shown by the list in Figure 1:

Figure 1 IPsec VPN WAN Design Guides



Each technology uses IPsec as the underlying transport mechanism for each VPN. The operation of IPsec is outlined in the *IPsec VPN WAN Design Overview*, which also outlines the criteria for selecting a specific IPsec VPN WAN technology. This document should be used to select the correct technology for the proposed network design.

This design guide builds on the following series of design guides, which are available at http://cco.cisco.com/go/srnd/:

- *Voice and Video Enabled IPsec VPN (V3PN) Design Guide*
- *Enterprise Class Teleworker: V3PN for Teleworkers Design Guide*

- *Enterprise Class Teleworker: Teleworker Design Guide*
- *IPsec V3PN: Redundancy and Load Sharing*

This design guide is based on Cisco VPN routers running Cisco IOS software, with IPsec as the tunneling method, using site-to-site VPN topologies. This guide helps evaluate Cisco VPN product performance in scalable and resilient designs and addresses the following applications of the solution:

- Dead Peer Detection (DPD)
- Converged data and VoIP traffic requirements
- Quality of service (QoS) features enabled
- Use of Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) as the routing protocol across the VPN

Design Overview

This section provides an overview of the design considerations when implementing VTIs.

Starting Assumptions

Enterprise customers deploy IPsec-based VPNs over public and private networks for secrecy, authentication, and data integrity. However, IPsec is viewed as a tunnel between two IPsec peers regardless of the underlying WAN transport.

A VTI is an interface that supports native IPsec tunneling, and allows you to apply interface commands directly to the IPsec tunnels. The configuration of this tunnel interface is similar to a GRE tunnel interface and is well understood.

A VTI has most of the properties of a physical interface. It provides a comprehensive solution, creating dynamic virtual tunnel interfaces (similar to what is currently done in the dialup world) to enable the deployment of large-scale IPsec networks with minimal configuration.

The design approach presented in this design guide makes several starting assumptions.

- All performance tests were executed with the following:
  - A hierarchical Class-Based Weighted Fair Queuing (CBWFQ), which provides queuing within a shaped rate, on the VTI interface pre-crypto on both headend and branch routers
  - Dynamic VTI (DVTI) on headend crypto systems, and static VTI on the branches
- The design supports a typical converged traffic profile for customers (see Scalability Test Results (Unicast Only), page 54).
- It is assumed that the customer has a need for diverse traffic requirements, such as IP multicast (IPmc), and support for routing. The use of VTI and routing protocols are also discussed in more detail in Design and Implementation, page 11.
- Cisco products should be maintained at reasonable CPU utilization levels. This is discussed in more detail in Scalability Considerations, page 51, including recommendations for both headend and branch routers, and software revisions.
- Although costs are certainly considered, the design recommendations assume that the customer deploys current VPN technologies, including hardware-accelerated encryption.

- Voice over IP (VoIP) and video are assumed to be requirements in the network. Detailed design considerations for handling VoIP and other latency-sensitive traffic are not explicitly addressed in this design guide, but may be found in *Voice and Video Enabled IPsec VPN (V3PN) Design Guide* at the following URL: http://www.cisco.com/go/srnd
- This design is targeted for deployment by enterprise-owned VPNs. However, the concepts and conclusions are valid regardless of the ownership of the edge tunneling equipment, and are therefore valuable for service provider-managed VPNs as well.

Design Components

VPNs have many applications, including extending reachability of an enterprise WAN, or replacing classic WAN technologies such as leased lines, Frame Relay, and ATM. Site-to-site VPNs are primarily deployed to connect branch office locations to the central site (or sites) of an enterprise.

The requirements of enterprise customers for traditional private WAN services, such as high availability, scalability, and security, are also requirements for VPNs. VPNs can often meet these requirements more cost effectively and with greater flexibility than private WAN services.

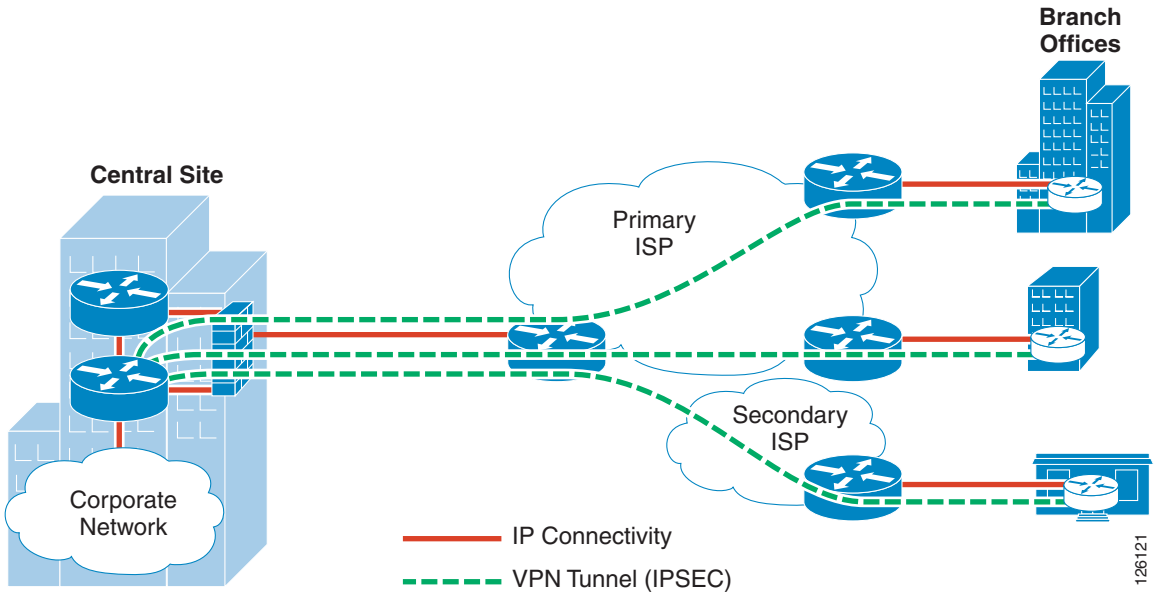
The key components of this site-to-site VPN design are the following:

- Cisco high-end VPN routers serve as VPN headend termination devices at a central campus (headend devices)
- Cisco VPN access routers serve as VPN branch termination devices at branch office locations (branch devices)
- Dynamic VTI (DVTI) performs headend-to-branch interconnections
- Internet services are provided by a third-party ISP (or ISPs) serving as the WAN interconnection medium

Cisco VPN routers are a good choice for site-to-site VPN deployments because they can accommodate any network requirement inherited from a Frame Relay or private line network, such as support for multicast and latency-sensitive traffic, and routing for resiliency. See Scalability Considerations, page 51 for a discussion about selecting headend and branch products.

In a VTI design, a hub-and-spoke topology is used, as shown in Figure 2.

Figure 2 Hub-and-Spoke Topology



Comparing DVTI with other VPN Topologies

Table 1 shows a comparison of DVTI with other VPN topologies for a headend deployment.

Table 1 Dynamic Virtual Tunnel Interface (DVTI)

	Common Features	Advantages	Disadvantages
IPsec Direct Encapsulation (Dynamic crypto map)	Simple configuration of headend "once and done" • DVTI uses virtual templates • IPsec uses dynamic crypto maps	Support for IPmc Support for IGP dynamic routing protocol over the VPN (EIGRP or OSPF, and so forth) Support for per-branch QoS and traffic shaping (pre-crypto)	Larger packet header bloat: • VTI = +4 bytes • IPsec = +0 bytes DVTI requires IP unnumbered
p2p GRE over IPsec (p2p GRE over an IPsec dynamic crypto map)	Support for IPmc Support for IGP dynamic routing protocol over the VPN (EIGRP or OSPF, and so forth) Support for per branch QoS and traffic shaping (pre-crypto)	Backward compatibility with IPsec direct encapsulation branches Smaller packet header bloat: • VTI = +4 bytes • p2p GRE = +24 bytes Simple configuration of headend "once and done" • DVTI uses virtual templates • p2p GRE uses statically defined independent tunnel interfaces per branch	No support for non-IP protocol (multiprotocol) No support for IPsec transport mode DVTI requires IP unnumbered
DMVPN (hub-and-spoke)	Support for IPmc Support for IGP dynamic routing protocol over the VPN (EIGRP or OSPF, and so forth) Supports only IPsec tunnel mode Simple configuration of headend "once and done" • DVTI uses virtual templates • DMVPN uses a common mGRE interface	Backward compatibility with IPsec direct encapsulation branches Smaller packet header bloat: • VTI = +4 bytes • mGRE = +28 bytes Support for per branch QoS and traffic shaping (pre-crypto) No NHRP required	DVTI requires IP unnumbered

Understanding Scalability Results

In the Cisco test lab, all headend scalability results were performed on a Cisco 7200VXR with NPE-G1 with Dual SA-VAM2. Results were obtained with an LLQ service policy with Generic Traffic Shaping applied per virtual access or branch tunnel interface. The rationale for this testing methodology was to find out the scalability of the platform with the service policies applied to the following issues:

- Removing anti-replay issues induced by the crypto routers
- Gaining the ability to shape per tunnel to avoid overrunning the branch router downlink speed

The current performance results proved less than desirable. The primary reason for this degradation is because of the Generic Traffic Shaping feature being process-switched and CPU-intensive. Note that in a p2p GRE over IPsec design, if the identical service policies are applied to the same number of p2p GRE tunnel interfaces, the performance would likely be similar. The impact of queuing on performance is described later in this document.

Best Practices and Known Limitations

The following sections contain a summary of the best practices and limitations for the design. More detailed information is provided in Design and Implementation, page 11.

Best Practices Summary

This section summarizes the best practices for a VTI deployment.

General Best Practices

The following are general best practices:

- When using Traffic Shaping on a tunnel interface or a virtual template interface, *do not* use the **qos pre-classify** command because it is not required or useful in this topology.
- Headend and branch routers should use the “ip unnumbered” interface in their VTI configurations.
- If EZVPN is configured on the branch router, see EZVPN Remote Client—Mode Network-Plus, page 22 for implementation details.
- Use PKI/Digital Certificates or IKE aggressive mode as the IKE authentication method.
- Use IPsec tunnel mode for transform sets in IPsec.
- Configure Triple DES (3DES) or AES for encryption of transported data (exports of encryption algorithms to certain countries may be prohibited by law).
- Implement DPD to detect loss of communication between crypto peers.
- Deploy hardware-acceleration of IPsec to minimize router CPU overhead, to support traffic with low-latency/jitter requirements, and for the highest performance for cost.
- Keep IPsec packet fragmentation to a minimum on the customer network by setting MTU size or using Path MTU Discovery (PMTUD).
- Configure a routing protocol (for example, EIGRP or OSPF) with route summarization for dynamic routing.

Headend Best Practices

The following are best practices that should be implemented on the headend device:

- Create a virtual template for each unique branch characteristic so that branches that share these characteristics can all reference the appropriate common virtual template.
- Summarize network advertisements to the fullest extent possible on the virtual template.
- Use a loopback interface address as the “borrowed” address for the “ip unnumbered” interface configuration on the virtual template. All configured virtual templates may reference the same loopback.
- If high availability is a requirement, implement a design with redundancy of headend equipment and WAN circuits.
- Distribute branch office tunnels across a number of headend routers to balance loading and aggregation capacity of the hub(s).
- Select Cisco VPN router products at the headend based on considerations for the following:
  - Number of tunnels to be aggregated
  - Maximum throughput in both pps and bps to be aggregated
  - Performance margin for resiliency and failover scenarios
  - Maintaining CPU utilization below design target
  - Whether a traffic shaper is applied “pre-crypto”

See Scalability Considerations, page 51 for more information.

Branch Office Best Practices

The following are best practices that should be implemented on the branch office device:

- If EIGRP is the routing protocol, EIGRP Stub should be configured
- If the inside LAN interface is the “borrowed” address for the “ip unnumbered” interface configuration of the tunnel interface, disable interface keepalives (**no keep**) so the interface line protocol is always up. For branch routers with VLAN interfaces, an Ethernet crossover cable connecting two switch ports ensures that the VLAN interface line protocol is up.
- Configure multiple VTI tunnels to redundant headends.
- Select Cisco VPN router products at the branch offices based on considerations for the following:
  - Maximum throughput in both pps and bps
  - Allowances for other integrated services that may be running on the router (for example, firewall, IPS, NAT/PAT, and so forth)
  - Maintaining CPU utilization below 65–80 percent

See Scalability Considerations, page 51 for more information.

Known Limitations Summary

This section provides a high-level summary of the known limitations for a VTI deployment.

General Limitations

The following are the general limitations that apply to the solution:

- VTI is not currently available in the Cisco Catalyst 6500 or Cisco 7600 Series routers.
- Tunnel interface keepalives are not supported. A dynamic routing protocol must be used because the headend interface is dynamic, a virtual access interface.
- "ip unnumbered" interfaces may confuse some NMS network mapping abilities.
- There are significant scalability limitations for supporting IPmc over VTI tunnel designs. For more information, see the *Multicast over IPsec VPN Design Guide* at the following URL: http://www.cisco.com/go/srnd.
- All VTI implementations can be implemented only in a Single Tier Headend Architecture.
- There are additional limitations specific to EZVPN; see Easy VPN with Dynamic Virtual Tunnel Interface Support, page 16.

Headend Limitations

Using optional downstream traffic shaping, although effective for preserving voice quality, consumes too many CPU cycles while shaping is active. When the shaper is engaged, packets are process-switched.

Branch Office Limitations

The following limitations apply to the branch office device:

- Do not use IP unnumbered on the headend and a static IP address on the branch tunnel interface.
- A static VTI tunnel must be initiated by the remote branch to a DVTI headend. The crypto headend cannot initiate the tunnel to the branch.

Additional detailed information about these recommendations is discussed in the sections that follow.

Design and Implementation

This section addresses design and implementation issues and provides implementation examples for reference.

Overview

The VTI is characterized by the following features:

- Provides a routable interface
- Supports per-tunnel features (or peer) configurations
- Reordering of packets by QoS features occurs pre-encryption; anti-replay drops because of QoS on originating router are eliminated

- Supports encryption of IPmc
- Headend routers can be configured with virtual templates, rather than a static tunnel interface per remote peer
- Load balancing and high availability (failover) are functions of the routing protocol in use
- The virtual access/virtual template interfaces are point-to-point, unlike the point-to-multipoint used with DMVPN. The point-to-multipoint interface of DMVPN does not currently support capability to do per-tunnel features.

A limitation of VTI is the lack of an interface keepalive equivalent to a GRE keepalive. Many network managers prefer to use a GRE keepalive and a redistributed static route to the tunnel interface instead of using a routing protocol hello and adjacency over the interface. Although the routing protocol and GRE keepalive can be functionally equivalent, there may be less CPU overhead incurred by using a GRE keepalive.

Design Considerations

This section defines the design considerations for implementing VTIs.

Virtual Tunnel Interface

VTI may be configured statically on both peers. Alternatively, the headend can use a dynamic VTI configuration. This topology allows a “once and done” configuration of the headend and also incorporates a tunnel interface by way of a virtual access interface for each remote router.

When EZVPN is configured on the branch router, VTI is configured as dynamic on both the branch and headend router.

Note Do not confuse virtual tunnel interface with virtual template interface service. See the next section for details.

Virtual Template Interface Service

Virtual template interface service originally was for use primarily with large numbers of dial-in users. Virtual templates can be configured independently of any physical interface and applied dynamically, per “session”, to create virtual access interfaces. Virtual templates have been used for virtual private dialup networks (VPDN), with PPP over ATM, in a multilink PPP, or in a multichasses multilink PPP configuration.

The virtual tunnel interface *makes use of* the virtual template interface service feature on the headend crypto router. An example of a **show interface** command from a crypto headend router is as follows:

```
CRYPTO_HEADEND#show int virtual-access 4 | inc Tunnel|Inter|is up
Virtual-Access4 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback1 (10.8.100.1)
  Tunnel vaccess, cloned from Virtual-Template1
  Tunnel source 192.168.131.39, destination 192.168.128.198
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPsec (profile "VirtualTunnelInterface")
```

In the above example, the tunnel source IP address of 192.168.131.39 is an address on this router, the IP address of the remote router is 192.168.128.198, and in this example is dynamically assigned to the remote (branch) router by DHCP. Note from the display that this interface is *cloned* from Virtual-Template1. The unique configuration characteristics of the virtual template are applied to the virtual access interface on a session-by-session, peer-by-peer basis.

VTI provides for a dynamically cloned point-to-point logical interfaces for each branch. For more information about virtual templates, see the following website:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/vtemp.htm

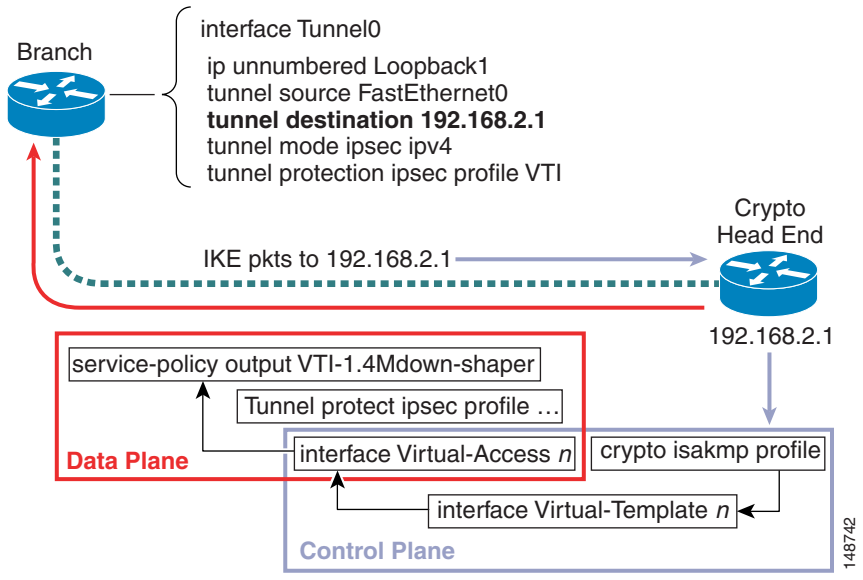
Per-Tunnel Features

VTI enables the implementation of QoS and other features from a crypto headend to a branch router on a per-crypto peer basis. An ISAKMP and IPsec security association between two crypto peers is a "session", similar to a PPP session; therefore, per-tunnel features can be implemented on a session-by-session basis.

A branch router can be configured to have multiple sessions between the same or multiple crypto headend routers. Later in this document is an example where two branch routers have sessions or tunnels to a single crypto headend router. One branch has one tunnel to the crypto headend and the other branch has two tunnels to the same crypto headend. The early scale testing of this feature had two Cisco 7200VXR routers; one branch and one crypto headend with sixteen tunnels and sixteen equal cost paths in the routing table between the two routers. This configuration is not recommended, but it can be configured.

Branch routers that share a common per-tunnel feature, such as a downlink QoS shaper rate, can reference the same virtual template on the crypto headend router. The crypto headend virtual template that is invoked is determined by the branch router configuration. The tunnel destination IP address on the branch router determines the virtual template to use. The crypto headend router has a unique IP address per virtual template. This concept is illustrated in Figure 3.

Figure 3 Virtual Template Invoked by Branch Router



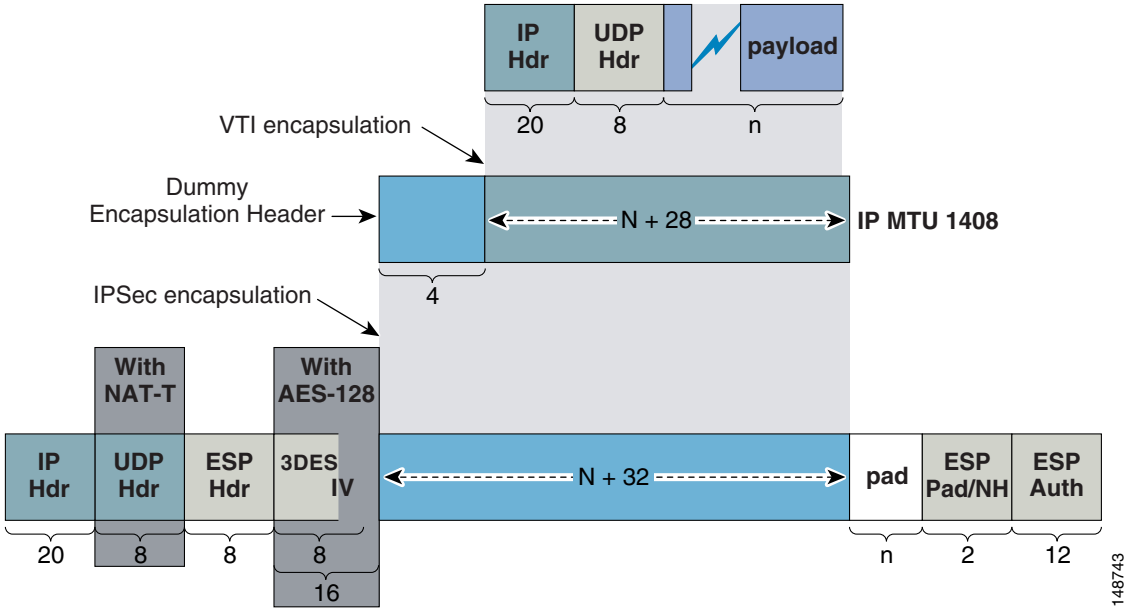
A crypto headend router can have multiple virtual templates defined. The ISAKMP packets of the branch router destination address select the ISAKMP profile to use on the headend, which is then cross-referenced to a IPsec profile and virtual template. The virtual access interface is spawned from the virtual template and inherits the configured QoS service policy. The control plane selects the appropriate QoS service policy for the data plane.

