

IS-IS

- Feature history for IS-IS, on page 1
- Understand IS-IS, on page 1
- Understand IS-IS authentication, on page 5
- Understand IS-IS for IPv6, on page 6
- Configure IS-IS, on page 7
- Configure IS-IS authentication, on page 15
- Monitor IS-IS configuration, on page 20
- Configure IS-IS for IPv6, on page 20
- Verify IPv6 IS-IS configuration, on page 27

Feature history for IS-IS

This table provides release and platform support 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 name and description	Supported platform
Cisco IOS XE 26.2.1ea	IS-IS: IS-IS feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	IS-IS: IS-IS is an ISO dynamic routing protocol, described in ISO 105890.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Understand IS-IS

Integrated Intermediate System-to-Intermediate System (IS-IS) is an ISO dynamic routing protocol, described in ISO 105890. To enable IS-IS, create an IS-IS routing process and assign it to a specific interface. Do not assign it to a network. Specify more than one IS-IS routing process per Layer 3 device using the multiarea IS-IS configuration syntax. Configure the parameters for each instance of the IS-IS routing process.

Small IS-IS networks form a single area including all devices in the network. As the network expands, it organizes into a backbone area consisting of all connected 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 device can participate in routing for up to 29 areas and perform Level 2 routing in the backbone. Each routing process generally 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. 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. When 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 by 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 global parameters

You can configure these optional global IS-IS parameters.

- 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). You can also summarize routes learned from other routing protocols. The summary metric is the smallest of all 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 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 network link 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

Configure interface-specific IS-IS parameters independently. If you change a default value, such as multipliers or time intervals, adjust them on all relevant devices and interfaces. You can configure most interface parameters for level 1, level 2, or both.

Interface-level parameters that you can configure include:

- 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 determines the time between hello packets sent on the interface. The hello packet multiplier is used to calculate the hold time 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.

Nonstop Forwarding awareness

The integrated IS-IS Nonstop Forwarding (NSF) Awareness feature is supported for IPv4G. The feature enables NSF-aware customer premises equipment (CPE) devices to assist NSF-capable devices with nonstop packet forwarding. 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.

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 Level 2 (area) router. Multiarea IS-IS: The first instance of the IS-IS routing process is a Level 1-2 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 milliseconds. Initial LSP generation delay: 50 milliseconds. Hold time between the first and second LSP generation: 200 milliseconds.
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 a neighboring Nonstop Forwarding-capable router during hardware or software changes.
Partial route computation (PRC) throttling timers	Maximum PRC wait interval: 5000 milliseconds. Initial PRC calculation delay after a topology change: 50 milliseconds. Hold time between the first and second PRC calculation: 200 milliseconds.
Partition avoidance	Disabled.
Password	No area or domain password is defined, and authentication is disabled.
Set-overload-bit	Disabled. When enabled, if no arguments are entered, the overload bit is set immediately and remains set until you enter the **no set-overload-bit** command.

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

Understand IS-IS authentication

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

Plain text passwords are insecure for unauthorized user access. 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 remains visible to agents accessing IS-IS packets.

The new style of IS-IS authentication provides several 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, either IS-IS authentication or plain text password, can be configured on a given scope, such as an IS-IS instance or interface, or a specific level, but not both simultaneously. 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 for added security compared to 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.

Benefits of HMAC-MD5 authentication include:

- Passwords can be changed 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, including SHA-1, SHA-256, SHA-384, and SHA-512. This method is more secure than MD5 or clear text authentication.

When enabling the HMAC-SHA authentication method, configure a shared secret key on all devices connected to the common network. Use this key to generate and verify a message digest for each packet, adding the message digest to the packet. The message digest is a one-way function of the packet and the secret key.

Hitless upgrade

Complete these steps before switching from one type of security authentication to another:

1. All the devices must be loaded with the new image that supports the new authentication type. The devices continue to use the original authentication method until all devices are loaded with the new image that supports the new authentication method and 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 the current key has a later send-lifetime end date than the new key so 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. Once you complete step 2, remove the current key from the key chain for all devices in a link or area.

