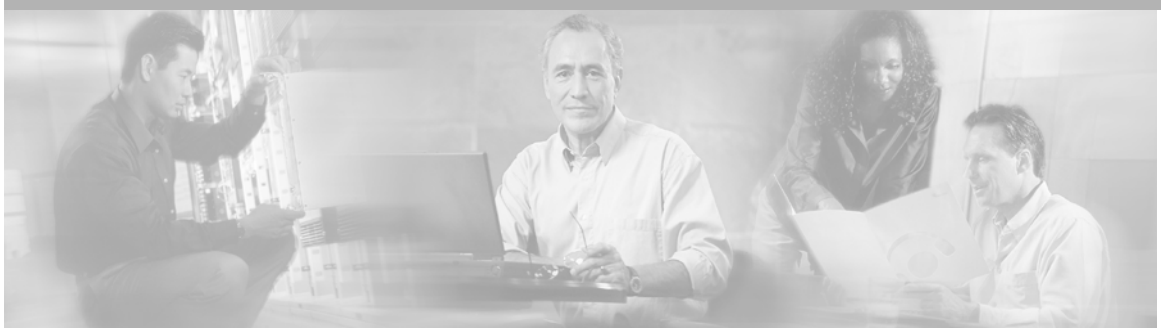
Cisco Systems



Multicast over IPsec VPN Design Guide

OL-9028-01

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Multicast over IPsec VPN Design Guide

CONTENTS

Multicast over IPsec VPN Design Guide

This design guide provides detailed configuration examples for implementing IP multicast (IPmc) in a QoS-enabled IP Security (IPsec) virtual private network (VPN).

Introduction

This design guide addresses implementing IPmc in a QoS-enabled IPsec VPN WAN for both site-to-site and small office/home office (SOHO).

This design guide is the fourth in a series of Voice and Video Enabled IPsec VPN (V3PN) design guides that are available under the general link http://ww.cisco.com/go/srnd, which also contains many useful design guides on QoS, IPmc, and WAN architectures:

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

IPmc Requirement in Enterprise Networks

IPmc is a means to conserve bandwidth and deliver packets to multiple receivers without adding any additional burden on the source or receivers of the packets. Applications that deliver their data content using IPmc include videoconferencing, Cisco IP/TV broadcasts, distribution of files or software packages, real-time price quotes of securities trading, news, and even video feeds from IP video surveillance cameras.

The distribution of large data files to all branches by means of a mass update is an efficient way to distribute parts lists, price sheets, or inventory data. Commercial software packages are available to optimize this file replication process by using IPmc as the transport mechanism. The corporate server sends one IPmc stream, and the networked routers replicate these packets so that all remote locations receive a copy of the file. The software can detect packet loss and at the end of the transfer, request an IP unicast stream of the missing portions to ensure the file is complete and valid.

CISCO SYSTEMS

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

IPsec Deployment with Point-to-Point GRE

Generic Routing Encapsulation (GRE) is often deployed with IPsec for several reasons, including the following:

- IPsec Direct Encapsulation supports unicast IP only. If network layer protocols other than IP are to be supported, an IP encapsulation method must be chosen so that those protocols can be transported in IP packets.
- IPmc is not supported with IPsec Direct Encapsulation. IPsec was created to be a security protocol between two and only two devices, so a service such as multicast is problematic. An IPsec peer encrypts a packet so that only one other IPsec peer can successfully perform the de-encryption. IPmc is not compatible with this mode of operation.

Until the introduction of IPsec Virtual Tunnel Interface (VTI), IPsec tunnels were not logical tunnel interfaces for routing purposes. A point-to-point (p2p) GRE tunnel, on the other hand, is a logical router interface for purposes of forwarding IP (or any other network protocol) traffic. A tunnel interface can appear as a next-hop interface in the routing table.

Virtual Tunnel Interface

VTI is introduced in Cisco IOS Release 12.3(14)T. A tunnel interface with the new Cisco IOS interface **tunnel mode ipsec ipv4** command along with the previously introduced tunnel protection interface command enables the VTI feature.

Note Tunnel protection alleviates the need to apply crypto maps to the outside interface.

VTI provides for a routable interface (*Interface Tunnel 0)* and therefore supports the encryption of IPmc.

Redundant VPN Headend Design

Because failsafe operation is a mandatory feature in many enterprise networks, redundancy should be built into headend designs. From each branch location, a minimum of two tunnels should be configured back to different headend devices. When sizing the headend installation, the failure of a single headend device should be taken into consideration. When adding an intelligent service such as IPmc, adding additional headend routers and spreading the load of the VPN terminations across more devices allows for the headend routers to “share” CPU load, thus making the solution more scalable.

Note In the interest of clarity and brevity, many of the examples shown in this design guide show only a single headend router in the topology. It is assumed in a customer deployment that redundant headend routers are configured similarly to the primary headend configuration shown.

IPmc Deployment

This chapter discusses recommended and optional configurations for IPmc deployments in an encrypted WAN topology. This section includes the following recommended guidelines:

- Use multiple rendezvous points (RPs) for high availability
- Use IP Protocol Independent Multicast (PIM) sparse mode and IP PIM Auto-RP listener.

Note Auto-RP is used in the deployment example but is not a requirement; statically configured RP address can be used instead.

- Disable fast switching of IPmc as required on IPsec routers.
- Mark the ToS byte of IPsec packets for proper classification and bandwidth allocation.

The use of GRE keepalives can be used in p2p GRE tunnels to eliminate the need for a routing protocol.

Topology

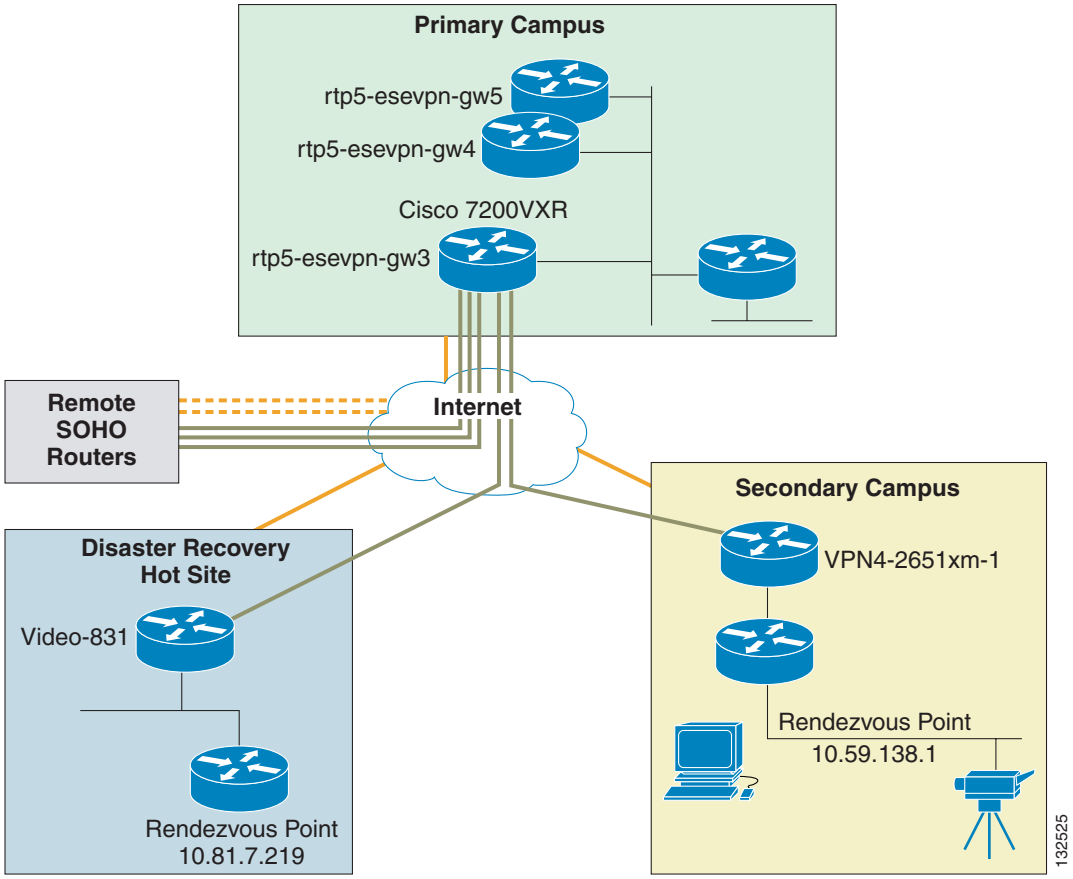
This section provides a high-level overview as well as details of the topology in use.

Topology Overview

This topology overview divides the network into the following four major components, as shown in Figure 1:

- Primary campus
- Secondary campus
- Disaster recovery hot site
- Remote SOHO routers

Figure 1 Topology Overview



Note The host names and series or model number of routers in this guide are not intended to imply performance characteristics suitable for all customer deployments. Various models of routers were used in developing this design guide to provide a variety of configuration examples. For example, a Cisco 831 router is typically deployed at a SOHO location rather than at a disaster recovery site.

The remote SOHO routers establish an IPsec-encrypted p2p GRE tunnel to one or more campus locations. For purposes of illustration, only one GRE tunnel is configured and shown, but it is assumed that in an actual customer deployment, a p2p GRE tunnel terminates at both major campus locations. Another option is for the customer to advertise a network prefix encompassing the IPsec and p2p GRE headend peer address from both the primary campus and the disaster recovery hot site. In the event of a failure of the primary campus, the IPsec and p2p GRE headend peer address, router, and configuration can be brought online at the disaster recovery site.

