



EIGRP MPLS VPN PE-CE Site of Origin (SoO)

The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature introduces the capability to filter Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) traffic on a per-site basis for Enhanced Interior Gateway Routing Protocol (EIGRP) networks. SoO filtering is configured at the interface level and is used to manage MPLS VPN traffic and to prevent transient routing loops from occurring in complex and mixed network topologies. This feature is designed to support the MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE) feature. Support for back door links is provided by this feature when Cisco IOS Release 12.0(27)S is installed to PE routers that support EIGRP MPLS VPNs.

Feature History for EIGRP MPLS VPN PE-CE Site of Origin (SoO)

Release	Modification
12.0(27)S	This feature was introduced.
12.3(8)T	This feature was integrated into Cisco IOS Release 12.3(8)T.
12.2(18)SXE	This feature was integrated into Cisco IOS Release 12.2(18)SXE.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for EIGRP MPLS VPN PE-CE Site of Origin \(SoO\)](#), page 2
- [Restrictions for EIGRP MPLS VPN PE-CE Site of Origin \(SoO\)](#), page 2
- [Information About EIGRP MPLS VPN PE-CE Site of Origin \(SoO\)](#), page 2
- [How to Configure EIGRP MPLS VPN PE-CE Site of Origin \(SoO\) Support](#), page 5
- [Additional References](#), page 10
- [Command Reference](#), page 11



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

Copyright © 2004, 2005 Cisco Systems, Inc. All rights reserved.

Prerequisites for EIGRP MPLS VPN PE-CE Site of Origin (SoO)

This document assumes that Border Gateway Protocol (BGP) is configured in the network core (or the service provider backbone). The following tasks will also need to be completed before you can configure this feature:

- This feature was introduced to support the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature and should be configured after the EIGRP MPLS VPN is created.
- All PE routers that are configured to support the EIGRP MPLS VPN must run Cisco IOS Release 12.0(27)S, which provides support for the SoO extended community.

Restrictions for EIGRP MPLS VPN PE-CE Site of Origin (SoO)

- If a VPN site is partitioned and the SoO extended community attribute is configured on a back door router interface, the back door link cannot be used as an alternate path to reach prefixes originated in other partition of the same site.
- A unique SoO value must be configured for each individual VPN site. The same value must be configured on all PE and CE interfaces (if SoO is configured on the CE routers) that support the same VPN site.

Information About EIGRP MPLS VPN PE-CE Site of Origin (SoO)

To configure this feature, you must understand the following concepts:

- [EIGRP MPLS VPN PE-CE Site of Origin \(SoO\) Support Overview, page 2](#)
- [Site of Origin \(SoO\) Support for Back Door Links, page 3](#)
- [Router Interoperation with the Site of Origin \(SoO\) Extended Community, page 3](#)
- [Redistributing BGP VPN Routes that Carry the Site of Origin \(SoO\) into EIGRP, page 4](#)
- [BGP Cost Community Support for EIGRP MPLS VPN PE-CE Network Topologies, page 4](#)
- [Benefits of the EIGRP MPLS VPN PE-CE Site of Origin \(SoO\) Support Feature, page 5](#)

EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support Overview

The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature provides support for the MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE) feature, which provides the capability to create MPLS VPN networks that connect separate EIGRP VPN sites.

The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature introduces SoO support for EIGRP-to-BGP and BGP-to-EIGRP redistribution. The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the re-advertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a PE router has learned a route. SoO support provides the capability to filter MPLS VPN traffic on a per-EIGRP site basis. SoO filtering is configured at the interface level and is used to manage MPLS VPN traffic and to prevent routing loops from occurring in complex and mixed network topologies, such as EIGRP VPN sites that contain both VPN and back door links.

The configuration of the SoO extended community allows MPLS VPN traffic to be filtered on a per-site basis. The SoO extended community is configured in an inbound BGP route map on the PE router and is applied to the interface with the `ip vrf sitemap` command. The SoO extended community can be applied to all exit points at the customer site for more specific filtering but must be configured on all interfaces of PE routers that provide VPN services to CE routers.