The actual limit of the number of virtual templates permitted in the configuration of a Cisco 7200VXR Series router in Cisco IOS 12.3(14)T2 is 1000. However, most deployments require only less than a dozen. From the standpoint of downlink shaping, most customer deployments would likely have 768 Kbps, 1.4 Mbps, or T1, E1, and perhaps 3 Mbps and 4 Mbps. These data rates are commonly seen on broadband links and T1/E1 serial links.

Encapsulation

For Cisco Express Forwarding to work, a dummy four-byte encapsulation string is used. The encapsulation string is stripped off during the fixup. Figure 4 illustrates this.

Figure 4 Encapsulation



The additional overhead of the four-byte VTI header is the same as p2p GRE (in transport mode) but less than mGRE. p2p GRE has a four-byte header and mGRE has an eight-byte header. VTI does not add an extra encapsulating IP header because both p2p GRE and mGRE add to a transiting packet.

QoS Service Policy

In this guide, the QoS service policy is applied to the tunnel interface on the branch router and to the virtual template on the crypto headend router, which is beneficial of two reasons: it reduces ESP replay check (anti-replay) errors, and invokes downstream QoS capability where not provisioned by the ISP.

Anti-Replay

The *Voice and Video Enabled IPsec VPN (V3PN) Design Guide* explains the concept of IPsec anti-replay in great detail. To summarize, a function of IPsec, and more specifically Encapsulating Security Payload (ESP), is to provide a means to detect whether packets have been captured in transit and changed and replayed, or simply duplicated and replayed between sender and receiver. This function is described in RFC 2406 in Section 3.4.3 “Sequence Number Verification” at the following URL: ftp://ftp.isi.edu/in-notes/rfc2406.txt

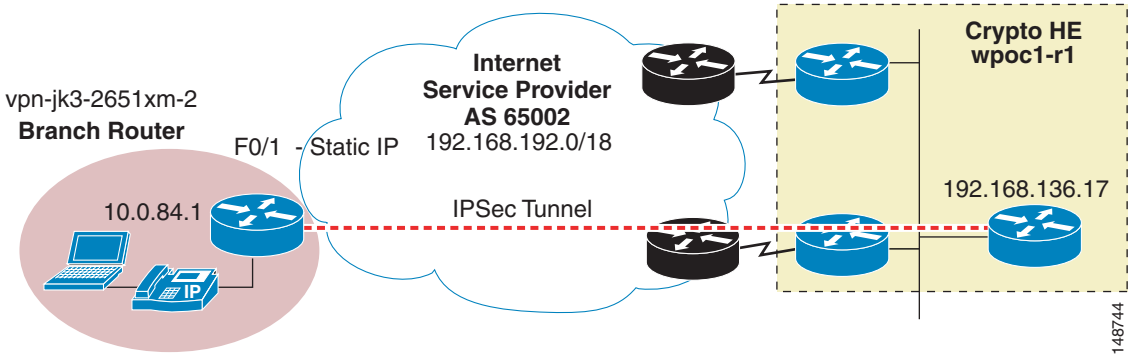
In configurations where the encrypting router re-orders packets post-encryption (after the ESP sequence number is assigned) as a function of an output interface QoS service policy, the likelihood of anti-replay drops induced by the sending crypto router and then received by the other crypto peer increases.

Pre-Encryption QoS

One advantage of VTI with the QoS service policy applied to the tunnel (or virtual access interface on the headend) is that packets are re-ordered before encryption and assignment of the ESP sequence number. In performance testing, the QoS service policy is applied pre-encryption. The net result of this is no re-ordering by the originating router post-ESP encapsulation.

To illustrate this point, a single branch router test is run to quantify the benefit of pre-encryption QoS (tunnel) compared to post-encryption (physical interface, FE0/1) QoS. The same traffic profile is used in two ten-minute tests. In these tests, QoS in the core network is not an issue; no core congestion or re-ordering takes place. Figure 5 shows the tested topology.

Figure 5 Pre-Encryption QoS Compared to Post-Encryption QoS



The first test was run with the service policy on the outside interface. This configuration is similar to a V3PN teleworker deployment where the outside interface is connected to a cable or DSL modem or bridge.

```
interface FastEthernet0/1
 description FastEthernet0/1
 ip address 192.168.192.22 255.255.255.0
 …
 service-policy output Shaper-768K
ip route 192.168.136.0 255.255.255.0 192.168.192.2 name ISP_router
```

At the end of the test, the replay error counter is displayed on the headend crypto peer.

```
show pas isa int
VPN Acceleration Module Version II in slot : 5
    Statistics for Hardware VPN Module since the last clear
     of counters 620 seconds ago
            342948 packets in                    342948 packets out
          88060130 bytes in                    87867591 bytes out
```

```
              553 paks/sec in                          553 paks/sec out
             1135 Kbits/sec in                        1133 Kbits/sec out
....
Errors:
       ppq full errors         :        0   ppq rx errors           :        0
       cmdq full errors        :        0   cmdq rx errors          :        0
       ppq down errors         :        0   cmdq down errors        :        0
       no buffer               :        0   replay errors           :     3297
```

There are 3297 replay errors out of 342,948 input packets; less than one percent of the total packets, which is a typical result based on past V3PN tests.

Now the service policy is removed from the outside interface and applied to the tunnel interface instead.

```
interface Tunnel1
 description VTI to wpoc1-r1
 …
 service-policy output Shaper-768K
```

The headend counters are cleared between tests and the test profile is executed for another ten minutes. At the end of this test, the counters are displayed again.

```
show pas isa int
VPN Acceleration Module Version II in slot : 5
    Statistics for Hardware VPN Module since the last clear
     of counters 620 seconds ago
            354714 packets in                     354714 packets out
          99807349 bytes in                     99953205 bytes out
              572 paks/sec in                       572 paks/sec out
             1287 Kbits/sec in                     1289 Kbits/sec out
...
Errors:
       ppq full errors         :        0   ppq rx errors           :        0
       cmdq full errors        :        0   cmdq rx errors          :        0
       ppq down errors         :        0   cmdq down errors        :        0
       no buffer               :        0   replay errors           :        0
```

For a similar pps rate (actually slightly higher), all anti-replay drops have been eliminated. There are configurations where it continues to be desirable to apply a service policy on the output interface, specifically in split tunnel or "spouse and child" configurations. However, these configurations are more typical with a teleworker deployment than a branch deployment.

Easy VPN with Dynamic Virtual Tunnel Interface Support

As of Cisco IOS version 12.4(4), Easy VPN (EZVPN) and DVTI incorporate features that allow network managers to position EZVPN to support branch offices as well as teleworker deployments.

These features include the following:

- Dual Tunnel
- Routing protocol support, enabling load sharing
- IPmc support
- Network-plus mode

The following two other features are available but are likely more suitably targeted at a remote access or teleworker deployment rather than a branch router deployment:

- Pushing a banner by the EZVPN server
- Pushing a configuration URL through a mode-configuration exchange

This section provides an overview of these features. Configuration and Implementation, page 25 shows sample configurations as a guide for implementation.

Dual Tunnel

EZVPN now includes a feature named Easy VPN Dual Tunnel, which supports a configuration with two EZVPN tunnels that have the same inside and outside interfaces.

Note For more information on Easy VPN Dual Tunnel, see the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/ftezvpnr.htm#wp1292665

Several caveats govern the use of this feature; these restrictions are incorporated into the configuration examples shown later in this document.

The restrictions are that both tunnels cannot do the following:

- Terminate on the same peer
- Use a non-split tunnel policy

The restriction on both tunnels terminating on the same peer is not important because the best practice is to terminate each tunnel on a separate headend router. This provides hardware redundancy if a headend fails, or is taken out of service for a software upgrade or other maintenance activity.

The second restriction is that both tunnels are not permitted to use a non-split tunnel policy; that is, one tunnel must be split tunnel and the other can be non-split tunnel. Although this may seem to be an issue for many network managers that are governed by security policies that require non-split tunnel, the configuration illustrates a workaround to this restriction. In the example, both headend routers are configured with an ACL keyword, enabling split tunnel, while using the routing protocol network advertisements to route all enterprise traffic into one or both tunnels. This effectively circumvents the split tunnel EZVPN configuration.

The branch configuration has two separate **crypto ipsec client ezvpn** configurations along with the associated virtual templates:

```
crypto ipsec client ezvpn VTI_SECOND
 connect auto
 group RTP_ezvpn_group key MrExcitement
 mode network-plus
 peer 192.168.136.19
 virtual-interface 52
 username EZVPN_Test_user password JimmyS
 xauth userid mode local
!
crypto ipsec client ezvpn VTI
 connect auto
 group RTP_ezvpn_group key MrExcitement
 mode network-plus
 peer 192.168.136.17
 virtual-interface 51
 username EZVPN_Test_user password JimmyS
 xauth userid mode local
!
interface Virtual-Template52 type tunnel
 description ->
 no ip address
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
```

```
 tunnel mode ipsec ipv4
!
interface Virtual-Template51 type tunnel
 description ->
 no ip address
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 tunnel mode ipsec ipv4
!
```

The outside interface references both **crypto ipsec client ezvpn** configurations as well as the inside interface:

```
!
interface FastEthernet0/1
 description Outside [VLAN 51 AS 65001]
 ip address dhcp
 crypto ipsec client ezvpn VTI_SECOND
 crypto ipsec client ezvpn VTI
!
interface Ethernet1/0
 description VLAN 208  Inside
 ip address 10.0.76.1 255.255.255.0
 crypto ipsec client ezvpn VTI_SECOND inside
 crypto ipsec client ezvpn VTI inside
!
!
```

Note CSCsc63242 (Cannot remove EZVPN configuration from inside interface) prevents the configuration from being removed as would be expected.

Routing Protocol Configuration

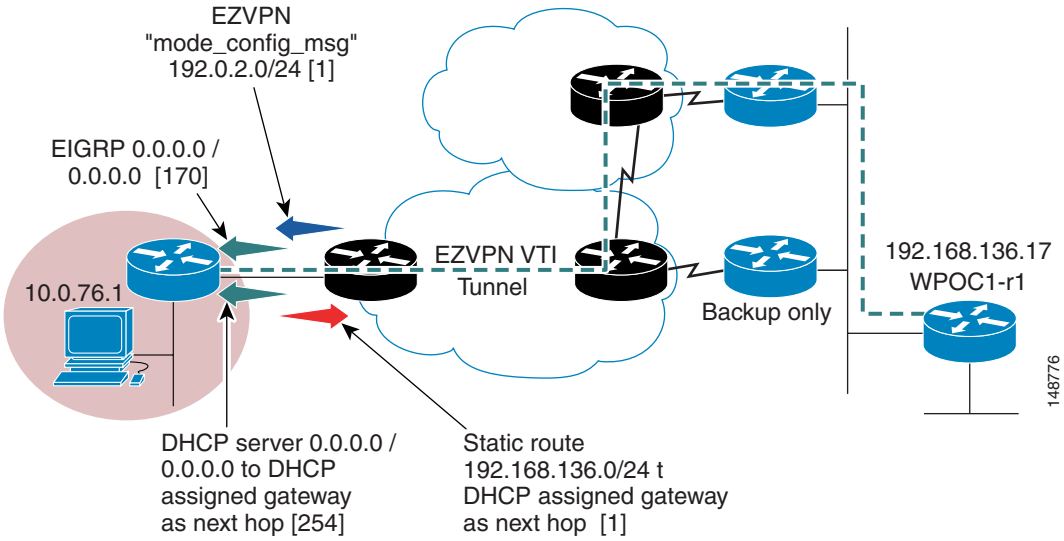
The branch and headend routers run EIGRP as the routing protocol. On the branch router, there is a static route for network 192.168.136.0/24 to the DHCP-learned default gateway. Both headend routers fall into this network, and it is assumed that only IPsec headend devices exist on the 192.168.136.0/24 network. In this example, the DHCP server that supplies the IP address of the outside interface of the branch router advertises the DHCP server as the next-hop address for the default route. Cisco IOS DHCP clients use 254 by default as the administrative distance of the DHCP-learned default route.

Given the split tunnel configuration, the EZVPN server advertises in the EZVPN mode_config_msg the network 192.0.2.0/24 to the remote router. This network is inserted in the routing table of the branch router with an administrative distance of 1, using the virtual access interface as the next hop.

The headend EIGRP neighbor advertises through the VTI tunnel a default route with an administrative distance of 170 to the branch router. Because 170 is lower (more preferred) than the DHCP default route (254), the default route learned from EIGRP is inserted into the branch routing table. This overrides the split tunnel configuration and forces all user traffic into the virtual access interface to the headend.

The relationship of these routing information sources is shown in Figure 6. Only one headend router is shown for clarity.

Figure 6 Routing Information Sources



Note: The number in square brackets is the administrative distance of the route specified. Example, [170] is an EIGRP external.

For purposes of documentation, assume that 192.168.0.0/16 and 172.26.0.0/16 represent Internet routable address space and 10.0.0.0/8 represents enterprise address space. The following is the branch router configuration:

```
router eigrp 100
 network 10.0.0.0
 no auto-summary
 eigrp stub connected
!
ip route 192.168.136.0 255.255.255.0 dhcp
!
end
```

The following commands are for one of the two headend routers. Both headend routers are configured similarly. The client configuration on the EZVPN server references an ACL, and thus split tunnel is enabled.

```
crypto isakmp client configuration group RTP_ezvpn_group
 …
 acl SPLIT_TUNNEL_LIST
!
```

In this example, the headend also runs EIGRP. The virtual-template interface 154 is referenced by the distribute list statement under the routing protocol definition.

```
!
crypto isakmp profile VTI_IKE_Profile_alpha
   …
   virtual-template 154
!
!
crypto ipsec profile EZVPN_VTI
 set transform-set 3DES_SHA_TUNNEL
 set isakmp-profile VTI_IKE_Profile_alpha
…
```

```
interface Virtual-Template154 type tunnel
 …
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile EZVPN_VTI
!
```

In the EIGRP configuration, only a default route is advertised out the virtual access interfaces cloned from virtual-template 154.

The network listed in the *SPLIT_TUNNEL_LIST* ACL is a special use IP address; it is reserved and not routed over the Internet. Any IP network in use by the Internet or by the enterprise can be used instead. The network address referenced by the split tunnel ACL is inserted into the routing table of the branch router, with the virtual access interface as the next hop.

The routing protocol advertises a default route through the VTI tunnel, effectively circumventing the split tunnel configuration.

This configuration is implemented on both headend routers to implement this concept.

```
crypto isakmp client configuration group RTP_ezvpn_group
 …
 acl SPLIT_TUNNEL_LIST
…
router eigrp 100
 redistribute static metric 256 100 255 1 1408 route-map REDIST_STATIC
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 network 192.168.136.0 0.0.1.255
 distribute-list ROUTES_for_REMOTE out Virtual-Template154
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Null0 20
ip route 192.0.2.0 255.255.255.0 Null0 240 name TEST-NET
!
ip access-list standard ROUTES_for_REMOTE
 permit 0.0.0.0
 deny   any
!
ip access-list extended SPLIT_TUNNEL_LIST
 permit ip 192.0.2.0 0.0.0.255 any
!
!
route-map REDIST_STATIC permit 10
 match ip address ROUTES_for_REMOTE
!
end
```

In the routing table of the branch router, EZVPN inserts a static route for 192.0.2.0/24 to both tunnel (virtual access) interfaces. The EIGRP routing protocol advertises a default route from both headend routers, providing load sharing across both headends.

```
vpn-jk3-2651xm-3#show ip route | beg Gateway
Gateway of last resort is 10.9.100.1 to network 0.0.0.0

C    192.168.128.0/24 is directly connected, FastEthernet0/1
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.76.0/24 is directly connected, Ethernet1/0
C       10.8.100.21/32 is directly connected, Loopback0
C       10.9.100.26/32 is directly connected, Loopback1
S    192.168.136.0/24 [1/0] via 192.168.128.1
S    192.0.2.0/24 [1/0] via 0.0.0.0, Virtual-Access2
                  [1/0] via 0.0.0.0, Virtual-Access3
D*EX 0.0.0.0/0 [170/297270016] via 10.9.100.1, 03:02:55, Virtual-Access3
               [170/297270016] via 10.8.100.1, 03:02:55, Virtual-Access2
```

Looking now at the relevant portion of the routing table of one of the two headend routers, the branch advertises the remove subnet and the loopback interface to the headend.

```
wpoc1-r1#show ip route | inc Vi
S       10.0.76.0/24 [1/0] via 0.0.0.0, Virtual-Access2
           [90/297372416] via 10.9.100.26, 03:03:22, Virtual-Access2
S       10.9.100.26/32 [1/0] via 0.0.0.0, Virtual-Access2
```

In summary, when an EZVPN server pushes split tunnel networks to a remote router, the remote router inserts those specific routes to the split network in its routing table, directing the traffic out the virtual tunnel interfaces. A routing protocol is then run to advertise a default route to the branch, directing all user traffic to the headend through the virtual tunnel interfaces. The configuration is such that the default route overrides any default route learned via DHCP or configured statically in the branch router.

If load sharing is not desired, all traffic should use a primary headend; the secondary headend is intended to be used only as a backup, and the cost or metric component is changed to make the tunnel less preferred. In the case of EIGRP shown in this example, change the delay to a value greater than the default of 50,000 on both the branch and headend router.

```
!
interface Virtual-Template52 type tunnel
….
delay 60000
…
 tunnel mode ipsec ipv4
end
```

After clearing the EZVPN connections, only one route is now in the routing table for the default route.

```
vpn-jk3-2651xm-3#show ip route | beg Gateway
Gateway of last resort is 10.9.100.1 to network 0.0.0.0

C    192.168.128.0/24 is directly connected, FastEthernet0/1
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.76.0/24 is directly connected, Ethernet1/0
C       10.8.100.22/32 is directly connected, Loopback1
C       10.9.100.27/32 is directly connected, Loopback0
S    192.168.136.0/24 [1/0] via 192.168.128.1
S    192.0.2.0/24 [1/0] via 0.0.0.0, Virtual-Access3
                  [1/0] via 0.0.0.0, Virtual-Access2
D*EX 0.0.0.0/0 [170/297270016] via 10.9.100.1, 00:00:17, Virtual-Access3
```

The EIGRP topology table continues to have both:

```
vpn-jk3-2651xm-3#show ip eigrp topology | beg 0.0.0.0
P 0.0.0.0/0, 1 successors, FD is 297270016
        via 10.9.100.1 (297270016/10025472), Virtual-Access3
        via 10.8.100.1 (299830016/10025472), Virtual-Access2
```

The less preferred path is inserted into the routing table in the event that the primary peer is unreachable or out of service.

IP Multicast

IPmc can be configured on the virtual template interfaces, and IPmc routing is supported with the EZVPN configuration shown in this guide. The following display is from the branch router:

```
vpn-jk3-2651xm-3#show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface               Uptime/Expires    Ver   DR
Address                                                           Prio/Mode
10.9.100.1        Virtual-Access3         00:20:33/00:01:23 v2    1 / S
```

```
10.8.100.1        Virtual-Access2          00:20:32/00:01:21 v2    1 / S
```

Note that there are PIM neighbors on both tunnel interfaces.