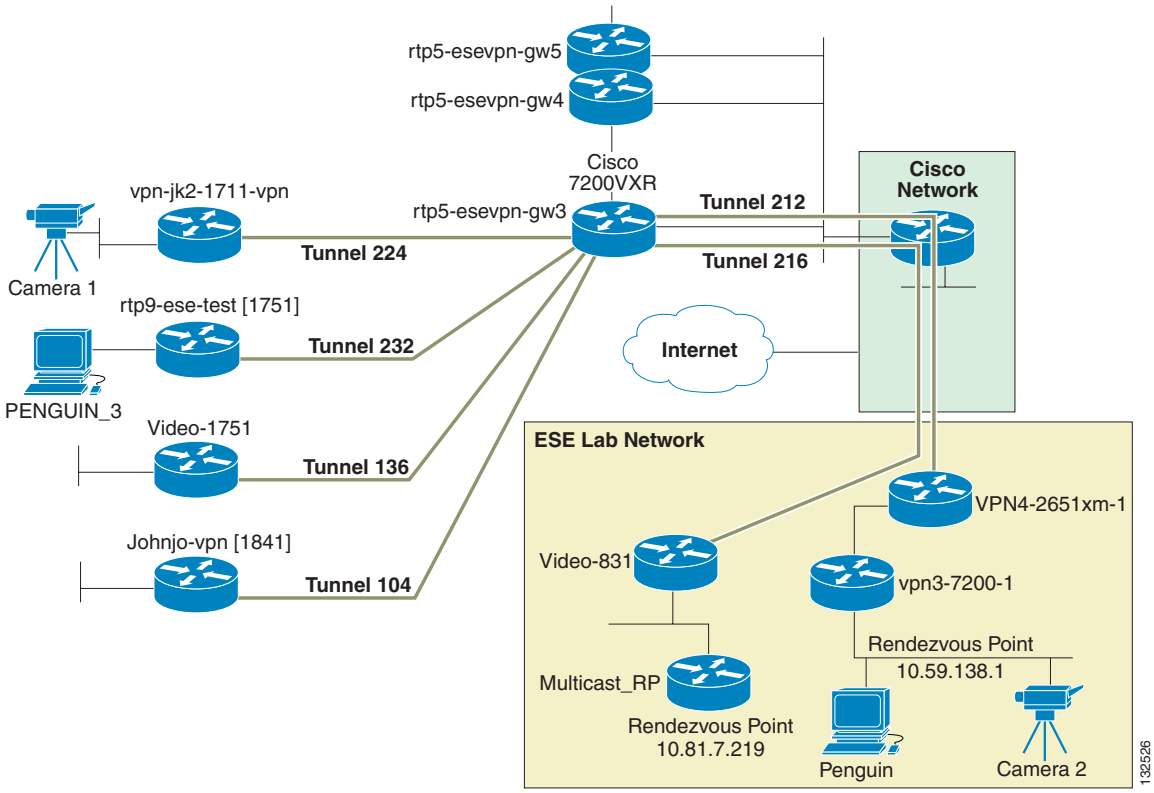
Two IPmc RPs are configured on routers dedicated for this purpose in the sample topology and are located at two separate physical locations. The RP IP addresses are not manually configured on the remote routers, but rather IP PIM Auto-RP is used. The interfaces of the routers are configured as IP PIM Sparse Mode and the **ip pim autorp listener** global configuration command is used on all remote routers. This command allows IP PIM Auto-RP to function over IP PIM Sparse Mode interfaces. The rendezvous points transmit an RP-Discovery to the Cisco discovery multicast group (224.0.1.40). The remote routers join the 224.0.1.40 group when **ip pim autorp listener** is configured.

The WAN links in this topology consist of broadband DSL and cable for the remote branch routers, DS3 or greater Internet links at the campus, and FastEthernet and GigabitEthernet between the primary, secondary, and disaster recovery site.

Detailed Topology

In a closer look at the topology, the individual remote routers are identified as well as the p2p GRE tunnel interface numbers on the headend IPsec and GRE router. All remote routers use the nomenclature of Tunnel0 for their primary p2p GRE tunnel, and Tunnel1 (where configured) as their backup or secondary p2p GRE tunnel. (See Figure 2.)

Figure 2 Topology Video Surveillance



The IPsec headend router uses dynamic crypto maps and static p2p GRE tunnels. A DMVPN configuration using multipoint GRE (mGRE) and Next Hop Resolution Protocol (NHRP) is a suitable alternative, and this configuration is used as discussed in Performance Testing, page 33. However, DMVPN and VTI do not support GRE keepalive, which is used in this sample configuration. As such, a dynamic IGP routing protocol such as EIGRP is configured.

To demonstrate the IPmc configuration, several IPmc-capable Panasonic WV-NM100 network color cameras are deployed. These cameras can source MPEG-4 compressed video streams to a configurable UDP unicast or multicast IP address, and are a feature rich and relatively inexpensive means of generating and viewing an IPmc application.

For more information on these cameras, see the following URL: http://www.panasonic.com.

Point-to-Point GRE over IPsec Configuration

This section provides sample configurations used in testing and internal Cisco deployments of IPmc in a teleworker environment. The IPmc application in use consists of IP video surveillance cameras streaming MPEG-4, both from a home office to a campus location and from the campus to the home office.

The following examples are shown:

- Configuration commands common to most routers in the topology
- IPmc RP configuration
- Headend IPsec and p2p GRE router

- Secondary campus and disaster recovery
- Disaster recovery host site router
- Remote branch routers

Common Configuration Commands

The configurations provided in this section are common to most routers in the sample topology, and as such, are provided in this section to avoid repetition in the later sections.

IPmc Commands

On the routers in this topology, IPmc routing is enabled globally, interfaces required to participate in the IPmc domain have IP PIM Sparse Mode enabled, and all routers except the IPmc RP routers are configured as IP PIM Auto-RP listeners.

```
!
ip multicast-routing
!
ip pim autorp listener
!
no ip pim dm-fallback
!
interface Ethernet0
 description [Inside Interface]
 ip pim sparse-mode
!
interface Tunnel0
 ip pim sparse-mode
 no ip mroute-cache
!
```

Note Because of CSCdu87170 (“IP Multicast not working over GRE tunnel when IPsec is enabled”), these configurations all process switch (**no ip mroute-cache**) IPmc packets.

Without implementing one of the problem circumventions listed, the IPmc encapsulated packets are transmitted out the outside interface in the clear. This presents a security exposure.

The **no ip pim dm-fallback** command prevents PIM Dense Mode fallback if all rendezvous points fail. This feature was introduced in Cisco IOS release 12.3(4)T.

QoS Configuration

The QoS configuration is similar to configurations used in V3PN deployments. Because the sample IPmc application is video surveillance, a *VIDEO-surveillance* class is included. Most Cisco IOS router hardware platforms support re-marking the ToS byte on an input interface, and as an illustration, the IPmc address space is remarked to IP Precedence 4 or DSCP value of CS4.

The output service policy allocates bandwidth for video surveillance as a percentage of the shaped rate. The percentage value should be adjusted based on the available bandwidth and the image size, quality, resolution, and encoding.

In this set of tests, voice, video, and data is present on the broadband link concurrently. The link speed in some cases was below 768 Kbps, and the **ip tcp adjust-mss** command is configured. The value of 542 is used on interfaces with IPsec direct encapsulation or unencrypted packets, and a value of 574 is used on interfaces with p2p GRE or mGRE and IPsec encryption.

```
!
class-map match-all VOICE
 match ip dscp ef
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match access-group name IKE
class-map match-any VIDEO-surveillance
 match ip dscp cs4
 match access-group name IPmc
!
ip access-list extended IPmc
 permit udp any 224.0.0.0 15.255.255.255 # Class 'D' address space
!
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
!
policy-map V3PN-teleworker
description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 128
 class VIDEO-surveillance
  bandwidth percent 45                  # Value depends on bandwidth and Video image
  queue-limit 10
 class class-default
  fair-queue
  random-detect
policy-map Shaper
 class class-default
  shape average 608000 6080             # Depends on link speed this value is used on a
                                        # Business class cable connection that is 768K up
  service-policy V3PN-teleworker
!
!
interface Ethernet1
 description Outside
 service-policy output Shaper
 ip route-cache flow
 ip tcp adjust-mss 542

interface Tunnel0
 ip mtu 1408
 ip tcp adjust-mss 574
 qos pre-classify
!
!                                     # Where supported, Video packets are marked on
!                                     # ingress. Not all IOS images support this feature
!
policy-map INGRESS
 class VIDEO-surveillance
  set ip dscp cs4
!
!
interface FastEthernet0/1
!
 service-policy input INGRESS
```

IPsec Configuration

The IPsec configuration is characterized by the following features:

- Digital certificates (PKI)
- IKE encrypted with 3DES and Diffie-Hellman group 2
- Dead Peer Detection and NAT Transparency (NAT-T) keepalives
- IPsec encrypted with 3DES, HMAC of SHA-1, and tunnel mode
- The branch router p2p GRE tunnel source is an RFC1918 address on Loopback1
- Headend routers use dynamic crypto maps

The outside interface is protected by an input access control list (ACL) where appropriate. Examples of the ACL and the spouse-and-child security configuration are shown in later configuration examples.

```
!
crypto pki trustpoint rtp5-esevpn-ios-ca
 enrollment url http://rtp5-esevpn-ios-ca:80
 revocation-check none
 source interface Ethernet0
 auto-enroll 70
!
crypto pki certificate chain rtp5-esevpn-ios-ca
 certificate 2E
 certificate ca 01
!
crypto isakmp policy 100
 encr 3des
 group 2
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
!
crypto map Encrypt_GRE 10 ipsec-isakmp
 set peer xx.xxx.223.23
 set transform-set 3DES_SHA_TUNNEL
 match address Encrypt_GRE
!
ip access-list extended Encrypt_GRE
 permit gre host _tunnel_source  host xx.xxx.223.23
!
interface Loopback1
 description Anchor for GRE tunnel
ip address _tunnel_source  255.255.255.255

!
interface Tunnel0
 tunnel source Loopback1
 tunnel destination xx.xxx.223.23
!
interface Ethernet1
 description Outside
 ip address dhcp
 ip access-group INPUT_ACL in
 no cdp enable
 crypto map Encrypt_GRE
!
!
```

Other Configuration Commands

These configuration commands are not characterized by the previous classifications. Note the following:

- Cisco Express Forwarding (CEF) is configured.
- Services such has SNMP, Syslog, Telnet, and TFTP are sourced so that they are protected by the encrypted p2p GRE tunnel.
- IP SLA, formerly known as Service Assurance Agent (SAA), is configured to provide a history for troubleshooting.

```
!
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
ip telnet source-interface Ethernet0             # Inside Interface
ip tftp source-interface Ethernet0               # Inside Interface
no ip domain lookup
ip domain name cisco.com
!
ip host rtp5-esevpn-ios-ca 10.81.0.27
ip host vpn3-7200-1 10.59.138.1
ip host multicast-RP 10.81.7.219
ip host harry 172.26.129.252
ip host CAMERA2 10.59.138.21
ip host CAMERA1 10.81.7.227
!
ip name-server 207.69.188.185
ip cef
!
ip classless
!
ip access-list extended INPUT_ACL
 remark Allow IKE and ESP from the RTP headends
 permit udp xx.xxx.223.16 0.0.0.15 any eq isakmp
 permit udp xx.xxx.223.16 0.0.0.15 any eq non500-isakmp
 permit esp xx.xxx.223.16 0.0.0.15 any
 permit gre xx.xxx.223.16 0.0.0.15 any
 permit udp any any eq bootpc
 remark NTP ACLs
 permit udp 192.5.41.40 0.0.0.1 eq ntp any
 permit udp host 216.210.169.40 eq ntp any
 remark SSH
 permit tcp xx.xxx.87.0 0.0.0.255 any eq 22
 permit icmp any any
 deny   ip any any

no ip http server
no ip http secure-server
ip flow-export version 5
!
logging source-interface Ethernet0       # Logging will be source always on the inside
                                         #  interface so they are encrypted

#
#
rtr responder
```

```
rtr 12
 type echo protocol ipIcmpEcho 172.26.129.252 source-ipaddr _Inside_IP_Address_
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 life forever start-time now
!
banner motd ^C
   C i s c o S y s t e m s
      ||               ||
      ||               ||       Cisco Systems, Inc.
     ||||             ||||      IT-Transport
 .:|||||||:.......:|||||||:..
  US, Asia & Americas support:    + 1 408 526 8888
 EMEA support:                     + 31 020 342 3888
  UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in disciplinary action.
^C
alias exec scr show running | b crypto isakmp
alias exec wrnet copy run tftp://harry/vpn/ECTW/_hostname_confg
alias exec crylife show cry ipsec sa det | inc eer|life|local|spi
!
line con 0
 exec-timeout 120 0
 login local
 no modem enable                                  # Cisco 830 Series specific
 transport preferred all
 transport output all
 stopbits 1
line aux 0
 transport preferred all
 transport output all
 stopbits 1
line vty 0 4
 exec-timeout 120 0
 login local
 transport preferred all
 transport input ssh
 transport output all
!
exception memory minimum 786432
scheduler max-task-time 5000
ntp server 192.5.41.41                           # External NTP Server
ntp server 192.5.41.40                           # External NTP Server
ntp server 216.210.169.40                        # External NTP Server
ntp server 10.81.254.202 source Ethernet0        # Internet NTP Server source off “Inside”
end
```

IPmc Rendezvous Point and IP PIM Auto-RP Configuration

Because this configuration uses IP PIM Sparse Mode, two routers (for availability) in the network core are configured to be RPs. RPs are used by senders to an IPmc group to announce their existence and by receivers of IPmc packets to learn about new senders.

The first hop router for an IPmc source (the video camera in this example) sends an IP PIM register message on behalf of the source to the RP, and the RP acknowledges receipt with a Register-Stop. An example of this exchange is shown in Appendix A—Output of debug ip pim, page 40.

The RP address is used by last hop routers (routers with workstations on a LAN interface interested in receiving IPmc packets) to send IP PIM join and prune messages to the RP to inform it about group membership. An example is shown in Appendix B—Output from Last Hop Router rtp9-ese-test, page 40.

Rather than manually configuring the RP in all routers, this configuration uses the Cisco IOS features IP PIM Auto-RP and RP-mapping agent. The IP PIM Auto-RP feature eliminates the need for this manual configuration because it automates the distribution of group-to-RP mappings. IP PIM Auto-RP requires the configuration of an RP-mapping agent to arbitrate conflicts between the two RPs. The RP-mapping agent provides consistent group-to-RP mappings to all other routers in the IP PIM network.

Primary

```
!
hostname multicast-RP
!
boot-start-marker
boot system flash:c3725-advipservicesk9-mz.123-12
boot-end-marker
!
ip multicast-routing
!
interface FastEthernet0/0
 ip address 10.81.7.219 255.255.255.248
 ip pim sparse-mode
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 10.81.7.217 name video831
!
ip pim send-rp-announce FastEthernet0/0 scope 32 group-list MY_IPmc_Groups
ip pim send-rp-discovery FastEthernet0/0 scope 5
!
ip access-list standard MY_IPmc_Groups
 permit 224.1.1.0 0.0.0.255
!  Do not code a  deny   any
!
end
```

Note Do not code an explicit “deny any” in the standard access list My_IPmc_Groups because it forces all groups other than the groups specified on the permit statement into IP PIM Dense Mode throughout the network.

Secondary

```
!
hostname vpn3-7200-1
!
boot system flash disk0:c7200-ik9o3s-mz.122-13.6.S
!
!
ip multicast-routing
!
interface FastEthernet1/0
 description vpn4-2651xm-1 for Joel's Multicast Testing
 ip address 10.59.136.13 255.255.255.252
```

```
 ip pim sparse-mode
 load-interval 30
 duplex full
 speed 100
!
!
interface GigabitEthernet4/0
 description To vpn3-2948-1
 ip address 10.59.138.1 255.255.254.0
 ip pim sparse-mode
 !
 load-interval 30
 negotiation auto
!
ip route 10.81.7.0 255.255.255.0 10.59.136.14 name ECT_SUBNETS
!
ip pim send-rp-announce GigabitEthernet4/0 scope 16
ip pim send-rp-discovery GigabitEthernet4/0 scope 16
!
end
```

Headend p2p GRE over IPsec Router

This section provides the configuration of a headend p2p GRE over IPsec router. Only one router is shown, but as previously noted, Cisco recommends having redundant headends for greater availability.

Unlike the configuration of the remote routers, the headend routers require certificate revocation checking. Because this topology includes branches with broadband connections that obtain IP addresses dynamically, the headend router uses a dynamic crypto map.

There is no routing protocol configured on the p2p GRE tunnel interfaces. Rather, static routes to the p2p GRE interfaces are redistributed into EIGRP, and reachability to the remote router is validated by GRE keepalives. The IP maximum transmission unit (MTU) of the p2p GRE interfaces forces fragmentation before encryption if required.

This router is configured as a “router on a stick”; encrypted and de-encrypted packets enter and leave on the same physical interface. In this configuration, there are two other IPsec headend routers, and EIGRP neighbors are formed with these routers on interface FastEthernet1/1. The gateway router to the enterprise campus network (10.81.0.17) advertises a summary address to the core network. This gateway router forwards all packets for the remote subnets to an IP HSRP address (10.81.0.20), and the active IP HSRP router forwards the packets to the appropriate IPsec headend router based on the specific network advertisements from EIGRP.

```
!
hostname rtp5-esevpn-gw3
!
boot-start-marker
boot system disk0:c7200-ik9o3s-mz.123-8.T6
boot-end-marker
!
aaa authentication login default group tacacs+ enable
aaa session-id common
!
ip multicast-routing
!
crypto pki trustpoint rtp5-esevpn-ios-ca
 enrollment url http://rtp5-esevpn-ios-ca:80
 revocation-check crl                        # Unlike the remote routers
!                                            # the headend checks CRLs
 auto-enroll 70
```

```
!
controller ISA 2/1
!
crypto isakmp keepalive 10
!
crypto dynamic-map DYNOMAP 10
 set transform-set 3DES_SHA_TUNNEL
!
crypto map DynamicGRE local-address Loopback0
crypto map DynamicGRE 10 ipsec-isakmp dynamic DYNOMAP
!
interface Tunnel104
 ip address 10.81.7.192 255.255.255.254
 ip mtu 1408
 ip pim sparse-mode
 no ip mroute-cache
 keepalive 10 3                              # There is no routing protocol configured
 tunnel source Loopback0
 tunnel destination 10.81.7.209              # Remote Router Loopback 1
!
interface Tunnel136
 ip address 10.81.7.190 255.255.255.254
 ip mtu 1408
 ip pim sparse-mode
 no ip mroute-cache
 keepalive 10 3                              # There is no routing protocol configured
 tunnel source Loopback0
 tunnel destination 10.81.7.214              # Remote Router Loopback 1
!
interface Tunnel212
 ip address 10.81.7.184 255.255.255.254
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow                  # Netflow enabled on some tunnels for illustration
 no ip mroute-cache
 load-interval 30
 keepalive 10 3                              # There is no routing protocol configured
 tunnel source Loopback0
 tunnel destination 10.81.7.212              # Remote Router Loopback 1
!
interface Tunnel216
 ip address 10.81.7.194 255.255.255.254
 ip mtu 1408
 ip pim sparse-mode
 no ip mroute-cache
 keepalive 10 3                              # There is no routing protocol configured
 tunnel source Loopback0
 tunnel destination 10.81.7.213              # Remote Router Loopback 1
!
interface Tunnel224
 ip address 10.81.7.188 255.255.255.254
 ip mtu 1408
 ip pim sparse-mode
 no ip mroute-cache
 keepalive 10 3                              # There is no routing protocol configured
 tunnel source Loopback0
 tunnel destination 10.81.7.210              # Remote Router Loopback 1
!
interface Tunnel232
 ip address 10.81.7.186 255.255.255.254
 ip mtu 1408
 ip pim sparse-mode
 no ip mroute-cache
 keepalive 10 3                              # There is no routing protocol configured
```

```
 tunnel source Loopback0
 tunnel destination 10.81.7.211              # Remote Router Loopback 1
!
interface Loopback0
 description Public address
 ip address xx.xxx.223.23 255.255.255.255
!
interface Loopback10
 description Loopback
 ip address 10.81.7.208 255.255.255.255
 ip pim sparse-mode
!
!
interface FastEthernet1/0
 description Private – Campus Network
 ip address 10.81.0.23 255.255.255.240
 ip route-cache same-interface               # Router on a Stick
 ip route-cache flow
 duplex full
 speed 100
 standby 1 ip 10.81.0.20
 standby 1 priority 90
 standby 1 preempt
 standby 1 authentication [removed]
 crypto map DynamicGRE
!
!                                            # Exchange routing with IPsec direct DPD/RRI
!                                            # headends on this F1/1 interface
!                                            # See network statement 'router eigrp 64'
interface FastEthernet1/1
description VLAN 101
 ip address 192.168.82.23 255.255.255.0
 duplex full
 speed 100
!
!
router eigrp 64
 redistribute static metric 9 5000 255 1 1408 route-map REMOTE_NETS
 network 192.168.82.0
 no auto-summary
 no eigrp log-neighbor-warnings
!
ip route 0.0.0.0 0.0.0.0 10.81.0.17
ip route 10.81.7.208 255.255.255.248 10.81.0.17 name Remote_loopbacks
!
!       # Instead of running a routing protocol on the Tunnel interface, will
!       # use GRE keepalives and a static route to the respective tunnel interface
!       # for the remote network[s] addresses
!
ip route 10.59.136.12 255.255.255.252 Tunnel212 name LAB_NET
ip route 10.59.138.0 255.255.254.0 Tunnel212 name LAB_NET
ip route 10.81.7.104 255.255.255.248 Tunnel104 name johnjo-1841-vpn
ip route 10.81.7.136 255.255.255.248 Tunnel136 name Video1751
ip route 10.81.7.216 255.255.255.248 Tunnel216 name Video831
ip route 10.81.7.224 255.255.255.248 Tunnel224 name vpn-jk2-1711-vpn
ip route 10.81.7.232 255.255.255.248 Tunnel232 name rtp9-ese-test
!
!
ip pim autorp listener
!
!       # Candidates for redistribution provided the respective tunnel interface is UP/UP
!
ip access-list standard REMOTE_NETS
 permit 10.81.7.0 0.0.0.255          # These networks are in the remote branch locations
```

```
 permit 10.59.138.0 0.0.1.255            # This network is in the secondary campus
 permit 10.59.136.12 0.0.0.3             # This network is in the secondary campus
 deny   any
!
ip radius source-interface Loopback0
!
route-map REMOTE_NETS permit 10
 description Redistribute remote subnets from static to GRE
 match ip address REMOTE_NETS
!
tacacs-server host xxx.xx.10.137
tacacs-server host xxx.xx.11.123
tacacs-server directed-request
!
radius-server attribute 69 clear
radius-server attribute 6 on-for-login-auth
radius-server host 10.81.0.19 auth-port 1645 acct-port 1646 key 7 [removed]
exception memory fragment 32768
exception memory minimum io 262144
exception memory minimum 1048576
end
```

