



# Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links

---

**First Published: August 14, 2006**

**Last Updated: July 31, 2006**

This module documents an Optimized Edge Routing (OER) solution that describes how to configure IP security (IPsec)/Generic Routing Encapsulation (GRE) tunnel interfaces as OER-managed exit links. The VPN IPsec/GRE Tunnel Optimization solution was introduced in Cisco IOS Release 12.3(11)T, and only network-based IPsec Virtual Private Networks (VPNs) are supported.

OER provides automatic route optimization and load distribution for multiple connections between networks. OER is an integrated Cisco IOS solution that allows you to monitor IP traffic flows and then define policies and rules based on prefix performance, link load distribution, link bandwidth monetary cost, and traffic type. OER provides active and passive monitoring systems, dynamic failure detection, and automatic path correction. Deploying OER enables intelligent load distribution and optimal route selection in an enterprise network.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links”](#) section on page 20.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



---

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

© 2006–2009 Cisco Systems, Inc. All rights reserved.

# Contents

- [Prerequisites for Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links, page 2](#)
- [Restrictions for Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links, page 2](#)
- [Information About Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links, page 3](#)
- [How to Configure VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links, page 4](#)
- [Configuration Examples for Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links, page 10](#)
- [Where to Go Next, page 18](#)
- [Additional References, page 18](#)
- [Feature Information for Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links, page 20](#)

## Prerequisites for Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links

- Before implementing VPN IPsec/GRE tunnel interfaces as OER-managed exit links you need to understand how to configure a basic OER-managed network. See the [“Cisco IOS Optimized Edge Routing Overview”](#) and [“Setting Up OER Network components”](#) modules for more details. For a list of other OER configuration modules, see the [“Where to Go Next” section on page 18](#) and the [“Related Documents” section on page 18](#).
- Cisco Express Forwarding (CEF) must be enabled on all participating routers.
- Routing protocol peering or static routing is configured in the OER-managed network.
- Standard Cisco OER border router and master controller configurations are completed.

## Restrictions for Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links

Cisco IOS OER supports the optimization of prefixes that are routed over IPsec/GRE tunnel interfaces. Only GRE and multipoint GRE VPN tunnels are supported.

# Information About Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links

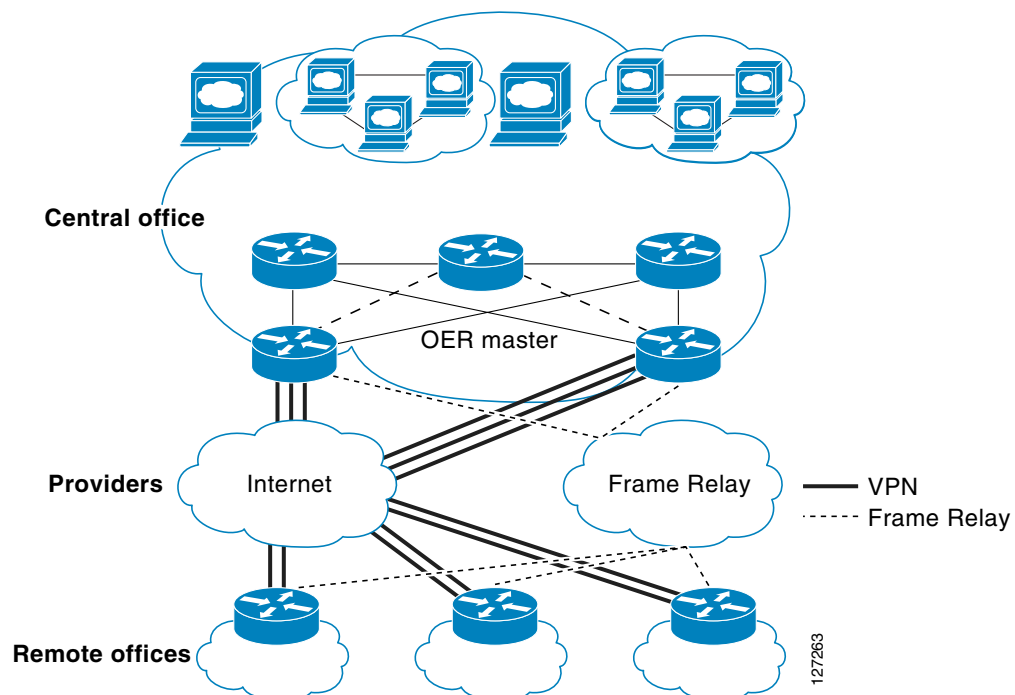
To configure VPN IPsec/GRE tunnel interfaces as OER-managed exit links you should understand the following concepts:

- [VPN IPsec/GRE Tunnel Interface Optimization, page 3](#)
- [Protection of Route Prefixes with IPsec over GRE Tunnels, page 4](#)

## VPN IPsec/GRE Tunnel Interface Optimization

Cisco IOS OER supports the optimization of prefixes that are routed over IPsec/GRE tunnel interfaces. The VPN tunnel interface is configured as OER external interfaces on the master controller. [Figure 1](#) shows an OER-managed network that is configured to optimize VPN traffic. Cisco IOS OER is deployed at the central office and remote offices.

