Chapter 6

Configuring IS-IS

This chapter describes how to configure Intermediate System–to–Intermediate System (IS-IS) routing on your E-series router; it contains the following sections:

Overview

IS-IS is a dynamic routing protocol developed by the International Organization for Standardization (ISO) and commonly referred to as ISO 10589. IS-IS was originally developed at Digital Equipment Corporation for Phase V DECnet. The motivation to standardize IS-IS, however, was through the efforts of the American National Standards Institute (ANSI) X3S3.3 Network and Transport Layers Committee.

Similar to the Open Shortest Path First (OSPF) routing protocol, IS-IS is a link-state protocol. It builds a complete and consistent picture of a network's topology by sharing link-state information across all network Intermediate System (IS) devices.

The IS-IS routing protocol provides routing for pure Open Systems Interconnection (OSI) environments. IS-IS as implemented on the E-series router supports IP networks and enables you to configure IS-IS as an IP routing protocol only. In IS-IS, networks are partitioned into routing domains, which are further divided into areas. A two-level hierarchical routing design is used. With this model, routing is referred to as level 1, level 2, or both level 1 and level 2.

IS-IS Terms

OSI internetworking has its own terminology. A number of terms used in IS-IS routing discussions are defined in Table 13.

Table 13: IS-IS Terms

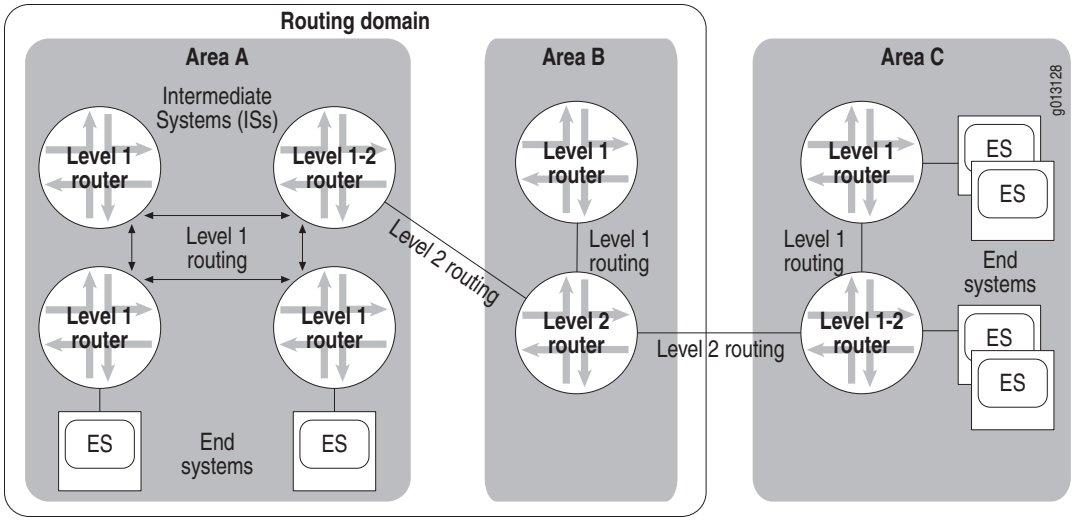
Term	Meaning
area	A group of contiguous networks and their attached hosts. Area boundaries are normally assigned by a network administrator.
complete sequence number PDU (CSNP)	PDU sent by designated router to ensure database synchronization
Connectionless Network Protocol (CLNP)	An OSI network layer protocol used by CLNS to handle data at the transport layer; the OSI equivalent of IP
Connectionless Network Service Protocol (CLNS)	An OSI network layer service that enables data transmission without establishing a circuit and that routes messages independently of any other messages.
end system (ES)	Any nonrouting network node or host
intermediate system (IS)	A router
level 1 routing	■ Routing *within* an area ■ Level 1 routers (or intermediate systems) track all the individual links, routers, and end systems within a level 1 area. ■ Level 1 routers do not know the identity of routers or destinations outside their area. ■ A level 1 router forwards all traffic for destinations outside its area to the nearest level 2 router within its area.

Table 13: IS-IS Terms (continued)

Term	Meaning
level 2 routing	■ Routing *between* areas ■ Level 2 routers know the level 2 topology and know which addresses are reachable via each level 2 router. ■ Level 2 routers track the location of each level 1 area. ■ Level 2 routers are not concerned with the topology within any level 1 area (for example, the details internal to each level 1 area). ■ Level 2 routers can identify when a level 2 router is also a level 1 router within the same area. ■ Only a level 2 router can exchange packets with external routers located outside its routing domain.
link-state PDU (LSP)	PDU broadcast by link-state protocols that contains information about neighbors and path costs; used to maintain routing tables; also known as link-state advertisement
network entity title (NET)	ISO network addresses used by CLNS networks; an identifier of a network entity in an end system or intermediate system. A NET consists of an area address (routing domain), system identifier, and selector.
network service access point (NSAP)	Hierarchical network address that specifies the point at which network services are made available to a transport layer entity in the OSI reference model. A valid NSAP address is unique and unambiguously identifies a single system.
partial sequence number PDU (PSNP)	PDU sent by designated router to acknowledge and request link-state information
protocol data unit (PDU)	OSI term equivalent to packet, containing protocol control information and, possibly, user data. This chapter uses the term packet interchangeably with PDU.
route tag	A numeric value assigned to the IP addresses on an IS-IS route before the route is propagated to other routers in an IS-IS domain. You can use this tag to control IS-IS route redistribution, route leaking, or route summarization by referencing it in a route map.
routing domain	A collection of connected areas that provide full connectivity to all end systems located within them. A routing domain is partitioned into areas.
system identifier	Uniquely identifies a system within an area
table map	A mechanism for applying a route map to an IS-IS route as a way to filter and manipulate route attributes before the route is added to the routing table.

Figure 18 illustrates some of the terms described in Table 13.

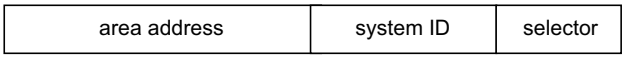
Figure 18: Overview of IS-IS Topology



ISO Network Layer Addresses

ISO network layer addresses are flexible enough to make routing feasible in a worldwide Internet. Network layer addresses in ISO and IP are hierarchical and clearly identify level 1 and level 2 areas. These addresses can be up to 20 octets long; any packet that contains an address has one additional octet to specify the length of the address.

An ISO address—also known as the NSAP address—is broken into three parts: the area address, the system identifier (ID), and the NSAP selector.



The area address defines the routing domain and the area within the routing domain. The length of the ID field can be from 1 to 8 octets and uses a single fixed length for any one routing domain. The selector field is always 1 octet long. Usually, all end systems within the same area have the same area address. Some areas can have multiple addresses. The NSAP address is defined by the network entity title (NET) during configuration.

Level 1 Routing

A level 1 router looks at a packet's area address and compares it with a destination address. If the area portion of the destination address matches its own area's address, the level 1 router uses the ID portion of the address to route the packet. If the area portion of the address does not match, the level 1 router routes the packet to a level 2 router within its area.

Level 2 Routing

Level 2 routers do not look at an area's internal structure, but simply route toward an area based on the area address. It is common for a level 2 router to also be a level 1 router in a particular area; these routers are sometimes referred to as level 1-2 routers. See Figure 18.

Dynamic Hostname Resolution

The system identifier of the NSAP address identifies a node in a network. System operators often find symbolic hostnames to be easier to use and remember than the system identifier. However, a static mapping of hostname to system identifier requires every router to maintain a table of the mappings; each table must contain the hostnames and system identifiers of every router in the network. The static mapping must be managed by router operators, and every change or addition of a mapping requires all the tables to be updated. Consequently, the static tables are likely to become rapidly outdated.

The router supports dynamic resolution of hostnames to system identifiers. You can use the **clns host** command to map the hostname to the NSAP address, and therefore to the system ID. This mapping is inserted in the dynamic hostname type-length-value tuple (TLV type 137), and subsequently advertised when LSPs are transmitted. The value field contains the hostname, preferably the fully qualified domain name (FQDN) of the host, or a subset of the FQDN. You can display the TLV by issuing the **show isis database detail** command.

Authentication

The router supports two authentication methods for IS-IS: simple authentication and hash function–based message authentication code (HMAC) MD5 authentication. These authentication methods prevent unauthorized routers from injecting false routing information into your network or forming adjacencies with your router.