EZVPN Remote Client—Mode Network-Plus

Network extension plus (mode network-plus) is similar to network extension mode, except that an IP address is allocated from the address pool configured on the headend router and automatically assigned to an available loopback interface on the branch router. In effect, the pool is created on the headend when the branch router requests or initiates this mode. The branch router CLI is as follows:

```
vpn-jk3-2651xm-3(config)#crypto ipsec client ezvpn VTI
vpn-jk3-2651xm-3(config-crypto-ezvpn)#mode ?
  client             Client
  network-extension  Network Extension
  network-plus       Request a IP address identifier in NEM
```

Best Practices

The headend router defines a pool, in this case named *MODE_network-plus*, and allocates a range of IP addresses out of the 10.9.100.0/24 block. The first IP address in this block is configured on a loopback address. This loopback address is the borrowed IP address for the "ip unnumbered" statement in the virtual template.

```
crypto isakmp client configuration group RTP_ezvpn_group
 …
 pool MODE_network-plus
 !
  …

interface Loopback901
 description Anchor for VTI
 ip address 10.9.100.1 255.255.255.255
…
ip local pool MODE_network-plus 10.9.100.2 10.9.100.253

interface Virtual-Template154 type tunnel
 ip unnumbered Loopback901
```

The branch router uses this dynamically allocated loopback interface by default as the source of the borrowed address for the branch virtual template. As such, with the above configuration, the headend router sees the branch router identified as an address allocated from the pool MODE_network-plus, as follows:

```
wpoc1-r1#show ip eigrp neighbors | inc Vi
21  10.9.100.26             Vi2               12 00:22:56  103  5000  0  192
```

The branch router can identify the respective headend router as the first address from the 10.9.100.0/24 network, 10.9.100.1, as follows:

```
vpn-jk3-2651xm-3#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.9.100.1              Vi3               13 00:23:17   19  5000  0  1664
0   10.8.100.1              Vi2               13 00:23:18   55  5000  0  1389
```

In the above example, the neighbor identified by 10.8.100.1 is the second headend, similarly configured to the primary headend but using 10.8.100.0/24 as the address block.

Caveats

There are two caveats that the network manager must consider. If a **write memory** or **copy running-config startup-config** command is issued while the tunnels are up, the dynamically assigned loopback interfaces are saved in the startup configuration. If the router is then reloaded or ISAKMP disabled and re-enabled, new (additional) interfaces are created and addresses are assigned from the headend pool.

The following is an example from a branch router configuration where the configuration was saved with the tunnel up to the headend peer, allocating the address from the 10.8.100.0/24 block.

```
!
interface Loopback0
 ip address 10.8.100.15 255.255.255.255
!
interface Loopback1
 ip address 10.9.100.25 255.255.255.255
!
interface Loopback2
 ip address 10.8.100.20 255.255.255.255
```

The tunnel was then re-initiated, causing the headend to allocate the Loopback2 interface with another address from the pool. To clear this condition, disable ISAKMP on the branch router (**no crypto isakmp enable**), delete all loopback interfaces, and then re-enable ISAKMP (**crypto isakmp enable**).

The second caveat is that configuring an **ip unnumbered** command on the branch router virtual template is ignored, and the outside IP address is used as the "borrowed" IP address when network-extension mode is used instead of network-plus.

The network manager must become familiar with, and understand the implications of, this feature along with the associated caveats related to the enterprise network management scheme. Because the IP addresses are allocated dynamically and are not associated permanently with any one branch, this feature may present problems for the support desk.

Banner

A banner can be pushed to the branch router. It is configured on the headend router.

```
crypto isakmp client configuration group RTP_ezvpn_group
 …
 banner ^C
==
====
====== Hello from wpoc1-r1
====
==
 ^C
```

When the branch connects to the headend, the banner is displayed on the console and logging buffer. Following is an example from the dual tunnel configuration used in this section:

```
Dec  8 14:44:34 est: %CRYPTO-6-EZVPN_CONNECTION_DOWN: (Client)  User=EZVPN_Test_user
Group=RTP_ezvpn_group  Server_public_addr=…
==
====
====== Hello from vpn-jk3-2651xm-9
====
==

==
====
====== Hello from wpoc1-r1
====
```

```
==

Dec  8 14:44:35 est: %CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=EZVPN_Test_user
Group=RTP_ezvpn_group
```

This feature may have applications for debugging but from a branch router perspective, the individual users are not viewing the console and do not see the message.

Configuration URL

The configuration URL feature is designed to help push a configuration template to all members of the group as part of the tunnel establishment. The file served is in Cisco IOS CLI format. By default, the commands are considered persistent, and are present whether or not the tunnel is up to the headend. The commands are not written to NVRAM. Keywords in the file identify the nature of the CLI commands that follow: **!%transient** (the keyword should be on a single line), or optionally **!%persistent**. The following examples show how this is configured on the Easy VPN server and on the FTP server from which the file is obtained by the Easy VPN remote.

The Easy VPN server configuration is as follows:

```
crypto isakmp client configuration group RTP_ezvpn_group
 …
 configuration url ftp://root:cisco@172.26.157.11//usr/tmp/CFG-version11.txt
 configuration version 11
```

The FTP server and the source file is as follows:

```
# ifconfig -a | grep inet
        inet 127.0.0.1 netmask ff000000
        inet 172.26.157.11 netmask fffffe00 broadcast 172.26.157.255


# cat /usr/tmpCFG-version11.txt
!%persistent
banner exec $
==
=== This is a persistent (tunnel up or down) configuration section
==
$
!%transient
banner motd $
==
=== This is a transient (tunnel up only) configuration section
==
$
end
```

No configuration need be specified on the Easy VPN remote. The following is an example of verifying the configuration status. Obviously, the commands can also be viewed by issuing a **show running-config** from the console or VTY port of the remote router.

```
vpn-jk3-2651xm-3#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 6

Tunnel name : VTI_SECOND
Inside interface list: Ethernet1/0
Outside interface: Virtual-Access2 (bound to FastEthernet0/1)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.8.100.31
Mask: 255.255.255.255
Default Domain: cisco.com
```

```
Save Password: Allowed
Split Tunnel List: 1
       Address    : 192.0.2.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Configuration URL [version]: ftp://root:cisco@172.26.157.11//usr/tmp/CFG-version26.txt
[26]
Config status: applied, Last successfully applied version: 26
Current EzVPN Peer: 192.168.136.19
```

The following two issues currently limit the functionality of this feature:

- CSCsc72005—EZVPN transient configuration not removed when tunnel down
- CSCsc77978—EZVPN configuration URL not applied

Verify the resolution and integration of these defects as part of the planning and implementation process before attempting to implement this feature.

Appendix C—Output for debug crypto ipsec client ezvpn Command, page 77 includes the complete output of a **debug crypto ipsec client ezvpn** command that shows the debug output associated with the configuration URL processing.

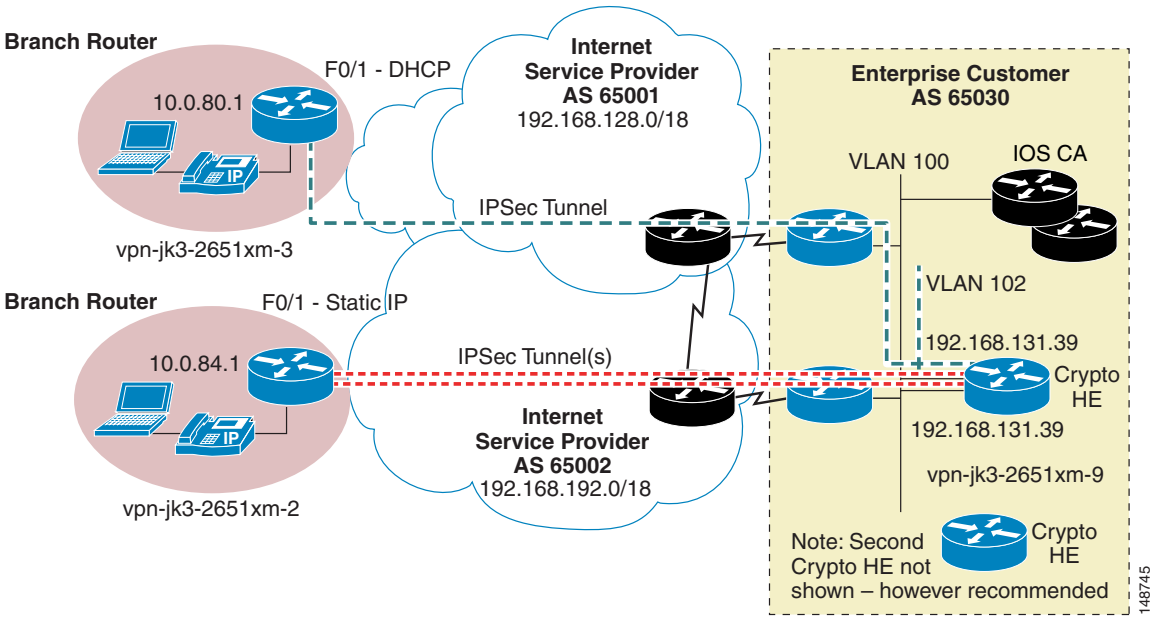
Configuration and Implementation

This section provides sample configurations for a basic deployment of VTI. Two branch routers are used, one with a static IP address and a second with a dynamic IP address assigned by the ISP equipment. One crypto headend router is shown; however, most customer deployments have two crypto headend routers for better availability. This example uses a PKI/CA infrastructure with two separate Cisco IOS CA servers. There is no requirement for this type of implementation, it is simply shown as an example.

Topology

The topology shown in Figure 7 is used for reference.

Figure 7 Basic Deployment Topology



VTI Configuration Overview

VTI is introduced in Cisco IOS release 12.3(14)T. To enable the VTI feature, use the **tunnel protection** interface command with the following new Cisco IOS interface command:

```
tunnel mode ipsec ipv4
```

A sample interface configuration is shown:

```
interface Tunnel0
 ip unnumbered Loopback n
 tunnel source FastEthernet n/n
 tunnel destination n.n.n.n
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VirtualTunnelInterface
```

The configuration example above is representative of a branch router. The crypto headend router configuration is shown later and is configured with DVTI in this guide.

QoS Configuration

The branch and headend routers use a similar QoS configuration, as follows:

```
!
class-map match-any VOICE
 match ip dscp ef
 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
!
```

```
policy-map V3PN
description Voice + VT Advantage
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
   priority percent 50
 class class-default
  fair-queue
  random-detect
policy-map Shaper-1544K
description 1544Kbps * .85 = 131Kbps
 class class-default
  shape average 1310000 13100
  service-policy V3PN
policy-map Shaper-768K
description 768Kbps * .85 = 652Kbps
 class class-default
  shape average 652000 6520
  service-policy V3PN
!
```

In the above example, note that the VOICE class matches on either DSCP value of EF or AF41. Cisco VT Advantage marks both voice and video packets with the value of AF41 during a voice and video call. As a result, AF41 must now be included in the VOICE class.

The VOICE class priority queue is allocated as a percentage. For ease of configuration, it is advantageous to configure this as a percentage so different shapers (parent service policies) can reference the same child service policy. In a hierarchical CBWFQ configuration, the percentage is calculated on the shaped rate.

Note In the performance testing for this design chapter, the priority queue was allocated at a fixed size, 256 Kbps, because the test profile did not include any video and at most there were four concurrent G.729 voice calls.

ISAKMP DSCP Value

In past design guides, the V3PN service policy matched ISAKMP packets and included them in the INTERNETWORK-CONTROL class and optionally set the DSCP value to CS6. For example:

```
ip access-list extended IKE
    permit udp any eq isakmp any eq isakmp
```

As of 12.3(4)T, this is no longer necessary on a router configured for both crypto and QoS. The ISAKMP packets are marked as INTERNETWORK CONTROL or IP Precedence 6, DSCP CS6. See the following for more detailed information:

- CSCeb18618—IKE traffic needs to be marked as Precedence 6
- CSCdz01484—IKE keepalive packets should be IP Precedence 6

For an explanation of ISAKMP (IKE) DSCP, see the *Voice and Video Enabled IPsec VPN (V3PN) Design Guide* at the following URL: http://www.cisco.com/go/srnd.

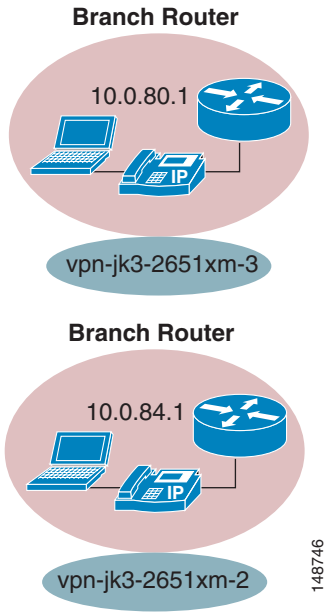
Trustpoints

This sample configuration uses the PKI/CA infrastructure for authentication. The branch and the headend trustpoint configuration is shown. For more information, see the *Digital Certification/PKI for IPsec VPN Design Guide* at the following URL: http://www.cisco.com/go/srnd.

Branch

The two branch routers are shown in Figure 8.

Figure 8 Branch Trustpoint



In the following example, CA server at 192.168.131.25 is accessible within the sample topology and the server at 172.26.179.249 IP address.

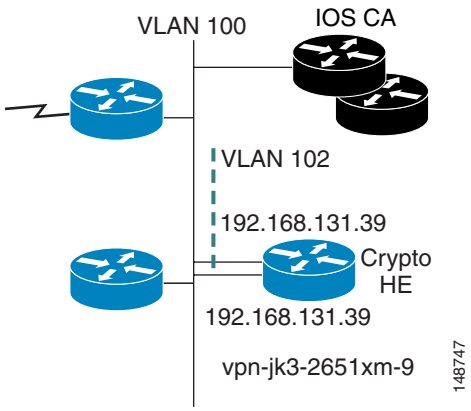
```
hostname vpn-jk3-2651xm-2
!
ip host ese-ios-ca 172.26.179.249
crypto pki trustpoint ese-ios-ca
 enrollment url http://ese-ios-ca:80
 revocation-check none
 auto-enroll 70
!
crypto pki certificate chain ese-ios-ca
 certificate 49
 certificate ca 01
!

hostname vpn-jk3-2651xm-3
ip host Joe_Cisco_LAB_ca_server 192.168.131.25
crypto pki trustpoint ESE_JK_RACK
 enrollment url http://Joe_Cisco_LAB_ca_server:80
 revocation-check none
 auto-enroll 70
crypto pki certificate chain ESE_JK_RACK
 certificate 08
 certificate ca 01
```

Headend

The crypto headend makes reference to both CA servers, because one branch references a different CA server than the other branch (see Figure 9).

Figure 9 Headend



These are two independent CA servers, which are referenced in the ISAKMP profile section later in this guide.

```
hostname vpn-jk3-2651xm-9
ip host ese-ios-ca 172.26.179.249
ip host Joe_Cisco_LAB_ca_server 192.168.131.25
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://ese-ios-ca:80
 revocation-check crl
 auto-enroll 70
!
crypto pki trustpoint ESE_JK_RACK
 enrollment url http://Joe_Cisco_LAB_ca_server:80
 revocation-check crl
 auto-enroll 70
!
crypto pki certificate chain ese-ios-ca
 certificate 4B
 certificate ca 01
crypto pki certificate chain ESE_JK_RACK
 certificate 07
 certificate ca 01
!
```

ISAKMP Policy

All branch and headend routers use a similar ISAKMP policy configuration.

```
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
```

IPsec Profile

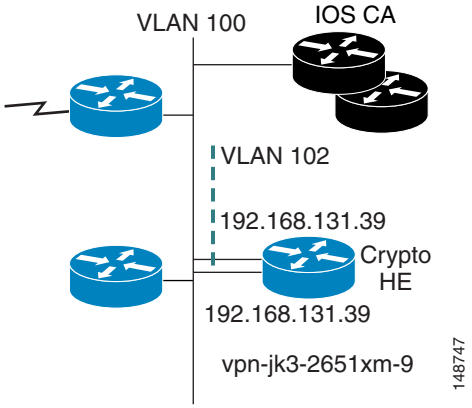
The IPsec profiles always use tunnel mode. Even if a network manager were to add a “transport mode” transform set of a higher priority, VTI would still choose tunnel mode.

```
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
!
crypto ipsec profile VirtualTunnelInterface
 set transform-set 3DES_SHA_TUNNEL
!   Headend
interface Virtual-Template[n] type tunnel
 tunnel protection ipsec profile VirtualTunnelInterface
!    Branch
interface Tunnel [n]
 tunnel protection ipsec profile VirtualTunnelInterface
However, VTI negotiates tunnel mode in all tested configurations.
vpn-jk3-2651xm-9# show crypto ipsec sa detail | inc peer|endpt|in use
   current_peer 192.168.192.22 port 500
     local crypto endpt.: 192.168.131.19, remote crypto endpt.: 192.168.192.22
        in use settings ={Tunnel, }
        in use settings ={Tunnel, }
   current_peer 192.168.128.198 port 500
     local crypto endpt.: 192.168.131.39, remote crypto endpt.: 192.168.128.198
        in use settings ={Tunnel, }
        in use settings ={Tunnel, }
```

Headend Router Configuration

The remaining relevant crypto headend configuration is shown in this section. In Figure 10, note that this crypto headend has two outside interfaces: 192.168.131.39 and 192.168.131.19. These outside interfaces allow the branch router configuration to select the downstream shaper rate, because the crypto peer local address and the virtual template configurations reference each other.

Figure 10 Basic Configuration—Headend Addressing



ISAKMP Profiles and Virtual Templates

The following configuration is the headend ISAKMP profile and virtual template configuration:

```
hostname vpn-jk3-2651xm-9
crypto isakmp profile VTI_1
   description TEST for VTI Templates 1.544Kbps
   ca trust-point ese-ios-ca
   ca trust-point ESE_JK_RACK
   match identity host domain ese.cisco.com
   keepalive 10 retry 2
   virtual-template 1
   local-address FastEthernet0/1.102
crypto isakmp profile VTI_7
   description TEST for VTI Templates 768Kbps
   ca trust-point ese-ios-ca
   match identity host domain ese.cisco.com
   keepalive 10 retry 2
   virtual-template 7
   local-address FastEthernet0/1.100
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 ip summary-address eigrp 100 10.0.0.0 255.0.0.0 5
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VirtualTunnelInterface
 service-policy output Shaper-1544K
!
interface Virtual-Template7 type tunnel
 ip unnumbered Loopback1
 ip summary-address eigrp 100 10.0.0.0 255.0.0.0 5
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VirtualTunnelInterface
 service-policy output Shaper-768K
```

In this configuration, there are two ISAKMP profiles: VTI_1 and VTI_7. Profile VTI_1 references two separate trustpoints as referenced in a previous section. The branch routers do not all use the same PKI/CA infrastructure. Each ISAKMP profile references a different outside (local-address) IP address. Note that each ISAKMP profile references a different virtual template that have different QoS service policies shaping at different rates.

Both virtual templates borrow the IP address of the same interface, Loopback 1.

Headend Addressing

```
interface Loopback1
 description Anchor for VTI
 ip address 10.8.100.1 255.255.254.0
interface FastEthernet0/1.100
 description Outside interface for 768Kbps
 encapsulation dot1Q 100
 ip address 192.168.131.19 255.255.255.224
interface FastEthernet0/1.102
 description Outside interface for 1544Kbps
 encapsulation dot1Q 102
 ip address 192.168.131.39 255.255.255.224
!
interface FastEthernet0/1.128
 description Inside interface
 encapsulation dot1Q 128
 ip address 10.2.128.19 255.255.255.0
!
router eigrp 100
```

```
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 no auto-summary
!
```

Branch Router Configuration

The configuration listing below is an example of one of the two branch router configurations. This branch router learns the outside IP address by DHCP from the ISP.

In this example, the branch is shaping at a T1 data rate. The tunnel destination address is 192.168.131.19. This address also selects the downstream T1 data rate defined in Virtual-Template1 on the crypto headend.

```
hostname vpn-jk3-2651xm-3
!
interface Tunnel1
 description VTI to xm-9 VLAN 102 Interface
 ip unnumbered Loopback1
 tunnel source FastEthernet0/1
 tunnel destination 192.168.131.39
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VirtualTunnelInterface
 service-policy output Shaper-1544K
interface Loopback1
 ip address 10.8.100.3 255.255.254.0
interface FastEthernet0/1
 description Outside [AS 65001]
 ip address dhcp
interface Ethernet1/0
 description Inside
 ip address 10.0.80.1 255.255.255.0
! You may also want to advertise the Loopback 1
! IP network to the headend to enable reachability
! to that interface.
router eigrp 100
 network 10.0.0.0
 distribute-list LAN_Subnet out Tunnel1
 no auto-summary
ip route 192.168.131.39 255.255.255.255 dhcp  # tunnel dest
ip access-list standard LAN_Subnet
 permit 10.0.80.0
end
```

In this example, the remote loopback IP address and the crypto headend loopback address are in the same network and share the same network mask. Sharing the network and mask is not required and a later section shows other means of configuring IP unnumbered using the inside Ethernet and any arbitrary address on the crypto headend.

Dynamic VTI for EZVPN Remote and Server—Dual Tunnel Support

This section shows the configuration and implementation of EZVPN with dynamic VTI interfaces on both the remote and headend routers. The branch or remote router has two EZVPN tunnels to separate headends. Both tunnels are configured on one outside interface, which obtains an IP address dynamically from the Internet service provider.

This deployment topology is typical of a small branch or teleworker deployment that connects to the Internet by means of a broadband (DSL or cable) link or through a single leased line.

