Configuring Routing Policies

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

This chapter contains the following topics:

BGP Routing on Cisco IOS Routers

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

BGP is an Exterior Gateway Protocol (EGP) that guarantees the loop-free exchange of routing information between autonomous systems (ASs). The *primary* function of a BGP system is to exchange information with other BGP systems about the networks it can reach, including AS path information. This information can be used to construct a graph of AS connectivity from which routing loops can be pruned and with which AS-level policy decisions can be enforced.

BGP is the routing protocol used on the Internet and is commonly used between Internet service providers. To achieve scalability at this level, BGP uses several route parameters (attributes) to define routing policies and maintain a stable routing environment. Additionally, BGP uses classless interdomain routing (CIDR) to greatly reduce the size of Internet routing tables.

A BGP route consists of a network number, a list of ASs through which information has passed (called the *autonomous system path*), and the defined path attributes.

A BGP router exchanges routing information only with those routers that you define as its neighbors. BGP neighbors exchange complete routing information when the TCP connection between them is established. Updates are sent to neighbors only when changes to the routing table are detected. BGP routers do not send regular, periodic updates.

The following topics describe the tasks you perform to create a BGP routing policy:

- Defining BGP Routes , on page 2
- Redistributing Routes into BGP , on page 3

Note Security Manager supports versions 2, 3 and 4 of BGP, as defined in RFCs 1163, 1267 and 1771.

Related Topics

- Static Routing on Cisco IOS Routers , on page 59
- RIP Routing on Cisco IOS Routers , on page 50
- OSPF Routing on Cisco IOS Routers , on page 27
- EIGRP Routing on Cisco IOS Routers , on page 9

Defining BGP Routes

As with all EGPs, when you configure a BGP routing policy, you must define the relationship the router has with its neighbors. BGP supports two kinds of neighbors: internal (located in the same AS) and external (located in a different AS). Typically, external neighbors are adjacent to each other and share a subnet; internal neighbors can be anywhere in the same AS.

In addition, you can select whether to enable the following optional features:

- Auto-summarization
- Synchronization
- Neighbor logging

If enabled, *auto-summarization* injects only the network route when a subnet is redistributed from an Interior Gateway Protocol (IGP) such as OSPF or EIGRP into BGP. *Synchronization* is useful if your AS acts as an intermediary, passing traffic from one AS to another AS, because it ensures that your AS is consistent about the routes it advertises. For example, if BGP were to advertise a route before all routers in your network had learned about the route through your IGP, your AS might receive traffic that some routers cannot yet route. *Neighbor logging* enables the router to keep track of messages issued by BGP neighbors when they reset, become unreachable, or restore their connection to the network.

This procedure describes how to define a BGP route. You can define only one BGP route on each router.

Related Topics

- Redistributing Routes into BGP , on page 3
- BGP Routing on Cisco IOS Routers , on page 1

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **BGP** from the Policy selector, then click the **Setup** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **BGP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Setup** tab.

The BGP Setup is displayed. See Table 1: BGP Setup Tab , on page 5 for a description of the fields on this tab.

Step 2 On the BGP Setup tab, enter the AS number to which the router belongs.

Step 3 (Optional) Enter the addresses of the networks that are local to this AS. You can use a combination of addresses and network/host objects, or click **Select** to select an object from a list or to create a new one. For more information, see Specifying IP Addresses During Policy Definition.

Step 4 Define external and internal BGP neighbors for the routers:

a) Click **Add** under Neighbors to display the BGP Neighbors dialog box. See Table 2: Neighbors Dialog Box , on page 6 for a description of the fields in this dialog box.
b) Enter an AS number and then click **Select** to select the hosts that are neighbors within the defined AS. Internal neighbors are located in the same AS as the router; external neighbors are located in a different AS.
c) Click **OK** to save your definitions and return to the BGP Neighbors dialog box.
d) (Optional) Repeat 4.b, on page 3 and 4.c, on page 3 to define neighbors in additional ASs.

Note When you define BGP neighbors, the IP addresses cannot belong to an interface on the selected router. In addition, you cannot define the same IP address in more than one AS.

When you finish, click **OK** in the BGP Neighbors dialog box to return to the BGP Setup tab. Your selections are displayed in the Neighbors field.

Step 5 (Optional) Select the Auto-Summary check box to enable automatic summarization. If automatic summarization is enabled, only the network route is injected into the BGP table when a subnet is redistributed from an IGP (such as OSPF or EIGRP) into BGP.

Step 6 (Optional) Select the **Synchronization** check box to synchronize BGP with the IGP. Enabling this feature causes BGP to wait until the IGP propagates routing information across the AS.

You do not need synchronization if your AS does not pass traffic it receives from one AS to another AS, or if all the routers in your AS run BGP. Disabling synchronization enables BGP to converge more quickly.

Step 7 (Optional) Select the **Log-Neighbor** check box to enable the logging of messages generated when a BGP neighbors resets, comes up, or goes down.

Redistributing Routes into BGP

Redistribution refers to using a routing protocol, such as BGP, to advertise routes that are learned by some other means, such as a different routing protocol, static routes, or directly connected routes. For example, you can redistribute routes from the OSPF routing protocol into your BGP autonomous system (AS). Redistribution is necessary in networks that operate in multiple-protocol environments and can be applied to all IP-based routing protocols.

Before You Begin

- Define a BGP AS. See Defining BGP Routes , on page 2.

Related Topics

- Defining BGP Routes , on page 2
- BGP Routing on Cisco IOS Routers , on page 1

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **BGP** from the Policy selector, then click the **Redistribution** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **BGP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Redistribution** tab.

The BGP Redistribution tab is displayed. See Table 3: BGP Redistribution Tab , on page 7 for a description of the fields on this tab.

Step 2 On the BGP Redistribution tab, select a row from the BGP Redistribution Mappings table, then click **Edit**, or click **Add** to create a mapping. The BGP Redistribution Mapping dialog box appears. See Table 4: BGP Redistribution Mapping Dialog Box , on page 9 for a description of the fields in this dialog box.

Step 3 Select the protocol whose routes you want to redistribute into BGP.

Note You can create a single mapping for each static route, RIP route, EIGRP AS, and OSPF process.

Step 4 (Optional) Modify the default metric (cost) of the redistributed routes. The metric determines the priority of the routes.

Step 5 Click **OK** to save your definitions locally on the client and close the dialog box. The redistribution mapping appears in the Redistribution Mapping table in the BGP Redistribution tab.

BGP Routing Policy Page

Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP) that performs routing between multiple autonomous systems or domains and exchanges routing and reachability information with other BGP systems. BGP is used to exchange routing information on the Internet and is the protocol used between Internet service providers.

You can configure BGP routing policies from the following tabs on the BGP Routing page:

- BGP Page—Setup Tab , on page 5
- BGP Page—Redistribution Tab , on page 7

For more information, see BGP Routing on Cisco IOS Routers , on page 1.

Navigation Path

- (Device view) Select **Platform** > **Routing** > **BGP** from the Policy selector.
- (Policy view) Select **Router Platform** > **Routing** > **BGP** from the Policy Type selector. Right-click **BGP** to create a policy, or select an existing policy from the Shared Policy selector.

BGP Page—Setup Tab

Use the BGP Setup tab to define the number of the autonomous system (AS) in which the selected router is located. You must then define which networks are included in the AS and which networks are the internal and external neighbors of the router. Additionally, you can enable or disable options that govern the interaction between BGP and Interior Gateway Protocols (IGPs), such as OSPF and EIGRP. Use a third option to enable the logging of messages from BGP neighbors.

Navigation Path

Go to the BGP Routing Policy Page , on page 4, then click the **Setup** tab.

Related Topics

- Defining BGP Routes , on page 2
- BGP Page—Redistribution Tab , on page 7
- Specifying IP Addresses During Policy Definition
- Understanding Networks/Hosts Objects

Field Reference

Table 1: BGP Setup Tab

Element	Description
AS Number	The number of the autonomous system in which the router is located. Valid values range from 1 to 65535. This number enables a BGP routing process. If BGP is already configured on the device, you cannot successfully change and deploy this number. If you need to change the AS number, first unassign the BGP policy, deploy your change (thus removing the BGP configuration from the device), then configure the BGP policy with the new number and redeploy the configuration.
Networks	The networks associated with the BGP route. Enter one or more network addresses or network/host objects, or click **Select** to select the object from a list or to create a new one. **Note** To remove a network from the route, select it from the Network field, then click **Delete**.
Neighbors	The *internal* neighbors (those located in the same AS as the router) and *external* neighbors (located in different ASs) of the router. See Neighbors Dialog Box , on page 6.

Element	Description
Auto-Summary	When selected, automatic summarization is enabled. When a subnet is redistributed from an IGP (such as RIP, OSPF or EIGRP) into BGP, this BGP version 3 feature injects only the network route into the BGP table. Automatic summarization reduces the size and complexity of the routing table that the router must maintain. When deselected, automatic summarization is disabled. This is the default.
Synchronization	When selected, synchronization is enabled. Use this feature to ensure that all routers in your network are consistent about the routes they advertise. Synchronization forces BGP to wait until the IGP propagates routing information across the AS. When deselected, synchronization is disabled. You can disable synchronization if this router does not pass traffic from a different AS to a third AS, or if all the routers in the AS are running BGP. Disabling this feature has the benefit of reducing the number of routes the IGP must carry, which improves convergence times. This is the default.
Log-Neighbor	When selected, enables the logging of messages that are generated when a BGP neighbors resets, connects to the network, or is disconnected. This is the default. When deselected, message logging is disabled.

Neighbors Dialog Box

Use the Neighbors dialog box to define the internal and external neighbors of the selected router.

Navigation Path

Go to the BGP Page—Setup Tab , on page 5, then click the **Add** or **Edit** button in the Neighbors field.

Related Topics

- Defining BGP Routes , on page 2
- Specifying IP Addresses During Policy Definition
- Understanding Networks/Hosts Objects

Field Reference

Table 2: Neighbors Dialog Box

Element	Description
AS Number	The number of the AS containing BGP neighbors. Internal neighbors have the same AS number as the network of the selected router. External neighbors have a different AS number.

Element	Description
IP Address	The IP addresses of the hosts that are neighbors of the router. BGP neighbors exchange routing information with each other whenever changes to the routing table are detected. When you define BGP neighbors, the IP addresses cannot belong to an interface on the selected router. In addition, you cannot define the same IP address in more than one AS. Enter one or more addresses or network/host objects, or click **Select** to select an object from a list or to create a new one. **Note** To remove a host from the list of BGP neighbors, select it from the Hosts field, then click **Delete**.

BGP Page—Redistribution Tab

Use the BGP Redistribution tab to view, create, edit, and delete redistribution settings when performing redistribution into a BGP autonomous system (AS).

Note You must define BGP setup parameters before you can access the BGP Redistribution tab. See BGP Page—Setup Tab , on page 5.

Navigation Path

Go to the BGP Routing Policy Page , on page 4, then click the **Redistribution** tab.

Related Topics

- Redistributing Routes into BGP , on page 3
- BGP Page—Setup Tab , on page 5
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 3: BGP Redistribution Tab

Element	Description
Protocol	The protocol that is being redistributed.
AS/Process ID	The AS number or process ID of the route being redistributed.
Metric	The value that determines the priority of the redistributed route.
Match	When redistributing an OSPF process, indicates the types of OSPF routes that are being redistributed.

Element	Description
Static Type	When redistributing static routes, indicates the type of static route, IP or OSI.
Add button	Opens the BGP Redistribution Mapping Dialog Box , on page 8. From here you can define BGP redistribution mappings.
Edit button	Opens the BGP Redistribution Mapping Dialog Box , on page 8. From here you can edit the selected BGP redistribution mapping.
Delete button	Deletes the selected BGP redistribution mappings from the table.

BGP Redistribution Mapping Dialog Box

Use the BGP Redistribution Mapping dialog box to add or edit the properties of a BGP redistribution mapping.

Navigation Path

Go to the BGP Page—Redistribution Tab , on page 7, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Redistributing Routes into BGP , on page 3

Field Reference

Table 4: BGP Redistribution Mapping Dialog Box

Element	Description
Protocol to Redistribute	The routing protocol that is being redistributed: • Static—Redistributes IP or OSI static routes. You can define a single mapping for each route. • EIGRP—Redistributes an EIGRP autonomous system. Enter the AS number in the displayed field. You can define a single mapping for each AS. • RIP—Redistributes RIP routes. You can define a single mapping for each route. • OSPF—Redistributes a different OSPF process. You can define a single mapping for each process. Select a process from the displayed list, then select one or more match criteria: • Internal—Routes that are internal to a specific AS. • External1—Routes that are external to the AS and imported into OSPF as a Type 1 external route. • External2—Routes that are external to the AS and imported into the selected process as a Type 2 external route. • NSAAExternal1—Not-So-Stubby Area (NSSA) routes that are external to the AS and imported into the selected process as Type 1 external routes. • NSAAExternal2—(NSSA) routes that are external to the AS and imported into the selected process as Type 2 external routes. • Connected—Redistributes routes that are established automatically by virtue of having enabled IP on an interface. These routes are redistributed as external to the AS.
Metric	A value representing the cost of the redistributed route. Valid values range from 0 to 4294967295.

EIGRP Routing on Cisco IOS Routers

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced distance vector protocol developed by Cisco Systems that integrates the capabilities of link-state protocols. EIGRP is suited for many different topologies and media. Key capabilities that distinguish EIGRP from other routing protocols are fast convergence, support for variable-length subnet masks, partial updates, and multiple network-layer protocols. .

