IS-IS

This chapter describes the Intermediate System to Intermediate System (IS-IS) routing protocol.

About IS-IS

IS-IS routing protocol is a link state Interior Gateway Protocol (IGP). Link-state protocols are characterized by the propagation of the information required to build a complete network connectivity map on each participating device. That map is then used to calculate the shortest path to destinations. The IS-IS implementation supports IPv4 and IPv6.

You can divide a routing domain into one or more subdomains. Each subdomain is called an area and is assigned an area address. Routing within an area is known as Level-1 routing. Routing between Level-1 areas is known as Level-2 routing. A router is referred to as an Intermediate System (IS). An IS can operate at Level 1, Level 2, or both. ISes that operate at Level 1 exchange routing information with other Level-1 ISes in the same area. ISes that operate at Level 2 exchange routing information with other Level-2 routers regardless of whether they are in the same Level-1 area. The set of Level-2 routers and the links that interconnect them form the Level-2 subdomain, which must not be partitioned in order for routing to work properly.

About NET

An IS is identified by an address known as a Network Entity Title (NET). The NET is the address of a Network Service Access Point (NSAP), which identifies an instance of the IS-IS routing protocol running on an IS. The NET is 8 to 20 octets in length and has the following three parts:

- Area address—This field is 1 to 13 octets in length and is composed of high-order octets of the address.

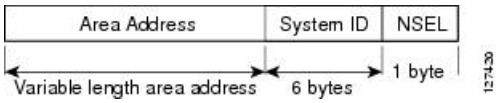
Note You can assign multiple area addresses to an IS-IS instance; in this case, all area addresses are considered synonymous. Multiple synonymous area addresses are useful when merging or splitting areas in the domain. Once the merge or split has been completed, you do not need to assign more than one area address to an IS-IS instance.

- System ID—This field is 6 octets long and immediately follows the area address. When the IS operates at Level 1, the system ID must be unique among all the Level-1 devices in the same area. When the IS operates at Level 2, the system ID must be unique among all devices in the domain.

Note You assign one system ID to an IS instance.

- NSEL—The N-selector field is 1 octet in length and immediately follows the system ID. It must be set to 00.

Figure 1: NET Format



IS-IS Dynamic Hostname

In the IS-IS routing domain, the system ID is used to represent each ASA. The system ID is part of the NET that is configured for each IS-IS ASA. For example, an ASA with a configured NET of 49.0001.0023.0003.000a.00 has a system ID of 0023.0003.000a. ASA-name-to-system-ID mapping is difficult for network administrators to remember during maintenance and troubleshooting on the ASAs.

Entering the **show isis hostname** command displays the entries in the system-ID-to-ASA-name mapping table.

The dynamic hostname mechanism uses link-state protocol (LSP) flooding to distribute the ASA-name-to-system-ID mapping information across the entire network. Every ASA on the network will try to install the system ID-to-ASA name mapping information in its routing table.

If an ASA that has been advertising the dynamic name type, length, value (TLV) on the network suddenly stops the advertisement, the mapping information last received will remain in the dynamic host mapping table for up to one hour, allowing the network administrator to display the entries in the mapping table during a time when the network experiences problems.

IS-IS PDU Types

ISes exchange routing information with their peers using protocol data units (PDUs). Intermediate System-to-Intermediate System Hello PDUs (IIHs), Link-State PDUs (LSPs), and Sequence Number PDUs (SNPs) types of PDUs are used.

IIHs

IIHs are exchanged between IS neighbors on circuits that have the IS-IS protocol enabled. IIHs include the system ID of the sender, the assigned area address(es), and the identity of neighbors on that circuit that are known to the sending IS. Additional optional information can also be included.

There are two types of IIHs:

- Level-1 LAN IIHs—These are sent on multiaccess circuits when the sending IS operates as a Level-1 device on that circuit.
- Level-2 LAN IIHs—These are sent on multiaccess circuits when the sending IS operates as a Level-2 device on that circuit.

LSPs

An IS generates LSPs to advertise its neighbors and the destinations that are directly connected to the IS. An LSP is uniquely identified by the following:

- System ID of the IS that generated the LSP
- Pseudonode ID—This value is always 0 except when the LSP is a pseudonode LSP
- LSP number (0 to 255)
- 32-bit sequence number

Whenever a new version of an LSP is generated, the sequence number is incremented.

Level-1 LSPs are generated by ISs that support Level 1. The Level-1 LSPs are flooded throughout the Level-1 area. The set of Level-1 LSPs generated by all Level-1 ISs in an area is the Level-1 LSP Database (LSPDB). All Level-1 ISs in an area have an identical Level-1 LSPDB and therefore have an identical network connectivity map for the area.

Level-2 LSPs are generated by ISs that support Level 2. Level-2 LSPs are flooded throughout the Level-2 subdomain. The set of Level-2 LSPs generated by all Level-2 ISs in the domain is the Level-2 LSP Database (LSPDB). All Level-2 ISs have an identical Level-2 LSPDB and therefore have an identical connectivity map for the Level-2 subdomain.

SNPs

SNPs contain a summary description of one or more LSPs. There are two types of SNPs for both Level 1 and Level 2:

- Complete Sequence Number PDUs (CSNPs) are used to send a summary of the LSPDB that an IS has for a given level.
- Partial Sequence Number PDUs (PSNPs) are used to send a summary of a subset of the LSPs for a given level that an IS either has in its database or needs to obtain.

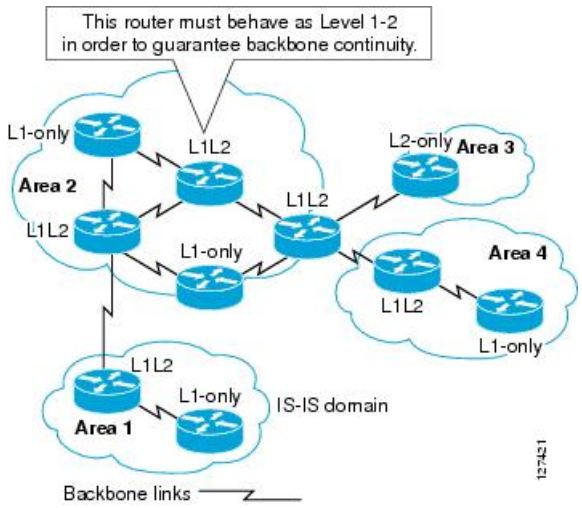
Operation of IS-IS on Multiaccess Circuits

Multiaccess circuits support multiple ISes, that is, two or more operating on the circuit. For multiaccess circuits a necessary prerequisite is the ability to address multiple systems using a multicast or broadcast address. An IS that supports Level 1 on a multiaccess circuit sends Level-1 LAN IIHs on the circuit. An IS that supports Level 2 on a multiaccess circuit sends Level-2 LAN IIHs on the circuit. ISes form separate adjacencies for each level with neighbor ISes on the circuit.

An IS forms a Level-1 adjacency with other ISes that support Level 1 on the circuit and has a matching area address. Two ISes with disjointed sets of area addresses supporting Level 1 on the same multiaccess circuit is NOT supported. An IS forms a Level-2 adjacency with other ISes that support Level 2 on the circuit.

The devices in the IS-IS network topology in the following figure perform Level 1, Level 2, or Level 1 and 2 routing along the backbone of the network.

Figure 2: Level-1, Level-2, Level 1-2 Devices in an IS-IS Network Topology



IS-IS Election of the Designated IS

If each IS advertised all of its adjacencies on a multiaccess circuit in its LSPs, the total number of advertisements required would be N 2 (where N is the number of ISes that operate at a given level on the circuit). To address this scalability issue, IS-IS defines a pseudonode to represent the multiaccess circuit. All ISes that operate on the circuit at a given level elect one of the ISes to act as the Designated Intermediate System (DIS) on that circuit. A DIS is elected for each level that is active on the circuit.

The DIS is responsible for issuing pseudonode LSPs. The pseudonode LSPs include neighbor advertisements for all of the ISes that operate on that circuit. All ISes that operate on the circuit (including the DIS) provide a neighbor advertisement to the pseudonode in their non-pseudonode LSPs and do not advertise any of their neighbors on the multiaccess circuit. In this way the total number of advertisements required varies as a function of N-the number of ISes that operate on the circuit.

A pseudonode LSP is uniquely classified by the following identifiers:

- System ID of the DIS that generated the LSP
- Pseudonode ID (ALWAYS NON-ZERO)
- LSP number (0 to 255)
- 32-bit sequence number

The nonzero pseudonode ID is what differentiates a pseudonode LSP from a non-pseudonode LSP and is chosen by the DIS to be unique among any other LAN circuits for which it is also the DIS at this level.

The DIS is also responsible for sending periodic CSNPs on the circuit. This provides a complete summary description of the current contents of the LSPDB on the DIS. Other ISes on the circuit can then perform the

following activities, which efficiently and reliably synchronizes the LSPDBs of all ISes on a multiaccess circuit:

- Flood LSPs that are absent from or are newer than those that are described in the CSNPs sent by the DIS.
- Request an LSP by sending a PSNP for LSPs that are described in the CSNPs sent by the DIS that are absent from the local database or older than what is described in the CSNP set.

IS-IS LSPDB Synchronization

Proper operation of IS-IS requires a reliable and efficient process to synchronize the LSPDBs on each IS. In IS-IS this process is called the update process. The update process operates independently at each supported level. Locally generated LSPs are always new LSPs. LSPs received from a neighbor on a circuit may be generated by some other IS or may be a copy of an LSP generated by the local IS. Received LSPs can be older, the same age, or newer than the current contents of the local LSPDB.

Handling Newer LSPs

When a newer LSP is added to the local LSPDB, it replaces an older copy of the same LSP in the LSPDB. The newer LSP is marked to be sent on all circuits on which the IS currently has an adjacency in the UP state at the level associated with the newer LSP—excluding the circuit on which the newer LSP was received.

