



# Reverse Route Injection

---

**First Published: August 16, 2001**

**Last Updated: November 5, 2007**

Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted.

Enhancements to the default behavior of RRI, the addition of a route tag value, and enhancements to how RRI is configured were added to the Reverse Route Injection feature in Cisco IOS Release 12.3(14)T.

An enhancement was added in Cisco IOS Release 12.4(15)T that allows a distance metric to be set for routes that are created by a VPN process so that the dynamically learned route on a router can take precedence over a locally configured static route.

## **Finding Feature Information in This Module**

Your Cisco IOS software release may not support all of the features documented in this module. 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 Reverse Route Injection](#)” section on [page 25](#).

## **Finding Support Information for Platforms and Cisco IOS 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.

## Contents

- [Prerequisites for Reverse Route Injection, page 2](#)
- [Restrictions for Reverse Route Injection, page 2](#)
- [Information About Reverse Route Injection, page 2](#)
- [How to Configure Reverse Route Injection, page 4](#)



---

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

© 2001–2007 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for Reverse Route Injection, page 10](#)
- [Additional References, page 16](#)
- [Command Reference, page 17](#)
- [Feature Information for Reverse Route Injection, page 25](#)

## Prerequisites for Reverse Route Injection

- IP routing should be enabled and static routes should be redistributed if dynamic routing protocols are to be used to propagate RRI-generated static routes.

## Restrictions for Reverse Route Injection

- If RRI is applied to a crypto map, that map must be unique to one interface on the router. In other words, the same crypto map cannot be applied to multiple interfaces. If more than one crypto map is applied to multiple interfaces, routes may not be cleaned up correctly. If multiple interfaces require a crypto map, each must use a uniquely defined map. This restriction applies only to RRI before Cisco IOS Release 12.3(14)T.
- For static crypto maps, routes are always present if RRI is configured on an applied crypto map. In Cisco IOS Release 12.3(14)T, the default behavior—of routes always being present for a static map—will not apply unless the **static** keyword is added to the **reverse-route** command.

## Information About Reverse Route Injection

To configure the Reverse Route Injection enhancements, you should understand the following concepts:

- [Reverse Route Injection, page 2](#)
- [Enhancements to Reverse Route Injection in Cisco IOS Release 12.4\(15\)T, page 3](#)

## Reverse Route Injection

RRI is the ability for static routes to be automatically inserted into the routing process for those networks and hosts that are protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote VPN router as the next hop, the traffic is forced through the crypto process to be encrypted.

After the static route is created on the VPN router, this information is propagated to upstream devices, allowing them to determine the appropriate VPN router to which to send returning traffic in order to maintain IPsec state flows. Being able to determine the appropriate VPN router is particularly useful if multiple VPN routers are used at a site to provide load balancing or failover or if the remote VPN devices are not accessible via a default route. Routes are created in either the global routing table or the appropriate virtual route forwarding (VRF) table.

RRI is applied on a per-crypto map basis, whether this is via a static crypto map or a dynamic crypto map template. The default behavior for the two map types is as follows:

- In the case of a dynamic crypto map, routes are created upon the successful establishment of IPsec security associations (SAs) for those remote proxies. The next hop back to those remote proxies is via the remote VPN router whose address is learned and applied during the creation of the dynamic crypto map template. The routes are deleted after the SAs are deleted. In Cisco IOS Release 12.3(14)T, the creation of routes on the basis of IPsec source proxies on static crypto maps was added. This behavior became the default behavior on static maps and overrode the creation of routes on the basis of crypto ACLs (see the next bullet).
- For static crypto maps, routes are created on the basis of the destination information defined in the crypto access list. The next hop is taken from the first set peer statement that is attached to the crypto map. If at any time, RRI, the peer, or the access list is removed from the crypto map, routes will be deleted. This behavior changes with the addition of the RRI enhancements, as explained in the sections below.

## Enhancements to Reverse Route Injection in Cisco IOS Release 12.4(15)T

The following enhancements have been added to the Reverse Route Injection feature in Cisco IOS Release 12.4(15)T:

- [RRI Distance Metric, page 3](#)
- [Gateway Option, page 3](#)
- [Support for RRI on IPsec Profiles, page 4](#)
- [Tag Option Configuration Changes, page 4](#)
- [show crypto route Command, page 4](#)

### RRI Distance Metric

In general, a static route is created having an administrative distance of 1, which means that static routes always have precedence in the routing table. In some scenarios, however, it is required that dynamically learned routes take precedence over static routes, with the static route being used in the absence of a dynamically learned route. The addition of the **set reverse-route distance** command under either a crypto map or IPsec profile allows you to specify a different distance metric for VPN-created routes so that those routes will be in effect only if a dynamic or more favored route becomes unavailable.

### Gateway Option

This RRI gateway option is relevant to the crypto map only.

