# Implementing EIGRP Route Manipulations
# Created by Mark Johnson

This document is prepared exclusively for the Cisco Routing & Switching CCIE® Certification on the Cisco Learning Network (CLN). This document addresses configuration, verification, and troubleshooting of the two more recent new features added for the Enhanced Interior Gateway Routing Protocol (EIGRP).

The two new EIGRP features to be covered in this document are as follows:

- Route map filtering
- Leaking routes

## Route Map Filtering

EIGRP support for route map filtering, added in Cisco IOS Release 12.3(8)T and in later Cisco IOS code, enables EIGRP to filter inbound and outbound traffic based on route map options. New match options allow EIGRP to filter internal and external routes based on source protocols, to match a metric against a range, and to match on an external protocol metric. You can filter routes that are dynamically received from, or advertised to, EIGRP peers by adding a route map option to the **distribute-list** or the **redistribute** command.

### Configuration

The use of route maps is quite extensive; this document assumes that you are generally familiar with the usage and general configuration syntax of route maps.

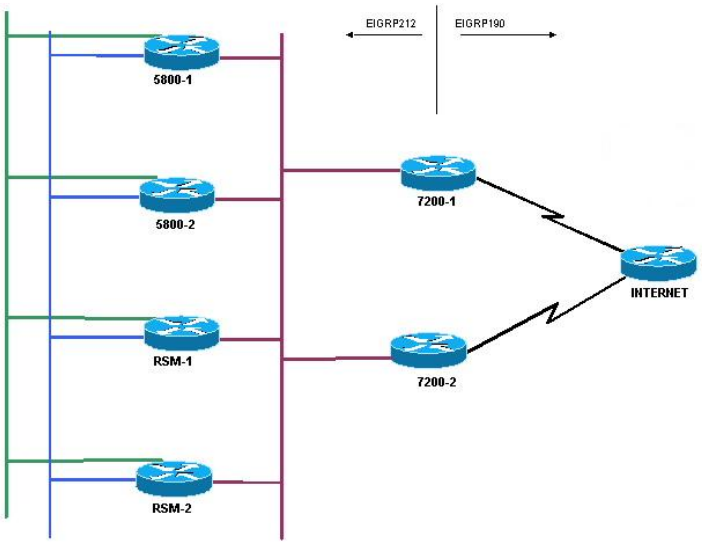


**Figure 1**

The topology used here to demonstrate route map filtering for EIGRP is shown in Figure 1. There are two distinct EIGRP processes in this network topology, with redistribution between the two at the parallel 7200s. The routing configuration portion of either 7200 is as follows:

```
router eigrp 190
 redistribute eigrp 212
 network 191.0.0.0 0.0.0.3
 no auto-summary
!
router eigrp 212
 redistribute eigrp 190
 network 212.50.185.96 0.0.0.31
 no auto-summary
```

Assume that the downstream devices in the EIGRP 212 AS do not need to learn all the routes to the Internet, but that instead, it would suffice for a default route to be sent down from the 7200s with the ability to expand the list of networks passed on at a later date. Route map filtering would be one solution to consider.

To filter outbound EIGRP traffic and updates using route maps at the 7200, you would need to add the following commands to both 7200s:

```
access-list 101 permit ip any host 0.0.0.0
!
route-map import_only_internet_default_route permit 10
  match ip address 101
!
router eigrp 212
  redistribute eigrp 190 route-map import_only_internet_default_route
```

 

**Verification**

There are a few show commands that you could refer to for verification of the effect of the route map filter at the downstream devices. The commands **show ip route summary** and **show ip eigrp topology summary** are used here to illustrate the effect.

Before adding the route map, you see the following command output at the downstream devices:

5800-2#**show ip route summary**
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 16

| Route Source | Networks | Subnets | Overhead | Memory (bytes) |
|---|---|---|---|---|
| Connected | 0 | 5 | 360 | 680 |
| static | 0 | 0 | 0 | 0 |
| eigrp 212 | 15 | 6 | 2808 | 2856 |
| internal | 5 | | | 5780 |
| Total | 20 | 11 | 3168 | 9316 |

5800-2#**show ip eigrp topology summary**
IP-EIGRP Topology Table for AS(212)/ID(212.50.167.20)
Head serial 1, next serial 656
26 routes, 0 pending replies, 0 dummies
IP-EIGRP(0) enabled on 6 interfaces, 6 neighbors present on 2 interfaces
Quiescent interfaces: Et1/0 Et2/0

After adding the route map commands and applying them to the redistribution on both 7200s, you again review the same show command output; pay attention to the content highlighted in blue.

