CHAPTER 7

Configuring EIGRP

This chapter describes how to configure the Enhanced Interior Gateway Routing Protocol (*EIGRP*).

This chapter includes the following sections:

Information About EIGRP

EIGRP combines the benefits of distance vector protocols with the features of link-state protocols. EIGRP sends out periodic Hello messages for neighbor discovery. Once EIGRP learns a new neighbor, it sends a one-time update of all the local EIGRP routes and route metrics. The receiving EIGRP router calculates the route distance based on the received metrics and the locally assigned cost of the link to that neighbor. After this initial full route table update, EIGRP sends incremental updates to only those neighbors affected by the route change. This process speeds convergence and minimizes the bandwidth used by EIGRP.

This section includes the following topics:

EIGRP Components

EIGRP has the following basic components:

Reliable Transport Protocol

The *Reliable Transport Protocol* guarantees ordered delivery of EIGRP packets to all neighbors. (See the "Neighbor Discovery and Recovery" section on page 7-2.) The Reliable Transport Protocol supports an intermixed transmission of multicast and unicast packets. The reliable transport can send multicast packets quickly when unacknowledged packets are pending. This provision helps to ensure that the convergence time remains low for various speed links. See the "Configuring Advanced EIGRP" section on page 7-12 for details about modifying the default timers that control the multicast and unicast packet transmissions.

The Reliable Transport Protocol includes the following message types:

- Hello—Used for neighbor discovery and recovery. By default, EIGRP sends a periodic multicast Hello message on the local network at the configured *hello interval*. By default, the hello interval is 5 seconds.
- Acknowledgement—Verify reliable reception of Updates, Queries, and Replies.
- Updates—Send to affected neighbors when routing information changes. Updates include the route destination, address mask, and route metrics such as delay and bandwidth. The update information is stored in the EIGRP topology table.
- Queries and Replies—Sent as necessary as part of the Diffusing Update Algorithm used by EIGRP.

Neighbor Discovery and Recovery

EIGRP uses the Hello messages from the Reliable Transport Protocol to discover neighboring EIGRP routers on directly attached networks. EIGRP adds neighbors to the neighbor table. The information in the neighbor table includes the neighbor address, the interface it was learned on, and the *hold time*, which indicates how long EIGRP should wait before declaring a neighbor unreachable. By default, the hold time is three times the hello interval or 15 seconds.

EIGRP sends a series of Update messages to new neighbors to share the local EIGRP routing information. This route information is stored in the EIGRP topology table. After this initial transmission of the full EIGRP route information, EIGRP sends Update messages only when a routing change occurs. These Update messages contain only the new or changed information and are sent only to the neighbors affected by the change. See the "EIGRP Route Updates" section on page 7-3'.

EIGRP also uses the Hello messages as a keepalive to its neighbors. As long as Hello messages are received, Cisco NX-OS can determine that a neighbor is alive and functioning.

Diffusing Update Algorithm

The *Diffusing Update Algorithm* (DUAL) calculates the routing information based on the destination networks in the topology table. The topology table includes the following information:

- IP address/mask—The network address and network mask for this destination.

- Successors—The IP address and local interface connection for all *feasible successors* or neighbors that advertise a shorter distance to the destination than the current *feasible distance*.
- Feasibility distance (FD)—The lowest calculated distance to the destination. The feasibility distance is the sum of the advertised distance from a neighbor plus the cost of the link to that neighbor.

DUAL uses the distance metric to select efficient, loop-free paths. DUAL selects routes to insert into the unicast Routing Information Base (RIB) based on feasible successors. When a topology change occurs, DUAL looks for feasible successors in the topology table. If there are feasible successors, DUAL selects the feasible successor with the lowest feasible distance and inserts that into the unicast RIB, avoiding unnecessary recomputation.

When there are no feasible successors but there are neighbors advertising the destination, DUAL transitions from the passive state to the active state and triggers a recomputation to determine a new successor or next-hop router to the destination. The amount of time required to recompute the route affects the convergence time. EIGRP sends Query messages to all neighbors, searching for feasible successors. Neighbors that have a feasible successor send a Reply message with that information. Neighbors that do not have feasible successors trigger a DUAL recomputation.

EIGRP Route Updates

When a topology change occurs, EIGRP sends an Update message with only the changed routing information to affected neighbors. This Update message includes the distance information to the new or updated network destination.

The distance information in EIGRP is represented as a composite of available route metrics, including bandwidth, delay, load utilization, and link reliability. Each metric has an associated weight that determines if the metric is included in the distance calculation. You can configure these metric weights. You can fine-tune link characteristics to achieve optimal paths, but we recommend that you use the default settings for most configurable metrics.

This section includes the following topics:

Internal Route Metrics

Internal routes are routes that occur between neighbors within the same EIGRP autonomous system. These routes have the following metrics:

- Next hop—The IP address of the next-hop router.
- Delay—The sum of the delays configured on the interfaces that make up the route to the destination network. Configured in tens of microseconds.
- Bandwidth—The calculation from the lowest configured bandwidth on an interface that is part of the route to the destination.