**Figure 1** Cisco IOS OER Network Optimized for VPN Routing



This enhancement allows you to configure two-way VPN optimization. A master controller and border router process are enabled on each side of the VPN. Each site maintains a separate master controller database. VPN routes can be dynamically learned through the tunnel interfaces or can be configured. Prefix and exit link policies are configured for VPN prefixes through a standard Cisco IOS OER configuration.

## Protection of Route Prefixes with IPsec over GRE Tunnels

The IPsec-to-GRE model allows a service provider to provide VPN services over the IP backbone. Both the central and remote VPN clients terminate according to the IPsec-to-IPsec model. Prefixes are encapsulated using GRE tunnels. The GRE packet is protected by IPsec. The encapsulated prefixes are forwarded from the central VPN site to a customer headend router that is the other endpoint for GRE. The IPsec-protected GRE packets provide secure connectivity across the IP backbone of the service provider network.

For more information about configuring IPsec over GRE tunnels, see the *Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs)* document published at the following URL:

[http://www.cisco.com/en/US/tech/tk583/tk372/technologies\\_white\\_paper09186a008018983e.shtml](http://www.cisco.com/en/US/tech/tk583/tk372/technologies_white_paper09186a008018983e.shtml)

## How to Configure VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links

This section contains the following task:

- [Configuring OER to Monitor and Control IPsec VPN Prefixes over GRE Tunnels, page 4](#)

## Configuring OER to Monitor and Control IPsec VPN Prefixes over GRE Tunnels

Perform this task to configure the IPsec VPN configuration over GRE tunnels. Initially the IPsec VPN is configured on a border router, and the tunnel interface is configured as an OER-managed external interface on the master controller. In this task an IKE policy is defined, a transform set is configured, a crypto profile and a crypto map are defined, and a GRE tunnel is configured.

The GRE tunnel and IPsec protection in this task are configured on the border router. The configuration steps in this task show how to configure a single tunnel. At least two tunnels must be configured on border routers in an OER-managed network. The IPsec configuration must be applied at each tunnel endpoint (the central and remote site).

## Configuration of GRE Tunnel Interfaces As OER-Managed Exit Links

GRE tunnel interfaces on the border routers are configured as OER external interfaces on the master controller. At least two external tunnel interfaces must be configured on separate physical interfaces in an OER-managed network. These interfaces can be configured on a single border router or multiple border routers. Internal interfaces are configured normally using a physical interface that is on the border router and is reachable by the master controller.

## Restrictions

Cisco IOS OER supports only IPsec/GRE VPNs. No other VPN types are supported.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto ipsec security-association lifetime** {seconds *seconds* | kilobytes *kilobytes*}
4. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
5. **mode** [tunnel | transport]
6. **exit**
7. **crypto map** *map-name seq-num* [ipsec-isakmp]
8. **set peer** {*host-name* [dynamic] [default] | *ip-address* [default]}
9. **set transform-set** *transform-set-name* [*transform-set-name2*...*transform-set-name6*]
10. **match address** [*access-list-id* | *name*]
11. **exit**
12. **crypto ipsec profile** *name*
13. **set transform-set** *transform-set-name* [*transform-set-name2*...*transform-set-name6*]
14. **exit**
15. **crypto map** *map-name local-address interface-id*
16. **crypto isakmp key** *encryption-level key-string* {address *peer-address* [*mask*] | hostname *name*} [no-xauth]
17. **crypto isakmp keepalive** *seconds* [*retries*] [periodic | on-demand]
18. **crypto isakmp policy** *priority*
19. **encryption** {des | 3des | aes | aes 192 | aes 256}
20. **authentication** {rsa-sig | rsa-encr | pre-share}
21. **exit**
22. **interface** *type number* [*name-tag*]
23. **ip address** *ip-address mask* [secondary]
24. **crypto map** *map-name* [redundancy *standby-name*]
25. **exit**
26. **interface** *type number* [*name-tag*]
27. **ip address** *ip-address mask* [secondary]
28. **keepalive** [*period* [*retries*]]
29. **bandwidth** {*kbits* | inherit [*kbits*]}
30. **tunnel mode gre ip**
31. **tunnel source** {*ip-address* | *interface-type interface-number*}
32. **tunnel destination** {*host-name* | *ip-address*}
33. **tunnel protection ipsec profile** *name* [shared]
34. **exit**
35. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [dhcp] [*distance*] [*name*] [permanent] [tag *tag*]