By default, IS-IS authentication is disabled on the router until you enable it with the commands described in the following sections.

Simple Authentication

Simple authentication uses a text password (authentication key) that can be entered in encrypted or unencrypted form. The receiving router uses this authentication key to verify the packet.

You can configure the password for simple authentication by using the following commands:

- The **area-authentication-key** command assigns a password used by neighboring routers to authenticate IS-IS level 1 link-state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs). This command also enables simple authentication of level 1 LSPs.
- The **domain-authentication-key** command assigns a password used by neighboring routers to authenticate IS-IS level 2 LSPs, CSNPs, and PSNPs. This command also enables simple authentication of level 2 LSPs.

- The **isis authentication-key** command assigns a password associated with a specific interface for authentication of IS-IS level 1 or level 2 hello packets. This command also enables simple authentication of level 1 or level 2 hello packets.

These commands enable simple authentication of LSPs and (for the **isis authentication-key** command) hello packets only; they do not enable authentication of CSNP and PSNP packets. To enable authentication of CSNPs or PSNPs, you must issue either the **area-authentication** command or the **domain-authentication** command. For information, see *Enabling and Disabling Authentication of CSNPs and PSNPs* on page 317.

NOTE: The router supports simple authentication for compatibility with existing IS-IS implementations. However, we recommend that you do *not* use the simple authentication method because it is insecure (the text can be "sniffed").

HMAC MD5 Authentication

When you enable IS-IS HMAC MD5 authentication (also referred to as MD5 authentication), the router creates secure digests of the packets, encrypted according to the HMAC MD5 message-digest algorithms. The digests are inserted into the packets from which they are created. Depending on the commands you issue, the digests can be inserted into hello packets, link-state PDUs, complete sequence number PDUs, and partial sequence number PDUs.

You can configure an HMAC MD5 authentication key by using the following commands:

- The **area-message-digest-key** command specifies an HMAC MD5 key that the router uses to create a message digest of each level 1 packet—LSPs, CSNPs, and PSNPs—transmitted by area routers. Using MD5 authentication for area routers protects against unauthorized routers injecting false routing information into the area portions of your network. This command also enables MD5 authentication of level 1 LSPs.

- The **domain-message-digest-key** command specifies an HMAC MD5 key that the router uses to create a message digest of each level 2 packet—LSPs, CSNPs, and PSNPs—transmitted by domain routers. Using MD5 authentication for domain routers protects against unauthorized routers injecting false routing information into the routing domain portions of your network. This command also enables MD5 authentication of level 2 LSPs.

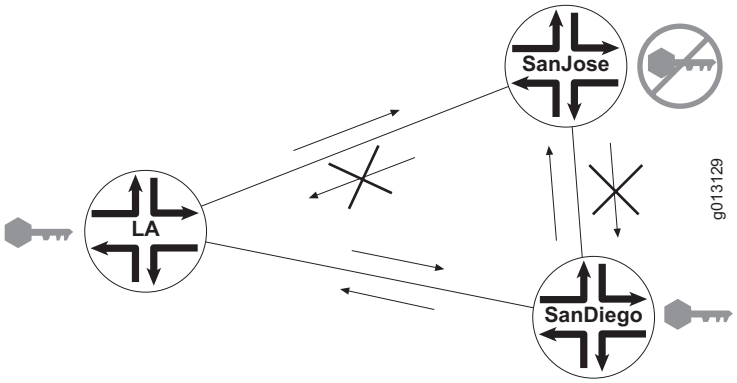
- The **isis message-digest-key** command specifies an HMAC MD5 key that the router uses to create a message digest of level 1 or level 2 hello packets on the interface. Level 1 packets are the default. Using MD5 authentication on interfaces protects against intrusion by preventing unauthorized routers from forming adjacencies with your router. This command also enables MD5 authentication of level 1 or level 2 hello packets.

These commands enable MD5 authentication of LSPs and (for the **isis message-digest-key** command) hello packets only; they do not enable authentication of CSNP and PSNP packets. To enable authentication of CSNPs or PSNPs, you must issue either the **area-authentication** command or the **domain-authentication** command. For information, see *Enabling and Disabling Authentication of CSNPs and PSNPs* on page 317.

MD5 Authentication Example

In the example shown in Figure 19, authentication is configured on router LA and router SanDiego, but not on router SanJose. Router LA and router SanDiego accept packets from each other because they contain message digests generated by an accepted key. Router SanJose accepts packets from router LA and router SanDiego, and simply ignores the message digest included in their packets. Router LA and router SanDiego reject packets from router SanJose because those packets do not include a message digest.

Figure 19: Packet Flow Between Routers With and Without Authentication Set



Specifying MD5 Start and Stop Timing

With each of the MD5 commands, you can specify when the router will start and stop *accepting* packets that include a digest made with this key. You can also specify when the router will start and stop *generating* packets that include a digest made with this key. If you specify a time for any of these actions, you can further specify the day, month, and year. The default times are as follows:

- Start accepting keys (startAcceptTime)—Current time
- Stop accepting keys (stopAcceptTime)—Never
- Start generating keys (startGenTime)—Current time plus 2 minutes
- Stop generating keys (stopGenTime)—Never

If you specify times, you must follow these guidelines to achieve appropriate timing between the actions:

- startAcceptTime must be less than startGenTime.
- stopGenTime must be less than stopAcceptTime.
- When a new key replaces an old one, the startGenTime time for the new key must be less than or equal to the stopGenTime time of the old key.

For example, suppose you configure authentication on router A and router B. If the startGenTime for router A is earlier than the startAcceptTime for router B, router B does not accept packets from router A until the current time matches its startAcceptTime.

The router accepts any packet authenticated with a key you have defined if the packet is received within the period defined for the key by its startAcceptTime and stopAcceptTime. If more than one key has been defined for that period, the router determines which key to use by comparing the startGenTime with the current time. When the startGenTime of a key matches the current time, the router starts using this key to transmit packets and stops using the previous key.

Example

The following commands configure both key 1 and key 2 to be accepted between 08:00:00 and 23:00:00. When the current time reaches 09:00:00, the router begins using key 1 to transmit packets. When the current time reaches 10:00:00, the router begins using key 2 to transmit packets; key 1 is no longer used. Key 2 will continue to be used until a new key is configured and the new key's startGenTime matches the current time on the router.

```
host1(config-router)#area-message-digest-key 1 hmac-md5 mr942s7n
start-accept 08:00:00 start-generate 9:00:00 stop-accept 23:00:00
stop-generate 22:59:59

host1(config-router)#area-message-digest-key 2 hmac-md5 dsb38h5f
start-accept 08:00:00 start-generate 10:00:00 stop-accept 23:00:00
stop-generate 22:59:59
```

Halting MD5 Authentication

To prevent key expiration from causing your network to revert to an unauthenticated condition, you cannot halt MD5 authentication by using the timers. When the stopGenTime time for a key is reached, the router does not stop generating the key if it was the last key issued. You must delete all keys to halt authentication. Use the **no** version of the command to delete a key.

Managing and Replacing MD5 Keys

A key has an infinite lifetime if you do not specify stopGenTime and stopAcceptTime. (As noted previously, if the last key expires, the router continues to generate that key.) Many system operators choose to change their keys on a regular basis, such as every month. If you determine that a key is no longer secure, configure a new key immediately. We recommend the following practice for configuring new keys:

1. Configure the new key on all routers in the IS-IS network.
2. Verify that the new key is working.
3. Delete the old key from every router.

Each key has an associated key-ID that you specify. The key-ID is sent with the message digest, so that the receiving routers know which key was used to generate the digest. You also use the key-ID to delete a key.

Enabling and Disabling Authentication of CSNPs and PSNPs

When the E-series router interoperates with other vendors' routers in the same network, you might want to enable or disable (suppress) authentication for some PDU types but not for others. For example, some vendors' routing software might not authenticate any PDUs, whereas other vendors' routing software might authenticate CSNPs and PSNPs separately from LSPs.