The following features are shown in this configuration:

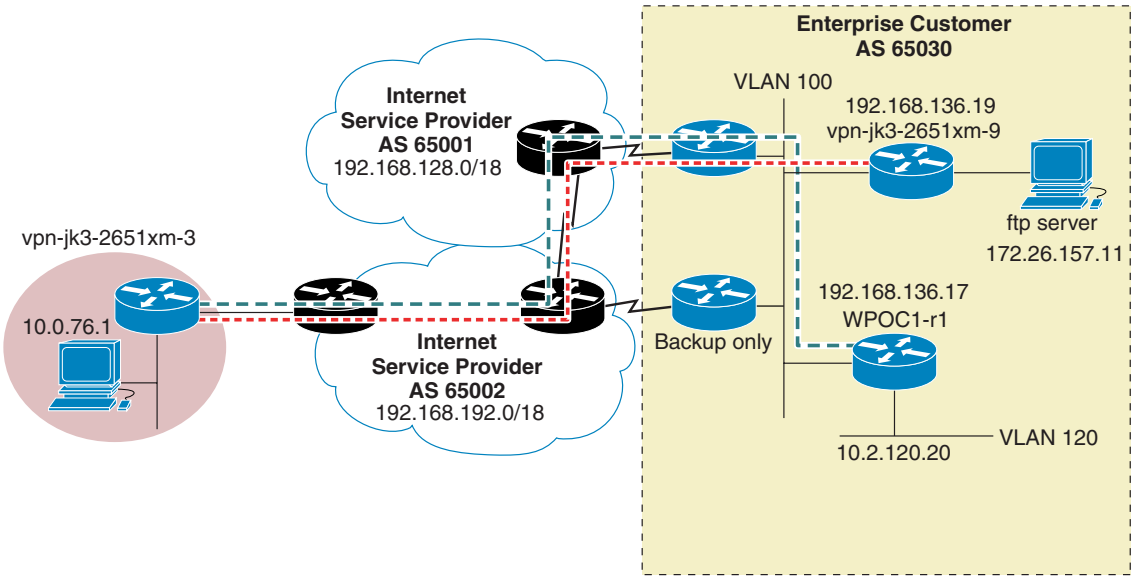
- QoS to support a VoIP deployment
- IPmc routing to support both IPmc applications
- An IGP routing protocol, EIGRP, to support load sharing and redundancy

Note On the branch router, the QoS service policy is applied to the outside physical interface if load sharing across both headends is desired. If the branch router is configured to route traffic only to the secondary headend when the primary headend is out of service, the QoS service policy can be applied to both branch virtual template interfaces instead of the outside physical interface. An advantage of applying the QoS service policy to the logical versus the physical interface is that QoS is invoked before encryption, thereby eliminating anti-replay drops induced by queueing on the encrypting router.

Topology

Figure 11 shows the topology diagram that is referenced by the configuration files that follow.

Figure 11 Topology Diagram



The branch or remote router is *hostname vpn-jk3-2651xm-3*. One headend is considered the primary, *hostname wpoc1-r1*, the second headend is hostname *vpn-jk3-2651xm-9*. The second headend is configured to push configuration updates to the branch routers. Both headend routers advertise an equal cost default route to the branches, and are therefore both used for forwarding user traffic.

The IP addressing scheme is such that 192.168.0.0/16 and 172.16.0.0/12 represent Internet routable address space, and 10.0.0.0/8 represents enterprise address space.

Branch Router

```
!
! Last configuration change at 14:41:54 est Tue Dec 6 2005
! NVRAM config last updated at 13:36:25 est Tue Dec 6 2005
!
version 12.4
```

```
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
no service password-encryption
!
hostname vpn-jk3-2651xm-3
!
boot-start-marker
boot system flash c2600-advipservicesk9-mz.124-4.T
boot system flash
boot-end-marker
!
logging buffered 8192 debugging
!
no aaa new-model
!
resource policy
!
clock timezone est -5
clock summer-time edt recurring
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
!
ip cef
no ip domain lookup
ip domain name ese.cisco.com
ip multicast-routing
ip sla responder
ip sla 26
 icmp-echo 10.2.120.20
 tos 192
 owner JOEL
 tag VTI TEST Enhanced EZVPN
 frequency 10
ip sla schedule 26 life forever start-time now
!
!
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
!
policy-map V3PN-768
  description V3PN branch (4calls-768 BW)
  class CALL-SETUP
  bandwidth percent 2
  class INTERNETWORK-CONTROL
  bandwidth percent 5
  class VOICE
  priority 256
  class class-default
  fair-queue
  random-detect
policy-map Shaper-768K
  description 768K * .85 = 652
  class class-default
  shape average 652000 6520
  service-policy V3PN-768
!
!
```

```
crypto logging session
crypto logging ezvpn
crypto isakmp keepalive 10
!
!
crypto ipsec client ezvpn VTI_SECOND
 connect auto
 group RTP_ezvpn_group key MrExcitement
 mode network-plus
 peer 192.168.136.19
 virtual-interface 52
 username EZVPN_Test_user password JimmyS
 xauth userid mode local
crypto ipsec client ezvpn VTI
 connect auto
 group RTP_ezvpn_group key MrExcitement
 mode network-plus
 peer 192.168.136.17
 virtual-interface 51
 username EZVPN_Test_user password JimmyS
 xauth userid mode local
!
!
! These interfaces are created by mode network-plus and are not a permnanent part of the
! configuration unless the config is saved to NVRAM while the tunnels are up. If the
! config is saved, additional loopbacks are created upon next tunnel establishment.
!
interface Loopback0
 ip address 10.8.100.15 255.255.255.255
!
interface Loopback1
 ip address 10.9.100.25 255.255.255.255
!
!
!
interface FastEthernet0/1
 description Outside [To Internet AS 65001]
 ip address dhcp
 crypto ipsec client ezvpn VTI_SECOND
 crypto ipsec client ezvpn VTI
 service-policy output Shaper-768K
!
interface Ethernet1/0
 description Inside
 ip address 10.0.76.1 255.255.255.0
 no keepalive
 crypto ipsec client ezvpn VTI_SECOND inside
 crypto ipsec client ezvpn VTI inside
!
interface Virtual-Template51 type tunnel
 description -> Referenced in 'crypto ipsec client ezvpn VTI'
 no ip address
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 tunnel mode ipsec ipv4
!
interface Virtual-Template52 type tunnel
 description -> Referenced in 'crypto ipsec client ezvpn VTI_SECOND'
 no ip address
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 tunnel mode ipsec ipv4
```

```
!
router eigrp 100
 network 10.0.0.0
 no auto-summary
 eigrp stub connected
 no eigrp log-neighbor-warnings
!
ip classless
!
! This route forces the headend IP address space to the ISP supplied next hop.
!
ip route 192.168.136.0 255.255.255.0 dhcp
!
!
ip pim autorp listener
! [ Lines and Console not shown]
!
!
end
```

Headend (Primary)

```
!
! Last configuration change at 14:41:36 est Tue Dec 6 2005 by mrcisco
! NVRAM config last updated at 16:14:46 est Tue Dec 6 2005 by mrcisco
!
version 12.4
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname wpoc1-r1
!
boot-start-marker
boot system disk2:c7200-adventerprisek9-mz.124-4.T
boot system disk2:c7200-advipservicesk9-mz.124-4.T.bin
boot-end-marker
!
logging buffered 32768 debugging
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login VTY local
!
! In large deployments, a Radius server would be used to store passwords,
! here they are stored locally.
!
aaa authentication login EZVPNauthenlist local
aaa authorization network EZVPNauthorlist local
!
!
aaa session-id common
!
resource policy
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
ip cef
!
```

```
!
ip flow-cache timeout inactive 120
ip flow-cache timeout active 2
no ip domain lookup
ip domain name ese.cisco.com
ip multicast-routing
ip sla responder
!
!
username EZVPN_Test_user password 7 032E52060B1612 # Must match remote "JimmyS"
!
controller ISA 5/1
!
controller ISA 6/1
!
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
!
policy-map V3PN-768
  description V3PN branch (4calls-768 BW)
  class CALL-SETUP
  bandwidth percent 2
  class INTERNETWORK-CONTROL
  bandwidth percent 5
  class VOICE
  priority 256
  class class-default
  fair-queue
  random-detect
policy-map Shaper-768K
  description 768K * .85 = 652
  class class-default
  shape average 652000 6520
  service-policy V3PN-768
!
!
crypto logging session
crypto logging ezvpn
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group RTP_ezvpn_group
 key MrExcitement
 domain cisco.com
 pool MODE_network-plus
 acl SPLIT_TUNNEL_LIST
 save-password
 banner ^C
==
====
====== Hello from wpoc1-r1
====
==
 ^C
crypto isakmp profile VTI_IKE_Profile_alpha
   match identity group RTP_ezvpn_group
```

```
   client authentication list EZVPNauthenlist
   isakmp authorization list EZVPNauthorlist
   client configuration address respond
   keepalive 10 retry 2
   virtual-template 154
   local-address Loopback117
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
!
crypto ipsec profile EZVPN_VTI
 description TEST 7200vxr
 set transform-set 3DES_SHA_TUNNEL
 set isakmp-profile VTI_IKE_Profile_alpha
!
!
interface Loopback117
!
!  Assume this is a routable IP address
!
 ip address 192.168.136.17 255.255.255.255
!
interface Loopback901
 description Anchor for VTI
 ip address 10.9.100.1 255.255.255.255
!
!
interface FastEthernet0/1
 description Dot1Q Trunk
 no ip address
 load-interval 30
 duplex auto
 speed auto
!
interface FastEthernet0/1.100
 description fa0/1.100 outside
 encapsulation dot1Q 100
 ip address 192.168.131.20 255.255.255.224
 no snmp trap link-status
!
interface FastEthernet0/1.120
 description fa0/1.120 inside
 encapsulation dot1Q 120
 ip address 10.2.120.20 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.128
 encapsulation dot1Q 128
 ip address 10.2.128.20 255.255.255.0
 no snmp trap link-status
!
!
interface Virtual-Template154 type tunnel
 ip unnumbered Loopback901
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile EZVPN_VTI
 service-policy output Shaper-768K
!
router eigrp 100
 redistribute static metric 256 100 255 1 1408 route-map REDIST_STATIC
 network 10.0.0.0
```

```
 network 192.168.130.0 0.0.1.255
 network 192.168.136.0 0.0.1.255
 distribute-list ROUTES_for_REMOTE out Virtual-Template154
 no auto-summary
!
ip local pool MODE_network-plus 10.9.100.2 10.9.100.253
ip classless
ip route 0.0.0.0 0.0.0.0 Null0 20
ip route 172.26.0.0 255.255.0.0 172.26.170.1
ip route 192.0.2.0 255.255.255.0 Null0 240 name TEST-NET
!
!
ip pim autorp listener
!
ip access-list standard ROUTES_for_REMOTE
 permit 0.0.0.0
 deny   any
!
ip access-list extended SPLIT_TUNNEL_LIST
 permit ip 192.0.2.0 0.0.0.255 any
!
!
route-map REDIST_STATIC permit 10
 match ip address ROUTES_for_REMOTE
!
!
line con 0
 exec-timeout 120 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 15
 exec-timeout 0 0
 logging synchronous
 login authentication VTY
 transport input telnet ssh
!
ntp clock-period 17179944
ntp server 172.26.170.10
ntp server 192.168.130.1
!
!
!
end
```

Headend (Secondary)

```
!
! Last configuration change at 14:41:47 est Tue Dec 6 2005 by mrcisco
! NVRAM config last updated at 16:14:42 est Tue Dec 6 2005 by mrcisco
!
version 12.4
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname vpn-jk3-2651xm-9
!
boot-start-marker
boot-end-marker
```

```
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login VTY local
aaa authentication login EZVPNauthenlist local
aaa authorization network EZVPNauthorlist local
!
aaa session-id common
!
resource policy
!
clock timezone est -5
clock summer-time edt recurring
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
!
!
ip cef
no ip domain lookup
ip domain name ese.cisco.com
ip multicast-routing
!
!
username EZVPN_Test_user password 7 032E52060B1612 # Must match remote "JimmyS"
!
!
class-map match-any 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
!
policy-map V3PN-768
  description V3PN branch (4calls-768 BW)
  class CALL-SETUP
  bandwidth percent 2
  class INTERNETWORK-CONTROL
  bandwidth percent 5
  class VOICE
  priority 256
  class class-default
  fair-queue
  random-detect
!
policy-map Shaper-768K
  description 768K * .85 = 652
  class class-default
  shape average 652000 6520
  service-policy V3PN-768
!
!
crypto logging session
crypto logging ezvpn
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
```

```
crypto isakmp keepalive 10
!
crypto isakmp client configuration group RTP_ezvpn_group
 key MrExcitement
 domain cisco.com
 pool MODE_network-plus
 acl SPLIT_TUNNEL_LIST
 save-password
 configuration url ftp://root:cisco@172.26.157.11//usr/tmp/CFG-version11.txt
 configuration version 11
 banner ^C
==
====
====== Hello from vpn-jk3-2651xm-9
====
==
 ^C
crypto isakmp profile VTI_IKE_Profile_alpha
   match identity group RTP_ezvpn_group
   client authentication list EZVPNauthenlist
   isakmp authorization list EZVPNauthorlist
   client configuration address respond
   keepalive 10 retry 2
   virtual-template 154
   local-address Loopback119
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
!
crypto ipsec profile EZVPN_VTI
 description TEST of dual head-ends
 set transform-set 3DES_SHA_TUNNEL
 set isakmp-profile VTI_IKE_Profile_alpha
!
interface Loopback119
!
!   Assume this is Internet routable address space
!
 ip address 192.168.136.19 255.255.255.255
!
interface Loopback801
 description Anchor for VTI
 ip address 10.8.100.1 255.255.255.255
!
interface FastEthernet0/0
 description FLASH156  ***  The FTP Server is on this Interface
 ip address 172.26.157.39 255.255.254.0
 no ip proxy-arp
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description TRUNK
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.100
 description Outside interface
 encapsulation dot1Q 100
 ip address 192.168.131.19 255.255.255.224
 no snmp trap link-status
!
interface FastEthernet0/1.102
```

```
 description Outside interface
 encapsulation dot1Q 102
 ip address 192.168.131.39 255.255.255.224
 no snmp trap link-status
!
interface FastEthernet0/1.128
 description Inside interface
 encapsulation dot1Q 128
 ip address 10.2.128.19 255.255.255.0
 no snmp trap link-status
!
interface Virtual-Template154 type tunnel
 ip unnumbered Loopback801
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile EZVPN_VTI
 service-policy output Shaper-768K
!
router eigrp 100
 redistribute static metric 256 100 255 1 1408 route-map REDIST_STATIC
 network 10.0.0.0
 network 172.26.156.0 0.0.1.255
 network 192.168.130.0 0.0.1.255
 network 192.168.136.19 0.0.0.0
 distribute-list ROUTES_for_REMOTE out Virtual-Template154
 no auto-summary
!
ip local pool MODE_network-plus 10.8.100.2 10.8.100.253
ip classless
ip route 0.0.0.0 0.0.0.0 Null0 20
ip route 172.26.0.0 255.255.0.0 172.26.156.1 name FLASH156net
ip route 172.26.179.249 255.255.255.255 172.26.156.1 name ese-ios-ca
ip route 192.0.2.0 255.255.255.0 Null0 240 name TEST-NET
!
ip pim autorp listener
!
ip access-list standard ROUTES_for_REMOTE
 permit 0.0.0.0
 deny   any
!
ip access-list extended SPLIT_TUNNEL_LIST
 permit ip 192.0.2.0 0.0.0.255 any
!
route-map REDIST_STATIC permit 10
 match ip address ROUTES_for_REMOTE
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password 7 00071A150754
!
ntp clock-period 17208438
ntp server 192.168.130.1
!
end
```

IP Multicast

This section describes VTI support of IPmc.

Topology

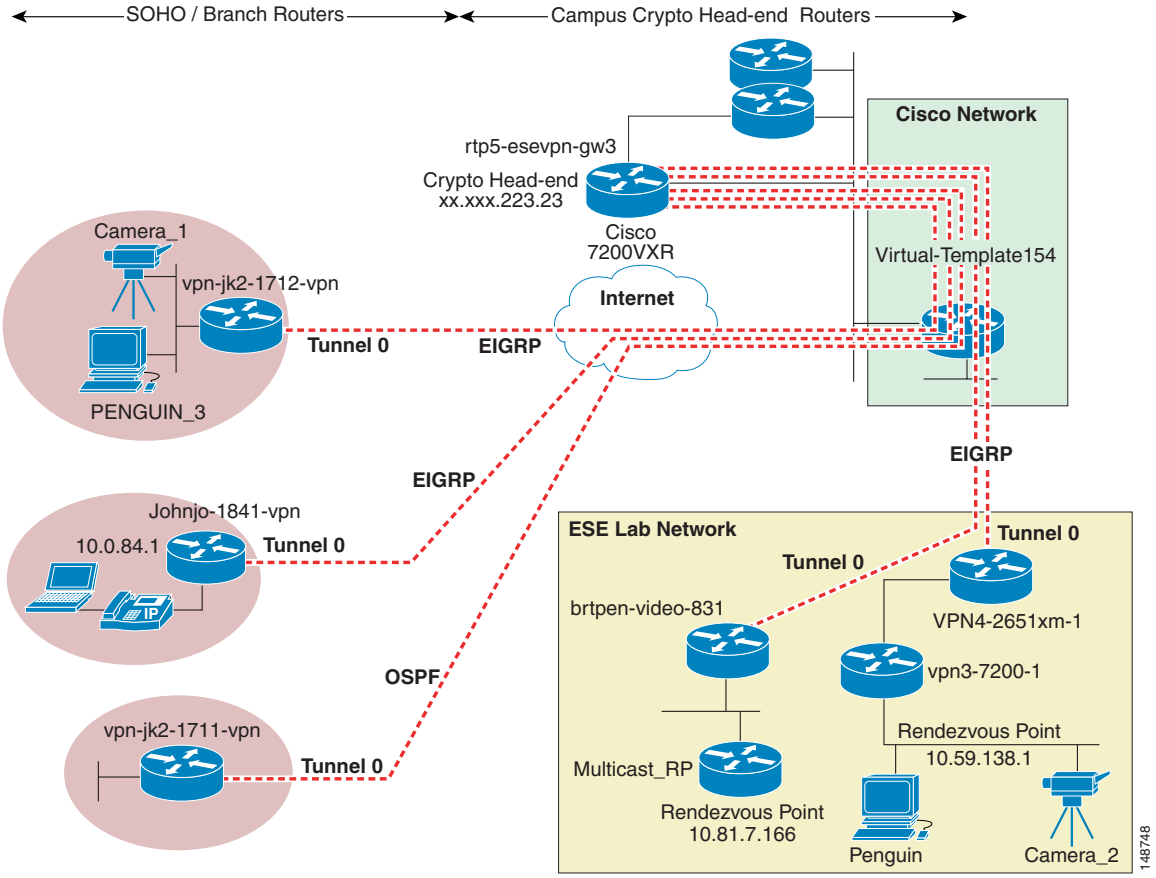
To demonstrate a working configuration of VTI support of IPmc, this deployment is implemented over broadband Internet connections and the internal Cisco network. Several different series of branch routers are deployed: Cisco 830, 1700, 1800, and 2600 Series along with a 7200VXR Series headend router.

All of the following were configured: EIGRP, OSPF, and PIM sparse mode with the **ip pim autorp listener** command and two *rendezvous points*. Panasonic video surveillance cameras are deployed as IPmc sources, and the Panasonic multicast plug-in for a web browser is the sink.

Note *Multicast over IPsec VPN Design Guide* uses this topology with GRE tunnels and dynamic IPsec crypto maps.

The basic topology is implemented as shown in Figure 12.

Figure 12 IP Multicast Topology



There are two cameras, and any branch can view both cameras. Additionally, there are two rendezvous points.

EIGRP Headend Router Configuration

The relevant portion of the Cisco 7200VXR Series headend router is shown as follows:

```
hostname rtp5-esevpn-gw3
interface Loopback0
 description Public address
 ip address xx.xxx.223.23 255.255.255.255
interface Loopback10
 description Loopback for VTI/Virtual-Template154
 ip address 10.81.7.216 255.255.255.255
 ip pim sparse-mode
interface Virtual-Template154 type tunnel
 description 1.544Kbps DOWNLINK
 ip unnumbered Loopback10
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 ip ospf mtu-ignore
 no ip mroute-cache
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VirtualTunnelInterface
 service-policy output Shaper-1544K
!
router eigrp 64
 redistribute static metric 9 5000 255 1 1408 route-map QUAD_ZERO
 redistribute ospf 64 metric 9 5000 255 1 1408
 network 10.81.7.0 0.0.0.255
 network 192.168.82.0
 distribute-list Quad_ZERO_to_BRANCH out Virtual-Template154
 no auto-summary
ip access-list standard Quad_ZERO_to_BRANCH
 permit 0.0.0.0
route-map QUAD_ZERO permit 10
 match ip address Quad_ZERO_to_BRANCH
!
ip route 0.0.0.0 0.0.0.0 10.81.0.17
end
```

Interface Loopback10 has PIM enabled as the Virtual-Template154 borrows the IP address of loopback10. This is required in the configuration. The virtual template is process-switching IPmc. The DDTs for this caveat are listed later in the section. QoS is enabled on the virtual template and the EIGRP configuration is advertising only a default route to the branch routers.