This option allows you to configure unique next hops or gateways for remote tunnel endpoints. The option is identical to the way the **reverse-route remote-peer** *{ip-address}* command worked prior to Cisco IOS Release 12.3(14)T in that two routes are created for each VPN tunnel. The first route is to the destination-protected subnet via the remote tunnel endpoint. The second route specifies the next hop to be taken to reach this tunnel endpoint. This RRI gateway option allows specific default paths to be specified for specific groups of VPN connections on platforms that support recursive route lookups.



#### Note

In 12.4(15)T and later releases, the **gateway** keyword option replaces the **reverse-route remote-peer** command (with no *ip-address*). Due to changes to Cisco Express Forwarding (CEF), an interface as a next-hop cannot be used without also adding a next-hop IP address.

## Support for RRI on IPsec Profiles

Previously RRI was available for crypto map configurations only. Cisco IOS Release 12.4(15)T introduces support for relevant RRI options on IPsec profiles that are predominantly used for virtual tunnel interfaces. On tunnel interfaces, only the distance metric and tag options are useful with the generic RRI capability.

**Note**

It is not necessary to specifically enable RRI on dynamic virtual interfaces for Easy VPN clients. Route support is enabled by default. It is necessary to specify tag or distance metric values if these are required.

## Tag Option Configuration Changes

The tag option was introduced in 12.3(14)T for crypto maps. This option is now supported with IPsec profiles under the **set reverse-route tag** command syntax. The **set reverse-route tag** command is also available under the crypto map for uniformity although the legacy **reverse-route tag** command is no longer supported.

## show crypto route Command

The **show crypto route** command displays routes that are created through IPsec via RRI or Easy VPN virtual tunnel interfaces (VTIs). The routes are displayed in one table. To see sample output for the **show crypto route** command, see the section “[show crypto route Command Output: Example.](#)”

# How to Configure Reverse Route Injection

The following sections show how to configure reverse route injection for Cisco IOS software before Release 12.4(15)T and for Release 12.4(15)T.

- [Configuring RRI on Crypto Maps for Cisco IOS Releases Prior to 12.4\(15\)T, page 4](#)
- [Configuring RRI with Enhancements Added in Cisco IOS Release 12.4\(15\)T, page 6](#)

## Configuring RRI on Crypto Maps for Cisco IOS Releases Prior to 12.4(15)T

This section includes the following tasks:

- [Configuring RRI Under a Static Crypto Map, page 4](#)
- [Configuring RRI Under a Dynamic Map Template, page 5](#)

## Configuring RRI Under a Static Crypto Map

To configure RRI under a static crypto map for Cisco IOS software prior to Release 12.4(15)T, perform the following steps.

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto map {map-name} {seq-name} ipsec-isakmp`
4. `reverse-route [static | tag tag-id [static] | remote-peer [static] | remote-peer ip-address [static]]`

## 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 map {map-name} {seq-name} ipsec-isakmp</b>  <b>Example:</b> Router (config)# crypto map mymap 1 ipsec-isakmp	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 4	<b>reverse-route [static   tag tag-id [static]   remote-peer [static]   remote-peer ip-address [static]]</b>  <b>Example:</b> Router (config-crypto-map)# reverse-route remote-peer 10.1.1.1	Creates source proxy information for a crypto map entry.

## Configuring RRI Under a Dynamic Map Template

To configure RRI under a dynamic map template for Cisco IOS software prior to Release 12.4(15)T, perform the following steps.

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto dynamic-map dynamic-map-name dynamic-seq-name`
4. `reverse-route [static | tag tag-id [static] | remote-peer [static] | remote-peer ip-address [static]]`

## 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 dynamic-map</b> <i>dynamic-map-name</i> <i>dynamic-seq-name</i>  <b>Example:</b> Router (config)# crypto dynamic-map mymap 1	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
Step 4	<b>reverse-route</b> [ <b>static</b>   <b>tag</b> <i>tag-id</i> [ <b>static</b> ]   <b>remote-peer</b> [ <b>static</b> ]   <b>remote-peer</b> <i>ip-address</i> [ <b>static</b> ]]  <b>Example:</b> Router (config-crypto-map)# reverse-route remote-peer 10.1.1.1	Creates source proxy information for a crypto map entry.

## Configuring RRI with Enhancements Added in Cisco IOS Release 12.4(15)T

The following sections show how to configure RRI with the enhancements that were added in Cisco IOS Release 12.4(15)T:

- [Configuring RRI with Enhancements Under a Static Crypto Map, page 6](#)
- [Configuring RRI with Enhancements Under a Dynamic Map Template, page 7](#)
- [Configuring a RRI Distance Metric Under an IPsec Profile, page 8](#)
- [Verifying Routes That Are Created Through IPsec via RRI or Easy VPN VTIs, page 9](#)

### Configuring RRI with Enhancements Under a Static Crypto Map

To configure RRI with enhancements under a static crypto map (for Cisco IOS Release 12.4(15)T and later releases), perform the following steps.

