EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary routing protocol that:

- is an open-standard Interior Gateway Protocol (IGP),
- is an enhancement to the original Interior Gateway Routing Protocol (IGRP) developed by Cisco,
- does not fully update if there are no changes in the network, which reduces flooding activities in other IGPs.

EIGRP is supported only on Cisco IOS XE Catalyst SD-WAN devices. For more information, see Introduction to EIGRP.

Benefits of EIGRP

EIGRP provides several advantages that enhance network performance and simplify management for network administrators.

These are the key benefits of using EIGRP:

- Increased network width: EIGRP supports an increased network width from 15 to 100 hops.
- Fast convergence: EIGRP provides fast convergence.
- Incremental updates: EIGRP uses incremental updates, which minimizes bandwidth consumption.
- Protocol-independent neighbor discovery: EIGRP supports protocol-independent neighbor discovery.
- Easy scaling: EIGRP is designed for easy scaling.

EIGRP restrictions

When implementing EIGRP, note these limitations and restrictions

- EIGRP is not supported on the transport side network on Cisco IOS XE Catalyst SD-WAN devices.

- EIGRP route match is not supported in Cisco Catalyst SD-WAN Controller centralized control policy.

Configure EIGRP

Use this task to set up EIGRP for routing in Cisco Catalyst SD-WAN, enabling efficient and scalable routing across your overlay.

You can EIGRP using Cisco SD-WAN Manager templates, configuration groups, or directly via the CLI on Cisco IOS XE Catalyst SD-WAN devices.

Before you begin

Follow one of these steps to configure EIGRP:

Procedure

Step 1 Configure EIGRP using Cisco SD-WAN Manager templates.

This method involves creating a reusable EIGRP feature template in Cisco SD-WAN Manager, which defines the basic EIGRP parameters such as the autonomous system ID, and specifies how routes are redistributed. This template can then be applied to multiple devices. For more information, see Configure EIGRP using Cisco SD-WAN Manager, on page 2.

Step 2 Configure EIGRP using a configuration group.

This method applies EIGRP configurations within a service profile using configuration groups in Cisco SD-WAN Manager, suitable for service-side routing within specific VPNs. For more information, see Configure EIGRP using a configuration group, on page 4.

Step 3 Configure EIGRP using CLI.

This method involves directly entering EIGRP configuration commands on the Cisco IOS XE Catalyst SD-WAN device's command-line interface, providing granular control over the configuration.

What to do next

After configuring EIGRP, verify the configuration using the appropriate `show` commands on the device. For example, `show ip route vrf <vpn-id>` for IPv4 EIGRP routes. For more information, see Verification commands for EIGRP configuration, on page 6.

Configure EIGRP using Cisco SD-WAN Manager

Use this task to configure the EIGRP routing protocol using the EIGRP feature template in Cisco SD-WAN Manager.

This template defines the basic EIGRP parameters, such as the autonomous system ID. It also specifies how routes are redistributed. You can apply this template to multiple devices.

Before you begin

Follow these steps to create an EIGRP template:

Procedure

Step 1 From the Cisco SD-WAN Managermenu, choose **Configuration** > **Templates** > **Feature Templates**.

Step 2 Click **Add Template** and select a device from the list.

Step 3 From the **Other Templates** section, choose **EIGRP** and enter a name and a description for the template.

Step 4 Click **Basic Configuration** to configure the local autonomous system number for the template.

a) In the **Autonomous System ID** field, enter the local AS number (Range: 1-65,535).

Step 5 To redistribute routes from one protocol into an EIGRP routing domain, click **New Redistribute** under **IP4 Unicast Address Family** and enter the following parameter values:

a) Select **Mark as Optional Row**.

This action marks the configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.

b) Choose the **Protocol** from which to redistribute routes into EIGRP (e.g., **omp**, **connected**, **static**, **ospf**, **bgp**, **nat-route**).

c) Enter the name of the **Route Policy** to apply to redistributed routes.

d) Click **Add** to save the redistribution information.

Step 6 To advertise a prefix into the EIGRP routing domain, click **Network**, then click **New Network** and enter the following parameter values:

a) Select **Mark as Optional Row**.

This action marks the configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.

b) In the **Network Prefix** field, enter the network prefix you want EIGRP to advertise in the format of prefix/mask.

c) Click **Add** to save the network prefix.