Understand IS-IS for IPv6

IS-IS is an Interior Gateway Protocol (IGP) used to advertise link-state information across the network, forming a representation of the network topology. IS-IS is an OSI hierarchical routing protocol that you can use to designate an intermediate system as either a Level 1 or Level 2 device. Level 2 devices route traffic between Level 1 areas, creating an intradomain routing backbone. Integrated IS-IS employs a single routing algorithm to support IPv6, IPv4, and OSI network families.

IS-IS in IPv6 functions similarly to IS-IS in IPv4 and offers many of the same advantages. IPv6 enhancements to IS-IS support advertising IPv6 prefixes alongside both IPv4 and OSI routes. You can configure IPv6-specific parameters through extensions to the IS-IS CLI. Using IPv6 IS-IS, you can extend the address families supported by IS-IS to include IPv6, alongside OSI and IPv4.

A device that is running IS-IS IPv6 maintains a local RIB to store all routes to destinations learned from neighbors. At the end of each SPF, the best and least-cost routes are installed into the global IPv6 routing table.

IS-IS in IPv6 supports either single-topology mode or multiple topology mode.

IS-IS single-topology for IPv6

Single-topology support for IPv6 allows IS-IS for IPv6 to be configured on interfaces along with other network protocols (for example, IPv4 and Connectionless Network Service [CLNS]). Configure all interfaces with the same set of network address families. In addition, all routers in the IS-IS area (for Level 1 routing) or the domain (for Level 2 routing) must support the identical set of network layer address families on all interfaces.

You can use either old-style or new-style TLVs when using single-topology support for IPv6. However, the TLVs used to advertise reachability to IPv6 prefixes use extended metrics. If you have not configured support for only new-style TLVs for IPv4, set the interface metric to 63 or less. In single-topology IPv6 mode, the configured metric is always the same for both IPv4 and IPv6.

IS-IS multitopology for IPv6

IS-IS multitopology support for IPv6 enables IS-IS to maintain distinct topologies within a single area or domain. This mode removes the restriction requiring all IS-IS-configured interfaces to support the same network address families. The restriction requiring all routers in the IS-IS area (Level 1 routing) or domain (Level 2 routing) to support the same network layer address families is eliminated. Multiple SPFs are performed, one for each configured topology. Connectivity among a subset of routers in the area or domain is enough for a given network address family to be routable.

You can use the **isis ipv6 metric** command to configure different metrics on an interface for IPv6 and IPv4.

The **metric-style wide** command configures IS-IS to use new-style TLVs, which are essential when IPv6 information is advertised in link-state packets (LSPs) and must use extended metrics.

Transition from single-topology to multitopology for IPv6

Ensure that all routers in the area or domain use the same type of IPv6 support. A router operating in multitopology mode will not recognize the IPv6 support of a single-topology router, resulting in gaps in the IPv6 topology. To transition from single-topology support to multitopology support, a multitopology transition mode is provided.

The multitopology transition mode allows a network operating in single-topology IS-IS IPv6 support mode to continue to work while upgrading routers to include multitopology IS-IS IPv6 support. While in transition mode, both types of TLVs (single-topology and multitopology) are sent in LSPs for all configured IPv6 addresses, but the router continues to operate in single-topology mode (that is, the topological restrictions of the single-topology mode are still in effect). After upgrading all routers to support multitopology IPv6 and achieving transition mode operation, transition mode can be removed from the configuration. Once all routers in the area or domain are operating in multitopology IPv6 mode, the topological restrictions of single-topology mode are no longer in effect.

Configure IS-IS

These procedures 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.

Enable 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** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**clns routing** **Example:** `Device(config)# clns routing`	Enables ISO connectionless routing on the device.
Step 4	**router isis** [*area tag*] **Example:** `Device(config)# router isis tag1`	Enables IS-IS routing for the specified routing process and enters IS-IS routing configuration mode. (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. 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* **Example:** `Device(config-router)# net 47.0004.004d.0001.0001.0c11.1111.00`	Configures the NETs for the routing process. While configuring multiarea IS-IS, specify a 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**} **Example:** `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): • **level 1**: Acts as a station router only.

	Command or Action	Purpose
		• **level 1-2**: Acts as both a station router and an area router. • **level 2**: Acts as an area router only.
Step 7	**exit** **Example:** `Device(config-router)# end`	Returns to global configuration mode.
Step 8	**interface** *interface-id* **Example:** `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*] **Example:** `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* **Example:** `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** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 12	**show isis** [*area tag*] **database detail** **Example:** `Device# show isis database detail`	Verifies your entries.