For multiaccess circuits, the IS floods the newer LSP once. The IS examines the set of CNSPs that are sent periodically by the DIS for the multiaccess circuit. If the local LSPDB contains one or more LSPs that are newer than what is described in the CSNP set (this includes LSPs that are absent from the CSNP set), those LSPs are reflooded over the multiaccess circuit. If the local LSPDB contains one or more LSPs that are older than what is described in the CSNP set (this includes LSPs described in the CSNP set that are absent from the local LSPDB), a PSNP is sent on the multiaccess circuit with descriptions of the LSPs that require updating. The DIS for the multiaccess circuit responds by sending the requested LSPs.

Handling Older LSPs

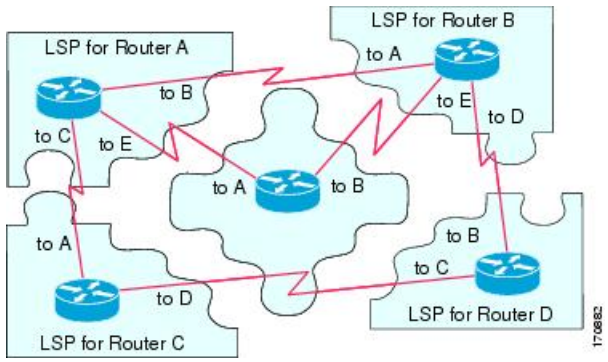
An IS may receive an LSP that is older than the copy in the local LSPDB. An IS may receive an SNP (complete or partial) that describes an LSP that is older than the copy in the local LSPDB. In both cases the IS marks the LSP in the local database to be flooded on the circuit on which the older LSP or SNP that contained the older LSP was received. Actions taken are the same as described above after a new LSP is added to the local database.

Handling Same-Age LSPs

Because of the distributed nature of the update process, it is possible than an IS may receive copies of an LSP that is the same as the current contents of the local LSPDB. In multiaccess circuits receipt of a same-age LSP is ignored. Periodic transmission of a CSNP set by the DIS for that circuit serves as an implicit acknowledgment to the sender that the LSP has been received.

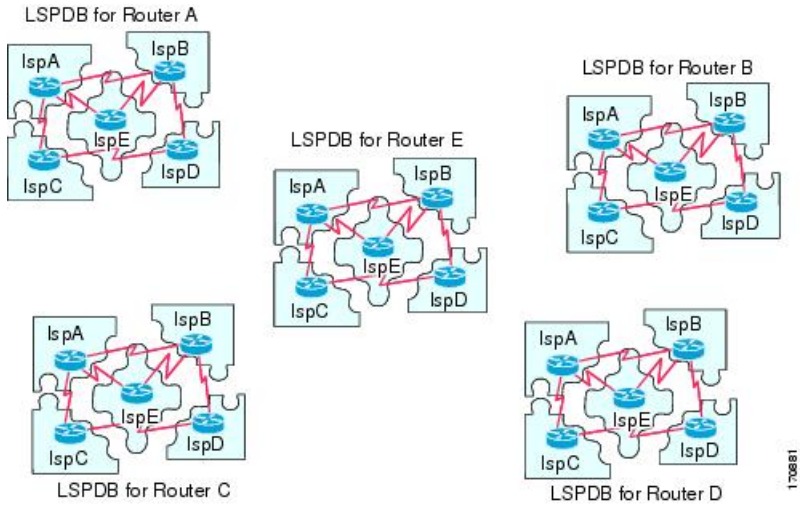
The following figure shows how LSPs are used to create a network map. Think of the network topology as a jigsaw puzzle. Each LSP (representing an IS) is one of the pieces. It is applicable to all Level-1 devices in an area or to all Level-2 devices in a Level-2 subdomain.

Figure 3: IS-IS Network Map



The following figure shows each device in the IS-IS network with its fully updated link-state database after the adjacencies have been formed among the neighbor devices. It is applicable to all Level-1 devices in an area or to all Level-2 devices in a Level-2 subdomain.

Figure 4: IS-IS Devices with Synchronized LSPDBs



IS-IS Shortest Path Calculation

When the contents of the LSPDB change, each IS independently reruns a shortest path calculation. The algorithm is based on the well-known Dijkstra algorithm for finding the shortest paths along a directed graph where the ISes are the vertices of the graph and the links between the ISes are edges with a nonnegative weight. A two-way connectivity check is performed before considering a link between two ISes as part of the graph. This prevents the use of stale information in the LSPDB, for example, when one IS is no longer operating in the network but did not purge the set of LSPs that it generated before stopping operation.

The output of the SPF is a set of tuples (destination, next hop). The destinations are protocol-specific. Multiple equal-cost paths are supported, in which case multiple next hops would be associated with the same destination.

Independent SPFs are performed for each level supported by the IS. When the same destination is reachable by both Level-1 and Level-2 paths, the Level-1 path is preferred.

A Level-2 IS that indicates that it has one or more Level-2 neighbors in other areas may be used by Level-1 devices in the same area as the path of last resort, also called the default route. The Level-2 IS indicates its attachment to other areas by setting an attached bit (ATT) in its Level-1 LSP 0.

Note An IS can generate up to 256 LSPs at each level. The LSPs are identified by the numbers 0 through 255. LSP 0 has special properties, including the significance of the setting of the ATT bit to indicate attachment to other areas. When LSPs that are numbered 1 through 255 have the ATT bit set, it is not significant.

IS-IS Shutdown Protocol

You can shut down IS-IS (placing it in an administrative down state) to make changes to the IS-IS protocol configuration without losing your configuration parameters. You can shut down IS-IS at the global IS-IS process level or at the interface level. If the device was rebooted when the protocol was turned off, the protocol would be expected to come back up in the disabled state. When the protocol is set to the administrative down state, network administrators are allowed to administratively turn off the operation of the IS-IS protocol without losing the protocol configuration, to make a series of changes to the protocol configuration without having the operation of the protocol transition through intermediate-and perhaps undesirable-states, and to then reenable the protocol at a suitable time.

Prerequisites for IS-IS

The following prerequisites are necessary before configuring IS-IS:

- Knowledge of IPv4 and IPv6.
- Knowledge of your network design and how you want traffic to flow through it before configuring IS-IS.
- Define areas, prepare an addressing plan for the devices (including defining the NETs), and determine the interfaces that will run IS-IS.
- Before you configure your devices, prepare a matrix of adjacencies that shows what neighbors should be expected in the adjacencies table. This will facilitate verification.

Guidelines for IS-IS

Firewall Mode Guidelines

Supported only in routed firewall mode. Transparent firewall mode is not supported.

Cluster Guidelines

Supported only in Individual Interface mode; Spanned EtherChannel mode is not supported.

Additional Guidelines

IS-IS is not supported with bidirectional forwarding.

Configure IS-IS

This section describes how to enable and configure the IS-IS process on your system.

Procedure

Step 1 Enable IS-IS Routing Globally, on page 8.
Step 2 Enable IS-IS Authentication, on page 12.
Step 3 Configure IS-IS LSP, on page 15
Step 4 Configure IS-IS Summary Addresses, on page 19.
Step 5 Configure IS-IS Passive Interfaces, on page 20.
Step 6 Configure IS-IS Interfaces, on page 21.
Step 7 Configure IS-IS Interface Hello Padding, on page 25
Step 8 Configure IS-IS IPv4 Address Family, on page 28.
Step 9 Configure IS-IS IPv6 Address Family, on page 32.

Enable IS-IS Routing Globally

IS-IS configuration is done in two parts. First, you configure the IS-IS process in global configuration mode, then specify the NET and the routing level for IS-IS in router configuration mode. There are other general parameters you can configure in router configuration mode that may make more sense for your network than configuring them per interface. This section contains those commands.

Second, you enable IS-IS protocol on individual interfaces in interface configuration mode so that the interface participates in dynamic routing and forms adjacencies with neighboring devices. You must enable routing on one or more interfaces before adjacencies can be established and dynamic routing is possible. See Configure IS-IS Interfaces, on page 21 for the procedures for configuring IS-IS on interfaces.

This procedure describes how to enable IS-IS as an IP routing protocol on the ASA and other general options in router configuration mode.

Before you begin

In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the **changeto context** *name* command.

Procedure

Step 1 Enable IS-IS as a routing protocol on the ASA:

router isis

Example:

```
ciscoasa(config)# router isis
```

```
ciscoasa(config-router)#
```

Step 2 Specify the NET for the routing process:

net *network-entity-title*

Example:

```
ciscoasa(config-router)# net 49.1234.aaaa.bbbb.cccc.00
```

The NET identifies the device for IS-IS. See About NET, on page 1 for more information on the NET.

Step 3 (Optional) Assign the routing level for the IS-IS routing process:

is-type [level-1 | level-2-only | level-1-2]

Example:

```
ciscoasa(config-router)# is-type level-1
```

- (Optional) **level-1**—Indicates intra-area routing. The ASA only learns destinations inside its area.
- (Optional) **level-2-only**—Indicates inter-area routing. The ASA is part of the back bone and does not communicate with Level-1 routers in its own area.
- (Optional) **level-1-2**—The ASA performs both Level 1 and Level 2 routing. This router runs two instances of the routing process. It has one LSDB for destinations inside the area (Level 1 routing) and runs an SPF calculation to discover the area topology. It also has another LSDB with LSPs of all other backbone (Level 2) routers, and runs another SPF calculation to discover the topology of the backbone, and the existence of all other areas.

In conventional IS-IS configurations, the ASA acts as both a Level 1 (intra-area) and a Level 2 (inter-area) router. In multi-area IS-IS configurations, the first instance of the IS-IS routing process configured is by default a Level 1-2 (intra-area and inter-area) router. The remaining instances of the IS-IS process configured by default are Level 1 routers.