## SUMMARY STEPS

- enable**
- configure terminal**
- crypto map** *map-name seq-name ipsec-isakmp*
- reverse-route** [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]]
- set reverse-route** [**distance** *number* | **tag** *tag-id*]

## 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 map</b> <i>map-name seq-name ipsec-isakmp</i>  <b>Example:</b> Router (config)# crypto map mymap 1 ipsec-isakmp	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 4	<b>reverse-route</b> [ <b>static</b>   <b>remote-peer</b> <i>ip-address</i> [ <b>gateway</b> ] [ <b>static</b> ]]  <b>Example:</b> Router (config-crypto-map)# reverse-route	Creates source proxy information for a crypto map entry. <b>Note</b> The <b>gateway</b> keyword can be added to enable the dual route functionality for default gateway support.
Step 5	<b>set reverse-route</b> [ <b>distance</b> <i>number</i>   <b>tag</b> <i>tag-id</i> ]  <b>Example:</b> Router (config-crypto-map)# set reverse-route distance 20	Specifies a distance metric to be used or a tag value to be associated with these routes.

## Configuring RRI with Enhancements Under a Dynamic Map Template

To configure RRI with enhancements under a dynamic map template (for Cisco IOS Release 12.4(15)T and later releases), perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name dynamic-seq-name*
4. **reverse-route** [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]]
5. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

## 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 dynamic-map</b> <i>dynamic-map-name</i> <i>dynamic-seq-name</i>  <b>Example:</b> Router (config)# crypto dynamic-map mymap 1	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
Step 4	<b>reverse-route</b> [ <b>static</b>   <b>remote-peer</b> <i>ip-address</i> <i>gateway</i> ] [ <b>static</b> ]  <b>Example:</b> Router (config-crypto-map)# reverse-route remote-peer 10.1.1.1 gateway	Creates source proxy information for a crypto map entry.
Step 5	<b>set reverse-route</b> [ <b>distance</b> <i>number</i>   <b>tag</b> <i>tag-id</i> ]  <b>Example:</b> Router (config-crypto-map)# set reverse-route distance 20	Specifies a distance metric to be used or a tag value to be associated with these routes.

## Configuring a RRI Distance Metric Under an IPsec Profile

To configure a RRI distance metric under an IPsec profile for Cisco IOS Release 12.4(15)T and later releases, perform the following steps:

## SUMMARY STEPS

- enable**
- configure terminal**
- crypto ipsec profile** *name*
- set reverse-route** [**distance** *number* | **tag** *tag-id*]

## 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 profile name</b>  <b>Example:</b> Router (config)# crypto ipsec profile myprofile	Creates or modifies an IPsec profile and enters IPsec profile configuration mode.
Step 4	<b>set reverse-route [distance number   tag tag-id]</b>  <b>Example:</b> Router (config-crypto-profile)# set reverse-route distance 20	Defines a distance metric for each static route or tags a reverse route injection- (RRI-) created route. <ul style="list-style-type: none"> <li><b>distance</b>—Defines a distance metric for each static route.</li> <li><b>tag</b>—Sets a tag value that can be used as a “match” value for controlling distribution using route maps.</li> </ul>

## Verifying Routes That Are Created Through IPsec via RRI or Easy VPN VTIs

To display routes that are created through IPsec via RRI or Easy VPN VTIs, perform the following steps.

## SUMMARY STEPS

- enable
- show crypto route

## 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>show crypto route</b>  <b>Example:</b> Router# show crypto route	Displays routes that are created through IPsec via RRI or Easy VPN VTIs.

## Troubleshooting Tips

To observe the behavior of RRI and its relationship to the creation and deletion of an IPsec SA, you can use the **debug crypto ipsec** command (see the *Cisco IOS Debug Command Reference*, Release 12.4T).

# Configuration Examples for Reverse Route Injection

This section contains the following sections:

- [Configuring RRI Prior to Cisco IOS Release 12.3\(14\)T: Examples, page 10](#)
- [Configuring RRI with Enhancements Added in Cisco IOS Release 12.3\(14\)T: Examples, page 11](#)
- [Configuring RRI with Enhancements Added in Cisco IOS Release 12.4\(15\)T: Examples, page 12](#)

## Configuring RRI Prior to Cisco IOS Release 12.3(14)T: Examples

The following are examples of RRI configurations and output before Cisco IOS Release 12.3(14)T:

- [Configuring RRI When Crypto ACLs Exist: Example, page 10](#)
- [Configuring RRI When Two Routes Are Created, One for the Remote Endpoint and One for Route Recursion: Example, page 11](#)