Site of Origin (SoO) Support for Back Door Links

The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature introduces support for back door links. A back door link or a route is a connection that is configured outside of the VPN between a remote and main site, for example, a WAN leased line that connects a remote site to the corporate network. Back door links are typically used as back up routes between EIGRP sites if the VPN link is down or not available. A metric is set on the back door link so that the route through the back door router is not selected unless there is a VPN link failure.

The SoO extended community is defined on the interface of the back door router. It identifies the local site-ID, which should match the value that is used on the PE routers that support the same site. When the back door router receives an EIGRP update (or reply) from a neighbor across the back door link, the router checks the update for a SoO value. If the SoO value in the EIGRP update matches the SoO value on the local back door interface, the route is rejected and not installed to the EIGRP topology table. This typically occurs when the route with the local SoO valued in the received EIGRP update was learned by the other VPN site and then advertised through the back door link by the back door router in the other VPN site. SoO filtering on the back door link prevents transient routing loops from occurring by filtering out EIGRP updates that contain routes that carry the local site-ID.



Note

If a VPN site is partitioned and the SoO extended community attribute is configured on a back door router interface, the back door link cannot be used as an alternate path to reach prefixes originated in other partition of the same site.

If this feature is enabled on the PE routers and the back door routers in the customer sites, and SoO values are defined on both the PE and back door routers, both the PE and back door routers will support convergence between the VPN sites. The other routers in the customer sites need only propagate the SoO values carried by the routes, as the routes are forwarded to neighbors. These routers do not otherwise affect or support convergence beyond normal DUAL computations.

Router Interoperation with the Site of Origin (SoO) Extended Community

The configuration of the SoO extended community allows routers that support this feature to identify the site from which each route originated. When this feature is enabled, the EIGRP routing process on the PE or CE router checks each received route for the SoO extended community and filters based on the following conditions:

- A received route from BGP or a CE router contains a SoO value that matches the SoO value on the receiving interface.

If a route is received with an associated SoO value that matches the SoO value that is configured on the receiving interface, the route is filtered out because it was learned from another PE router or from a back door link. This behavior is designed to prevent routing loops.

- A received route from a CE router is configured with a SoO value that does not match.
If a route is received with an associated SoO value that does not match the SoO value that is configured on the receiving interface, the route is accepted into the EIGRP topology table so that it can be redistributed into BGP.
If the route is already installed to the EIGRP topology table but is associated with a different SoO value, the SoO value from the topology table will be used when the route is redistributed into BGP.
- A received route from a CE router does not contain a SoO value.
If a route is received without a SoO value, the route is accepted into the EIGRP topology table, and the SoO value from the interface that is used to reach the next hop CE router is appended to the route before it is redistributed into BGP.

When BGP and EIGRP peers that support the SoO extended community receive these routes, they will also receive the associated SoO values and pass them to other BGP and EIGRP peers that support the SoO extended community. This filtering is designed to prevent transient routes from being relearned from the originating site, which prevents transient routing loops from occurring.

Redistributing BGP VPN Routes that Carry the Site of Origin (SoO) into EIGRP

When an EIGRP routing process on the PE router redistributes BGP VPN routes into the EIGRP topology table, EIGRP extracts the SoO value (if one is present) from the appended BGP extended community attributes and appends the SoO value to the route before installing it to the EIGRP topology table. EIGRP tests the SoO value for each route before sending updates to CE routers. Routes that are associated with SoO values that match the SoO value configured on the interface are filtered out before they are passed to the CE routers. When an EIGRP routing process receives routes that are associated with different SoO values, the SoO value is passed to the CE router and carried through the CE site.