Note We highly recommend that you configure the type of IS-IS routing process.

Step 4 Enable IS-IS dynamic hostname capability on the ASA:

hostname dynamic

This command is enabled by default. See IS-IS Dynamic Hostname, on page 2 for detailed information about the dynamic hostname in IS-IS.

Step 5 Configure hello padding for all interfaces on the ASA:

hello padding multi-point

This command is enabled by default. It configures IS-IS hellos to the full MTU size. This allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

You can disable hello padding (**no hello padding multi-point** for all interfaces on a router for the IS-IS routing process) to avoid wasting network bandwidth in case the MTU of both interfaces is the same or in the

case of translational bridging. When hello padding is disabled, the ASA still sends the first five IS-IS hellos padded to the full MTU size to maintain the benefits of discovering MTU mismatches.

Enter the **show clns interface** command in privileged EXEC mode to show that hello padding has been turned off at the router level, See Monitoring IS-IS, on page 37 for more information.

Step 6 (Optional) Enable the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down):

log-adjacency-changes [all]

This command is disabled by default. Logging adjacency changes is useful when monitoring large networks. Messages are in the following form:

Example:

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

all—(Optional) Includes changes generated by non_IIH events.

Step 7 (Optional) Disable the IS-IS protocol so that it cannot form any adjacency on any interface and will clear the LSP database:

protocol shutdown

This command lets you disable the IS-IS protocol for a specific routing instance without removing any existing IS-IS configurations parameters. When you enter this command, the IS-IS protocol continues to run on the router, and you can use the current IS-IS configuration, but IS-IS does not form any adjacencies on any interface, and it also clears the IS-IS LSP database. To disable IS-IS for a specific interface, use the **isis protocol shutdown** command. See Configure IS-IS Interfaces, on page 21 for the procedure.

Step 8 (Optional) Assign a high priority to an IS-IS IP prefix:

route priority high tag *tag-value*

Example:

```
ciscoasa(config-router)# route priority high tag 100
```

tag *tag-value*—Assigns a high priority to IS-IS IP prefixed with a specific route tag. The range is 1 to 4294967295.

Use this command to tag higher priority IS-IS IP prefixes for faster processing and installation in the global routing table, which results in faster convergence. For example, you can help VoIP gateway addresses get processed first to help VoIP traffic get updated faster than other types of packets.

Step 9 (Optional) Globally change the metric value for all IS-IS interfaces:

metric *default-value* **[level-1 | level-2]**

Example:

```
ciscoasa(config-router)# metric 55 level-1
```

- *default-value*—The metric value to be assigned to the link and used to calculate the path cost via the links to destinations. The range is 1 to 63. The default is 10.

- (Optional) **level-1**— Sets Level 1 IPv4 or IPv6 metric.
- (Optional) **level-2**— Sets Level 2 IPv4 or IPv6 metric.

We recommend you use the **metric** command when you need to change the default metric for all IS-IS interfaces. This prevents user errors, such as unintentionally removing a set metric from an interface without configuring a new value and unintentionally allowing the interface to revert to the default metric of 10, thereby becoming a highly preferred interface in the network.

Step 10 (Optional) Configure the ASA to generate and only accept new-style, length, value objects (TLVs):

metric-style narrow | transition | wide [level-1 | level-2 | level-1-2]

Example:

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**—Uses the old style of TLVs with narrow metrics.
- **transition**— Instructs the ASA to accept both old- and new-style TLVs.
- **wide**—Use the new style of TLVs to carry wider metrics.
- (Optional) **level-1**—Enables this command on routing Level 1.
- (Optional) **level-2**—Enables this command on routing Level 2.
- (Optional) **level-1-2**—Enables this command on routing Level 1 and Level 2.

This command causes the ASA to generate and accept only new-style TLVs, which causes the ASA to use less memory and other resources than if it generates both old-style and new-style TLVs.

Step 11 (Optional) Configure the priority of designated ASAs on all interfaces:

priority *number-value*

Example:

```
ciscoasa(config-router)# priority 80
```

number-value—The priority of the ASA. The range is 0 to 127. The default is 64.

Step 12 (Optional) Configure additional manual addresses for an IS-IS area:

max-area-addresses *number*

Example:

```
ciscoasa(config-router)# max-area-addresses 3
```

number—The number of manual addresses to add. The range is 3 to 254. There is no default value.

This command lets you maximize the size of an IS-IS area by configuring additional manual addresses. You specify the number of addresses you want to add and assign a NET address to create each manual address. See About NET, on page 1 for information on the NET.

Step 13 Configure multipath load sharing for IS-IS:

maximum-paths *number-of-paths*

Example:

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths—The number of routes to install in the routing table. The range is 1 to 8. The default is 1.

The **maximum-path** command is used to configure IS-IS multi-load sharing when ECMP is configured in the ASA.

Enable IS-IS Authentication

IS-IS route authentication prevents the introduction of unauthorized or false routing messages from unapproved sources. You can set a password for each IS-IS area or domain to prevent unauthorized routers from injecting false routing information into the link-state database, or you can configure a type of IS-IS authentication, either IS-IS MD5 or enhanced clear text authentication. You can also set authentication per interface. All IS-IS neighbors on interfaces configured for IS-IS message authentication must be configured with the same authentication mode and key for adjacencies to be established.

See About IS-IS, on page 1 for more information on areas and domains.

Before you begin

Before you can enable IS-IS route authentication, you must enable IS-IS and set up an area. See Enable IS-IS Routing Globally, on page 8 for the procedure.

Procedure

Step 1 Enter IS-IS router configuration mode and configure an IS-IS area authentication password:

area-password *password* [**authenticate snp {validate | send-only}**]

Example:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

- *password*—The password you assign.
- (Optional) **authenticate snp**—Causes the system to insert the password into SNPs.
- **validate**—Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
- **send-only**—Causes the system to insert only the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

Using this command on all ASAs in an area prevents unauthorized routers from injecting false routing information in the link-state database. However, this password is exchanged as plain text and thus provides only limited security.

The password is inserted in Level 1 (station router level) PDU LSPs, CSNPs, and PSNPs. If you do not specify the **authenticate snp** keyword with either the **validate** or **send-only** keyword, the IS-IS protocol does not insert the password into SNPs.

Step 2 Enter IS-IS router configuration mode and configure an IS-IS domain authentication password:

domain-password *password* [**authenticate snp {validate | send-only}**]

Example:

```
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

- *password*—The password you assign.
- (Optional) **authenticate snp**—Causes the system to insert the password into sequence number PDUs (SNPs).
- **validate**—Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
- **send-only**—Causes the system to insert only the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

This password is exchanged as plain text and thus provides only limited security.

The password is inserted in Level 2 (area router level) PDU LSPs, CSNPs, and PSNPs. If you do not specify the **authenticate snp** keyword with either the **validate** or **send-only** keyword, the IS-IS protocol does not insert the password into SNPs.

Step 3 Configure the IS-IS instance globally or per interface to have authentication performed only on IS-IS packets being sent (not received):

Router mode:**authentication send-only [level-1 | level-2]**

Example:

```
ciscoasa(config-router)# authentication send-only level-1
```

Interface mode:**isis authentication send-only [level-1 | level-2]**

Example:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis authentication send-only level-1
```

- (Optional) **level-1**—Authentication is performed only on Level 1 packets that are being sent (not received).
- (Optional) **level-2**—Authentication is performed only on Level 2 packets that are being sent (not received).

Use this command before configuring the authentication mode and authentication key chain so that the implementation of authentication goes smoothly. If you do not specify Level 1 or Level 2, send only applies to both levels.

Note ASAs will have more time for the keys to be configured on each ASA if authentication is inserted only on the packets being sent, not checked on packets being received. After all of the ASAs that must communicate are configured with this command, enable the authentication mode and key chain on each ASA.

Step 4 Specify the type of authentication mode used in IS-IS packets for the IS-IS instance globally or per interface:

Router mode:**authentication mode {md5 | text} [level-1 | level-2]**

Example:

```
ciscoasa(config-router)# authentication mode md5 level-1
```

Interface mode:**isis authentication mode {md5 | text} [level-1 | level-2]**

Example:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#  isis authentication mode md5 level-1
```

- **md5**—Enables Message Digest 5 authentication.
- **text**—Uses clear text authentication.
- (Optional) **level-1**—Enables the specified authentication for Level 1 packets only.
- (Optional) **level-2**—Enables the specified authentication for Level 2 packets only.

If you have clear text authentication configured by using the **area-password** or **domain-password**, the isis authentication mode overrides both of those commands. If you configure **isis authentication mode** and then try to configure the **area-password** or **domain-password**, you are not allowed to do so. If you do not specify Level 1 or Level 2, the mode applies to both levels.

Step 5 Enable authentication for IS-IS globally or per interface:

Router mode: **authentication key [0 | 8]** *password* **[level-1 | level-2]**

Example:

```
ciscoasa(config-router)# authentication key 0 site1 level-1
```

Interface mode: **isis authentication key [0 | 8]** *password* **[level-1 | level-2]**

Example:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# router isis
ciscoasa(config-if)# isis authentication key 0 second level-1
```

- **0**—Specifies an unencrypted password will follow.
- **8**—Specifies an encrypted password will follow.
- *password*—Enables authentication and specifies the key.
- (Optional) **level-1**—Enables authentication for Level 1 packets only.

- (Optional) **level-2**—Enables authentication for Level 2 packets only.

If no password is configured with the **key** command, no key authentication is performed. Key authentication can apply to clear text or MD5 authentication. See Step 4 to set the mode. Only one authentication key is applied to IS-IS at one time. If you configure a second key, the first is overridden. If you do not specify Level 1 or Level 2, the password applies to both levels.