Configure IS-IS global parameters

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router isis** **Example:** `Device(config)# router isis`	Specifies the IS-IS routing protocol and enters router configuration mode.
Step 4	**metric** *default-value* [**level-1** | **level-2**] **Example:** `Device(config-router)# metric 25 level-2`	(Optional) Globally sets a new default metric value for all IS-IS interfaces. • The value 25 shown in the example will apply only to Level 2 IS-IS interfaces. If you do not enter the **level-1** or **level-2** keyword, the metric will be applied to both Level 1 and Level 2 IS-IS interfaces.
Step 5	**default-information originate** [**route-map** *map-name*] **Example:** `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 6	**ignore-lsp-errors** **Example:** `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 7	**area-password** *password* **Example:** `Device(config-router)# area-password 1password`	(Optional Configures the area authentication password that is inserted in Level 1 (station router level) LSPs.
Step 8	**domain-password** *password* **Example:** `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 9	**summary-address** *address mask* [**level-1** | **level-1-2** | **level-2**] **Example:** `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 10	**set-overload-bit** [**on-startup** {*seconds* | **wait-for-bgp**}] **Example:** `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. • (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**. • *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. • **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 11	**lsp-refresh-interval** *seconds* **Example:** `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 12	**max-lsp-lifetime** *seconds* **Example:** `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 13	**lsp-gen-interval** [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*] **Example:** `Device(config-router)# lsp-gen-interval level-2 2 50 100`	(Optional) Sets the IS-IS LSP generation throttling timers: • *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. • *lsp-initial-wait*: Initial LSP generation delay (in milliseconds). The range is from 1 to 10000; the default is 50. • *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 14	**spf-interval** [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*] **Example:** `Device(config-router)# spf-interval level-2 5 10 20`	(Optional) Sets IS-IS SPF throttling timers. • *spf-max-wait*: Maximum interval between consecutive SFPs (in milliseconds). The range is from 1 to 120; the default is 5000. • *spf-initial-wait*: Initial SFP calculation after a topology change (in milliseconds). The range is from 1 to 10000; the default is 50. • *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 15	**prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*] **Example:** `Device(config-router)# prc-interval 5 10 20`	(Optional) Sets IS-IS PRC throttling timers. • *prc-max-wait*: Maximum interval (in milliseconds) between two consecutive PRC calculations. The range is from 1 to 120; the default is 5000. • *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. • *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 16	**log-adjacency-changes** [**all**] **Example:** `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 17	**lsp-mtu** *size* **Example:** `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. **Note** 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 18	**partition avoidance** **Example:** `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 19	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configure IS-IS interface parameters

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **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**] **Example:** `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**] **Example:** `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. • **minimal**: Causes the system to compute the hello interval based on the hello multiplier so that the resulting hold time is 1 second. • *seconds*: Range is from 1 to 65535; default is 10 seconds.
Step 6	**isis hello-multiplier** *multiplier* [**level-1** | **level-2**] **Example:** `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. **Note** Using a smaller hello multiplier causes fast convergence, but might result in routing instability.
Step 7	**isis csnp-interval** *seconds* [**level-1** | **level-2**] **Example:** `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* **Example:** `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* **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**] **Example:** `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**} **Example:** `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). • **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. • **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. • **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**] **Example:** `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** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configure IS-IS authentication

These procedures provide information on how to generate authentication keys, configure IS-IS authentication for an interface, and configure IS-IS authentication for an instance.

Configuring authentication keys

You can configure multiple keys with lifetimes. The key with the latest send lifetime setting is selected to send authentication packets. The key is randomly selected if multiple keys have the same send lifetime setting. 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** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *name-of-chain* **Example:** `Device(config)# key chain key10`	Identifies a key chain, and enters key chain configuration mode.
Step 4	**key** *number* **Example:** `Device(config-keychain)# key 2000`	Identifies the key number. The range is from 0 to 65535.
Step 5	**key-string** *text* **Example:** `Device(config-keychain-key)# key-string 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*} **Example:** `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. 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*} **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** } **Example:** `Device(config-keychain-key)# cryptographic-algorithm hmac-sha1-256`	(Optional) Specifies the cryptographic algorithm.
Step 9	**end** **Example:** `Device(config-keychain-key)# end`	Returns to privileged EXEC mode.
Step 10	**show key chain** **Example:** `Device# show key chain`	Displays authentication key information.