Note We recommend that you use the default bandwidth value. This bandwidth parameter is also used by EIGRP.

- MTU—The smallest maximum transmission unit value along the route to the destination.

- Hop count—The number of hops or routers that the route passes through to the destination. This metric is not directly used in the DUAL computation.
- Reliability—An indication of the reliability of the links to the destination.
- Load—An indication of how much traffic is on the links to the destination.

By default, EIGRP uses the bandwidth and delay metrics to calculate the distance to the destination. You can modify the metric weights to include the other metrics in the calculation.

External Route Metrics

External routes are routes that occur between neighbors in different EIGRP autonomous systems. These routes have the following metrics:

- Next hop—The IP address of the next-hop router.
- Router ID—The router ID of the router that redistributed this route into EIGRP.
- AS Number—The autonomous system number of the destination.
- Protocol ID—A code that represents the routing protocol that learned the destination route.
- Tag—An arbitrary tag that can be used for route maps.
- Metric—The route metric for this route from the external routing protocol.

EIGRP and the Unicast RIB

EIGRP adds all learned routes to the EIGRP topology table and the unicast RIB. When a topology change occurs, EIGRP uses these routes to search for a feasible successor. EIGRP also listens for notifications from the unicast RIB for changes in any routes redistributed to EIGRP from another routing protocol.

Advanced EIGRP

You can use the advanced features of EIGRP to optimize your EIGRP configuration.

This section includes the following topics:

Authentication

You can configure authentication on EIGRP messages to prevent unauthorized or invalid routing updates in your network. Cisco NX-OS supports MD5 authentication digest.

You can configure the EIGRP authentication per virtual routing and forwarding (VRF) instance or interface using key-chain management for the authentication keys. Key-chain management allows you to control changes to the authentication keys used by MD5 authentication digest. See the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.0* for more details about creating key-chains.

For MD5 authentication, you configure a password that is shared at the local router and all remote EIGRP neighbors. When an EIGRP message is created, Cisco NX-OS creates an MD5 one-way message digest based on the message itself and the encrypted password and sends this digest along with the EIGRP message. The receiving EIGRP neighbor validates the digest using the same encrypted password. If the message has not changed, the calculation is identical and the EIGRP message is considered valid.

MD5 authentication also includes a sequence number with each EIGRP message that is used to ensure that no message is replayed in the network.

Stub Routers

You can use the EIGRP stub routing feature to improve network stability, reduce resource usage, and simplify stub router configuration. Stub routers connect to the EIGRP network through a remote router. See the "Stub Routing" section on page 1-7.

When using EIGRP stub routing, you need to configure the distribution and remote routers to use EIGRP and configure only the remote router as a stub. EIGRP stub routing does not automatically enable summarization on the distribution router. In most cases, you need to configure summarization on the distribution routers.

Without EIGRP stub routing, even after the routes that are sent from the distribution router to the remote router have been filtered or summarized, a problem might occur. For example, if a route is lost somewhere in the corporate network, EIGRP could send a query to the distribution router. The distribution router could then send a query to the remote router even if routes are summarized. If a problem communicating over the WAN link between the distribution router and the remote router occurs, EIGRP could get stuck in active condition and cause instability elsewhere in the network. EIGRP stub routing allows you to prevent queries to the remote router.

Route Summarization

You can configure a summary aggregate address for a specified interface. Route summarization simplifies route tables by replacing a number of more-specific addresses with an address that represents all the specific addresses. For example, you can replace 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24 with one summary address, 10.1.0.0/16.

If more specific routes are in the routing table, EIGRP advertises the summary address from the interface with a metric equal to the minimum metric of the more specific routes.

Note Cisco NX-OS does not support automatic route summarization.

Route Redistribution

You can use EIGRP to redistribute static routes, routes learned by other EIGRP autonomous systems, or routes from other protocols. You configure route map with the redistribution to control which routes are passed into EIGRP. A route map allows you to filter routes based on attributes such as the destination, origination protocol, route type, route tag, and so on. See Chapter 15, "Configuring Route Policy Manager."

You also configure the default metric that is used for all imported routes into EIGRP.

Load Balancing

You can use load balancing to allow a router to distribute traffic over all the router network ports that are the same distance from the destination address. Load balancing increases the utilization of network segments which increases effective network bandwidth.

Cisco NX-OS supports the Equal Cost Multiple Paths (ECMP) feature with up to 16 equal-cost paths in the EIGRP route table and the unicast RIB. You can configure EIGRP to load balance traffic across some or all of those paths.

Split Horizon

You can use split horizon to ensure that EIGRP never advertises a route out of the interface where it was learned.

Split horizon is a method that controls the sending of EIGRP update and query packets. When you enable split horizon on an interface, Cisco NX-OS does not send update and query packets for destinations that were learned from this interface. Controlling update and query packets in this manner reduces the possibility of routing loops.

Split horizon with poison reverse configures EIGRP to advertise a learned route as unreachable back through that the interface that EIGRP learned the route from.