To facilitate interoperability with other vendors' routers, the E-series router allows you to enable and disable authentication of CSNPs and PSNPs separately from authentication of LSPs by using the following commands:

- The **area-authentication { csnp | psnp }** command enables or disables simple authentication or HMAC MD5 authentication of IS-IS level 1 CSNP packets or PSNP packets. By default, authentication of CSNPs and PSNPs is disabled.
- The **domain-authentication { csnp | psnp }** command enables or disables simple authentication or HMAC MD5 authentication of IS-IS level 2 CSNP packets or PSNP packets. By default, authentication of CSNPs and PSNPs is disabled.

When you suppress authentication of CSNPs, the router does not authenticate CSNP packets that it receives from neighboring routers, nor does it include authentication information in CSNP packets that it sends to other routers. Similarly, when you suppress authentication of PSNPs, the router neither authenticates PSNP packets that it receives nor sends authentication information in PSNP packets that it transmits.

Extensions for Traffic Engineering

The router supports *new-style* TLV tuples described in the Internet draft, *IS-IS Extensions for Traffic Engineering*. The router ID TLV (TLV type 134) contains the ID of the router that originates the LSP, providing a stable address that can always be referenced regardless of the state of node interfaces.

The extended IP reachability TLV (type 135) carries IP prefixes and is similar to the IP reachability TLVs (types 128 and 130). The extended IS reachability TLV (type 22) contains information about a series of IS neighbors and is similar to the IS neighbor TLV (type 2).

The older TLVs—2, 128, 130—each have a narrow metric field, providing for metric values ranging only from 0–63. The new TLVs—22 and 135—have a new data structure that includes a wide metric field of 3 bytes (extended IS reachability; configurable) or four bytes (extended IP reachability; calculated). Both new TLVs provide for the use of sub-TLVs to carry more information about IS neighbors; however, only the extended IS reachability TLV currently has defined sub-TLVs, such as IPv4 interface and neighbor addresses.

Use the **metric-style** commands to configure what style the router generates and accepts. The following behaviors are supported:

- Generates and accepts only old-style metrics
- Generates only old-style metrics, but accepts old style and new style
- Generates and accepts both old-style and new-style metrics (this option consumes the most system resources)
- Generates only new-style metrics, but accepts old style and new style
- Generates and accepts only new-style metrics

Refer to the Internet draft, *IS-IS Extensions for Traffic Engineering*, for more information about these extensions.

Integrated IS-IS

The E-series router supports the Integrated IS-IS version of IS-IS. Integrated IS-IS provides a single routing algorithm to route both TCP/IP and OSI Connectionless Network Protocol (CLNP) packets. This design adds IP-specific information to the OSI IS-IS routing protocol. It supports IP subnetting, variable subnet masks, type of service (ToS), and external routing.

Integrated IS-IS allows for the mixing of routing domains; that is, IP-only routers, OSI-only routers, and dual (IP and OSI) routers. OSI and IP packets are forwarded directly over the link-layer services without needing mutual encapsulation. The E-series router supports IS-IS only for the routing and forwarding of TCP/IP packets. Forwarding of OSI packets is not supported.

Equal-Cost Multipath

IS-IS supports equal-cost multipath (ECMP) and installs into the routing table multiple entries for paths to the same destination. Each of these multiple paths to a given destination must have the same cost as the others, but a different next hop.

Static PPP Interfaces

When IS-IS has been configured on a static PPP interface, the IS-IS neighbor does not come up if you remove the IP address from the interface and then add the IP address back to the interface. Consequently, when you remove and add back the IP address, you must also remove the IS-IS configuration from the interface and then add the configuration back to the interface by issuing the **no router isis** and **router isis** commands.

Route Tags

E-series routers support the use of route tags, also known as administrative tags, as a means of tagging the IP addresses on an IS-IS route before the route is propagated to other routers in an IS-IS domain. You must reference the tag in a route map to apply administrative policies to the IS-IS route that matches this tag.

Route Tag Applications

An administrative policy controls how a router handles the routes it receives from and sends to neighboring routers, and governs the installation of routes in the routing table. Examples of the types of administrative policies that you might apply with a route tag include:

- Policies for redistributing routes received from other protocols in the routing table to IS-IS
- Policies for redistributing routes between levels in an IS-IS routing hierarchy; this is also referred to as *route leaking*
- Policies for summarizing routes redistributed into IS-IS or within IS-IS by creating aggregate (summary) addresses

Route Tag Structure

On E-series routers, an IS-IS route tag is a 32-bit (4-octet) nonzero number that is stored as sub-TLV 1 inside the extended IP reachability TLV (type 135). TLV type 135, in turn, is part of an IS-IS LSP. The route tag is therefore advertised when LSPs are transmitted in an IS-IS network.

Because TLV type 135 is a new-style TLV tuple, it has a data structure that includes a wide metric field of four octets. As a result, to use IS-IS route tags you must issue the **metric-style wide** command (in Router Configuration mode) to specify that the router generate and accept only new-style TLV tuples.

For a discussion of IS-IS support for TLV tuples, see *Extensions for Traffic Engineering* on page 317.

Setting Route Tags

You can set IS-IS route tags in any of the following ways:

- Tagging a route for IP addresses on an IS-IS passive interface
- Tagging a route for IP addresses on an IS-IS interface
- Tagging IS-IS routes by using an associated route map to set the tag
- Tagging an IS-IS summary address

For instructions and examples on configuring IS-IS route tags, see the sections listed in Table 14.

Table 14: Configuration Tasks for Setting IS-IS Route Tags

To Learn About	Using This Command	See
Setting a route tag for an IS-IS passive interface	**passive-interface**	*Configuring Passive Interfaces* on page 337
Setting a route tag for an IS-IS interface	**isis tag**	*Configuring Route Tags for IS-IS Interfaces* on page 339
Setting a route tag for a route redistributed from another protocol to IS-IS by using an associated route map	**redistribute**	*Configuring Redistribution* on page 345
Setting a route tag for a route redistributed from one IS-IS level to another IS-IS level by using an associated route map	**redistribute isis ip**	*Redistributing Routes Between Levels* on page 347
Setting a route tag for an IS-IS default route by using an associated route map	**default-information originate**	*Configuring Default Routes* on page 352
Setting a route tag for an IS-IS summary address	**summary-address**	*Summarizing Routes* on page 354

Using Route Tags

You can set only a single route tag per IS-IS route. However, setting a tag for an IS-IS route has no effect by itself. To use the route tag to apply administrative policies such as route redistribution, route summarization, or route leaking, you must reference the tag value in a route map by issuing the **match tag** command (in Route Map Configuration mode). The route map must also include one or more **set** commands that modify attributes of the routes matching the tag value. These routes can reside on a different router than the one on which you set the route tag.

For example, the following commands define a route map to modify the metric and metric type attributes of IS-IS routes configured with a route tag value of 221. The **redistribute isis ip** command, as described in *Redistributing Routes Between Levels* on page 347, applies this route map when redistributing the routes from level 1 into level 2.

```
host1(config)#route-map map1 permit 5
host1(config-route-map)#match tag 221
host1(config-route-map)#set metric 10
host1(config-route-map)#set metric-type external
host1(config-route-map)#exit
host1(config)#router isis engineering
host1(config-router)#redistribute isis ip level-1 into level-2 route-map map1
```

Alternatively, you can use a route map to set the tag for an IS-IS route by issuing the **set tag** command (in Route Map Configuration mode). For example, the following commands define a route map that sets route tag 33 for those IS-IS routes configured with an administrative distance of 25:

```
host1(config)#route-map map2 permit 10
host1(config-route-map)#match distance 25
host1(config-route-map)#set tag 33
```

```
host1(config-route-map)#exit
host1(config)#router isis marketing
host1(config-router)#table-map map2
```

The **table-map** command, described in *Configuring Table Maps* on page 364, applies this route map to the IS-IS routes before they are added to the routing table. For details about configuring and using route maps, see *Route Maps* in *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*.

Unsupported Features

E-series routers do not currently support the following route tag features:

- Multiple route tags for a single IS-IS route

  Although the router accepts IS-IS routes with multiple route tags and propagates these routes in LSPs, it uses only the first route tag assigned to a route to determine routing policy.

- 64-bit (8-octet) route tags

  Although the router accepts IS-IS routes with 64-bit route tags and propagates these routes in LSPs, it does not use 64-bit route tags to determine routing policy.

