IS-IS Inbound Filtering

The Intermediate System-to-Intermediate System (IS-IS) Inbound Filtering feature prevents unwanted IS-IS routes from being installed in a routing table. A user can deny or permit a route from being installed in a routing table using the feature in combination with access lists, prefix lists, route maps, or gateways.

- Finding Feature Information, page 1
- Prerequisites for IS-IS Inbound Filtering, page 1
- Information About IS-IS Inbound Filtering, page 2
- How to Configure IS-IS Inbound Filtering, page 3
- Configuration Examples for IS-IS Inbound Filtering, page 9
- Verifying IS-IS Inbound Filtering, page 10
- Additional References, page 12
- Feature Information for IS-IS Inbound Filtering, page 12

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IS-IS Inbound Filtering

IS-IS must be configured on the network.
Information About IS-IS Inbound Filtering

You can deny or permit Intermediate System-to-Intermediate System (IS-IS) routes from being installed in the routing table.

Devices configured with IS-IS run Shortest Path First (SPF) on the routes received through link-state packet (LSP) updates and install updated routes in a routing table. You can configure access lists, prefix lists, gateways, or route maps with permit or deny rules and apply these to the routing table using the `distribute-list` command.

The distribution list can be applied globally or to routes using a specific interface as the outgoing interface.

Filtering Based on a Route Tag

Users can assign tags to external routes when they are redistributed to IS-IS routes. Then, the user can deny or permit those routes in the IS-IS domain by identifying that tag in the `route-map` and `distribute-list in commands`.

In the route map, you can create rules for specific route attributes that are defined using the match command. The match options are as follows:

- `match interface`
- `match ip address`
- `match ip next-hop`
- `match ip route-source`
- `match metric`
- `match route-type`
- `match tag`

One application of filtering based on route tags is on Autonomous System Boundary Routers (ASBRs), where users can tag prefixes when they are distributed on the ASBRs, and later use the tags to filter the prefixes and prevent them from getting installed on the routing table of other external devices.

Filtering Based on an Interface

When a match is done on the interface, the interface represents the outgoing interface of the route that IS-IS is trying to install in the routing table.

Filtering Based on Next Hop/Source of Updates

When a match is done on the next hop, the next hop represents the next-hop IP address of the route that IS-IS is trying to install in the routing table. You can thus filter routes based on the source of the updates.
How to Configure IS-IS Inbound Filtering

Configuring Route Filtering by Route Destination Using an Access List

Perform this task to filter a route by route destination. An access list is defined to permit or deny a destination IP address and this access list is applied to the routing table.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `access-list access-list-number {permit | deny} ip any destination-address destination-wildcard`
4. `interface type number`
5. `ip router isis route-tag`
6. `router isis route-tag`
7. `distribute-list access-list-number in [interface-type interface-number]`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable`
| **Example:** | `Device> enable`
| **Purpose:** | Enables privileged EXEC mode. |
| **Step 2** | `configure terminal`
| **Example:** | `Device# configure terminal`
| **Purpose:** | Enters global configuration mode. |
| **Step 3** | `access-list access-list-number {permit | deny} ip any destination-address destination-wildcard`
| **Example:** | `Device(config)# access-list 101 deny ip any 198.51.100.15 0.0.0.63`
| **Purpose:** | Defines an access list permitting or denying an IP address or a subnet. |
| | * 1 in the source-wildcard indicates that the corresponding position in the source-address need not be considered. |
| **Step 4** | `interface type number`
| **Example:** | `Device(config)# interface fastethernet 0/0`
| **Purpose:** | Configures an interface type and enters interface configuration mode. |
| **Step 5** | `ip router isis route-tag`
| **Example:** | `Device(config-if)# ip router isis 121`
| **Purpose:** | Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process. |
### Configuring Route Filtering by Next Hop (or Route Source)

Perform this task to filter a route by the next-hop IP address of the route (source of routing updates). A prefix list is defined to permit or deny a next-hop IP address and applied to the routing table.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list prefix-list-name [seq number] {permit | deny} network/length [ge ge-length] [le le-length]**
4. **interface type number**
5. **ip router isis route-tag**
6. **router isis route-tag**
7. **distribute-list gateway prefix-list-name in [interface-type interface-number]**