EIGRP uses split horizon or split horizon with poison reverse in the following scenarios:

- Exchanging topology tables for the first time between two routers in startup mode.
- Advertising a topology table change.
- Sending a Query message.

By default, the split horizon feature is enabled on all interfaces.

Virtualization Support

Cisco NX-OS supports multiple instances of the EIGRP protocol that runs on the same system. EIGRP supports Virtual Routing and Forwarding instances (VRFs). VRFs exist within virtual device contexts (VDCs). By default, Cisco NX-OS places you in the default VDC and default VRF unless you specifically configure another VDC and VRF. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0* and Chapter 14, “Configuring Layer 3 Virtualization.”

By default, every instance uses the same system router ID. You must manually configure the router ID for each instance if the instances are in the same EIGRP autonomous system.

Graceful Restart and High Availability

Cisco NX-OS supports nonstop forwarding and graceful restart for EIGRP.

You can use nonstop forwarding for EIGRP to forward data packets along known routes in the FIB while the EIGRP routing protocol information is being restored following a failover. With NSF, peer networking devices do not experience routing flaps. During failover, data traffic is forwarded through intelligent modules while the standby supervisor becomes active.

If a Cisco NX-OS system experiences a cold reboot, network does not forward traffic to the system and removes the system from the network topology. In this scenario, EIGRP experiences a stateless restart, and all neighbors are removed. Cisco NX-OS applies the startup configuration, and EIGRP rediscovers the neighbors and shares the full EIGRP routing information again.

A dual supervisor platform that runs Cisco NX-OS can experience a stateful supervisor switchover. Before the switchover occurs, EIGRP uses a graceful restart to announce that EIGRP will be unavailable for some time. During a switchover, EIGRP uses nonstop forwarding to continue forwarding traffic based on the information in the FIB, and the system is not taken out of the network topology.

The graceful restart-capable router uses Hello messages to notify its neighbors that an graceful restart operation has started. When an graceful restart-aware router receives a notification from a graceful restart-capable neighbor that a graceful restart operation is in progress, both routers immediately exchange their topology tables. The graceful restart-aware router then performs the following actions to assist the restarting router:

- The router expires the EIGRP Hello hold timer to reduce the time interval set for Hello messages. This allows the graceful restart-aware router to reply to the restarting router more quickly and reduces the amount of time required for the restarting router to rediscover neighbors and rebuild the topology table.
- The router starts the route-hold timer. This timer sets the period of time that the graceful restart-aware router will hold known routes for the restarting neighbor. The default time period is 240 seconds.
- The router notes in the peer list that the neighbor is restarting, maintains adjacency, and holds known routes for the restarting neighbor until the neighbor signals that it is ready for the graceful restart-aware router to send its topology table or the route-hold timer expires. If the route-hold timer expires on the graceful restart-aware router, the graceful restart-aware router discards held routes and treats the restarting router as a new router joining the network and reestablishing adjacency.

After the switchover, Cisco NX-OS applies the running configuration, and EIGRP informs the neighbors that it is operational again.

Note You must enable graceful restart to support in-service software upgrades (ISSU) for EIGRP. If you disable graceful restart, Cisco NX-OS issues a warning that ISSU cannot be supported with this configuration.

Licensing Requirements for EIGRP

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	EIGRP requires an Enterprise Services license. For a complete explanation of the NX-OS licensing scheme and how to obtain and apply licenses, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0.*

Prerequisites for EIGRP

EIGRP has the following prerequisites:

- You must enable the EIGRP feature (see the "Enabling the EIGRP Feature" section on page 7-8).

- If you configure VDCs, install the Advanced Services license and enter the desired VDC (see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0).*

Configuration Guidelines and Limitations

EIGRP has the following configuration guidelines and limitations:

- A metric configuration (either through the default-metric configuration option or through a route map) is required for redistribution from any other protocol, connected routes, or static routes (see Chapter 15, "Configuring Route Policy Manager").
- For graceful restart, an NSF-aware router must be up and completely converged with the network before it can assist an NSF-capable router in a graceful restart operation.
- For graceful restart, neighboring devices participating in the graceful restart must be NSF-aware or NSF-capable.
- Cisco NX-OS EIGRP is compatible with EIGRP in Cisco IOS.
- Do not change the metric weights without a good reason. If you change the metric weights, you must apply the change to all EIGRP routers in the same autonomous system.
- Consider using stubs for larger networks.
- Avoid redistribution between different EIGRP autonomous systems because the EIGRP vector metric will not be preserved.
- The **no ip next-hop-self** command does not guarantee reachability of next hop.
- The **ip passive-interface eigrp** command suppresses neighbor formation.
- Cisco NX-OS does not support IGRP or connecting IGRP and EIGRP clouds.
- Autosummarization is not enabled by default.
- Cisco NX-OS supports only IP.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Configuring Basic EIGRP

This section contains the following topics:

Enabling the EIGRP Feature

You must enable the EIGRP feature before you can configure EIGRP.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **feature eigrp**
3. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**feature eigrp** **Example:** `switch(config)# feature eigrp`	Enables the EIGRP feature.
Step 3	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves this configuration change.