Step 7 To configure advanced parameters for EIGRP, click **Advanced** and configure the following parameter values:

a) In the **Hold Time (seconds)** field, set the interval after which EIGRP considers a neighbor to be down (Range: 0-65,535, Default: 15 seconds).

b) In the **Hello Interval (seconds)** field, set the interval at which the router sends EIGRP hello packets (Range: 0-65,535, Default: 5 seconds).

c) In the **Route Policy Name** field, enter the name of an EIGRP route policy.

Step 8 To configure authentication for EIGRP routes click **Authentication**:

a) Click **Authentication**

b) Choose **global** in the **Authentication Key** drop-down list, and then choose **md5** or **hmac-sha-256**.

- For **MD5**: Enter an **MD5 Key ID** and **MD5 Authentication Key**.
- For **HMAC-SHA-256:** Enter an Authentication Key.

c) Click **Add** to save the authentication parameters.

Note
To use a preferred route map, specify both an MD5 key (ID or auth key) and a route map.

Step 9 To configure interface parameters for EIGRP routes, click **Interface**, and enter the following parameter values:

a) Select **Mark as Optional Row**.

This action marks the configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.

b) In the **Interface name** field, enter the interface name(s) on which EIGRP should run.

c) Set **Shutdown** to **No** (default) to enable the interface to run EIGRP, or **Yes** to disable it.

d) Click **Add** to save the interfaces.

An EIGRP feature template is created, ready to be applied to devices.

What to do next

When the configuration has been applied to the devices, verify the EIGRP configuration using the appropriate `show` commands on the device. For example, `show ip route vrf <vpn-id>` for IPv4 EIGRP routes. For more information, see Verification commands for EIGRP configuration, on page 6.

Configure EIGRP using a configuration group

Use this task to apply EIGRP configurations within a service profile using configuration groups in Cisco SD-WAN Manager.

This method is suitable for service-side routing within specific VPNs and leverages configuration groups for simplified management.

Before you begin

Follow these steps to configure EIGRP routing in a service profile:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Configure an EIGRP Routing feature in a Service Profile.

Step 3 Configure basic settings.

a) In the **Autonomous System ID** field, enter the local autonomous system (AS) number (Range: 1-65535).

b) For Network: Enter the IP address and subnet mask.

c) For Interface:

1. Select one of the **Protocol** options from which to redistribute routes into EIGRP (e.g., bgp, connected, nat-route, omp, ospf, ospfv3, static).

Note
From Cisco IOS XE Catalyst SD-WAN Release 16.12.1b and later, you can set metric values for redistribution by using the CLI add-on feature template. Use the following command:

```
redistribute ospf 1 metric 1000000 1 1 1 1500
```

For more information, see *CLI Add-on Feature Templates*. .

2. Enter the name of the Route Policy to apply to redistributed routes.

d) Configure IPv4 unicast address family:

1. Click **Add Interface**.
2. Provide a value for the **AF Interface**.
3. Set **Shutdown** to OFF (default) to enable the interface, or ON to disable it.
4. (Optional) Click **Add Summary Address** and enter an IPv4 address and choose a subnet mask.

e) Configure authentication:

1. **MD5 ID**
   - **MD5 key ID**: Enter an MD5 key ID to compute an MD5 hash over the contents of the EIGRP packet using that value.
   - **MD5 Authentication Key**: Enter an MD5 authentication key to use an encoded MD5 checksum in the transmitted packet.
   - **Authentication Key**: A 256-byte unique key that is used to compute the Hashed Message Authentication Code (HMAC) and is known both by the sender and the receiver of the message.
2. **HMAC-SHA-256**: A 256-byte unique key that is used to compute the Hashed Message Authentication Code (HMAC) and is known both by the sender and the receiver of the message.

f) Configure advanced settings:

1. In the **Hold Time (seconds)** field, set the interval after which EIGRP considers a neighbor to be down. Specify a value in the range of 0-65535. The default is 15 seconds.
2. In the **Hello Interval (seconds)** field, set the interval at which the router sends EIGRP hello packets. Specify a value between 0 and 65535. The default is 5 seconds.
3. In the **Route Policy** field, enter the name of an EIGRP route policy.
4. Toggle **Filter** to **ON**. This filters routes that do not match the policy.

EIGRP routing is configured within the specified service profile, ready for deployment.

What to do next

Verify the EIGRP configuration using the appropriate `show` commands on the device. For example, `show ip route vrf <vpn-id>` for IPv4 EIGRP routes. For more information, see Verification commands for EIGRP configuration, on page 6.