EIGRP Branch Router Configuration

A portion of one branch router configuration is shown below:

```
hostname johnjo-1841-vpn
interface Tunnel0
 description -> rtp5-esevpn-gw3
 ip unnumbered Loopback1
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 no ip mroute-cache
 tunnel source FastEthernet0/0
 tunnel destination xx.xxx.223.23
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VirtualTunnelInterface
interface Loopback1
 ip address 10.81.7.227 255.255.255.255
```

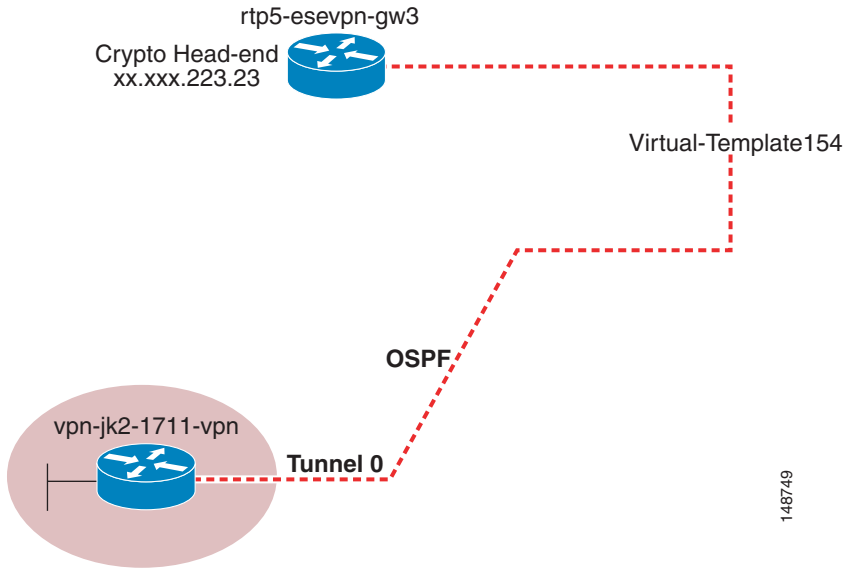
```
 ip pim sparse-mode
!
interface FastEthernet0/1
 description Inside
 ip address 10.81.7.105 255.255.255.248
ip route xx.xxx.223.23 255.255.255.255 dhcp                    #Crypto Head-end
ip route 192.5.41.40 255.255.255.254 dhcp                      #NTP Servers
router eigrp 64
 network 10.0.0.0
 distribute-list ENTERPRISE_NET out Tunnel0
 no auto-summary
!
ip access-list standard ENTERPRISE_NET
 permit 10.81.7.104
 permit 10.81.7.227
end
```

The Tunnel0 interface of the branch router is similarly configured to the virtual template on the crypto headend. However, no QoS service policy is configured under the Tunnel0 because this router is configured with VLANs to support a “spouse-and-child” subnet, and therefore the QoS service policy must be on the outside physical interface to prioritize all traffic properly. EIGRP is configured to advertise the inside network and the Loopback1 interface to the headend. The Tunnel0 interface is borrowing the IP address of Loopback1.

OSPF and PIM Headend Router Configuration

OSPF is now introduced to the headend router configuration (see Figure 13). OSPF is enabled on the same Virtual-Template154 as is currently configured with EIGRP. One branch router, named vpn-jk2-1711-vpn, is enabled with OSPF, and after it connects with the headend, an OSPF neighbor relationship forms.

Figure 13 OSPF and PIM Headend Router Configuration



The following is the relevant portion of the headend configuration:

```
hostname rtp5-esevpn-gw3
interface Loopback0
```

```
 description Public address
 ip address xx.xxx.223.23 255.255.255.255
interface Loopback10
 description Loopback for VTI/Virtual-Template154
 ip address 10.81.7.216 255.255.255.255
 ip pim sparse-mode
interface Virtual-Template154 type tunnel
 description 1.544Kbps DOWNLINK
 ip unnumbered Loopback10
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 ip ospf mtu-ignore
 no ip mroute-cache
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VirtualTunnelInterface
 service-policy output Shaper-1544K
router ospf 64
 router-id 10.81.7.216
 log-adjacency-changes detail
 network 10.81.7.0 0.0.0.255 area 154
 default-information originate always
!
router eigrp 64
 redistribute static metric 9 5000 255 1 1408 route-map QUAD_ZERO
 redistribute ospf 64 metric 9 5000 255 1 1408
 network 10.81.7.0 0.0.0.255
 network 192.168.82.0
 distribute-list Quad_ZERO_to_BRANCH out Virtual-Template154
 no auto-summary
 no eigrp log-neighbor-warnings
!
end
```

The OSPF configuration advertises a default route to the branch router. The routes learned from the branch are redistributed into the base EIGRP configuration. The redistribution is not a requirement; it is simply for illustration because the core network IGP is EIGRP in this instance.

OSPF and PIM Branch Router Configuration

The branch router configuration is similar to the other configurations in this section.

```
hostname vpn-jk2-1711-vpn
interface Tunnel0
 description -> rtp5-esevpn-gw3
 ip unnumbered Loopback1
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 ip ospf mtu-ignore
 no ip mroute-cache

 tunnel source FastEthernet0
 tunnel destination xx.xxx.223.23
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VirtualTunnelInterface
interface Loopback1
 ip address 10.81.7.225 255.255.255.255
 ip pim sparse-mode
interface Vlan1
 description Inside
 ip address 10.81.7.201 255.255.255.248
```

```
 ip pim sparse-mode
...
router ospf 64
 router-id 10.81.7.225
 log-adjacency-changes detail
 network 10.81.7.200 0.0.0.7 area 154
 network 10.81.7.225 0.0.0.0 area 154
ip route xx.xxx.223.23 255.255.255.255 dhcp              #Crypto Head-end
ip route 192.5.41.40 255.255.255.254 dhcp                #NTP Servers
ip pim autorp listener
ip multicast-routing
end
```

Note that there are two OSPF network statements: one covering the inside VLAN network, and a second network statement with a single address covering the loopback interface.

Note For more information, see the following CCO Tech Note: "Why are OSPF Neighbors Stuck in Exstart/Exchange State?" at the following URL: http://www.cisco.com/en/US/partner/tech/tk365/technologies_tech_note09186a0080093f0d.shtml

Caveats

There are two caveats for the configurations in this section:

- When using IP unnumbered, include **ip pim sparse-mode** on the interface providing the address for the IP unnumbered interface, as well as the tunnel interface.
- As documented in the *Multicast over IPsec VPN Design Guide*, IPmc is configured as process switched.

Address Conservation

This section discusses advantages and disadvantages of addressing schemes for VTI.

Overview of IP Unnumbered

Dynamic VTI configurations as shown in this guide require the use of an IP unnumbered interface on the headend virtual template because they are session-based. The branch tunnel interface should also be IP unnumbered for routing protocols such as OSPF to properly form neighbor relationships. Do not use IP unnumbered on the headend and a static IP address on the branch tunnel interface.

Note With OSPF using a static IP address on the branch router and IP unnumbered on the virtual template, OSPF neighbors come up but the branch does not receive any OSPF routes from the headend.

Use of the IP unnumbered is valid only on point-to-point interfaces. An IP unnumbered interface should reference an interface that is up and running. This is why loopback interfaces are generally recommended.

Routes learned through the IP unnumbered interface have the *interface* as the next hop instead of the source address of the routing update.

The disadvantage of the IP unnumbered interface is that the tunnel interface is unavailable by IP address for remote testing and management.

The headend router can use the same IP unnumbered interface when multiple ISAKMP profiles reference the same virtual template.

Unlike mGRE (DMVPN) interfaces, the VTI tunnel interface consume no IP network addresses. Point-to-point interfaces may be IP unnumbered; multipoint interfaces cannot.

Migrating branch routers among available headends for capacity planning is very simple. The *tunnel destination* IP address on the branch router is simply changed from the existing crypto headend IP address to the new crypto headend IP address. The routing protocol forms a new adjacency with the new crypto headend, and the remote subnet is advertised to the network core. No WAN addressing need be changed.

For a more thorough description of IP unnumbered, see *Understanding and Configuring the ip unnumbered Command* (Document ID: 13786) at the following URL: http://www.cisco.com/warp/public/701/20.html.

Loopback versus Inside Ethernet/FastEthernet

Many of the examples in this guide show the use of a loopback interface on the branch router as the target of the branch tunnel IP unnumbered interface configuration. The inside Ethernet interface of the branch router can be used as an alternative. This eliminates the need to allocate address space for the loopback interface and may simplify the routing protocol portion of the configuration.

An IP unnumbered interface should reference an interface that is up and running.

Note The **no keepalive** command can be configured on Ethernet/FastEthernet interfaces to prevent an UP/DOWN status. However, on the Cisco 1700 Series routers that have switchports and VLAN configurations (as is the case with the 1711), you must have one switchport in the VLAN connected to a device before the VLAN interface is UP/UP.

Examples

This section provides examples of using an inside address instead of a loopback.

EIGRP Stub

The following example shows the use of the FastEthernet0/1 interface as the borrowed IP address for **ip unnumbered** and the use of EIGRP stub.

```
hostname johnjo-1841-vpn
interface Tunnel0
 description -> rtp5-esevpn-gw3
 ip unnumbered FastEthernet0/1
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 no ip mroute-cache
 tunnel source FastEthernet0/0
 tunnel destination xx.xxx.223.23
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
interface FastEthernet0/1
 description Inside
 ip address 10.81.7.105 255.255.255.248
 …
interface FastEthernet0/0
 description Outside
```

```
 ip address dhcp
 …
!
router eigrp 64
 network 10.0.0.0
 no auto-summary
 eigrp stub connected
end
```

OSPF

The following example shows the use of the VLAN1 interface as the borrowed IP address for **ip unnumbered** and the use of OSPF.

```
hostname vpn-jk2-1711-vpn
interface Tunnel0
 description -> rtp5-esevpn-gw3
 ip unnumbered Vlan1
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 ip ospf mtu-ignore
 no ip mroute-cache
 load-interval 30
 tunnel source FastEthernet0
 tunnel destination xx.xxx.223.23
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
!
interface FastEthernet0
 description Outside
 ip address dhcp
 …
interface Vlan1
 description Inside
 ip address 10.81.7.201 255.255.255.248
 …
router ospf 64
 router-id 10.81.7.201
 log-adjacency-changes detail
 network 10.81.7.200 0.0.0.7 area 154
end
```

High Availability

VTI failover and high availability have not currently been thoroughly tested. The topology and performance should be similar to the "p2p GRE–Single Tier Headend Architecture" section in the *Point-to-Point GRE over IPsec Design Guide* at the following URL: http://www.cisco.com/go/srnd. High availability depends on the settings of the routing protocol being used for timing and path selection.

Interaction with other Networking Functions

Other networking functions such as PAT, DHCP, and firewall considerations apply to designing an IPsec direct encapsulation network. This section describes these functions.

Network Address Translation and Port Address Translation

Although NAT and PAT can result in an added layer of security and address conservation, they both present challenges to the implementation of an IPsec VPN. Internet Key Management Protocol (ISAKMP) relies on an individual IP address per crypto peer for proper operation. PAT works by masquerading multiple crypto peers behind a single IP address.

The IPsec NAT Traversal feature (NAT-T) introduces support for IPsec traffic to travel through NAT or PAT devices by encapsulating both the IPsec SA and the ISAKMP traffic in a UDP wrapper. NAT-T was first introduced in Cisco IOS version 12.2(13)T, and is auto-detected by VPN devices. There are no configurations steps for a Cisco IOS router running this release or later because it is enabled by default as a global command. NAT-T feature detects a PAT device between the crypto peers and negotiates NAT-T if it is present.

For information about IPsec NAT Traversal (also known as NAT Transparency), see the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftipsnat.htm

Dynamic Host Configuration Protocol

For a host at a remote site to be able to use a DHCP server over an IPsec tunnel at a central site, an IP helper address must be configured on the router interface associated with the host.

One drawback of this approach is that if connectivity to the central site is lost, a host at a remote site may not receive or renew an IP address. The inability to receive an IP address results in the host being unable to communicate to the local network.

A Cisco IOS router can be configured as a DHCP server. Using the router as a stand-alone DHCP server is recommended for branch offices with no redundant links.

Firewall Considerations

This section describes various firewall considerations when implementing a DVTI design.

Headend or Branch

Depending on the DVTI headend or branch placements, the following protocols and ports are required to be allowed:

- UDP Port 500—ISAKMP as source and destination
- UDP Port 4500—NAT-T as a destination
- IP Protocol 50—ESP
- IP Protocol 51—AH (if AH is implemented)

Network location of the crypto headend in relation to the headend firewall(s) impacts both the accessibility and performance of the both systems. The network manager must ensure that all firewalls are properly configured to allow bi-directional tunnel traffic. The crypto headend must be accessible to the branch router.

Common Configuration Mistakes

The following sections outline some common mistakes and problems encountered when configuring DVTI.

Transform Set Matching

At least one matching IPsec transform set must be configured between two crypto peers. When specifying a particular strength of encryption algorithm, a similar strength encryption algorithm should also be configured. Failure to do so could weaken the encryption strength of the entire solution.

ISAKMP Policy Matching

There is a default ISAKMP policy present in all Cisco IOS devices. This default is encryption DES, HMAC of SHA, IKE Authentication of RSA signature, DH group 1. If a stronger ISAKMP policy is desired, both sides must support that policy.

It is common, but not required, to use the same encryption level transform-set and hash methods in the ISAKMP policy and the IPsec transform set.

Scalability Considerations

The following scalability testing was performed with traffic shaping and CBWFQ on all the tests. There are currently no results for DVTI without the traffic shaping and CBWFQ or with Enhanced EZVPN features. It is expected that the DVTI scalability results will be similar to the p2p GRE over IPsec if traffic shaping is applied to the tunnel interfaces.

QoS Configuration for Performance Testing

The same policy map configuration is used on the branch and headend router. This QoS configuration is typical of a V3PN deployment.

Policy Map for Branch and Headend

The following branch service policy is applied to a tunnel interface, and on the headend it is applied to a virtual template or to an ATM sub-interface:

```
policy-map V3PN
  description V3PN branch (4calls-768 BW)
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 256
 class class-default
  fair-queue
  random-detectpolicy-map Shaper-768K
  description 768Kbps * .85 = 652Kbps
 class class-default
  shape average 652000 6520
  service-policy V3PN
```

Note CALL-SETUP is configured but no traffic matching this class is included in the traffic profile.

Note The traffic profile includes packets marked AF21; these fall into class-default and can be seen being counted under the WRED configuration as IP Precedence

Branch Configuration

The following branch configuration is used in all testing:

```
interface Tunnel1
 description VTI to wpoc1-r1
 bandwidth 768
 ip unnumbered Ethernet1/0
 tunnel source FastEthernet0/1
 tunnel destination 192.168.136.17
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
 service-policy output Shaper-768K
```

Headend using Virtual Template Interface

The following headend configuration is used when testing hierarchical CBWFQ on the virtual template interface:

```
interface Virtual-Template1 type tunnel
 bandwidth 768
 ip unnumbered Loopback901
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0 5
 ip summary-address eigrp 100 10.0.0.0 255.0.0.0 5
 tunnel source Loopback117
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
 service-policy output Shaper-768K
```

Target-Shaped Rate

Shaping packets is very CPU-intensive. Typically, in a teleworker environment, this CPU consumption is of no consequence for the branch router, but it is a concern for the crypto headend router. These performance tests use branch rather than teleworker or SOHO class devices. In some cases, shaping at T1 data rates using a Cisco 2651XM as a branch router exhausted the CPU of that branch router.

The target-shaped rate is 768 Kbps upstream and downstream. Upstream refers to the branch router shaping (hierarchical CBWFQ) on the tunnel interface. Downstream refers to the configuration of the headend router, including a hierarchical CBWFQ in the virtual template interface or CBWFQ on an ATM PVC. VTI allows each connected branch to have its own virtual access interface spawned from the virtual template. Essentially, this implementation creates a “dynamic” tunnel interface on the headend. VTI is used in all tests; the only difference is where the QoS service policy is configured.

The goal of this testing and configuration is to shape the traffic to a rate so that as the encrypted packets reach the core network (assumed to be an ISP) the volume of data approaches but does not generally exceed the target-shaped rate. For example, if an ISP is providing a T1 link to the branch with no downstream QoS, the headend should not send more than 1.5 Mbps of encrypted data for that branch to the service provider.

Upstream QoS can be accomplished by either hierarchical CBWFQ inside the branch tunnel interface or on the physical interface itself if it is a physical interface such as a serial T1 link. However, because branch routers can be connected by a broadband link with the physical link terminated on a cable or DSL modem with no congestion feedback from the physical interface, the test configurations use hierarchical CBWFQ on the tunnel interface of the branch router.

The target-shaped rate for most of the testing is 768 Kbps, because it is the lowest data rate voice that can be transmitted without addressing Layer 2 fragmentation (LFI or FRF.12). The traffic profile is expected to engage the shaper logic more frequently than at a higher data rate.

The actual configured shaped rate may be more or less that the target-shaped rate. This depends on whether the packets are shaped pre-crypto or post-crypto and whether shaping is at Layer 3 or at Layer 2 (for example, on ATM cells).

Netflow is used in the WAN to verify that the configured shaped rates send sufficient data to approach but not exceed the target-shaped rate.

Figure 14 illustrates how different configured shaped rates can produce a similar target-shaped rate in the ISP core.

Figure 14 Illustration of Target-Shaped Rate

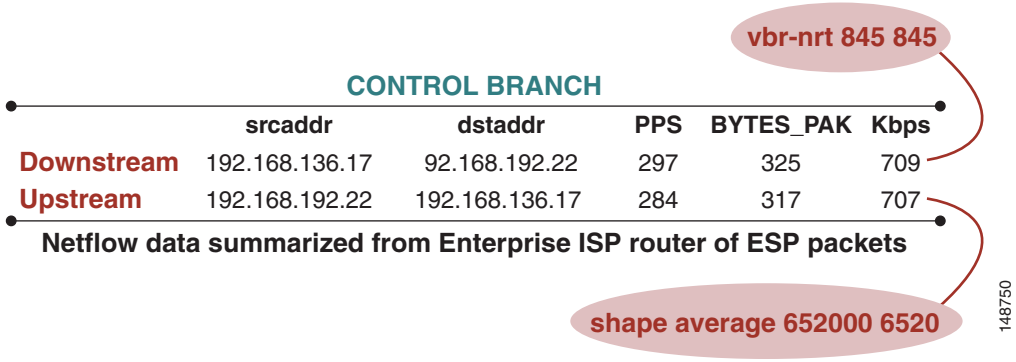


Figure 14 represents the upstream and downstream flows. Netflow data exports include a time stamp that is used to calculate the duration of the flow in milliseconds (ms). It also includes the number of packets and total bytes in the flow. From this data, the packet per second rate, average bytes per packet, and Kbps can be accurately calculated for the duration of the test. These packet sizes are based on the Layer 3 size of the packet.

By shaping at an average rate of 652,000 bps on the tunnel interface, after tunnel and IPsec encapsulation is added and the ESP packet arrives on the WAN router, the Kbps is observed at 707 Kbps.

Scaling Recommendations

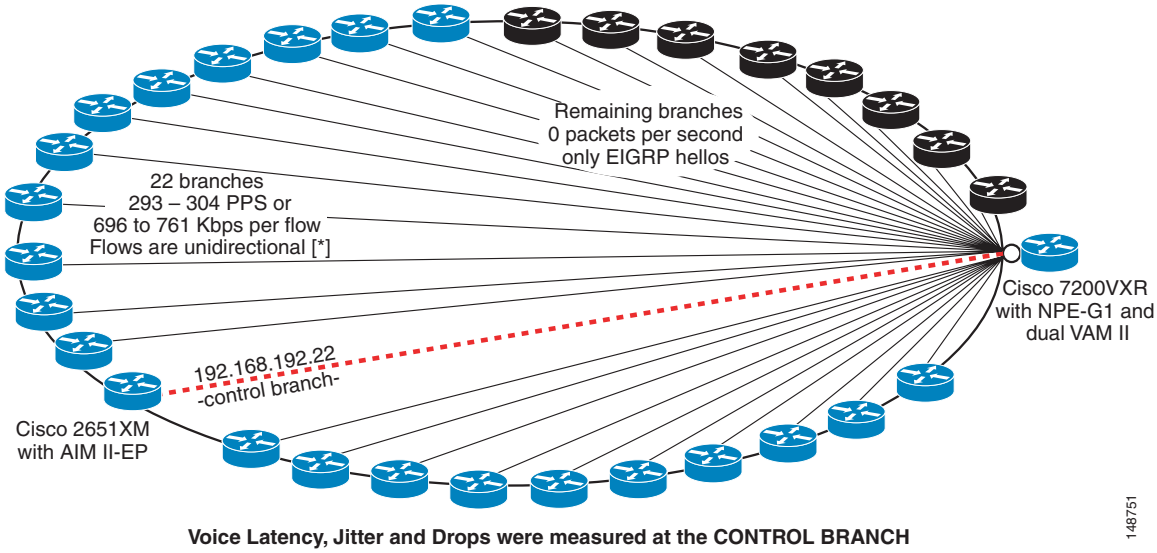
In testing, so as not to exceed 80 percent CPU utilization on the crypto headend router, the number of branches using an upstream/downstream target-shaped rate of 768 Kbps must not exceed 22.

