# Configuring IS-IS Routing


- Information About IS-IS Routing, on page 1
- How to Configure IS-IS, on page 5
- How to Configure IS-IS Authentication, on page 13
- Monitoring and Maintaining IS-IS, on page 18
- Feature History for IS-IS, on page 18


## Information About IS-IS Routing

Integrated Intermediate System-to-Intermediate System (IS-IS) is an ISO dynamic routing protocol (described in ISO 105890). To enable IS-IS you should create an IS-IS routing process and assign it to a specific interface, rather than to a network. You can specify more than one IS-IS routing process per Layer 3 device by using the multiarea IS-IS configuration syntax. You should then configure the parameters for each instance of the IS-IS routing process.

Small IS-IS networks are built as a single area that includes all the devices in the network. As the network grows larger, the network reorganizes itself into a backbone area that is made up of all the connected set of Level 2 devices that are still connected to their local areas. Within a local area, devices know how to reach all system IDs. Between areas, devices know how to reach the backbone, and the backbone devices know how to reach other areas.

Devices establish Level 1 adjacencies to perform routing within a local area (station routing). Devices establish Level 2 adjacencies to perform routing between Level 1 areas (area routing).

A single Cisco device can participate in routing in up to 29 areas and can perform Level 2 routing in the backbone. In general, each routing process corresponds to an area. By default, the first instance of the routing process that is configured performs both Level 1 and Level 2 routing. You can configure additional device instances, which are automatically treated as Level 1 areas. You must configure the parameters for each instance of the IS-IS routing process individually.

For IS-IS multiarea routing, you can configure only one process to perform Level 2 routing, although you can define up to 29 Level 1 areas for each Cisco unit. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1. You can configure this process to perform Level 1 routing at the same time. If Level 2 routing is not desired for a device instance, remove the Level 2 capability using the **is-type** command in global configuration mode. Use the **is-type** command also to configure a different device instance as a Level 2 device.

# IS-IS Authentication

To prevent unauthorized devices from injecting false routing information into the link-state database, you can either set a plain text password for each interface and an area password for each IS-IS area, or you can configure an IS-IS authentication.

Plain text passwords do not provide security against unauthorized users. You can configure a plain text password to prevent unauthorized networking devices from forming adjacencies with the router. The password is exchanged as plain text and is visible to agents having access to view the IS-IS packets.

The new style of IS-IS authentication provides the following advantages over the plain text password configuration commands:

- Passwords are encrypted when the software configuration is displayed.
- Passwords are easier to manage and change.
- Passwords can be changed to new passwords without disrupting network operations.
- Authentication transitions which are nondisruptive.

Authentication modes (IS-IS authentication or plain text password) can either be configured on a given scope (IS-IS instance or interface) or level, but not both. However, different modes can be configured for different scopes or levels. In case mixed modes are configured, different keys must be used for different modes to ensure that the encrypted passwords in the protocol data units (PDUs) are not compromised.

## Clear Text Authentication

IS-IS clear text authentication provides the same functionality that is provided by the **area-password** or **domain-password** command.

## HMAC-MD5 Authentication

IS-IS supports message digest algorithm 5 (MD5) authentication, which is more secure than clear text authentication.

Hashed Message Authentication Code (HMAC) is a mechanism for message authentication codes (MACs) using cryptographic hash functions. HMAC-MD5 authentication adds an HMAC-MD5 digest to each IS-IS PDU. The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing messages from being injected into the network routing domain.

The following are the benefits of HMAC-MD5 authentication:

- Passwords can be changed to new passwords without disrupting routing messages.
- Authentication transitions which are nondisruptive. The device accepts PDUs with either no authentication information or stale authentication information and sends PDUs with current authentication information. These transitions are useful when migrating from no authentication to some type of authentication, when changing the authentication type, and when changing the authentication keys.

## HMAC-SHA Authentication

IS-IS supports Secure Hash Algorithm (SHA) authentication, that is, SHA-1, SHA-256, SHA-384, and SHA-512, which is more secure than MD5 authentication or clear text authentication.

When you enable the HMAC-SHA authentication method, a shared secret key is configured on all the devices that are connected on a common network. For each packet, this key is used to generate and verify a message digest that gets added to the packet. The message digest is a one-way function of the packet and the secret key.