Configure EIGRP using CLI

You can use this task to configure EIGRP parameters directly on Cisco IOS XE Catalyst SD-WAN devices via the command-line interface.

Before you begin

To configure EIGRP using the CLI, complete these steps:

Procedure

Step 1 Configure EIGRP on Cisco IOS XE Catalyst SD-WAN devices using these commands:

```
config-transaction
router eigrp vpn
 !
 address-family ipv4 unicast vrf 1 autonomous-system 100
  !
  topology base
   table-map foo filter
   redistribute omp
  exit-af-topology
  network 10.1.44.0 255.0.0.0
 exit-address-family
 !
 address-family ipv6 unicast vrf 1 autonomous-system 200
  !
  topology base
   table-map bar
   redistribute omp
  exit-af-topology
 exit-address-family
!
```

Step 2 (Optional) To advertise EIGRP routes to OMP, use these commands:

```
config-transaction
sdwan
 omp
  no shutdown
  graceful-restart
  address-family ipv4 vrf 1
   advertise eigrp
  !
  address-family ipv6 vrf 1
   advertise eigrp
  !
  address-family ipv4
   advertise connected
   advertise static
  !
 !
```

EIGRP is configured on the Cisco IOS XE Catalyst SD-WAN device via CLI.

Verification commands for EIGRP configuration

This section details the essential verification commands used to verify the EIGRP configuration on Cisco IOS XE Catalyst SD-WAN devices.

View IPv4 EIGRP routes

Use the `show ip route vrf <vpn-id>` command to view IPv4 EIGRP routes for a specific VRF.

```
Device# show ip route vrf 1
m        192.168.22.22 [251/0] via 192.168.11.12, 00:28:00
      192.168.55.0/32 is subnetted, 1 subnets
D EX     192.168.55.55 [170/1] via 10.1.44.2, 00:33:58, GigabitEthernet3.2
      192.168.66.0/32 is subnetted, 1 subnets
B        192.168.66.66 [20/0] via 192.168.1.3, 00:33:57
      192.168.1.0/32 is subnetted, 3 subnets
D EX     192.168.1.3 [170/1] via 10.1.44.2, 00:33:58, GigabitEthernet3.2
m        192.168.1.33 [251/0] via 192.168.11.14 (3), 00:28:01
```

View IPv6 EIGRP routes

Use the `show ip route vrf <vpn-id>` command to view IPv6 EIGRP routes for a specific VRF.

```
Device# show ipv6 route vrf 1
C   300:4::/64 [0/0]
     via GigabitEthernet3.2, directly connected
L   300:4::1/128 [0/0]
     via GigabitEthernet3.2, receive
D   2000:1:3::1/128 [90/1]
     via FE80::20C:29FF:FEF5:C767, GigabitEthernet3.2
L   FF00::/8 [0/0]
     via Null0, receive
cEdge4-Naiming#show ipv6 route vrf 1 2000:1:3::1/128
Routing entry for 2000:1:3::1/128
  Known via "eigrp 200", distance 90, metric 1
  OMP Tag 888, type internal
  Redistributing via omp
  Route count is 1/1, share count 0
  Routing paths:
    FE80::20C:29FF:FEF5:C767, GigabitEthernet3.2
      From FE80::20C:29FF:FEF5:C767
      Last updated 00:22:06 ago
```

View OMP routes in EIGRP

Use the `show eigrp address-family ipv4 vrf <vpn-id> topology <ipv4-prefix>` command to view OMP routes that have been redistributed into EIGRP for a specific VRF and IPv4 prefix.

```
Device# show eigrp address-family ipv4 vrf 1 topology 192.168.44.4/24
EIGRP-IPv4 VR(vpn) Topology Entry for AS(100)/ID(192.168.1.44)
           Topology(base) TID(0) VRF(1)
EIGRP-IPv4(100): Topology base(0) entry for 192.168.44.4/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 1
  Descriptor Blocks:
  192.168.1.5, from Redistributed, Send flag is 0x0
      Composite metric is (1/0), route is External
      Vector metric:
        Minimum bandwidth is 0 Kbit
        Total delay is 0 picoseconds
        Reliability is 0/255
        Load is 0/255
        Minimum MTU is 0
        Hop count is 0
        Originating router is 192.168.1.44
      External data:
        AS number of route is 0
        External protocol is OMP-Agent, external metric is 4294967294
        Administrator tag is 0 (0x00000000)
```