- Mathematical (ordered) set operations on multiple route tags

Table Maps

E-series routers support the use of table maps to filter and manipulate the attributes of an IS-IS route before the route is installed in the routing table. Issuing the **table-map** command (in Router Configuration mode) applies a specified route map as a policy filter on the route before the route is installed in the routing table.

For IS-IS routes, the route map you apply by using the **table-map** command contains one or more **set** commands that can modify the following route attributes:

distance	origin
level	preference
metric	route type
metric type	tag

The router applies the specified route map to all routes currently and subsequently installed in the routing table. If any previously redistributed routes are changed as a result of applying the route map, the router redistributes these routes again with the changes caused by the route map.

For details about configuring and using route maps, see *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*.

Graceful Restart

E-series routers support IS-IS graceful restart as defined in RFC 3847—Restart Signaling for Intermediate System to Intermediate System (IS-IS) (July 2004). Graceful restart is also known as nonstop forwarding (NSF). When graceful restart is enabled on an IS-IS router, it allows the router to restart with minimal routing disruption to the network.

Features

When a router running in an IS-IS domain restarts, it typically causes routers in that domain to reset their adjacencies, thus generating unnecessary LSP flooding and shortest-path-first (SPF) calculations throughout the domain. Enabling graceful restart minimizes these effects by providing a mechanism by which a restarting router can do the following:

- Notify neighboring IS-IS routers that it is restarting and request help resynchronizing its LSP database. Neighbors with active adjacencies to the restarting router can thereby reestablish these adjacencies without having to reset them.
- Determine when complete LSP database synchronization with its neighbors has occurred.
- Optimize the process of LSP database synchronization while minimizing temporary routing disruption.

IS-IS graceful restart on E-series routers supports both restart and helper capabilities. These capabilities mean that an E-series router can not only notify neighboring IS-IS routers that it is restarting and request help resynchronizing its LSP database, but can also cooperate with other restarting routers to help them with the restart process.

How Graceful Restart Works

Graceful restart is disabled on the router by default. When you enable graceful restart by issuing the **nsf ietf** command, the router sends restart requests to neighboring routers to notify them that it is restarting. The restarting router includes the restart TLV (type 211) in its hello PDUs to signal the other routers that it supports graceful restart and to request help resynchronizing its LSP database. Including the restart TLV in hello packets also ensures that neighboring routers will maintain their active adjacencies to the restarting router and keep the restarting router in the network topology.

Graceful restart uses a set of configurable timers to support the restart mechanism. Table 15 briefly describes these timers and lists the associated commands that you can use to configure the timer values on the router.

Table 15: IS-IS Graceful Restart Timers

Timer	Description	Associated Command
Interface wait	Sets the maximum time (in seconds) that the router waits for all interfaces with IS-IS adjacencies to come up before completing the restart process	**nsf interface wait**
T1	Sets the time interval (in seconds) between restart requests sent by the router, and the number of times that the router resends unacknowledged restart requests	**nsf t1**
T2	Sets the maximum time (in seconds) that the router waits for the LSP database to synchronize	**nsf t2**
T3	Sets the maximum time (in seconds) that the restarting router waits before setting the overload bit to indicate that graceful restart has failed	**nsf t3**

For details about configuring graceful restart, see *Configuring Graceful Restart* on page 365.

IS-IS for IPv6

E-series routers support IPv6 routing for IS-IS. The IPv6 Reachability TLV propagates reachability information by flooding and is used in SPF calculations. The IPv6 Interface TLV is used for next hop calculation and is exchanged by means of IS-IS hello packets. A single SPF calculation computes both IPv6 and IPv4 routing tables.

IS-IS routers learn about their neighbors' support for IPv6 through the ISO network layer IPv6 protocol identifier, NLPID 142. The NLPID is contained in the NLPID TLV and is sent out in IS-IS hello packets when IS-IS IPv6 routing is enabled on an interface. A mismatch in support prevents an IS-IS adjacency from being established, because both neighbors must run the same protocols.

IPv6 aggregation, leaking, redistribution, export policies and import policies are supported similarly as for IP, but must be configured within the IS-IS IPv6 address family.

Graceful restart is supported for IS-IS IPv6 traffic depending on the availability of IPv6 high availability. It does not affect IP traffic.

Platform Considerations

For information about modules that support IS-IS on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support IS-IS.

For information about modules that support IS-IS on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support IS-IS.

References

For more information about the IS-IS protocol, consult the following resources:

- *JUNOSe Release Notes*, *Appendix A*, *System Maximums*—See the Release Notes corresponding to your software release for information about maximum values.
- ISO International Standard 8473-1:1993—Information technology – Protocol for providing the connectionless-mode network service
- ISO International Standard 9542:1988 (E)—Information processing systems – Telecommunications and information exchange between systems – End System-to-Intermediate System Routing Exchange Protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)
- ISO/IEC 10589:1992—Information technology – Telecommunications and information exchange between systems – Intermediate System-to-Intermediate System Intra-Domain Routing Exchange Protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)
- Extended Ethernet Frame Size Support—draft-ietf-isis-ext-eth-01.txt (November 2001 expiration)
- Management Information Base for IS-IS—draft-ietf-isis-wg-mib-16.txt (January 2005 expiration)
- Point-to-point operation over LAN in link-state routing protocols—draft-ietf-isis-igp-p2p-over-lan-05.txt (January 2005 expiration)
- RFC 1195—Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (December 1990)
- RFC 2763—Dynamic Hostname Exchange Mechanism for IS-IS (February 2000)
- RFC 2966—Domain-wide Prefix Distribution with Two-Level IS-IS (October 2000)
- RFC 2973—IS-IS Mesh Groups (October 2000)
- RFC 3277—Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance (April 2002)

- RFC 3373—Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies (September 2002)
- RFC 3784—Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE) (June 2004)
- RFC 3847—Restart Signaling for Intermediate System to Intermediate System (IS-IS) (July 2004)
- A Policy Control Mechanism in IS-IS Using Administrative Tags—draft-ietf-isis-admin-tags-02.txt (January 2005 expiration)

Features

Some of the major IS-IS features supported by the router include:

- Optimization of route leaking from level 1 to level 2
- Equal-cost paths maximum 16 equal paths
- Adjacency and LSP overrun
- Dynamic resolution of hostnames to system IDs
- Mesh groups
- Configurable LSP transmit and throttle intervals
- Route redistribution policies based on access lists between IS-IS levels
- Three-way handshake for point-to-point adjacencies
- Simple text and HMAC MD5 authentication
- Support for bigger metric TLVs
- Domain-wide prefix distribution
- Traffic engineering for MPLS
- 32-bit (4-octet) route tags
- Table maps
- Graceful restart
- IPv6 routing

Before You Run IS-IS

At least one IP address/router ID must be configured on your router for IS-IS to run.

Configuration Tasks

Configure Integrated IS-IS by completing the following tasks in the order presented. You must enable IS-IS. All other tasks are optional.

1. Enable IS-IS.
2. Configure selected IS-IS interface-specific parameters.
3. Configure selected global IS-IS parameters.
4. Configure selected IS-IS parameters for monitoring and debugging purposes.
5. Configure IS-IS parameters to enable CLNS packets to be recognized by your router and to monitor CLNS information.

Enabling IS-IS for IP Routing

When enabling IS-IS, you must create an IS-IS routing process and assign it to specific interfaces rather than to networks. You can specify only a single IS-IS process per router.

To enable IS-IS routing, enter Global Configuration mode, and follow this procedure:

1. Specify an IS-IS process for IP. In this example, floor12 is specified as the tag name.

   host1(config)#**router isis floor12**

   The router is now in Router Configuration mode.