36. **access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
37. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto ipsec security-association lifetime</b> { <b>seconds</b> <i>seconds</i>   <b>kilobytes</b> <i>kilobytes</i> }  <b>Example:</b> Router(config)# crypto ipsec security-association lifetime kilobytes 530000000	Sets global lifetime values used when negotiating IPsec security associations. <ul style="list-style-type: none"> <li>The example sets volume of traffic, in kilobytes, that can pass between IPsec peers for this security association.</li> </ul>
Step 4	<b>crypto ipsec transform-set</b> <i>transform-set-name transform1</i> [ <i>transform2</i> ] [ <i>transform3</i> ] [ <i>transform4</i> ]  <b>Example:</b> Router(config)# crypto ipsec transform-set VPN_1 esp-des esp-3des esp-sha-hmac	Enters crypto transform configuration mode to create or modify a transform set—an acceptable combination of security protocols and algorithms. <ul style="list-style-type: none"> <li>The example specifies 56-bit Data Encryption Standard (DES), 168-bit DES, or Secure Hash Algorithm (SHA) for authentication.</li> </ul>
Step 5	<b>mode</b> [ <b>tunnel</b>   <b>transport</b> ]  <b>Example:</b> Router(cfg-crypto-trans)# mode transport	Sets the mode for the transform set. <ul style="list-style-type: none"> <li>The example sets the mode to transport. The default mode is tunnel. Under tunnel mode, the entire packet is protected. Under transport mode, only the payload is protected. Encapsulation is performed by GRE.</li> </ul>
Step 6	<b>exit</b>  <b>Example:</b> Router(cfg-crypto-trans)# exit	Exits crypto transform configuration mode and enters global configuration mode.
Step 7	<b>crypto map</b> <i>map-name seq-num</i> [ <b>ipsec-isakmp</b> ]  <b>Example:</b> Router(config)# crypto map TUNNEL 10 ipsec-isakmp	Enters crypto map configuration mode to create or modify a crypto map. <ul style="list-style-type: none"> <li>The example creates a crypto map named TUNNEL and configures IKE to establish the security association.</li> </ul>

	Command or Action	Purpose
Step 8	<pre>set peer {host-name [dynamic] [default]   ip-address [default]}</pre> <p><b>Example:</b> Router(config-crypto-map)# set peer 10.4.9.81</p>	Specifies the IPsec peer in the crypto map entry.
Step 9	<pre>set transform-set transform-set-name [transform-set-name2...transform-set-name6]</pre> <p><b>Example:</b> Router(config-crypto-map)# set transform-set VPN_1</p>	Specifies which transform sets can be used with the crypto map entry. <ul style="list-style-type: none"> <li>Specifies the transform set VPN_1, which was configured in <a href="#">Step 4</a>.</li> </ul>
Step 10	<pre>match address [access-list-id   name]</pre> <p><b>Example:</b> Router(config-crypto-map)# match address 100</p>	Specifies an extended access list to define IPsec peers for the crypto map entry. <ul style="list-style-type: none"> <li>The access list is defined in <a href="#">Step 36</a>.</li> </ul>
Step 11	<pre>exit</pre> <p><b>Example:</b> Router(config-crypto-map)# exit</p>	Exits crypto map configuration mode and enters global configuration mode.
Step 12	<pre>crypto ipsec profile name</pre> <p><b>Example:</b> Router(config)# crypto ipsec profile OER</p>	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and enters IPsec profile configuration mode. <ul style="list-style-type: none"> <li>The example creates a profile named OER.</li> </ul>
Step 13	<pre>set transform-set transform-set-name [transform-set-name2...transform-set-name6]</pre> <p><b>Example:</b> Router(ipsec-profile)# set transform-set VPN_1</p>	Specifies which transform sets can be used with the crypto map entry. <ul style="list-style-type: none"> <li>Specifies the transform set VPN_1, which was configured in <a href="#">Step 4</a>.</li> </ul>
Step 14	<pre>exit</pre> <p><b>Example:</b> Router(ipsec-profile)# exit</p>	Exits IPsec profile configuration mode and enters global configuration mode.
Step 15	<pre>crypto map map-name local-address interface-id</pre> <p><b>Example:</b> Router(config)# crypto map TUNNEL local-address FastEthernet 0/0</p>	Attaches a defined crypto map to the specified interface. <ul style="list-style-type: none"> <li>The example attaches the crypto map named TUNNEL to interface FastEthernet 0/0.</li> </ul>
Step 16	<pre>crypto isakmp key encryption-level key-string {address peer-address [mask]   hostname name} [no-xauth]</pre> <p><b>Example:</b> Router(config)# crypto isakmp key 0 CISCO address 10.4.9.81 no-xauth</p>	Creates the preshared authentication key. <ul style="list-style-type: none"> <li>The example configures encryption level 0 and configures the router to not prompt the IPsec peer for extended authentication. However, any encryption level or authentication level can be specified.</li> </ul>

