Add Path Support in EIGRP

The Add Path Support in EIGRP feature enables hubs in a single Dynamic Multipoint VPN (DMVPN) domain to advertise multiple best paths to connected spokes when the Enhanced Interior Gateway Routing Protocol (EIGRP) is the routing protocol between the hubs and the spokes. This module provides information about the Add Path Support in EIGRP feature and explains how to configure it.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Add Path Support in EIGRP

All interfaces in an Enhanced Interior Gateway Routing Protocol (EIGRP) topology are by default configured with the **next-hop-self** command. This command enables EIGRP to set the local outbound interface as the next-hop value while advertising a route to a peer, even when advertising routes out of the interface on which the routes were learned. This default EIGRP behavior may interfere with the **add-paths**command that helps configure the Add Path Support in EIGRP feature. Therefore, before you configure this feature on a hub device in a Dynamic Multipoint VPN (DMVPN) domain, you must disable the **next-hop-self** command that is configured on the hub interface that connects to spokes in the DMVPN domain.

Restrictions for Add Path Support in EIGRP

- The Add Path Support in EIGRP feature can be enabled only in Enhanced Interior Gateway Routing Protocol (EIGRP) named mode configurations.
- The **variance** command should not be configured when the Add Path Support in EIGRP feature is enabled. The **variance** command alters the metrics of routes in an EIGRP topology, thereby enabling EIGRP to balance traffic among desired paths. Therefore, if you configure the **variance** command on a hub device, the command may interfere with the configuration of this feature.

Information About Add Path Support in EIGRP

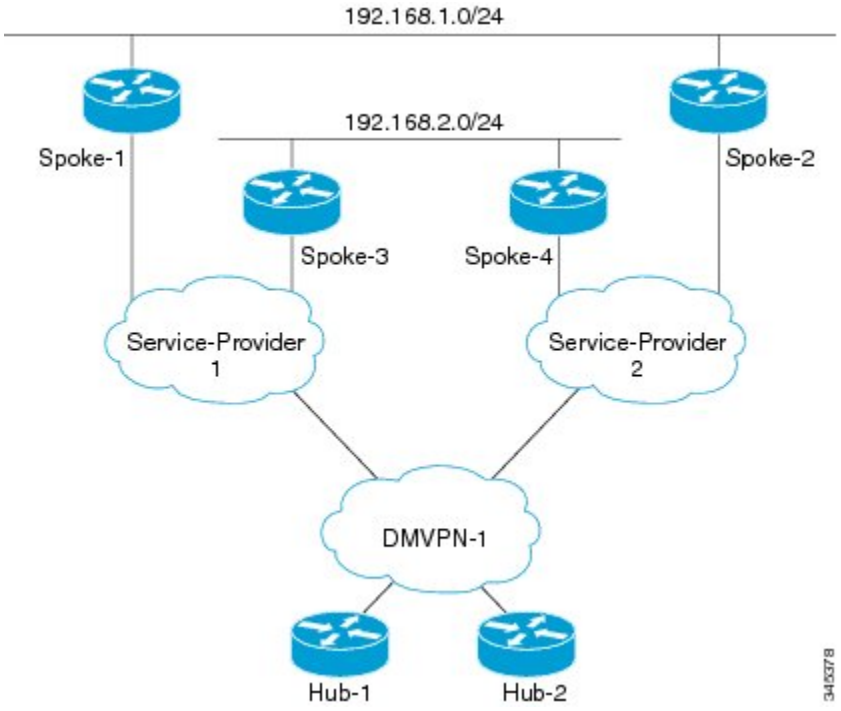
EIGRP Add Path Support Overview

In most Dynamic Multipoint VPN (DMVPN) domains, two or more spokes are connected to the same LAN segment. These spokes connect to more than one hub (for hub redundancy) through different service providers (for service-provider redundancy). In a single DMVPN domain, a hub connects to all spokes through one tunnel interface. In Enhanced Interior Gateway Routing Protocol (EIGRP) topologies, when a hub has more than one path (with the same metric but through different spokes) to reach the same network, both paths are chosen as best paths. However, by default, EIGRP advertises only one path as the best path to connected spokes. With the implementation of the Add Path Support in EIGRP feature, hubs in an EIGRP-DMVPN domain can advertise up to four additional best paths to connected spokes, thereby allowing load balancing and path redundancy. This feature supports both IPv4 and IPv6 configurations.

How Add Path Support in EIGRP Works

A typical single Dynamic Multipoint VPN (DMVPN) domain consists of dual hubs (for hub redundancy) connected to more than one service provider (for service-provider redundancy). In the figure below, two hub devices—Hub-1 and Hub-2—are connected through tunnel interfaces to a DMVPN domain.

Figure 1: Single DMVPN Domain



The DMVPN domain is in turn connected to two service providers—Service-Provider 1 and Service-Provider 2. Four spoke devices in this DMVPN domain—Spoke-1, Spoke-2, Spoke-3, and Spoke-4. Spoke-1 and Spoke-3 are connected to Service-Provider 1, and Spoke-2 and Spoke-4 are connected to Service-Provider 2. The Enhanced Interior Gateway Routing Protocol (EIGRP) is the routing protocol between the hubs and the spokes over the tunnel interfaces.