Configure 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** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**router isis** [**area** *tag*] **Example:** `Device(config)# router isis 1`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required, and enters router configuration mode.
Step 4	**authentication send-only** [**level-1** | **level-2**] **Example:** `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**] **Example:** `Device(config-router)# authentication mode md5`	Specifies the types of authentication to be used in PDUs for the specified IS-IS instance: • **md5**: MD5 authentication. • **text**: Clear text authentication.
Step 6	**authentication key-chain** *name-of-chain* [**level-1** | **level-2**] **Example:** `Device(config-router)# authentication key-chain remote3754`	Enables authentication for the specified IS-IS instance.
Step 7	**no authentication send-only** **Example:** `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.

Configure 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** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface ethernet 0`	Configures an interface.
Step 4	**isis authentication send-only** [**level-1** | **level-2**] **Example:** `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**] **Example:** `Device(config-if)# isis authentication mode md5`	Specifies the types of authentication to be used in PDUs for the specified IS-IS interface: • **md5**: MD5 authentication. • **text**: Clear text authentication.
Step 6	**isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**] **Example:** `Device(config-if)# isis authentication key-chain multistate87723`	Enables MD5 authentication for the specified IS-IS interface.
Step 7	**no isis authentication send-only** **Example:** `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.

Monitor IS-IS configuration

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.

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

Table 2: IS-IS show commands

Command	Purpose
show ip route isis	Displays the current state of the IS-IS IP routing table.
show isis database	Displays the IS-IS link-state database.
show isis routes	Displays the IS-IS Level 1 routing table.
show isis spf-log	Displays a history of the SPF calculations for IS-IS.
show isis topology	Displays a list of all the connected routers in all the areas.
show route-map	Displays all the route maps configured or only the one that is specified.
show clns interface	Displays the CLNS-specific information about each interface.
trace clns *destination*	Traces the paths taken to a specified destination by packets in the network.

Configure IS-IS for IPv6

This section provides configuration information about IS-IS for IPv6.

Configure single-topology IS-IS for IPv6

Configuring IS-IS comprises two activities. You create the IS-IS routing process using protocol-independent IS-IS commands during the first activity, and configure IPv6 IS-IS for operation of the IS-IS protocol on an interface during the second activity.

Before you begin

Before configuring the router to run IPv6 IS-IS, globally enable IPv6 using the **ipv6 unicast-routing** global configuration command.



Note If you are using IS-IS single-topology support for IPv6, IPv4, or both IPv6 and IPv4, you may configure both IPv6 and IPv4 on an IS-IS interface for Level 1, Level 2, or both Level 1 and Level 2. However, if both IPv6 and IPv4 are configured on the same interface, they must be running the same IS-IS level. You cannot configure IPv4 to run on IS-IS Level 1 only on a specified GigabitEthernet or FastEthernet interface while configuring IPv6 to run IS-IS Level 2 only on the same interface.

>

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**net** *network-entity-title* **Example:** `Device(config-router)# net 49.0001.0000.0000.000c.00`	Configures an IS-IS network entity title (NET) for the routing process. • The *network-entity-title* argument defines the area addresses for the IS-IS area and the system ID of the router.
Step 5	**exit** **Example:** `Device(config-router)# exit`	Exits router configuration mode and enters global configuration mode.
Step 6	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/1`	Specifies the interface type and number, and enters interface configuration mode.

	Command or Action	Purpose
Step 7	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8::3/64`	Specifies the IPv6 network assigned to the interface and enables IPv6 processing on the interface. **Note** Refer to the Implementing IPv6 Addressing and Basic Connectivity module for more information on configuring IPv6 addresses.
Step 8	**ipv6 router isis** *area-name* **Example:** `Device(config-if)# ipv6 router isis area2`	Enables the specified IPv6 IS-IS routing process on an interface.