Step 6 Configure the authentication password for an interface:

isis password *password* **[level-1 | level-2]**

Example:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis password analyst level-1
```

- *password*—Authentication password you assign to an interface.
- (Optional) **level-1**—Configures the authentication password for Level 1 independently. For Level 1 routing, the ASA acts as a station router only.
- (Optional) **level-2**—Configures the authentication password for Level 2 independently. For level 2 routing, the ASA acts as an area router only.

This command lets you prevent unauthorized routers from forming adjacencies with this ASA and thus protects the network from intruders. The password is exchanged as plain text and thus provides limited security. You can assign different passwords for different routing levels using the **level-1** and **level-2** keywords.

Examples

The following example shows an IS-IS instance with MD5 authentication performed on Level 1 packets and to send any key belonging to the key chain named site1:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

Configure IS-IS LSP

An IS generates LSPs to advertise its neighbors and the destinations that are directly connected to IS-IS. See IS-IS PDU Types, on page 2 for more detailed information on LSPs.

Use the following commands to configure LSPs so that you have a faster convergence configuration.

Before you begin

In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the **changeto context** *name* command.

Procedure

Step 1 Enter router configuration mode:

router isis

Example:

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Step 2 Configure the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs:

ignore-lsp-errors

Example:

```
ciscoas(config-router)# ignore-lsp-errors
```

IS-IS requires that an LSP with an incorrect data link checksum be purged by the receiver, which causes the initiator of the packet to regenerate it. If a network has a link that causes data corruption while still delivering LSPs with correct data link checksums, a continuos cycle of purging and regenerating large numbers of packets can occur, which can render the network nonfunctional. Use this command to ignore the LSPs rather than purge them. The default is enabled.

Step 3 Configure IS-IS to advertise only prefixes that belong to passive interfaces:

advertise passive-only

This command excludes IP prefixes of connected networks from LSP advertisements and thus reduces IS-IS convergence time, because fewer prefixes are advertised in the router non-pseudonode LSP.

Step 4 Configure IS-IS LSPs to be full:

fast-flood *lsp-number*

Example:

```
ciscoasa(config-router)# fast-flood 7
```

(Optional) *lsp-number*—The number of LSPs to be flooded before starting SPF.

This command sends a specified number of LSPs from the ASA. The LSPs invoke SPF before running SPF. Speeding up the LSP flooding process improves overall convergence time. The range is 1 to 15. The default is 5.

Note We recommend that you enable fast flooding of LSPs before the router runs the SPF computation.

Step 5 Configure the MTU size of IS-IS LSPs:

lsp-mtu *bytes*

Example:

```
ciscoasa(config-router)# lsp-mtu 1300
```

bytes—The maximum packet size in bytes. The number of bytes must be less than or equal to the smallest MTU of any link in the network. The range is 128 to 4352.

Step 6 Set the maximum time that LSPs persist in the ASA's database without being refreshed:

max-lsp-lifetime *seconds*

Example:

```
ciscoasa(config-router)# max-lsp-lifetime 2400
```

seconds—The lifetime of the LSP in seconds. The range is 1 to 65,535. The default is 1200.

If the lifetime is exceeded before a refresh LSP arrives, the LSP is dropped from the database.

Step 7 Customize IS-IS throttling of SPF calculations:

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

Example:

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- (Optional) **level-1**—Apply intervals to Level 1 areas only.
- (Optional) **level-2**—Apply intervals to Level 2 areas only.
- *spf-max-wait*— Indicates the maximum interval between two consecutive SPF calculations. The range is 1 to 120 seconds. The default is 10 seconds.
- (Optional) *spf-initial-wait*— Indicates the initial wait time after a topology change before the first SPF calculation. The range is 1 to 120,000 milliseconds. The default is 5500 milliseconds (5.5 seconds).

  Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the SPF maximum wait interval specified.
- (Optional) *spf-second-wait*—Indicates the interval between the first and second SPF calculation. The range is 1 to 120,000 milliseconds. The default is 5500 milliseconds (5.5 seconds).

SPF calculations are performed only when the topology changes. This command controls how often the software performs the SPF calculation.

Note The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often this is done, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the ASA, but potentially slows down the rate of convergence.

Step 8 Customize IS-IS throttling of LSP generation:

lsp-gen-interval [level-1 | level-2] *lsp-max-wait [lsp-intial-wait lsp-second wait]*

Example:

```
ciscoasa(config-router)#  lsp-gen-interval level-1 2 50 100
```

- (Optional) **level-1**—Apply intervals to Level 1 areas only.
- (Optional) **level-2**—Apply intervals to Level 2 areas only.
- *lsp-max-wait*— Indicates the maximum interval between two consecutive occurrences of an LSP being generated. The range is 1 to 120 seconds. The default is 5 seconds.
- (Optional) *lsp-initial-wait*— Indicates the initial wait time before generating the first LSP. The range is 1 to 120,000 milliseconds. The default is 50 milliseconds.

  Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the LSP maximum wait interval specified.
- (Optional) *lsp-second-wait*—Indicates the interval between the first and second LSP generation. The range is 1 to 120,000 milliseconds. The default is 5000 milliseconds (5 seconds).

  This command controls the delay between LSPs being generated.

Step 9 Set the LSP refresh interval:

lsp-refresh-interval *seconds*

Example:

```
ciscoasa(config-router)# lsp-refresh-interval 1080
```

(Optional) *seconds*— The interval at which LSPs are refreshed. The range is 1 to 65535 seconds. The default value is 900 seconds (15 minutes).

The refresh interval determines the rate at which the software periodically transmits in LSPs the route topology information that it originates. This is done to keep the database information from becoming too old.

Note LSPs must be periodically refreshed before their lifetimes expire. The value set for the **lsp-refresh-interval** command should be less than the value set for the **max-lsp-lifetime** command; otherwise, LSPs will time out before they are refreshed. If you set the LSP lifetime too low compared to the LSP refresh interval, the software reduces the LSP refresh interval to prevent the LSPs from timing out.

Step 10 Customize IS-IS throttling of PRCs:

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

Example:

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait*— Indicates the maximum interval between two consecutive PRC calculations. The range is 1 to 120 seconds. The default is 5 seconds.
- (Optional) *prc-initial-wait*— Indicates the initial PRC wait time after a topology change. The range is 1 to 120,000 milliseconds. The default is 2000 milliseconds.

  Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the PRC maximum wait interval specified.

- (Optional) *prc-second-wait*—Indicates the interval between the first and second PRC calculation. The range is 1 to 120,000 milliseconds. The default is 5000 milliseconds (5 seconds).

  PRC is the software process of calculating routes without performing an SPF calculation. This is possible when the topology of the routing system itself has not changed, but a change is detected in the information announced by a particular IS or when it is necessary to attempt to reinstall such routes in the RIB.

Step 11 Configure which routes are suppressed when the PDU becomes full:

lsp-full suppress {external [interlevel] | interlevel [external] | none}

Example:

```
ciscoasa(config-router)# lsp-full suppress interlevel external
```

- **external**—Suppresses any redistributed routes on this ASA.
- **interlevel**—Suppresses any routes coming from the other level. For example, if the Level 2 LSP becomes full, routes from Level 1 are suppressed.
- **none**—Suppresses no routes.

In networks where there is no limit placed on the number of redistributed routes into IS-IS (that is, the **redistribute maximum-prefix** command is not configured), it is possible that the LSP will fill up and routes are dropped. Use the **lsp-full suppress** command to define in advance which routes are suppressed if the LSP gets full.

Configure IS-IS Summary Addresses

Multiple groups of addresses can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This helps to reduce the size of the routing table.

You need to manually define summary addresses if you want to create summary addresses that do not occur at a network number boundary or if you want to use summary addresses on an ASA with automatic route summarization disabled.

Procedure

Step 1 Enter router configuration mode:

router isis

Example:

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Step 2 Create aggregate addresses for IS-IS:

summary-address *address mask* **[level-1 | level-1-2 | level-2] tag** *tag-number* **metric** *metric-value*

Example:

```
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

- *address*—Summary address designated for a range of IP addresses.
- *mask*—IP subnet mask used for the summary route.
- (Optional) **level-1**—Only routes redistributed into Level 1 are summarized with the configured address and mask value.
- (Optional) **level-1-2**—Summary routes are applied when redistributing routes into Level 1 and Level 2 and when Level 2 IS-IS advertises Level 1 routes as reachable in its area.
- (Optional) **level-2**—Routes learned by Level 1 routing are summarized into the Level 2 backbone with the configured address and mask value. Redistributed routes into Level 2 IS-IS are summarized also.
- (Optional) **tag** *tag-number*—Specifies the number used to tag the summary route. The range is 1 to 4294967295.
- (Optional) **metric** *metric-value* —Specifies the metric value applied to the summary route. The **metric** keyword is assigned to the link and used to calculate the path cost via the links to destinations. You can configure this metric for Level 1 or Level 2 routing only. The range is 1 to 4294967295. The default value is 10.

Enter the **show clns interface** command to verify metric values for interfaces, See Monitoring IS-IS, on page 37 for more information.

Configure IS-IS Passive Interfaces

You can disable IS-IS hello packets and routing updates on interfaces while still including the interface addresses in the topology database. These interfaces will not form IS-IS neighbor adjacencies

If you have an interface that you do not want to participate in IS-IS routing, but that is attached to a network that you want advertised, configure the passive interfaces (using the **passive-interface** command) to prevent that interface from using IS-IS. Additionally, you can specify the version of IS-IS that is used by the ASA for updates. Passive routing assists in controlling the advertisement of IS-IS routing information and disables the sending and receiving of IS-IS routing updates on an interface.

Procedure

Step 1 Enter router configuration mode:

router isis

Example:

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Step 2 Configure a passive interface on the ASA:

passive-interface *interface-name*

Example:

```
ciscoasa(config-router)# passive-interface inside
```

- **default**—Suppress routing updates on all interfaces.
- **management**—Suppress updates on Management 0/1 interface.
- **management2**—Suppress updates on Management 0/2 interface.
- **inside**—Suppress updates on the inside interface.