Secondary Campus and Disaster Recovery

Two routers in this topology represent secondary and tertiary branch locations.

Secondary Campus

This router supports the secondary campus. The secondary RP, CAMERA_2, and workstations are present at this location.

```
!
hostname vpn4-2651xm-1
!
!       System image file is "flash:c2600-advsecurityk9-mz.123-8.T5"
!
interface Tunnel0
 ip address 10.81.7.185 255.255.255.254
 ip pim sparse-mode
 no ip mroute-cache
 load-interval 30
 qos pre-classify
 keepalive 10 3                          # There is no routing protocol configured
 tunnel source Loopback1
 tunnel destination xx.xxx.223.23
!
interface Loopback1
 description Anchor for GRE tunnel
 ip address 10.81.7.212 255.255.255.255
!
interface FastEthernet0/0
 description FlashNet [Outside Interface]
 ip address 172.26.177.250 255.255.252.0
 ip access-group INPUT_ACL in
 service-policy output Shaper        # The shaped value depends on the bandwidth between
!                                    # this and the primary campus
 load-interval 30
 speed 100
 full-duplex
 crypto map Encrypt_GRE
!
```

```
interface FastEthernet0/1
 description To vpn3-7200-1 [Inside Interface]
 ip address 10.59.136.14 255.255.255.252
 ip pim sparse-mode
 service-policy input INGRESS
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 Tunnel0
!
!   The 10.59.138.0/23 network is on GigE 4/0 on vpn3-7200-1, the IPmc RP
!
ip route 10.59.138.0 255.255.254.0 10.59.136.13 name vpn3-7200-1
ip route 10.81.254.131 255.255.255.255 172.26.176.1 name NTP
ip route 10.81.254.202 255.255.255.255 172.26.176.1 name NTP
ip route xx.xxx.223.23 255.255.255.255 172.26.176.1 name rtp5-esevpn-gw3# Crypto Peer
ip route 172.26.129.252 255.255.255.255 172.26.176.1 name HARRY
ip pim autorp listener
!
end
```

Disaster Recovery Host Site Router

This router is the third campus location. It supports the primary RP.

```
version 12.3
!
hostname video-831
!
!   System image file is "flash:c831-k9o3sy6-mz.123-8.T5"
!
ip dhcp excluded-address 10.81.7.219     # Address of the IPmc RP on this network
ip dhcp pool Client
   import all
   network 10.81.7.216 255.255.255.248
   default-router 10.81.7.217
   dns-server xx.xxx.6.247 171.68.226.120
   domain-name cisco.com
   option 150 ip xx.xxx.2.93
   netbios-name-server xxx.xx.235.228 xxx.xx.235.229
!
interface Tunnel0
 ip address 10.81.7.195 255.255.255.254
 ip mtu 1408
 ip pim sparse-mode
 ip tcp adjust-mss 574
 no ip mroute-cache
 load-interval 30
 qos pre-classify
 keepalive 10 3                          # There is no routing protocol configured
!                                        # Using GRE keepalives instead
 tunnel source Loopback1
 tunnel destination xx.xxx.223.23
!
interface Loopback1
 description Anchor for GRE tunnel
 ip address 10.81.7.213 255.255.255.255
!
interface Ethernet0
 description [Inside Interface]
```

```
 ip address 10.81.7.217 255.255.255.248
 ip pim sparse-mode
 ip virtual-reassembly
 ip tcp adjust-mss 574
 no ip mroute-cache
 load-interval 30
 no cdp enable
 hold-queue 32 in
!
interface Ethernet1
 description Outside
 ip address dhcp
 ip access-group INPUT_ACL in
 ip virtual-reassembly
 service-policy output Shaper         # The shaped value depends on the bandwidth between
!                                     # this and the primary campus
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 duplex auto
 no cdp enable
 crypto map Encrypt_GRE
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet3
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 Tunnel0             # All enterprise packets in tunnel
ip route xx.xxx.223.23 255.255.255.255 dhcp  # Route for headend crypto peer
ip route 192.5.41.40 255.255.255.254 dhcp    # Route for NTP server[s]
!
end
```

Remote Branch Routers

Two branch routers are shown: a branch with a camera, CAMERA_1, and a branch with a workstation configured to view both CAMERA_1 and CAMERA_2.

Branch with Camera_1

This branch is also configured to allow direct access to the Internet for a spouse-and-child subnet. All enterprise packets are sent to the campus via the p2p GRE over IPsec tunnel. This type of configuration is also useful for a branch location that needs to provide Internet access for customers or employees.

```
!
hostname vpn-jk2-1711-vpn
!
boot-start-marker
boot system flash c1700-k9o3sy7-mz.123-8.T5
boot system flash
boot-end-marker
!
ip dhcp excluded-address 192.168.1.1 192.168.1.99
!
ip dhcp pool Client                          # This is the enterprise subnet
   import all
   network 10.81.7.224 255.255.255.248
   default-router 10.81.7.225
   dns-server xx.xxx.6.247 171.68.226.120
   domain-name cisco.com
   option 150 ip 10.59.138.51
   netbios-name-server xxx.xx.235.228 xxx.xx.235.229
!
ip dhcp pool SpouseChild                     # This is the Spouse and Child subnet
   import all
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
!
ip flow-cache feature-accelerate             # See VLAN2 Interface comments
ip cef
!
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
!
!
!
!
class-map match-all SpouseChild
 match access-group name pNAT_ACL
!
policy-map Shaper
 class class-default
  shape average 182400 1824                  # DSL with 256K uplink
  service-policy V3PN-teleworker
!
policy-map INGRESS
 class VIDEO-surveillance
  set ip dscp cs4
 class SpouseChild                           # On ingress all packets from this network
!                                            # will be re-marked to best effort
  set ip dscp default
 class class-default

crypto isakmp keepalive 10
crypto isakmp nat keepalive 10               # NAT-T is being used
!
!
interface Tunnel0
 description tunnel 0
 ip address 10.81.7.189 255.255.255.254
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 ip tcp adjust-mss 574
 no ip mroute-cache
 load-interval 30
 qos pre-classify
```

```
 keepalive 10 3                                    # There is no routing protocol configured
 tunnel source Loopback1
 tunnel destination xx.xxx.223.23
!
interface Tunnel1
 description Tunnel 1 [secondary tunnel - NOT IMPLEMENTED]
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 ip tcp adjust-mss 574
 load-interval 30
 qos pre-classify
 keepalive 10 3                                    # There is no routing protocol configured
 tunnel source Loopback1
!
interface Loopback1
 description Anchor for GRE tunnel
 ip address 10.81.7.210 255.255.255.255
!
interface FastEthernet0
 description Outside
 ip address dhcp
 ip access-group INPUT_ACL in
 ip nat outside
 ip inspect CBAC out
 ip virtual-reassembly
 service-policy output V3PN-teleworker
 ip route-cache flow
 ip tcp adjust-mss 542
 duplex auto
 speed auto
 no cdp enable
 crypto map Encrypt_GRE
!
interface FastEthernet1
 description CORPORATE NETWORK PORT - VLAN 1 by default
 no ip address
!
interface FastEthernet2
 description CORPORATE NETWORK PORT - VLAN 1 by default
 no ip address
!
interface FastEthernet3
 description SPOUSE_CHILD PORT - VLAN 2
 switchport access vlan 2
 no ip address
!
interface FastEthernet4
 description SPOUSE_CHILD PORT - VLAN 2
 switchport access vlan 2
 no ip address
!
interface Vlan1
 description Inside
 ip address 10.81.7.225 255.255.255.248
 ip pim sparse-mode
 service-policy input INGRESS
 ip route-cache flow
 ip tcp adjust-mss 574
 no ip mroute-cache
 load-interval 30
 hold-queue 40 out
!
interface Vlan2
```

```
 description SPOUSE_CHILD
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 service-policy input INGRESS
 ip route-cache flow
 ip tcp adjust-mss 542
 ip policy route-map SPOUSE_CHILD
 load-interval 30
!
!                                                # All enterprise packets in tunnel
ip route 0.0.0.0 0.0.0.0 Tunnel0 20 name primary_tunnel
ip route 0.0.0.0 0.0.0.0 Tunnel1 40 name secondary_tunnel
!
ip route xx.xxx.223.23 255.255.255.255 dhcp  # Route for headend crypto peer
ip route 192.5.41.40 255.255.255.254 dhcp    # Route for NTP server[s]
!
ip nat inside source list pNAT_ACL interface FastEthernet0 overload
ip pim autorp listener
!
ip access-list extended pNAT_ACL
 permit ip 192.168.1.0 0.0.0.255 any
!
route-map SPOUSE_CHILD permit 10
!
 description Force all SPOUSE_CHILD to Internet unencrypted
 match ip address pNAT_ACL
 set interface FastEthernet0
 set ip next-hop dynamic dhcp
!
alias exec show_vlan_database vlan database
alias exec update_vlan_databas vlan database
!
end
```