Test results are as follows:

- Headend CPU is 80 percent at 13,125 pps, or approximately 32 Mbps
- Control branch CPU is 49 percent and is 100 percent process-switched

This is illustrated in Figure 15.

Figure 15 Active Branches per Headend



Voice Latency, Jitter and Drops were measured at the CONTROL BRANCH

[*] Each active branch in total (RX + TX) approximately 600 pps or 1.4M bps

As shown in Figure 15, more than 22 branches can be configured; however, these branches cannot send any appreciable amount of packets per second.

The summarized Netflow data per branch used to derive the above figure is shown in Netflow Summary Table, page 72.

Scalability Test Results (Unicast Only)

This section provides scalability results to provide a better understanding of VTI performance.

Scalability Test Methodology

For most of the traffic sent through the network, flows are established using the Ixia Chariot testing tool. The bps mix of traffic is approximately 35 percent UDP and 65 percent TCP; application types represented in the mix include the following: VoIP, FTP, DNS, HTTP, POP3, and TN3270. The average packet size is 188 bytes, from headend-to-branch, and 144 bytes from branch to headend. This relatively small average packet size ensures that the scalability results presented support a converged network design, and tend to be fairly conservative. A network carrying data-only traffic, with a larger average packet size, may achieve better bps performance than that listed here. However, the pps performance given a specific CPU value should be the same.

The traffic profile used in testing is shown in Table 2.

Table 2 Traffic Profile Used for Testing

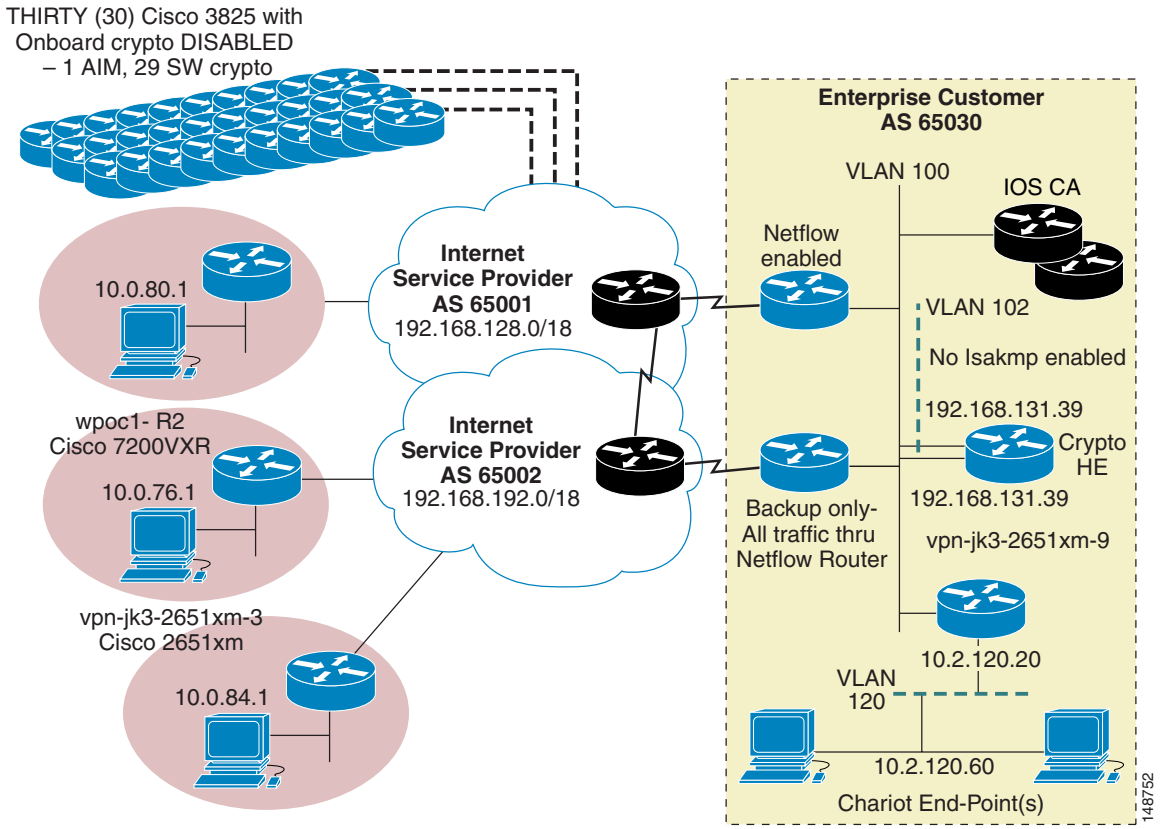
Flows/Streams	Description
4 calls	G.729 Voice (8 streams or 400 pps)
9	DNS
4	POP3
12	TN3270 (6 Best Effort and 6 AF21)
6	HTTP (3 Best Effort and 3 AF21)
4	FTP (2 upstream, 2 downstream 768 Kbps file size)

This profile is also used in V3PN testing.

Scalability Test Bed Network Diagram

The test topology diagram is shown in Figure 16.

Figure 16 Scalability Test Bed Network Diagram



Key elements of the topology shown in Figure 16 are as follows:

- A second headend crypto router is configured on some branch routers because this is the preferred configuration in an actual customer deployment. Most customers expect to have an active tunnel to at least two headend crypto routers for backup and optionally load sharing. However, to facilitate testing, ISAKMP is disabled (**no crypto isakmp enable**) on this backup headend.
- The topology simulates the Internet connectivity of a typical enterprise customer. Two eBGP-speaking routers in the enterprise campus network connect to their respective ISP routers by an ATM OC3 interface. The ISP routers are also interconnected by an ATM OC3 interface.
- To simplify the Netflow capture, only one ISP link is used. The second ISP link is a backup. To accomplish this, as-path prepend is configured on each eBGP router supporting the backup link.
- The enterprise eBGP router on the primary ISP link has Netflow enabled and is exporting data to a UNIX workstation. The flows are captured and summarized and are included in the stored test results. Netflow Summary Table, page 72 provides a detailed summary table as an illustration. The captured Netflow data is used to calculate the packets per second, average bytes per packet, and Kbps for the ESP (protocol 0x “50”) flows between branch and headend for each branch.
- Both pre-shared keys and PKI/CA are used, at different times, in these tests.

Voice Performance for the Control Branch

The traffic upstream and downstream for the control branch in this test is shown in Figure 17.

Figure 17 Control Branch Performance

CONTROL BRANCH

	srcaddr	dstaddr	PPS	BYTES_PAK	Kbps
Downstream	192.168.136.17	92.168.192.22	297	325	709
Upstream	192.168.192.22	192.168.136.17	284	317	707

Netflow data summarized from Enterprise ISP router of ESP packets

Voice -G.729 Average	Branch to Head	Head to Branch
Loss	.5%	0%
Delay	24ms	9ms
Jitter	3.8ms	3.0ms

148753

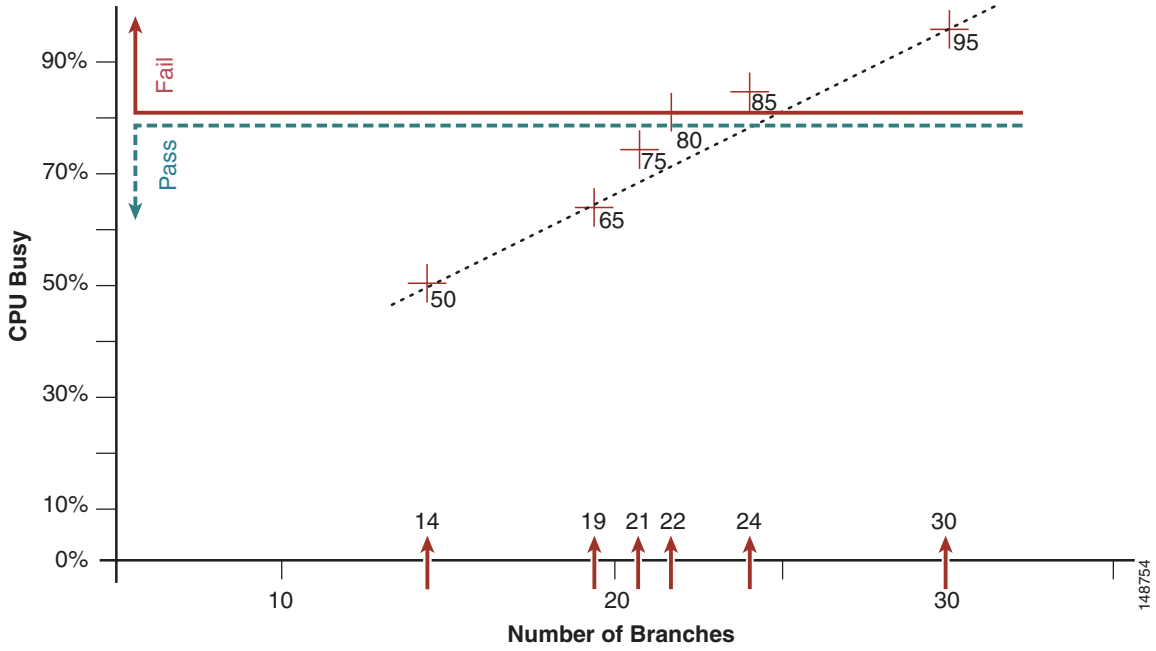
Because the traffic flow included 4 G.729 voice calls, 200 pps in each direction are the result of these four calls. Therefore, approximately 96–99 pps are data.

The reported characteristics of voice loss, delay, and jitter are all very good. The only value approaching a testing threshold is voice loss from branch to head.

Headend CPU Utilization (by Number of Branches)

Figure 18 shows the CPU utilization of the headend crypto router when the number of active branches varies from a low of 14 to the upper bound of 30. Both the upstream and downstream target-shaped rate is 768 Kbps.

Figure 18 Headend CPU by Number of Branches



This test determines whether CPU consumption increases linearly as the number of branches increases.

A target-shaped rate of 768 Kbps is very likely too low for many branch deployments. Various rates are shown in the next section.

Tests Varying the Shaped Rate

The goal of this test phase is to vary the target shaper rate above and below 768 Kbps to determine the change in headend CPU utilization. Table 3 shows the results.

Table 3 Varying the Shaped Rates

Headend CPU %	Number of Branches	Shaper Target Rate (in Kbps)	Approx. pps per Branch	Result
36%	30	192	174	Passed
67%	30	512	433	Passed
80%	12	1536	1148	Control branch, Cisco 2651XM CPU too high

The number of branches available for testing is limited to 30. The traffic profile is modified to maintain the voice calls at 33 percent of the target-shaped rate. It is unlikely enterprise customers would want to limit the downstream rate at 512 Kbps or below when transporting voice, because these rates would need some form of Layer 2 fragmentation and interleaving. These data rates are shown only for illustration.

The T1 target-shaped rate is a more common value in that many customers can purchase Internet T1s cost-effectively. Shaping downstream is desired if the ISP does not offer QoS on the edge. However, supporting only 12 branches makes this a very costly solution. It is unlikely any customer would deploy this solution.

Scalability Conclusion

Downstream QoS, queueing within a shaped rate per tunnel, is effective for preserving voice quality. However, the number of branches that can be supported while maintaining a reasonable headend CPU load may be less that many customer deployments require.

Software Releases Evaluated and Caveats

Table 4 lists the software releases used in the scalability testing.

Table 4 Software Releases Evaluated for Scale Test

Cisco Product Family	Software Release
Cisco headend routers Cisco 7206VXR with NPE-G1 and dual VAM-II	Cisco IOS 12.4(3.6)
Cisco branch router Cisco 2651XM (AIM-II EP)	Cisco IOS 12.4(3.6)
Cisco branch router Cisco 3825 (onboard crypto engine)	Cisco IOS 12.4(3.6)

The test topology consists of 30 Cisco 3825 routers with onboard crypto engines as branch routers added to the proof-of-concept lab network of the design engineer. One branch is the control branch. Voice latency, loss, and jitter are determined from traffic flowing through the control branch. The control branch is a Cisco 2651XM with an AIM II–EP.

During the setup phase of the test, the following software defect was identified and subsequently opened: CSCsb68839-”3825 onboard crypto engine HW” is not marking TTL on IPsec IP hdr 255.

One Cisco 3825 is using an AIM II as part of this troubleshooting process. The onboard crypto accelerator on the other 29 Cisco 3825 routers is disabled. No voice statistics are taken from these branches; only the control branch.

The crypto headend router is a Cisco 7200VXR NPE-G1 with dual VAM II. There is no performance requirement for two VAM II adapters because in all cases the main CPU busy percentage is the limiting factor.

Scalability Test Bed Configuration Files

This section provides scalability test bed configurations.

Cisco 7200VXR Headend Configuration

The VTI headend router in the testbed has VTI with an IP address that is the target of the branch that belongs to that group. The following configuration is for Headend #1:

```
hostname wpoc1-r1
no aaa new-model
ip subnet-zero
ip cef
controller ISA 5/1
controller ISA 6/1
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
policy-map V3PN
  description V3PN branch (4calls-768 BW)
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 256
 class class-default
  fair-queue
  random-detect
policy-map Shaper-768K
  description 768Kbps * .85 = 652
 class class-default
  shape average 652000 6520
  service-policy V3PN
crypto keyring PRESHARE
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
crypto isakmp policy 8
 encr 3des
 authentication pre-share
 group 2
crypto isakmp profile PRESHARE
   description TEST for 30 branch routers VTI Templates 768Kbps
   keyring PRESHARE
   match identity address 0.0.0.0
   keepalive 10 retry 2
   virtual-template 1
   local-address Loopback117
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec profile VTI
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
 set isakmp-profile PRESHARE
interface Loopback117
 ip address 192.168.136.17 255.255.255.255
interface Loopback901
 ip address 10.9.100.1 255.255.255.255
interface FastEthernet0/1
```

```
 description Dot1Q Trunk
 no ip address
 load-interval 30
 duplex auto
 speed auto
interface FastEthernet0/1.100
 description fa0/1.100 - Outside
 encapsulation dot1Q 100
 ip address 192.168.131.20 255.255.255.224
 no snmp trap link-status
interface FastEthernet0/1.120
 description fa0/1.120 - Inside
 encapsulation dot1Q 120
 ip address 10.2.120.20 255.255.255.0
 no snmp trap link-status
interface FastEthernet0/1.128
 encapsulation dot1Q 128 - Other Inside
 ip address 10.2.128.20 255.255.255.0
 no snmp trap link-status
interface Virtual-Template1 type tunnel
bandwidth 768
 ip unnumbered Loopback901
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0 5
 ip summary-address eigrp 100 10.0.0.0 255.0.0.0 5
 tunnel source Loopback117
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
 service-policy output Shaper-768K
router eigrp 100
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 network 192.168.136.0 0.0.1.255
 no auto-summary
ip classless
```

Branch Office Configuration

The following shows relevant configurations for one branch router. The crypto peer is the crypto peer of the VTI headend. The following configuration for Branch #1 shows QoS for VoIP flows (shaping and queuing) applied to the tunnel interface:

```
hostname vpn-jk3-2651xm-2
no aaa new-model
ip subnet-zero
ip cef
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
policy-map V3PN
  description V3PN branch (4calls-768 BW)
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 256
```

```
 class class-default
  fair-queue
  random-detect
policy-map Shaper-768K
  description 768Kbps * .85 = 652
 class class-default
  shape average 652000 6520
  service-policy V3PN
crypto isakmp policy 8
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco address 192.168.136.17
crypto isakmp keepalive 10
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec profile VTI
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
interface Tunnel1
 description VTI to wpoc1-r1
 bandwidth 768
 ip unnumbered Ethernet1/0
 tunnel source FastEthernet0/1
 tunnel destination 192.168.136.17
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
 service-policy output Shaper-768K
interface FastEthernet0/1
 description FastEthernet0/1 - Outside
 ip address 192.168.192.22 255.255.255.0
 ip virtual-reassembly
 duplex auto
 speed auto
interface Ethernet1/0
 description Ethernet1/0 - Inside
 ip address 10.0.84.1 255.255.255.0
 ip virtual-reassembly
 half-duplex
 no keepalive
router eigrp 100
 network 10.0.0.0
 no auto-summary
 eigrp stub connected
ip classless
ip route 192.168.136.0 255.255.255.0 192.168.192.2 name ISP_router
```

Alternate Method for Scaling Traffic Shaping Using an ATM PA-A3 Interface

This case study is provided as an alternative method for scaling traffic shaping using an ATM PA-A3 interface.

Goal

The primary goal of these tests is to quantify the performance characteristics of queuing within a shaped rate at the enterprise campus headend for traffic destined to branch routers.

Enterprise customers are interested in this concept as traditional Frame Relay WANs or Frame-to-ATM service interworking WANs are replaced with IPsec VPNs using lower cost ISP connectivity. Customers want to preserve the headend shaping functionality of Frame Relay and ATM on a per-PVC basis because many ISPs do not offer QoS-enabled links to the branch location.

The tested designs shape and queue traffic within the shaped rate on a per-branch basis. These methods are the following:

- Hierarchical CBWFQ-virtual template interface (this method is discussed in the main body of this document)
- ATM shaping before encryption

The IPsec configuration is based on VTI, which offers the enterprise customer the advantage of a dynamically spawned tunnel interface. It is similar to implementing dynamic IPsec crypto maps with static p2p GRE tunnels per branch; however, the need to pre-define the p2p GRE tunnel interface on the headend is eliminated.

Performance Testing Overview

The performance test goals are to determine the number of branch routers a Cisco 7200VXR NPE-G1 with dual VAM II hardware encryption accelerators can support in a customer deployment. One known limitation of hierarchical CBWFQ, queuing within a shaped rate, is that all packets are punted to the process-switched path when the shaping is engaged. When the shaper is not active, packets can be switched in the fast or CEF switching paths.

As an alternative method, using an ATM PA-A3 interface to shape at the ATM cell level and queue within that rate is also tested. Packets do not need be process-switched because the shaping is offloaded to the PA-A3.

QoS Configuration for Performance Testing

The same policy map configuration is used on the branch and headend router. This QoS configuration is typical of a V3PN deployment.

Policy Map for Branch and Headend

The branch service policy is applied to a tunnel interface, and on the headend, it is applied to a virtual template or to an ATM sub-interface.

Note Note that CALL-SETUP is configured, but no traffic matching this class is included in the traffic profile.

```
policy-map V3PN
  description V3PN branch (4calls-768 BW)
 class CALL-SETUP
bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 256
 class class-default
  fair-queue
  random-detect
policy-map Shaper-768K
  description 768Kbps * .85 = 652
```

```
 class class-default
  shape average 652000 6520
  service-policy V3PN
```

Note Note that in the configuration above, the traffic profile includes packets marked AF21; these fall into class-default and can be seen being counted under the WRED configuration as IP Precedence 2.

Branch

The following branch configuration is used in all testing:

```
interface Tunnel1
 description VTI to wpoc1-r1
 bandwidth 768
 ip unnumbered Ethernet1/0
 tunnel source FastEthernet0/1
 tunnel destination 192.168.136.17
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
 service-policy output Shaper-768K
```

Headend Using Virtual Template Interface

The following headend configuration is used when testing hierarchical CBWFQ on the virtual template interface:

```
interface Virtual-Template1 type tunnel
 bandwidth 768
 ip unnumbered Loopback901
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0 5
 ip summary-address eigrp 100 10.0.0.0 255.0.0.0 5
 tunnel source Loopback117
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
 service-policy output Shaper-768K
```

Headend Using ATM Shaping Pre-Crypto

The following configuration is used when shaping on the ATM interface before the crypto headend router. It is an example of a sub-interface for one branch. Each branch has a similarly configured sub-interface on the ATM PA-A3 OC3 interface.

