EIGRP Over the Top

The EIGRP Over the Top feature enables a single end-to-end routing domain between two or more Enhanced Interior Gateway Routing Protocol (EIGRP) sites that are connected using a private or a public WAN connection. This module provides information about the EIGRP Over the Top feature and how to configure it.

Information About EIGRP Over the Top

EIGRP Over the Top Overview

The EIGRP Over the Top feature enables a single end-to-end Enhanced Interior Gateway Routing Protocol (EIGRP) routing domain that is transparent to the underlying public or private WAN transport that is used for connecting disparate EIGRP customer sites. When an enterprise extends its connectivity across multiple sites through a private or a public WAN connection, the service provider mandates that the enterprise use an additional routing protocol, typically the Border Gateway Protocol (BGP), over the WAN links to ensure end-to-end routing. The use of an additional protocol causes additional complexities for the enterprise, such as additional routing processes and sustained interaction between EIGRP and the routing protocol to ensure connectivity, for the enterprise. With the EIGRP Over the Top feature, routing is consolidated into a single protocol (EIGRP) across the WAN, which provides the following benefits:

- There is no dependency on the type of WAN connection used.
- There is no dependency on the service provider to transfer routes.
- There is no security threat because the underlying WAN has no knowledge of enterprise routes.
- This feature simplifies dual carrier deployments and designs by eliminating the need to configure and manage EIGRP-BGP route distribution and route filtering between customer sites.
- This feature allows easy transition between different service providers.
- This feature supports both IPv4 and IPv6 environments.

How EIGRP Over the Top Works

The EIGRP Over the Top solution can be used to ensure connectivity between disparate Enhanced Interior Gateway Routing Protocol (EIGRP) sites. This feature uses EIGRP on the control plane and Locator ID Separation Protocol (LISP) encapsulation on the data plane to route traffic across the underlying WAN architecture. EIGRP is used to distribute routes between customer edge (CE) devices within the network, and the traffic forwarded across the WAN architecture is LISP encapsulated. Therefore, to connect disparate EIGRP sites, you must configure the **neighbor** command with LISP encapsulation on every CE in the network.

If your network has many CEs, then you can use EIGRP Route Reflectors (E-RRs) to form a half-mesh topology and ensure connectivity among all CEs in the network. An E-RR is an EIGRP peer that receives EIGRP route updates from CEs in the network and reflects these updates to other EIGRP CE neighbors without changing the next hop or metrics for the routes. An E-RR can also function as a CE in the network. You must configure E-RRs with the **remote-neighbors source** command to enable E-RRs to listen to unicast messages from peer CE devices and reflect the messages to other EIGRP CE neighbors. You must configure the CEs with the **neighbor** command to allow them to identify the E-RRs in their network and exchange routes with the E-RRs. Upon learning routes from E-RRs, the CEs install these routes into their routing information base (RIB). You can use dual or multiple E-RRs for redundancy. The CEs form adjacencies with all E-RRs configured in the network, thus enabling multihop remote neighborship amongst themselves.

Security Groups and SGTs

A security group is a grouping of users, endpoint devices, and resources that share access control policies. Security groups are defined by the administrator in the ACS. As new users and devices are added to the Cisco TrustSec (CTS) domain, the authentication server assigns these new entities to appropriate security groups. CTS assigns to each security group a unique 16-bit security group number whose scope is global within a CTS domain. The number of security groups in the router is limited to the number of authenticated network entities. Security group numbers do not need to be manually configured.

Once a device is authenticated, CTS tags any packet that originates from that device with an SGT that contains the security group number of the device. The packet carries this SGT throughout the network within the CTS header. The SGT is a single label that determines the privileges of the source within the entire CTS domain. The SGT is identified as the source because it contains the security group of the source. The destination device is assigned a destination group tag (DGT).

Note The CTS packet tag does not contain the security group number of the destination device.

EIGRP OTP Support to Propagate SGT

The EIGRP OTP Support enables to propagate SGT from site-to-site across WAN using OTP transport. OTP uses LISP to send the data traffic. OTP carries the SGT over the Layer 3 (L3) clouds across multiple connections/network and also provides access control at a remote site.

How to Configure EIGRP Over the Top

Configuring EIGRP Over the Top on a CE Device

You must enable the EIGRP Over the Top feature on all customer edge (CE) devices in the network so that the CEs know how to reach the Enhanced Interior Gateway Routing Protocol (EIGRP) Route Reflector configured in the network. Perform the following task to configure the EIGRP Over the Top feature on a CE device and enable Locator ID Separation Protocol (LISP) encapsulation for traffic across the underlying WAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 autonomous-system** *as-number*
5. **neighbor**{*ip-address* | *ipv6-address*} *interface-type interface-number* [**remote** *maximum-hops* [**lisp-encap** [*lisp-id*]]]
6. **network** *ip-address*[*wildcard-mask*]
7. **end**

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 test`	Configures an 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 100`	Enters address family configuration mode and configures an EIGRP routing instance.
Step 5	**neighbor**{*ip-address* | *ipv6-address*} *interface-type interface-number* [**remote** *maximum-hops* [**lisp-encap** [*lisp-id*]]]	Defines a neighboring device with which an EIGRP device can exchange routing information.