Branch with Workstation

This section shows both the router configuration as well as the software application configuration.

Router Configuration

```
!
hostname rtp9-ese-test
!
boot-start-marker
boot system flash c1700-k9o3sy7-mz.123-12a
boot system flash
boot-end-marker
!
ip host CAMERA2 10.59.138.21
ip host CAMERA1 10.81.7.227
!
ip dhcp pool Client
   import all
   network 10.81.7.232 255.255.255.248
   default-router 10.81.7.233
   dns-server xx.xxx.6.247 xxx.xx.226.120
   domain-name cisco.com
   option 150 ip xx.xxx.2.93
   netbios-name-server xxx.xx.235.228 xxx.xx.235.229
!
!
```

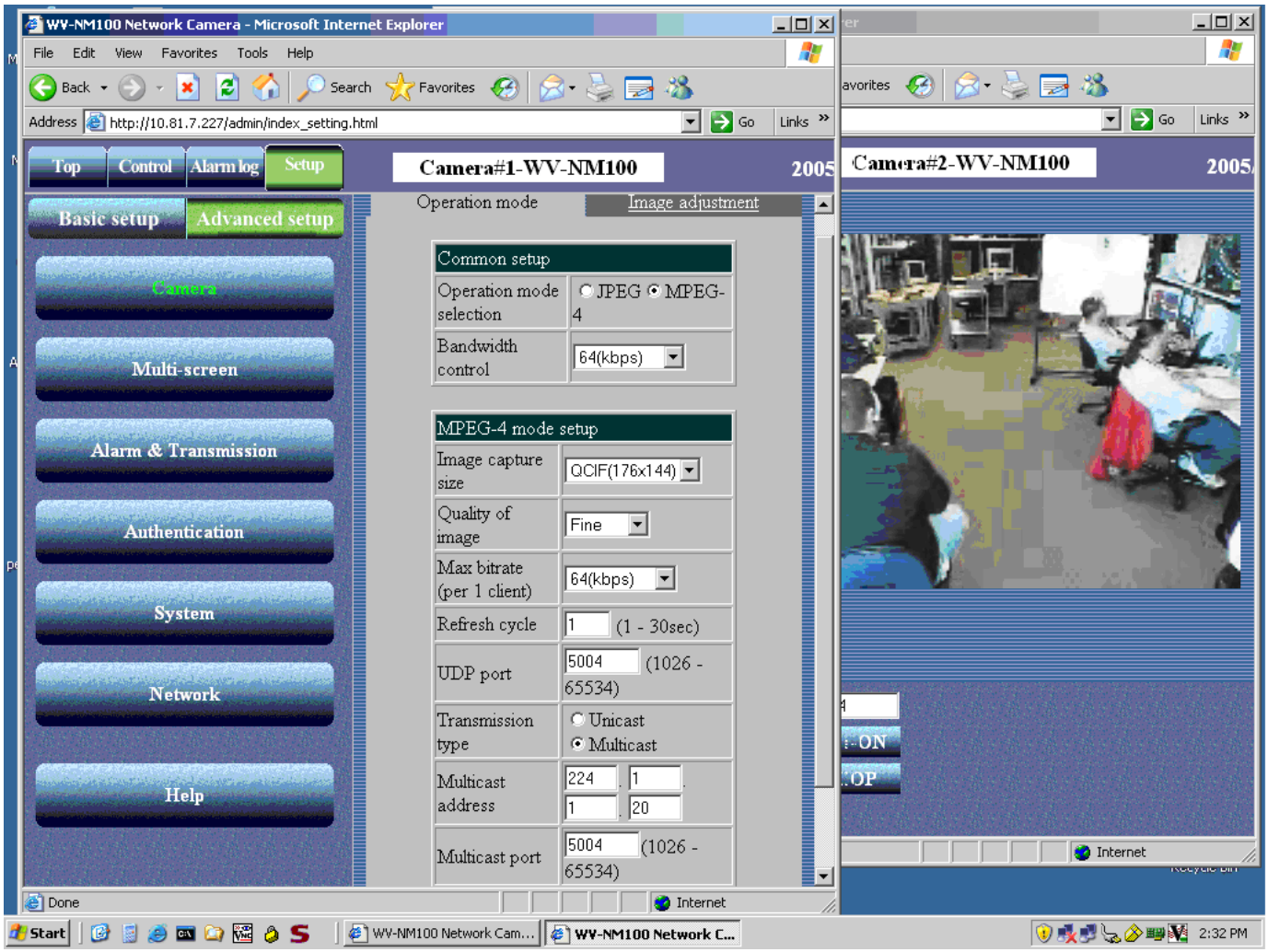
```
interface Loopback1
 description Anchor for GRE tunnel
 ip address 10.81.7.211 255.255.255.255
!
interface Tunnel0
 ip address 10.81.7.187 255.255.255.254
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 ip tcp adjust-mss 574
 no ip mroute-cache
 load-interval 30
 qos pre-classify
 keepalive 10 3
 tunnel source Loopback1
 tunnel destination xx.xxx.223.23
!
interface Ethernet0/0
 description Outside
 ip address dhcp
 ip access-group INPUT_ACL in
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 half-duplex
 no cdp enable
 crypto map Encrypt_GRE
 service-policy output Shaper
!
interface FastEthernet0/0
 description Inside
 ip address 10.81.7.233 255.255.255.248
 ip pim sparse-mode
 ip route-cache flow
 ip tcp adjust-mss 574
 no ip mroute-cache
 load-interval 30
 speed auto
 no keepalive
 service-policy input INGRESS
 hold-queue 40 out
!
ip route 0.0.0.0 0.0.0.0 Tunnel0 40# All enterprise packets in tunnel
ip route xx.xxx.223.23 255.255.255.255 dhcp# Route for headend crypto peer
ip route 192.5.41.40 255.255.255.254 dhcp# Route for NTP server[s]
!
end
```

Workstation—Network Camera Software Configuration

Camera_1 uses IPmc group 224.1.1.20 and UDP port 5004, while Camera_2 uses IPmc group 224.1.1.21 and UDP port 5004.

Figure 3 shows the Advanced Setup screen for Camera 1 in the foreground, while the background browser is displaying the IPmc transported MPEG-4 image.

Figure 3 Camera 1—Advanced Setup Screen and Background Browser



Virtual Tunnel Interface Configuration

This section shows how the previous configuration example may be implemented using Dynamic Virtual Tunnel Interface (DVTI). The VTI feature can be configured using static tunnels on both the branch and headend routers, or a static tunnel on the branch router and a dynamic tunnel configuration by means of virtual templates on the headend router. This example shows the use of the dynamic feature on the headend routers.

VTI Support for IPmc

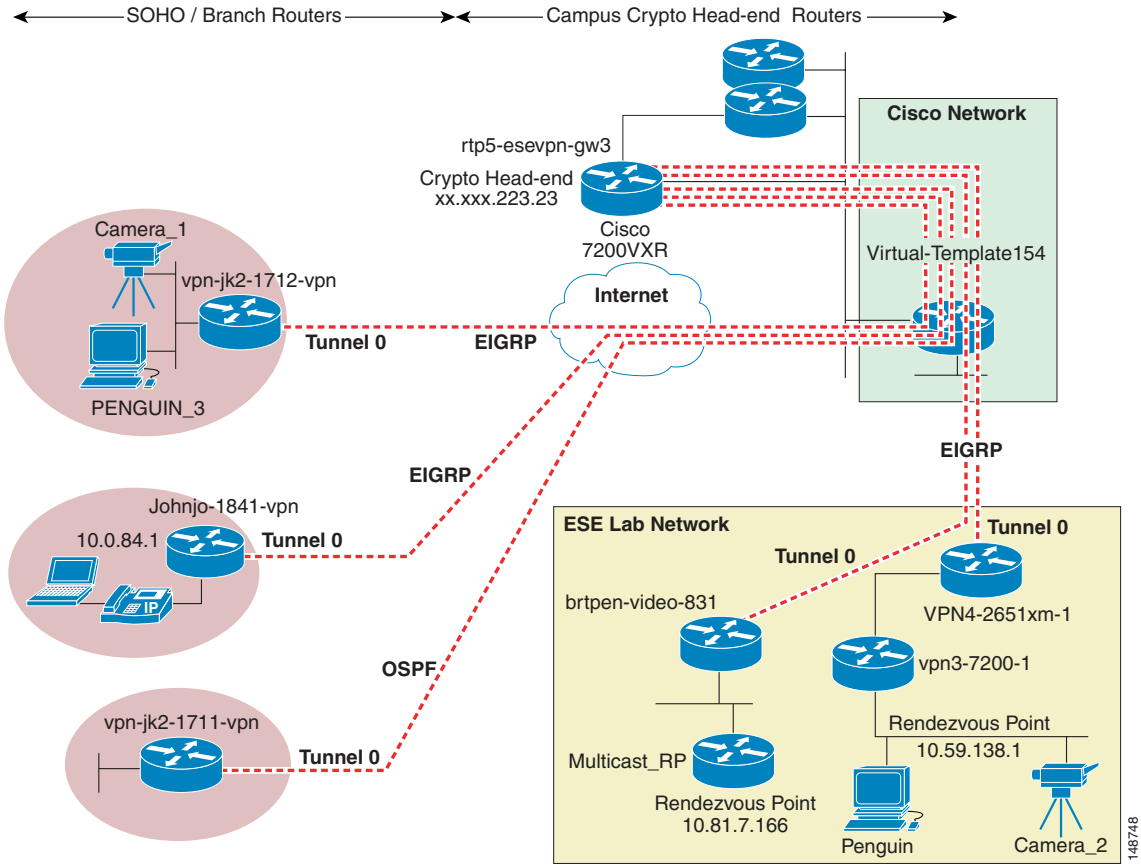
To demonstrate a working configuration of VTI support of IPmc, this deployment is implemented over broadband Internet connections and the internal Cisco network.