Configure multitopology IS-IS IPv6

Use the **transition** keyword to allow single-topology SPF users to operate while upgrading to multitopology IS-IS. After you configure every router with the **transition** keyword, remove it from each router. When transition mode is not enabled, IPv6 connectivity between routers operating in single-topology mode and routers operating in multitopology mode is not possible.

Continue using your existing IPv6 topology while you upgrade to multitopology IS-IS. Use the optional **isis ipv6 metric** command to differentiate link costs for IPv6 and IPv4 traffic in multitopology mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**metric-style wide** [**transition**] [**level-1** | **level-2** | **level-1-2**] **Example:**	Configures a router running IS-IS to generate and accept only new-style TLVs.

	Command or Action	Purpose
	`Device(config-router)# metric-style wide level-1`	
Step 5	**address-family ipv6** [**unicast** | **multicast**] **Example:** `Device(config-router)# address-family ipv6`	Specifies the IPv6 address family, and enters address family configuration mode. • The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the router is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 6	**multi-topology** [**transition**] **Example:** `Device(config-router-af)# multi-topology`	Enables multitopology IS-IS for IPv6. • The optional **transition** keyword allows an IS-IS IPv6 user to continue to use single-topology mode while upgrading to multitopology mode.

Customize IPv6 IS-IS

To configure IPv6 IS-IS, set a new administrative distance, define the maximum number of equal-cost paths, configure summary prefixes, and advertise the default IPv6 route (::/0). This section explains how to configure the hold-down period between partial route calculations (PRCs) and the frequency of SPF calculations when using multitopology IS-IS.

Customize IS-IS multitopology for IPv6 if needed. Most customers find that the default settings meet their requirements. Refer to the IPv4 configuration guide and the IPv6 command reference for the appropriate syntax if you decide to change the defaults.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:**	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.

	Command or Action	Purpose
	`Device(config)# router isis area2`	
Step 4	**address-family ipv6** [**unicast** | **multicast**] **Example:** `Device(config-router)# address-family ipv6`	Specifies the IPv6 address family, and enters address family configuration mode. • The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the router is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 5	**default-information originate** [**route-map** *map-name*] **Example:** `Device(config-router-af)# default-information originate`	(Optional) Injects a default IPv6 route into an IS-IS routing domain. • The **route-map** keyword and *map-name* argument specify the conditions under which the IPv6 default route is advertised. • If the **route map** keyword is omitted, then the IPv6 default route will be unconditionally advertised at Level 2.
Step 6	**distance** *value* **Example:** `Device(config-router-af)# distance 90`	(Optional) Defines an administrative distance for IPv6 IS-IS routes in the IPv6 routing table. • The *value*argument is an integer from 10 to 254. (The values 0 to 9 are reserved for internal use).
Step 7	**maximum-paths** *number-paths* **Example:** `Device(config-router-af)# maximum-paths 3`	(Optional) Defines the maximum number of equal-cost routes that IPv6 IS-IS can support. • This command also supports IPv6 Border Gateway Protocol (BGP) and Routing Information Protocol (RIP). • The *number-paths* argument is an integer from 1 to 64. The default for BGP is one path; the default for IS-IS and RIP is 16 paths.
Step 8	**summary-prefix** *ipv6-prefix prefix-length* **level-1** | **level-1-2** | **level-2**] **Example:** `Device(config-router-af)# summary-prefix 2001:DB8::/24`	(Optional) Allows a Level 1-2 router to summarize Level 1 prefixes at Level 2, instead of advertising the Level 1 prefixes directly when the router advertises the summary. • The *ipv6-prefix* argument in the **summary-prefix** command must be in the form documented in RFC 2373 where

	Command or Action	Purpose
		the address is specified in hexadecimal using 16-bit values between colons. • The *prefix-length* argument is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
Step 9	**prc-interval** *seconds* [*initial-wait*] [*secondary-wait* **Example:** `Device(config-router-af)# prc-interval 20`	(Optional) Configures the hold-down period between PRCs for multitopology IS-IS for IPv6.
Step 10	**spf-interval** {[**level-1** | **level-2**] | *seconds* [*initial-wait*] [*secondary-wait*]} **Example:** `Device(config-router-af)# spf-interval 30`	(Optional) Configures how often Cisco IOS XE software performs the SPF calculation for multitopology IS-IS for IPv6.
Step 11	**exit** **Example:** `Device(config-router-af)# exit`	Exits address family configuration mode, and returns the router to router configuration mode. • Repeat this step to exit router configuration mode and return the router to global configuration mode.
Step 12	**interface** *type number* **Example:** `Device(config-router)# interface GigabitEthernet 0/0/1`	Specifies the interface type and number, and enters interface configuration mode.
Step 13	**isis ipv6 metric** *metric-value* [**level-1** | **level-2**] **Example:** `Device(config-if)# isis ipv6 metric 20`	(Optional) Configures the value of an multitopology IS-IS for IPv6 metric.