BGP Cost Community Support for EIGRP MPLS VPN PE-CE Network Topologies

The BGP cost community is a non-transitive extended community attribute that is passed to internal BGP (iBGP) and confederation peers but not external BGP (eBGP) peers. The cost community feature allows you to customize the local route preference and influence the BGP best path selection process.

Before EIGRP SoO BGP Cost Community support was introduced, BGP preferred locally sourced routes over routes learned from BGP peers. Back door links in an EIGRP MPLS VPN topology were preferred by BGP when the back door link was learned first. (A back door link or a route is a connection that is configured outside of the VPN between a remote and main site, for example, a WAN leased line that connects a remote site to the corporate network).

The “pre-bestpath” point of insertion (POI) has been introduced in the BGP Cost Community feature to support mixed EIGRP VPN network topologies that contain VPN and back door links. This POI is applied automatically to EIGRP routes that are redistributed into BGP. The “pre-bestpath” POI carries the EIGRP route type and metric. This POI influences the best path calculation process by influencing BGP to consider this POI before any other comparison step. No configuration is required. This feature is enabled automatically for EIGRP VPN sites when Cisco IOS Release 12.0(27)S is installed to the PE routers or the CE and back door router at the customer sites.

For more information about the BGP Cost Community feature, refer to the BGP Cost Community feature documentation in Cisco IOS Release 12.0(27)S.

Benefits of the EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support Feature

The configuration of the EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support feature introduces per-site VPN filtering, which improves support for complex topologies, such as, MPLS VPNs with back door links, Customer Edge (CE) routers that are dual-homed to different Provider Edge (PE) routers, and PE routers that support CE routers from different sites within the same Virtual Routing and Forwarding (VRF) instance.

How to Configure EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support

This section contains the following procedures:

- [Configuring the Site of Origin \(SoO\) Extended Community, page 5](#)
- [Verifying the Configuration of the SoO Extended Community, page 8](#)

Configuring the Site of Origin (SoO) Extended Community

The configuration of the SoO extended community allows MPLS VPN traffic to be filtered on a per-site basis. The SoO extended community is configured in an inbound BGP route map on the PE router and is applied to the interface with the **ip vrf sitemap** command. The SoO extended community can be applied to all exit points at the customer site for more specific filtering but must be configured on all interfaces of PE routers that provide VPN services to CE routers.

Prerequisites

- This feature was introduced to support the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature and should be configured afterwards.
- All PE routers that are configured to support the EIGRP MPLS VPN must support the SoO extended community.
- A unique SoO value must be configured for each VPN site. The same value must be used on the interface of the PE router that connects to the CE router for each VPN site.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-name* {**permit** | **deny**}[*sequence-number*]
4. **set extcommunity** {**rt** *extended-community-value* [**additive**] | **soo** *extended-community-value*}
5. **exit**
6. **interface** *interface-type*
7. **ip vrf forwarding** *vrf-name*
8. **ip vrf sitemap** *route-map-name*
9. **ip address** *ip-address subnet-mask*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	route-map <i>map-name</i> { permit deny }[<i>sequence-number</i>] Example: Router(config)# route-map Site-of-Origin permit 10	Enters route map configuration mode and creates a route map. <ul style="list-style-type: none">• The route map is created in this step so that SoO extended community can be applied