All routers are configured with IP PIM Sparse Mode and **ip pim autorp listener** and two RPs. Panasonic video surveillance cameras are deployed as IPmc sources, and the Panasonic IPmc plug-in for a web browser is the sink.

Topology

The basic topology shown in Figure 4 is implemented. It is similar to the sample topology in Figure 2. The main difference is the incorporation of VTI in place of an encrypted p2p GRE tunnel. The GRE keepalive has been replaced with both EIGRP and OSPF. The branch router configuration shown is an EIGRP configuration.

Figure 4 IPmc Topology—VTI



There are two cameras and any branch can view images from both cameras. There are two RPs.

Configuration Examples

The IPmc configuration is identical to the p2p GRE over IPsec configuration in the previous section. The headend router configuration shown now includes the IPmc commands on the virtual template interface rather than a p2p GRE interface. Because the interface is created dynamically, which means a virtual access interface is cloned from the virtual template interface, a dynamic IGP routing protocol must be used instead of redistributing static routes that use the p2p GRE interface as their next hop.

Headend Router Configuration

The following is the relevant portion of the Cisco 7200VXR Series headend router.

```
!
hostname rtp5-esevpn-gw3
!
boot-start-marker
boot system disk0:c7200-advipservicesk9-mz.124-2.T1.bin
boot system disk0:
boot-end-marker
!
ip multicast-routing
!
crypto pki trustpoint rtp5-esevpn-ios-ca
 enrollment url http://rtp5-esevpn-ios-ca:80
 revocation-check crl
 auto-enroll 70
!
crypto pki certificate chain rtp5-esevpn-ios-ca
 certificate 21
 certificate ca 01
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
crypto isakmp profile VTI_1544K
   description TEST for VTI Templates 1.544K
   ca trust-point rtp5-esevpn-ios-ca
   match identity host domain cisco.com
   keepalive 10 retry 2
   virtual-template 154
   local-address Loopback0
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set COMPRESS esp-3des esp-sha-hmac comp-lzs
!
crypto ipsec profile VirtualTunnelInterface
 set transform-set COMPRESS 3DES_SHA_TUNNEL
 set isakmp-profile VTI_1544K
!
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 1.544K DOWNLINK
 ip unnumbered Loopback10
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 no ip mroute-cache
 ip ospf mtu-ignore
 load-interval 30
 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 VTI_plus_RRI
 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
!
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
!
ip route 0.0.0.0 0.0.0.0 10.81.0.17
!
ip pim autorp listener
!
ip access-list standard Quad_ZERO_to_BRANCH
 permit 0.0.0.0
!
ip access-list standard REMOTE_NETS
 permit 0.0.0.0
 permit 10.81.7.0 0.0.0.255
 permit 10.59.138.0 0.0.1.255
 permit 10.59.136.12 0.0.0.3
 deny   any
!
route-map VTI_plus_RRI permit 10
 match ip address REMOTE_NETS
!
end
```

Note the following in this configuration:

- Interface Loopback10 has IP PIM enabled because Virtual-Template154 borrows the IP address of Loopback10. This is required in the configuration.
- The virtual template is process switching IPmc.
- QoS is enabled on the virtual template; however, the class maps and policy maps are not shown. The EIGRP (and OSPF) configuration is advertising only a default route to the branch routers.

This headend router supports both IPsec VTI branches as well as IPsec Direct Encapsulation branches, which is why the route map that redistributes static routes into EIGRP is named *VTI_plus_RRI.* For the VTI branches, the default (0.0.0.0/0.0.0.0) route is redistributed so that the branch routers can learn this route by means of EIGRP. For the IPsec Direct Encapsulation branches, RRI is enabled automatically. The RRI-injected static routes are redistributed to the other headend EIGRP neighbors.

Note The IPsec Direct Encapsulation branches cannot send or receive IPmc traffic.

Both EIGRP and OSPF are enabled for the virtual template interface. The branch router configuration, depending on whether EIGRP or OSPF is configured, determines which routing protocol forms a neighbor relationship over the VTI tunnel.

Lempel-Ziv Stac (LZS—a registered trademark of Hi/fn, Inc.) compression is also included in the transform set. If the branch router supports and is also configured for LZS compression, LZS compression is enabled between the crypto peers.

This headend configuration is therefore very generic; it can support a mixture of EIGRP or OSPF peers, as well as branch routers that support compression and those that do not.