Use the **no feature eigrp** command to disable the EIGRP feature and remove all associated configuration.

Command	Purpose
no feature eigrp **Example:** `switch(config)# no feature eigrp`	Disables the EIGRP feature and removes all associated configuration.

Creating an EIGRP Instance

You can create an EIGRP instance and associate an interface with that instance. You assign a unique autonomous system number for this EIGRP process (see the "Autonomous Systems" section on page 1-5). Routes are not advertised or accepted from eternal autonomous systems unless you enable route redistribution.

BEFORE YOU BEGIN

Ensure that you have enabled the EIGRP feature (see the "Enabling the EIGRP Feature" section on page 7-8).

EIGRP must be able to obtain a router ID (for example, a configured loopback address) or you must configure the router ID option.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **router eigrp** *instance-tag*
3. <configure optional parameters>
4. **interface** *interface-type slot/port*
5. **ip router eigrp** *instance-tag*
6. **show ip eigrp interfaces**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**router eigrp** *instance-tag*
	
	Example:
	`switch(config)# router eigrp 201`
	`switch(config-router)#`
		Creates a new EIGRP process with the configured autonomous system number.

Step 3	**eigrp router-id** *ip-address* **Example:** `switch(config-router)# eigrp router-id 192.0.2.1`	(Optional) Configures the EIGRP router ID. This IP address identifies this EIGRP instance and must exist on a configured interface in the system.
	router-id *ip-address* **Example:** `switch(config-router)# router-id 192.0.2.1`	(Optional) Configures the EIGRP router ID. This command is identical to the **eigrp router-id** command.

Step 4	**log-adjacency-changes**
	
	Example:
	`switch(config-router)#`
	`log-adjacency-changes`
		(Optional). Generates a system message whenever an adjacency changes state. This command is enabled by default.

Step 5	**log-neighbor-warnings** [*seconds*]
	
	Example:
	`switch(config-router)#`
	`log-neighbor-warnings`
		(Optional) Generates a system message whenever a neighbor warning occurs. You can configure the time between warning messages, from 1 to 65535, in seconds. The default is 10 seconds. This command is enabled by default.

Step 6	**interface** *interface-type slot/port*
	
	Example:
	`switch(config-router)# interface ethernet 1/2`
	`switch(config-if)#`
		Enters interface configuration mode.

	Command	Purpose
Step 7	**ip router eigrp** *instance-tag* **Example:** `switch(config-if)# ip router eigrp 201`	Associates this interface with the configured EIGRP process.
Step 8	**show ip eigrp interfaces** **Example:** `switch(config-if)# show ip eigrp interfaces`	Displays information about EIGRP interfaces.
Step 9	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves this configuration change.

Use the **no router eigrp** command to remove the EIGRP process and the associated configuration.

Command	Purpose
no router eigrp *instance-tag* **Example:** `switch(config)# no router eigrp 201`	Deletes the EIGRP process and all associated configuration.

Note You must also remove any EIGRP commands configured in interface mode.

The following example shows how to create an EIGRP process and configure an interface for EIGRP:

```
switch# config t
switch(config)# router eigrp 201
switch(config)# interface ethernet 1/2
switch(config-if)# ip router eigrp 201
switch(config-if)# no shutdown
switch(config-if)# copy running-config startup-config
```

For more information about other EIGRP parameters, see the "Configuring Advanced EIGRP" section on page 7-12.

Restarting an EIGRP Instance

You can restart an EIGRP instance. This clears all neighbors for the instance.

To restart an EIGRP instance and remove all associated neighbors, use the following command:

Command	Purpose
restart eigrp instance-tag **Example:** `switch(config)# restart eigrp 201`	Restarts the EIGRP instance and removes all neighbors.

Disabling an EIGRP Instance

To disable an EIGRP instance, use the following command in router configuration mode:

Command	Purpose
`switch(config-router)# shutdown` **Example:** `switch(config-router)# shutdown`	Disables this instance of EIGRP

Disabling EIGRP on an Interface

To disable EIGRP on an interface, use the following command in interface configuration mode:

Command	Purpose

`switch(config-if)# ip eigrp` *as-numver* `shutdown`
 	
Example:
`switch(config-router)# ip eigrp 201 shutdown`
	Disables EIGRP on this interface.

Configuring Advanced EIGRP

This section includes the following topics:

Configuring Authentication in EIGRP

You can configure authentication between neighbors for EIGRP. See the "Authentication" section on page 7-4.

BEFORE YOU BEGIN

Ensure that you have enabled the EIGRP feature (see the "Enabling the EIGRP Feature" section on page 7-8).

Ensure that all neighbors for an EIGRP process share the same authentication configuration, including the shared authentication key.