The metric that the router uses to reach the destination, and to advertise to other routers, is the sum of the best-advertised metrics from all neighbors and the link cost to the best neighbor.

EIGRP uses neighbor tables to store address and interface information about each of the router’s neighbors. Hello packets advertise hold times, which is the length of time a neighbor can be considered reachable and operational. Topology tables contain all destinations advertised by neighboring routers. For each neighbor, the entry records the advertised metric, which the neighbor stores in its routing table.

A router running EIGRP stores all its neighbors’ routing tables so that it can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbors to discover an alternate route. These queries propagate until an alternate route is found. EIGRP sends incremental updates when the state of a destination changes, instead of sending the entire contents of the routing table. EIGRP ensures that only those routers needing the information are updated. This feature minimizes the bandwidth required for EIGRP packets.

EIGRP supports both internal and external routes. Internal routes originate within an EIGRP Autonomous System (AS). Therefore, a directly attached network that is configured to run EIGRP is considered an internal route and is propagated with this information throughout the AS. External routes are learned by another routing protocol or reside in the routing table as static routes. These routes are tagged individually with the identity of their origin.

The following topics describe the tasks you perform to create an EIGRP routing policy:

- Defining EIGRP Routes , on page 10
- Defining EIGRP Interface Properties , on page 11
- Redistributing Routes into EIGRP , on page 13

Related Topics

- Static Routing on Cisco IOS Routers , on page 59
- RIP Routing on Cisco IOS Routers , on page 50
- OSPF Routing on Cisco IOS Routers , on page 27
- BGP Routing on Cisco IOS Routers , on page 1

Defining EIGRP Routes

To configure an EIGRP routing policy, you must assign each autonomous system a number, which identifies the autonomous system to other routers. You then must select the networks to which routes will be created. In addition, you can select which interfaces should be passive. Unlike other routing protocols, passive interfaces in EIGRP neither send nor receive routing updates from their neighbors, resulting in the loss of their neighbor relationship.

When you configure EIGRP routing policies, you can also decide whether to enable auto-summarization, which greatly simplifies routing tables and the exchange of routing information by having many subnets represented by a single network entry.

Related Topics

- Defining EIGRP Interface Properties , on page 11
- Redistributing Routes into EIGRP , on page 13
- EIGRP Routing on Cisco IOS Routers , on page 9

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **EIGRP** from the Policy selector, then click the **Setup** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **EIGRP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Setup** tab.

The EIGRP Setup tab is displayed (see EIGRP Page—Setup Tab , on page 21).

Step 2 On the EIGRP Setup tab, select an EIGRP route from the table, then click **Edit**, or click **Add** to create a route. The EIGRP Setup dialog box appears. See Table 6: EIGRP Setup Dialog Box , on page 22 for a description of the fields in this dialog box.

Step 3 Enter the autonomous system number for the route. This number identifies the autonomous system to other routers.

Step 4 Enter the addresses of the passive interfaces, which are interfaces that should not send routing updates to their neighbors, if any. Enter the names of one or more interfaces or interface roles; separate addresses with commas. Click **Select** to select interface names or roles from a list of existing objects, or to create new interface role objects. For more information, see Specifying IP Addresses During Policy Definition.

Step 5 Click **OK** to save your definitions. The EIGRP route appears in the table displayed in the EIGRP Setup tab.

Defining EIGRP Interface Properties

You can optionally modify the default values of the following two interface properties in a selected EIGRP autonomous system:

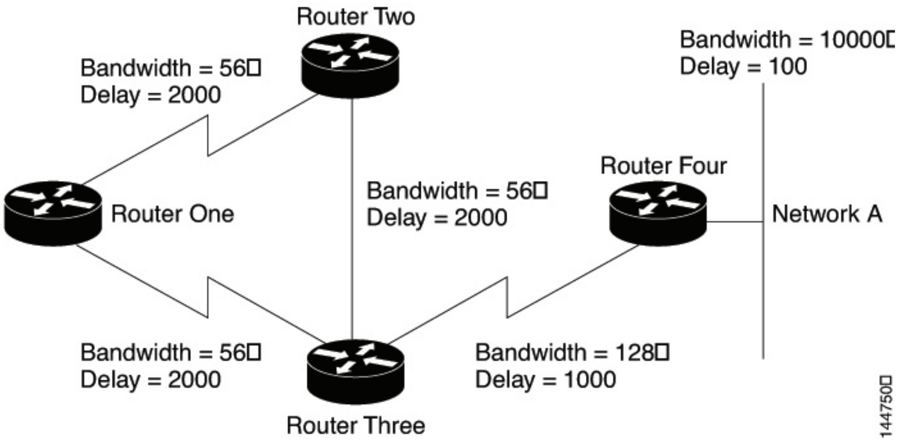
- Hello interval.
- Split horizon.

The hello interval defines the interval between hello packets. Routing devices periodically send these packets to each other to dynamically learn of other routers on their directly attached networks. This information is used to discover neighbors and to learn when neighbors become unreachable or inoperative. By default, hello packets are sent every 5 seconds. The default interval for low speed (T1 or slower), nonbroadcast multiaccess (NBMA) media is every 60 seconds.

Split horizon is a feature that prevents route information from being sent back in the direction from which that information originated. If you enable split horizon on an interface (this is the default), update and query packets are not sent to destinations for which this interface is the next hop. This helps to prevent routing loops.

For example, as shown in Figure 1: EIGRP Split Horizon Example, on page 12, if Router One is connected to Routers Two and Three through a single multipoint interface, and Router One learned about Network A from Router Two, Router One does not advertise the route to Network A over that same multipoint interface to Router Three. Router One assumes that Router Three would learn about Network A directly from Router Two.

Figure 1: EIGRP Split Horizon Example



Split horizon is enabled by default on all EIGRP interfaces, because it typically optimizes communications among multiple routing devices. However, in certain cases with nonbroadcast networks (such as Frame Relay and SMDS), you might want to disable split horizon.

If you decide to disable split horizon on an EIGRP interface, keep the following in mind:

- In a hub-and-spoke network, you should disable split horizon only at the hub. This is because disabling split horizon on the spokes greatly increases EIGRP memory consumption on the hub router, as well as the amount of traffic generated on the spoke routers.
- Changing the split horizon setting on an interface resets all adjacencies with the EIGRP neighbors that are reachable over that interface.

Before You Begin

- Define at least one EIGRP autonomous system. See Defining EIGRP Routes , on page 10.

Related Topics

- Defining EIGRP Routes , on page 10
- Redistributing Routes into EIGRP , on page 13
- EIGRP Routing on Cisco IOS Routers , on page 9

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **EIGRP** from the Policy selector, then click the **Interfaces** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **EIGRP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Interfaces** tab.

The EIGRP Interfaces tab is displayed. See Table 7: EIGRP Interfaces Tab , on page 23 for a description of the fields on this tab.

Step 2 On the EIGRP Interfaces tab, select an interface from the table, then click **Edit**, or click **Add** to create an interface definition. The EIGRP Interface dialog box appears. See Table 8: EIGRP Interface Dialog Box , on page 24 for a description of the fields in this dialog box.

Step 3 Select the AS number of the autonomous system whose interface properties you want to modify. See Defining EIGRP Routes , on page 10 for more information about defining an autonomous system.

Step 4 Enter the name of the interface or interface role to define, or click **Select** to select an interface role from a list or to create a new one. For more information, see Specifying IP Addresses During Policy Definition.

Step 5 (Optional) In the Hello Interval field, modify the default interval between hello packets sent over the selected interfaces.

The default is 5 seconds for all interfaces, except for low-speed (T1 or less) NBMA media, for which the default interval is 60 seconds.

Step 6 (Optional) Deselect the **Split Horizon** check box to disable the split horizon feature. If you disable this feature, the selected interfaces can advertise a route out of the interface from which they learned the route.

Note In general, we recommend that you not disable split horizon unless you are certain that your application requires the change to properly advertise routes. If you disable split horizon on a serial interface, and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in all relevant multicast groups on that network.

Step 7 Click **OK** to save your definitions locally on the client and close the dialog box. The interface definition appears in the table on the EIGRP Interfaces tab.

Redistributing Routes into EIGRP

Redistribution refers to using a routing protocol, such as EIGRP, to advertise routes that are learned by some other means, such as a different routing protocol, static routes, or directly connected routes. For example, you can redistribute routes from the RIP routing protocol into your EIGRP autonomous system (AS). Redistribution is necessary in networks that operate in multiple-protocol environments and can be applied to all IP-based routing protocols.

Before You Begin

- Define at least one EIGRP autonomous system. See Defining EIGRP Routes , on page 10.

Related Topics

- Defining EIGRP Routes , on page 10
- Defining EIGRP Interface Properties , on page 11
- EIGRP Routing on Cisco IOS Routers , on page 9

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **EIGRP** from the Policy selector, then click the **Redistribution** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **EIGRP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Redistribution** tab.

The EIGRP Redistribution tab is displayed. See Table 9: EIGRP Redistribution Tab , on page 25 for a description of the fields on this tab.

Step 2 On the EIGRP Redistribution tab, select a row from the EIGRP Redistribution Mappings table, then click **Edit**, or click **Add** to create a mapping. The EIGRP Redistribution Mapping dialog box appears. See Table 10: EIGRP Redistribution Mapping Dialog Box , on page 26 for a description of the fields in this dialog box.

Step 3 Select an existing EIGRP AS from the displayed list.

Step 4 Select the protocol whose routes you want to redistribute into the selected EIGRP AS.

Note You can create a single mapping for each static route, RIP route, BGP AS, EIGRP AS, and OSPF process.

Step 5 (Optional) Under Metrics, modify the default metric (cost) of the redistributed routes by entering values in the fields used to calculate the metric. The metric determines the priority of the routes.

Note Entering a metric is optional, but if you do specify a value, you must enter values for all five parameters. You need not define metric values when redistributing one EIGRP process into another.

Step 6 Click **OK** to save your definitions locally on the client and close the dialog box. The redistribution mapping appears in the Redistribution Mapping table in the EIGRP Redistribution tab.

EIGRPv6

Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced distance vector protocol developed by Cisco Systems that integrates the capabilities of link-state protocols. From version 4.27, EIGRPv6 is supported. EIGRPv6 is an enhancement to EIGRP with IPv6. IPv6 support was added for routing data, performing authentication, and redistributing and monitoring routing information using the Enhanced Interior Gateway Routing Protocol (EIGRP). EIGRPv6 feature is Supported in ASA 9.20(1) and above in Single context mode. It is not supported in Multi context and Transparent mode.

The following topics describe the tasks you perform to create an EIGRPv6 routing policy:

- Defining IPv6 EIGRP Routes , on page 14
- Defining Filtering Rules for EIGRPv6, on page 15
- Defining Neighbors for EIGRPv6, on page 16
- Redistributing Routes into EIGRPv6 , on page 17
- Defining Address Summary for EIGRPv6, on page 18
- Defining EIGRPv6 Interface Properties , on page 19

Defining IPv6 EIGRP Routes

To configure an EIGRPv6 routing policy, you must enable IPv6 EIGRP and then assign each autonomous system a number which identifies the autonomous system to other routers. You can then select the Advanced option to configure settings such as the router ID, stub routing, and adjacency changes.

Related Topics

- Defining EIGRPv6 Interface Properties , on page 19
- Defining Filtering Rules for EIGRPv6, on page 15

- Defining Neighbors for EIGRPv6, on page 16
- Defining Address Summary for EIGRPv6, on page 18
- Redistributing Routes into EIGRPv6 , on page 17
- EIGRPv6, on page 14

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **EIGRP** from the Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform** > **Routing** > **EIGRP** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Click the **IPv6 Family** tab.

Step 3 Enter the autonomous system number for the route. This number identifies the autonomous system to other routers.

Step 4 Select the **Advanced** tab to configure settings such as router ID, stub routing, and adjacency changes. See IPv6 EIGRP Advanced for a description of the fields in this dialog box.

Step 5 On the **Setup** tab, select or enter the values in the dialog box. See Setup Tab for all the description of the fields in this tab.

Step 6 Click on **Filter** tab, then click the **Add** or **Edit** button beneath the table. See Add/Edit IPv6 EIGRP Filter Rule Page Dialog Box for all the description of the fields in this tab.

Step 7 Select the **Naeighbors** tab, then click the **Add** or **Edit** button beneath the table. See Add/Edit EIGRP Neighbor Dialog Box for the description of fields in this tab.

Step 8 Select the **Redistribution** tab, then click the **Add** or **Edit** button beneath the table. See Add/Edit EIGRP Redistribution Dialog Box for the description of fields in this tab.

Step 9 Select the **Summary Address** tab, then click the **Add** or **Edit** button beneath the table. See Add/Edit IPv6 EIGRP Summary Address Page Dialog Box for the description of fields in this tab.

Step 10 Select the **Interfaces** tab, then click the **Add** or **Edit** button beneath the table. SeeAdd/Edit IPv6 EIGRP Interface Page Dialog Box for the description of fields in this tab.

Step 11 Click **Save** to save your definitions.

Defining Filtering Rules for EIGRPv6

Use the route filtering rules configured for the EIGRPv6 routing process. Filter rules let you control which routes are accepted or advertised by the EIGRPv6 routing process.

- Define at least one EIGRPv6 autonomous system. See Defining IPv6 EIGRP Routes , on page 14.