EIGRP Branch Router Configuration

The relevant portion of one branch router configuration is as follows:

```
!
hostname johnjo-1841-vpn
!
boot-start-marker
boot system flash:c1841-advipservicesk9-mz.124-4.9.T
boot-end-marker
!
ip multicast-routing
ip multicast-routing vrf employee
!
interface Tunnel0
 description -> rtp5-esevpn-gw3
 ip vrf forwarding employee
 ip unnumbered FastEthernet0/1
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 ip tcp adjust-mss 574
 no ip mroute-cache
 load-interval 30
 tunnel source FastEthernet0/0
 tunnel destination xx.xxx.223.23
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
!
!       This headend route is not shown in the topology or configuration.
!
interface Tunnel1
 description -> rtp5-esevpn-gw5
 ip vrf forwarding employee
 ip unnumbered FastEthernet0/1
 ip mtu 1408
 ip pim sparse-mode
 ip route-cache flow
 ip tcp adjust-mss 574
 no ip mroute-cache
 load-interval 30
 delay 60000
 tunnel source FastEthernet0/0
 tunnel destination xx.xxx.223.25
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VTI
!
interface FastEthernet0/0
 description Outside
 ip address dhcp
 ip access-group INPUT_ACL in
 ip nat outside
 ip virtual-reassembly
 ip route-cache flow
 load-interval 30
 service-policy output Shaper
!
!
interface FastEthernet0/1
 description Inside
```

```
 ip vrf forwarding employee
 ip address 10.81.7.105 255.255.255.248
 ip pim sparse-mode
 ip route-cache flow
 ip tcp adjust-mss 574
 no ip mroute-cache
!
router eigrp 64
 passive-interface FastEthernet0/1
 auto-summary
 !
 address-family ipv4 vrf employee
 network 10.0.0.0
 no auto-summary
 autonomous-system 64
 eigrp stub connected
 exit-address-family
!
ip pim autorp listener
!
ip route xx.xxx.223.23 255.255.255.255 dhcp
ip route 192.5.41.40 255.255.255.254 dhcp
ip route xx.xxx.223.25 255.255.255.255 dhcp
!
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 (connected) network to the headend. EIGRP stub is configured. The headend router advertises only a default route to this branch router through the Tunnel0 interface. The Tunnel0 interface borrows the IP address of the inside employee network.

DMVPN Hub-and-Spoke (mGRE) Configuration

This configuration is shown in Performance Testing, page 33.

IPmc Deployment Summary

IPmc deployments in IPsec-encrypted WAN networks require the use of p2p GRE, mGRE, or VTI to encapsulate the IPmc packet in an IP unicast packet for encryption.

The recommended configuration uses IP PIM Sparse Mode and IP PIM Auto-RP listener.

Although not shown or tested in this example configuration, Anycast RP is an implementation strategy that provides load sharing and redundancy in PIM Sparse Mode networks. Anycast RP allows two or more RPs to share the load for source registration and the ability to act as hot backup routers for each other. Anycast RP can increase the availability by quickening convergence. Network managers may wish to consider such an implementation if their network so requires.

There are limitations in some Cisco IOS releases in supporting IPsec encryption of IPmc in the fast switching path. In these instances, IPmc must be processed switched. On the branch router, the performance impact of this is minimal. On the headend, implementing the encryption function from the IPmc replication and p2p GRE encapsulation circumvents this limitation. The following section shows an example of this headend topology.

Performance Testing

This section provides performance test results for a large-scale voice, data, and IPmc deployment.

Overview

Although the sender and receiver of the IPmc stream do not incur any additional burden of sending or receiving a IPmc stream, regardless of the number of receivers present in the network, the routers in the network do consume additional CPU resources. The routers consume additional resources with both the control plane of IPmc and the data replication function.

The control plane consists primarily of Internet Group Management Protocol (IGMP) and PIM. Routers listen to IGMP messages from hosts on their local networks and periodically send out queries to discover which groups are active or inactive. PIM is often called an IPmc routing protocol, but actually it uses the global routing table rather than creating its own IPmc routing table. After the router has been configured globally for IPmc routing, interfaces are enabled for multicast based on the presence of some form of PIM configured on the interface. Depending on the configuration option used, PIM can force the packet replication for all IPmc packets (PIM Dense Mode) or only replicate packets for interfaces that have active receivers (IP PIM Sparse Mode). The recommended configuration uses IP PIM Sparse Mode and IP PIM Auto-RP listener.

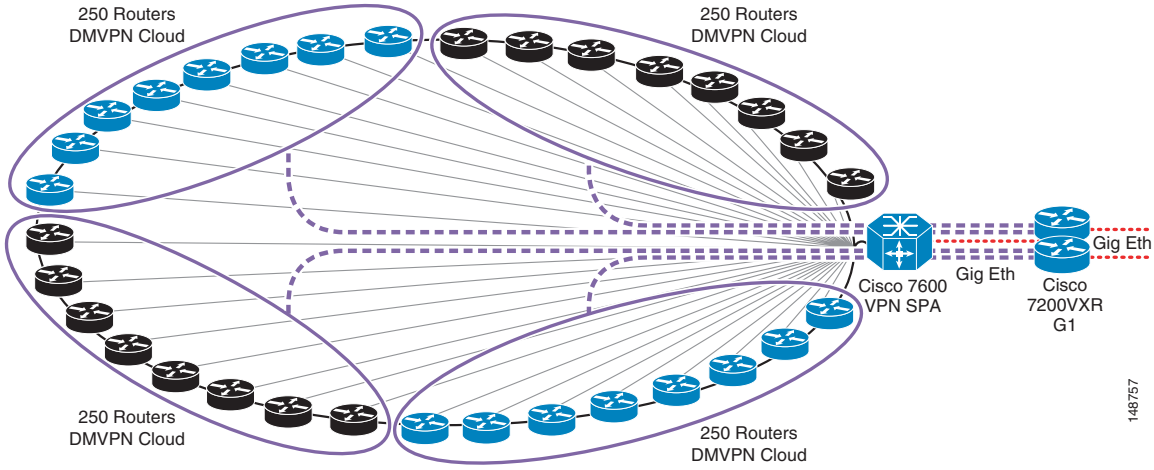
IPsec technologies that support IPmc, p2p GRE over IPsec, DMVPN hub-and-spoke (mGRE), and VTI, all share one common characteristic: the IPmc replication is hub-to-spoke. When DMVPN is configured for spoke-to-spoke, the IP unicast routing protocol is hub-to-spoke only. IP PIM relies on the IP unicast routing protocol to make IPmc forwarding decisions, IPmc is therefore supported only from hub-to-spoke, never spoke-to-spoke.

Because of the hub-to-spoke, one-to-many requirement, the hub router must incur considerable additional overhead with the data plane or packet replication function. If the application is an IPmc file transfer and all spokes have active receivers, the headend router must replicate each received packet corresponding to the number of spokes. Assuming a topology of 1000 branch routers, this replication ratio is 1:1000. This CPU load on top of the CPU resources consumed by IPsec encryption can present a challenge to the network manager in adequately scaling IPsec-encrypted IPmc for large numbers of spokes.

Topology

This topology is chosen to provide scale test results for a 1000 branch (spoke) deployment, as shown in Figure 5.

Figure 5 Performance Testing Topology Overview



To facilitate a high degree of scalability, the encryption process has been separated from the IPmc replication, tunnel termination, and IGP routing protocol processes. This design is applicable to a Dual Tier Headend Architecture DMVPN hub-and-spoke topology design, and a p2p GRE with dynamic crypto map.

Note DVTI is not currently supported on the Cisco Catalyst 6500 or Cisco 7600 platform. This design is not applicable to a DVTI deployment. However, it is applicable to a p2p GRE over IPsec with dynamic crypto maps.

There are two Cisco 7200VXR routers, each with two mGRE interfaces. Each mGRE interface has 250 neighbors.

The Cisco 7600 router with the VPN SPA is configured using dynamic crypto maps and provides bulk encryption and decryption of mGRE-encapsulated IP unicast packets. This crypto device need not be aware that the enterprise network is IPmc enabled.

Traffic Profile

The traffic profile is the same profile as used for all branch V3PN testing. It includes both TCP and UDP data, and G.729 VoIP and IPmc packets. The voice latency, drops, and jitter are used as a testing control to determine whether the network performance is suitable for customer deployment. Rarely are voice drops an issue in this type of testing environment. One-way latency in this lab environment is expected to average at or below 50 ms; jitter less than or equal to 8 ms is ideal.

For more information on the traffic profile and test tools, see *Voice and Video Enabled IPsec VPN (V3PN) Design Guide* at the following URL: http://www.cisco.com/go/srnd.

The performance test results are shown in Table 1. Three tests are reported. The first test, labeled “IP unicast”, is a baseline with no IPmc. In this baseline, the 1000 branches have over 4000 G.729 voice calls active, plus the data packets per second and bits per second as listed in the table.

Table 1 Performance Test Results

mGRE	G.729 Calls	VoIP Kpps	VoIP Mbps	Data Kpps	Data Mbps	Average Jitter/Delay
IP unicast	4140	414	523	187	723	8 ms 16 ms
IP unicast 1 IPmc	4140	414	523	73	607	7.8 ms 16 ms
IP unicast 3 IPmc	3237	324	409	98	707	8.7 ms 17 ms

The second test, “IP unicast 1 IPmc”, is the same traffic profile with the addition of an IPmc stream to each of the 1000 branches in the topology. The number of VoIP calls remained the same, and although the reported data packets per second and bits per second were less, the IPmc packets consumed some of the available bandwidth.

The third test, “IP unicast 3 IPmc”, had a reduction in the number of voice calls that can be supported, because there are now three concurrent IPmc streams to each of the 1000 branches. Also be aware that the CPU busy of the Cisco 7200VXR routers in this test averaged 93 percent during the test. This CPU busy level is considered too high for an acceptable deployment recommendation. The voice jitter also exceeded the target of less than or equal to 8 ms. Therefore, the third test is considered to approach an unacceptable level of performance.

Voice drops are 0 percent in all tests, and VoIP packet loss is therefore not a factor.

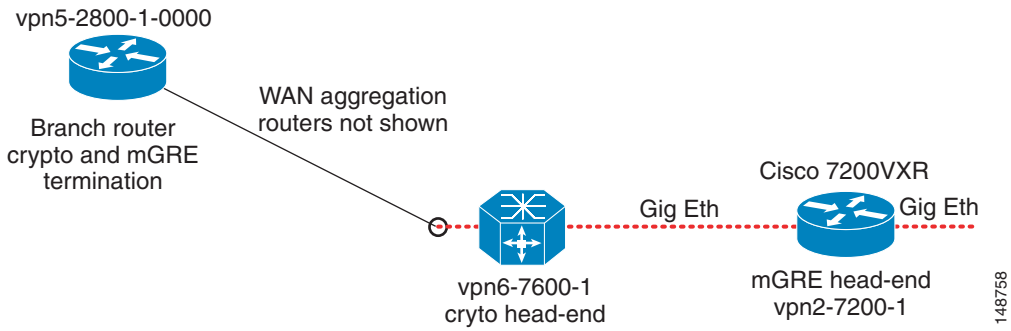
Configurations

Although the test topology comprises over 1000 routers, the configuration concepts can be shown with three routers in the topology: one branch router, the crypto headend router, and one mGRE headend router. For purposes of headend redundancy, the branch router should have two tunnels. One tunnel should have a path through one crypto headend and mGRE headend router, and the second tunnel should be serviced by a second crypto headend chassis and mGRE headend.

Sample Configuration Topology

The three configuration examples relate to the topology diagram shown in Figure 6.

Figure 6 Configuration Concept Topology



Branch Router

The branch router terminates the mGRE tunnel interface from the headend Cisco 7200VXR router (mGRE headend), and terminates an IPsec tunnel to the headend Cisco 7600 (crypto headend) router. There are 250 branch routers in each DMVPN cloud.

Note that the EIGRP hold-time is increased from the default value of 15 seconds to 35 seconds. This increases the time to select an alternate path in the event of a service disruption.

The tunnel interface configuration does not include **tunnel mode gre multipoint** on the branch router, although it is included on the headend mGRE router. This configuration is therefore solely a hub-to-spoke deployment.

```
!
hostname vpn5-2800-1-0000
!
ip multicast-routing
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.241.1
crypto isakmp keepalive 10
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto map static-map local-address Serial0/0/0
crypto map static-map 10 ipsec-isakmp
!
!                            Peer 192.168.241.1 is Vlan 100 of vpn6-7600-1
 set peer 192.168.241.1
 set transform-set vpn-test
 match address b000
!
interface Tunnel0
 description Tunnel0 => to vpn2-7200-1 Tunnel 0
 bandwidth 512
 ip address 10.56.1.0 255.255.252.0
 ip hold-time eigrp 1 35
 ip pim sparse-mode
 ip nhrp authentication test
 ip nhrp map 10.56.0.1 192.168.161.1
 ip nhrp map multicast 192.168.161.1
 ip nhrp network-id 105600
 ip nhrp holdtime 1800
 ip nhrp nhs 10.56.0.1
 ip nhrp registration timeout 120
 ip summary-address eigrp 1 10.60.0.0 255.255.255.0 5
 load-interval 30
 tunnel source 192.168.0.2
 tunnel destination 192.168.161.1
 tunnel key 105600
!
interface Loopback0
 description Loopback0
 ip address 10.60.0.254 255.255.255.255
 ip pim sparse-mode
 ip igmp join-group 224.2.51.79
!
interface Serial0/0/0
 description Serial0/0/0
```

```
 bandwidth 512
 ip address 192.168.0.2 255.255.255.252
 service-policy output 512kb-shaper
 load-interval 30
 tx-ring-limit 1
 tx-queue-limit 1
 crypto map static-map
!
router eigrp 1
 passive-interface FastEthernet0/1
 network 10.0.0.0
 no auto-summary
 eigrp stub connected summary
!
ip pim bidir-enable
ip pim autorp listener
!
ip access-list extended b000
!                            The crypto ACL matches the tunnel destination address
 permit gre host 192.168.0.2 host 192.168.161.1
!
end
```

mGRE Headend Router

The mGRE headend router terminates the mGRE tunnels from two DMVPN clouds. Each cloud consists of 250 branch routers. There are two mGRE headend routers; however, only the configuration from one is shown. The CPU resources on this router are consumed by IPmc replication, IGP outing protocol hellos and updates, and switching IP unicast packets.

This router does not decrypt the IPsec packets; that is the function of the Cisco 7600 crypto headend with the VPN SPA.

Note that the EIGRP hold-time is increased from the default value of 15 seconds to 35 seconds. This increases the time to select an alternate path in the event of a service disruption.