	Command or Action	Purpose
Step 4	<p>set extcommunity {rt <i>extended-community-value</i> [additive] soo <i>extended-community-value</i>}</p> <p>Example: Router(config-route-map)# set extcommunity soo 100:1</p>	<p>Sets BGP extended community attributes.</p> <ul style="list-style-type: none"> The rt keyword specifies the route target extended community attribute. The soo keyword specifies the site of origin extended community attribute. The <i>extended-community-value</i> argument specifies the value to be set. The value can be one of the following formats: <ul style="list-style-type: none"> autonomous-system-number : network-number ip-address : network-number <p>The colon is used to separate the autonomous system number and network number or IP address and network number.</p> The additive keyword adds a route target to the existing route target list without replacing any existing route targets.
Step 5	<p>exit</p> <p>Example: Router(config-route-map)# exit</p>	Exits route-map configuration mode and enters global configuration mode.
Step 6	<p>interface <i>interface-type</i></p> <p>Example: Router(config)# interface FastEthernet 0/0</p>	Enters interface configuration mode to configure the specified interface.
Step 7	<p>ip vrf forwarding <i>vrf-name</i></p> <p>Example: Router(config-if)# ip vrf forwarding RED</p>	<p>Associates the VRF with an interface or subinterface.</p> <ul style="list-style-type: none"> The VRF name configured in this step should match the VRF name created for the EIGRP MPLS VPN with the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature.
Step 8	<p>ip vrf sitemap <i>route-map-name</i></p> <p>Example: Router(config-if)# ip vrf sitemap Site-of-Origin</p>	<p>Associates the VRF with an interface or subinterface.</p> <ul style="list-style-type: none"> The route map name configured in this step should match the route map name created to apply the SoO extended community in step 3.
Step 9	<p>ip address <i>ip-address subnet-mask</i></p> <p>Example: Router(config-if)# ip address 10.0.0.1 255.255.255.255</p>	<p>Configures the IP address for the interface.</p> <ul style="list-style-type: none"> The IP address needs to be reconfigured after enabling VRF forwarding.
Step 10	<p>end</p> <p>Example: Router(config-if)# end</p>	Exits interface configuration mode and enters privileged EXEC mode.

Examples

The following example, beginning in global configuration mode, configures SoO filtering on an interface:

```
Router(config)# route-map Site-of-Origin permit 10
Router(config-route-map)# set extcommunity soo 100:1
Router(config-route-map)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip vrf forwarding RED
Router(config-if)# ip vrf sitemap Site-of-Origin
Router(config-if)# ip address 10.0.0.1 255.255.255.255
Router(config-if)# end
```

What to Do Next

- To verify the configuration of the SoO extended community, follow the steps in the next section, “Verifying the Configuration of the SoO Extended Community.”
- For mixed EIGRP MPLS VPN network topologies that contain back door routes, the next task is to configure the “pre-bestpath” cost community for back door routes.

Verifying the Configuration of the SoO Extended Community

Use the following steps to verify the configuration of the SoO extended community attribute.

SUMMARY STEPS

1. **enable**
2. **show ip bgp vpnv4** { all | rd *route-distinguisher* | vrf *vrf-name* } [*ip-prefix/length*] [**longer-prefixes**] [*output-modifiers*] [*network-address* [*mask*] [**longer-prefixes**] [*output-modifiers*] [**cidr-only**] [**community**] [**community-list**] [**dampened-paths**] [**filter-list**] [**flap-statistics**] [**inconsistent-as**] [**neighbors**] [**paths** [*line*]] [**peer-group**] [**quote-regexp**] [**regexp**] [**summary**] [**tags**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>show ip bgp vpnv4 {all rd route-distinguisher vrf vrf-name} [ip-prefix/length] [longer-prefixes] [output-modifiers] [network-address [mask] [longer-prefixes] [output-modifiers] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [line] [peer-group] [quote-regexp] [regexp] [summary] [tags]</p> <p>Example: Router# show ip bgp vpnv4 all 10.0.0.1</p>	<p>(Optional) Displays VPN address information from the BGP table.</p> <ul style="list-style-type: none"> Use the show ip bgp vpnv4 command with the all keyword to verify that the specified route has been configured with the SoO extended community attribute.

Examples

This example shows VPN address information from the BGP table and verifies the configuration of the SoO extended community:

```
Router# show ip bgp vpnv4 all 10.0.0.1
BGP routing table entry for 100:1:10.0.0.1/32, version 6
Paths: (1 available, best #1, no table)
  Advertised to update-groups:
    1
  100 300
    192.168.0.2 from 192.168.0.2 (172.16.13.13)
      Origin incomplete, localpref 100, valid, external, best
      Extended Community: SOO:100:1
```

Where to Go Next

For information about configuring EIGRP MPLS VPNs, refer to the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge document in Cisco IOS Release 12.0(27)S.