### Hitless Upgrade

Before you migrate from using one type of security authentication to another, you must do the following:

1. All the devices must be loaded with the new image that supports the new authentication type. The devices will continue to use the original authentication method until all the devices have been loaded with the new image that supports the new authentication method, and all the devices have been configured to use the new authentication method.
2. Add a key chain with both the current key and a new key. For example when migrating from HMAC-MD5 to HMAC-SHA1-20, the current key is HMAC-MD5, and the new key is HMAC-SHA1-20. Ensure that the current key has a later end date for the send-lifetime field than the new key so that IS-IS continues to send the current key. Set the accept-lifetime value of both the keys to infinite so that IS-IS accepts both the keys.
3. After step 2 is completed, for all the devices in a link or area the current key can be removed from the key chain.

## Nonstop Forwarding Awareness

The integrated IS-IS Nonstop Forwarding (NSF) Awareness feature is supported for IPv4G. The feature allows customer premises equipment (CPE) devices that are NSF-aware to help NSF-capable devices perform nonstop forwarding of packets. The local device is not necessarily performing NSF, but its NSF awareness capability allows the integrity and accuracy of the routing database and the link-state database on the neighboring NSF-capable device to be maintained during the switchover process.

The integrated IS-IS Nonstop Forwarding (NSF) Awareness feature is automatically enabled and requires no configuration.

## IS-IS Global Parameters

The following are the optional IS-IS global parameters that you can configure:

- You can force a default route into an IS-IS routing domain by configuring a default route that is controlled by a route map. You can also specify the other filtering options that are configurable under a route map.
- You can configure the device to ignore IS-IS link-state packets (LSPs) that are received with internal checksum errors, or to purge corrupted LSPs, and cause the initiator of the LSP to regenerate it.
- You can assign passwords to areas and domains.
- You can create aggregate addresses that are represented in the routing table by a summary address (based on route summarization). Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the specific routes.
- You can set an overload bit.
- You can configure the LSP refresh interval and the maximum time that an LSP can remain in the device database without a refresh.

- You can set the throttling timers for LSP generation, shortest path first computation, and partial route computation.
- You can configure the device to generate a log message when an IS-IS adjacency changes state (Up or Down).
- If a link in the network has a maximum transmission unit (MTU) size of less than 1500 bytes, you can lower the LSP MTU so that routing still occurs.
- You can use the **partition avoidance** command to prevent an area from becoming partitioned when full connectivity is lost among a Level 1-2 border device, adjacent Level 1 devices, and end hosts.

# IS-IS Interface Parameters

You can optionally configure certain interface-specific IS-IS parameters independently from other attached devices. However, if you change default value, such as multipliers and time intervals, it makes sense to also change them on multiple devices and interfaces. Most of the interface parameters can be configured for level 1, level 2, or both.

The following are the interface-level parameters that you can configure:

- The default metric on the interface that is used as a value for the IS-IS metric and assigned when quality of service (QoS) routing is not performed.
- The hello interval (length of time between hello packets sent on the interface) or the default hello packet multiplier used on the interface to determine the hold time sent in IS-IS hello packets. The hold time determines how long a neighbor waits for another hello packet before declaring the neighbor down. This determines how quickly a failed link or neighbor is detected so that routes can be recalculated. Change the hello multiplier in circumstances where hello packets are lost frequently and IS-IS adjacencies are failing unnecessarily. You can raise the hello multiplier and lower the hello interval correspondingly to make the hello protocol more reliable, without increasing the time required to detect a link failure.
- Other time intervals:
  - Complete sequence number PDU (CSNP) interval—CSNPs are sent by the designated device to maintain database synchronization.
  - Retransmission interval—This is the time between retransmission of IS-IS LSPs for point-to-point links.
  - IS-IS LSP retransmission throttle interval—This is the maximum rate (number of milliseconds between packets) at which IS-IS LSPs are resent on point-to-point links. This interval is different from the retransmission interval, which is the time between successive retransmissions of the same LSP.
- Designated device-election priority, which allows you to reduce the number of adjacencies required on a multiaccess network, which in turn reduces the amount of routing protocol traffic and the size of the topology database.
- The interface circuit type, which is the type of adjacency required for neighbors on the specified interface.
- Password authentication for the interface.

# How to Configure IS-IS

The following sections provide information on how to enable IS-IS on an interface, how to configure IS-IS global parameters, and how to configure IS-IS interface parameters.