Create the key-chain for this authentication configuration. See the *Cisco NX-OS Security Configuration Guide.*

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **router eigrp** *instance-tag*
3. **vrf** *vrf-name*
4. **authentication key-chain** *key-chain*
5. **authentication mode md5**
6. **interface** *interface-type slot/port*
7. **ip router eigrp** *instance-tag*
8. **ip authentication key-chain eigrp** *instance-tag key-chain*
9. **ip authentication mode eigrp** *instance-tag* **md5**
10. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**router eigrp** *instance-tag* **Example:** switch(config)# router eigrp 201 switch(config-router)#	Creates a new EIGRP process with the configured autonomous system number.
Step 3	**vrf** *vrf-name* **Example:** switch(config-router)# vrf red switch(config-router-vrf)#	Enters VRF configuration mode.
Step 4	**authentication key-chain** *key-chain* **Example:** switch(config-router-vrf)# authentication key-chain routeKeys	Associates a key-chain with this EIGRP process for this VRF.

	Command	Purpose
Step 5	**authentication mode md5** **Example:** switch(config-router-vrf)# authentication mode md5	Configures MD5 message digest authentication mode for this VRF.
Step 6	**interface** *interface-type slot/port* **Example:** switch(config)interface ethernet 1/2 switch(config-if)#	Enters interface configuration mode.
Step 7	**ip router eigrp** *instance-tag* **Example**: switch(config-if)# ip router eigrp 201	Associates this interface with the configured EIGRP process.
Step 8	**ip authentication key-chain eigrp** *instance-tag key-chain* **Example:** switch(config-if)# ip authentication key-chain eigrp 201 routeKeys	Associates a key-chain with this EIGRP process for this interface. This configuration overrides the authentication configuration set in the router VRF mode.
Step 9	**ip authentication mode eigrp** *instance-tag* **md5** **Example:** switch(config-if)# ip authentication mode eigrp 201 md5	Configures MD5 message digest authentication mode for this interface. This configuration overrides the authentication configuration set in the router VRF mode.
Step 10	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	(Optional) Saves this configuration change.

The following example shows how to configure MD5 message digest authentication for EIGRP over Ethernet interface 1/2:

```
switch# config t
switch(config)# router eigrp 201
switch(config-router)# exit
switch(config)# interface ethernet 1/2
switch(config-if)# ip router eigrp 201
switch(config-if)# ip authentication key-chain eigrp 201 routeKeys
switch(config-if)# ip authentication mode eigrp 201 md5
switch(config-if)# copy running-config startup-config
```

Configuring EIGRP Stub Routing

To configure a router for EIGRP stub routing, use the following command in router configuration mode:

Command	Purpose
switch(config-router)# **stub** [**leak-map** *map-name* | **receive-only** | **redistributed** [**direct**]] **Example:** switch(config-router)# eigrp stub redistributed	Configures a remote router as an EIGRP stub router.

The following example shows how to configure a stub router to advertise directly connected and redistributed routes:

```
switch# config t
switch(config)# router eigrp 201
switch(config-router)# stub direct redistributed
switch(config-router)# copy running-config startup-config
```

Use the **show ip eigrp neighbor detail** command to verify that a router has been configured as a stub router. The last line of the output shows the stub status of the remote or spoke router. The following example shows that output from the **show ip eigrp neighbor detail** command:

```
Router# show ip eigrp neighbor detail
IP-EIGRP neighbors for process 201
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   10.1.1.2                Se3/1         11 00:00:59    1  4500  0  7
   Version 12.1/1.2, Retrans: 2, Retries: 0
   Stub Peer Advertising ( CONNECTED SUMMARY ) Routes
```

Configuring a Summary Address for EIGRP

You can configure a summary aggregate address for a specified interface. If any more specific routes are in the routing table, EIGRP will advertise the summary address out the interface with a metric equal to the minimum of all more specific routes. See the "Route Summarization" section on page 7-5.

To configure a summary aggregate address, use the following command in interface configuration mode:

Command	Purpose
switch(config-if)# **ip summary-address eigrp** *instance-tag ip-prefix/length* [*distance* | **leak-map** *map-name*] **Example:** switch(config-if)# ip summary-address eigrp 201 209.0.2.0/8	Configures a summary aggregate address as either an IP address and network mask, or an IP prefix/length. You can optionally configure the administrative distance for this aggregate address. The default administrative distance is 5 for aggregate addresses.