	Command or Action	Purpose
Step 17	<b>crypto isakmp keepalive</b> <i>seconds</i> [ <i>retries</i> ] [ <i>periodic</i>   <i>on-demand</i> ]  <b>Example:</b> Router(config)# crypto isakmp keepalive 10	Allows the gateway to send dead peer detection (DPD) messages to the peer.
Step 18	<b>crypto isakmp policy</b> <i>priority</i>  <b>Example:</b> Router(config)# crypto isakmp policy 1	Defines an Internet Key Exchange (IKE) policy and enters ISAKMP policy configuration mode.
Step 19	<b>encryption</b> { <i>des</i>   <i>3des</i>   <i>aes</i>   <i>aes 192</i>   <i>aes 256</i> }  <b>Example:</b> Router(config-isakmp)# encryption 3des	Specifies the encryption algorithm within the IKE policy. <ul style="list-style-type: none"> <li>The example specifies 168-bit DES encryption.</li> </ul>
Step 20	<b>authentication</b> { <i>rsa-sig</i>   <i>rsa-encr</i>   <i>pre-share</i> }  <b>Example:</b> Router(config-isakmp)# authentication pre-share	Specifies the authentication method within the IKE policy. <ul style="list-style-type: none"> <li>The example specifies that a preshared key will be used.</li> </ul>
Step 21	<b>exit</b>  <b>Example:</b> Router(config-isakmp)# exit	Exits ISAKMP policy configuration mode and enters global configuration mode.
Step 22	<b>interface</b> <i>type number</i> [ <i>name-tag</i> ]  <b>Example:</b> Router(config)# interface FastEthernet0/0	Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>The physical interface is defined in this step.</li> </ul>
Step 23	<b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]  <b>Example:</b> Router(config-if)# ip address 10.4.9.14 255.255.255.0	Sets a primary or secondary IP address for an interface.
Step 24	<b>crypto map</b> <i>map-name</i> [ <b>redundancy</b> <i>standby-name</i> ]  <b>Example:</b> Router(config-if)# crypto map TUNNEL	Applies the crypto map set to the interface. <ul style="list-style-type: none"> <li>The example specifies the crypto map named TUNNEL, which was defined in <a href="#">Step 7</a>.</li> </ul>
Step 25	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits interface configuration mode and enters global configuration mode.
Step 26	<b>interface</b> <i>type number</i> [ <i>name-tag</i> ]  <b>Example:</b> Router(config)# interface Tunnel0	Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>The tunnel interface is defined in this step.</li> </ul>

	Command or Action	Purpose
Step 27	<p><b>ip address</b> <i>ip-address mask</i> [<b>secondary</b>]</p> <p><b>Example:</b> Router(config-if) ip address 10.100.2.1 255.255.0.0</p>	Sets a primary or secondary IP address for an interface.
Step 28	<p><b>keepalive</b> [<i>period</i> [<i>retries</i>]]</p> <p><b>Example:</b> Router(config-if) keepalive 30 5</p>	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface or before bringing the tunnel protocol down for a specific interface.
Step 29	<p><b>bandwidth</b> {<i>kbps</i>   <b>inherit</b> [<i>kbps</i>]}</p> <p><b>Example:</b> Router(config-if)# bandwidth 500  Router(config-if)# bandwidth inherit</p>	Sets and communicates the current bandwidth value for an interface to higher-level protocols.
Step 30	<p><b>tunnel mode gre ip</b></p> <p><b>Example:</b> Router(config-if)# tunnel mode gre ip</p>	<p>Sets the encapsulation mode for the tunnel interface.</p> <p><b>Note</b> Only partial syntax is shown here. For more details, see the <a href="#">Cisco IOS Interface and Hardware Component Command Reference</a>, 12.4T.</p>
Step 31	<p><b>tunnel source</b> {<i>ip-address</i>   <i>interface-type interface-number</i>}</p> <p><b>Example:</b> Router(config-if)# tunnel source 10.4.9.14</p>	<p>Sets the source address for a tunnel interface.</p> <ul style="list-style-type: none"> <li>The source interface in the example was defined in <a href="#">Step 22</a>. The interface name or IP address can be specified.</li> </ul>
Step 32	<p><b>tunnel destination</b> {<i>host-name</i>   <i>ip-address</i>}</p> <p><b>Example:</b> Router(config-if)# tunnel destination 10.4.9.81</p>	<p>Specifies the destination for a tunnel interface.</p> <ul style="list-style-type: none"> <li>The IP address of the physical interface where the remote tunnel end point is attached is configured in this step.</li> </ul>
Step 33	<p><b>tunnel protection ipsec profile</b> <i>name</i> [<b>shared</b>]</p> <p><b>Example:</b> Router(config-if)# tunnel protection ipsec profile OER</p>	<p>Associates the tunnel interface with the IPsec profile.</p> <ul style="list-style-type: none"> <li>The IPsec profile named OER that is configured in the example was defined in Step 19.</li> </ul>
Step 34	<p><b>exit</b></p> <p><b>Example:</b> Router(config-if)# exit</p>	Exits interface configuration mode and enters global configuration mode.
Step 35	<p><b>ip route</b> <i>prefix mask</i> [<i>ip-address</i>   <i>interface-type interface-number</i> [<i>ip-address</i>]] [<b>dhcp</b>] [<i>distance</i>] [<i>name</i>] [<b>permanent</b>] [<b>tag</b> <i>tag</i>]</p> <p><b>Example:</b> Router(config)# ip route 10.2.2.2 255.255.255.255 Tunnel0</p>	<p>Establishes a static route.</p> <ul style="list-style-type: none"> <li>A default route is configured for the tunnel destination host or network.</li> </ul>