## Default IS-IS Configuration

***Table 1: Default IS-IS Configuration***

| Feature | Default Setting |
|---|---|
| Ignore link-state PDU (LSP) errors | Enabled. |
| IS-IS type | Conventional IS-IS—The router acts as both a Level 1 (station) and a router.<br>Multiarea IS-IS—The first instance of the IS-IS routing process is a router. Remaining instances are Level 1 routers. |
| Default-information originate | Disabled. |
| Log IS-IS adjacency state changes. | Disabled. |
| LSP generation throttling timers | Maximum interval between two consecutive occurrences—5000 mi<br>Initial LSP generation delay—50 milliseconds.<br>Hold time between the first and second LSP generation—200 millis |
| LSP maximum lifetime (without a refresh) | 1200 seconds (20 minutes) before the LSP packet is deleted. |
| LSP refresh interval | Every 900 seconds (15 minutes). |
| Maximum LSP packet size | 1497 bytes. |
| NSF Awareness | Enabled. Allows Layer 3 devices to continue forwarding packets from Nonstop Forwarding-capable router during hardware or software ch |
| Partial route computation (PRC) throttling timers | Maximum PRC wait interval—5000 milliseconds.<br>Initial PRC calculation delay after a topology change—50 milliseco<br>Hold time between the first and second PRC calculation—200 milli |
| Partition avoidance | Disabled. |
| Password | No area or domain password is defined, and authentication is disabl |
| Set-overload-bit | Disabled. When enabled, if no arguments are entered, the overload b immediately and remains set until you enter the **no set-overload-bit** |

| Feature | Default Setting |
|---|---|
| Shortest path first (SPF) throttling timers | Maximum interval between consecutive SFPs—5000 milliseconds.<br>Initial SFP calculation after a topology change—200 milliseconds.<br>Hold time between the first and second SFP calculation—50 millisecon |
| Summary-address | Disabled. |

# Enabling IS-IS Routing

To enable IS-IS, specify a name and a network entity title (NET) for each routing process. Enable IS-IS routing on the interface and specify the area for each instance of the routing process.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device>enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |
| **Step 3** | **clns routing**<br>**Example:**<br>`Device(config)#clns routing` | Enables ISO connectionless routing on the device. |
| **Step 4** | **router isis** [*area tag*]<br>**Example:**<br>`Device(config)#router isis tag1` | Enables IS-IS routing for the specified routing process and enters IS-IS routing configuration mode.<br>(Optional) Use the *area tag* argument to identify the area to which the IS-IS router is assigned. Enter a value if you are configuring multiple IS-IS areas.<br>The first IS-IS instance that is configured is Level 1-2 by default. Later instances are automatically configured as Level 1. You can change the level of routing by using the **is-type** command in global configuration mode. |
| **Step 5** | **net** *network-entity-title*<br>**Example:** | Configures the NETs for the routing process. While configuring multiarea IS-IS, specify a |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-router)#net 47.0004.004d.0001.0001.0c11.1111.00` | NET for each routing process. Specify a name for a NET and for an address. |
| **Step 6** | **is-type** {**level-1** \| **level-1-2** \| **level-2-only**}<br>**Example:**<br>`Device(config-router)#is-type level-2-only` | (Optional) Configures the router to act as a Level 1 (station) router, a Level 2 (area) router for multiarea routing, or both (the default):<br>• **level 1**—Acts as a station router only.<br>• **level 1-2**—Acts as both a station router and an area router.<br>• **level 2**—Acts as an area router only. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-router)#end` | Returns to global configuration mode. |
| **Step 8** | **interface** *interface-id*<br>**Example:**<br>`Device(config)#interface gigabitethernet 1/0/1` | Specifies an interface to route IS-IS, and enters interface configuration mode. If the interface is not already configured as a Layer 3 interface, enter the **no switchport** command to configure the interface into Layer 3 mode. |
| **Step 9** | **ip router isis** [*area tag*]<br>**Example:**<br>`Device(config-if)#ip router isis tag1` | Configures an IS-IS routing process on the interface and attaches an area designator to the routing process. |
| **Step 10** | **ip address** *ip-address-mask*<br>**Example:**<br>`Device(config-if)#ip address 10.0.0.5 255.255.255.0` | Defines the IP address for the interface. An IP address is required for all the interfaces in an area, that is enabled for IS-IS, if any one interface is configured for IS-IS routing. |
| **Step 11** | **end**<br>**Example:**<br>`Device(config)#end` | Returns to privileged EXEC mode. |
| **Step 12** | **show isis** [*area tag*] **database detail**<br>**Example:**<br>`Device#show isis database detail` | Verifies your entries. |