Related Topics

- Defining IPv6 EIGRP Routes , on page 14
- Defining Neighbors for EIGRPv6, on page 16
- EIGRPv6 Page—Redistribution Tab
- Defining Address Summary for EIGRPv6, on page 18

- Defining EIGRPv6 Interface Properties , on page 19
- EIGRPv6, on page 14

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **EIGRP** from the Policy selector, then click the **Filter Rule** tab in the work area.
- (Policy view) Select **PIX/ASA/FWSM Platform** > **Routing** > **EIGRP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Filter Rules** tab.

The IPv6 Filter Rules tab is displayed. See for a description of the fields on this tab

Step 2 On the Filter Rules tab, select a row from the IPv6 Filter Rules Mappings table, then click **Edit**, or click **Add** to create a filter rule. See Add/Edit EIGRP Filter Rule Dialog Box for a description of the fields in this dialog box.

Step 3 Select the direction for the Filter Rule from the dropdown list.

Step 4 Select the Interface from the Interface Selector dialog box to which you want to add the Filter Rule.

Step 5 Select the IPv6 prefix list name from the Prefix List Object IPv6 Selector to which networks are to be received and suppressed in routing updates.

Step 6 Click **OK** to save your definitions locally on the client and close the dialog box. The Filter Rules definitions will appear in the table on the EIGRPv6 Filter Rules tab.

Defining Neighbors for EIGRPv6

The Neighbors tab contains the Neighbors table, through which you can define neighbors for EIGRPv6. When you manually define an EIGRPv6 neighbor, hello packets are sent to that neighbor as unicast messages.

- Define at least one EIGRPv6 autonomous system. See Defining IPv6 EIGRP Routes , on page 14.

Related Topics

- Defining IPv6 EIGRP Routes , on page 14
- Defining Filtering Rules for EIGRPv6, on page 15
- Defining Address Summary for EIGRPv6, on page 18
- Redistributing Routes into EIGRPv6 , on page 17
- Defining EIGRPv6 Interface Properties , on page 19
- EIGRPv6, on page 14

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **EIGRP** from the Policy selector, then click the **Neighbors** tab in the work area.

- (Policy view) Select **PIX/ASA/FWSM Platform** > **Routing** > **EIGRP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Neighbors** tab.

The IPv6 Neighbors tab is displayed. See Neighbors Tab for a description of the fields on this tab

Step 2 On the Neighbors tab, select a row from the IPv6 Neighbors table, then click **Edit**, or click **Add** to add a neighbor. See Neighbors Tab for the description of fields in this dialog box.

Step 3 Select the Interface from the Interface Selector dialog box through which the neighbor is available.

Step 4 Select/Enter the IPv6 address of the neighbor.

Note You can click **Select** to select the neighbor from a list of host-objects.

Step 5 Click **OK** to save your definitions locally on the client and close the dialog box. The neighbor will appear in the table on the IPv6 neighbor tab.

Redistributing Routes into EIGRPv6

Redistribution refers to using a routing protocol, such as EIGRPv6, to advertise routes that are learned by some other means, such as a different routing protocol, static routes, or directly connected routes. For example, you can redistribute routes from the BGP routing protocol into your EIGRPv6 autonomous system (AS). Redistribution is necessary in networks that operate in multiple-protocol environments and can be applied to all IP-based routing protocols.

Before You Begin

- Define at least one EIGRPv6 autonomous system. See Defining IPv6 EIGRP Routes , on page 14.

Related Topics

- Defining IPv6 EIGRP Routes , on page 14
- Defining EIGRPv6 Interface Properties , on page 19
- Defining Filtering Rules for EIGRPv6, on page 15
- Defining Neighbors for EIGRPv6, on page 16
- Defining Address Summary for EIGRPv6, on page 18
- EIGRPv6, on page 14

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **EIGRP** from the Policy selector, click the **IPv6 Family** tab, and then click the **Redistribution** tab in the work area.
- (Policy view) Select **PIX/ASA/FWSM Platform** > **Routing** > **EIGRP** from the Policy Type selector. Select an existing policy or create a new one. Click the **IPv6 Family** tab and click the **Redistribution** tab.

The EIGRPv6 Redistribution tab is displayed. See Redistribution Tab for the description of fields on this tab.

Step 2 On the EIGRPv6 Redistribution tab, select a row from the EIGRPv6 Redistribution Mappings table, then click **Edit**, or click **Add** to create a mapping. The EIGRPv6 Redistribution Mapping dialog box appears. See Add/Edit IPv6 EIGRP Redistribution Dialog Box for the description of fields in this dialog box.

Step 3 Select the protocol whose routes you want to redistribute into the selected EIGRPv6 AS.

Note You can create a single mapping for each static route, Connected, BGP, OSPF process, and ISIS.

Step 4 (Optional) Under Optional Metrics, modify the default metric (cost) of the redistributed routes by entering values in the fields used to calculate the metric. The metric determines the priority of the routes.

Note Entering a metric is optional, but if you do specify a value, you must enter values for all five parameters. You need not define metric values when redistributing one EIGRPv6 process into another.

Step 5 (Optional) Click or Select to open the **Route Map Object Selector** from which you can select a route map object. You can also create new route map objects from the Route Map Object Selector

Step 6 (Optional) If you have chosen ISIS as the Route Type, choose the ISIS level from the drop down list. The available levels are Level 1, Level 1-2, and Level 2.

Step 7 (Optional) If you have chosen OSPF as the Route Type, choose the conditions used for redistributing routes from one routing protocol to another. The routes must match the selected condition to be redistributed.

Step 8 Click **OK** to save your definitions locally on the client and close the dialog box. The redistribution mapping appears in the Redistribution Mapping table in the EIGRPv6 Redistribution tab.

Defining Address Summary for EIGRPv6

You can use the Summary Address tab to configure a summary for EIGRPv6 on a specific interface. You can configure summary addresses on a per-interface basis. You need to manually define summary addresses if you want to create summary addresses that do not occur at a network number boundary or if you want to use summary addresses on an ASA with automatic route summarization disabled. If any more specific routes are in the routing table, EIGRPv6 will advertise the summary address out the interface with a metric equal to the minimum of all more specific routes.

- Define at least one EIGRPv6 autonomous system. See Defining IPv6 EIGRP Routes , on page 14.

Related Topics

- Defining IPv6 EIGRP Routes , on page 14
- Defining Filtering Rules for EIGRPv6, on page 15
- Defining Neighbors for EIGRPv6, on page 16
- Redistributing Routes into EIGRPv6 , on page 17
- Defining EIGRPv6 Interface Properties , on page 19
- EIGRPv6, on page 14

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **EIGRP** from the Policy selector, then click the **Address Summary** tab in the work area.

- (Policy view) Select **PIX/ASA/FWSM Platform** > **Routing** > **EIGRP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Address Summary** tab.

The IPv6 Address Summary tab is displayed. See Summary Address Tab for th description of fields on this tab

Step 2 On the Address Summary tab, select a row from the IPv6 Address Summary table, then click **Edit**, or click **Add** to create a summary for EIGRPv6. See Add/Edit IPv6 EIGRP Summary Address Page Dialog Box for the description of fields in this dialog box.

Step 3 Select the Interface from the Interface Selector dialog box through which the neighbor is available.

Step 4 Select/Enter the network mask of the summary address.

Note You can click **Select** to select the network mask from a list of host-objects.

Step 5 Enter the administrative distance of the summary route.

Note The value should be in between 1-255.

Step 6 Click **OK** to save your definitions locally on the client and close the dialog box. The Summary Address definitions will appear in the table on the EIGRPv6 Summary Address tab.

Defining EIGRPv6 Interface Properties

You can optionally modify the default values of the following two interface properties in a selected EIGRPv6 autonomous system:

- Hello interval—The hello interval defines the interval between hello packets. Routing devices periodically send these packets to each other to dynamically learn of other routers on their directly attached networks. This information is used to discover neighbors and to learn when neighbors become unreachable or inoperative.

- Split horizon—Split horizon is a feature that prevents route information from being sent back in the direction from which that information originated. If you enable split horizon on an interface (this is the default), update and query packets are not sent to destinations for which this interface is the next hop. This helps to prevent routing loops.

- Hold Time—The number of seconds the router will wait to receive a hello message before invalidating the connection.

Split horizon is enabled by default on all EIGRPv6 interfaces, because it typically optimizes communications among multiple routing devices. However, in certain cases with nonbroadcast networks (such as Frame Relay and SMDS), you might want to disable split horizon.

If you decide to disable split horizon on an EIGRPv6 interface, keep the following in mind:

- In a hub-and-spoke network, you should disable split horizon only at the hub. This is because disabling split horizon on the spokes greatly increases EIGRPv6 memory consumption on the hub router, as well as the amount of traffic generated on the spoke routers.

- Changing the split horizon setting on an interface resets all adjacencies with the EIGRPv6 neighbors that are reachable over that interface.

Before You Begin

- Define at least one EIGRPv6 autonomous system. See Defining IPv6 EIGRP Routes , on page 14.

Related Topics

- Defining IPv6 EIGRP Routes , on page 14
- Defining Filtering Rules for EIGRPv6, on page 15
- Defining IPv6 EIGRP Routes , on page 14
- Redistributing Routes into EIGRPv6 , on page 17
- EIGRPv6, on page 14

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **EIGRP** from the Policy selector, click the **IPv6 Family** tab, and then click the **Interfaces** tab in the work area.
- (Policy view) Select **PIX/ASA/FWSM Platform** > **Routing** > **EIGRP** from the Policy Type selector. Select an existing policy or create a new one. Click the **IPv6 Family** tab and click the **Interfaces** tab.

The EIGRPv6 Interfaces tab is displayed. See Interfaces Tab for a description of the fields on this tab.

Step 2 On the EIGRPv6 Interfaces tab, select an interface from the Interface Selector tab, then click **Ok**. The EIGRPv6 Interface dialog box appears. See Add/Edit IPv6 EIGRP Interface Page Dialog Box for a description of the fields in this dialog box.

Step 3 (Optional) In the Hello Interval field, modify the default interval between hello packets sent over the selected interfaces.

The default is 5 seconds for all interfaces, except for low-speed (T1 or less) NBMA media, for which the default interval is 60 seconds.

Step 4 (Optional) In the Hello Time field, modify the number of seconds router will wait to receive a hello message before invalidating the connection.

Note The range is between 1 and 65535. The default hold time is 15 seconds (three times the hello interval).

Step 5 (Optional) Deselect the **Split Horizon** check box to disable the split horizon feature. If you disable this feature, the selected interfaces can advertise a route out of the interface from which they learned the route.

Note In general, we recommend that you not disable split horizon unless you are certain that your application requires the change to properly advertise routes. If you disable split horizon on a serial interface, and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in all relevant multicast groups on that network.

Step 6 Click **OK** to save your definitions locally on the client and close the dialog box. The interface definition appears in the table on the EIGRPv6 Interfaces tab.

EIGRP and EIGRPv6 Routing Policy Page

Enhanced Interior Gateway Routing Protocol (EIGRP) is a scalable interior gateway protocol that provides extremely quick convergence times with minimal network traffic.

You can configure EIGRP routing policies from the following tabs on the EIGRP Routing page:

- EIGRP Page—Setup Tab , on page 21
- EIGRP Page—Interfaces Tab , on page 23
- EIGRP Page—Redistribution Tab , on page 24

For more information, see EIGRP Routing on Cisco IOS Routers , on page 9.

Navigation Path

- (Device view) Select **Platform** > **Routing** > **EIGRP** from the Policy selector.
- (Policy view) Select **Router Platform** > **Routing** > **EIGRP** from the Policy Type selector. Right-click **EIGRP** to create a policy, or select an existing policy from the Shared Policy selector.

EIGRP Page—Setup Tab

Use the EIGRP Setup tab to view, create, edit, and delete EIGRP routes.

Navigation Path

Go to the EIGRP and EIGRPv6 Routing Policy Page , on page 20, then click the **Setup** tab.

Related Topics

- Defining EIGRP Routes , on page 10
- EIGRP Page—Interfaces Tab , on page 23
- EIGRP Page—Redistribution Tab , on page 24
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 5: EIGRP Setup Tab

Element	Description
AS Number	The autonomous system number that identifies the autonomous system to other routers.
Networks	The names of the networks included in the route.
Passive Interfaces	The interfaces that neither send nor receive routing updates from their neighbors.
Auto-Summary	Indicates whether auto summarization is activated on the selected route.
Add button	Opens the EIGRP Setup Dialog Box , on page 22. From here you can create an EIGRP route.

Element	Description
Edit button	Opens the EIGRP Setup Dialog Box , on page 22. From here you can edit the selected EIGRP route.
Delete button	Deletes the selected EIGRP routes from the table.

EIGRP Setup Dialog Box

Use the EIGRP Setup dialog box to add or edit EIGRP routes.

Navigation Path

Go to the EIGRP Page—Setup Tab , on page 21, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining EIGRP Routes , on page 10
- Specifying IP Addresses During Policy Definition
- Understanding Networks/Hosts Objects

Field Reference

Table 6: EIGRP Setup Dialog Box

Element	Description
AS Number	The autonomous system number for the EIGRP route. This number is used to identify the autonomous system to other routers. Valid values are from 1 to 65535.
Networks	The networks associated with the EIGRP route. Enter one or more network addresses or network/host objects, separated by commas. Click **Select** to select network/host objects from a list of existing objects, or to create new objects.
Passive Interfaces	The interfaces that do not send updates to their routing neighbors. Enter one or more interface names or roles, separated by commas. Click **Select** to select interface names or roles from a list of existing objects, or to create new interface role objects. **Note** When you make an interface passive, EIGRP suppresses the exchange of hello packets between routers, resulting in the loss of their neighbor relationship. This not only stops routing updates from being advertised but also suppresses incoming routing updates.
Auto-Summary	When selected, enables the automatic summarization of subnet routes into network-level routes. Summarization reduces the size of routing tables, thereby reducing the complexity of the network. When deselected, automatic summarization is disabled.