	Command or Action	Purpose
Step 36	<pre>access-list access-list-number [<b>dynamic</b> dynamic-name [timeout minutes]] {deny   permit} protocol source source-wildcard destination destination-wildcard [<b>precedence</b> precedence] [<b>tos</b> tos] [<b>log</b>   <b>log-input</b>] [<b>time-range</b> time-range-name] [<b>fragments</b>]</pre> <p><b>Example:</b> Router(config)# access-list 100 permit gre host 10.4.9.14 host 10.4.9.81</p>	<p>Creates or configures an extended IP access list.</p> <ul style="list-style-type: none"> <li>An extended access list is defined to permit only the GRE hosts.</li> <li>The access list in this example is referenced in the <b>match address</b> statement in <a href="#">Step 10</a>.</li> </ul>
Step 37	<pre>end</pre> <p><b>Example:</b> Router(config)# end</p>	<p>Exits global configuration mode and enters privileged EXEC mode.</p>

## Configuration Examples for Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links

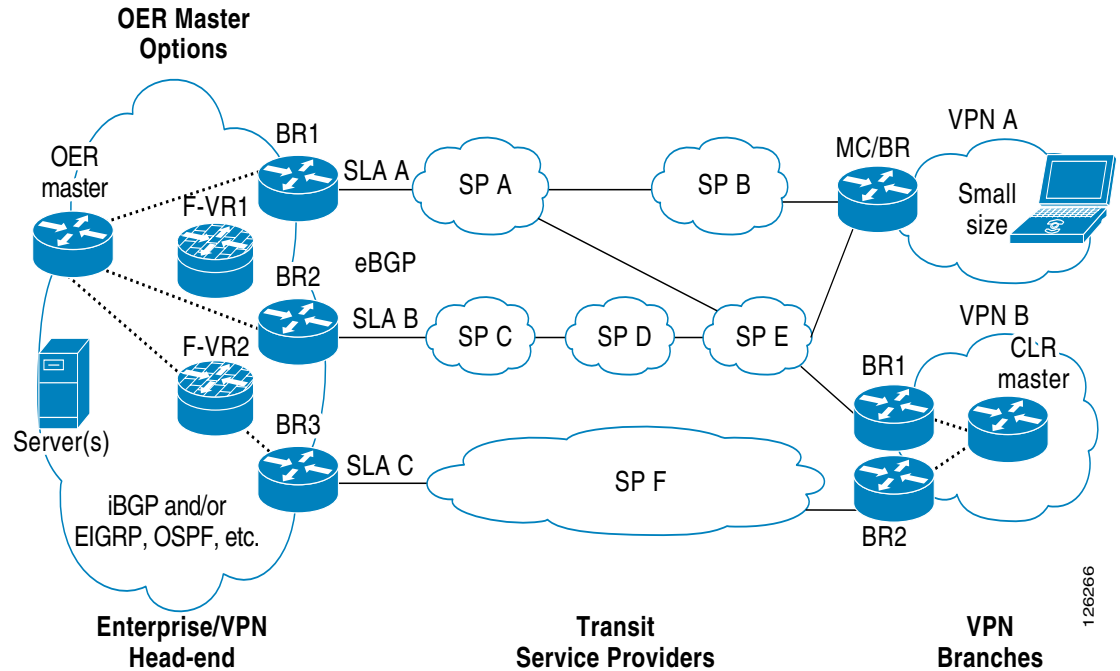
This section contains the following example:

- [Configuring OER to Monitor and Control GRE/IPsec VPN Prefixes: Example, page 10](#)

### Configuring OER to Monitor and Control GRE/IPsec VPN Prefixes: Example

[Figure 2](#) shows a central VPN site and two remote VPN sites. VPN peering is established through the service provider clouds. An OER-managed network is configured at each site where Cisco IOS OER configuration is applied independently. Each site has a separate master controller and border router process, and each site maintains a separate master controller database.

Figure 2 VPN Sites Controlled by OER-Managed Networks



Two GRE tunnels are configured between each remote site and the central site. VPN prefixes are encapsulated in GRE tunnels, which in turn are protected by IPsec encryption. The examples in this section show the configuration for the central VPN site, VPN A, and VPN B.

**Central VPN Configuration: OER Master Controller**

The central VPN site peers with VPN A and VPN B. A separate policy is defined for each site using an OER map. For VPN A prefixes, a delay policy of 80 ms is configured and out-of-policy prefixes are moved to the first in-policy exit. For VPN B prefixes, a delay policy of 40 ms and a relative loss policy are configured, and out-of-policy prefixes are moved to the best available exit.

```
key chain OER
  key 1
    key-string CISCO
  !
oer master
  logging
  border 10.4.9.6 key-chain OER
    interface Ethernet 0/0 external
    interface Ethernet 0/1 internal
  !
  border 10.4.9.7 key-chain OER
    interface Ethernet 0/0 external
    interface Ethernet 0/1 internal
  !
  mode route control
  mode monitor both
  exit
  !
ip prefix VPN A permit 10.4.9.25
oer-map VPNA
  match ip address prefix-list VPNA
  set delay 800
  set mode select-exit good
  exit
```

```

!
ip prefix VPNE permit 10.4.9.254
oer-map VPNE
  match ip address prefix-list VPNE
  set delay 400
  set loss relative 100
  set resolve loss priority 1 variance 10
  set mode select-exit best
end

```

### Central VPN Configuration: BR1

The following example, starting in global configuration mode, shows the central VPN configuration for BR1:

```

key chain OER
  key 1
    key-string CISCO
!
oer border
  local serial 0/1
  master 10.4.9.4 key-chain OER
!
ip route 10.70.1.0 255.255.255.0
!
route-map REDISTRIBUTE_STATIC
  match tag 5000
  set metric -10
  exit
!
router eigrp 1
  network 10.70.0.0 0.0.0.255
  redistribute static route-map REDISTRIBUTE_STATIC
  exit
!
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime second 14400
crypto ipsec transform-set VPN_1 esp-3des esp-sha-hmac
  mode transport
  exit
!
crypto map TUNNEL 10 ipsec-isakmp
  set peer 10.4.9.81
  set transform-set VPN_1
  match address 100
!
crypto ipsec profile OER
  set transform-set VPN_1
  exit
crypto map TUNNEL local-address Ethernet 0/0
!
crypto isakmp key 0 CISCO address 10.4.9.81 no-xauth
crypto isakmp keepalive 10
crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  exit
!
interface Ethernet0/0
  ip address 10.4.9.14 255.255.255.0
  crypto map TUNNEL
  exit
!
interface Tunnel0

```

```

ip address 10.100.2.1 255.255.0.0
keepalive 30 5
bandwidth 500
bandwidth inherit
tunnel mode gre ip
tunnel source 10.4.9.14
tunnel destination 10.4.9.81
tunnel protection ipsec profile OER
exit

```

### Central VPN Configuration: BR2

The following example, starting in global configuration mode, shows the central VPN configuration of BR2:

```

key chain OER
  key 1
    key-string CISCO
  !
oer border
  local Ethernet 0/1
  master 10.4.9.4 key-chain OER
  !
ip route 10.70.1.0 255.255.255.0
!
route-map REDISTRIBUTE_STATIC
  match tag 5000
  set metric -10
  exit
!
router eigrp 1
  network 10.70.0.0 0.0.0.255
  redistribute static route-map REDISTRIBUTE_STATIC
  !
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime second 14400
crypto ipsec transform-set VPN_1 esp-3des esp-sha-hmac
  mode transport
  exit
!
crypto map TUNNEL 10 ipsec-isakmp
  set peer 10.4.9.82
  set transform-set VPN_1
  match address 100
!
crypto ipsec profile OER
  set transform-set VPN_1
  exit
crypto map TUNNEL local-address Ethernet 0/0
!
crypto isakmp key 0 CISCO address 10.4.9.82 no-xauth
crypto isakmp keepalive 10
crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  exit
!
interface Ethernet0/0
  ip address 10.4.9.15 255.255.255.0
  crypto map TUNNEL
  exit
!
interface Tunnel0
  ip address 10.100.2.2 255.255.0.0