# Configuring IS-IS Global Parameters

To configure global IS-IS parameters, perform this procedure:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device>enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |
| **Step 3** | **router isis**<br>**Example:**<br>`Device(config)#router isis` | Specifies the IS-IS routing protocol and enters router configuration mode. |
| **Step 4** | **default-information originate** [**route-map** *map-name*]<br>**Example:**<br>`Device(config-router)#default-information originate route-map map1` | (Optional) Forces a default route into the IS-IS routing domain. When you enter the **route-map** *map-name* command, the routing process generates the default route for a valid route map. |
| **Step 5** | **ignore-lsp-errors**<br>**Example:**<br>`Device(config-router)#ignore-lsp-errors` | (Optional) Configures the device to ignore LSPs with internal checksum errors, instead of purging the LSPs. This command is enabled by default (corrupted LSPs are dropped). To purge the corrupted LSPs, enter the **no ignore-lsp-errors** command in router configuration mode. |
| **Step 6** | **area-password** *password*<br>**Example:**<br>`Device(config-router)#area-password 1password` | (Optional Configures the area authentication password that is inserted in Level 1 (station router level) LSPs. |
| **Step 7** | **domain-password** *password*<br>**Example:**<br>`Device(config-router)#domain-password 2password` | (Optional) Configures the routing domain authentication password that is inserted in Level 2 (area router level) LSPs. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **summary-address** *address mask* [**level-1** \| **level-1-2** \| **level-2**]<br>**Example:**<br>`Device(config-router)#summary-address 10.1.0.0 255.255.0.0 level-2` | (Optional) Creates a summary of addresses for a given level. |
| **Step 9** | **set-overload-bit** [**on-startup** {*seconds* \| **wait-for-bgp**}]<br>**Example:**<br>`Device(config-router)#set-overload-bit on-startup wait-for-bgp` | (Optional) Sets an overload bit to allow other devices to ignore the device in their shortest path first (SPF) calculations if the device is having problems.<br>• (Optional) **on-startup**—Sets the overload bit only on startup. If **on-startup** is not specified, the overload bit is set immediately and remains set until you enter the **no set-overload-bit** command. If **on-startup** is specified, you must either enter number of seconds or enter **wait-for-bgp**.<br>• *seconds*—When the **on-startup** keyword is configured, it causes the overload bit to be set when the system is started and remains set for the specified number of seconds. The range is from 5 to 86400 seconds.<br>• **wait-for-bgp**—When the **on-startup** keyword is configured, causes the overload bit to be set when the system is started and remains set until BGP has converged. If BGP does not signal the IS-IS that it is converged, the IS-IS will turn off the overload bit after 10 minutes. |
| **Step 10** | **lsp-refresh-interval** *seconds*<br>**Example:**<br>`Device(config-router)#lsp-refresh-interval 1080` | (Optional) Sets an LSP refresh interval, in seconds. The range is from 1 to 65535 seconds. The default is to send LSP refreshes every 900 seconds (15 minutes). |
| **Step 11** | **max-lsp-lifetime** *seconds*<br>**Example:**<br>`Device(config-router)#max-lsp-lifetime 1000` | (Optional) Sets the maximum time that LSP packets remain in the router database without being refreshed. The range is from 1 to 65535 seconds. The default is 1200 seconds (20 minutes). After the specified time interval, the LSP packet is deleted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 12** | **lsp-gen-interval** [**level-1** \| **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*]<br>**Example:**<br>`Device(config-router)#lsp-gen-interval level-2 2 50 100` | (Optional) Sets the IS-IS LSP generation throttling timers:<br>• *lsp-max-wait*—Maximum interval (in milliseconds) between two consecutive occurrences of an LSP being generated. The range is from 1 to 120; the default is 5000.<br>• *lsp-initial-wait*—Initial LSP generation delay (in milliseconds). The range is from 1 to 10000; the default is 50.<br>• *lsp-second-wait*—Hold time between the first and second LSP generation (in milliseconds). The range is from 1 to 10000; the default is 200. |
| **Step 13** | **spf-interval** [**level-1** \| **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]<br>**Example:**<br>`Device(config-router)#spf-interval level-2 5 10 20` | (Optional) Sets IS-IS SPF throttling timers.<br>• *spf-max-wait*—Maximum interval between consecutive SFPs (in milliseconds). The range is from 1 to 120; the default is 5000.<br>• *spf-initial-wait*—Initial SFP calculation after a topology change (in milliseconds). The range is from 1 to 10000; the default is 50.<br>• *spf-second-wait*—Hold time between the first and second SFP calculation (in milliseconds). The range is from 1 to 10000; the default is 200. |
| **Step 14** | **prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*]<br>**Example:**<br>`Device(config-router)#prc-interval 5 10 20` | (Optional) Sets IS-IS PRC throttling timers.<br>• *prc-max-wait*—Maximum interval (in milliseconds) between two consecutive PRC calculations. The range is from 1 to 120; the default is 5000.<br>• *prc-initial-wait*—Initial PRC calculation delay (in milliseconds) after a topology change. The range is from 1 to 10,000; the default is 50.<br>• *prc-second-wait*—Hold time between the first and second PRC calculation (in milliseconds). The range is from 1 to 10,000; the default is 200. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 15** | **log-adjacency-changes** [**all**]<br>**Example:**<br>`Device(config-router)#log-adjacency-changes all` | (Optional) Sets the router to log IS-IS adjacency state changes. Enter **all** to include all the changes generated by events that are not related to the IS-IS hellos, including End System-to-Intermediate System PDUs and LSPs. |
| **Step 16** | **lsp-mtu** *size*<br>**Example:**<br>`Device(config-router)#lsp mtu 1560` | (Optional) Specifies the maximum LSP packet size, in bytes. The range is from 128 to 4352; the default is 1497 bytes.<br>**Note**<br>If a link in the network has a reduced MTU size, you must change the LSP MTU size on all the devices in the network. |
| **Step 17** | **partition avoidance**<br>**Example:**<br>`Device(config-router)#partition avoidance` | (Optional) Causes an IS-IS Level 1-2 border router to stop advertising the Level 1 area prefix into the Level 2 backbone when full connectivity is lost among the border router, all adjacent level 1 routers, and end hosts. |
| **Step 18** | **end**<br>**Example:**<br>`Device(config)#end` | Returns to privileged EXEC mode. |