Disable IPv6 protocol-support consistency checks

Perform this task to disable protocol-support consistency checks in IPv6 single-topology mode.

For single-topology IS-IS IPv6, routers must be configured to run the same set of address families. IS-IS checks consistency on hello packets and will reject packets lacking the same configured address families. A router running IS-IS for both IPv4 and IPv6 will not form an adjacency with one running IS-IS for IPv4 only

or IPv6 only. To allow adjacency to form in mismatched address-families network, the **adjacency-check** command in IPv6 address family configuration mode must be disabled.

Note Entering the **no adjacency-check** command may adversely affect your network configuration. Enter the **no adjacency-check** command only when you are running IPv4 IS-IS on all your routers and you want to add IPv6 IS-IS to your network but you need to maintain all your adjacencies during the transition. After completing the IPv6 IS-IS configuration, remove the **no adjacency-check** command.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**address-family ipv6** [**unicast** | **multicast**] **Example:** `Device(config-router)# address-family ipv6`	Specifies the IPv6 address family, and enters address family configuration mode. • The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the router is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 5	**no adjacency-check** **Example:** `Device(config-router-af)# no adjacency-check`	Disables the IPv6 protocol-support consistency checks performed on hello packets, allowing IPv6 to be introduced into an IPv4-only network without disrupting existing adjacencies. • The **adjacency-check** command is enabled by default.

Disable IPv4 subnet consistency checks

To disable IPv4 subnet consistency checking when forming adjacencies, follow this task. The software checks hello packets to verify that the IPv4 address is present and matches the neighbor's subnet. To disable this check, use the **no adjacency-check** command in the router configuration mode. However, if multitopology IS-IS is configured, this check is automatically suppressed, because multitopology IS-IS requires routers to form an adjacency regardless of whether or not all routers on a LAN support a common protocol.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**no adjacency-check** **Example:** `Device(config-router-af)# no adjacency-check`	Disables the IPv6 protocol-support consistency checks performed on hello packets, allowing IPv6 to be introduced into an IPv4-only network without disrupting existing adjacencies. • The **adjacency-check**command is enabled by default.

Verify IPv6 IS-IS configuration

In this example, output information about the parameters and current state of that active IPv6 routing processes is displayed using the **show ipv6 protocols**command:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    GigabitEthernet0/0/3
    GigabitEthernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
```

```
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Address Summarization:
    L2: 2001:DB8:33::/16  advertised with metric 0
    L2: 2001:DB8:44::/16  advertised with metric 20
    L2: 2001:DB8:66::/16  advertised with metric 10
    L2: 2001:DB8:77::/16  advertised with metric 10
```

In this example, output information about all connected routers running IS-IS in all areas is displayed using the **show isis topology**command:

```
Device# show isis topology

IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.000C
0000.0000.000D  20      0000.0000.00AA  Se1/0/1         *HDLC*
0000.0000.000F  10      0000.0000.000F  GE0/0/1         0050.e2e5.d01d
0000.0000.00AA  10      0000.0000.00AA  Se1/0/1         *HDLC*
IS-IS paths to level-2 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.000A  10      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000B  20      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000C  --
0000.0000.000D  30      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000E  30      0000.0000.000A  GE0/0/3         0010.f68d.f063
```

In this example, output information to confirm that the local router has formed all the necessary IS-IS adjacencies with other IS-IS neighbors is displayed using the **show clns is-neighbors**command. To display the IPv6 link-local addresses of the neighbors, specify the **detail** keyword.