```
!
hostname vpn2-7200-1
!
boot-start-marker
boot system flash disk0:c7200-ik9o3s-mz.123-11.T2
boot-end-marker
!
ip multicast-routing
!
interface Tunnel0
 description Tunnel0
 bandwidth 100000
 ip address 10.56.0.1 255.255.252.0
 no ip redirects
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 1800
 ip nhrp registration timeout 120
 no ip split-horizon eigrp 1
 load-interval 30
 tunnel source 192.168.161.1
```

```
 tunnel mode gre multipoint
 tunnel key 105600
!
interface Tunnel1
 description Tunnel1
 bandwidth 100000
 ip address 10.56.16.1 255.255.252.0
 no ip redirects
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 1056160
 ip nhrp holdtime 1800
 ip nhrp registration timeout 120
 no ip split-horizon eigrp 1
 load-interval 30
 tunnel source 192.168.181.1
 tunnel mode gre multipoint
 tunnel key 1056160
!
interface GigabitEthernet0/1
 description Outside => to vpn6-7600-1 GigabitEthernet5/1
 ip address 192.168.181.1 255.255.255.0 secondary
 ip address 192.168.161.1 255.255.255.0
!
interface GigabitEthernet0/2
 description Inside
 ip address 10.57.1.1 255.255.255.0
 ip pim sparse-mode
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
!
ip pim autorp listener
!
end
```

Crypto Headend Router

This router decrypts packets from all 1000 branch routers in the topology and forwards the plain text mGRE packets to the mGRE headend routers. Regardless of the content of the packet encapsulated in the mGRE packet, this router encounters only unicast packets. The packets arriving on the outside interface are ESP and ISAKMP packets from the branch routers, and when successfully decrypted, are IP unicast packets to one of the two mGRE headend routers.

```
!
hostname vpn6-7600-1
!
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.throttle3
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
```

```
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
!
!
crypto map dynamic-map local-address Vlan100
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!
!
interface GigabitEthernet3/1
 description GigabitEthernet3/1 Outside Interface
 no ip address
 load-interval 30
 crypto connect vlan 100
!
!
interface GigabitEthernet5/1
 description GigabitEthernet5/1 to vpn2-7200-1 GE0/1
 ip address 192.168.181.2 255.255.255.0 secondary
 ip address 192.168.161.2 255.255.255.0
 no ip redirects
 load-interval 30
!
interface GigabitEthernet5/2
 description GigabitEthernet5/2 to vpn2-7200-2 GE0/1
 ip address 192.168.191.2 255.255.255.0 secondary
 ip address 192.168.171.2 255.255.255.0
 no ip redirects
 load-interval 30
!
interface Vlan100
 description Vlan100
 ip address 192.168.241.1 255.255.255.0
 load-interval 30
 no mop enabled
 crypto map dynamic-map
 crypto engine subslot 4/0
!
end
```

Summary

With the wider adoption of IPsec VPNs, enterprise customers who have previously implemented IPmc in the unencrypted portions of their network seek to extend this capability to the encrypted WAN.

IPmc has been a feature in Cisco IOS for many years, and often the network manager assumes that two features that work independently will merge seamlessly and scale infinitely.

Evidence of this is apparent in an excerpt from a press release from the Cisco news release entitled "Cisco Multicast VPN Technology Helps NTT Communications Deliver Video Services; Japanese Service Provider Reduces Cost, Simplifies Management of Network", news@cisco, March 23, 2005:

"Cisco IP multicast is a mature technology that has been included in the Cisco IOS Software since version 10.0, making it possible to support multicast VPN without adding any new functions to the core routing device."

Some of the issues that have been documented in this design guide demonstrate that IPmc presents issues in both headend scaling and also switching path support on branch routers that need to be better understood before large-scale implementations.

Appendix A—Output of debug ip pim

```
vpn-jk2-1711-vpn#debug ip pim

Mar 18 16:30:07.310 est: PIM(0): Building Periodic Join/Prune message for 224.1.1.20
Mar 18 16:30:07.710 est: PIM(0): Send v2 Data-header Register to 10.81.7.219 for
10.81.7.227, group 224.1.1.20
Mar 18 16:30:07.822 est: PIM(0): Received v2 Register-Stop on Tunnel0 from 10.81.7.219
Mar 18 16:30:07.822 est: PIM(0):   for source 10.81.7.227, group 224.1.1.20
Mar 18 16:30:07.822 est: PIM(0): Clear register flag to 10.81.7.219 for (10.81.7.227/32,
224.1.1.20)
Mar 18 16:30:13.986 est: PIM(0): Received v2 Join/Prune on Tunnel0 from 10.81.7.188, to us
Mar 18 16:30:13.986 est: PIM(0): Join-list: (10.81.7.227/32, 224.1.1.20), S-bit set
Mar 18 16:30:13.986 est: PIM(0): Update Tunnel0/10.81.7.188 to (10.81.7.227, 224.1.1.20),
Forward state, by PIM SG Join
```

In the above example, 10.81.7.219 is the IP address of the RP. This address is shown in the configuration for the primary RP later in this section. That IP address is of FastEthernet0/0 router "multicast-RP". The IP unicast address of the sending camera is 10.81.7.227 and the configured group number is 224.1.1.20. The IP PIM neighbor on interface Tunnel0 is 10.81.7.188.

Appendix B—Output from Last Hop Router *rtp9-ese-test*

The workstation PENGUIN_3 is on the FastEthernet0/0 interface of this router and is viewing CAMERA_1 (group address 224.1.1.20, IP unicast address 10.81.7.227) and CAMERA_2 (group address 224.1.1.21, IP unicast address 10.59.138.21).

```
rtp9-ese-test#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
224.1.1.20       FastEthernet0/0          00:55:46  00:02:21  10.81.7.234
224.1.1.21       FastEthernet0/0          06:15:35  00:02:19  10.81.7.234
224.0.1.40       FastEthernet0/0          3d06h     00:02:15  10.81.7.233
239.255.255.250  FastEthernet0/0          06:17:21  00:02:17  10.81.7.234

rtp9-ese-test#debug ip pim
PIM debugging is on
Mar 18 16:33:36.164 est: PIM(0): Building Join/Prune packet for nbr 10.81.7.186
Mar 18 16:33:36.164 est: PIM(0): Adding v2 (10.81.7.219/32, 224.0.1.39) Prune
Mar 18 16:33:36.164 est: PIM(0): Send v2 join/prune to 10.81.7.186 (Tunnel0)
Mar 18 16:34:01.296 est: PIM(0): Building Periodic Join/Prune message for 224.1.1.21
Mar 18 16:34:01.296 est: PIM(0): Insert (*,224.1.1.21) join in nbr 10.81.7.186's queue
Mar 18 16:34:01.296 est: PIM(0): Insert (10.59.138.21,224.1.1.21) join in nbr
10.81.7.186's queue
Mar 18 16:34:01.296 est: PIM(0): Building Join/Prune packet for nbr 10.81.7.186
Mar 18 16:34:01.296 est: PIM(0): Adding v2 (10.81.7.219/32, 224.1.1.21), WC-bit, RPT-bit,
S-bit Join
Mar 18 16:34:01.296 est: PIM(0): Adding v2 (10.59.138.21/32, 224.1.1.21), S-bit Join
Mar 18 16:34:01.300 est: PIM(0): Send v2 join/prune to 10.81.7.186 (Tunnel0)
Mar 18 16:34:28.728 est: PIM(0): Building Periodic Join/Prune message for 224.1.1.20
Mar 18 16:34:28.728 est: PIM(0): Insert (*,224.1.1.20) join in nbr 10.81.7.186's queue
Mar 18 16:34:28.728 est: PIM(0): Insert (10.81.7.227,224.1.1.20) join in nbr 10.81.7.186's
queue
Mar 18 16:34:28.728 est: PIM(0): Building Join/Prune packet for nbr 10.81.7.186
Mar 18 16:34:28.728 est: PIM(0): Adding v2 (10.81.7.219/32, 224.1.1.20), WC-bit, RPT-bit,
S-bit Join
Mar 18 16:34:28.728 est: PIM(0): Adding v2 (10.81.7.227/32, 224.1.1.20), S-bit Join
Mar 18 16:34:28.732 est: PIM(0): Send v2 join/prune to 10.81.7.186 (Tunnel0)
Mar 18 16:34:47.297 est: PIM(0): Received RP-Reachable on Tunnel0 from 10.81.7.219
```

```
Mar 18 16:34:47.297 est: PIM(0): Received RP-Reachable on Tunnel0 from 10.81.7.219
Mar 18 16:34:47.297 est:      for group 224.1.1.21
Mar 18 16:34:47.297 est: PIM(0): Update RP expiration timer (270 sec) for 224.1.1.21
Mar 18 16:34:48.909 est: PIM(0): Received RP-Reachable on Tunnel0 from 10.81.7.219
Mar 18 16:34:48.909 est: PIM(0): Received RP-Reachable on Tunnel0 from 10.81.7.219
Mar 18 16:34:48.909 est:      for group 224.1.1.20
```

Appendix C—IPmc and Dynamic VTI

Each branch router is accessible by way of a point-to-point interface, which is the virtual access interface that is spawned from the virtual template.

```
rtp5-esevpn-gw3#show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
10.59.136.14      Virtual-Access3          3w5d/00:01:16     v2    1 / S
10.81.7.161       Virtual-Access6          2w6d/00:01:31     v2    1 / S
10.81.7.33        Virtual-Access2          1w0d/00:01:19     v2    1 / S
10.81.7.1         Virtual-Access8          1d08h/00:01:24    v2    1 / S
10.81.7.201       Virtual-Access13         01:52:47/00:01:17 v2    1 / S
10.81.7.169       Virtual-Access9          16:03:26/00:01:33 v2    1 / S
10.81.7.9         Virtual-Access4          00:00:02/00:01:42 v2    1 / S
10.81.7.145       Virtual-Access12         11:51:46/00:01:33 v2    1 / S
10.81.7.113       Virtual-Access5          01:58:16/00:01:38 v2    1 / S
```