### Configuring RRI When Crypto ACLs Exist: Example

The following example shows that all remote VPN gateways connect to the router via 192.168.0.3. RRI is added on the static crypto map, which creates routes on the basis of the source network and source netmask that are defined in the crypto access control list (ACL):

```
crypto map mymap 1 ipsec-isakmp
  set peer 10.1.1.1
  reverse-route
  set transform-set esp-3des-sha
  match address 102
```

```
Interface FastEthernet 0/0
ip address 192.168.0.2 255.255.255.0
standby name group1
standby ip 192.168.0.3
crypto map mymap redundancy group1
```

```
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

In Cisco IOS Release 12.3(14)T and later releases, for the static map to retain this same behavior of creating routes on the basis of crypto ACL content, the **static** keyword is required, that is, **reverse-route static**.



#### Note

The **reverse-route** command in this situation creates routes that are analogous to the following static route command-line interface (CLI) commands (**ip route**):

#### Remote Tunnel Endpoint

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
```

**VPNSM**

```
ip route 10.1.1.1 255.255.255.255 vlan0.1
```

---

## Configuring RRI When Two Routes Are Created, One for the Remote Endpoint and One for Route Recursion: Example

In the following example, two routes are created, one for the remote endpoint and one for route recursion to the remote endpoint via the interface on which the crypto map is configured:

```
reverse-route remote-peer
```

## Configuring RRI with Enhancements Added in Cisco IOS Release 12.3(14)T: Examples

The following are examples of configurations and output for RRI enhancements that were added in Cisco IOS Release 12.3(14)T.

- [Configuring RRI When Crypto ACLs Exist: Example, page 11](#)
- [Configuring RRI with Route Tags: Example, page 11](#)
- [Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop: Example, page 12](#)

## Configuring RRI When Crypto ACLs Exist: Example

The following example shows that RRI has been configured for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
  set peer 172.17.11.1
  reverse-route static
  set transform-set esp-3des-sha
  match address 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

## Configuring RRI with Route Tags: Example

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
  reverse-route tag 5

router ospf 109
  redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
  match tag 5
  set metric 5
  set metric-type type1
```

```
Router# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
   via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

## Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop: Example

**Note** This option is applicable only to crypto maps.

The preceding example shows that one route has been created to the remote proxy via a user-defined next hop. This next hop should not require a recursive route lookup unless it will recurse to a default route.

```
reverse-route remote-peer 10.4.4.4
```

The preceding example yields the following prior to Cisco IOS Release 12.3(14)T:

```
10.0.0.0/24 via 10.1.1.1 (in the VRF table if VRFs are configured)
10.1.1.1/32 via 10.4.4.4 (in the global route table)
```

And this result occurs with RRI enhancements:

```
10.0.0.0/24 via 10.4.4.4 (in the VRF table if VRFs are configured, otherwise in the global
table)
```

## Configuring RRI with Enhancements Added in Cisco IOS Release 12.4(15)T: Examples

The following are examples of configurations and output for RRI enhancements that were added in Cisco IOS Release 12.4(15)T.

- [Configuring a RRI Distance Metric Under a Crypto Map: Example, page 12](#)
- [Configuring RRI with Route Tags: Example, page 13](#)
- [debug and show Command Output for a RRI Distance Metric Configuration Under a Crypto Map: Example, page 13](#)
- [Configuring a RRI Distance Metric for a VTI: Example, page 14](#)
- [debug and show Command Output for a RRI Metric Configuration Having a VTI: Example, page 14](#)
- [show crypto route Command Output: Example, page 15](#)

## Configuring a RRI Distance Metric Under a Crypto Map: Example

The following configuration shows a server and client configuration for which a RRI distance metric has been set under a crypto map:

### Server

```
crypto dynamic-map mymap
 set security-association lifetime seconds 300
 set transform-set 3dessa
 set isakmp-profile profile1
 set reverse-route distance 20
 reverse-route
```

**Client**

```
crypto ipsec client ezvpn ez
connect auto
group cisco key cisco
mode client
peer 10.0.0.119
username XXX password XXX
xauth userid mode local
```

**Configuring RRI with Route Tags: Example**

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
set reverse-route tag 5

router ospf 109
redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
match tag 5
set metric 5
set metric-type type1

Router# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

**debug and show Command Output for a RRI Distance Metric Configuration Under a Crypto Map: Example**

The following are **debug** and **show** command output for a RRI distance metric configuration under a crypto map on a server:

```
Router# debug crypto ipsec

00:23:37: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.0.0.119, remote= 10.0.0.14,
local_proxy= 0.0.0.0/0.0.0.0/0 (type=4),
remote_proxy= 192.168.6.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
00:23:37: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:23:37: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
10.0.0.128
00:23:37: IPSEC(rte_mgr): VPN Route Refcount 1 FastEthernet0/0
00:23:37: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via 10.0.0.14 in IP
DEFAULT TABLE with tag 0 distance 20
00:23:37: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```

        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

C    192.200.200.0/24 is directly connected, Loopback0
    10.20.20.20/24 is subnetted, 1 subnets
C    10.30.30.30 is directly connected, Loopback4
C    192.168.5.0/24 is directly connected, Loopback3
    10.20.20.20/24 is subnetted, 2 subnets
S    10.3.1.0 [1/0] via 10.0.0.113
C    10.20.20.20 is directly connected, FastEthernet0/0
    192.168.6.0/32 is subnetted, 1 subnets
S    192.168.6.1 [20/0] via 10.0.0.14
C    192.168.3.0/24 is directly connected, Loopback2
    10.15.0.0/24 is subnetted, 1 subnets
C    10.15.0.0 is directly connected, Loopback6
S*   0.0.0.0/0 [1/0] via 10.0.0.14