The following configuration is from the ATM shaping router:

```
interface ATM2/0.133 point-to-point
 bandwidth 845
 ip address 10.2.122.33 255.255.255.252
 pvc peer133 1/33
  vbr-nrt 845 845
  tx-ring-limit 3
  no ilmi manage
  oam-pvc manage
  oam retry 2 5 5
  encapsulation aal5snap
  max-reserved-bandwidth 100
  service-policy output V3PN-768
 ip route 10.0.76.0 255.255.255.0 10.2.122.34
```

The following configuration is from the headend crypto router, the other side of the ATM PA-A3 OC3 interface. In this test, the crypto router does not have a QoS service policy configured on the virtual template interface.

```
interface ATM2/0.133 point-to-point
 bandwidth 845
 ip address 10.2.122.34 255.255.255.252
 pvc peer133 1/33
  tx-ring-limit 3
  no ilmi manage
  oam-pvc manage
  oam retry 2 5 5
  encapsulation aal5snap
  max-reserved-bandwidth 100
```

Traffic from branch to headend does not traverse the above VC. There is no static route or EIGRP neighbor across the VC.

ATM Shaping Pre-Crypto

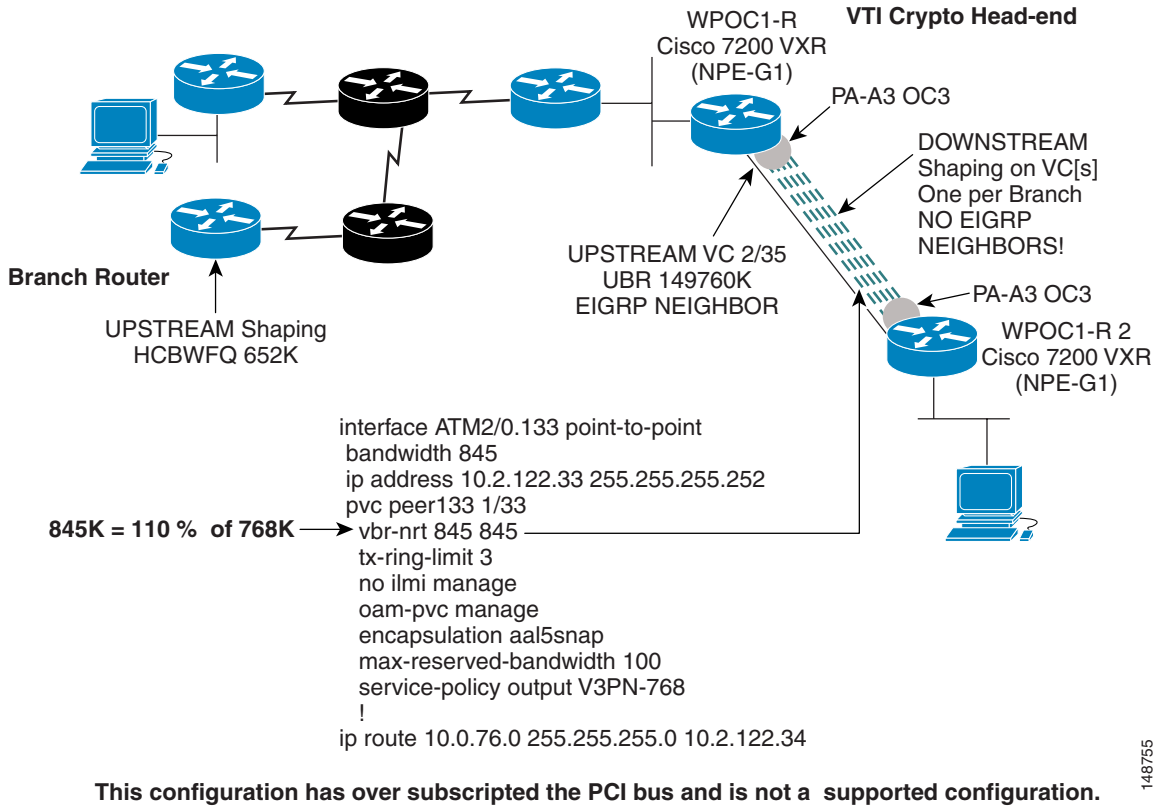
One means of reducing the CPU consumption associated with shaping on the headend crypto router is to pre-shape on a per-branch basis before reaching the crypto router. The goal is to offload shaping from the CPU on the crypto headend to hardware on a PA-A3

Note For more information about PA-A3, see *Understanding Per-VC Transmit Queuing on the PA-A3* and *NM-1A ATM Interfaces [IP to ATM Class of Service]* (Document ID: 6187), at the following URL: http://www.cisco.com/en/US/partner/tech/tk39/tk824/technologies_tech_note09186a0080094b48.shtml

Testbed Network Topology

For this test phase, the topology now includes a Cisco 7200VXR NPE-G1 with a PA-A3-OC3 interface adapter. The crypto headend is also upgraded to include a PA-A3-OC3 adapter. For each branch router, a single ATM VC is configured as sub-interfaces on the back-to-back PA-A3-OC3 network (see Figure 19.

Figure 19 Pre-shaping using the ATM PA-A3 OC3



This configuration has over subscripted the PCI bus and is not a supported configuration.

One VC is configured for all upstream traffic. This is shown as VC 2/35. An EIGRP neighbor relationship is formed on this VC. The downstream VCs (1/33 is shown in Figure 19) by the configuration do not form EIGRP neighbors. Rather, OAM is configured to validate VC availability. One static route per VC is configured using the remote branch LAN network. This eliminates the need to policy route. In the event a VC is administratively shutdown or improperly configured, connectivity to all branch subnets is maintained by way of the VC 2/35. Each VC is configured with ATM traffic-shaping using the VBR-nrt construct, a TX-ring-limit value of 3, and an output QoS service policy.

To facilitate configuration, a script language is used to generate the configuration, which is then cut-and-pasted into both ATM PA-A3 interface configurations.

Test Results

Performance test results using this configuration for 22 and 30 branches are shown in Table 5.

Table 5 ATM PA-A3 Test Results

Number of Branches	Crypto Headend CPU %	ATM Shaper CPU %	Shaper Target Rate (in Kbps)	Approx. pps per Branch	Approx. Mbps Bi-directional
22	38%	18% (all interrupt)	768	600	34.8
30	49%	25% (all interrupt)	768	600	47.0

When using ATM to pre-shape the ATM cells for the traffic before reaching the encrypting headend router, a VBR-nrt configured for a burst and sustained cell rate (SCR) of 845 Kbps results in 709 Kbps on the WAN router.

Note SCR is the cell rate with ATM overhead included. As a rule of thumb, shape at 85 percent of the target-shaped rate for hierarchical CBWFQ configured on a tunnel interface. The rate of 652,000 is approximately 85 percent of 768 Kbps

Comments and Observations

Comments and observations are as follows:

- The CPU busy percentage of the ATM shaping router was nearly all at the interrupt level, rather than the process switch level.
- The CPU busy percentage of the crypto router was off-loaded by this configuration. It was 95 percent busy with 30 branches when hierarchical CBWFQ was configured on the virtual template, as opposed to 49 percent when the ATM router was doing the shaping.
- The control branch voice jitter from headend-to-branch (downstream) is in the 15–16 ms range, versus approximately 3 ms for hierarchical CBWFQ configured on the virtual template.
- With the crypto headend shaping 30 branches, CPU is 95 percent. With pre-shaping, the combined CPU is 49 percent + 25 percent, or a total of 74 percent for both routers. Pre-shaping saved a net of 21 percent CPU.

The net savings of 21 percent CPU comes at a cost of an additional Cisco 7200VXR NPE-G1 plus two PA-A3 OC3 interfaces. It also includes a considerable amount of configuration complexity.

Scalability Test Bed Configuration Files

All configurations in this section use PSKs for ISAKMP authentication in a lab environment for simplicity.

Crypto Cisco 7200VXR Headend Configuration

The VTI headend router in the test bed has VTI with an IP address that is the target of the branch that belongs to that group. In these topologies, the VTI headend is connected via an ATM connection to the ATM headend on the private side and each branch as a sub-interface (VC) from the VTI headend to the ATM headend. These VCs are administratively configured. The following abbreviated sample configuration is for crypto headend #1:

```
hostname wpoc1-r1
no aaa new-model
ip cef
controller ISA 5/1
controller ISA 6/1
crypto keyring PRESHARE
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
crypto isakmp policy 8
 encr 3des
 authentication pre-share
 group 2
crypto isakmp profile PRESHARE
   description TEST for 30 branch routers VTI Templates 768 Kbps
```

```
   keyring PRESHARE
   match identity address 0.0.0.0
   keepalive 10 retry 2
   virtual-template 1
   local-address Loopback117
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec profile VTI
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
 set isakmp-profile PRESHARE
interface Loopback117
 ip address 192.168.136.17 255.255.255.255
interface Loopback901
 ip address 10.9.100.1 255.255.255.255
interface FastEthernet0/1
 description FastEthernet0/1 - Outside
 ip address 192.168.131.20 255.255.255.224
 load-interval 30
 duplex auto
 speed auto
interface ATM2/0
 description ATM2/0 to-core
 no ip address
 load-interval 30
 no atm ilmi-keepalive
interface ATM2/0.133 point-to-point
 bandwidth 845
 ip address 10.2.122.34 255.255.255.252
 pvc peer133 1/33
  tx-ring-limit 3
  no ilmi manage
  oam-pvc manage
  oam retry 2 5 5
  encapsulation aal5snap
  max-reserved-bandwidth 100
 interface ATM2/0.134 point-to-point
 bandwidth 845
 ip address 10.2.122.38 255.255.255.252
 pvc peer134 1/34
  tx-ring-limit 3
  no ilmi manage
  oam-pvc manage
  oam retry 2 5 5
  encapsulation aal5snap
  max-reserved-bandwidth 100
 interface ATM2/0.135 point-to-point
 bandwidth 845
 ip address 10.2.122.42 255.255.255.252
 pvc peer135 1/35
  tx-ring-limit 3
  no ilmi manage
  oam-pvc manage
  oam retry 2 5 5
  encapsulation aal5snap
  max-reserved-bandwidth 100
interface ATM2/0.172 point-to-point
 bandwidth 845
 ip address 10.2.122.190 255.255.255.252
 pvc peer172 1/72
  tx-ring-limit 3
  no ilmi manage
  oam-pvc manage
  oam retry 2 5 5
  encapsulation aal5snap
  max-reserved-bandwidth 100
```

```
 interface ATM2/0.235 point-to-point
 description BIG PIPE
 ip address 10.2.122.194 255.255.255.252
 pvc peer235 2/35
  encapsulation aal5snap
 interface Virtual-Template1 type tunnel
 description *** note no ip mtu 1408
 bandwidth 768
 ip unnumbered Loopback901
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0 5
 ip summary-address eigrp 100 10.0.0.0 255.0.0.0 5
 tunnel source Loopback117
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
router eigrp 100
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 network 192.168.136.0 0.0.1.255
 no auto-summary
ip classless
ip route 10.2.120.0 255.255.255.0 10.2.122.193
```

ATM Cisco 7200VXR Headend Configuration

The ATM headend device is deployed on the protected side of the VTI crypto headend and has numerous VCs over the ATM PA-A3 to the VTI device. This is shown in the following configuration for ATM headend #1:

```
hostname wpoc1-r2
no aaa new-model
ip subnet-zero
ip cef
controller ISA 5/1
controller ISA 6/1
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
policy-map V3PN-768
  description V3PN branch (4calls-768 BW)
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 256
 class class-default
  fair-queue
  random-detect
  random-detect precedence 0   4     8
policy-map Shaper-768K
  description 768Kbps * .85 = 652
 class class-default
  shape average 652000 6520
  service-policy V3PN-768
interface FastEthernet1/0
 description FastEthernet1/0
 ip address 10.2.128.20 255.255.255.0
```

```
 load-interval 30
 duplex auto
 speed auto
interface FastEthernet1/1
 description FastEthernet1/1
 ip address 10.2.120.20 255.255.255.0
 ip route-cache flow
 duplex auto
 speed auto
interface ATM2/0
 description ATM2/0 to-cryHE
 no ip address
 no atm ilmi-keepalive
interface ATM2/0.133 point-to-point
 bandwidth 845
 ip address 10.2.122.33 255.255.255.252
 pvc peer133 1/33
  vbr-nrt 845 845
  tx-ring-limit 3
  no ilmi manage
  oam-pvc manage
  oam retry 2 5 5
  encapsulation aal5snap
  max-reserved-bandwidth 100
  service-policy output V3PN-768
 interface ATM2/0.134 point-to-point
 bandwidth 845
 ip address 10.2.122.37 255.255.255.252
 pvc peer134 1/34
  vbr-nrt 845 845
  tx-ring-limit 3
  no ilmi manage
  oam-pvc manage
  oam retry 2 5 5
  encapsulation aal5snap
  max-reserved-bandwidth 100
  service-policy output V3PN-768
 interface ATM2/0.135 point-to-point
 bandwidth 845
 ip address 10.2.122.41 255.255.255.252
 pvc peer135 1/35
  vbr-nrt 845 845
  tx-ring-limit 3
  no ilmi manage
  oam-pvc manage
  oam retry 2 5 5
  encapsulation aal5snap
  max-reserved-bandwidth 100
  service-policy output V3PN-768
interface ATM2/0.172 point-to-point
 bandwidth 845
 ip address 10.2.122.189 255.255.255.252
 pvc peer172 1/72
  vbr-nrt 845 845
  tx-ring-limit 3
  no ilmi manage
  oam-pvc manage
  oam retry 2 5 5
  encapsulation aal5snap
  max-reserved-bandwidth 100
  service-policy output V3PN-768
 interface ATM2/0.235 point-to-point
 description BIG PIPE
 ip address 10.2.122.193 255.255.255.252
```

```
 pvc peer235 2/35
  encapsulation aal5snap
 ip classless
ip route 10.0.76.0 255.255.255.0 10.2.122.34
ip route 10.0.80.0 255.255.255.0 10.2.122.38
ip route 10.0.84.0 255.255.255.0 10.2.122.42
!...repeat appropriate static route into each VC...static routes removed for brevity
ip route 10.0.132.0 255.255.255.0 10.2.122.190
ip route 192.168.128.192 255.255.255.255 10.2.122.34
ip route 192.168.128.193 255.255.255.255 10.2.122.38
ip route 192.168.128.194 255.255.255.255 10.2.122.42
!... repeat route to each branch as appropriate... One router per branch...
```

Branch Office Configuration

Branch configuration is the same as in Branch Office Configuration, page 60.

Alternate Scaling Using PA ATM-PA3 Conclusion

It is unlikely any customer would implement this option based on the increased cost, increased voice jitter, configuration complexity, and limited amount of net CPU savings.

Headend Scale Testing—No QoS on the Logical Interface

This section describes a series of performance tests without QoS enabled on the headend crypto router as a benchmark to compare against IPsec direct encapsulation tunnels or IPsec-encrypted GRE tunnels.

Test Overview

In these tests, QoS is enabled on the enterprise WAN router Frame Relay PVC to each branch. On the branch, QoS is enabled on the physical interface but not the logical interface. This Frame Relay traffic shaping rate is 95 percent of the target rate, which is 192 Kbps. This is the same configuration as is used in the *Voice and Video Enabled IPSec VPN (V3PN) Design Guide.*

The headend VPN aggregation router is a Cisco 7200VXR NPE-G1 with dual VAM2 hardware encryption accelerators running Cisco IOS release 12.3(14)T5. In each test, there are 500 EIGRP neighbors. The headend advertises a summary 10.0.0.0/8 route to each branch. All branches are configured as EIGRP stubs advertising a summary of the connected interfaces. The EIGRP hello interval is the default of 5 seconds with a dead interval configured at 35 seconds.

The traffic profile is a converged voice and data profile. Each branch with active data has one G.729 call active plus data traffic. For example, the test instance with 148 branches with active voice and data has 148 G.729 calls being switched at the headend plus data from each of the 148 branches. Each call represents 100 packets per second; 50 packets per second in each direction.

Test Results

Figure 20 shows the test results in graphical format. The CPU busy reported are approximate values, plus or minus 5 percent. Both pps and Mbps are reported for each test.

Figure 20 Headend Scale Testing—No QoS on Logical Interface

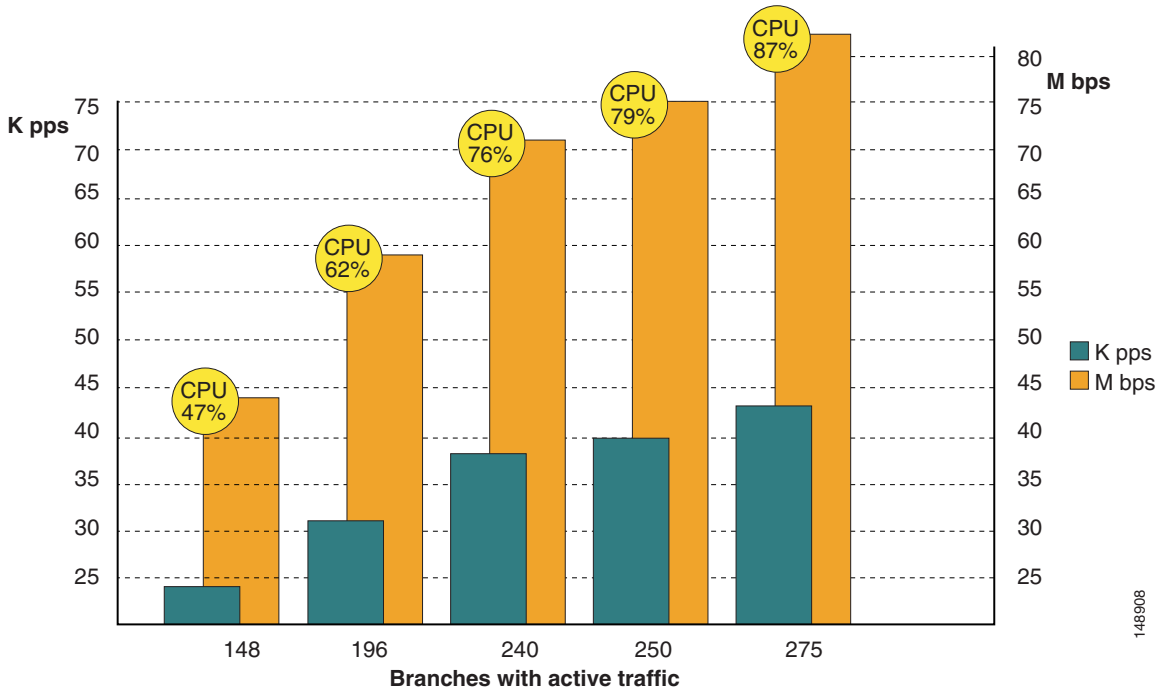


Table 6 shows the test results in table format.

Table 6 Headend Scale Testing—No QoS on Logical Interface

Test	1	2	3	4	5
CPU busy	47%	62%	76%	79%	87%
Mbps voice and data	44	59	72	75	83
Packets per second	23,236	30,716	37,560	39,077	42,977
Number of branches with active voice/data	148	196	240	250	275

Analysis of Performance Data

In the same test bed environment, with a Cisco 7200VXR NPE-G1 with dual VAM2 hardware encryption accelerators running, a Cisco IOS 12.3 experimental (pre-release) image was tested with 500 IPsec direct encapsulation with DPD/RRI. With 275 branches with active traffic, using the same traffic profile, the CPU busy was reported at 86 percent, with 43 Kpps and 86 Mbps.

The performance results in test 5 from Table 6 align very closely to the IPsec direct encapsulation and DPD/RRI results. The notable difference between the two topologies is that IPsec direct encapsulation with DPD/RRI does not have a routing protocol neighbor with each of the 500 branches in the test bed.

This testing shows that an IPsec VTI configuration using an optimally configured EIGRP topology can scale as well as IPsec direct encapsulation with DPD/RRI.

Appendix A—Detailed Test Results

This section provides detailed test results.

Netflow Summary Table

This section is for the hierarchical CBWFQ-virtual template interface test using a target-shaped rate of 768 Kbps and no more than 80 percent headend CPU utilization. There are twenty-two branch routers active; the control branch and 21 filler branches.

Control Branch

The branch IP address is 192.168.192.22 and the headend IP address is 192.168.136.17 for the results shown in Table 7.

Table 7 Control Branch Results

srcaddr	dstaddr	PPS	BYTES_PAK	Kbps
192.168.136.17	192.168.192.22	296	315	729
192.168.192.22	192.168.136.17	299	323	758

Branch to Headend Upstream

The headend IP address is 192.168.136.17, with 21 branches with pps greater than 0 pps for the results shown in Table 8.