2. Configure a Network Entity Title (NET) for the routing process that specifies the ISO network address.

   host1(config-router)#**net**
   47.0010.0000.0000.0000.0001.0001.1111.1111.1111.00

3. Enter Interface Configuration mode, and specify the interface that you want to actively route IS-IS.

   host1(config)#**interface atm 2/0**

4. Specify the IS-IS process to apply to the interface. Use the same tag name that you specified with the **router isis** command.

   host1(config-if)#**ip router isis floor12**

   You can repeat Steps 3 and 4 to apply the IS-IS process to multiple interfaces.

ip router isis

- Use to configure an IS-IS routing process on an IP interface.
- Before the IS-IS router process is useful, you must assign a NET with the **net** command, and enable some interfaces with IS-IS.
- Use the tag parameter to specify a meaningful name for a routing process. It must be unique among all IP routing processes for a given router. If you choose not to specify a tag name, a null tag is assumed, and the process is referenced with a null tag. Use the same tag name for **ip router isis** as you did for the **router isis** command.
- Example

  host1(config-if)#**ip router isis floor12**

- Use the **no** version to disable IS-IS for IP on the interface.

net

- Use to configure a NET for a specified routing process. The NET defines the ISO address and consists of an area address or ID, a system ID, and a selector.
- You must configure a minimum of one NET.
- You can have a maximum of three NETs per router.
- You can manually add multiple area IDs by adding multiple NETs with the same system ID.
- There is no default value; **net** must be configured for an IS-IS process to start.
- Multiple NETs can be temporarily useful when there has been a network reconfiguration where either multiple areas are merged, or one area is in the process of being split into more areas. Multiple area addresses enable you to renumber an area slowly, without needing to set aside time to renumber areas all at once.
- When you use IS-IS to do IP routing only, a NET must be configured to instruct the router about its system ID and area ID.
- Example—The following commands configure a router with the area ID 47.0005.80ff.f800.0000.0001.0001 and the system ID 0000.0c11.1111. The last byte of the NET is the N-selector byte and is always 0.

  host1(config-router)#**net**
  47.0010.0000.0000.0000.0001.0001.1111.1111.1111.00

- Use the **no** version to remove a specific NET. Remember that you must specify the NET. The last NET cannot be removed.

router isis

- Use to enable the IS-IS routing protocol and to specify an IS-IS process for IP.
- Specify only one IS-IS process per router.
- Use the tag parameter to specify a meaningful name for a routing process. If you choose not to specify a tag name, a null tag is assumed, and the process is referenced with a null tag.
- Example

  host1(config)#**router isis floor12**

- Use the **no** version to disable IS-IS routing.

Summary Example

```
host1(config)#router isis floor12
host1(config-router)#net 47.0010.0000.0000.0000.0001.0001.1111.1111.1111.00
host1(config-router)#exit
host1(config)#interface atm 2/0
host1(config-if)#ip router isis floor12
host1(config-router)#exit
host1(config-if)#interface atm 2/1
host1(config-if)#ip router isis floor12
```

Enabling and Configuring IS-IS for IPv6 Routing

When enabling IS-IS IPv6, you must create an IS-IS IPv6 routing process and assign it to specific interfaces rather than to networks. You can specify only a single IS-IS process per router.

To enable IS-IS routing, enter Global Configuration mode, and follow this procedure:

1. Access Global Configuration mode and specify an IPv6 license.

   host1(config)#**license ipv6** *license-value*

2. Configure an IP address on the router to serve as the router ID.

   host1(config)#**interface loopback0**
   host1(config-if)#**ip address 10.6.5.4/32**

3. Configure the lower-layer interfaces over which the IPv6 traffic flows.

   host1(config-if)#**interface fastEthernet 1/0**

4. Configure an IPv6 address on the interface.

   host1(config-if)#**ipv6 address 2008::1/48**

5. Specify the IS-IS IPv6 process to apply to the interface. Use the same tag name that you specify with the **router isis** command for the VR.

   host1(config-if)#**ipv6 router isis floor12**

   Repeat Steps 3–5 for all desired IPv6 interfaces.

6. Specify an IS-IS process globally for the VR. Use the same tag name that you specify with the **ipv6 router isis** command on the interface.

   host1(config)#**router isis floor12**

7. Configure a Network Entity Title (NET) for the routing process that specifies the ISO network address.

   host1(config-router)#**net**
   47.0010.0000.0000.0000.0001.0001.1111.1111.1111.00

8. Create the IS-IS IPv6 address family for the interface.

   host1(config-router)#**address-family ipv6 unicast**

9. Configure any of the following desired IS-IS options for the address family: redistributing routes from other protocols, redistributing IS-IS IPv6 routes between levels, distributing level 2 routing information to level 1 routers throughout the IS-IS routing domain, summarizing IPv6 routes, applying a route map to modify routes before they are installed in the routing table,

   host1(config-router-af)#**redistribute ospf level-1-2**
   host1(config-router-af)#**redistribute isis level-2 into level-1**
   host1(config-router-af)#**distribute-domain-wide**
   host1(config-router-af)#**summary-prefix 2001:2000::0/8 level-1 metric 10 tag 100**
   host1(config-router-af)#**table-map ospfFilter**

10. Exit the IS-IS IPv6 address family.

    host1(config-router-af)#**exit-address-family**

NOTE: Enabling IPv6 for the interface also enables IPv4 for that interface. However, this interface does not participate in IS-IS IPv4 routing.

address-family

- Use to configure IS-IS to exchange IPv6 addresses by creating the IPv6 address family.
- Use the **unicast** keyword to exchange unicast addresses. Use the **multicast** keyword to exchange multicast addresses. Use the **unicast** and **multicast** keywords together, or omit both of them to exchange both unicast and multicast addresses.
- Examples

  host1(config)#**address-family ipv6 unicast**

- Use the **no** version to disable the exchange of IPv6 addresses.

exit-address-family

- Use to exit Address Family Configuration mode and access Router Configuration mode.
- Example

  host1:vr1(config-router-af)#**exit-address-family**

- There is no **no** version.

ipv6 router isis

- Use to configure an IS-IS routing process on an IPv6 interface.
- Before the IS-IS router process is useful, you must assign a NET with the **net** command, and enable some interfaces with IS-IS.
- Use the tag parameter to specify a meaningful name for a routing process. It must be unique among all IPv6 routing processes for a given router. If you choose not to specify a tag name, a null tag is assumed, and the process is referenced with a null tag. Use the same tag name for **ipv6 router isis** as you did for the **router isis** command.
- Example—Enables ISIS for IPv6 on an interface.

  host1(config-if)#**ipv6 router isis bldg1**

- Use the **no** version to disable IS-IS on the interface.

Summary Example

```
host1(config)#license ipv6 license-value
host1(config)#interface loopback0
host1(config-if)#ip address 10.6.5.4/32
host1(config-if)#interface fastEthernet 1/0
host1(config-if)#ipv6 address 2008::1/48
host1(config-if)#ipv6 router isis floor12
host1(config)#router isis floor12
host1(config-router)#net
47.0010.0000.0000.0000.0001.0001.1111.1111.1111.00
host1(config-router)#address-family ipv6 unicast
host1(config-router-af)#redistribute ospf level-1-2
host1(config-router-af)#redistribute isis level-2 into level-1
host1(config-router-af)#distribute-domain-wide
host1(config-router-af)#summary-prefix 2001:2000::0/8 level-1 metric 10 tag
100
host1(config-router-af)#table-map ospfFilter
```

Configuring IS-IS Interface-Specific Parameters

You can change IS-IS interface–specific parameters; most can be configured independently of other attached routers. You are not required to alter any interface parameters; however, some parameters must be consistent across all routers in your network. If you change certain values from the defaults, you must configure them on multiple interfaces and routers.

In the following command guidelines, many parameters are preset to a default value. If that parameter has been modified from its default, use the **no** version of the command to restore its default value.

Configuring Authentication

You can set a password to authenticate IS-IS hello packets, and you can configure HMAC MD5 authentication for IS-IS interfaces.

isis authentication-key

- Use to specify a password associated with an interface for authentication of IS-IS hello packets, and to enable simple authentication of level 1 or level 2 hello packets.
- You can specify whether the password is for level 1 or level 2 hellos.
- Example

  host1(config-if)#**isis authentication-key 0 red5flower6**

- Use the **no** version to delete the password.

isis message-digest-key

- Use to configure HMAC MD5 authentication for an interface, and to enable MD5 authentication of level 1 or level 2 hello packets.
- Generates a secure, encrypted message digest of level 1 or level 2 hello packets and inserts the digest into the packet from which it is created. Level 1 is the default.
- You can specify whether the key is entered in unencrypted or encrypted format. If you do not specify which, the string is assumed to be unencrypted.
- Example

  host1(config-if)#**isis message-digest-key 3 hmac-md5 wdi6c3s39n level-2**

- For point-to-point interfaces, configure keys only for level 1, because only one hello packet is sent (at level 1), not one at level 1 and one at level 2. Keys configured at level 2 are ignored for point-to-point interfaces.
- Use the **no** version to delete the MD5 key, specified by the key ID, from the interface.