# Configuring IS-IS Interface Parameters

To configure IS-IS interface-specific parameters, perform this procedure:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device>enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-id*<br>**Example:** | Specifies the interface to be configured and enters interface configuration mode. If the interface is not already configured as a Layer |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)#interface gigabitethernet 1/0/1` | 3 interface, enter the **no switchport** command to configure the interface into Layer 3 mode. |
| **Step 4** | **isis metric** *default-metric* [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)#isis metric 15` | (Optional) Configures the metric (or cost) for the specified interface. The range is from 0 to 63; the default is 10. If no level is entered, the default is applied to both Level 1 and Level 2 routers. |
| **Step 5** | **isis hello-interval** {*seconds* \| **minimal**} [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)#isis hello-interval minimal` | (Optional) Specifies the length of time between the hello packets that are sent by the device. By default, a value that is three times the hello interval *seconds* is advertised as the *holdtime* in the hello packets sent. With smaller hello intervals, topological changes are detected faster, but there is more routing traffic.<br>• **minimal**—Causes the system to compute the hello interval based on the hello multiplier so that the resulting hold time is 1 second.<br>• *seconds*—Range is from 1 to 65535; default is 10 seconds. |
| **Step 6** | **isis hello-multiplier** *multiplier* [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)#isis hello-multiplier 5` | (Optional) Specifies the number of IS-IS hello packets that a neighbor must miss before the device declares the adjacency as down. The range is from 3 to 1000; default is 3.<br>**Note**<br>Using a smaller hello multiplier causes fast convergence, but might result in routing instability. |
| **Step 7** | **isis csnp-interval** *seconds* [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)#isis csnp-interval 15` | (Optional) Configures the IS-IS complete sequence number PDU (CSNP) interval for the interface. The range is from 0 to 65535; default is 10 seconds. |
| **Step 8** | **isis retransmit-interval** *seconds*<br>**Example:**<br>`Device(config-if)#isis retransmit-interval 7` | (Optional) Configures the number of seconds between the retransmission of IS-IS LSPs for point-to-point links. Specify an integer that is greater than the expected round-trip delay between any two routers on the network. The range is from 0 to 65535; default is 5 seconds. |
| **Step 9** | **isis retransmit-throttle-interval** *milliseconds*<br>**Example:** | (Optional) Configures the IS-IS LSP retransmission throttle interval, which is the maximum rate (number of milliseconds |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-if)#isis retransmit-throttle-interval 4000` | between packets) at which IS-IS LSPs will be resent on point-to-point links. The range is from 0 to 65535; default is determined by the **isis lsp-interval** command. |
| **Step 10** | **isis priority** *value* [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)#isis priority 50` | (Optional) Configures the priority for the designated router. The range is from 0 to 127; default is 64. |
| **Step 11** | **isis circuit-type** {**level-1** \| **level-1-2** \| **level-2-only**}<br>**Example:**<br>`Device(config-if)#isis circuit-type level-1-2` | (Optional) Configures the type of adjacency that is required for neighbors on the specified interface (specify the interface circuit type).<br>• **level-1**—Level 1 adjacency is established if there is at least one area address that is common to both this node and its neighbors.<br>• **level-1-2**—Level 1 and Level 2 adjacency are established if the neighbor is also configured as both Level 1 and Level 2, and there is at least one area in common. If there is no area in common, a Level 2 adjacency is established. This is the default option.<br>• **level 2**—Level 2 adjacency is established. If the neighbor router is a Level 1 router, no adjacency is established. |