EIGRP Page—Interfaces Tab

Use the EIGRP Interfaces tab to create, edit, and delete interface properties for selected EIGRP autonomous systems. This includes modifying the default hello interval and disabling split horizon.

Note You can access the EIGRP Interfaces tab only after defining at least one EIGRP autonomous system in the Setup tab. See EIGRP Page—Setup Tab , on page 21.

Navigation Path

Go to the EIGRP and EIGRPv6 Routing Policy Page , on page 20, then click the **Interfaces** tab.

Related Topics

- Defining EIGRP Interface Properties , on page 11
- EIGRP Page—Setup Tab , on page 21
- EIGRP Page—Redistribution Tab , on page 24
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 7: EIGRP Interfaces Tab

Element	Description
AS Number	The EIGRP autonomous system number for which interface properties are defined.
Interfaces	The interfaces related to the selected EIGRP autonomous system that have specially defined values.
Split Horizon	Indicates whether the split horizon feature is enabled or disabled for the selected interface.
Hello Interval	The defined interval between hello packets sent to neighboring routers.
Add button	Opens the EIGRP Interface Dialog Box , on page 24. From here you can create an EIGRP interface definition.
Edit button	Opens the EIGRP Interface Dialog Box , on page 24. From here you can edit the selected EIGRP interface definition.
Delete button	Deletes the selected EIGRP interface definitions from the table.

EIGRP Interface Dialog Box

Use the EIGRP Interface dialog box to add or edit interface definitions for a selected EIGRP autonomous system.

Navigation Path

Go to the EIGRP Page—Interfaces Tab , on page 23, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining EIGRP Interface Properties , on page 11
- Basic Interface Settings on Cisco IOS Routers
- Understanding Interface Role Objects

Field Reference

Table 8: EIGRP Interface Dialog Box

Element	Description
AS Number	Selects the EIGRP autonomous system number whose interface properties you want to modify. For more information about EIGRP autonomous systems, see EIGRP Setup Dialog Box , on page 22.
Interface	Specifies the EIGRP interface you wish to configure. Enter the name of an interface or interface role, or click **Select** to select an interface role object from a list or to create a new one.
Hello Interval	The default interval between hello packets sent by the router to its neighbors. Routers send hello packets to each other to dynamically learn of other routers on their directly attached networks. Valid values range from 1 to 65535 seconds. The default is 5 seconds.
Split Horizon	When selected, the split horizon feature is used to prevent routing loops. When deselected, split horizon is disabled. When split horizon is disabled, the router can advertise a route out of the same interface through which it learned the route. Disabling split horizon is often useful when dealing with nonbroadcast networks, such as Frame Relay and SMDS. **Note** Changing the split horizon setting on an interface resets all adjacencies with EIGRP neighbors that are reachable over that interface.

EIGRP Page—Redistribution Tab

Use the EIGRP Redistribution tab to create, edit, and delete EIGRP redistribution mappings.

Navigation Path

Go to the EIGRP and EIGRPv6 Routing Policy Page , on page 20, then click the **Redistribution** tab.

Related Topics

- Redistributing Routes into EIGRP , on page 13
- EIGRP Page—Setup Tab , on page 21
- EIGRP Page—Interfaces Tab , on page 23
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 9: EIGRP Redistribution Tab

Element	Description
EIGRP AS Number	The area ID of the EIGRP route into which other routes are being redistributed.
Protocol	The protocol that is being redistributed.
AS/Process ID	The AS number or process ID of the route being redistributed.
Bandwidth	The minimum bandwidth of the path for the EIGRP route, as defined for the route metric.
Delay	The mean latency of the path, as defined for the route metric.
Reliability	A value representing the estimated reliability of the path, as defined for the route metric.
Effective Bandwidth	A value representing the effective load on the link, as defined for the route metric.
MTU	The minimum MTU of the path, as defined for the route metric.
Match	When redistributing an OSPF process, indicates the types of OSPF routes that are being redistributed.
Add button	Opens the EIGRP Redistribution Mapping Dialog Box , on page 25. From here you can define EIGRP redistribution mappings.
Edit button	Opens the EIGRP Redistribution Mapping Dialog Box , on page 25. From here you can edit the selected EIGRP redistribution mapping.
Delete button	Deletes the selected EIGRP redistribution mappings from the table.

EIGRP Redistribution Mapping Dialog Box

Use the EIGRP Redistribution Mapping dialog box to add or edit the properties of an EIGRP redistribution mapping.

Navigation Path

Go to the EIGRP Page—Redistribution Tab , on page 24, then click the **Add** or **Edit** button beneath the table.

Note You must create at least one EIGRP AS before you can access the EIGRP Redistribution dialog box. See EIGRP Page—Setup Tab , on page 21.

Related Topics

- Redistributing Routes into EIGRP , on page 13

Field Reference

Table 10: EIGRP Redistribution Mapping Dialog Box

Element	Description
EIGRP AS Numbers	The EIGRP AS into which other routes are being redistributed. You must select an ID number from the list of EIGRP autonomous systems defined in the EIGRP Page—Setup Tab , on page 21.
Protocol to Redistribute	The routing protocol that is being redistributed: • Static—Redistributes static routes. You can define a single mapping for each route. • EIGRP—Redistributes an EIGRP autonomous system. Enter the AS number in the displayed field. You can define a single mapping for each AS. • BGP—Redistributes a BGP autonomous system. You can define a single BGP mapping on each device. If you configured a BGP AS in the BGP Setup tab, the AS number is displayed. Otherwise, a message is displayed indicating that no BGP AS was defined. See BGP Page—Redistribution Tab , on page 7.
Protocol to Redistribute (continued)	• OSPF—Redistributes a different OSPF process. You can define a single mapping for each process. Select a process from the displayed list, then select one or more match criteria: • Internal—Routes that are internal to a specific AS. • External1—Routes that are external to the AS and imported into OSPF as a Type 1 external route. • External2—Routes that are external to the AS and imported into the selected process as a Type 2 external route. • NSAAExternal1—Not-So-Stubby Area (NSSA) routes that are external to the AS and imported into the selected process as Type 1 external routes. • NSAAExternal2—(NSSA) routes that are external to the AS and imported into the selected process as Type 2 external routes. • RIP—Redistributes RIP routes. • Connected—Redistributes routes that are established automatically by virtue of having enabled IP on an interface. These routes are redistributed as external to the AS.

Element	Description
Metrics	The default metric (cost) of the redistributed route. Metric parameters include: • Bandwidth—The minimum bandwidth of the path in kilobits per second. Valid values range from 1 to 4294967295. • Delay—The mean latency of the path in units of 10 microseconds. Valid values range from 0 to 4294967295. • Reliability—A value expressing the estimated reliability of the link. Valid values range from 0 to 255, where 255 represents 100% reliability. • Effective Bandwidth—A value expressing the effective load on the link. Valid values range from 1 to 255, where 255 represents 100% utilization. • MTU of Path—The maximum transmission unit of the path. Valid values range from 1 to 65535 bytes.

OSPF Routing on Cisco IOS Routers

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

Open Shortest Path First (OSPF) is an interior gateway routing protocol that uses link states instead of distance vectors to distribute routing information within a single autonomous system (AS). OSPF propagates link-state advertisements (LSAs) instead of routing table updates, which allows OSPF networks to converge more quickly than RIP networks. You define areas to limit the number of LSAs that need to be propagated to changes that occur within the area.

A router that has interfaces in multiple OSPF areas is called an Area Border Router (ABR). An ABR uses LSAs to send information about available routes to other OSPF routers. A router that acts as a gateway to redistribute traffic between routers using OSPF and routers using other routing protocols is called an Autonomous System Boundary Router (ASBR). Any router can act as an ABR or ASBR.

The following topics describe the tasks you perform to create an OSPF routing policy:

- Defining OSPF Process Settings , on page 28
- Defining OSPF Area Settings , on page 28
- Redistributing Routes into OSPF , on page 30
- Defining OSPF Interface Settings , on page 32

Related Topics

- Static Routing on Cisco IOS Routers , on page 59
- RIP Routing on Cisco IOS Routers , on page 50
- EIGRP Routing on Cisco IOS Routers , on page 9

- BGP Routing on Cisco IOS Routers , on page 1

Defining OSPF Process Settings

You configure OSPF process parameters by specifying a process ID number, which identifies the OSPF process to other routers, and by deciding whether any interfaces should be passive. Passive interfaces do not send routing updates to their neighbors.

Related Topics

- Defining OSPF Area Settings , on page 28
- Defining OSPF Interface Settings , on page 32
- Redistributing Routes into OSPF , on page 30
- OSPF Routing on Cisco IOS Routers , on page 27

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **OSPF Process** from the Policy selector, then click the **Setup** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **OSPF Process** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Setup** tab.

The OSPF Process Setup tab is displayed. See Table 13: OSPF Process Setup Tab , on page 43 for a description of the fields on this tab.

Step 2 On the OSPF Process Setup tab, select an OSPF process from the table, then click **Edit**, or click **Add** to create a process. The OSPF Setup dialog box appears. See Table 14: OSPF Setup Dialog Box , on page 44 for a description of the fields in this dialog box.

Step 3 Enter the process ID number in the field provided. The process ID defined here does not need to match the process ID on any other devices.

Step 4 Define which interfaces should not send routing updates to its neighbors:

a) Click **Edit** under Passive Interfaces to display the Edit Interfaces dialog box. Use this dialog box to define which interfaces should *not* send routing updates to its neighbors.
b) Enter the names of one or more interfaces or interface roles, or click **Select** to select an interface role from a list or to create a new one. For more information, see Specifying IP Addresses During Policy Definition.
c) Click **OK** to save your changes and return to the OSPF Setup dialog box.

Step 5 Click **OK** to save your definitions locally on the client and close the dialog box.

Defining OSPF Area Settings

You configure OSPF area settings by associating an area ID with a particular OSPF process, selecting the networks included in the area, and selecting the type of authentication used by the routers in the area.

Each OSPF process that you define should contain at least one defined area. If you define more than one area, one area must be area 0. This is called the backbone. All other areas must be physically connected to the backbone. This enables other areas to inject routing information into the backbone, which the backbone distributes to the remaining areas.

You must configure at least one OSPF process before defining OSPF area/network settings for that process.

Related Topics

- Defining OSPF Process Settings , on page 28
- Defining OSPF Interface Settings , on page 32
- Redistributing Routes into OSPF , on page 30
- OSPF Routing on Cisco IOS Routers , on page 27

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **OSPF Process** from the Policy selector, then click the **Area** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **OSPF Process** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Area** tab.

The OSPF Process Area tab is displayed. See Table 15: OSPF Process Area Tab , on page 45 for a description of the fields on this tab.

Step 2 On the OSPF Process Area tab, select an OSPF area from the table, then click **Edit**, or click **Add** to create an area. The OSPF Area dialog box appears. See Table 16: OSPF Area Dialog Box , on page 46 for a description of the fields in this dialog box.

Step 3 Select a process ID from the displayed list.

Step 4 Enter an area ID to associate with the selected OSPF process.

Step 5 Enter the addresses of the networks to include in the OSPF area. You can enter a combination of addresses and network/host objects, or click **Select** to select a network/host object from a list or to create a new one. For more information, see Specifying IP Addresses During Policy Definition.

Step 6 Select the authentication type to use in the OSPF area: MD5, clear text, or none. We recommend MD5 when security is of concern. Please note the following:

- The authentication type must be the same for all routers and access servers in the same area.
- Specifying clear-text authentication for an area sets the authentication to Type 1 (simple password). All routers on a network must use the same clear-text password to communicate with each other using OSPF.
- MD5 passwords need not be the same throughout an area, but they must be the same between neighbors.
- If you use interface authentication (see Defining OSPF Interface Settings , on page 32), the authentication type used for the area must match the authentication type used for the interface.

Step 7 Click **OK** to save your definitions. The OSPF area appears in the table displayed on the OSPF Area tab.

Redistributing Routes into OSPF

Redistribution refers to using a routing protocol, such as OSPF, to advertise routes that are learned by some other means, such as a different routing protocol, static routes, or directly connected routes. For example, you can redistribute routes from the RIP routing protocol into your OSPF domain. Redistribution is necessary in networks that operate in multiple-protocol environments and can be applied to all IP-based routing protocols.

Redistributing routes into OSPF from other routing protocols or from static routes causes these routes to become OSPF external routes (Type 1 or Type 2).

Redistributing routes into OSPF involves:

- Defining OSPF Redistribution Mappings , on page 30
- Defining OSPF Maximum Prefix Values , on page 31

Related Topics

- Defining OSPF Process Settings , on page 28
- Defining OSPF Area Settings , on page 28
- Defining OSPF Interface Settings , on page 32
- OSPF Routing on Cisco IOS Routers , on page 27

Defining OSPF Redistribution Mappings

When you define OSPF redistribution mappings, you must select the protocol to redistribute and the OSPF process into which routes from that protocol are redistributed. Additionally, you can manually define the metric, which determines the priority of the redistributed routes, and the type of external OSPF route to create, Type 1 or Type 2.