This command configures interfaces NOT to form IS-IS neighbor adjacencies yet to include the interface addresses in the IS-IS database.

Step 3 Configure the ASA to advertise passive interfaces:

advertise passive-only

Example:

```
ciscoasa(config-router)# advertise passive-only
```

This command configures IS-IS to advertise only prefixes that belong to passive interfaces. It excludes IP prefixes of connected networks from LSP advertisements, which reduces IS-IS convergence time.

Configure IS-IS Interfaces

This procedure describes how to modify individual ASA interfaces for IS-IS routing. You can modify the following:

- General settings such as enabling IS-IS, enabling IS-IS shutdown protocol, priorities, tags, and adjacency filters on an interface.
- Authentication key and mode—See Enable IS-IS Authentication, on page 12 for the procedures for configuring authentication on interfaces.
- Hello padding values—See Configure IS-IS Interface Hello Padding, on page 25 for the procedures for configuring hello padding on interfaces.
- LSP settings
- The interface delay metric used in IS-IS metric calculations.

Before you begin

Before the IS-IS routing process is useful, you must assign a NET and some interfaces must have IS-IS enabled. You can configure only one process to perform Level 2 (inter-area) routing. 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 intra-area (Level 1) routing at the same time. An interface cannot be part of more than one

area, except in the case where the associated routing process is performing both Level 1 and Level 2 routing. See Enable IS-IS Routing Globally, on page 8 for the procedure.

Procedure

Step 1 Enter interface configuration mode:

interface *interface_id*

Example:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

Step 2 Filter the establishment of IS-IS adjacencies:

isis adjacency-filter *name* **[match-all]**

Example:

```
ciscoasa(config-if)# isis adjacency-filter ourfriends match-all
```

- *name*—The name of the filter set or expression to apply.
- (Optional) **match-all**—All NSAP addresses must match the filter to accept the adjacency. If not specified (the default), only one address needs to match the filter for the adjacency to be accepted.

Filtering is performed by building NSAP addresses out of incoming IS-IS hello packets by combining each area address in the hello with the system ID. Each of these NSAP addresses is then passed through the filter. If any one NSAP matches, the filter is considered passed, unless the **match-all** keyword is specified, in which case all addresses must pass. The functionality of the **match-all** keyword is useful in performing negative tests, such as accepting an adjacency only if a particular address is not present.

Step 3 Advertise IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface:

isis advertise prefix

Example:

```
ciscoasa(config-if)# isis advertise prefix
```

By default, this command is enabled. Thus, the connected routes are distributed even though they are not intended to get distributed. To stop unnecessary redistribution of connected routes and to improve IS-IS convergence time, use the **no isis advertise prefix** command. This excludes IP prefixes of connected network from LSP advertisements and reduces IS-IS convergence time.

Note Configuring the **no** form of this command per IS-IS interface is a small-scale solution to reduce IS-IS convergence time because fewer prefixes are advertised in the router non-pseudonode LSP. An alternative to the **isis advertise prefix** command is the **advertise passive-only** command, which is a scalable solution because it is configured per IS-IS instance.

Step 4 Enable IPv6 on an IS-IS interface:

ipv6 router isis

Example:

```
ciscoasa(config-if)# ipv6 router isis
```

Step 5 Configure the time-delay between successive IS-IS LSP transmissions per interface:

isis lsp-interval *milliseconds*

Example:

```
ciscoasa(config-if)# isis lsp-interval 100
```

milliseconds—The time delay between successive LSPs. The range is 1 to 4294967298. The default is 33 milliseconds.

In topologies with a large number of IS-IS neighbors and interfaces, an ASA may have difficulty with the CPU load imposed by LSP transmission and reception. This command reduces the LSP transmission rate (and by implication the reception rate of other systems).

Step 6 Configure the value of an IS-IS metric:

isis metric {*metric-value* | **maximum**} [**level-1 | level-2**]

Example:

```
ciscoasa(config-if)# isis metric 15 level-1
```

- *metric-value*—Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 1 to 63. The default value is 10.
- **maximum**—Excludes a link or adjacency from the SPF calculation.
- (Optional) **level-1**—Specifies that this metric should be used only in the SPF calculation for Level 1 (intra-area) routing. If no optional keyword is specified, the metric is enabled on routing Level 1 and Level 2.
- (Optional) **level-2**—Specifies that this metric should be used only in the SPF calculation for Level 2 (inter-area) routing. If no optional keyword is specified, the metric is enabled on routing Level 1 and Level 2.

Step 7 Configure the priority of designated ASAs on the interface:

isis priority *number-value* **[level-1 | level-2]**

Example:

```
ciscoasa(config-if)# isis priority 80 level-1
```

- *number-value*—Sets the priority of an ASA. The range is 0 to 127. The default is 64.
- (Optional) **level-1**—Sets the priority for Level 1 independently.
- (Optional) **level-2**—Sets the priority for Level 2 independently.

The priority is used to determine which ASA on a LAN will be the designated router or DIS. The priorities are advertised in the hello packets. The ASA with the highest priority becomes the DIS.

Note In IS-IS there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it takes over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.

Step 8 Disable IS-IS protocol so that it cannot form adjacencies on a specified interface and place the IP address of the interface into the LSP that is generated by the ASA:

isis protocol shutdown

Example:

```
ciscoasa(config-if)# isis protocol shutdown
```

This command lets you disable the IS-IS protocol for a specified interface without removing the configuration parameters. The IS-IS protocol does not form any adjacencies for the interface for which this command has been configured, and the IP address of the interface is put into the LSP that is generated by the router. Use the **protocol shutdown** command if you do not want IS-IS to form any adjacency on any interface and to clear the IS-IS LSP database. See Enable IS-IS Routing Globally, on page 8 for the procedure.

Step 9 Configure the amount of time between retransmission of each IS-IS LSP:

isis retransmit-interval *seconds*

Example:

```
ciscoasa(config-if)#  isis retransmit-interval 60
```

(Optional) *seconds*— Time between retransmission of each LSP. The number should be greater than the expected round-trip delay between any two routers on the attached network. The range is 0 to 65535. The default is 5 seconds.

Make sure the *seconds* argument is conservative, otherwise needless retransmission results. This command has no effect on LAN (multi-point) interfaces.

Step 10 Configure the amount of time between retransmissions of each IS-IS LSP:

isis retransmit-throttle-interval *milliseconds*

Example:

```
ciscoasa(config-if)#  isis retransmit-throttle-interval 300
```

(Optional) *milliseconds*— Minimum delay between LSP retransmissions on the interface. The range is 0 to 65535.

This command can be useful in very large networks with many LSPs and many interfaces as a way of controlling LSP retransmission traffic. This command controls the rate at which LSPs can be resent on the interface.

This command is distinct from the rate at which LSPs are sent on the interface (controlled by the **isis lsp-interval** command) and the period between retransmissions of a single LSP (controlled by the **isis retransmit-interval** command). You can use these commands in combination to control the offered load of routing traffic from one ASA to its neighbors.

Step 11 Set a tag on the IP address configured for an interface when the IP prefix is put into an IS-IS LSP:

isis tag *tag-number*

Example:

```
ciscoasa(config-if)# isis tag 100
```

tag-number—The number that serves as a tag on an IS-IS route. The range is 1 to 4294967295.

No action occurs on a tagged route until the tag is used, for example, to redistribute routes or summarize routes. Configuring this command triggers the ASA to generate new LSPs because the tag is a new piece of information in the packet.

Examples

In this example, two interfaces are tagged with different tag values. By default, these two IP addresses would have been put into the IS-IS Level 1 and Level 2 database. However, if you use the **redistribute** command with a route map to match tag 110, only IP address 172.16. 0.0 is put into the Level 2 database.

```
ciscoasa (config)# interface GigabitEthernet1/0
ciscoasa (config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 120
ciscoasa (config)# interface GigabitEthernet1/1
ciscoasa (config-if)# ip address 172.16.0.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 110
ciscoasa (config-router)# route-map match-tag permit 10
ciscoasa (config-router)# match tag 110
ciscoasa (config)# router isis
ciscoasa (config-router)# net 49.0001.0001.0001.0001.00
ciscoasa (config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
```

Configure IS-IS Interface Hello Padding

Hello packets are responsible for discovering and maintaining neighbors. You can configure the following hello padding parameters at the interface level. See Enable IS-IS Routing Globally, on page 8 to enable/disable hello padding for the whole IS-IS.

Procedure

Step 1 Enter interface configuration mode:

interface *interface_id*

Example:

```
ciscoasa(config)# interface GigabitEthernet0/0
```

```
ciscoasa(config-if)# isis
```

Step 2 Enter interface configuration mode to configure padding on IS-IS hello protocol data units (IIH PDUs) for all interfaces on the ASA:

isis hello padding

Example:

```
ciscoasa(config-if)# isis hello padding
```

Hellos are padded to the full MTU, which allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces. IS-IS hello padding is enabled by default.

Note You can disable hello padding to avoid wasting network bandwidth in case the MTU of both interfaces is the same or in case of translational bridging. While hello padding is disabled, the ASAs still send the first five IS-IS hellos padded to the full MTU size to maintain the benefits of discovering MTU mismatches.