Spoke-1 and Spoke-2 are connected to a LAN with the network address 192.168.1.0/24. Both these spokes are connected to both the hubs through two different service providers, and hence, these spokes advertise the same LAN network to both hubs. Typically, spokes on the same LAN advertise the same metric; therefore, based on the metric, Hub-1 and Hub-2 have dual Equal-Cost Multipath (ECMP) routes to reach network 192.168.1.0/24. However, because EIGRP is a distance vector protocol, it advertises only one best path to the destination. Therefore, in this EIGRP-DMVPN domain, the hubs advertise only one route (for example, through Spoke-1) to reach network 192.168.1.0/24. When clients in subnet 192.168.2.0/24 communicate with clients in subnet 192.168.1.0/24, all traffic is directed to Spoke-1. Because of this default EIGRP behavior, there is no load balancing on Spoke-3 and Spoke-4. Additionally, if Spoke-1 fails or if the network of Service-Provider 1 goes down, EIGRP must reconverge to provide connectivity to 192.168.1.0/24.

The Add Path Support in EIGRP feature enables EIGRP to advertise up to four additional paths to connected spokes in a single DMVPN domain. If you configure this feature in the example topology discussed above, both Spoke-1 and Spoke-2 will be advertised to Spoke-3 and Spoke-4 as best paths to network 192.168.1.0, thereby allowing load balancing among all spokes in this DMVPN domain.

How to Configure Add Path Support in EIGRP

Configuring IPv4 Add Path Support on a Hub

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 autonomous-system** *as-number*
5. **af-interface** {**default** | *interface-type interface-number*}
6. **no next-hop-self** [**no-ecmp-mode**]
7. **add-paths** *number*
8. **end**
9. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name`	Configures an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process and enters router configuration mode.
Step 4	**address-family ipv4 autonomous-system** *as-number* **Example:** `Device(config-router)# address-family ipv4 autonomous-system 3`	Enters address family configuration mode and configures an EIGRP routing instance.
Step 5	**af-interface** {**default** | *interface-type interface-number*} **Example:** `Device(config-router-af)# af-interface tunnel 0`	Enters address family interface configuration mode and configures interface-specific EIGRP commands.

	Command or Action	Purpose
Step 6	**no next-hop-self** [**no-ecmp-mode**] **Example:** `Device(config-router-af-interface)# no next-hop-self no-ecmp-mode`	Instructs EIGRP to use the received next hop and not the local outbound interface address as the next hop to be advertised to neighboring devices.
Step 7	**add-paths** *number* **Example:** `Device(config-router-af-interface)# add-paths 4`	Enables EIGRP to advertise multiple paths as best paths to connected spokes in a single Dynamic Multipoint VPN (DMVPN) domain.
Step 8	**end** **Example:** `Device(config-router-af-interface)# end`	Exits address family interface configuration mode and returns to privileged EXEC mode.
Step 9	**show running-config** **Example:** `Device# show running-config | section eigrp`	Displays contents of the current running configuration file. • Use the output modifier "|" to display the EIGRP section of the running configuration, and to verify whether the **add-paths** command is enabled in the configuration.

Configuring IPv6 Add Path Support on a Hub

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **router eigrp** *virtual-name*
5. **address-family ipv6 autonomous-system** *as-number*
6. **af-interface** {**default** | *interface-type interface-number*}
7. **no next-hop-self** [**no-ecmp-mode**]
8. **add-paths** *number*
9. **end**
10. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 4	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name`	Configures an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process and enters router configuration mode.
Step 5	**address-family ipv6 autonomous-system** *as-number* **Example:** `Device(config-router)# address-family ipv6 autonomous-system 3`	Enters address family configuration mode and configures an EIGRP routing instance.
Step 6	**af-interface** {**default** | *interface-type interface-number*} **Example:** `Device(config-router-af)# af-interface tunnel 0`	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
Step 7	**no next-hop-self** [**no-ecmp-mode**] **Example:** `Device(config-router-af-interface)# no next-hop-self no-ecmp-mode`	Instructs EIGRP to use the received next-hop address and not the local outbound interface address as the next hop to be advertised to neighboring devices.
Step 8	**add-paths** *number* **Example:** `Device(config-router-af-interface)# add-paths 4`	Enables EIGRP to advertise multiple paths as best paths to connected spokes in a single Dynamic Multipoint VPN (DMVPN) domain.
Step 9	**end** **Example:** `Device(config-router-af-interface)# end`	Exits address family interface configuration mode and returns to privileged EXEC mode.
Step 10	**show running-config** **Example:** `Device# show running-config | section eigrp`	Displays contents of the current running configuration file. • Use the output modifier "|" to display the EIGRP section of the running configuration, and to verify whether the **add-paths** command is enabled in the configuration.

Configuration Examples for Add Path Support in EIGRP

Example: Configuring IPv4 Add Path Support on a Hub

```
Device(config)# router eigrp name
Device(config-router)# address-family ipv4 autonomous-system 10
Device(config-router-af)# af-interface tunnel 0
Device(config-router-af-interface)# no next-hop-self no-ecmp-mode
Device(config-router-af-interface)# add-paths 4
Device(config-router-af-interface)# end
```

Example: Configuring IPv6 Add Path Support on a Hub

```
Device(config)# ipv6 unicast-routing
Device(config)# router eigrp name
Device(config-router)# address-family ipv6 autonomous-system 10
Device(config-router-af)# af-interface tunnel 0
Device(config-router-af-interface)# no next-hop-self no-ecmp-mode
Device(config-router-af-interface)# add-paths 4
Device(config-router-af-interface)# end
```

Additional References for Add Path Support in EIGRP

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference
EIGRP FAQ	EIGRP Frequently Asked Questions
EIGRP technology white papers	Enhanced Interior Gateway Routing Protocol

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Overview of Cisco TrustSec

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
IPv6 enablement - Inline Tagging	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.