You can create multiple mappings to the same OSPF process. For example, you can redistribute both RIP and EIGRP routes into the same OSPF process. You can also redistribute routes from other OSPF processes.

Note Redistribution into an OSPF Not-So-Stubby Area (NSSA) creates a special type of link-state advertisement (LSA) called type 7, which can exist only in an NSSA area. An NSSA autonomous system router (ASBR) generates this LSA, and an NSSA area border router (ABR) translates it into a type 5 LSA, which is propagated into the OSPF domain.

Type 1 versus Type 2 External Routes

Two types of OSPF external routes exist, Type 1 and Type 2. The difference between the two is related to how the cost (metric) of the route is calculated. The cost of a Type 1 route is the sum of the external cost and the internal cost used to reach that route. The cost of a Type 2 route is based on the external cost only. By default, external routes are defined as Type 2. However, a Type 1 route is always preferred over a Type 2 route to the same destination.

Before You Begin

- Define at least one OSPF process. See Defining OSPF Process Settings , on page 28.

Related Topics

- Defining OSPF Maximum Prefix Values , on page 31
- Redistributing Routes into OSPF , on page 30

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **OSPF Process** from the Policy selector, then click the **Redistribution** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **OSPF Process** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Redistribution** tab.

The OSPF Process Redistribution tab is displayed. See Table 17: OSPF Process Redistribution Tab , on page 47 for a description of the fields on this tab.

Step 2 On the OSPF Process Redistribution tab, select a row from the OSPF Redistribution Mappings table, then click **Edit**, or click **Add** to create a mapping. The OSPF Redistribution Mapping dialog box is displayed. See Table 18: OSPF Redistribution Mapping Dialog Box , on page 48 for a description of the fields in this dialog box.

Step 3 Select an existing OSPF process from the displayed list.

Step 4 Select the protocol whose routes you want to redistribute into the selected OSPF process.

Note You can create a single mapping for each static route, RIP route, BGP AS, EIGRP AS, and OSPF process.

Step 5 (Optional) Modify the default metric (cost) of the redistributed routes. The metric determines the priority of the routes.

Step 6 Select the Metric Type of external route to create, Type 1 or Type 2. The default is Type 2.

Step 7 (Optional) Select the **Limit to Subnets** check box to redistribute only subnetted routes. By default, this option is not selected.

Step 8 Click **OK** to save your definitions. The redistribution mapping appears in the Redistribution Mapping table on the OSPF Process Redistribution tab.

Defining OSPF Maximum Prefix Values

You can define a maximum number of prefixes (routes) that may be redistributed from other protocols or OSPF processes into a selected OSPF process. Setting a limit helps prevent the router from being flooded by too many redistributed routes. For example, without a defined maximum, flooding can occur when BGP is redistributed into OSPF.

When you define a maximum prefix value, you can decide whether to prevent additional routes from being redistributed once this maximum is reached, or whether to only issue a warning.

The redistribution limit applies to all IP redistributed prefixes, including summarized ones. The limit does not apply to default routes or prefixes that are generated as a result of type 7 to type 5 translations.

Before You Begin

- Define at least one OSPF process. Define at least one OSPF process. See Defining OSPF Process Settings , on page 28.
- Define at least one OSPF redistribution mapping. See Defining OSPF Redistribution Mappings , on page 30.

Related Topics

- Defining OSPF Redistribution Mappings , on page 30
- Redistributing Routes into OSPF , on page 30

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **OSPF Process** from the Policy selector, then click the **Redistribution** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **OSPF Process** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Redistribution** tab.

The OSPF Process Redistribution tab is displayed. See Table 17: OSPF Process Redistribution Tab , on page 47 for a description of the fields on this tab.

Step 2 On the OSPF Process Redistribution tab, select a row from the Max Prefix Mapping table, then click **Edit**, or click **Add** to create a definition. The Max Prefix Mapping dialog box appears. See Table 19: OSPF Max Prefix Mapping Dialog Box , on page 50 for a description of the fields in this dialog box.

Step 3 Select an existing OSPF process from the displayed list.

Step 4 In the Max Prefix field, enter the maximum number of routes that can be redistributed into the selected OSPF process.

Step 5 (Optional) Modify the default threshold percentage. When the number of redistributed routes reaches this threshold, a warning is issued. By default, the threshold value is 75% of the defined maximum prefix value.

Step 6 (Optional) Select what should happen when the maximum prefix value is reached:

- Enforce Maximum Route—Prevents additional routes from being redistributed to the selected process.
- Warning Only—Issues an additional warning, but allows route redistribution to continue even after the maximum prefix value is reached.

Note Flooding can result if you allow route redistribution to continue after exceeding the maximum prefix value.

Step 7 Click **OK** to save your definitions. The maximum prefix definition appears in the Maximum Prefix table on the OSPF Process Redistribution tab.

Defining OSPF Interface Settings

You can modify a variety of interface-specific OSPF parameters. This procedure describes how to define these parameters. For more information about a particular parameter, see the following topics:

- Understanding Interface Cost , on page 33
- Understanding Interface Priority , on page 34
- Disabling MTU Mismatch Detection , on page 35
- Understanding OSPF Timer Settings , on page 35
- Blocking LSA Flooding , on page 35
- Understanding the OSPF Network Type , on page 36
- Understanding OSPF Interface Authentication , on page 37

Related Topics

- Defining OSPF Process Settings , on page 28
- Defining OSPF Area Settings , on page 28
- Redistributing Routes into OSPF , on page 30
- OSPF Routing on Cisco IOS Routers , on page 27

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **OSPF Interface** from the Policy selector.
- (Policy view) Select **Router Platform** > **Routing** > **OSPF Interface** from the Policy Type selector. Select an existing policy or create a new one.

The OSPF Interface page is displayed. See Table 11: OSPF Interface Page , on page 38 for a description of the fields on this page.

Step 2 On the OSPF Interface page, select an interface definition from the table, then click **Edit**, or click **Add** to create a definition. The OSPF Interface dialog box appears. See Table 12: OSPF Interface Dialog Box , on page 39 for a description of the fields in this dialog box.

Step 3 Enter the name of the interface or interface role to define, or click **Select** to select an interface role from a list or to create a new one. For more information, see Specifying Interfaces During Policy Definition.

Step 4 Define interface authentication. The authentication type you select for the interface must match the authentication type you select for the area (see Defining OSPF Area Settings , on page 28).

All neighboring routers on the same network must have the same password to be able to exchange OSPF information. For more information, see Understanding OSPF Interface Authentication , on page 37.

The key ID number can be associated with multiple passwords. This is an easy and secure way to migrate passwords. For example, to migrate from one password to another, configure a password under a different key ID, then remove the first key.

Tip The key ID number can be associated with multiple passwords. This is an easy and secure way to migrate passwords. For example, to migrate from one password to another, configure a password under a different key ID, then remove the first key.

Note Do not use clear text authentication in OSPF packets for security purposes, because the unencrypted authentication key is sent in every packet. Use clear text authentication only when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.

Step 5 (Optional) Under **Properties**, configure interface parameters as required. See Table 12: OSPF Interface Dialog Box , on page 39 for information about each parameter.

Step 6 Click **OK** to save your definitions. The defined interfaces appear on the OSPF Interface page.

Step 7 Repeat the process to define interface-specific parameters on additional OSPF interfaces.

Understanding Interface Cost

The cost of an OSPF interface is a metric representing the cost of sending a packet over that interface. By default, this cost is calculated using this formula:

10^8 / bandwidth [bits per second]

For example, if the bandwidth of a Fast Ethernet interface is 10 Mbps (equal to 10^7), the cost of sending packets over that interface is calculated as $10^8/10^7$ or 10. This formula establishes an inverse relationship between the bandwidth of an interface and its cost; the greater the bandwidth, the lower the cost.

Although cost is a calculated value, you can manually enter the cost of a selected interface.

Related Topics

- Understanding Interface Priority , on page 34
- Disabling MTU Mismatch Detection , on page 35
- Blocking LSA Flooding , on page 35
- Understanding OSPF Timer Settings , on page 35
- Understanding the OSPF Network Type , on page 36
- Understanding OSPF Interface Authentication , on page 37
- Defining OSPF Interface Settings , on page 32

Understanding Interface Priority

Routers that share a common segment are elected through the Hello protocol to be neighbors on that segment. Election occurs as soon as the routers see themselves listed in their neighbor's hello packet. Adjacency is the next step. Adjacent routers are routers that proceed beyond the simple Hello exchange to a database exchange.

On each multiaccess (as opposed to point-to-point) segment, OSPF elects one router as the designated router (DR) for that segment. The DR acts as a central point of contact to minimize information exchange. Each router in the segment sends updates to the DR, which in turn relays the information to the other routers. A second router is elected as the backup designated router (BDR) in case the DR goes down.

DR and BDR election is performed via the Hello protocol. The router with the highest OSPF priority becomes the DR for that segment. The same process is then repeated for the BDR. In the case of a tie, the router with the higher router ID (RID) is elected. By default, each interface is given a priority of 1, but you can assign a higher priority to selected interfaces, as required.

Note The priority setting does not apply to point-to-point, nonbroadcast interfaces.

Related Topics

- Understanding Interface Cost , on page 33
- Disabling MTU Mismatch Detection , on page 35
- Blocking LSA Flooding , on page 35
- Understanding OSPF Timer Settings , on page 35
- Understanding the OSPF Network Type , on page 36
- Understanding OSPF Interface Authentication , on page 37

- Defining OSPF Interface Settings , on page 32

Disabling MTU Mismatch Detection

The MTU is the largest packet size that a particular interface can handle. If one router sends a DBD packet that is larger than the MTU setting on a neighboring router, the neighboring router ignores the packet. In many cases, an MTU mismatch causes the two routers to become stuck in exstart/exchange state, which prevents OSPF adjacency from being established. This is why it is important that all neighboring routers share the same MTU setting and that MTU mismatch detection be enabled.

You can, however, disable MTU mismatch detection. This is useful in cases where mismatch detection is preventing adjacency from taking place in an otherwise valid setup between two devices with different MTUs.

Related Topics

- Understanding Interface Cost , on page 33
- Understanding Interface Priority , on page 34
- Blocking LSA Flooding , on page 35
- Understanding OSPF Timer Settings , on page 35
- Understanding the OSPF Network Type , on page 36
- Understanding OSPF Interface Authentication , on page 37
- Defining OSPF Interface Settings , on page 32

Blocking LSA Flooding

By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives. Although some redundancy is desirable, too much redundancy can waste bandwidth. In certain topologies, such as full mesh, LSA flooding can destabilize the network because of excessive link and CPU usage. Therefore, you can block LSA flooding to selected interfaces on broadcast, nonbroadcast, and point-to-point networks.

Related Topics

- Understanding Interface Cost , on page 33
- Understanding Interface Priority , on page 34
- Disabling MTU Mismatch Detection , on page 35
- Understanding OSPF Timer Settings , on page 35
- Understanding the OSPF Network Type , on page 36
- Understanding OSPF Interface Authentication , on page 37
- Defining OSPF Interface Settings , on page 32

Understanding OSPF Timer Settings

OSPF uses a series of timers during operation:

- Hello Interval—Determines how often an interface sends hello packets, which are used to acquire neighbors and act as indicators that the router is still functioning. The smaller the interval, the faster topological changes on the network are detected. However, a smaller interval also results in more traffic being sent over the interface. The hello interval must be the same on all routers and access servers on a specific network.
- Transmit Delay—Determines the delay before an LSA is flooded over the link. The transmit delay setting should take into account the transmission and propagation delays for the interface. These factors are particularly important when configuring low-speed and on-demand links.
- Retransmit Interval—Determines how long to wait before retransmitting an unacknowledged database description (DBD) packet to its neighbors. The retransmit interval setting should be low enough to prevent excessive retransmissions.

Note You should increase the retransmit interval for serial lines and virtual links.

- Dead Interval—Determines how long an interface should wait before declaring its neighbor to be down. This declaration is caused by an absence of hello packets from the neighbor during this interval. The dead interval setting must be the same for all routers and access servers on a specific network. By default, this interval is four times the hello interval.

Related Topics

- Understanding Interface Cost , on page 33
- Understanding Interface Priority , on page 34
- Disabling MTU Mismatch Detection , on page 35
- Blocking LSA Flooding , on page 35
- Understanding the OSPF Network Type , on page 36
- Understanding OSPF Interface Authentication , on page 37
- Defining OSPF Interface Settings , on page 32

Understanding the OSPF Network Type

You can manually configure the OSPF network type on an interface as either broadcast or nonbroadcast multiaccess (NBMA), regardless of the default media type. For example, you can use this feature to configure broadcast networks (such as Ethernet, Token Ring, and FDDI) as NBMA when your network contains routers that do not support multicast addressing. You can also configure NBMA networks (such as X.25, Frame Relay, and SMDS) as broadcast networks, which eliminates the need to configure neighbors.

Configuring NBMA networks as either broadcast or nonbroadcast assumes the existence of virtual circuits (VCs) from every router to every router (fully meshed network). If VCs do not exist between each router, due to cost constraints or the existence of an only partially meshed network, you can configure the OSPF network type as point-to-multipoint. An OSPF point-to-multipoint interface is defined as a numbered point-to-point interface having one or more neighbors. It creates multiple host routes.