Step 3 Specify the length of time between consecutive hello packets sent by IS-IS:

isis hello-interval {*seconds* | **minimal**} **[level-1 | level-2]**

Example:

```
ciscoasa(config-if)# isis hello-interval 5 level-1
```

- *seconds*—The length of time between hello packets. By default, a value three times the hello interval seconds is advertised as the hold time in the hello packets sent. You can change the multiplier of 3 by configuring the **isis hello-multiplier** command. With smaller hello intervals, topological changes are detected faster, but there is more routing traffic. The range is 0 to 65535. The default is 10.
- **minimal**—Causes the system to compute the hello interval based on the hello multiplier (specified by the **isis hello-multiplier** command) so that the resulting hold time is 1 second.
- (Optional) **level-1**—Configures the hello interval for Level 1 independently. Use this on X.25, Switched Multimegabit Data Service (SMDS), and Frame Relay multi-access networks.
- (Optional) **level-2**—Configures the hello interval for Level 2 independently. Use this on X.25, SMDS, and Frame Relay multi-access networks.

Note Although a slower hello interval saves bandwidth and CPU usage, there are some situations when a faster hello interval is preferred, for example, a large configuration that uses Traffic Engineering (TE) tunnels. If the TE tunnel uses IS-IS as the Interior Gateway Protocol (IGP), and the IP routing process is restarted at the router at the ingress point of the network (head-end), then all the TE tunnels get resignaled with the default hello interval. A faster hello interval prevents this resignaling. To configure a faster hello interval, you need to increase the IS-IS hello interval manually using the **isis hello-multiplier** command.

Step 4 Specify the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down:

isis hello-multiplier *multiplier* **[level-1 | level-2]**

Example:

```
ciscoasa(config-if)# isis hello-multiplier 10 level-1
```

- *multipler*—The advertised hold time in IS-IS hello packets is set to the hello multiplier times the hello interval. Neighbors declare an adjacency to this ASA down after not having received any IS-IS hello packets during the advertised hold time. You can set the hold time (and thus the hello multiplier and the hello interval) on a per-interface basis, and it can be different between different routers in one area. The range is 3 to 1000. The default is 3.
- (Optional) **level-1**—Configures the hello multiplier independently for Level 1 adjacencies.
- (Optional) **level-2**—Configures the hello multiplier independently for Level 2 adjacencies.

Use this command in circumstances where hello packets are lost frequently and IS-IS adjacencies are failing unnecessarily.

Note Using a smaller hello multiplier will give fast convergence, but can result in more routing instability. Change the hello multiplier to a larger value to help network stability when needed. Never configure a hello multiplier lower than the default value of 3.

Step 5 Configure the type of adjacency used for the IS-IS:

isis circuit-type [level-1 | level-1-2 | level-2-only]

Example:

```
ciscoasa(config-if)# isis circuit-type level-2-only
```

- (Optional) **level-1**— Configures an ASA for Level 1 adjacency only.
- (Optional) **level-1-2**—Configures an ASA for Level 1 and Level 2 adjacency.
- (Optional) **level-2**—Configures an ASA for Level 2 adjacency only.

You do not normally need to configure this command. The correct way is to configure the level on an ASA. See Enable IS-IS Routing Globally, on page 8 for the procedure. You should configure some interfaces as Level 2 only on ASAs that are between areas (Level 1-2 routers). This saves bandwidth by sending out unused Level 1 hello packets.

Step 6 Configure the interval at which periodic CSNP packets are sent on broadcast interfaces:

isis csnp-interval *seconds* **[level-1 | level-1-2 | level-2]**

Example:

```
ciscoasa(config-if)#  isis csnp-interval 30 level-1
```

- *seconds*— Interval of time between transmission of CSNPs on multi-access networks. This interval only applies for the designated ASA. The range is 0 to 65,535. The default is 10 seconds.
- (Optional) **level-1**—Configures the interval of time between transmission of CSNPs for Level 1 independently.

- (Optional) **level-2**—Configures the interval of time between transmission of CSNPs for Level 2 independently.

It is unlikely that you will need to change the default value for this command.

This command applies only for the DR for a specified interface. Only DRs send CSNP packets to maintain database synchronization. You can configure the CSNP interval independently for Level 1 and Level 2.

Configure IS-IS IPv4 Address Family

Routers are allowed to redistribute external prefixes or routes that are learned form any other routing protocol, static configuration, or connected interface. The redistributed routes are allowed in either a Level 1 router or a Level 2 router.

You can set up adjacency, Shortest Path First (SPF), and you can define conditions for redistributing routes from another routing domain into ISIS (redistribution) for IPv4 addresses.

Before you begin

Before you can enable IS-IS route authentication, you must enable IS-IS and set up an area. See Enable IS-IS Routing Globally, on page 8 for the procedure.

Procedure

Step 1 Enter router configuration mode to configure an IPv4 address familiy:

router isis

Example:

```
ciscoasa(config)# router isis
cisco(config-router)#
```

Step 2 Perform an adjacency check to check for IS-IS protocol support:

adjacency-check

Example:

```
cisco(config-router)# adjacency-check
```

Step 3 Define the administrative distance assigned to routes discovered by the IS-IS protocol:

distance *weight*

weight—Administrative distance assigned to IS-IS routes. The range is 1 to 255. The default is 115.

Example:

```
ciscoasa(config-router)# distance 20
```

This command configures the distances applied to IS-IS routes when they are inserted in the RIB and influence the likelihood of these routes being preferred over routes to the same destination addresses discovered by other protocols.

Note In general, the higher the value of the administrative distance, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored. Weight values are subjective; no quantitative method exists for choosing weight values.

Step 4 Configure multi-path load sharing for IS-IS:

maximum-paths *number-of-paths*

Example:

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths—Number of routes to install in the routing table. The range is 1 to 8. The default is 1.

The **maximum-path** command is used to configure IS-IS multi-load sharing when ECMP is configured in the ASA.

Step 5 Generate a default route into an IS-IS routing domain:

default-information originate [**route-map** *map-name*]

Example:

```
ciscoasa(config-router)# default-information originate route-map RMAP
```

(Optional) **route-map** *map-name*—The routing process generates the default route if the route map is satisfied.

If an ASA configured with this command has a route to 0.0.0.0 in the routing table, IS-IS will originate an advertisement for 0.0.0.0 in its LSPs. Without a route map, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the ATT in Level 1 LSPs. With a **match ip address** *standard-access-list* command, you can specify one or more IP routes that must exist before the ASA will advertise 0/0.

Step 6 Set the IS-IS metric globally for Level 1 and Level 2:

metric *default-value* **[level-1 | level-2]**

Example:

```
ciscoasa(config-router)# metric 55 level-1
ciscoasa(config-router)# metric 45 level-2
```

- *default-value*—The metric value to be assigned to the link and used to calculate the path cost via the links to destinations. The range is 1 to 63. The default is 10.
- (Optional) **level-1**— Sets Level 1 IPv4 or IPv6 metric.
- (Optional) **level-2**— Sets Level 2 IPv4 or IPv6 metric.

Step 7 Specify the metric style and which levels to apply it to:

metric-style [narrow | transition | wide] [level-1 | level-2 | level-1-2]

Example:

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**—Instructs the ASA to use the old style of TLVs with the narrow metric.
- **transition**— Instructs the ASA to accept both old- and new-style TLVs during transition.
- **wide**—Instructs the ASA to use the new style of TLVs to carry the wider metric.
- (Optional) **level-1**— Sets Level 1 IPv4 or IPv6 metric.
- (Optional) **level-2**— Sets Level 2 IPv4 or IPv6 metric.
- (Optional) **level-1-2**—Sets Level 1 and Level 2 IPv4 or IPv6 metric.

Step 8 Specify constraints for when a Level 1-Level 2 router should set its attached bit:

set-attached-bit route-map *map-tag*

Example:

```
ciscoasa(config-router)# set-attached-bit route-map check-for-L2_backbone_connectivity
```

route-map *map-tag*—Identifier of a configured route map. If the specified route map is matched, the router continues to set its attached bit. This command is disabled by default.

In the current IS-IS implementation, as specified in ISO 10589, Level 1-Level 2 routers set their Level 1 LSP attached bit when they see other areas in their own domain or see other domains. However, in some network topologies, adjacent Level 1-Level 2 routers in different areas may lose connectivity to the Level 2 backbone. Level 1 routers may then send traffic destined outside of the area or domain to Level 1-Level 2 routers that may not have such connectivity.

This command allows more control over the attached bit setting for Level 1-Level 2 routers. The route map can specify one or more CLNS routes. If at least one of the match address route map clauses matches a route in the Level 2 CLNS routing table, and if all other requirements for setting the attached bit are met, the Level 1-Level 2 router continues to set the attached bit in its Level 1 LSP. If the requirements are not met or no match address route map clauses match a route in the Level 2 CLNS routing table, the attached bit is not set.