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>2</strong></td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>**ip prefix-list prefix-list-name [seq number] {permit</td>
<td>deny} network/length [ge ge-length] [le le-length]**</td>
</tr>
</tbody>
</table>

---

### IS-IS Inbound Filtering

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>Enables an Intermediate System-to-Intermediate System (IS-IS) routing protocol and enters router configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**
Device(config-if)# router isis 121

**Step 7**

Filters the routing table based on the access list.

**Example:**
Device(config-router)# distribute-list 101 in
### Command or Action | Purpose
--- | ---
**Example:**  
Device(config)# ip prefix-list List2 seq 5 deny 198.51.100.21/24  | • The optional *ge* keyword represents the greater than or equal to operator.  
• The optional *le* keyword represents the lesser than or equal to operator.

**Step 4**  
**interface type number**  
**Example:**  
Device(config)# interface fastethernet 0/0  | Configures an interface type and enters interface configuration mode.

**Step 5**  
**ip router isis route-tag**  
**Example:**  
Device(config-if)# ip router isis 125  | Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.

**Step 6**  
**router isis route-tag**  
**Example:**  
Device(config-if)# router isis 125  | Enables an IS-IS routing protocol and enters router configuration mode.

**Step 7**  
**distribute-list gateway prefix-list-name in [interface-type interface-number]**  
**Example:**  
Device(config-router)# distribute-list gateway List2 in  | Filters the routing table based on the next hop (or route source).

### Configuring Route Filtering by Route Destination Using a Prefix List

Perform this task to filter a route by route destination. A prefix list is defined to permit or deny a destination IP address and applied to the routing table.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip prefix-list prefix-list-name [seq number] {permit | deny} network/length [ge ge-length] [le le-length]`
4. `interface type number`
5. `ip router isis route-tag`
6. `router isis route-tag`
7. `distribute-list prefix prefix-list-name in [interface-type interface-number]`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip prefix-list prefix-list-name [seq number] [permit</td>
<td>Defines a prefix list permitting or denying an IP address or a subnet.</td>
</tr>
<tr>
<td>deny] network/length [ge ge-length] [le le-length]</td>
<td>- The optional <code>ge</code> keyword represents the greater than or equal to operator.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ip prefix-list List1 seq 5 deny 198.51.100.23/24</td>
</tr>
<tr>
<td><strong>Step 4</strong> interface type number</td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# interface fastethernet 0/0</td>
</tr>
<tr>
<td><strong>Step 5</strong> ip router isis route-tag</td>
<td>Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# ip router isis 122</td>
</tr>
<tr>
<td><strong>Step 6</strong> router isis route-tag</td>
<td>Enables an IS-IS routing protocol and enters router configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# router isis 122</td>
</tr>
<tr>
<td><strong>Step 7</strong> distribute-list prefix prefix-list-name in [interface-type interface-number]</td>
<td>Filters the routing table based on the prefix list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-router)# distribute-list prefix List1 in</td>
</tr>
</tbody>
</table>

### Configuring Route Filtering Using Tags

Perform this task to filter a route using route tags. A route map is defined to permit or deny a route tag and applied to the routing table.
SUMMARY STEPS

1. enable
2. configure terminal
3. route-map route-map-name [permit | deny] sequence-number
4. match tag tag-value
5. exit
6. interface type number
7. ip router isis route-tag
8. router isis route-tag
9. distribute-list route-map route-map-name in

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> route-map route-map-name [permit</td>
<td>deny] sequence-number</td>
</tr>
<tr>
<td>Example: Device(config)# route-map Map1 deny 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> match tag tag-value</td>
<td>Associates a match tag rule with the route map and matches routes with a specified name to be used as the route map is referenced.</td>
</tr>
<tr>
<td>Example: Device(config-route-map)# match tag 200</td>
<td></td>
</tr>
<tr>
<td>- At least one match command is required, but it need not be this match command. This is just an example.</td>
<td></td>
</tr>
<tr>
<td>- The list of match commands available to be used in this type of route map appears on the distribute-list in command reference page.</td>
<td></td>
</tr>
<tr>
<td>- This type of route map will have no set commands.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-route-map)# exit</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Route Filtering by IPv6 Route Destination Using a Prefix List