If you use the point-to-multipoint network type, routing between two routers that are not directly connected go through a third router that has VCs to both routers. You do not need to configure neighbors when using this feature. OSPF point-to-multipoint networks have the following benefits compared to NBMA and point-to-point networks:

- Point-to-multipoint is easier to configure because it consumes only one IP subnet and does not require neighbor configuration or designated router election.
- It costs less because it does not require a fully meshed topology.
- It is more reliable because it maintains connectivity in the event of VC failure.

Note For point-to-multipoint, broadcast networks, you can optionally define neighbors, in which case you should specify the cost to each neighbor. For point-to-multipoint, nonbroadcast networks, you must identify neighbors, but specifying a cost to each neighbor is optional. In both cases, you define neighbors using FlexConfig. See Understanding FlexConfig Policies and Policy Objects for more information.

Related Topics

- Understanding Interface Cost , on page 33
- Understanding Interface Priority , on page 34
- Disabling MTU Mismatch Detection , on page 35
- Blocking LSA Flooding , on page 35
- Understanding OSPF Timer Settings , on page 35
- Understanding OSPF Interface Authentication , on page 37
- Defining OSPF Interface Settings , on page 32

Understanding OSPF Interface Authentication

You define neighbor authentication settings for OSPF interfaces by selecting the interfaces and selecting an authentication type, either MD5 or clear text.

When you use MD5 authentication, neighboring routers must share the same password. When you use clear-text authentication, all routers on the network using OSPF must share the same password.

Whenever you configure an interface with a new key, the router sends multiple copies of the same packet, each authenticated by different keys. The router stops sending duplicate packets when it detects that all of its neighbors have adopted the new key.

Note You should use authentication with all routing protocols when possible, because attackers can use route redistribution between OSPF and other protocols (such as RIP) to subvert routing information.

Related Topics

- Understanding Interface Cost , on page 33

- Understanding Interface Priority , on page 34
- Disabling MTU Mismatch Detection , on page 35
- Blocking LSA Flooding , on page 35
- Understanding OSPF Timer Settings , on page 35
- Understanding the OSPF Network Type , on page 36
- Understanding OSPF Interface Authentication , on page 37

OSPF Interface Policy Page

Use the OSPF Interface page to view, create, edit, and delete interface-specific OSPF settings. For more information, see Defining OSPF Interface Settings , on page 32.

Navigation Path

- (Device view) Select **Platform** > **Routing** > **OSPF Interface** from the Policy selector.
- (Policy view) Select **Router Platform** > **Routing** > **OSPF Interface** from the Policy Type selector. Right-click **OSPF Interface** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- OSPF Process Policy Page , on page 42
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 11: OSPF Interface Page

Element	Description
Interfaces	The name of an interface (as defined by an interface role) on which OSPF is enabled.
Authentication	The type of OSPF neighbor authentication enabled for the selected interface.
Key ID	The identification number of the authentication key used for MD5 authentication.
Cost	The cost of sending packets over the selected interface, if this value is different from the cost as normally calculated.
Priority	The priority of the selected interface.
MTU Ignore	Indicates whether Maximum Transmission Rate (MTU) detection is disabled on the selected interface.
Database Filter	Indicates whether link-state advertisement (LSA) flooding is disabled on the selected interface.

Element	**Description**
Hello Interval	The interval between hello packets (in seconds) sent over this interface.
Transmit Delay	The amount of time OSPF waits (in seconds) before flooding an LSA over the link.
Retransmit Interval	The interval between LSA retransmissions (in seconds) over the selected interface.
Dead Interval	The interval OSPF waits (in seconds) before declaring a neighboring router dead because of an absence of hello packets.
Network Type	The network type configured for the selected interface, if it differs from the default medium.
Add button	Opens the OSPF Interface Dialog Box , on page 39. From here you can define the properties of an OSPF interface.
Edit button	Opens the OSPF Interface Dialog Box , on page 39. From here you can edit the properties of the selected OSPF interface.
Delete button	Deletes the selected OSPF interface definitions from the table.

OSPF Interface Dialog Box

Use the OSPF Interface dialog box to add or edit the properties of OSPF interfaces.

Navigation Path

Go to the OSPF Interface Policy Page , on page 38, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining OSPF Interface Settings , on page 32
- OSPF Routing on Cisco IOS Routers , on page 27
- Basic Interface Settings on Cisco IOS Routers
- Understanding Interface Role Objects

Field Reference

Table 12: OSPF Interface Dialog Box

Element	**Description**
Interface	The OSPF interface to configure. Enter the name of an interface or interface role, or click **Select** to select the object from a list or to create a new one.

Element	Description
Authentication	Type—The authentication type used by the selected interface: - MD5—Uses the MD5 hash algorithm for authentication. This is the default. - Clear Text—Uses a clear text password for authentication. - None—Uses no authentication. **Note** The authentication type used on an interface must match the authentication type defined for the area. **Note** Use plain text authentication only when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing. - Key ID—Available only when MD5 is selected as the authentication type. The identification number of the authentication key. This number must be shared with all other devices sending updates to, and receiving updates from, the selected device. Valid values range from 1 to 255. - Key—The shared key used for authentication (MD5 or clear text). This key must be shared with all other devices sending updates to, and receiving updates from, the selected device. Enter this key again in the Confirm field. When using clear text, the key can include any continuous string of characters that can be entered from the keyboard (up to 8 bytes). When using MD5, the key can include alphanumeric characters only (up to 16 bytes).
Cost	The cost of sending packets over this interface. A value entered here overrides the default calculated cost (10 8 /bandwidth in bits per second). Valid values range from 1 to 65535.
Priority	The default priority of the interface. The priority is used to determine which routers become the designated router (DR) and backup designated router (BDR) for that segment. The higher the number, the higher the priority. The default priority is 1. Valid values range from 0 to 255. **Note** To exclude the interface from election as DR or BDR, assign a priority of 0. Configure router priority only for interfaces to multiaccess networks, not point-to-point networks.
MTU Ignore	When selected, ignores MTU mismatches between neighboring routers. When deselected, MTU mismatch detection is enabled. **Note** Typically, this option is not used, because it can cause routers to become stuck in exstart/exchange state, which prevents OSPF adjacency from being established.

Element	Description
Database Filter	When selected, blocks link-state advertisement (LSA) flooding to the selected interface. When deselected, LSA flooding is permitted. **Note** We recommend that you enable this option on fully-meshed networks. This option is not available for point-to-multipoint networks.
Hello Interval	The default interval (in seconds) between hello packets sent over the selected interface. These packets are used by neighboring routers to confirm the router sending the packets is still operating. Valid values range 1 to 65535 seconds. **Note** The hello interval must be the same for all routers and access servers in the network.
Transmit Delay	The amount of time OSPF waits (in seconds) before flooding an LSA over the link. The default is 1 second. Valid values range from 1 to 65535 seconds. **Note** When you configure slow links or on-demand links that queue traffic before sending it in bursts, we recommend that you take these link delays into account when defining this value.
Retransmit Interval	The interval between LSA retransmissions (in seconds) over the selected interface. The default is 5 seconds. Valid values range from 1 to 65535 seconds. **Note** We recommend that you increase this value for serial lines and virtual links.
Dead Interval	The interval (in seconds) after which an interface declares its neighbor dead if no hello packets are received. Valid values range from 1 to 655335 seconds. **Note** The value of the dead interval is typically the hello interval value multiplied by 4. The dead interval must be the same for all routers and access servers in the network.

Element	Description
Configure Network Type	When selected, enables you to select a network type that differs from the default medium used by the interface. When deselected, the network type is equivalent to the default medium used by the interface. For nonbroadcast multiaccess (NBMA) networks (such as ATM and Frame Relay), options are: • Broadcast—Treats the NBMA network as a broadcast network, which eliminates the need to configure neighbors. Use this option when there are virtual circuits from every router to every router (fully meshed network). • Point-to-Multipoint—Treats the nonbroadcast network as a series of point-to-point links. This option is easier to configure, less costly, and more reliable than NBMA or point-to-point networks. • Point-to-Multipoint Non-Broadcast—Statically maintains the known neighbors of the network. Selecting this option helps avoid the problem of losing neighbors that were learned dynamically through the reception of hello packets. **Note** Another option for NBMA networks is to configure neighbors manually using FlexConfigs. See Understanding FlexConfig Policies and Policy Objects. For broadcast networks (such as Ethernet, Token Ring, and FDDI), you can select: • Non-Broadcast—Treats the broadcast network as a nonbroadcast network. • Point-to-Point—Treats the broadcast network as a point-to-point network. You can use this option, for example, to configure a broadcast network (such as Ethernet) as a nonbroadcast multiaccess (NBMA) network if not all routers in the network support multicast addressing.

OSPF Process Policy Page

OSPF is an interior gateway routing protocol that uses link states instead of distance vectors for path selection. OSPF propagates link-state advertisements (LSAs) instead of routing table updates, which enables OSPF networks to converge quickly.

You can configure OSPF process policies from the following tabs on the OSPF Process page:

- OSPF Process Page—Setup Tab , on page 43
- OSPF Process Page—Area Tab , on page 44
- OSPF Process Page—Redistribution Tab , on page 46

For more information, see OSPF Routing on Cisco IOS Routers , on page 27.

Note For more information about OSPF interface policies, see OSPF Interface Policy Page , on page 38.

Navigation Path

- (Device view) Select **Platform** > **Routing** > **OSPF Process** from the Policy selector.
- (Policy view) Select **Router Platform** > **Routing** > **OSPF Process** from the Policy Type selector. Right-click **OSPF Process** to create a policy, or select an existing policy from the Shared Policy selector.

OSPF Process Page—Setup Tab

Use the OSPF Process Setup tab to create, edit, and delete OSPF processes. This includes selecting those interfaces that will remain passive, which means that they will not send routing updates to their neighbors. You can create as many processes for each router as required.

Navigation Path

Go to the OSPF Process Policy Page , on page 42, then click the **Setup** tab.

Related Topics

- Defining OSPF Process Settings , on page 28
- OSPF Process Page—Area Tab , on page 44
- OSPF Process Page—Redistribution Tab , on page 46
- OSPF Interface Policy Page , on page 38
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 13: OSPF Process Setup Tab

Element	Description
Process ID	The process ID that identifies the OSPF routing process to other routers.
Passive Interfaces	The interfaces that do not send out routing updates.
Add button	Opens the OSPF Setup Dialog Box , on page 43. From here you can define an OSPF process.
Edit button	Opens the OSPF Setup Dialog Box , on page 43. From here you can edit the selected OSPF process.
Delete button	Deletes the selected OSPF processes from the table.

OSPF Setup Dialog Box

Use the OSPF Setup dialog box to add or edit an OSPF process.

Navigation Path

Go to the OSPF Process Page—Setup Tab , on page 43, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining OSPF Process Settings , on page 28

Field Reference

Table 14: OSPF Setup Dialog Box

Element	Description
Process ID	The process ID number for the OSPF process. This number identifies the OSPF process to other routers. It does not need to match the process ID on other devices. Valid values are from 1 to 65535.
Passive Interfaces	The interfaces that do not send updates to their routing neighbors. Click **Edit** to display the Edit Interfaces Dialog Box—OSPF Passive Interfaces , on page 44. From here you can define these interfaces. **Note** When you make an interface passive, OSPF suppresses the sending of hello packets to neighboring routers. The interface will continue to receive routing updates, however.

Edit Interfaces Dialog Box—OSPF Passive Interfaces

When you configure an OSPF routing policy on a Cisco IOS router, use the Edit Interfaces dialog box to specify which interfaces will not send updates to their routing neighbors. Separate multiple names or roles with commas. Click **Select** to select interface names or roles from a list of existing objects, or to create new interface role objects.

Navigation Path

Go to the OSPF Setup Dialog Box , on page 43, then click the **Edit** button in the Passive Interfaces field.

Related Topics

- OSPF Process Page—Setup Tab , on page 43
- Defining OSPF Process Settings , on page 28

OSPF Process Page—Area Tab

Use the OSPF Area tab to create, edit, and delete the areas and networks contained in each OSPF process. This includes selecting the type of authentication used by each area.

Navigation Path

Go to the OSPF Process Policy Page , on page 42, then click the **Area** tab.

Related Topics

- Defining OSPF Area Settings , on page 28
- OSPF Process Page—Setup Tab , on page 43
- OSPF Process Page—Redistribution Tab , on page 46
- OSPF Interface Policy Page , on page 38
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 15: OSPF Process Area Tab

Element	Description
Area ID	The ID number of the area associated with the process.
Process ID	The process ID that identifies the OSPF routing process to other routers.
Networks	The networks included in the area.
Authentication	The authentication type used by the area—MD5, clear text, or none.
Add button	Open the OSPF Area Dialog Box , on page 45. From here you can define an OSPF area.
Edit button	Opens the OSPF Area Dialog Box , on page 45. From here you can edit the selected OSPF area.
Delete button	Deletes the selected OSPF areas from the table.

OSPF Area Dialog Box

Use the OSPF Area dialog box to add or edit the properties of an OSPF area. You should define at least one area for each OSPF process (see OSPF Setup Dialog Box , on page 43), but deployment will not fail if you do not.