```

## Configuring a RRI Distance Metric for a VTI: Example

The following configuration shows a server and client configuration in which a RRI distance metric has been set for a VTI:

### Server Configuration

```

crypto isakmp profile profile1
  keyring mykeyring
  match identity group cisco
  client authentication list authenlist
  isakmp authorization list autholist
  client configuration address respond
  virtual-template 1
crypto ipsec profile vi
  set transform-set 3dessha
  set reverse-route distance 20
  set isakmp-profile profile1
!
interface Virtual-Template1 type tunnel
  ip unnumbered
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile vi

```

### Client Configuration

```

crypto ipsec client ezvpn ez
  connect auto
  group cisco key cisco
  mode client
  peer 10.0.0.119
  username XXX password XXX
  virtual-interface 1

```

## debug and show Command Output for a RRI Metric Configuration Having a VTI: Example

The following are **debug** and **show** command output for a RRI metric configuration for a VTI on a server:

```

Router# debug crypto ipsec

00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)

```

```

00:47:56: Crypto mapdb : proxy_match
          src addr   : 0.0.0.0
          dst addr   : 192.168.6.1
          protocol   : 0
          src port    : 0
          dst port    : 0
00:47:56: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same pro
xies and peer 10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
 10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Refcount 1 Virtual-Access2
00:47:56: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via Virtua
l-Access2 in IP DEFAULT TABLE with tag 0 distance 20
00:47:56: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0

00:47:56: IPSEC(create_sa): sa created,
          (sa) sa_dest= 10.0.0.110, sa_proto= 50,
          sa_spi= 0x19E1175C(434181980),
          sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 87
00:47:56: IPSEC(create_sa): sa created,
          (sa) sa_dest= 10.0.0.14, sa_proto= 50,
          sa_spi= 0xADC90C5(182227141),
          sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 88
00:47:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, chang
ed state to up
00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:47:56: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP
00:47:56: IPSEC(key_engine_enable_outbound): enable SA with spi 182227141/50
00:47:56: IPSEC(update_current_outbound_sa): updated peer 10.0.0.14 current outb
ound sa to SPI ADC90C5

```

Router# **show ip route**

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

```

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

```

C    192.200.200.0/24 is directly connected, Loopback0
    10.20.20.20/24 is subnetted, 1 subnets
C      10.30.30.30 is directly connected, Loopback4
C    192.168.5.0/24 is directly connected, Loopback3
    10.20.20.20/24 is subnetted, 2 subnets
S      10.3.1.0 [1/0] via 10.0.0.113
C    10.20.20.20 is directly connected, FastEthernet0/0
    192.168.6.0/32 is subnetted, 1 subnets
S      192.168.6.1 [20/0] via 0.0.0.0, Virtual-Access2
C    192.168.3.0/24 is directly connected, Loopback2
    10.15.0.0/24 is subnetted, 1 subnets
C      10.15.0.0 is directly connected, Loopback6
S*   0.0.0.0/0 [1/0] via 10.0.0.14

```

## show crypto route Command Output: Example

The following output example displays routes, in one table, that are created through IPsec via RRI or Easy VPN VTIs:

```

Router# show crypto route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
       S - Static Map ACLs

Routes created in table GLOBAL DEFAULT
192.168.6.2/255.255.255.255 [0/0] via 10.0.0.133
                        on Virtual-Access3 RRI
10.1.1.0/255.255.255.0 [10/0] via Virtual-Access2 VTI
192.168.6.1/255.255.255.255 [0/0] via Virtual-Access2 VTI

```

## Additional References

The following sections provide references related to Reverse Route Injection enhancements.

### Related Documents

Related Topic	Document Title
Cisco IOS Security commands	<a href="#">Cisco IOS Security Command Reference</a> , Release 12.4T
Other Cisco IOS commands	<a href="#">Cisco IOS Command Reference</a> , Release 12.4T

### Standards

Standards	Title
None	—

### MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFCs	Title
None	—

## 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>

## Command Reference

This section documents only commands that are new or modified.

- [reverse-route](#)
- [set reverse-route](#)
- [show crypto route](#)

## reverse-route

To create source proxy information for a crypto map entry, use the **reverse-route** command in crypto map configuration mode. To remove the source proxy information from a crypto map entry, use the **no** form of this command.

### Effective with Cisco IOS Release 12.4(15)T