Configuring Link-State Metrics

You can configure the routing metric (cost) for an IS-IS interface. Routes with lower total path metrics are preferred over those with higher path metrics.

isis metric

- Use to configure a cost for a specified interface.
- You can select a number in the range 0–63 if you configured the router with the **metric-style narrow** command. You can select a number in the range 0–16277215 if you configured the router with the **metric-style transition** or the **metric-style wide** command.
- The default value is 10. The default metric is the value assigned when no quality of service (QoS) routing is performed.
- You can configure the default metric for a specified interface by selecting level 1 or level 2 routing. This resets the metric only for level 1 or level 2 routing, respectively. If you do not specify a level, the command specifies both level 1 and level 2 by default.
- We recommend that you configure a reference bandwidth if you want the default cost on interfaces to be related to link speed. If you do not, the default IS-IS metrics are simply hop-count-like metrics.
- Example

  host1(config-if)#**isis metric 20 level-2**

- Use the **no** version to restore the default value, 10.

Configuring a Reference Bandwidth to Set a Default Metric

By default, all IS-IS interfaces without a configured metric have the same routing metric, 10, However, when you configure a reference bandwidth for IS-IS, the default metric is calculated differently for each IS-IS interface. The default routing metric in this case is the reference bandwidth divided by the bandwidth of the particular interface.

For example, if you set the IS-IS reference bandwidth to 50,000,000, the default metric for a 10-Mbps interface is calculated as 5. Interfaces with lower bandwidths have higher default metrics than this interface. Similarly, links with higher bandwidths have lower default metrics than this interface.

reference-bandwidth

- Use to set a reference bandwidth from which a default metric can be calculated by IS-IS for interfaces without a configured metric.
- Example

  host1(config-router)#**reference-bandwidth 100000000**

- Use the **no** version to remove the reference bandwidth. When you do so, the default metric reverts to 10.

Setting the CSNP Interval

You can set the advertised complete sequence number PDU (CSNP) interval for an IS-IS interface.

isis csnp-interval

- Use to configure the **isis csnp-interval** level for a specified interface. The level can be configured independently for level 1 and level 2.
- For LAN interfaces: the default value is 10 seconds, which you probably do not need to change. For WAN interfaces: the default value is 0 seconds or disabled.
- On point-to-point subinterfaces use **isis csnp-interval** with the **isis mesh-group** command.
- Completed sequence number PDUs are sent by the designated router to maintain database synchronization.
- Example

  host1(config-if)#**isis csnp-interval 30 level-1**

- Use the **no** version to restore the default value.

Configuring Hello Packet Parameters

You can set the hello interval and the hello multiplier for IS-IS hello packets.

isis hello-interval
isis hello-multiplier

- Use the **isis hello-interval** command to set the length of time (in seconds) between hello packets sent on a specific interface. Configure independently for level 1 and level 2, except on point-to-point interfaces because only a single type of hello packet is sent on serial links. For this reason, it is independent of levels 1 and 2. For example, you can specify an optional level for Frame Relay multiaccess networks.

  The hello-interval is equal to the *hello multiplier* times the *hello interval seconds* and is advertised as the *holdtime* in the hello packets transmitted. The range is 0–65535; the default value is 10 seconds.

NOTE: The hello-interval value must be the same for all routers attached to a common network. With smaller hello intervals, topological changes are detected faster, but there is more routing traffic.

- Use the **isis hello-multiplier** command to set a number by which to multiply the hello interval seconds. This number determines the total *holding time* transmitted in the IS-IS hello packet. The default is 3. Use when hello packets are frequently lost and IS-IS adjacencies are failing unnecessarily.

  The advertised hold time in IS-IS hellos is set to the hello-multiplier times the hello-interval. Neighbors declare an adjacency to this router to be down after not having received any IS-IS hellos during the advertised hold time.

  - The hold time (and thus the hello-multiplier and the hello-interval) can be set on a per interface basis, and can be different between different routers in one area.
  - Using a smaller hello-multiplier will give fast convergence, but can result in more routing instability.
  - Increment the hello-multiplier to a larger value to help network stability when needed.

CAUTION: Never configure a hello-multiplier lower than the default.

- Holding time—Time a neighbor waits for another hello packet before declaring the neighbor is down. It determines how quickly a failed link or neighbor is identified so that routes can be recalculated.

- Raise the hello multiplier and lower the hello interval simultaneously to make the hello protocol more reliable without increasing the time required to detect a link failure.
- Example

  host1(config-if)#**isis hello-interval 6 level-1**
  host1(config-if)#**isis hello-multiplier 10 level-1**

- Use the **no** version to restore a default value.

Padding IS-IS Hello Packets

You can use the **isis hello padding** command to configure IS-IS hello packet padding. Padding the hello packets promotes early error detection due to transmission problems with large frames or due to mismatched MTUs on adjacent interfaces.

When disabled (default), IS-IS hello packets are padded to the full MTU size until an adjacency is formed with the adjacent interface. After the adjacency is formed, the hello packets are no longer padded. When enabled, IS-IS hello packets are always padded.

isis hello padding

- Use to pad IS-IS hello packets to their full maximum transmission unit (MTU) size.
- Example

  host1(config-if)#**isis hello padding**

- Use the **no** version to restore the hello padding to its default, no padding.

Configuring LSP Parameters

You can configure the transmission interval, retransmission interval, and retransmission throttle interval for LSPs on an interface-specific basis.

isis lsp-interval

- Use to configure the delay between successive IS-IS link-state PDU (LSP) transmissions.
- You can choose an interval in the range 1–4294967295 milliseconds. For example, setting 100 milliseconds allows 10 packets per second.
- The default value is 33 milliseconds.
- If your network has many IS-IS neighbors and interfaces, a particular router may have difficulty with the CPU load imposed by LSP transmission and reception. If this is the case, you can reduce the LSP transmission rate by issuing this command.
- Example

  host1(config-if)#**isis lsp-interval 100**

- Use the **no** version to restore the default value, 33 milliseconds.

isis retransmit-interval

- Use to configure the number of seconds between the retransmission of IS-IS LSPs with the same LSP ID for point-to-point links.
- You can select an interval in the range 1–65535 seconds.
- The default value is 5 seconds.
- Specify a number greater than the expected round-trip delay between any two routers on your network.
- Always specify conservatively; otherwise, excessive retransmission can result.
- Because retransmissions occur only when LSPs are dropped, when you set **isis retransmit-interval** to a higher value, it has little effect on reconvergence.
- Set to a higher value when routers have many neighbors or more paths over which LSPs can be flooded.
- Use a large value for serial lines.
- Example

  host1(config-if)#**isis retransmit-interval 60**

- Use the **no** version to restore the default value, 5 seconds.

isis retransmit-throttle-interval

- Use to configure the maximum rate at which IS-IS LSPs are retransmitted on point-to-point links. The interval is the number of milliseconds between packets.
- You can choose an interval in the range 0–65535 milliseconds.
- The default delay value is 33 milliseconds.
- The **isis retransmit-throttle-interval** is the maximum rate at which IS-IS LSPs are retransmitted. It is different from **isis lsp-interval**, which is the rate at which LSPs are transmitted on the interface; and it is different from **isis retransmit-interval**, which is the period between successive retransmissions of the *same* LSP. Use all three commands with each other to control the load of routing traffic from one router to its neighbors.
- Typically, you can set this interval for very large networks with many LSPs and many interfaces as a way of controlling LSP retransmission traffic.
- Example

  host1(config-if)#**isis retransmit-throttle-interval 300**

- Use the **no** version to restore the default value, 33 milliseconds.

Setting the Designated Router Priority

You can set the priority for the designated IS-IS router that you have elected to use.

isis priority

- Use to set the priority of use for your designated router.
- You can configure an individual priority for level 1 and level 2 by choosing a priority level in the range 0–127.
- The default priority level is 64.
- Specifying the **level 1** or **level 2** keyword resets the priority only for level 1 or level 2 routing, respectively.
- Priorities are used to determine which router in the network is the designated intermediate system (DIS); the router with the highest priority becomes the DIS. Priorities are advertised in hellos.
- IS-IS has no backup designated router. Setting the priority to 0 reduces the chance of this router becoming the DIS, but does not prevent it. If a router with a higher priority is identified, it takes over the role from the current DIS. When priorities are equal, the highest MAC address breaks the tie and becomes the DIS.
- Example

  host1(config-if)#**isis priority 80 level-1**

- Use the **no** version to restore the default value, 64.