Navigation Path

Go to the OSPF Process Page—Area Tab , on page 44, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining OSPF Area Settings , on page 28
- Specifying IP Addresses During Policy Definition
- Understanding Networks/Hosts Objects

Field Reference

Table 16: OSPF Area Dialog Box

Element	Description
Process ID	The process ID associated with the OSPF area. The list contains the OSPF processes defined in the OSPF Process Page—Setup Tab , on page 43.
Area ID	The area ID number associated with the selected process. Valid values range from 0 to 4294967295.
Networks	The networks to add to the OSPF area. Enter one or more network addresses or network/host objects, or click **Select** to select the object from a list or to create a new one.
Authentication	The type of authentication used for the area: • MD5—(Recommended) Uses the MD5 hash algorithm for authentication. • Clear Text—Uses clear text for authentication. • None—No authentication is used. **Note** The authentication type must be the same for all routers and access servers in an area.

OSPF Process Page—Redistribution Tab

Use the OSPF Process Redistribution tab to create, edit, and delete OSPF redistribution mappings. This includes defining the maximum number of routes that can be redistributed into OSPF from other protocols or other OSPF processes.

Navigation Path

Go to the OSPF Process Policy Page , on page 42, then click the **Redistribution** tab.

Related Topics

- Redistributing Routes into OSPF , on page 30
- OSPF Process Page—Setup Tab , on page 43
- OSPF Process Page—Area Tab , on page 44
- OSPF Interface Policy Page , on page 38
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 17: OSPF Process Redistribution Tab

Element	Description
OSPF Redistribution Mapping Table	
OSPF Process ID	The ID of the OSPF routing domain into which other routes are being redistributed.
Protocol	The protocol that is being redistributed.
AS/Process ID	The AS number or process ID of the route that is being redistributed.
Match	When redistributing an OSPF process, indicates the types of OSPF routes that are being redistributed.
Metric	The value that determines the priority of the redistributed route.
Metric Type	The external link type associated with the default route advertised into the OSPF routing domain.
Subnets	Indicates whether routes that are subnetted are also being redistributed.
Add button	Opens the OSPF Redistribution Mapping Dialog Box , on page 48. From here you can define OSPF redistribution mappings.
Edit button	Opens the OSPF Redistribution Mapping Dialog Box , on page 48. From here you can edit the selected OSPF redistribution mapping.
Delete button	Deletes the selected redistribution mappings from the table.
OSPF Max Prefix Mapping Table	
OSPF Process ID	The ID of the OSPF routing domain for which a maximum prefix values has been defined.
Max Prefix	The maximum number of prefixes (routes) that may be redistributed to the selected OSPF process.
Threshold	The percentage of the maximum prefix value that acts as a threshold for triggering a warning message.
Action	Indicates whether redistribution to this OSPF process will stop when the maximum is reached, or whether only a warning is displayed.
Add button	Opens the OSPF Max Prefix Mapping Dialog Box , on page 49. From here you can define maximum prefix values for OSPF processes.
Edit button	Opens the OSPF Max Prefix Mapping Dialog Box , on page 49. From here you can edit the maximum prefix value defined for the selected OSPF process.
Delete button	Deletes the selected max prefix mappings from the table.

OSPF Redistribution Mapping Dialog Box

Use the OSPF Redistribution Mapping dialog box to add or edit the properties of an OSPF redistribution mapping.

Navigation Path

Go to the OSPF Process Page—Redistribution Tab , on page 46, then click the **Add** or **Edit** button beneath the Redistribution Mapping table.

Note You must create at least one OSPF process before you can access the OSPF Redistribution dialog box. See OSPF Process Page—Setup Tab , on page 43.

Related Topics

- OSPF Max Prefix Mapping Dialog Box , on page 49
- Redistributing Routes into OSPF , on page 30

Field Reference

Table 18: OSPF Redistribution Mapping Dialog Box

Element	Description
Process ID	The OSPF process into which other routes are being redistributed. You must select a process ID number from the list of OSPF processes defined in the OSPF Process Page—Setup Tab , on page 43.
Protocol to Redistribute	The routing protocol that is being redistributed: • Static—Redistributes static routes. You can define a single mapping for each route. • EIGRP—Redistributes an EIGRP autonomous system. Enter the AS number in the displayed field. You can define a single mapping for each AS. • BGP—Redistributes a BGP autonomous system. You can define a single BGP mapping on each device. If you configured a BGP AS in the BGP Setup tab, the AS number is displayed. Otherwise, a message is displayed indicating that no BGP AS was defined. See BGP Page—Redistribution Tab , on page 7.

Element	Description
Protocol to Redistribute (continued)	• OSPF—Redistributes a different OSPF process. You can define a single mapping for each process. Select a process from the displayed list, then select one or more match criteria: • Internal—Routes that are internal to a specific AS. • External1—Routes that are external to the AS and imported into OSPF as a Type 1 external route. • External2—Routes that are external to the AS and imported into the selected process as a Type 2 external route. • NSAAExternal1—Not-So-Stubby Area (NSSA) routes that are external to the AS and imported into the selected process as Type 1 external routes. • NSAAExternal2—(NSSA) routes that are external to the AS and imported into the selected process as Type 2 external routes. • RIP—Redistributes RIP routes. You can define a single mapping for each route. • Connected—Redistributes routes that are established automatically by virtue of having enabled IP on an interface. These routes are redistributed as external to the AS.
Default Metric	A value representing the cost of the redistributed route.
Metric Type	The external link type that is associated with the route being redistributed into the OSPF routing domain: • 1—Type 1 external route. The metric is the sum of the external redistributed cost and the internal OSPF cost. • 2—Type 2 external route. The metric is equal to the external redistributed cost, as defined in the Metric field. This is the default.
Limit to Subnets	When selected, only subnetted routes are redistributed. When deselected, subnetted routes are not redistributed.

OSPF Max Prefix Mapping Dialog Box

Use the OSPF Max Prefix Mapping dialog box to add or edit the maximum number of routes that can be redistributed into an OSPF process.

Navigation Path

Go to the OSPF Process Page—Redistribution Tab , on page 46, then click the **Add** or **Edit** button beneath the Prefix Mapping table.

Related Topics

- OSPF Redistribution Mapping Dialog Box , on page 48

- Redistributing Routes into OSPF , on page 30

Field Reference

Table 19: OSPF Max Prefix Mapping Dialog Box

Element	Description
Process ID	The OSPF process into which other routes are being redistributed. The list contains the OSPF processes defined in the OSPF Process Page—Setup Tab , on page 43.
Max Prefix	The maximum number of prefixes (routes) that can be redistributed into the selected OSPF process. Limiting the number of redistributed routes helps prevent the router from being flooded by an excessive number of routes.
Threshold	The percentage of the maximum prefix value that acts as a threshold for triggering warning messages. The default is 75%. **Note** This warning is triggered whether or not the Warning-Only check box is selected.
When maximum routes reached	The action to take when the maximum number of redistributed routes is reached: • Enforce Maximum Route—Prevents additional routes from being redistributed when the defined maximum prefix value is reached. This is the default. • Warning Only—Issues a warning when the maximum number of routes is reached, but does not prevent additional routes from being redistributed.

RIP Routing on Cisco IOS Routers

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) that was created for use in small, homogeneous networks. RIP is a distance-vector protocol that sends routing-update messages at regular intervals (in a process called *advertising*) and whenever the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the non-updating router as being unusable. If there is still no update after 240 seconds, the router removes all routing table entries for the non-updating router. Routing information is exchanged using UDP packets.

RIP evaluates routes by measuring the number of hops (the number of routers traversed) from the source to the destination. A directly connected network has a metric of zero. The maximum hop count allowed by RIP is 15. Any route with a hop count greater than 15 is considered unreachable.

Security Manager supports RIP version 2 only, which is described in RFC 1723. RIP 2 improves on the original RIP by enabling RIP messages to carry more information, which permits the use of a simple authentication mechanism (clear text or MD5) to secure table updates. RIP 2 also supports subnet masks, a critical feature that was not available in the original version of RIP.

The following topics describe the tasks you perform to create a RIP routing policy:

- Defining RIP Setup Parameters , on page 51
- Defining RIP Interface Authentication Settings , on page 52
- Redistributing Routes into OSPF , on page 30

Related Topics

- Static Routing on Cisco IOS Routers , on page 59
- OSPF Routing on Cisco IOS Routers , on page 27
- EIGRP Routing on Cisco IOS Routers , on page 9
- BGP Routing on Cisco IOS Routers , on page 1

Defining RIP Setup Parameters

You configure RIP setup parameters by selecting the networks to include in the route and deciding whether any interfaces should be passive. These interfaces do not send routing updates to their neighbors. Additionally, you can enable auto-summarization, which reduces the size and complexity of the routing tables the router must maintain.

Related Topics

- Defining RIP Interface Authentication Settings , on page 52
- Redistributing Routes into OSPF , on page 30
- RIP Routing on Cisco IOS Routers , on page 50

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **RIP** from the Policy selector, then click the **Setup** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **RIP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Setup** tab.

The RIP Setup tab is displayed (see RIP Page—Setup Tab , on page 54).

Step 2 Enter the addresses of the directly connected networks whose interfaces are to receive RIP updates. You can use a combination of addresses and network/host objects; separate addresses with commas. Click **Select** to select network/host objects from a list of existing objects, or to create new network/host objects. For more information, see Specifying IP Addresses During Policy Definition.

Step 3 Enter the addresses of the passive interfaces, which are interfaces that should not send routing updates to their neighbors, if any. These interfaces continue to receive RIP routing broadcasts, which they use to populate their routing tables. Enter the names of one or more interfaces or interface roles; separate addresses with commas. Click **Select** to select interface names or roles from a list of existing objects, or to create new interface role objects. For more information, see Specifying Interfaces During Policy Definition.

Step 4 (Optional) Select the **Auto Summary** check box to enable the automatic summarization of subnet routes into network-level routes. Summarization reduces the size of routing tables, thereby reducing the complexity of the network.

Disable automatic summarization when you perform routing between disconnected subnets. When automatic summarization is turned off, subnets are advertised.

Defining RIP Interface Authentication Settings

You define neighbor authentication settings for RIP interfaces by selecting the interfaces and then selecting an authentication type, either MD5 or clear text.

Related Topics

- Defining RIP Setup Parameters , on page 51
- Redistributing Routes into OSPF , on page 30
- RIP Routing on Cisco IOS Routers , on page 50

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **RIP** from the Policy selector, then click the **Authentication** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **RIP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Authentication** tab.

The RIP Authentication tab is displayed. See Table 21: RIP Authentication Tab , on page 55 for a description of the fields on this tab.

Step 2 On the RIP Authentication tab, select an interface definition from the table, then click **Edit**, or click **Add** to create a definition. The RIP Authentication dialog box appears. See Table 22: RIP Authentication Dialog Box , on page 56 for a description of the fields in this dialog box.

Step 3 Enter the name of the interface or interface role for which authentication is defined, or click **Select** to select an interface role from a list or to create a new one. For more information, see Specifying Interfaces During Policy Definition.

Step 4 Define interface authentication (MD5 or clear text).

Note We do not recommend that you use clear text authentication in RIP packets, because the unencrypted authentication key is sent in every packet. Use plain text authentication only when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.

Step 5 Click **OK** to save your definitions locally on the client and close the dialog box. The defined interface appears on the RIP Authentication tab.

Redistributing Routes into RIP

Redistribution refers to using a routing protocol, such as RIP, to advertise routes that are learned by some other means, such as a different routing protocol, static routes, or directly connected routes. For example, you can redistribute routes from the OSPF routing protocol into your RIP route. Redistribution is necessary in networks that operate in multiple-protocol environments and can be applied to all IP-based routing protocols.

When you redistribute into RIP, you can maintain the original metric of the route by redistributing it transparently.

Before You Begin

- Define at least one RIP route. See Defining RIP Setup Parameters , on page 51.

Related Topics

- Defining RIP Setup Parameters , on page 51
- Defining RIP Interface Authentication Settings , on page 52
- RIP Routing on Cisco IOS Routers , on page 50

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **RIP** from the Policy selector, then click the **Redistribution** tab in the work area.
- (Policy view) Select **Router Platform** > **Routing** > **RIP** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Redistribution** tab.

The RIP Redistribution tab is displayed. See Table 23: RIP Redistribution Tab , on page 57 for a description of the fields on this tab.

Step 2 On the RIP Redistribution tab, select a row from the RIP Redistribution Mappings table, then click **Edit**, or click **Add** to create a mapping. The RIP Redistribution Mapping dialog box appears. See Table 24: RIP Redistribution Mapping Dialog Box , on page 58 for a description of the fields in this dialog box.

Step 3 Select the protocol whose routes you want to redistribute into RIP.

Note You can create a single mapping for each static route, BGP AS, EIGRP AS, and OSPF process.

Step 4 Define the metric (cost) of the redistributed routes by doing one of the following:

- Select the **Default Metric** check box, then enter the default metric of the redistributed routes. The metric determines the priority of the routes.
- Select the **Transparent** check box to maintain the original metric of the routes being redistributed into RIP.

Step 5 Click **OK** to save your definitions locally on the client and close the dialog box. The redistribution mapping appears in the Redistribution Mapping table on the RIP Redistribution tab.

RIP Routing Policy Page

RIP is a distance-vector routing protocol that uses hop count as the metric for path selection. Security Manager supports RIP version 2 only, which includes support for neighbor authentication when routing updates are exchanged.

You can configure RIP routing policies from the following tabs on the RIP Routing page:

- RIP Page—Setup Tab , on page 54
- RIP Page—Authentication Tab , on page 55
- RIP Page—Redistribution Tab , on page 56

For more information, see RIP Routing on Cisco IOS Routers , on page 50.