The following example causes EIGRP to summarize network 209.0.2.0 out Ethernet 1/2 only:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip summary-address eigrp 201 209.0.2.0 255.255.255.0
```

Redistributing Routes into EIGRP

You can redistribute routes in EIGRP from other routing protocols.

BEFORE YOU BEGIN

Ensure that you have enabled the EIGRP feature (see the "Enabling the EIGRP Feature" section on page 7-8).

You must configure the metric (either through the default-metric configuration option or through a route map) for routes redistributed from any other protocol.

You must create a route map to control the types of routes that are redistributed into EIGRP. See Chapter 15, "Configuring Route Policy Manager."

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **router eigrp** *instance-tag*
3. **redistribute** {{**bgp** | **eigrp** | **isis** | **ospf** | **rip**} *instance-tag* | **direct** | **static**} **route-map** *name*
4. **default-metric** *bandwidth delay reliability loading mtu*
5. **show ip eigrp map statistics redistribute**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**router eigrp** *instance-tag* **Example:** switch(config)# router eigrp 201 switch(config-router)#	Creates a new EIGRP process with the configured autonomous system number.
Step 3	**redistribute** {{**bgp** | **eigrp** | **isis** | **ospf** | **rip**} *instance-tag* | **direct** | **static**} **route-map** *name* **Example:** switch(config-router)# redistribute bgp 100 route-map BGPFilter	Injects routes from one routing domain into EIGRP.

	Command	Purpose
Step 4	**default-metric** *bandwidth delay reliability loading mtu* **Example:** `switch(config-router)# default-metric 500000 30 200 1 1500`	Sets the metrics assigned to routes learned through route redistribution. The default values are as follows: • bandwidth—100000 Kb/s • delay—100 (10 microsecond units) • reliability—255 • loading—1 • MTU—1492
Step 5	**show ip eigrp route-map statistics redistribute** **Example:** `switch(config-router)# show ip eigrp route-map statistics redistribute bgp`	Displays information about EIGRP route map statistics.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves this configuration change.

The following example shows how to redistribute BGP into EIGRP:

```
switch# config t
switch(config)# router eigrp 201
switch(config-router)# redistribute bgp 100 route-map BGPFilter
switch(config-router)# default-metric 500000 30 200 1 1500
switch(config-router)# copy running-config startup-config
```

Configuring Load Balancing in EIGRP

You can configure load balancing in EIGRP. You can configure the number of Equal Cost Multiple Path (ECMP) routes using the maximum paths option. See the "Configuring Load Balancing in EIGRP" section on page 7-17.

BEFORE YOU BEGIN

Ensure that you have enabled the EIGRP feature (see the "Enabling the EIGRP Feature" section on page 7-8).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **router eigrp** *instance-tag*
3. **maximum-paths** *num-paths*
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**router eigrp** *instance-tag* **Example:** switch(config)# router eigrp 201 switch(config-router)#	Creates a new EIGRP process with the configured autonomous system number.
Step 3	**maximum-paths** *num-paths* **Example:** switch(config-router)# maximum-paths 5	Sets the number of equal cost paths EIGRP will accept in the route table. The range is from 1 to 16. The default is 8.
Step 4	**copy running-config startup-config** **Example:** switch(config-router)# copy running-config startup-config	(Optional) Saves this configuration change.

The following example shows how to configure equal cost load balancing for EIGRP with a maximum of 6 equal cost path:

```
switch# config t
switch(config)# router eigrp 201
switch(config-router)# maximum-paths 6
switch(config-router)# copy running-config startup-config
```

Configuring Graceful Restart for EIGRP

You can configure graceful restart or nonstop forwarding for EIGRP. See the "Graceful Restart and High Availability" section on page 7-6.

Note You must enable NSF and graceful restart for this feature.

BEFORE YOU BEGIN

Ensure that you have enabled the EIGRP feature (see the "Enabling the EIGRP Feature" section on page 7-8).

An NSF-aware router must be up and completely converged with the network before it can assist an NSF-capable router in a graceful restart operation.

Neighboring devices participating in the graceful restart must be NSF-aware or NSF-capable.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**

2. **router eigrp** *instance-tag*
3. **graceful-restart**
4. **timers nsf converge** *seconds*
5. **timers nsf route-hold** *seconds*
6. **timers nsf signal** *seconds*
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**router eigrp** *instance-tag* **Example:** switch(config)# router eigrp 201 switch(config-router)#	Creates a new EIGRP process with the configured autonomous system number.
Step 3	**eigrp graceful-restart** **Example:** switch(config-router)# graceful-restart	Enables graceful restart. This feature is enabled by default.
Step 4	**timers nsf converge** *seconds* **Example**: switch(config-router)# timers nsf converge 100	Sets the time limit for convergence after a switchover. The range is from 60 to 180 seconds. The default is 120.
Step 5	**timers nsf route-hold** *seconds* **Example**: switch(config-router)# timers nsf route-hold 200	Sets the hold time for routes learned from the graceful restart-aware peer. The range is from 20 to 300 seconds. The default is 240.
Step 6	**timers nsf signal** *seconds* **Example**: switch(config-router)# timers nsf signal 15	Sets the time limit for signaling a graceful restart. Range is 10 to 30 seconds. Default is 20.
Step 7	**copy running-config startup-config** **Example:** switch(config-router)# copy running-config startup-config	(Optional) Saves this configuration change.

The following example shows how to configure graceful restart using the default timer values:

```
switch# config t
switch(config)# router eigrp 201
switch(config-router)# graceful-restart
switch(config-router)# copy running-config startup-config
```

Adjusting the Interval Between Hello Packets and the Hold Time

You can adjust the interval between Hello messages and the hold time.

By default, Hello messages are sent every 5 seconds. The hold time is advertised in Hello messages and indicates to neighbors the length of time that they should consider the sender valid. The default hold time is three times the hello interval, or 15 seconds.

To change the interval between hello packets, use the following command in interface configuration mode:

Command	Purpose
`switch(config-if)# ip hello-interval eigrp` *instance-tag seconds*	Configures the hello interval for an EIGRP routing process. The range is from 1 to 65535 seconds. The default is 5.

On very congested and large networks, the default hold time might not be sufficient time for all routers to receive hello packets from their neighbors. In this case, you might want to increase the hold time.

To change the hold time, use the following command in interface configuration mode:

Command	Purpose
`switch(config-if)# ip hold-time eigrp` *autonomous-system-number seconds*	Configures the hold time for an EIGRP routing process. The range is from 1 to 65535.

Use the **show ip eigrp interface detail** command to verify timer configuration.

Disabling Split Horizon

You can use split horizon to block route information from being advertised by a router out of any interface from which that information originated. Split horizon usually optimizes communications among multiple routing devices, particularly when links are broken.

By default, split horizon is enabled on all interfaces.

To disable split horizon, use the following command in interface configuration mode:

Command	Purpose
`switch(config-if)# no ip split-horizon eigrp` *instance-tag*	Disables split horizon.

Tuning EIGRP

You can configure optional parameters to tune EIGRP for your network.

You can configure the following optional parameters in router configuration mode:

Command	Purpose
default-information originate [**always** | **route-map** *map-name*] **Example:** switch(config-router)# default-information originate always	Originates or accepts the default route with prefix 0.0.0.0/0. When a route-map is supplied, the default route is originated only when the route-map yields a true condition.
distance *internal external* Example: switch(config-router)# distance 25 100	Configures the administrative distance for this EIGRP process. Range is 1to 255. The internal value sets the distance for routes learned from within the same autonomous system (the default value is 90). The external value sets the distance for routes learned from an external autonomous system (the default value is 170).
metric max-hops *hop-count* **Example:** switch(config-router)# metric max-hops 70	Set maximum allowed hops for an advertised route. Routes over this maximum are advertised as unreachable. The range is from 1 to 255. The default is 100.
metric weights *tos k1 k2 k3 k4 k5* **Example:** switch(config-router)# metric weights 0 1 3 0 1 0	Adjusts the EIGRP metric or K value. EIGRP uses the following formula to determine the total metric to the network: metric = [k1*bandwidth + (k2*bandwidth)/(256 – load) + k3*delay] * [k5/(reliability + k4)] Default values and ranges are as follows: • TOS—0. The range is from 0 to 8. • k1—1. The range is from 0 to 255. • k2—0. The range is from 0 to 255. • k3—1. The range is from 0 to 255. • k4—0. The range is from 0 to 255. • k5—0. The range is from 0 to 255.
timers active-time {*time-limit* | **disabled**} **Example**: switch(config-router)# timers active-time 200.	Sets the time the router waits in minutes (after sending a query) before declaring the route to be stuck in the active (SIA) state. The range is from 1 to 65535. The default is 3.

You can configure the following optional parameters in interface configuration mode:

Command	Purpose
ip bandwidth eigrp *instance-tag bandwidth*	Configures the bandwidth metric for EIGRP on an interface, The range is from 1 to 10000000 Kb/s.
ip bandwidth-percent eigrp *instance-tag percent*	Configures the percentage of bandwidth that EIGRP might use on an interface, The default is 50 percent.

Command	Purpose
no ip delay eigrp *instance-tag delay*	Configures the delay metric for EIGRP on an interface, The range is from 1 to 16777215 (in tens of microseconds).
ip distribute-list eigrp *instance-tag* {**prefix-list** *name*| **route-map** name} {**in** | **out**}	Configures the route filtering policy for EIGRP on this interface.
no ip next-hop-self eigrp *instance-tag*	Configures EIGRP to use the received next-hop address rather than the address for this interface. The default is to use the IP address of this interface for the next-hop address.
ip offset-list eigrp *instance-tag* {**prefix-list** *name*| **route-map** name} {**in** | **out**} *offset*	Adds an offset to incoming and outgoing metrics to routes learned by EIGRP.
ip passive-interface eigrp *instance-tag*	Suppresses routing updates on an EIGRP interface.

Configuring Virtualization for EIGRP

You can configure multiple EIGRP processes in each VDC. You can also create multiple VRFs within each VDC and use the same or multiple EIGRP processes in each VRF. You assign an interface to a VRF

Note Configure all other parameters for an interface after you configure the VRF for an interface. Configuring a VRF for an interface deletes all other configuration for that interface.

BEFORE YOU BEGIN

Ensure that you have enabled the EIGRP feature (see the "Enabling the EIGRP Feature" section on page 7-8).

Create the VDCs and VRFs.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **vrf context** *vrf-name*
3. **router eigrp** *instance-tag*
4. **interface ethernet** *slot/port*
5. **vrf member** *vrf-id*
6. **ip-address** *ip-prefix/length*
7. **ip router eigrp** *instance-tag*
8. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**vrf context** *vrf-name* **Example:** switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#	Creates a new VRF and enters VRF configuration mode.
Step 3	**router eigrp** *instance-tag* **Example:** switch(config)# router eigrp 201 switch(config-router)#	Creates a new EIGRP process with the configured autonomous system number.
Step 4	**interface ethernet** *slot/port* **Example**: switch(config)# interface ethernet 1/2 switch(config-if)#	Enters interface configuration mode.
Step 5	**vrf member** *vrf-name* **Example:** switch(config-if)# vrf member RemoteOfficeVRF	Adds this interface to a VRF.
Step 6	**ip router eigrp** *instance-tag* **Example**: switch(config-if)# ip router eigrp 201	Adds this interface to the EIGRP process.
Step 7	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	(Optional) Saves this configuration change.

The following example shows how to create a VRF and add an interface to the VRF:

```
switch# config t
switch(config)# vrf context NewVRF
switch(config-vrf)# router eigrp 201
switch(config-router)# interface ethernet 1/2
switch(config-if)# ip router eigrp 201
switch(config-if)# vrf NewVRF
switch(config-if)# copy running-config startup-config
```

Verifying EIGRP Configuration

To verify the EIGRP configuration, use the following commands:

Command	Purpose
show ip eigrp [*instance-tag*]	Displays information about the EIGRP configuration.
show ip eigrp [*instance-tag*] **interfaces** [*type number*] [**brief**] [**detail**]	Displays information about the EIGRP configuration on an interface.
show ip eigrp *instance-tag* **neighbors** [*type number*] [**detail**]	Displays information about the EIGRP neighbors.
show ip eigrp [*instance-tag*] **route** [*ip-prefix/length*] [**active**] [**all-links**] [**detail-links**] [**pending**] [**summary**] [**zero-successors**] [**vrf** *vrf-name*]	Displays information about the EIGRP routes.
show ip eigrp [*instance-tag*] **topology** [*ip-prefix/length*] [**active**] [**all-links**] [**detail-links**] [**pending**] [**summary**] [**zero-successors**] [**vrf** *vrf-name*]	Displays information about the EIGRP topology.
show running-configuration eigrp	Displays the current running EIGRP configuration.

Use the **show ip eigrp neighbors** command to verify the EIGRP neighbor configuration.

Displaying EIGRP Statistics

To display EIGRP statistics, use the following commands:

Command	Purpose
show ip eigrp [*instance-tag*] **accounting** [**vrf** *vrf-name*]	Displays accounting statistics for EIGRP.
show ip eigrp [*instance-tag*] **route-map statistics redistribute**	Displays redistribution statistics for EIGRP.
show ip eigrp [*instance-tag*] **traffic** [**vrf** *vrf-name*]	Displays traffic statistics for EIGRP.

EIGRP Example Configuration

The following example shows how to configure EIGRP:

```
feature eigrp
interface ethernet 1/2
 ip address 209.0.2.55/24
 ip router eigrp 201
  no shutdown
router eigrp 201
  router-id 209.0.2.1
```

Related Topics

See the Chapter 15, "Configuring Route Policy Manager" for more information on route maps.

Default Settings

Table 7-1 lists the default settings for EIGRP parameters.

Table 7-1 Default EIGRP Parameters

Parameters	Default
Administrative distance	• Internal routes—90 • External routes—170
Bandwidth percent	50 percent
Default metric for redistributed routes	• bandwidth—100000 Kb/s • delay—100 (10 microsecond units) • reliability—255 • loading—1 • MTU—1500
EIGRP feature	Disabled
Hello interval	5 seconds
Hold time	15 seconds
Maximum equal cost paths	16
Metric weights	1 0 1 0 0
Next-hop address advertised	IP address of local interface
NSF convergence time	120
NSF route-hold time	240
NSF signal time	20
Redistribution	Disabled
Split horizon	Enabled

Additional References

For additional information related to implementing EIGRP, see the following sections:

- Related Documents, page 7-26

Related Documents

Related Topic	Document Title
EIGRP CLI commands	*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.0*
VDCs and VRFs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0*
http://www.cisco.com/warp/public/103/1.html	*Introduction to EIGRP Tech Note*
http://www.cisco.com/en/US/tech/tk365/technologies_q_and_a_item09186a008012dac4.shtml	EIGRP Frequently Asked Questions

MIBs

MIBs	MIBs Link
CISCO-EIGRP-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for EIGRP

Table 7-2 lists the release history for this feature.

Table 7-2 Feature History for EIGRP

Feature Name	Releases	Feature Information
EIGRP authentication	4.0(3)	Added the ability to configure authentication within a VRF for EIGRP.
EIGRP parameters	4.0(3)	Removed the **eigrp** keyword from the **graceful-restart**, **log-adjacency-changes**, and **log-neighbor-warnings** commands. Removed the **nsf** command. Replaced the **log-neighbor-changes** command with the **log-adjacency-changes** command. Added the **brief** keyword to the **show ip eigrp interfaces** command**.** Added the * and **soft** keywords to the **show ip eigrp neighbors** command. Changed EIGRP process identifier from an AS number to an instance tag.
EIGRP statistics	4.0(3)	Changed the **policy** keyword to **route-map** in the show **ip eigrp policy statistics** command and the **clear ip eigrp policy statistics** command.
EIGRP	4.0(1)	This feature was introduced.