```
reverse-route [static | remote-peer ip-address [gateway ] [static]]
```

```
no reverse-route [static | remote-peer ip-address [gateway ] [static]]
```

### Before Cisco IOS Release 12.4(15)T

```
reverse-route [static | tag tag-id [static] | remote-peer [static] | remote-peer ip-address [static]]
```

```
no reverse-route [static | tag tag-id [static] | remote-peer [static] | remote-peer ip-address [static]]
```

Syntax Description	
<b>tag</b> <i>tag-id</i>	(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps.  <b>Note</b> The <b>tag</b> keyword and <i>tag-id</i> argument were deleted effective with Cisco IOS Release 12.4(15)T.
<b>remote-peer</b>	(Optional) Indicates two routes: one for the tunnel endpoint, with the next hop being the interface to which the crypto map is bound.  <b>Note</b> The <b>remote-peer</b> keyword and its variants ( <i>ip-address</i> argument and <b>gateway</b> keyword) are applicable only to crypto maps.
<i>ip-address</i>	(Optional) If used without the optional <b>gateway</b> keyword, there is only one route: the protected subnet. The next hop is determined by the user-added value for the <i>ip-address</i> argument.
<b>gateway</b>	(Optional) Used with the <i>ip-address</i> argument. If the <b>gateway</b> keyword is used, there are two routes: one to the protected subnet by way of the remote-tunnel endpoint and the other to the remote-tunnel endpoint that is determined by the user-added value for the <i>ip-address</i> argument.  <b>Note</b> The optional <b>gateway</b> keyword enables the behavior of the <b>reverse-route remote-peer ip-address</b> command syntax used for software releases before Cisco IOS Release 12.3(14)T.
<b>static</b>	(Optional) Creates routes on the basis of crypto ACLs, regardless of whether flows have been created for these ACLs.

**Defaults** No default behavior or values.

**Command Modes** Crypto map configuration (config-crypto-map)

**Command History**

Release	Modification
12.1(9)E	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	The <b>remote-peer</b> keyword and <i>ip-address</i> argument were added.
12.3(14)T	The <b>static</b> and <b>tag</b> keywords and <i>tag-id</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	The <b>tag</b> keyword and <i>tag-id</i> argument were deleted. The <b>gateway</b> keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

**Usage Guidelines**

This command can be applied on a per-crypto map basis.

Reverse route injection (RRI) provides a scalable mechanism to dynamically learn and advertise the IP address and subnets that belong to a remote site that connects through an IP Security (IPSec) Virtual Private Network (VPN) tunnel.

When enabled in an IPSec crypto map, RRI will learn all the subnets from any network that is defined in the crypto ACL as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPSec tunnel is torn down, the associated static routes will be removed. These static routes may then be redistributed into other dynamic routing protocols so that they can be advertised to other parts of the network (usually done by redistributing RRI routes into dynamic routing protocols on the core side).

**Examples****Before Cisco IOS Release 12.3(14)T**

The following is an example in which RRI has been configured when crypto ACLs exist. The example shows that all remote VPN gateways connect to the router via 192.168.0.3. RRI is added on the static crypto map, which creates routes on the basis of the source network and source netmask that are defined in the crypto ACL.

```
crypto map mymap 1 ipsec-isakmp
  set peer 10.1.1.1
  reverse-route
  set transform-set esp-3des-sha
  match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

**Note**

In Cisco IOS Release 12.3(14)T and later releases, for the static map to retain this same behavior of creating routes on the basis of crypto ACL content, the **static** keyword will be necessary, that is, **reverse-route static**.

The **reverse-route** command in this situation creates routes that are analogous to the following static route command-line interface (CLI) commands (**ip route**):

- Remote Tunnel Endpoint  

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
```
- VPN Services Module (VPNSM)  

```
ip route 10.1.1.1 255.255.255.255 vlan0.1
```

In the following example, two routes are created, one for the remote endpoint and one for route recursion to the remote endpoint via the interface on which the crypto map is configured.

```
reverse-route remote-peer
```

**Configuring RRI with the Enhancements Added in Cisco IOS Release 12.3(14)T**

The following configuration example shows that RRI has been configured for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
  set peer 172.17.11.1
  reverse-route static
  set transform-set esp-3des-sha
  match address 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
  reverse-route tag 5

router ospf 109
  redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
  match tag 5
  set metric 5
  set metric-type type1

Router# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

The following example shows that one route has been created to the remote proxy via a user-defined next hop. This next hop should not require a recursive route lookup unless it will recurse to a default route.