Navigation Path

- (Device view) Select **Platform** > **Routing** > **RIP** from the Policy selector.
- (Policy view) Select **Router Platform** > **Routing** > **RIP** from the Policy Type selector. Right-click **RIP** to create a policy, or select an existing policy from the Shared Policy selector.

RIP Page—Setup Tab

Use the RIP Setup tab to create, edit, and delete RIP routes.

Navigation Path

Go to the RIP Routing Policy Page , on page 53, then click the **Setup** tab.

Related Topics

- Defining RIP Setup Parameters , on page 51
- RIP Page—Authentication Tab , on page 55
- RIP Page—Redistribution Tab , on page 56
- Specifying IP Addresses During Policy Definition
- Understanding Networks/Hosts Objects

Field Reference

Table 20: RIP Setup Tab

Element	Description
Networks	The directly connected networks associated with the RIP route. Enter one or more network addresses or network/host objects, separated by commas. Click **Select** to select network/host objects from a list of existing objects, or to create new objects.
Passive Interfaces	The interfaces that do not send updates to their routing neighbors. Enter one or more interface names or roles, separated by commas. Click **Select** to select interface names or roles from a list of existing objects, or to create new interface role objects.

Element	Description
Auto-Summary	When selected, enables the automatic summarization of subnet routes into network-level routes. Summarization reduces the size of routing tables, thereby reducing the complexity of the network. When deselected, automatic summarization is disabled. **Note** Disable automatic summarization when performing routing between disconnected subnets. When this feature is disabled, subnets are advertised.

RIP Page—Authentication Tab

Use the RIP Authentication tab to view, create, edit, and delete the neighbor authentication settings of RIP interfaces.

Navigation Path

Go to the RIP Routing Policy Page , on page 53, then click the **Authentication** tab.

Related Topics

- Defining RIP Interface Authentication Settings , on page 52
- RIP Page—Setup Tab , on page 54
- RIP Page—Redistribution Tab , on page 56
- RIP Routing Policy Page , on page 53
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 21: RIP Authentication Tab

Element	Description
Interfaces	The name of an interface (as defined by an interface role) on which RIP is enabled.
Authentication	The type of RIP neighbor authentication that is enabled for the selected interface role—clear text or MD5.
Key ID	The identification number of the authentication key used for MD5 authentication.
Add button	Opens the RIP Authentication Dialog Box , on page 56. From here you can define authentication for an additional RIP interface.
Edit button	Opens the RIP Authentication Dialog Box , on page 56. From here you can edit the authentication properties of the selected RIP interface.
Delete button	Deletes the selected authentication definitions from the table.

RIP Authentication Dialog Box

Use the RIP Authentication dialog box to add or edit the neighbor authentication properties of RIP interfaces.

Navigation Path

Go to the RIP Page—Authentication Tab , on page 55, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining RIP Interface Authentication Settings , on page 52

Field Reference

Table 22: RIP Authentication Dialog Box

Element	Description
Interface	The interface for which you want to define authentication properties. Enter the name of an interface or interface role, or click **Select** to select the object from a list or to create a new one. **Note** You cannot specify two different authentication configurations for the same interface.
Authentication	The type of authentication to apply to the interface: • MD5—(Recommended) Uses the MD5 hash algorithm for authentication. • Clear Text—Uses clear text for authentication. **Note** Use plain text authentication only when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.
Key ID	Available only when MD5 is selected as the authentication type. The identification number of the authentication key. This number must be shared with all other devices sending updates to, and receiving updates from, the selected device. Valid values range from 0 to 2147483647.
Key	The shared key used for authentication (MD5 or clear text). This key must be shared with all other devices sending updates to, and receiving updates from, the selected device. The key can contain up to 80 alphanumeric characters; the first character cannot be a number. Spaces are allowed. Enter the key again in the Confirm field.

RIP Page—Redistribution Tab

Use the RIP Redistribution tab to view, create, edit, and delete redistribution settings when performing redistribution into an RIP routing domain.

Note You must define RIP setup parameters before you can access the RIP Redistribution tab. See RIP Page—Setup Tab , on page 54.

Navigation Path

Go to the RIP Routing Policy Page , on page 53, then click the **Redistribution** tab.

Related Topics

- Redistributing Routes into RIP , on page 52
- RIP Page—Authentication Tab , on page 55
- Filtering Tables

Field Reference

Table 23: RIP Redistribution Tab

Element	Description
Protocol	The protocol that is being redistributed.
AS/Process ID	The autonomous system (AS) number or process ID of the route being redistributed.
Metric	The value that determines the priority of the redistributed route.
Match	When redistributing an OSPF process, indicates which types of OSPF routes are being redistributed.
Add button	Opens the RIP Redistribution Mapping Dialog Box , on page 57. From here you can define a RIP redistribution mapping.
Edit button	Opens the RIP Redistribution Mapping Dialog Box , on page 57. From here you can edit the selected RIP redistribution mapping.
Delete button	Deletes the selected redistribution mappings from the table.

RIP Redistribution Mapping Dialog Box

Use the RIP Redistribution Mapping dialog box to add or edit the properties of an RIP redistribution mapping.

Navigation Path

Go to the RIP Page—Redistribution Tab , on page 56, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Redistributing Routes into RIP , on page 52

Field Reference

Table 24: RIP Redistribution Mapping Dialog Box

Element	Description
Protocol to Redistribute	The routing protocol that is being redistributed: • Static—Redistributes static routes. You can define a single mapping for each route. • EIGRP—Redistributes an EIGRP autonomous system. Enter the AS number in the displayed field. You can define a single mapping for each AS. • BGP—Redistributes a BGP autonomous system. You can define a single BGP mapping on each device. If you configured a BGP AS in the BGP Setup tab, the AS number is displayed. Otherwise, a message is displayed indicating that no BGP AS was defined. See BGP Page—Redistribution Tab , on page 7.
Protocol to Redistribute (continued)	• OSPF—Redistributes a different OSPF process. You can define a single mapping for each process. Select a process from the displayed list, then select one or more match criteria: ◦ Internal—Routes that are internal to a specific AS. ◦ External1—Routes that are external to the AS and imported into OSPF as a Type 1 external route. ◦ External2—Routes that are external to the AS and imported into the selected process as a Type 2 external route. ◦ NSAAExternal1—Not-So-Stubby Area (NSSA) routes that are external to the AS and imported into the selected process as Type 1 external routes. ◦ NSAAExternal2—(NSSA) routes that are external to the AS and imported into the selected process as Type 2 external routes. • Connected—Redistributes routes that are established automatically by virtue of having enabled IP on an interface. These routes are redistributed as external to the AS.
Default Metric	Establishes a default value for the redistributed route. Valid values range from 0 to 16.
Transparent Metric	When selected, maintains the original metric of the route being redistributed. When deselected, the value specified in the Metric field is used.

Static Routing on Cisco IOS Routers

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

You can configure static routing policies to ensure that the router correctly forwards packets to their destination when a route cannot be built dynamically. By default, static routes have a default administrative distance of 1 (implying a directly connected network), which causes them to override any dynamic routes discovered for the same host or network. You can, however, define a larger administrative distance to a static route so that it does not take precedence over a corresponding dynamic route.

For example, EIGRP routes have a default administrative distance of 5. To have a static route that can be overridden by an EIGRP route, you must specify an administrative distance greater than 5. This feature is useful when you define the static route as a "floating" route, which is inserted into the routing table only when the preferred route is unavailable.

Tip When you use the static route as a backup, "floating" route, specify the interface through which the next hop IP address can be reached instead of entering a specific IP address. Otherwise, the "floating" route is not inserted in the routing table if the primary link fails. For more information, see *Specifying a Next Hop IP Address for Static Routes* on Cisco.com at this URL: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800ef7b2.shtml

Related Topics

- Defining Static Routes , on page 59

Defining Static Routes

To define a static route, you must define the IP address (and optionally, the metric) of the hop gateway to which the router forwards packets destined to the selected host or network. You can define as many static routes as required.

Related Topics

- Static Routing on Cisco IOS Routers , on page 59
- RIP Routing on Cisco IOS Routers , on page 50
- OSPF Routing on Cisco IOS Routers , on page 27
- EIGRP Routing on Cisco IOS Routers , on page 9
- BGP Routing on Cisco IOS Routers , on page 1

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Routing** > **Static Routing** from the Policy selector.
- (Policy view) Select **Router Platform** > **Routing** > **Static Routing** from the Policy Type selector. Select an existing policy or create a new one.

The Static Routing page is displayed. See Table 25: Static Routing Page , on page 61 for a description of the fields on this page.

Step 2 On the Static Routing page, select a static route from the table, then click **Edit**, or click **Add** to create a route. The Static Routing dialog box appears. See Table 26: Static Routing Dialog Box , on page 62 for a description of the fields in this dialog box.

Step 3 (Optional) Select the **Use as Default Route** check box to make this route the default route for all unknown outbound packets.

Step 4 In the Prefix field, enter the address for the destination network, or click **Select** to select a network/host object from a list or to create a new one. For more information, see Specifying IP Addresses During Policy Definition.

Step 5 Select a forwarding option:

- To define the router interface that forwards packets to the remote network, select **Forwarding Interface** and enter the name of an interface or interface role. You can click Select to select an interface role from a list or to create a new one. See Understanding Interface Role Objects and Selecting Objects for Policies.
- To specify the next hop router that receives and forwards packets to the remote network, select **Forwarding IP**, then enter the address in the field provided, or click **Select** to select a network/host object from a list or to create a new one. For more information, see Specifying IP Addresses During Policy Definition.

Step 6 (Optional) In the Distance Metric field, enter the number of hops to the next hop address for this router. This metric identifies the priority of the static route. If two routing entries specify the same network, the route with the lower metric value (that is, the lower cost) is given a higher priority and is selected.

If no value is specified, the default is 1, which implies a directly connected network.

Step 7 (Optional) Select the **Permanent route** check box to prevent this static route entry from being deleted, even in cases in which the interface is shut down or the router cannot communicate with the next router.

Step 8 Click **OK** to save your definitions locally on the client and close the dialog box. The static route appears in the table on the Static Routing page.

Static Routing Policy Page

Use the Static Routing page to create, edit, and delete static routes. For more information, see Defining Static Routes , on page 59.

Navigation Path

- (Device view) Select **Platform** > **Routing** > **Static Routing** from the Policy selector.
- (Policy view) Select **Router Platform** > **Routing** > **Static Routing** from the Policy Type selector. Right-click **Static Routing** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Static Routing on Cisco IOS Routers , on page 59
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 25: Static Routing Page

Element	Description
Prefix	The destination IP address of the static route.
Prefix Mask	The net mask of the selected IP address.
Default Route	Indicates whether the static route is the default route for unknown packets being forwarded by this router.
Interface or IP Address	The IP address or the interface name associated with the gateway router that is the next hop address for this router.
Distance	The number of hops from the gateway IP to the destination. The metric determines the priority of this route. The fewer the hops, the higher the priority assigned to the route, based on lower costs. When two routing entries specify the same network, the entry with the lower metric (that is, the higher priority) is selected.
Permanent Route	Indicates whether the static route is defined as a permanent route, which means that it will not be removed even if the interface is shut down or if the router is unable to communicate with the next router.
Add button	Opens the Static Routing Dialog Box , on page 61. From here you can create a static route.
Edit button	Opens the Static Routing Dialog Box , on page 61. From here you can edit the selected static route.
Delete button	Deletes the selected static routes from the table.

Static Routing Dialog Box

Use the Static Routing dialog box to add or edit static routes.

Navigation Path

Go to the Static Routing Policy Page , on page 60, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining Static Routes , on page 59

- Static Routing on Cisco IOS Routers , on page 59

Field Reference

Table 26: Static Routing Dialog Box

Element	Description
Destination Network	Address information for the destination network defined by this static route. • Use as Default Route—When selected, makes this the default route on this router. A default route is used when the route from a source to a destination is unknown or when it is not feasible for the router to maintain many routes in its routing table. All unknown outbound packets are forwarded over the default route. When deselected, this static route is not the default route. • Prefix—The IP address of the destination network. Enter an IP address or the name of a network/host object, or click **Select** to select the object from a list or to create a new one. The prefix must be a class A, B, or C network or host IP. A host IP can begin with 0 unless it contains a discontiguous mask. All subnet addresses are valid.
Forwarding (Next Hop)	The method of forwarding data to the destination network: • Forwarding Interface—The router interface that forwards packets to the remote network. Enter the name of an interface or interface role, or click **Select** to select the object from a list or to create a new one. • Forwarding IP—The IP address of the next hop router that receives and forwards packets to the remote network. Enter an IP address or the name of a network/host object, or click **Select** to select the object from a list or to create a new one.
Distance Metric	The number of hops to the destination network (gateway IP). The default is 1 if no value is specified. The range is from 1 to 255. This metric (also known as *administrative distance*) is a measurement of route expense based on the number of hops to the network on which a specified host resides. This hop count includes all the networks a packet must traverse, including the destination network. Therefore, all directly connected networks have a metric of 1. Because the metric is based on expense, it is used to identify the priority of the static route. If two routing entries specify the same network, the route with the lower metric value (that is, the lower cost) is given a higher priority and is selected. **Note** Under certain circumstances, it is useful to assign a static route a lower priority (larger distance metric) than a dynamic route. This enables the static route to act as a backup, “floating,” route when the dynamic route is unavailable.
Permanent route	When selected, prevents this static route entry from being deleted, even in cases where the interface is shut down or the router cannot communicate with the next router. When deselected, this static route can be deleted.