```
Device# show clns is-neighbors detail

System Id      Interface   State  Type Priority  Circuit Id         Format
0000.0000.00AA Se1/0/1     Up     L1   0         00                 Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::YYYY:D37C:C854:5
  Uptime: 17:21:38
0000.0000.000F Et0/0/1     Up     L1   64        0000.0000.000C.02  Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::XXXX:E2FF:FEE5:D01D
  Uptime: 17:21:41
0000.0000.000A Et0/0/3     Up     L2   64        0000.0000.000C.01  Phase V
  Area Address(es): 49.000b
  IPv6 Address(es): FE80::ZZZZ:F6FF:FE8D:F063
  Uptime: 17:22:06
```

In this example, detailed output information that displays both end system (ES) and intermediate system (IS) neighbors is displayed using the **show clns neighbors** command with the **detail** keyword.

```
Device# show clns neighbors detail

System Id          Interface    SNPA            State  Holdtime  Type Protocol
0000.0000.0007     GE3/3        aa00.0400.6408  UP     26        L1   IS-IS
Area Address(es): 20
IP Address(es): 172.16.0.42*
Uptime: 00:21:49
0000.0C00.0C35     GE3/2        0000.0c00.0c36  Up     91        L1   IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.42*
Uptime: 00:21:52
```

```
0800.2B16.24EA     GE3/3        aa00.0400.2d05  Up     27         L1   M-ISIS
Area Address(es): 20
IP Address(es): 192.168.0.42*
IPv6 Address(es): FE80::2B0:8EFF:FE31:EC57
Uptime: 00:00:27
0800.2B14.060E     GE3/2        aa00.0400.9205  Up     8          L1   IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.30*
Uptime: 00:21:52
```

In this example, detailed output information about LSPs received from other routers and the IPv6 prefixes they are advertising is displayed using the **show isis database**command with the **detail** keyword specified:

```
Device# show isis database detail

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C   0x5696        325           0/0/0
  Area Address: 47.0004.004D.0001
  Area Address: 39.0001
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.0C35
 --More--
0000.0C00.40AF.00-00* 0x00000009   0x8452        608           1/0/0
  Area Address: 47.0004.004D.0001
  Topology: IPv4 (0x0) IPv6 (0x2)
  NLPID: 0xCC 0x8E
  IP Address: 172.16.21.49
  Metric: 10   IS 0800.2B16.24EA.01
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.40AF
  IPv6 Address: 2001:DB8::/32
  Metric: 10   IPv6 (MT-IPv6) 2001:DB8::/64
  Metric: 5    IS-Extended cisco.03
  Metric: 10   IS-Extended cisco1.03
  Metric: 10    IS (MT-IPv6) cisco.03
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.000A.00-00  0x00000059   0x378A        949               0/0/0
  Area Address: 49.000b
  NLPID:        0x8E
  IPv6 Address: 2001:DB8:1:1:1:1:1:1
  Metric: 10         IPv6 2001:DB8:2:YYYY::/64
  Metric: 10         IPv6 2001:DB8:3:YYYY::/64
  Metric: 10         IPv6 2001:DB8:2:YYYY::/64
  Metric: 10         IS-Extended 0000.0000.000A.01
  Metric: 10         IS-Extended 0000.0000.000B.00
  Metric: 10         IS-Extended 0000.0000.000C.01
  Metric: 0          IPv6 11:1:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:2:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:3:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:4:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:5:YYYY:1:1:1:1:1/128
0000.0000.000A.01-00  0x00000050   0xB0AF        491               0/0/0
  Metric: 0          IS-Extended 0000.0000.000A.00
  Metric: 0          IS-Extended 0000.0000.000B.00
```

This example shows output from the **show isis ipv6 rib** command. An asterisk (*) indicates prefixes that have been installed in the primary IPv6 RIB as IS-IS routes. Following each prefix is a list of all paths in order of preference, with optimal paths listed first and suboptimal paths listed after optimal paths.

```
Device# show isis ipv6 rib

IS-IS IPv6 process "", local RIB
  2001:DB8:88:1::/64
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L2  metric 20 LSP [3/7]
* 2001:DB8:1357:1::/64
    via FE80::202:7DFF:FE1A:9471/GigabitEthernet2/1/0, type L2  metric 10 LSP [4/9]
* 2001:DB8:45A::/64
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L1  metric 20 LSP [C/6]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L1  metric 20 LSP [C/6]
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L2  metric 20 LSP [3/7]
```