```

```

keepalive 30 5
bandwidth 500
bandwidth inherit
tunnel mode gre ip
tunnel source 10.4.9.15
tunnel destination 10.4.9.82
tunnel protection ipsec profile OER
end

```

### Central VPN Configuration: Internal Peers

The following example shows an EIGRP routing process created to establish peering with the border routers and internal peers:

```

router eigrp 1
 network 10.50.1.0 0.0.0.255
 redistribute static route-map REDISTRIBUTE_STATIC
end

```

### VPN A Configuration: MC/BR

The following configuration example, starting in global configuration mode, shows the configuration of VPN A. VPN A is a remote site that is configured for a small office home office (SOHO) client. A single router is deployed. This router peers with service provider B and service provider E. No Interior Gateway Protocol (IGP) is deployed at this network; only a static route is configured to the remote tunnel endpoint at the central site. A delay policy, a loss policy, and optimal exit link selection are configured so that traffic is always routed through the ISP with the lowest delay time and lowest packet loss. A resolve policy is configured to configure loss to have the highest priority. Neither the physical interface configuration nor the router IGP peering configurations are shown in this example.

```

key chain BR1
 key 1
  key-string CISCO
!

```



#### Note

---

The local border router process is enabled. Because the border router and master controller process is enabled on the same router, a loopback interface (192.168.0.1) is configured as the local interface.

---

```

oer border
 local Loopback0
 master 192.168.0.1 key-chain BR1
!
oer master
 learn
 delay
 mode route control
 delay threshold 100
 loss relative 200
 periodic 300
 mode select-exit good
 resolve loss priority 1 variance 20
 resolve delay priority 2 variance 10
!
 border 192.168.0.1 key-chain BR1
  interface Serial0/0 internal
  interface Tunnel0 external
  interface Tunnel0 external
  exit
!
 crypto ipsec security-association lifetime kilobytes 530000000
 crypto ipsec security-association lifetime second 14400
 crypto ipsec transform-set VPN_1 esp-3des esp-sha-hmac

```

```

mode transport
exit
!
crypto map TUNNEL 10 ipsec-isakmp
  set peer 10.4.9.81
  set transform-set VPN_1
  match address 100
!
crypto ipsec profile OER
  set transform-set VPN_1
  exit
crypto map TUNNEL local-address Ethernet 0/0
!
crypto isakmp key 0 CISCO address 10.4.9.81 no-xauth
crypto isakmp keepalive 10
crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  exit
!

interface Ethernet0/0
  ip address 10.4.9.14 255.255.255.0
  crypto map TUNNEL
  exit
!
interface Tunnel0
  ip address 10.100.2.1 255.255.0.0
  keepalive 30 5
  bandwidth 500
  bandwidth inherit
  tunnel mode gre ip
  tunnel source 10.4.9.14
  tunnel destination 10.4.9.81
  tunnel protection ipsec profile OER
  exit
!

```

**Note**

A single tunnel configuration is shown in this example. Two tunnels are required to configure VPN optimization.

**VPN B Configuration: OER Master Controller**

The following example, starting in global configuration mode, shows the master controller configuration in VPN B. Load distribution and route control mode are enabled. Out-of-policy prefixes are configured to be moved to the first in-policy exit.

```

key chain OER
  key 1
    key-string CISCO
!
oer master
  logging
  border 10.4.9.6 key-chain OER
    interface Ethernet 0/0 external
    interface Ethernet 0/1 internal
!
  border 10.4.9.7 key-chain OER
    interface Ethernet 0/0 external
    interface Ethernet 0/1 internal
!
mode route control

```

```

mode select-exit good
max-range utilization
!
learn
  delay
end

```

### VPN B Configuration: BR1

The following example, starting in global configuration mode, shows the VPN B configuration for BR1:

```

key chain OER
  key 1
    key-string CISCO
!
oer border
  local Ethernet 0/1
  master 10.4.9.4 key-chain OER
!
route-map REDISTRIBUTE_STATIC
  match tag 5000
  set metric -10
  exit
!
router rip
  network 10.60.1.0
  redistribute static route-map REDISTRIBUTE_STATIC
  end
!
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime second 14400
crypto ipsec transform-set VPN_1 esp-3des esp-sha-hmac
  mode transport
  exit
!
crypto map TUNNEL 10 ipsec-isakmp
  set peer 10.4.9.82
  set transform-set VPN_1
  match address 100
!
crypto ipsec profile OER
  set transform-set VPN_1
  exit
crypto map TUNNEL local-address Ethernet 0/0
!
crypto isakmp key 0 CISCO address 10.4.9.82 no-xauth
crypto isakmp keepalive 10
crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  exit
!
interface Ethernet0/0
  ip address 10.4.9.15 255.255.255.0
  crypto map TUNNEL
  exit
!
interface Tunnel0
  ip address 10.100.2.2 255.255.0.0
  keepalive 30 5
  bandwidth 500
  bandwidth inherit
  tunnel mode gre ip
  tunnel source 10.4.9.15