Step 9 Configure the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations:

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

Example:

```
ciscoasa(config-router)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- (Optional) **on-startup**—Sets the overload bit at system startup. The overload bit remains set for the number of seconds configured or until BGP has converged, depending on the subsequent argument or keyword specified.
- (Optional) *seconds*—The number of seconds the overload bit is set at system startup and remains set. The range is 5 to 86400.
- (Optional) **wait-for-bgp**—When the **on-startup** keyword is configured, causes the overload bit to be set at system startup and remain set until BGP has converged.

- (Optional) **suppress**—Causes the type of prefix identified by the subsequent keyword or keywords to be suppressed.
- (Optional) **interlevel**—When the **suppress** keyword is configured, prevents the IP prefixes learned from another IS-IS level from being advertised.
- (Optional) **external**—When the **suppress** keyword is configured, prevents the IP prefixes learned from other protocols being advertised.

This command forces the ASA to set the overload bit (also known as the hippity bit) in its non-pseudonode LSPs. Normally, the setting of the overload bit is allowed only when an ASA runs into problems. For example, when an ASA is experiencing a memory shortage, it might be that the link-state database is not complete, which results in an incomplete or inaccurate routing table. By setting the overload bit in its LSPs, other routers can ignore the unreliable router in their SPF calculations until the router has recovered from its problems. The result is that no paths through this router are seen by other routes in the IS-IS area. However, IP and CLNS prefixes are directly connected to this router.

Step 10 Customize IS-IS throttling of PRCs:

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

Example:

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait*— Indicates the maximum interval between two consecutive PRC calculations. The range is 1 to 120 seconds. The default is 5 seconds.
- (Optional) *prc-initial-wait*— Indicates the initial PRC wait time after a topology change. The range is 1 to 120,000 milliseconds. The default is 2000 milliseconds.

  Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the PRC maximum wait interval specified.
- (Optional) *prc-second-wait*—Indicates the interval between the first and second PRC calculation. The range is 1 to 120,000 milliseconds. The default is 5000 milliseconds (5 seconds).

  PRC is the software process of calculating routes without performing an SPF calculation. This is possible when the topology of the routing system itself has not changed, but a change is detected in the information announced by a particular IS or when it is necessary to attempt to reinstall such routes in the RIB.

Step 11 Customize IS-IS throttling of SPF calculations:

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

Example:

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- (Optional) **level-1**—Apply intervals to Level 1 areas only.
- (Optional) **level-2**—Apply intervals to Level 2 areas only.
- *spf-max-wait*—Indicates the maximum interval between two consecutive SPF calculations. The range is 1 to 120 seconds. The default is 10 seconds.

- (Optional) *spf-initial-wait*—Indicates the initial wait time after a topology change before the first SPF calculation. The range is 1 to 120,000 milliseconds. The default is 5500 milliseconds (5.5 seconds).

  Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the SPF maximum wait interval specified.

- (Optional) *spf-second-wait*—Indicates the interval between the first and second SPF calculation. The range is 1 to 120,000 milliseconds. The default is 5500 milliseconds (5.5 seconds).

SPF calculations are performed only when the topology changes. This command controls how often the software performs the SPF calculation.

Note The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often this is done, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the ASA, but potentially slows down the rate of convergence.

Step 12 Configure IS-IS to honor external metrics during SFP calculations:

use external-metrics

Step 13 Configure a BGP, connected, IS-IS, OSPF, or Static route redistribution:

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

Example:

```
ciscoasa(config-router)# redistribute static level-1 metric-type internal metric 6
```

metric *number*—Value for metric. The range is 1 to 4294967295.

Attached Bit Configuration

In the following example, the attached-bit will stay set when the router matches 49.00aa in the L2 CLNS routing table:

```
ciscoasa(config)# router isis
 ciscoasa(config-router)# clns filter-set L2_backbone_connectivity permit 49.00aa
 ciscoasa(config-router)# route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# match clns address L2_backbone_connectivity
ciscoasa(config)# router isis
 ciscoasa(config-router)#set-attached-bit route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# end
 ciscoasa# show clns route 49.00aa

Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
 via tr2, Serial0
   isis, route metric is 30, route version is 58
```

Configure IS-IS IPv6 Address Family

You can set up adjacency, SPF, and you can define conditions for redistributing routes from another routing domain into IS-IS (redistribution) for IPv6 addresses.

Before you begin

Before you can enable IS-IS route authentication, you must enable IS-IS and set up an area. See Enable IS-IS Routing Globally, on page 8 for the procedure.

Procedure

Step 1 Enter router configuration mode:

router isis

Example:

```
cisco(config-router)#
```

Step 2 Specify the metric style as wide:

metric-style wide [transition] [level-1 | level-2 | level-1-2]

Example:

```
ciscoas(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

- (Optional) **transition**— Instructs the router to accept both old- and new-style TLVs.
- (Optional) **level-1**— Sets Level 1 IPv4 or IPv6 metric.
- (Optional) **level-2**— Sets Level 2 IPv4 or IPv6 metric.
- (Optional) **level-1-2**—Sets Level 1 and Level 2 IPv4 or IPv6 metric.

We recommend you use the **metric** command when you need to change the default metric for all IS-IS interfaces. this prevents user errors, such as unintentionally removing a set metric from an interface without configuring a new value and unintentionally allowing the interface to revert to the default metric of 10, thereby becoming a highly preferred interface in the network.

Step 3 Enter address family configuration mode to configure IS-IS routing sessions that use standard IPv4 or IPv6 address prefixes:

address-family ipv6 [unicast]

Example:

```
ciscoasa(config-router)# address-family ipv6 unicast
cisco(config-router-af)#
```

Step 4 Perform an adjacency check to check for IS-IS protocol support:

adjacency-check

Example:

```
cisco(config-router-af)# adjacency-check
```

Step 5 Configure multi-path load sharing for IS-IS:

maximum-paths *number-of-paths*

Example:

```
ciscoasa(config-router-af)# maximum-paths 8
```

number-of-paths—The number of routes to install in the routing table. The range is 1 to 8. The default is 1.

The **maximum-path** command is used to configure IS-IS multi-load sharing when ECMP is configured in the ASA.

Step 6 Define the administrative distance assigned to routes discovered by the IS-IS protocol:

distance *weight*

weight—The administrative distance assigned to IS-IS routes. The range is 1 to 255. The default is 115.

Example:

```
ciscoasa(config-router-af)# distance 20
```

This command configures the distances applied to IS-IS routes when they are inserted in the RIB and influence the likelihood of these routes being preferred over routes to the same destination addresses discovered by other protocols.

Note In general, the higher the value of the administrative distance, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored. Weight values are subjective; no quantitative method exists for choosing weight values.

Step 7 Generate a default route into an IS-IS routing domain:

default-information originate [**route-map** *map-name*]

Example:

```
ciscoasa(config-router-af)# default-information originate route-map TEST7
```

(Optional) **route-map** *map-name*—The routing process generates the default route if the route map is satisfied.

If an ASA configured with this command has a route to 0.0.0.0 in the routing table, IS-IS will originate an advertisement for 0.0.0.0 in its LSPs. Without a route map, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the ATT in Level 1 LSPs. With a **match ip address** *standard-access-list* command, you can specify one or more IP routes that must exist before the ASA will advertise 0/0.

Step 8 Configure the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations:

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

Example:

```
ciscoasa(config-router-af)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- (Optional) **on-startup**—Sets the overload bit at system startup. The overload bit remains set for the number of seconds configured or until BGP has converged, depending on the subsequent argument or keyword specified.
- (Optional) *seconds*—The number of seconds the overload bit is set at system startup and remains set. The range is 5 to 86400.
- (Optional) **wait-for-bgp**—When the **on-startup** keyword is configured, causes the overload bit to be set at system startup and remain set until BGP has converged.
- (Optional) **suppress**—Causes the type of prefix identified by the subsequent keyword or keywords to be suppressed.
- (Optional) **interlevel**—When the **suppress** keyword is configured, prevents the IP prefixes learned from another IS-IS level from being advertised.
- (Optional) **external**—When the **suppress** keyword is configured, prevents the IP prefixes learned from other protocols being advertised.

This command forces the ASA to set the overload bit (also known as the hippity bit) in its non-pseudonode LSPs. Normally, the setting of the overload bit is allowed only when an ASA runs into problems. For example, when an ASA is experiencing a memory shortage, it might be that the link-state database is not complete, which results in an incomplete or inaccurate routing table. By setting the overload bit in its LSPs, other routers can ignore the unreliable router in their SPF calculations until the router has recovered from its problems. The result is that no paths through this router are seen by other routes in the IS-IS area. However, IP and CLNS prefixes are directly connected to this router.

Step 9 Customize IS-IS throttling of PRCs:

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

Example:

```
ciscoasa(config-router-af)#  prc-interval 5 10 20
```

- *prc-max-wait*— Indicates the maximum interval between two consecutive PRC calculations. The range is 1 to 120 seconds. The default is 5 seconds.
- (Optional) *prc-initial-wait*— Indicates the initial PRC wait time after a topology change. The range is 1 to 120,000 milliseconds. The default is 2000 milliseconds.

  Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the PRC maximum wait interval specified.
- (Optional) *prc-second-wait*—Indicates the interval between the first and second PRC calculation. The range is 1 to 120,000 milliseconds. The default is 5000 milliseconds (5 seconds).

  PRC is the software process of calculating routes without performing an SPF calculation. This is possible when the topology of the routing system itself has not changed, but a change is detected in the information announced by a particular IS or when it is necessary to attempt to reinstall such routes in the RIB.

Step 10 Customize IS-IS throttling of SPF calculations:

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

Example:

```
ciscoasa(config-router-af)#  spf-interval level-1 5 10 20
```

- (Optional) **level-1**—Apply intervals to Level 1 areas only.
- (Optional) **level-2**—Apply intervals to Level 2 areas only.
- *spf-max-wait*—Indicates the maximum interval between two consecutive SPF calculations. The range is 1 to 120 seconds. The default is 10 seconds.
- (Optional) *spf-initial-wait*—Indicates the initial wait time after a topology change before the first SPF calculation. The range is 1 to 120,000 milliseconds. The default is 5500 milliseconds (5.5 seconds).

  Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the SPF maximum wait interval specified.
- (Optional) *spf-second-wait*—Indicates the interval between the first and second SPF calculation. The range is 1 to 120,000 milliseconds. The default is 5500 milliseconds (5.5 seconds).

SPF calculations are performed only when the topology changes. This command controls how often the software performs the SPF calculation.

Note The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often this is done, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the ASA, but potentially slows down the rate of convergence.

Step 11 Configure a BGP, connected, IS-IS, OSPF, or Static route redistribution:

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

Example:

```
ciscoasa(config-router-af)# redistribute static level-1 metric-type internal metric 6
```

metric *number*—The value for metric. The range is 1 to 4294967295.

Step 12 Redistribute IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1:

redistribute isis {level-1 | level-2} into {level-2 | level-1} [[distribute-list *list-number* | **[route-map** *map-tag***]]**

Example:

```
ciscoasa(config-router-af)# redistribute isis level-1 into level-2
distribute-list 100
```

- **level-1 | level-2**—The level from which and to which you are redistributing IS-IS routes.
- **into**—The keyword that separates the level of routes being redistributed from the level into which you are redistributing routes.
- (Optional) **distribute-list** *list-number*—The number of a distribute list that controls the IS-IS redistribution. You can specify either a distribute list or a route map, but not both.
- (Optional) **route-map** *map-tag*—The name of a route map that controls the IS-IS redistribution. You can specify either a distribute list or a route map, but not both.

Note You must specify the **metric-style wide** command for the **redistribute isis** command to work. See Step 1 of this procedure.

In IS-IS, all areas are stub areas, which means that no routing information is leaked from the backbone (Level 2) into areas (Level 1). Level 1-only routers use default routing to the closest Level 1-Level 2 router in their area. This command lets you redistribute Level 2 IP routes into Level 1 areas. This redistribution enables Level 1-only routers to pick the best path for an IP prefix to get out of the area. This is an IP-only feature, CLNS routing is still stub routing.

Note For more control and stability you can configure a distribute list or route map to control which Level 2 IP routes can be redistributed into Level 1. This allows large IS-IS-IP networks to use area for better scalability.

Step 13 Create aggregate prefixes for IS-IS IPv6 routes:

summary-prefix *ipv6-prefix* **[level-1 | level-1-2 | level-2]**

Example:

```
cisco(config-router-af)# summary-prefix 2001::/96 level-1
```

- *ipv6 address*—The IPv6 prefix in the form X.X.X.X.::X/0-128.
- (Optional) **level-1**—Only routes redistributed into Level 1 are summarized with the configured address and mask value.
- (Optional) **level-1-2**—Summary routes are applied when redistributing routes into Level 1 and Leve2 IS-IS and when Level 2 IS-IS advertises Level 1 routes as reachable in it area.
- (Optional) **level-2**—Routes learned by Level 1 routing are summarized into the Level 2 backbone with the configured address and mask value. Redistributed routes into Level 2 IS-IS are summarized also.

Monitoring IS-IS

You can use the following commands to monitor the IS-IS routing process. For examples and descriptions of the command output, see the command reference.

Monitoring the IS-IS Database

Use the following commands to monitor the IS-IS database:

- **show isis database [level-1 | l1] [level-2 | l2] [detail]** —Displays the IS-IS link-state database for Level 1, Level 2, and the detailed contents of each LSP.
- **show isis database verbose** —Displays more information about the IS-IS database, such as sequence number, checksum, and holdtime for LSPs.

Monitoring IS-IS Mapping Table Entries

Use the following command to monitor IS-IS hostnames:

show isis hostname—Displays the router-name-to-system-ID mapping table entries for an IS-IS router.

Monitoring IS-IS IPv4

Use the following commands to monitor IS-IS IPv4:

- **show isis ip rib**—Displays the IPv4 address family-specific RIB for an IS-IS routing process.
- **show isis ip spf-log**—Displays the IPv4 address family-specific SPF logs for an IS-IS routing process.
- **show isis ip topology**—Displays the IPv4 address family-specific topology for an IS-IS routing process.
- **show isis ip redistribution** [**level-1** | **level-2**] [*network-prefix*]—Displays IS-IS learned and installed IPv6 routes.
- **show isis ip unicast**—Displays the IPv4 address family-specific RIB, SPF logs, and paths to ISes.

Monitoring IS-IS IPv6

Use the following commands to monitor IS-IS IPV6:

- **show isis ipv6 rib**—Displays the IPv6 address family-specific RIB for an IS-IS routing process.
- **show isis ipv6 spf-log**—Displays the IPv6 address family-specific SPF logs for an IS-IS routing process.
- **show isis ipv6 topology**—Displays the IPv6 address family-specific topology for an IS-IS routing process.
- **show isis ipv6 redistribution** [**level-1** | **level-2**] [*network-prefix*]—Displays IS-IS learned and installed IPv6 routes.
- **show isis ipv6 unicast**—Displays the IPv6 address family-specific RIB, SPF logs, and paths to ISes.

Monitoring IS-IS Logs

Use the following commands to monitor IS-IS logs:

- **show isis lsp-log**—Displays the Level 1 and Level 2 IS-IS LSP log of the interfaces that triggered the new LSP.
- **show isis spf-log**—Displays how often and why the ASA has run an SPF calculation.

Monitoring IS-IS Protocol

Use the following command to monitor IS-IS protocol:

show clns protocol —Displays the protocol information for each IS-IS routing process on the ASA.

Monitoring IS-IS Neighbors and Routes

Use the following commands to monitor IS-IS neighbors:

- **show isis topology** —Displays a list of all connected routers in all areas. This command verifies the presence and connectivity between all routers in all areas.
- **show isis neighbors [detail]** —Displays IS-IS adjacency information.

- **show clns neighbors** [*process-tag*] [*interface-name*] [**detail**]—Displays end system (ES), intermediate system (IS) and multi-topology IS-IS (M-ISIS) neighbors. This command displays the adjacency learned through multitopology IS-IS for IPv6.
- **show clns is-neighbors** *[interface-name]* **[detail]** —Displays IS-IS information for IS-IS device adjacencies.

Monitoring IS-IS RIB

Use the following commands to monitor IS-IS RIB:

- **show isis rib** [*ip-address* | *ip-address-mask*]—Displays paths for a specific route or for all routes under a major network that are stored in the RIB.
- **show isis rib redistribution** [**level-1** | **level-2**] [*network-prefix*]—Displays the prefixes in the local redistribution cache.
- **show route isis** Displays the current state of the routing table.

Monitoring IS-IS Traffic

Use the following command to monitor IS-IS traffic:

show clns traffic [since {bootup | show}] —Displays the CLNS traffic statistics that the ASA has seen.

Debugging IS-IS

Use the following commands to debug IS-IS:

debug isis [adj-packets | authentication | checksum-errors | ip | ipv6 | local-updates | [rptpcp;-errors | rob | snp-packets | spf-events | spf-statistics | spf-triggers | update-packets]—Debugs various aspects of the IS-IS routing protocol.

History for IS-IS

Table 1: Feature History for IS-IS

Feature Name	Platform Releases	Feature Information
IS-IS routing	9.6(1)	The ASA now supports the Intermediate System to Intermediate System (IS-IS) routing protocol. Support was added for routing data, performing authentication, and redistributing and monitoring routing information using the IS-IS routing protocol. We introduced the following commands: **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, router isis, set-attached-bit, set-overload-bit, show clns, show isis, show route isis, spf-interval, summary-address**.

Examples for IS-IS

This section describes configuration examples with topology for different aspects of IS-IS.

IS-IS Routing Configuration

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   isis
```

IS-IS IPv6 Routing Configuration

```
router isis
```

```
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   ipv6 address 2001:192:16:32::1/64
   ipv6 router isis
```

Dynamic Routing Within the Same Area

```
iRouter --------(inside G0/1) ASA (G0/0 outside)------------ oRouter

ASA Configuration
  interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   ipv6 address 2001:192:16:32::1/64
   isis
   ipv6 router isis

  interface GigabitEthernet0/1
   nameif inside
   security-level 100
   ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
   ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
   isis
   ipv6 router isis

  router isis
   net 49.1234.2005.2005.2005.00
   is-type level-1
   metric-style wide

  interface GigabitEthernet0/0
   ip address 172.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:16:32::3/64
   ipv6 router isis
   isis priority 120

  interface GigabitEthernet0/1
   ip address 172.26.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:26:32::3/64
   ipv6 router isis

IOS Configuration
  iRouter
  router isis
   net 49.1234.2035.2035.2035.00
   is-type level-1
   metric-style wide

  oRouter
  interface GigabitEthernet0/0
   ip address 192.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:192:16:32::3/64
   ipv6 router isis

  oRouter
  interface GigabitEthernet0/1
   ip address 192.26.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:192:26:32::3/64
```

```
   ipv6 router isis

  oRouter
  router isis
   net 49.1234.2036.2036.2036.00
   is-type level-1
   metric-style wide
```

Dynamic Routing in More Than One Area

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis

 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis

 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 5
  exit-address-family
 !

IOS Configuration
 iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120


 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
  metric-style wide
```

```
 oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide

oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

Dynamic Routing in Overlapping Areas

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis

interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
```

```
 ipv6 router isis

router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis priority 120
 isis ipv6 metric 600


interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
 metric-style wide
 maximum-paths 6
!
 address-family ipv6
 summary-prefix 2001::/8 tag 301
 summary-prefix 6001::/16 level-1-2 tag 800
 redistribute static metric 800 level-1-2
exit-address-family


oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip pim sparse-dense-mode
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis
 isis tag 301


oRouter
router isis
 net 49.1234.2036.2036.2036.00
```

```
 is-type level-1
 metric-style wide

ASA Configuration
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family
!
```

Route Redistribution

```
iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis


 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 6
 exit-address-family
!

IOS Configuration
iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120


 iRouter
```

```
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
  metric-style wide

oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

Summary Address

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
```

```
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 redistribute static
 maximum-paths 5
address-family ipv6 unicast
 maximum-paths 6
exit-address-family
```

Passive Interfaces

```
 iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0
  ipv6 address 2001:192:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0
  ipv6 address 2001:172:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/2
  nameif dmz
  security-level 0
  ip address 40.40.50.1 255.255.255.0
  ipv6 address 2040:95::1/64


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  passive-interface default

IOS Configuration
 iRouter
  interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120

 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis
```

```
 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
  metric-style wide

 oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis

 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis

 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

Authentication

```
ASA ------------ Router

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
 ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
 ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
 metric-style wide
 authentication mode md5
 authentication key cisco#123 level-2

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
```

```
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis authentication mode md5
 isis authentication key-chain KeyChain level-2
 isis priority 120
 isis ipv6 metric 600


iRouter
key chain KeyChain
 key 1
  key-string cisco#123


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
```