| **Step 12** | **isis password** *password* [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)#isis password secret` | (Optional) Configures the authentication password for an interface. By default, authentication is disabled. Specifying Level 1 or Level 2 enables the password only for Level 1 or Level 2 routing, respectively. If you do not specify a level, the default is Level 1 and Level 2. |
| **Step 13** | **end**<br>**Example:**<br>`Device(config)#end` | Returns to privileged EXEC mode. |

# How to Configure IS-IS Authentication

The following sections provide information on how to generate authentication keys, how to configure IS-IS authentication for an interface, and how to configure IS-IS authentication for an instance.

# Configuring Authentication Keys

You can configure multiple keys with lifetimes. To send authentication packets, the key with the latest send lifetime setting is selected. If multiple keys have the same send lifetime setting, the key is randomly selected. Use the **accept-lifetime** command for examining and accepting the authentication packets that are received. The device must be aware of these lifetimes.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device>enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |
| **Step 3** | **key chain** *name-of-chain*<br>**Example:**<br>`Device(config)#key chain key10` | Identifies a key chain, and enters key chain configuration mode. |
| **Step 4** | **key** *number*<br>**Example:**<br>`Device(config-keychain)#key 2000` | Identifies the key number. The range is from 0 to 65535. |
| **Step 5** | **key-string** *text*<br>**Example:**<br>`Device(config-keychain-key)#Room 20, 10th floor` | Identifies the key string. The string can contain 1-80 uppercase and lowercase alphanumeric characters, but the first character cannot be a number. |
| **Step 6** | **accept-lifetime** *start-time* {**infinite** \| *end-time* \| **duration** *seconds*}<br>**Example:**<br>`Device(config-keychain-key)#accept-lifetime 12:30:00 Jan 25 1009 infinite` | (Optional) Specifies the time period during which the key can be received.<br>The *start-time* and *end-time* syntax can be either *hh:mm:ss month date year* or *hh:mm:ss date month year*. The default is forever with the default *start-time* and the earliest acceptable date is January 1, 1993. The default *end-time* and **duration** is **infinite**. |
| **Step 7** | **send-lifetime** *start-time* {**infinite** \| *end-time* \| **duration** *seconds*}<br>**Example:** | (Optional) Specifies the time period during which the key can be sent. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-keychain-key)#accept-lifetime 23:30:00 Jan 25 1019 infinite` | The *start-time* and *end-time* syntax can be either *hh:mm:ss month date year* or *hh:mm:ss date month year*. The default *start-time* is **infinite** and the earliest acceptable date is January 1, 1993. The default *end-time* and **duration** is **infinite**. |
| **Step 8** | **cryptographic-algorithm** {**hmac-sha-1** \| **hmac-sha-256** \| **hmac-sha-384** \| **hmac-sha-512** \| **md5** }<br>**Example:**<br>`Device(config-keychain-key)#cryptographic-algorithm hmac-sha1-256` | (Optional) Specifies the cryptographic algorithm. |
| **Step 9** | **end**<br>**Example:**<br>`Device(config-keychain-key)#end` | Returns to privileged EXEC mode. |
| **Step 10** | **show key chain**<br>**Example:**<br>`Device#show key chain` | Displays authentication key information. |