```
reverse-route remote-peer 10.4.4.4
```

The previous example yields the following before Cisco IOS Release 12.3(14)T:

```
10.0.0.0/24 via 10.1.1.1 (in the VRF table if VRFs are configured)
10.1.1.1/32 via 10.4.4.4 (in the global route table)
```

And this result occurs with RRI enhancements:

10.0.0.0/24 via 10.4.4.4 (in the VRF table if VRFs are configured, otherwise in the global table)

#### Effective with Cisco IOS Release 12.4(15)T

In the following example, routes are created from the destination information in the access control list (ACL). One route will list 10.2.2.2 as the next hop route to the ACL information, and one will indicate that to get to 10.2.2.2, the route will have to go by way of 10.1.1.1. All routes will have a metric of 10. Routes are created only at the time the map and specific ACL rule are created.

```
crypto map map1 1 ipsec-isakmp
  set peer 10.2.2.2
  reverse-route remote-peer 10.1.1.1 gateway
  set reverse-route distance 10
  match address 101
```

Configuring RRI with Route Tags 12.4(15)T or later: Example

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
  set reverse-route tag 5

router ospf 109
  redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
  match tag 5
  set metric 5
  set metric-type type1
```

Router# **show ip ospf topology**

```
P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

#### Related Commands

Command	Description
<b>crypto map (global IPsec)</b>	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
<b>crypto map local-address</b>	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
<b>show crypto map (IPsec)</b>	Displays the crypto map configuration.

## set reverse-route

To define a distance metric for each static route or to tag a reverse route injection- (RRI-) created route, use the **set reverse route** command in crypto map or ipsec profile configuration mode. To delete the tag or distance metric, use the **no** form of the command.

**set reverse-route** [**distance** *number* | **tag** *tag-id*]

**no set reverse-route** [**distance** *number* | **tag** *tag-id*]

### Syntax Description

<b>distance</b> <i>number</i>	(Optional) Defines a distance metric for each static route. The <i>number</i> value = 1 through 255.
<b>tag</b> <i>tag-id</i>	(Optional) Creates a route and tags it. The tag value can be used as a “match” value for controlling redistribution using route maps.

### Command Default

The distance metric is 1 and the tag is 0.

### Command Modes

Crypto map configuration (config-crypto-map)  
Ipsec profile configuration (config-crypto-profile)

### Command History

Release	Modification
12.4(15)T	This command was introduced. The <b>set reverse-route tag tag-id</b> command, keyword, and argument replaced the <b>reverse-route tag tag-id</b> command, keyword, and argument.

This command can be applied on a per-crypto map basis or to a virtual tunnel interface (VTI) in a reverse route (RRI) configuration.

RRI provides a scalable mechanism to dynamically learn and advertise the IP address and subnets that belong to a remote site that connects through an IP Security (IPsec) Virtual Private Network (VPN) tunnel.

When enabled in an IPsec crypto map, RRI will learn all the subnets from any network that is defined in the crypto ACL as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPsec tunnel is torn down, the associated static routes will be removed. These static routes may then be redistributed into other dynamic routing protocols so that they can be advertised to other parts of the network (usually by redistributing RRI routes into dynamic routing protocols on the core side).

The **set reverse-route** command provides a way to configure a server so that a dynamically learned route can take precedence over static routes. The static routes are used only in the absence of the dynamically learned route.

### Examples

The following example shows that the metric distance for each dynamically route is set to 20 in a crypto map situation. The configuration is on an Easy VPN server.

```
crypto dynamic-map mode 1
  set security-association lifetime seconds 300
```

```

set transform-set 3dessha
set isakmp-profile profile2
set reverse-route distance 20
reverse-route

```

The following example shows that the metric distance for each dynamic route is set to 20 for a virtual tunnel interface (VTI). The configuration is on an Easy VPN server.

```

crypto isakmp profile profile1
  keyring mykeyring
  match identity group examplegroup
  client authentication list authenlist
  isakmp authorization list autholist
  client configuration address respond
  virtual-template 1
crypto ipsec profile vi
  set transform-set 3dessha
  set reverse-route distance 20
  set isakmp-profile profile1
!
interface Virtual-Templat1 type tunnel
  ip unnumbered
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile vi

```

#### Related Commands

Command	Description
<b>debug crypto ipsec</b>	Displays IPsec events.
<b>reverse-route</b>	Creates source proxy information for a crypto map entry.

# show crypto route

To display routes that are created through IPsec via Reverse Route Injection (RRI) or Easy VPN virtual tunnel interfaces (VTIs) in one table, use the **show crypto route** command in privileged EXEC mode.

**show crypto route**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.4(15)T	This command was introduced.

**Examples** The following example displays routes that were created through IPsec using RRI and VTIs:

```
Router# show crypto route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
       S - Static Map ACLs