Table 8 Branch to Headend Downstream Test Results

srcaddr	dstaddr	PPS	BYTES_PAK	Kbps
192.168.128.197	192.168.136.17	0	120	0
192.168.128.198	192.168.136.17	299	324	759
192.168.128.199	192.168.136.17	302	322	760
192.168.128.200	192.168.136.17	304	319	761
192.168.128.201	192.168.136.17	0	120	0
192.168.128.202	192.168.136.17	299	324	759
192.168.128.203	192.168.136.17	297	326	758
192.168.128.204	192.168.136.17	301	322	759
192.168.128.206	192.168.136.17	0	120	0
192.168.128.229	192.168.136.17	298	324	758
192.168.128.230	192.168.136.17	301	322	759
192.168.128.232	192.168.136.17	301	322	760
192.168.128.233	192.168.136.17	302	321	759
192.168.128.234	192.168.136.17	302	322	760
192.168.128.235	192.168.136.17	298	324	757

Table 8 Branch to Headend Downstream Test Results (continued)

srcaddr	dstaddr	PPS	BYTES_PAK	Kbps
192.168.128.236	192.168.136.17	302	321	760
192.168.128.238	192.168.136.17	301	322	760
192.168.128.239	192.168.136.17	0	120	0
192.168.128.240	192.168.136.17	0	120	0
192.168.128.241	192.168.136.17	0	120	0
192.168.128.243	192.168.136.17	0	120	0
192.168.128.244	192.168.136.17	0	120	0
192.168.128.245	192.168.136.17	297	325	758
192.168.128.246	192.168.136.17	0	120	0
192.168.128.247	192.168.136.17	301	322	759
192.168.128.248	192.168.136.17	302	322	760
192.168.128.249	192.168.136.17	300	323	759
192.168.128.250	192.168.136.17	301	321	756
192.168.128.251	192.168.136.17	300	322	758
192.168.128.252	192.168.136.17	0	120	0
192.168.128.253	192.168.136.17	301	322	759
192.168.128.254	192.168.136.17	0	120	0

Headend-to-Branch Downstream

The headend IP address is 192.168.136.17, with 21 branches with pps greater than 0 pps for the test results shown in Table 9.

Table 9 Headend to Branch Test Results

srcaddr	dstaddr	PPS	BYTES_PAK	Kbps
192.168.136.17	192.168.128.197	0	113	0
192.168.136.17	192.168.128.198	296	327	757
192.168.136.17	192.168.128.199	301	316	745
192.168.136.17	192.168.128.200	295	319	738
192.168.136.17	192.168.128.201	0	113	0
192.168.136.17	192.168.128.202	298	324	758
192.168.136.17	192.168.128.203	293	304	696
192.168.136.17	192.168.128.204	297	324	755
192.168.136.17	192.168.128.206	0	113	0
192.168.136.17	192.168.128.229	295	320	739
192.168.136.17	192.168.128.230	298	318	743
192.168.136.17	192.168.128.232	297	321	747

Table 9 Headend to Branch Test Results (continued)

srcaddr	dstaddr	PPS	BYTES_PAK	Kbps
192.168.136.17	192.168.128.233	298	321	749
192.168.136.17	192.168.128.234	298	324	758
192.168.136.17	192.168.128.235	294	307	706
192.168.136.17	192.168.128.236	301	316	746
192.168.136.17	192.168.128.238	299	320	751
192.168.136.17	192.168.128.239	0	113	0
192.168.136.17	192.168.128.240	0	113	0
192.168.136.17	192.168.128.241	0	113	0
192.168.136.17	192.168.128.243	0	113	0
192.168.136.17	192.168.128.244	0	113	0
192.168.136.17	192.168.128.245	304	302	719
192.168.136.17	192.168.128.246	0	113	0
192.168.136.17	192.168.128.247	298	323	755
192.168.136.17	192.168.128.248	299	322	756
192.168.136.17	192.168.128.249	299	323	755
192.168.136.17	192.168.128.250	297	320	744
192.168.136.17	192.168.128.251	298	324	756
192.168.136.17	192.168.128.252	0	113	0
192.168.136.17	192.168.128.253	301	318	751
192.168.136.17	192.168.128.254	0	113	0

Cisco IOS Software Versions Tested

The VTI feature is introduced in Cisco IOS 12.3(14)T. The hardware platforms and Cisco IOS images shown in Table 10 are used in the basic configuration in live testing.

Table 10 Software Releases Evaluated for Alternate Scale Test

Cisco Product Family	SW Release
Cisco headend routers Cisco 7206VXR-NPE-G1 and dual VAM-II	Cisco IOS 12.3(14)T2
Cisco 2651XM (AIM-II EP)	Cisco IOS 12.3(14)T2
Cisco 1700	Cisco IOS 12.3(14)T2
Cisco 1840	Cisco IOS 12.3(14)T2
Cisco 831	Cisco IOS 12.3(14)T2

As part of the performance testing, the platforms upgraded to Cisco IOS version 12(3)14.T3 on 1 August 05 before initial performance testing. Then on 5 August 2005, the platforms are upgraded to Cisco IOS 12.4(3.6) INTERIM to circumvent DDTS CSCei41674.

For EZVPN with Dynamic Virtual Tunnel Interface support, the release tested is 12.4(4)T. The platforms tested were Cisco 2651XM (AIM-II EP) and 7206VXR-NPE-G1 and dual VAM-II.

Caveats and DDTS Filed

VTI with virtual templates is currently not supported on the Cisco Catalyst 6500 or Cisco 7600 Series.

- CSCei41674—Traceback in IPsec tunnel: SYS-2-LINKED: Bad enqueue of 663CC3A8
- CSCsb68839—3825 onboard crypto engine HW - is not marking TTL on IPsec IP hdr 255
- CSCsb72292—**show policy-map int** output is incomplete when apply to a tunnel interface
- CSCsc63242—Cannot remove EZVPN configuration from inside interface
- CSCsc72005—EZVPN transient configuration not removed when tunnel down
- CSCsc77978—EZVPN configuration URL not applied

Line Protocol

The VTI interfaces do not support a keepalive such as a GRE tunnel keepalive. The **keepalive** command was modified to make it available for use on tunnel interfaces in Cisco IOS 12.2(8)T. However, the line protocol of the tunnel interface is changed by ISAKMP DPD/keepalives, as well as the existence the corresponding IPsec SAs.

Normal status of a **show ip int brief** is the interface is up/up:

```
Interface              IP-Address      OK? Method Status                Protocol
Tunnel1                10.0.84.1       YES TFTP   up                    up
```

With ISAKMP DPD/keepalives configured, following a WAN failure, the line protocol is shown as down:

```
Interface              IP-Address      OK? Method Status                Protocol
Tunnel1                10.0.84.1       YES TFTP   up                    down
```

On the crypto headend side, the corresponding virtual access interface for this branch shows down/down when connectivity is lost:

```
Interface              IP-Address      OK? Method Status                Protocol
Virtual-Access2        unassigned      NO  TFTP   down                  down
```

However, the virtual access interface is reused or reclaimed when the WAN failure clears, and the branch again connects to Virtual-Access2. This minimizes the number of virtual interfaces being “orphaned” on the headend crypto router.

Look at the Syslog for this series of events using an Internet connected (DSL router is a Cisco 877 with NAT/PAT) with the Cisco 871 connecting to the crypto headend by means of NAT-T. The EIGRP hold time and dead interval are default values, 5 and 15. IKE keepalive is configured at 10 seconds with a 2 second retry of five attempts:

```
cisco-vpn-871#show clock          DSL line unplugged at this time [approximately]
17:27:22.036 edt Tue Sep 6 2005
cisco-vpn-871#
Sep  6 17:27:34.739 edt: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 64: Neighbor 10.81.7.216 (Tunnel0)
is down: holding time expired
Sep  6 17:27:44.029 edt: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to down
```

```
Sep  6 17:27:44.033 edt: %PIM-5-NBRCHG: neighbor 10.81.7.216 DOWN on interface Tunnel0
(vrf default) non DR
cisco-vpn-871#
cisco-vpn-871#show clock        DSL line inserted at this time [approximately]
17:28:49.623 edt Tue Sep 6 2005
cisco-vpn-871#
Sep  6 17:29:32.000 edt: %PIM-5-NBRCHG: neighbor 10.81.7.216 UP on interface Tunnel0 (vrf
default)
Sep  6 17:29:32.008 edt: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
Sep  6 17:29:33.771 edt: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 64: Neighbor 10.81.7.216 (Tunnel0)
is up: new adjacency
```

In the above example, EIGRP detected the failure approximately 12 seconds after the cable was unplugged, and the tunnel interface line protocol went down approximately 22 seconds following the line failure.

It took approximately 43 seconds to recover after the DSL/POTS line was re-inserted into the Cisco 877 router. Recovering from the failure is longer than detecting the failure, because the Cisco 877 router must re-train the DSL interface and negotiate PPPoE with the ISP before the Cisco 871 router can build the ISAKMP and IPsec SAs and begin passing traffic to build the EIGRP neighbor.

Appendix B—Peer has IPsec Interface Support

A configuration error that may be difficult to identify is not including the **virtual-interface** command on the remote router when there is a virtual interface configured on the headend router, as follows:

```
crypto ipsec client ezvpn VTI
 connect auto
 group RTP_ezvpn_group key MrExcitement
 mode network-plus
 peer 192.168.136.17
 virtual-interface 51
 username EZVPN_Test_user password JimmyS
 xauth userid mode local
!
```

If **virtual-interface 51** is missing, the remote router displays repeatedly (assuming **connect auto**):

```
debug cry ipsec client ezvpn

Dec  1 11:26:27 est:         Peer has  IPsec Interface support
Dec  1 11:26:27 est: EZVPN(VTI): ezvpn_mode_config
Dec  1 11:26:27 est: EZVPN(VTI): New State: SS_OPEN
Dec  1 11:26:27 est: EZVPN(VTI): Current State: SS_OPEN
Dec  1 11:26:27 est: EZVPN(VTI): Event: SOCKET_READY
Dec  1 11:26:27 est: EZVPN(VTI): No state change
Dec  1 11:26:27 est: EZVPN(VTI): Current State: SS_OPEN
Dec  1 11:26:27 est: EZVPN(VTI): Event: SOCKET_READY
Dec  1 11:26:27 est: EZVPN(VTI): No state change
Dec  1 11:26:27 est: EZVPN(VTI): Current State: SS_OPEN
Dec  1 11:26:27 est: EZVPN(VTI): Event: MTU_CHANGED
Dec  1 11:26:27 est: EZVPN(VTI): No state change
Dec  1 11:26:27 est: EZVPN(VTI): Current State: SS_OPEN
Dec  1 11:26:27 est: EZVPN(VTI): Event: SOCKET_UP
Dec  1 11:26:27 est: ezvpn_socket_up
Dec  1 11:26:27 est: %CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=EZVPN_Test_u
Dec  1 11:26:27 est: EZVPN(VTI): Tunnel UP! Letting user know about it
Dec  1 11:26:27 est: EZVPN(VTI): New State: IPSEC_ACTIVE
Dec  1 11:26:27 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  . Peer
```

The display continues to repeat itself. No EIGRP neighbor forms because there is no virtual interface on the branch router. If you encounter this, verify that the branch router is referencing a “virtual-interface” in the configuration. While the tunnel is “up”, you do not pass any traffic without the virtual interface configured.

Appendix C—Output for debug crypto ipsec client ezvpn Command

The following is an example of a successful tunnel establishment showing the output of the **debug crypto ipsec client ezvpn** command on the branch router:

```
Dec 12 13:12:03 est: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
.Dec 12 13:12:04 est: %SYS-5-CONFIG_I: Configured from console by console
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): Current State: READY
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): Event: RESET
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): ezvpn_close
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): VPN Route Deleted 0.0.0.0 0.0.0.0 via
Virtual-Access2 in IP DEFAULT TABLE
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): Deleted PSK for address 192.168.136.19

Dec 12 13:12:26 est: EzVPN(VTI_SECOND): rollback skipped!
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): No Connect ACL checking status change
Dec 12 13:12:26 est: %CRYPTO-6-EZVPN_CONNECTION_DOWN: (Client)  User=
Group=RTP_ezvpn_group  Server_public_addr=192.168.136.19
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): New active peer is 192.168.136.19
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): Ready to connect to peer 192.168.136.19
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): ezvpn_reset
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): New State: CONNECT_REQUIRED
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): Current State: CONNECT_REQUIRED
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): Event: CONNECT
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): ezvpn_connect_request
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): Found valid peer 192.168.136.19
Dec 12 13:12:26 est: EZVPN(VTI_SECOND): Added PSK for address 192.168.136.19

Dec 12 13:12:26 est: EzVPN(VTI_SECOND): sleep jitter delay 1277
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): VPN Route Deleted 192.168.136.19 255.255.255.255
via 192.168.136.19, in IP DEFAULT TABLE
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): Route exists for 192.168.136.19 via
192.168.128.1,FastEthernet0/1 in IP DEFAULT TABLE
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): New State: READY
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): Current State: READY
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): Event: IKE_PFS
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): No state change
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): Current State: READY
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): Event: CONN_UP
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): ezvpn_conn_up 0A9AFFD0 BBB72A00 4F5661B8 9F23BE18
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): No state change
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): Current State: READY
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): Event: XAUTH_REQUEST
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): ezvpn_xauth_request
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): ezvpn_parse_xauth_msg
Dec 12 13:12:27 est: EZVPN: Attributes sent in xauth request message:
Dec 12 13:12:27 est:          XAUTH_USER_NAME_V2(VTI_SECOND):
Dec 12 13:12:27 est:          XAUTH_USER_PASSWORD_V2(VTI_SECOND):
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): send saved username EZVPN_Test_user and password
<omitted>
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): New State: XAUTH_REQ
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): Current State: XAUTH_REQ
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): Event: XAUTH_REQ_INFO_READY
```

```
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): ezvpn_xauth_reply
Dec 12 13:12:27 est:         XAUTH_USER_NAME_V2(VTI_SECOND): EZVPN_Test_user
Dec 12 13:12:27 est:         XAUTH_USER_PASSWORD_V2(VTI_SECOND): <omitted>
Dec 12 13:12:27 est: EZVPN(VTI_SECOND): New State: XAUTH_REPLIED
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Current State: XAUTH_REPLIED
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Event: XAUTH_STATUS
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): xauth status received: Success
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): New State: READY
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Current State: READY
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Event: MODE_CONFIG_REPLY
Dec 12 13:12:28 est: EzVPN(VTI_SECOND): rollback skipped!
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): VPN Route Deleted 0.0.0.0 0.0.0.0 via
Virtual-Access2 in IP DEFAULT TABLE 0A9AFFD0 BBB72A008
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): ezvpn_parse_mode_config_msg
Dec 12 13:12:28 est: EZVPN: Attributes sent in message:
Dec 12 13:12:28 est:         Address: 10.8.100.31
Dec 12 13:12:28 est:         configuration URL:
ftp://root:cisco@172.26.157.11//usr/tmp/CFG-version26.txt
Dec 12 13:12:28 est:         configuration version: 26
Dec 12 13:12:28 est:         Split Tunnel List: 1
Dec 12 13:12:28 est:               Address    : 192.0.2.0
Dec 12 13:12:28 est:               Mask       : 255.255.255.0
Dec 12 13:12:28 est:               Protocol   : 0x0
Dec 12 13:12:28 est:               Source Port: 0
Dec 12 13:12:28 est:               Dest Port  : 0
Dec 12 13:12:28 est: EZVPN: Unknown/Unsupported Attr: SPLIT_DNS (0x7003)
Dec 12 13:12:28 est:         Default Domain: cisco.com
Dec 12 13:12:28 est:         Savepwd on
Dec 12 13:12:28 est: EZVPN: Unknown/Unsupported Attr: APPLICATION_VERSION (0x7)
Dec 12 13:12:28 est:         Banner:
==
====
====== Hello from vpn-jk3-2651xm-9
====
==

Dec 12 13:12:28 est:         Peer has  IPsec Interface support
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): New State: SS_OPEN
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Current State: SS_OPEN
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Event: MODE_CONFIG_REPLY
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): ezvpn_mode_config
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): ezvpn_nat_config
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): No state change
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Current State: SS_OPEN
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Event: SOCKET_READY
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): No state change
Dec 12 13:12:28 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
192.168.136.19:500       Id: 192.168.136.19
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Current State: SS_OPEN
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Event: MTU_CHANGED
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): No state change
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Current State: SS_OPEN
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Event: SOCKET_UP
Dec 12 13:12:28 est: ezvpn_socket_up
Dec 12 13:12:28 est: %CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=EZVPN_Test_user
Group=RTP_ezvpn_group  Server_public_addr=192.1
Dec 12 13:12:28 est: EZVPN: Static route change notify tableid 0, event UP, destination
192.0.2.0, gateway 0.0.0.0, interface Virtu2
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): VPN Route Added 192.0.2.0 255.255.255.0 via
Virtual-Access2 in IP DEFAULT TABLE
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): Tunnel UP! Letting user know about it
Dec 12 13:12:28 est: EZVPN(VTI_SECOND): New State: IPSEC_ACTIVE
Dec 12 13:12:28 est: EzVPN(VTI_SECOND): Faking the checkpointing of the base config, we'll
be back here
```

```
Dec 12 13:12:29 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed
state to up
Dec 12 13:12:29 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state
to up
Dec 12 13:12:29 est: %PIM-5-NBRCHG: neighbor 10.8.100.1 UP on interface Virtual-Access2
(vrf default)
Dec 12 13:12:29 est: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 10.8.100.1
(Virtual-Access2) is up: new adjacency
Dec 12 13:12:33 est: EzVPN(VTI_SECOND): Received 66 bytes of config from
ftp://root:cisco@172.26.157.11//usr/tmp/CFG-version26.txt
Dec 12 13:12:33 est: EzVPN(VTI_SECOND): Applying persistent_config
Dec 12 13:12:33 est: EzVPN(VTI_SECOND): Updating the version number: 26
```

Appendix D—Output for show crypto session detail Command

The following Cisco IOS CLI command is useful for showing the relationship between the virtual access interface, the hostname of the remote router, the outside IP address of the remote peer, and the session status:

```
alias exec crysum show cry session detail | inc Peer|Phase|status|Interf
```

If the port number is anything other than 500, the remote router is behind a NAT/PAT device, and NAT-T is in effect.

```
rtp5-esevpn-gw3#crysum
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection

Interface: Virtual-Access3
Session status: UP-ACTIVE
Peer: 172.26.177.250 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: vpn4-2651xm-1.cisco.com

Interface: Virtual-Access7
Session status: UP-ACTIVE
Peer: 24.199.214.75 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: sochmans-1811-vpn.cisco.com

Interface: Virtual-Access10
Session status: UP-ACTIVE
Peer: 172.26.134.106 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: brtpen-video-831.cisco.com
```

Appendix D—References

This section includes the following references for further information:

- Documents:
  - *VPN IPsec/GRE Tunnel Throughput and Scalability Test Results 2.0*
  - *SAFE VPN: Virtual Private Networks in Depth*
  - *AVVID QoS Quick Reference Guide*

- Request For Comment (RFC):
  - The TCP Maximum Segment Size and Related Topics—RFC 897
  - Path MTU Discovery—RFC 1191
  - RTP: A Transport Protocol for Real-Time Applications—RFC 1889
  - Transmitting PPP Over Ethernet—RFC 2516
  - Security Architecture for the Internet Protocol—RFC 2401
  - IP Authentication Header—RFC 2402
  - The Use of HMAC-MD5-96 within ESP and AH—RFC 2403
  - The Use of HMAC-SHA-1-96 within ESP and AH—RFC 2404
  - The ESP DES-CBC Cipher Algorithm With Explicit IV—RFC 2405
  - IP Encapsulating Security Payload (ESP)—RFC 2406
  - The Internet IP Security Domain of Interpretation for ISAKMP—RFC 2407
  - Internet and Key Management Protocol (ISAKMP)—RFC 2408
  - The Internet Key Exchange (IKE)—RFC 2409
  - The NULL Encryption Algorithm and Its Use With IPsec—RFC 2410
  - IP Security Document Roadmap—RFC 2411
  - The OAKLEY Key Determination Protocol—RFC 2412
- Other links
  - 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 Cisco 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/cpress/cc/td/cpress/ccie/ndcs798/nd2016.htm
  - Cisco TAC Security Technical Tips—http://www.cisco.com/warp/public/707/
  - IPsec Support Page—http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Internetworking:IPsec
  - Networking Professionals Connection—http://forums.cisco.com
  - Netflow—http://www.cisco.com/go/netflow

Appendix E—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
DVTI	Dynamic Virtual Tunnel Interface (virtual template)
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
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

Term	Definition
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
p2p GRE	Point-to-Point GRE
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
ToS	Type of Service
UDP	User Datagram Protocol
VAD	Voice Activity Detection
VoIP	Voice over IP
V^3PN	Voice and Video Enabled IPsec VPN
VAM	VPN Acceleration Module

Term	Definition
VPN	Virtual Private Network
VTI	Virtual Tunnel Interface
WAN	Wide Area Network
WRED	Weighted Random Early Detection