5800-2#**show ip route summary**
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 16

| Route Source | Networks | Subnets | Overhead | Memory (bytes) |
|---|---|---|---|---|
| connected | 0 | 5 | 360 | 680 |
| static | 0 | 0 | 0 | 0 |
| eigrp 212 | 2 | 3 | 504 | 680 |
| internal | 2 | | | 2312 |
| Total | 4 | 8 | 864 | 3672 |

5800-2#**show ip eigrp topology summary**
IP-EIGRP Topology Table for AS(212)/ID(212.50.167.20)
Head serial 1, next serial 784
10 routes, 0 pending replies, 0 dummies
IP-EIGRP(0) enabled on 6 interfaces, 6 neighbors present on 2 interfaces
Quiescent interfaces: Et1/0 Et2/0

On 5800-2 the savings in this simple example is 13 fewer networks and 3 fewer subnets (16 fewer routes overall) in the routing table, for a savings of 2304 bytes of overhead (additional memory involved in allocating the routes for the particular route source other than the memory specified in the Memory field) and 2176 bytes saved in other memory. This does not address the additional savings in processing on both the 7200s and 5800s.

This example is quite simple but still demonstrates how to configure and verify route map filtering for EIGRP, while also indicating the types of savings in memory and processing that one can leverage.

### Troubleshooting

If the outbound filtering is not behaving as expected at the downstream devices, the best item to check is the configuration.

## Leaking Routes

EIGRP support for leaking routes introduces the capability to advertise a component route of a manual summary address that would otherwise be suppressed. This new feature is available in Cisco IOS Release 12.3(14)T and later.

As background, since Cisco IOS Release 12.2(8)T, EIGRP does *not* autosummarize subnet routes into network-level routes by default; to enable this automatic summarization of subnet routes into network-level routes, you must configure the **auto-summary** command under the EIGRP process.

Additionally, you can configure a *summary aggregate address* for a specified interface for EIGRP (by default, summary aggregate addresses are not predefined) at any bit level. EIGRP summary routes are given an administrative distance value of 5; this metric is used to advertise a summary without actually installing it in the routing table. You can enable this manual summarization by using the **ip summary-address eigrp AS x.x.x.x mask** interface command.

For this scenario you again use the topology shown in Figure 1.

First, you enable subnet summarization with the **auto-summary** command. On the downstream router 5800-2, you are learning about six unique 10.0.0.0 subnets from the Internet:

```
5800-2#show ip route 10.0.0.0
Routing entry for 10.0.0.0/24, 6 known subnets
  Redistributing via eigrp 212

D EX    10.10.10.0 [170/2306816] via 212.50.185.66, 00:00:25, Ethernet1/0
                   [170/2306816] via 212.50.185.65, 00:00:25, Ethernet1/0
D EX    10.11.11.0 [170/2306816] via 212.50.185.66, 00:00:25, Ethernet1/0
                   [170/2306816] via 212.50.185.65, 00:00:25, Ethernet1/0
D EX    10.14.14.0 [170/2306816] via 212.50.185.66, 00:00:25, Ethernet1/0
                   [170/2306816] via 212.50.185.65, 00:00:25, Ethernet1/0
D EX    10.15.15.0 [170/2306816] via 212.50.185.66, 00:00:25, Ethernet1/0
                   [170/2306816] via 212.50.185.65, 00:00:25, Ethernet1/0
D EX    10.12.12.0 [170/2306816] via 212.50.185.66, 00:00:25, Ethernet1/0
                   [170/2306816] via 212.50.185.65, 00:00:25, Ethernet1/0
D EX    10.13.13.0 [170/2306816] via 212.50.185.66, 00:00:25, Ethernet1/0
                   [170/2306816] via 212.50.185.65, 00:00:25, Ethernet1/0
```

After enabling **auto-summary** on the upstream 7200 routers, 5800-2 now knows only about the 10.0.0.0 network-level route:

```
5800-2#show ip route 10.0.0.0
Routing entry for 10.0.0.0/8, 1 known subnets
  Redistributing via eigrp 212

D EX    10.0.0.0 [170/2306816] via 212.50.185.66, 00:00:04, Ethernet1/0
                 [170/2306816] via 212.50.185.65, 00:00:04, Ethernet1/0
```

As an aside, the same reaction could be controlled more granularly per interface with the command **ip summary-addr eigrp 190 10.0.0.0 255.0.0.0** on the serial interface of the same upstream 7200 routers.