```

```
tunnel destination 10.4.9.82
tunnel protection ipsec profile OER
end
```

### VPN B Configuration: BR2

The following example, starting in global configuration mode, shows the VPN B configuration for BR2:

```
key chain OER
  key 1
    key-string CISCO
  !
oer border
  local Ethernet 0/1
  master 10.4.9.4 key-chain OER
  exit
  !
route-map REDISTRIBUTE_STATIC
  match tag 5000
  set metric -10
  exit
  !
router rip
  network 10.60.1.0
  redistribute static route-map REDISTRIBUTE_STATIC
  exit
  !
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime second 14400
crypto ipsec transform-set VPN_1 esp-3des esp-sha-hmac
  mode transport
  exit
  !
crypto map TUNNEL 10 ipsec-isakmp
  set peer 10.4.9.82
  set transform-set VPN_1
  match address 100
  !
crypto ipsec profile OER
  set transform-set VPN_1
  exit
crypto map TUNNEL local-address Ethernet 0/0
  !
crypto isakmp key 0 CISCO address 10.4.9.82 no-xauth
crypto isakmp keepalive 10
crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  exit
  !
interface Ethernet0/0
  ip address 10.4.9.15 255.255.255.0
  crypto map TUNNEL
  exit
  !
interface Tunnel0
  ip address 10.100.2.2 255.255.0.0
  keepalive 30 5
  bandwidth 500
  bandwidth inherit
  tunnel mode gre ip
  tunnel source 10.4.9.15
  tunnel destination 10.4.9.82
```

```
tunnel protection ipsec profile OER
end
```

### VPN B Configuration: Internal Peers

The following example shows a Routing Information Protocol (RIP) routing process created to establish peering with the border routers and internal peers:

```
router rip
 network 10.60.1.0
end
```

## Where to Go Next

This document describes a specific implementation of OER and presumes that you are familiar with the OER technology. If you want to review more information about OER, proceed to the [Cisco IOS Optimized Edge Routing Overview](#) module, followed by the [Setting Up OER Network Components](#) module. To learn more about the other OER phases, read through the other modules in the following list:

- [Using OER to Profile the Traffic Classes](#)
- [Measuring the Traffic Class Performance and Link Utilization Using OER](#)
- [Configuring and Applying OER Policies](#)
- [Using OER to Control Traffic Classes and Verify the Route Control Changes](#)

After you understand the various OER phases you may want to review other OER Solutions modules that are listed under “[Related Documents](#)” section on [page 18](#).

## Additional References

The following sections provide references related to configuring VPN IPsec/GRE tunnel interfaces as OER-managed exit links.

## Related Documents

Related Topic	Document Title
Cisco OER technology overview	<a href="#">“Cisco IOS Optimized Edge Routing Overview”</a> module
Concepts and configuration tasks required to set up OER network components.	<a href="#">“Setting Up OER Network Components”</a> module
OER solution module: voice traffic optimization using OER active probes.	<a href="#">“OER Voice Traffic Optimization Using Active Probes”</a> module
Cisco OER commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	<a href="#">Cisco IOS Optimized Edge Routing Command Reference</a>
IP Routing Protocol commands	<a href="#">Cisco IOS IP Routing Protocols Command Reference</a>
Key Chain Authentication: information about authentication key configuration and management in Cisco IOS software	“ <a href="#">Managing Authentication Keys</a> ” section of the “ <a href="#">Configuring IP Routing Protocol-Independent Features</a> ” chapter in the <a href="#">Cisco IOS IP Routing Protocols Configuration Guide</a>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# Feature Information for Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(11)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Cisco IOS Optimized Edge Routing Feature Roadmap](#).”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for VPN IPsec/GRE Tunnel Interface Optimization

Feature Name	Releases	Feature Information
VPN IPsec/GRE Tunnel Optimization	12.3(11)T	Introduces the ability to configure IPsec/GRE tunnel interfaces as OER-managed exit links.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2006–2009 Cisco Systems, Inc. All rights reserved.