For more information about configuring the BGP cost community, refer to the BGP Cost Community document in Cisco IOS Release 12.0(27)S.

Additional References

The following sections provide references related to the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature.

Related Documents

Related Topic	Document Title
BGP Cost Community feature and the “pre-bestpath” point of insertion	BGP Cost Community, Release 12.0(27)S
CEF commands	Cisco IOS Switching Services Configuration Guide, Release 12.3
CEF configuration tasks	Cisco IOS Switching Services Command Reference, Release 12.3
EIGRP commands	Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3
EIGRP configuration tasks	Cisco IOS IP Configuration Guide, Release 12.3
EIGRP MPLS VPNs	MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge, Cisco IOS Release 12.0(27)S.
MPLS VPNs	MPLS Virtual Private Networks, Cisco IOS Release 12.0(5)T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents a new command only.

- [ip vrf sitemap](#)

ip vrf sitemap

To configure Site of Origin (SoO) filtering on an interface, use the **ip vrf sitemap** command in interface configuration mode. To disable SoO filtering on an interface, use the **no** form of this command.

ip vrf sitemap *route-map*

no ip vrf sitemap

Syntax Description

<i>route-map</i>	The name of the route map that is configured with the as-number and network of the VPN site.
------------------	--

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

Usage Guidelines

The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the re-advertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a PE router has learned a route.

Examples

The following example, beginning in global configuration mode, configures SoO filtering on an interface:

```
Router(config)# route-map Site-of-Origin permit 10
Router(config-route-map)# set extcommunity soo 100:1
Router(config-route-map)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip vrf forwarding RED
Router(config-if)# ip vrf sitemap Site-of-Origin
Router(config-if)# ip address 10.0.0.1 255.255.255.255
Router(config-if)# end
```

Related Commands

Command	Description
ip vrf forwarding	Associates a VRF with an interface or subinterface.

Glossary

AFI—Address Family Identifier. Carries the identity of the network layer protocol that is associated with the network address.

Back door Router—a router that connects two or more sites, which are also connected to each other through an MPLS VPN EIGRP PE to CE links.

Back door link—a link connecting two back door routers.

BGP—Border Gateway Protocol. An interdomain routing protocol that exchanges reachability information with other BGP systems. It is defined by RFC 1163, *A Border Gateway Protocol (BGP)*. The current implementation of BGP is BGP Version 4 (BGP4). BGP4 is the predominant interdomain routing protocol that is used on the Internet. It supports CIDR and uses route aggregation mechanisms to reduce the size of routing tables.

Cost Community—an extended community attribute that can be inserted anywhere into the bestpath calculation.

Customer Edge (CE) router—a router that belongs to a customer network, which connects to a Provider Edge (PE) router to utilize MPLS VPN network services.

MBGP—multiprotocol BGP. An enhanced version of BGP that carries routing information for multiple network layer protocols and IP multicast routes. It is defined in RFC 2858, *Multiprotocol Extensions for BGP-4*.

Provider Edge (PE) router—the PE router is the entry point into the Service Provider network. The PE router is typically deployed on the edge of the network and is administered by the Service Provider. The PE router is the redistribution point between EIGRP and BGP in PE to CE networking.

Site—a collection of routers that have well-defined exit points to other “sites.”

Site of Origin (SoO)—a special purpose tag or attribute that identifies the site that injects a route into the network. This attribute is used for intersite filtering in MPLS VPN PE-to-CE topologies.

VPN—Virtual Private Network. Allows IP traffic to travel securely over public TCP/IP networks and the Internet by encapsulating and encrypting all IP packets. VPN uses a tunnel to encrypt all information at the IP level.

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)

Copyright © 2004, 2005 Cisco Systems, Inc. All rights reserved.