	Command or Action	Purpose
	Example: `Device(config-router-af)# neighbor 10.0.0.1 gigabitethernet 0/0/1 remote 2 lisp-encap 1`	
Step 6	**network** *ip-address*[*wildcard-mask*] **Example:** `Device(config-router-af)# network 192.168.0.0 255.255.0.0`	Specifies the network for the EIGRP routing process. In this case, configure all routes that the CE needs to be aware of.
Step 7	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.

Configuring EIGRP Route Reflectors

Perform this task to configure a customer edge (CE) device in a network to function as an Enhanced Interior Gateway Routing Protocol (EIGRP) Route Reflector.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 unicast autonomous-system** *as-number*
5. **af-interface** *interface-type interface-number*
6. **no next-hop-self**
7. **no split-horizon**
8. **exit**
9. **remote-neighbors source** *interface-type interface-number* **unicast-listen lisp-encap**
10. **network** *ip-address*
11. **end**

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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp test`	Configures an EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv4 unicast autonomous-system** *as-number* **Example:** `Device(config-router)# address-family ipv4 unicast autonomous-system 100`	Enters address family configuration mode and configures an EIGRP routing instance.
Step 5	**af-interface** *interface-type interface-number* **Example:** `Device(config-router-af)# af-interface gigabitethernet 0/0/1`	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
Step 6	**no next-hop-self** **Example:** `Device(config-router-af-interface)# no next-hop-self`	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. **Note** If **no next-hop-self** is not configured, the data traffic will flow through the EIGRP Route Reflector.
Step 7	**no split-horizon** **Example:** `Device(config-router-af-interface)# no split-horizon`	Disables EIGRP split horizon.
Step 8	**exit** **Example:** `Device(config-router-af-interface)# exit`	Exits address family interface configuration mode and returns to address family configuration mode.
Step 9	**remote-neighbors source** *interface-type interface-number* **unicast-listen lisp-encap** **Example:** `Device(config-router-af)# remote-neighbors source gigabitethernet 0/0/1 unicast-listen lisp-encap`	Enables remote neighbors to accept inbound connections from any remote IP address.
Step 10	**network** *ip-address* **Example:**	Specifies a network for the EIGRP routing process.

	Command or Action	Purpose
	`Device(config-router-af)# network 192.168.0.0`	• Enter all network routes that the EIGRP Route Reflector needs to be aware of.
Step 11	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode

Configuring EIGRP OTP Support to Propagate SGT

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual instance name*
4. **address-family ipv4 autonomous-system** *as-number*
5. **topology base**
6. **cts propagate sgt**
7. **end**

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 instance name* **Example:** `Device (config)# router eigrp kmd`	Configures an 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 100`	Enters address family configuration mode and configures an EIGRP routing instance.
Step 5	**topology base** **Example:** `Device (config-router-af)# topology base`	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

	Command or Action	Purpose
Step 6	**cts propagate sgt** **Example:** `Device (config-router-af)# cts propagate sgt`	Enables Security Group Tag (SGT) propagation over L3 network.
Step 7	**end** **Example:** `Device (config-router-af)# end`	Exits address family topology configuration mode and returns to privileged EXEC mode.

Configuration Examples for EIGRP Over the Top

Example: Configuring EIGRP Over the Top on a CE Device

The following example shows you how to configure the customer edge (CE) device in the network to advertise local routes to the Enhanced Interior Gateway Routing Protocol (EIGRP) Route Reflectors.

```
Device> enable
Device# configure terminal
Device(config)# router eigrp test
Device(config-router)# address-family ipv4 unicast autonomous-system 100
Device(config-router-af)# neighbor 10.0.0.2 gigabitethernet 0/0/1 remote 3 lisp-encap 1
Device(config-router-af)# network 192.168.0.0
Device(config-router-af)# network 192.168.1.0
Device(config-router-af)# network 192.168.2.0
Device(config-router-af)# end
```

Example: Configuring EIGRP Route Reflectors

```
Device> enable
Device# configure terminal
Device(config)# router eigrp test
Device(config-router)# address-family ipv4 unicast autonomous-system 100
Device(config-router-af)# af-interface gigabitethernet 0/0/1
Device(config-router-af-interface)# no next-hop-self
Device(config-router-af-interface)# no split-horizon
Device(config-router-af-interface)# exit
Device(config-router-af)# remote-neighbors source gigabitethernet 0/0/1 unicast-listen
lisp-encap 1
Device(config-router-af)# network 192.168.0.0
Device(config-router-af)# end
```

Example: Configuring EIGRP OTP Support to Propagate SGT

The following example shows how to configure EIGRP OTP to propagate SGT.

```
router eigrp kmd
!
address-family ipv4 unicast autonomous-system 100
  !
  topology base
   cts propagate sgt
  exit-af-topology
exit-address-family
```

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.