Configuring Passive Interfaces

You can configure an IS-IS passive interface. A passive interface only advertises its IP address in its LSPs; it does not send or receive IS-IS packets.

Optionally, you can set a route tag for an IS-IS passive interface by including the **tag** keyword and a numeric tag value in the **passive-interface** command.

Passive interfaces have a metric of zero by default. You can set a different metric for a particular passive interface by specifying the value along with the **metric** keyword. A global default metric set with the **metric** command does not affect any passive interface. Similarly, configuring a reference bandwidth for IS-IS has no effect on passive interfaces. Metrics specified for a passive interface apply to both level 1 and level 2 interfaces unless you restrict the metric to a single level.

passive-interface

- Use to configure an IS-IS interface so that its IP address is advertised in its link-state PDUs but no IS-IS packets are sent from or received on the interface.
- Use the optional **tag** keyword to specify a tag value for an IS-IS passive interface before the route is propagated to other routers in an IS-IS domain. The tag value must be a number in the range 1–4294967295.
- Use the optional **metric** keyword to specify a metric value for an IS-IS passive interface. The metric value must be a number in the range 1–16777215. This value overrides the default metric of zero.

- You can also accomplish the equivalent of the **passive-interface** command by using the **redistribute** command to redistribute a connected route to level 1.
- Example 1—Configures loopback 0 as a passive interface and enable IS-IS on subinterfaces ATM 2/0.1 and ATM 2/1.1. IS-IS advertises the IP address of loopback 0 in its link-state PDUs, but runs only on ATM 2/0.1 and ATM 2/1.1:

  ```
  host1(config)#router isis floor12
  host1(config-router)#net
  47.0010.0000.0000.0000.0001.0001.1111.1111.1111.00
  host1(config-router)#passive-interface loopback 0
  host1(config-router)#exit
  host1(config)#interface atm 2/0.1
  host1(config-subif)#ip router isis floor12
  host1(config-subif)#exit
  host1(config)#interface atm 2/1.1
  host1(config-subif)#ip router isis floor12
  ```

  You can override the passive-interface configuration simply by issuing the complementary command. For example, suppose you issue the following commands after the previous configuration:

  ```
  host1(config-router)#passive-interface atm 2/0.1
  host1(config-router)#exit
  host1(config)#interface loopback 0
  host1(config-if)#ip router isis floor12
  ```

  Now IS-IS advertises the IP address of ATM 2/0.1 in its link-state PDUs, but runs only on loopback 0 and ATM 2/1.1.

- Example 2—Sets a route tag on the IS-IS passive interface configured in Example 1.

  ```
  host1(config)#router isis floor12
  host1(config-router)#passive-interface loopback 0 tag 12
  ```

- Example 3—Sets a metric and level on the IS-IS passive interface configured in Example 1.

  ```
  host1(config)#router isis floor12
  host1(config-router)#passive-interface loopback 0 metric 45 level-2
  ```

- Use the **no** version to delete the passive interface, or to remove the tag, metric, or both.

Configuring Adjacency

You can configure the type (level) of adjacency you want to use on an IS-IS interface.

isis circuit-type

- Use to specify adjacency levels on a specified interface; however, normally, you do not need to use this command.
- Configure a router as a level 1-only, a level 1–level 2 system, or a level 2-only system.
- Configure some interfaces to be level 2-only for routers that are between areas. This prevents wasting bandwidth by sending out unused level 1 hellos.
- On point-to-point interfaces, the level 1 and level 2 hellos are in the same packet.
- Level 1-2 is the default.
- Example

  host1(config-if)#**isis circuit-type level-2-only**

- Use the **no** version to restore the default value, level-1-2.

Configuring Route Tags for IS-IS Interfaces

To configure a route tag for the IP addresses on an IS-IS interface:

1. Specify an IS-IS routing process, and access Router Configuration mode.

   host1(config)#**router isis engineering**
   host1(config-router)#

2. Configure a NET for the IS-IS process.

   host1(config-router)#**net**
   47.0010.0000.0000.0000.0001.0001.1111.1111.1111.00

3. Configure the router to accept and generate only new-style TLV tuples with a wider metric field. New-style TLV tuples include TLV type 135, which contains the route tag.

   host1(config-router)#**metric-style wide**

4. Exit Router Configuration mode.

   host1(config-router)#**exit**

5. Specify the interface on which you want to route IS-IS.

   The procedure assumes that at least one IP address is already configured on this interface.

   host1(config)#**interface atm 2/2.1**

6. Configure a route tag for the interface.

   host1(config-subif)#**isis tag 221**

7. Specify the IS-IS process to apply to the interface.

   host1(config-subif)#**ip router isis engineering**

8. (Optional) Access Privileged Exec mode, and verify the route tag assignment.

   host1(config-subif)#**exit**
   host1(config)#**exit**
   host1#**show isis database detail**

isis tag

- Use to set a route tag for the IP addresses on an IS-IS interface before the route is propagated to other routers in an IS-IS domain.
- Specify a numeric tag value in the range 1–4294967295.
- To make use of the route tag to modify route attributes or redistribute routes, you must reference the tag value in a route map.
- Example

  host1(config)#**interface atm 3/0**
  host1(config-if)#**isis tag 45**

- Use the **no** version to remove the route tag from the interface.

Configuring Point-to-Point-over-LAN Circuits

You can deploy IS-IS on broadcast and point-to-point circuits. IS-IS treats these circuits differently in several ways, such as when establishing neighbor adjacencies or flooding link-state information.

Broadcast circuits use designated routers and are represented as virtual nodes in the network topology. They require periodic database synchronization. By default, IS-IS treats the broadcast link as LAN media and tries to bring up the LAN adjacency even when the interface is configured as unnumbered or only a single neighbor exists on that link.

In contrast, point-to-point circuits have less overhead, because they do not use designated routers, the link-state database has no representation of the pseudonode or network LSA, and they do not require periodic database synchronization. However, if more than two routers are connected on the LAN media, routing information in the network is reduced.

Although broadcast circuits are intended to handle more than two devices, in some circumstances you might connect only two routers over the physical or virtual LAN. Even though only two routers are connected, IS-IS treats the circuit as a broadcast circuit that has many more connected routers, with all the associated broadcast overhead but without the benefits of reduced routing information and of optimized flooding that result from having more than two routers on the LAN.

You can use the **isis network point-to-point** command to configure IS-IS to operate using point-to-point connections on a broadcast circuit when only two routers are on the circuit. This configuration is known as a point-to-point-over-LAN or P2P circuit. This interface configuration tears down the current LAN adjacency that IS-IS has over this interface. IS-IS then reestablishes the adjacency as a point-to-point connection and regenerates the LSPs. The broadcast link is thereafter treated as simple point-to-point interface.

Treating the LAN as a P2P circuit reduces the amount of information that IS-IS has to maintain and manage. For example, there is no need to elect a designated router for the interface. LSP flooding is performed as in P2P links without the need for using periodic CSNPs.

This circuit configuration can be advantageous even when many routers are on the LAN. For example, you might want to organize the routers into multiple smaller VLANs so that you can assign different costs to the IS-IS neighbors. You can apply this configuration to any such VLAN that has only two routers. IS-IS then views the LAN as a mesh of point-to-point connections.

The use of IP unnumbered interfaces makes the most of scarce IP address resources and provides for simpler network management and configuration. This configuration enables IP processing on a point-to-point interface without an explicit IP address. The IP unnumbered interface borrows the IP address of another interface on the node. Point-to-point-over-LAN circuits separate the concept of network type from media type, and enable you to apply unnumbered interface configurations to LANs.

The point-to-point-over-LAN feature requires the following:

- The LAN must have only two routers.
- Both routers must support the feature.
- You must configure the interface at each end as a P2P connection.
- If you are using numbered interfaces, both ends must be in same IPv4 subnet.
- If you are using unnumbered interfaces, both ends require static ARP entry configuration.

isis network point-to-point

- Use to specify that the broadcast circuit is to be treated as a point-to-point circuit.
- Issuing this command tears down existing adjacencies, originates or flushes LSPs, and establishes new adjacencies
- Example

  host1(config-intf)#**isis network point-to-point**

- Use the **no** version to restore the default value, treating the circuit as a broadcast circuit.