# Configuring HMAC-MD5 or Clear Text Authentication for an IS-IS Instance

To achieve a smooth transition from one authentication method to another and to allow for continuous authentication of IS-IS PDUs, perform this procedure on each device that communicates in the network.

### Before you begin

You should have generated an authentication string key. The same authentication string key should be configured on all the devices in the network.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device>enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device#configure terminal` | |
| **Step 3** | **router isis** [**area** *tag*]<br>**Example:**<br>`Device(config)#router isis 1` | Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. Enters router configuration mode. |
| **Step 4** | **authentication send-only** [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-router)#authentication send-only` | Specifies that authentication is performed only on the PDUs that are being sent (not received) for the specified IS-IS instance. |
| **Step 5** | **authentication mode** {**md5** \| **text**}[**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-router)#authentication mode md5` | Specifies the types of authentication to be used in PDUs for the specified IS-IS instance:<br>• **md5**—MD5 authentication.<br>• **text**—Clear text authentication. |
| **Step 6** | **authentication key-chain** *name-of-chain* [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-router)#authentication key-chain remote3754` | Enables authentication for the specified IS-IS instance. |
| **Step 7** | **no authentication send-only**<br>**Example:**<br>`Device(config-router)#no authentication send-only` | Specifies that authentication is performed only on the PDUs that are being sent and received for the specified IS-IS instance. |

# Configuring HMAC-MD5 or Clear Text Authentication for an IS-IS Interface

To achieve a smooth transition from one authentication method to another and to allow for continuous authentication of IS-IS PDUs, perform this procedure on each device that communicates in the network.

### Before you begin

You should have generated an authentication string key. The same authentication string key should be configured on all the devices in the network.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device>enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)#interface ethernet 0` | Configures an interface. |
| **Step 4** | **isis authentication send-only** [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)#isis authentication send-only` | Specifies that authentication is performed only on the PDUs being sent (not received) for the specified IS-IS interface. |
| **Step 5** | **isis authentication mode** {**md5** \| **text**}[**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)#isis authentication mode md5` | Specifies the types of authentication to be used in PDUs for the specified IS-IS interface:<br>• **md5**—MD5 authentication.<br>• **text**—Clear text authentication. |
| **Step 6** | **isis authentication key-chain** *name-of-chain* [**level-1** \| **level-2**]<br>**Example:**<br>`Device(config-if)#isis authentication key-chain multistate87723` | Enables MD5 authentication for the specified IS-IS interface. |
| **Step 7** | **no isis authentication send-only**<br>**Example:**<br>`Device(config-if)#no isis authentication send-only` | Specifies that authentication is performed only on the PDUs that are being sent and received for the IS-IS interface. |

# Monitoring and Maintaining IS-IS

You can display specific IS-IS statistics, such as the contents of routing tables, caches, and databases. You can also display information about specific interfaces, filters, or neighbors.

The following table lists the privileged EXEC commands for clearing and displaying IS-IS routing.

***Table 2: IS-IS show Commands***

| Command |
|---|
| **show ip route isis** |
| **show isis database** |
| **show isis routes** |
| **show isis spf-log** |
| **show isis topology** |
| **show route-map** |
| **trace clns** *destination* |

# Feature History for IS-IS

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Everest 16.5.1a | IS-IS Routing | Integrated Intermediate System-to-Intermediate System (IS-IS) is an ISO dynamic routing protocol (described in ISO 105890). |
| Cisco IOS XE Gibraltar 16.10.1 | Secure Hash Algorithm (SHA) authentication | IS-IS now supports Secure Hash Algorithm (SHA) authentication—SHA-1, SHA-256, SHA-384, and SHA-512. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.