**Configuration**

Given the preceding summarization, you now configure the 10.11.11.0/24 subnet to be leaked through the 10.0.0.0 summary address. The relevant configuration of the upstream 7200 routers are as follows:

```
router eigrp 190
!
access-list 11 permit 10.11.11.0 0.0.0.255
!
route-map LEAK-10-11-11 permit 10
  match ip address 11
!
interface Serial 1/0
  ip summary-address eigrp 190 10.0.0.0 255.0.0.0 leak-map LEAK-10-11-11
!
interface Serial 2/0
  ip summary-address eigrp 190 10.0.0.0 255.0.0.0 leak-map LEAK-10-11-11
```

Note that the keyword **leak-map** is configured to reference a nonexistent route map; the configuration of this keyword has no effect. The summary address is advertised while all component routes are suppressed. However, if the keyword **leak-map** is configured to reference a configured route map but the access list does not exist or the route map does not reference the access list, the summary address *and all subnet routes* are sent.

**Verification**

Before enabling the 10.11.11.0 leaky route, the summarization resulted in a single network-level 10.0.0.0 address being installed on the downstream 5800-2:

```
5800-2#show ip route 10.0.0.0
Routing entry for 10.0.0.0/8, 1 known subnets
  Redistributing via eigrp 212

D EX    10.0.0.0 [170/2306816] via 212.50.185.66, 00:00:06, Ethernet1/0
              [170/2306816] via 212.50.185.65, 00:00:06, Ethernet1/0
```

After adding the preceding leaky route configuration, you see that a new 10.0.0.0 subnet (10.11.11.0) has been installed on the downstream 5800-2, having intentionally “leaked through”:

```
5800-2#show ip route 10.0.0.0
Routing entry for 10.0.0.0/8, 2 known subnets
  Variably subnetted with 2 masks
  Redistributing via eigrp 212

D EX    10.11.11.0/24 [170/2306816] via 212.50.185.66, 00:00:11, Ethernet1/0
                [170/2306816] via 212.50.185.65, 00:00:11, Ethernet1/0
D EX    10.0.0.0/8 [170/2306816] via 212.50.185.66, 00:08:53, Ethernet1/0
              [170/2306816] via 212.50.185.65, 00:08:53, Ethernet1/0
```

 

### Troubleshooting

Again, if the route leaking is not behaving as expected at the downstream devices, the first item to check is the configuration. Next, using the **debug ip eigrp summary** command at the device leaking the route (the 7200 in the example) may help in determining where the problem lies.

7500-internet#**debug ip eigrp summary**
IP-EIGRP Summary route processing debugging is on

01:29:20: IP-EIGRP: update_configured_summary: Serial1/0 10.0.0.0/8 5 LEAK-10-11-11 1
01:29:20: IP-EIGRP: find_summary: add new sum: 10.0.0.0/8 5
01:29:20: IP-EIGRP: find_summary: add new if: Serial1/0 to 10.0.0.0/8 5
01:29:20: IP-EIGRP(Default-IP-Routing-Table:190): process_summary: 10.0.0.0/8 1
01:29:20: IP-EIGRP: update_configured_summary: Serial2/0 10.0.0.0/8 5 LEAK-10-11-11 1
01:29:20: IP-EIGRP: find_summary: add new if: Serial2/0 to 10.0.0.0/8 5
01:29:20: IP-EIGRP(Default-IP-Routing-Table:190): process_summary: 10.0.0.0/8 1
01:29:20: IP-EIGRP(Default-IP-Routing-Table:190): get_summary_metric: 10.0.0.0/8

## Conclusion

This document introduced the configuration, verification, and troubleshooting of route map filtering and leaking routes specific to the EIGRP. As is the case with many routing protocol features, it is important to understand what benefit a particular feature offers and how to correctly configure it within your network, with the goal of maximizing functionality while minimizing downtime and troubleshooting.

 