Perform this task to filter a route by IPv6 route destination. A prefix list is defined to permit or deny a destination IPv6 address and applied to the routing table.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ipv6 prefix-list prefix-list-name [seq number] {permit | deny} network/length [ge ge-length] [le le-length]`
4. `router isis`
5. `address-family ipv6`
6. `distribute-list prefix-list prefix-list-name in [interface-type interface-number]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Example:

```
Device> enable
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 prefix-list prefix-list-name [seq number] {permit</td>
<td>deny} network/length [ge ge-length] [le le-length]</td>
</tr>
<tr>
<td>Example: Device(config)# ipv6 prefix-list 101 seq 5 deny 2001:0DB8::/32</td>
<td>• The optional ge keyword represents the greater than or equal to operator.</td>
</tr>
<tr>
<td></td>
<td>• The optional le keyword represents the lesser than or equal to operator.</td>
</tr>
<tr>
<td><strong>Step 4</strong> router isis</td>
<td>Enters router configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# router isis</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> address-family ipv6</td>
<td>Enables configuration of IS-IS routing sessions for IPv6 address prefixes and enters address family configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-router)# address-family ipv6</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> distribute-list prefix-list prefix-list-name in [interface-type interface-number]</td>
<td>Filters the routing table based on the prefix list.</td>
</tr>
<tr>
<td>Example: Device(config-router-af)# distribute-list prefix-list 101 in</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Examples for IS-IS Inbound Filtering

#### Example: Configuring Route Filtering by Route Destination Using an Access List

The following example shows how to filter three routes from the routing table using a specified access list:

```
Device(config)# access-list 101 deny ip any 192.168.4.0 0.0.0.127
Device(config)# access-list 101 deny ip any 192.168.4.128 0.0.0.63
Device(config)# access-list 101 deny ip any 192.168.4.192 0.0.0.63
Device(config)# interface fastethernet 0/0
Device(config-if)# ip router isis 121
Device(config-if)# router isis 121
Device(config-router)# distribute-list 101 in
```
Example: Configuring Route Filtering by Next Hop (or Route Source)

The following example shows how to enable IS-IS inbound filtering using next hop or a route source:

```
Device(config)# ip prefix-list List2 seq 5 deny 198.51.100.31/24
Device(config)# interface fastethernet 0/0
Device(config-if)# ip router isis 125
Device(config-if)# router isis 125
Device(config-router)# distribute-list gateway List2 in
```

Example: Configuring Route Filtering by Route Destination Using a Prefix List

The following example shows how to filter three routes from a routing table using a prefix list.

```
Device(config)# ip prefix-list List1 seq 3 deny 192.0.2.1/24
Device(config)# ip prefix-list List1 seq 5 deny 192.168.4.0/24 ge 25 le 26
Device(config)# ip prefix-list List1 seq 10 permit 0.0.0.0/le 32
Device(config-if)# ip router isis 122
Device(config-if)# router isis 122
Device(config-router)# distribute-list prefix List1 in
```

Example: Configuring Route Filtering Using Tags

The following example shows how to enable IS-IS inbound filtering using a route map:

```
Device(config)# route-map Map1 deny 10
Device(config-route-map)# match tag 200
Device(config-route-map)# exit
Device(config)# interface fastethernet 0/0
Device(config-if)# ip router isis 150
Device(config-if)# router isis 150
Device(config-router)# distribute-list route-map Map1 in
```

Example: Configuring Route Filtering by IPv6 Route Destination Using a Prefix List

The following example shows how to enable IS-IS inbound filtering for routes that use standard IPv6 address prefixes:

```
Device(config)# ipv6 prefix-list 101 seq 5 deny 2001:db8::/32
Device(config)# ipv6 prefix-list 102 seq 4 permit 2001:db8::1/48 le 56
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# distribute-list prefix-list 101 in
Device(config-router-af)# distribute-list prefix-list 102 in ethernet 0/0
```

Verifying IS-IS Inbound Filtering

Perform this task to display the local Intermediate System-to-Intermediate System (IS-IS) routing information base (RIB). The `show` commands can be entered in any order.
SUMMARY STEPS

1. enable
2. show isis ip rib
3. show isis ipv6 rib

DETAILED STEPS

Step 1  enable
Enables privileged EXEC mode.

Example:
Device> enable

Step 2  show isis ip rib
Displays the IPv4 local RIB.

Example:
Device# show isis ip rib
IPv4 local RIB for IS-IS process
IPV4 unicast topology base (TID 0, TOPOID 0x0) ---------------
1.1.1.1/32
   [115/L2/20] via 30.30.30.20(Serial3/0), from 2.2.2.2, tag 0, LSP[3/3]
   [115/L2/20] via 100.100.100.20(Ethernet0/0), from 2.2.2.2, tag 0, LSP[3/3]
2.2.2.2/32
   [115/L1/20] via 30.30.30.20(Serial3/0), from 2.2.2.2, tag 0, LSP[4/2] -
   [115/L1/20] via 100.100.100.20(Ethernet0/0), from 2.2.2.2, tag 0, LSP[4/2] -
   [115/L2/20] via 30.30.30.20(Serial3/0), from 2.2.2.2, tag 0, LSP[3/3] -
   [115/L2/20] via 100.100.100.20(Ethernet0/0), from 2.2.2.2, tag 0, LSP[3/3] -
20.20.20.0/24
   [115/L1/20] via 30.30.30.20(Serial3/0), from 2.2.2.2, tag 0, LSP[4/2]
   [115/L1/20] via 100.100.100.20(Ethernet0/0), from 2.2.2.2, tag 0, LSP[4/2]
   [115/L2/20] via 30.30.30.20(Serial3/0), from 2.2.2.2, tag 0, LSP[3/3]
   [115/L2/20] via 100.100.100.20(Ethernet0/0), from 2.2.2.2, tag 0, LSP[3/3]

Step 3  show isis ipv6 rib
Displays the IPv6 local RIB.

Example:
Device# show isis ipv6 rib
IS-IS IPv6 process , local RIB
11::1/128
   via FE80::A8BB:CCFF:FE00::C800/Ethernet0/0, type L2 metric 20 tag 0 LSP [3/3]
20::/64
   via FE80::A8BB:CCFF:FE00::C800/Ethernet0/0, type L1 metric 20 tag 0 LSP [4/2]
   via FE80::A8BB:CCFF:FE00::C800/Ethernet0/0, type L2 metric 20 tag 0 LSP [3/3]
   * 22::2/128
   via FE80::A8BB:CCFF:FE00::C800/Ethernet0/0, type L1 metric 20 tag 0 LSP [4/2] -
   via FE80::A8BB:CCFF:FE00::C800/Ethernet0/0, type L2 metric 20 tag 0 LSP [3/3] -
2001:DB8::/64
   via FE80::A8BB:CCFF:FE00::C800/Ethernet0/0, type L1 metric 20 tag 0 LSP [4/2]
Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS-IS commands</td>
<td>Cisco IOS IP Routing: IS-IS Command Reference</td>
</tr>
<tr>
<td>Cisco IOS Commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for IS-IS Inbound Filtering

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
### Table 1: Feature Information for IS-IS Inbound Filtering

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS-IS Inbound Filtering</td>
<td>15.3(3)M</td>
<td>The Intermediate System-to-Intermediate System (IS-IS) Inbound Filtering feature allows users to define a route map to permit or deny IS-IS routes from being added to a routing table. You can configure access lists, prefix lists, gateways, or route maps with permit or deny rules, and apply these to the routing table using the <code>distribute-list</code> command. The following command was modified: <code>distribute-list in (IP).</code></td>
</tr>
</tbody>
</table>