Routes created in table GLOBAL DEFAULT
192.168.6.2/255.255.255.255 [0/0] via 10.0.0.133
                               on Virtual-Access3 RRI
10.1.1.0/255.255.255.0 [10/0] via Virtual-Access2 VTI
192.168.6.1/255.255.255.255 [0/0] via Virtual-Access2 VTI
```

The fields in the above display are self-explanatory.

Related Commands	Command	Description
	<b>reverse-route</b>	Creates source proxy information for a crypto map entry.
	<b>set reverse-route</b>	Defines a distance metric for each static route or tags a RRI-created route.

# Feature Information for Reverse Route Injection

Table 1 lists the release history for this feature.

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 Reverse Route Injection

Feature Name	Releases	Feature Information
Reverse Route Injection	12.1(9)E 12.2(8)T 12.2(8)YE	<p>Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.</p> <p>Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• “Reverse Route Injection” section on page 2</li> </ul> <p>The following commands were introduced or modified by this feature: <b>reverse-route</b>.</p>
Reverse Route Remote Peer Options	12.2(13)T 12.2(14)S	<p>An enhancement was added to RRI to allow you to specify an interface or address as the explicit next hop to the remote VPN device. This functionality allows the overriding of a default route to properly direct outgoing encrypted packets.</p> <p>The following sections provide information about the remote peer options:</p> <ul style="list-style-type: none"> <li>• “Enhancements to Reverse Route Injection in Cisco IOS Release 12.4(15)T” section on page 3.</li> </ul>

Table 1 Feature Information for Reverse Route Injection (continued)

Feature Name	Releases	Feature Information
Reverse Route Injection Enhancements	12.3(14)T 12.2(33)SRA 12.2(33)SXH	<p>The following enhancements were added to the Reverse Route Injection feature:</p> <ul style="list-style-type: none"> <li>• The default behavior of static crypto maps will be the same as that of dynamic crypto maps unless the <b>reverse-route</b> command and <b>static</b> keyword are used.</li> <li>• A route tag value was added for any routes that are created using RRI.</li> <li>• RRI can be configured on the same crypto map that is applied to multiple router interfaces.</li> <li>• RRI configured with the <b>reverse-route remote-peer {ip-address}</b> command, keyword, and argument will create one route instead of two.</li> </ul> <p>The following sections provide information about the Reverse Route Injection enhancements:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Reverse Route Injection” section on page 2</a></li> <li>• <a href="#">“Configuring RRI on Crypto Maps for Cisco IOS Releases Prior to 12.4(15)T” section on page 4</a></li> <li>• <a href="#">“Configuring RRI with Enhancements Added in Cisco IOS Release 12.4(15)T” section on page 6</a></li> <li>• <a href="#">“Configuring RRI When Crypto ACLs Exist: Example” section on page 10</a></li> <li>• <a href="#">“Configuring RRI with Route Tags: Example” section on page 11</a></li> <li>• <a href="#">“Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop: Example” section on page 12</a></li> </ul> <p>The following command was modified by these feature enhancements: <b>reverse-route</b>.</p>
Gateway Option	12.4(15)T	<p>This option allows you to configure unique next hops or gateways for remote tunnel endpoints.</p> <p>The following section provides information about the Gateway Option:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Gateway Option” section on page 3</a></li> </ul>

Table 1 Feature Information for Reverse Route Injection (continued)

Feature Name	Releases	Feature Information
RRI Distance Metric	12.4(15)T	<p>This enhancement allows you to define a metric distance for each static route.</p> <p>The following sections provide information about the RRI distance metric enhancement.</p> <ul style="list-style-type: none"> <li>• “RRI Distance Metric” section on page 3</li> <li>• “Configuring a RRI Distance Metric Under an IPsec Profile” section on page 8</li> <li>• “Configuring a RRI Distance Metric Under a Crypto Map: Example” section on page 12</li> <li>• “debug and show Command Output for a RRI Distance Metric Configuration Under a Crypto Map: Example” section on page 13</li> <li>• “Configuring a RRI Distance Metric for a VTI: Example” section on page 14</li> </ul> <p>The following commands were introduced or modified by this feature: <b>reverse-route</b>, <b>set reverse-route</b>.</p>
<b>show crypto route</b> Command	12.4(15)T	<p>This command displays routes that are created through IPsec via RRI or Easy VPN VTIs.</p> <p>The following section provides information about the <b>show crypto route</b> command:</p> <ul style="list-style-type: none"> <li>• “show crypto route” section on page 24</li> </ul>
Support for RRI on IPsec Profiles	12.4(15)T	<p>This feature provides support for relevant RRI options on IPsec profiles that are predominantly used by VTIs.</p> <p>The following section provides information about the Support for RRI on IPsec Profiles feature:</p> <ul style="list-style-type: none"> <li>• “Support for RRI on IPsec Profiles” section on page 4</li> </ul>
Tag Option Configuration Changes	12.4(15)T	<p>The tag option is now supported with IPsec profiles under the <b>set reverse-route tag</b> command.</p> <p>The following section provides information about this feature enhancement:</p> <ul style="list-style-type: none"> <li>• “Tag Option Configuration Changes” section on page 4</li> </ul>

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

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

© 2001–2007 Cisco Systems, Inc. All rights reserved.