Summary Example

```
host1(config-router)#passive-interface loopback 0
host1(config-if)#interface atm 8/0
host1(config-if)#isis tag 55
host1(config-if)#isis metric 20 level-2
host1(config-if)#isis csnp-interval 30 level-1
host1(config-if)#isis hello-interval 6 level-1
host1(config-if)#isis hello-multiplier 10 level-1
host1(config-if)#isis lsp-interval 100
host1(config-if)#isis retransmit-interval 60
host1(config-if)#isis retransmit-throttle-interval 300
host1(config-if)#isis priority 80 level-1
host1(config-if)#isis circuit-type level-2-only
host1(config-intf)#no isis network point-to-point
```

Configuring Global IS-IS Parameters

This section describes the commands you can use to globally configure optional IS-IS parameters.

In the following command guidelines, many parameters are preset to a default value. Use the **no** version of those commands to restore default values.

Setting Authentication Passwords

You can configure simple authentication or HMAC MD5 authentication for either an area or a domain.

area-authentication-key

- Use to specify a password used by neighboring routers for authentication of IS-IS level 1 LSPs, CSNPs, and PSNPs.
- Issuing this command enables simple authentication of level 1 LSPs only. To enable simple authentication of level 1 CSNPs or PSNPs, use the **area-authentication** command, described on page 344.
- You can specify whether the key is entered in unencrypted or encrypted format. If you do not specify which, the string is assumed to be unencrypted.
- Example

  ```
  host1(config-router)#area-authentication-key 0 bigtree
  ```

- Use the **no** version to delete the password.

area-message-digest-key

- Use to configure HMAC MD5 authentication for an area.
- Generates a secure, encrypted message digest of level 1 packets (LSPs, CSNPs, and PSNPs) and inserts the digest into the packet from which it is created.
- Issuing this command enables MD5 authentication of level 1 LSPs only. To enable MD5 authentication of level 1 CSNPs or PSNPs, use the **area-authentication** command, described on page 344.

- You can specify whether the key is entered in unencrypted or encrypted format. If you do not specify which, the string is assumed to be unencrypted.
- Example

  host1(config-router)#**area-message-digest-key 1 hmac-md5 kd4s8hnEK**

- Use the **no** version to delete the MD5 key specified by the key ID.

domain-authentication-key

- Use to specify a password used by neighboring routers for authentication of IS-IS level 2 LSPs, CSNPs, and PSNPs.
- Issuing this command enables simple authentication of level 2 LSPs only. To enable simple authentication of level 2 CSNPs or PSNPs, use the **domain-authentication** command, described on page 344.
- You can specify whether the key is entered in unencrypted or encrypted format. If you do not specify which, the string is assumed to be unencrypted.
- Example

  host1(config-router)#**domain-authentication-key 8 4kl6n39us**

- Use the **no** version to delete the password.

domain-message-digest-key

- Use to configure HMAC MD5 authentication for a domain.
- Generates a secure, encrypted message digest of level 2 packets (LSPs, CSNPs, and PSNPs) and inserts the digest into the packet from which it is created.
- Issuing this command enables MD5 authentication of level 2 LSPs only. To enable MD5 authentication of level 2 CSNPs or PSNPs, use the **domain-authentication** command, described on page 344.
- You can specify whether the key is entered in unencrypted or encrypted format. If you do not specify which, the string is assumed to be unencrypted.
- Example

  host1(config-router)#**domain-message-digest-key 4 hmac-md5 4bFjt7es**

- Use the **no** version to delete the MD5 key specified by the key ID.

Configuring Authentication of CSNPs and PSNPs

You must enable and disable authentication of CSNP packets and PSNP packets separately from authentication of LSP packets.

area-authentication

- Use to enable or disable (suppress) simple authentication or HMAC MD5 authentication of IS-IS level 1 CSNP packets or PSNP packets.
- When authentication is enabled, it uses either the simple text password specified by the **area-authentication-key** command, or the HMAC MD5 key specified by the **area-message-digest-key** command.
- You must specify either the **csnp** keyword to enable authentication of level 1 CSNP packets, or the **psnp** keyword to enable authentication of level 1 PSNP packets.
- Example

  host1(config-router)#**area-authentication csnp**

- Use the **no** version to restore the default behavior, in which authentication of level 1 CSNPs and PSNPs is disabled. When authentication of level 1 CSNPs or PSNPs is suppressed, the router does not authenticate these packets when it receives them, nor does it send authentication information in these packets when it transmits them.

domain-authentication

- Use to enable or disable (suppress) simple authentication or HMAC MD5 authentication of IS-IS level 2 CSNP packets or PSNP packets.
- When authentication is enabled, it uses either the simple text password specified by the **domain-authentication-key** command, or the HMAC MD5 key specified by the **domain-message-digest-key** command.
- You must specify either the **csnp** keyword to enable authentication of level 2 CSNP packets, or the **psnp** keyword to enable authentication of level 2 PSNP packets.
- Example

  host1(config-router)#**domain-authentication csnp**

- Use the **no** version to restore the default behavior, in which authentication of level 2 CSNPs and PSNPs is disabled. When authentication of level 2 CSNPs or PSNPs is suppressed, the router does not authenticate these packets when it receives them, nor does it send authentication information in these packets when it transmits them.

Configuring Redistribution

You can specify how IS-IS redistributes routes received from other routing protocols, redistributes routes according to new policies, and controls redistribution of routes with access lists and route maps.

Optionally, when you issue the **redistribute** command and specify a route map, you can use the map to set a route tag for a route redistributed from another protocol to IS-IS. Make sure the route map you specify includes the **set tag** command that defines a tag value for the routes destined for IS-IS. For details about configuring and using route maps, see *Route Maps* in *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*.

To redistribute IPv6 routes, issue the **redistribute** command from within the IS-IS IPv6 address family.

access-list route-map

- Use the **access-list** command to create a standard or extended access list.
- Use the **route-map** command to create a route map.
- For detailed information about configuring access lists and route maps, see *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*.
- Example—For IP route redistribution the access list filters IP routes; for IPv6 route redistribution, the access list must filter IPv6 routes.

  1. Configure three static routes:

     host1(config)#**ip route 10.20.20.0 255.255.255.0 192.168.1.0**
     host1(config)#**ip route 10.20.21.0 255.255.255.0 192.168.1.0**
     host1(config)#**ip route 10.21.0.0 255.255.255.0 192.168.1.0**

  2. Configure an access list with filters on routes 10.20.20.0/24 and 10.20.21.0/24:

     host1(config)#**access-list boston permit 10.20.0.0 0.0.255.255**

  3. Configure a route map that matches the previous access list and applies an internal metric type:

     host1(config)#**route-map 1**
     host1(config-route-map)#**match ip address 1**
     host1(config-route-map)#**set metric-type internal**

  4. Configure redistribution into IS-IS of the static routes with route map 1:

     host1(config)#**router isis testnet**
     host1(config-router)#**redistribute static ip route-map 1**

5. Use the **show isis database** command to verify the effect of the redistribution (that two static routes matching the route map are redistributed as level 2 internal routes):

```
host1#show isis database detail l2
IS-IS Level-2 Link State Database
LSPID LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.6666.00-00  0x000002B7   0x3E1F 1198 0/0/0
  Area Address: 47.0005.80FF.F800.0000.0001.0001
  NLPID:       0xcc
  IP Address:  192.168.1.105
  Metric: 10 IS 0000.0000.6666.01
  Metric: 10 IS 0000.0000.3333.00
  Metric: 10 IS 0000.0000.7777.00
  Metric: 30 IP 10.20.21.0 255.255.255.0
  Metric: 30 IP 10.20.20.0 255.255.255.0
```

- Use the **no** version of the **access-list** command to remove the access list or the specified entry in the access list.
- Use the **no** version of the **route-map** command to remove an entry.

clear ip isis redistribution
clear isis ipv6 redistribution

- Use to clear all the routes that have been previously redistributed into IS-IS and to redistribute them using the current policy configured. Use the IP version to redistribute IP routes. Use the IPv6 version to redistribute IPv6 routes.
- Use when you have made changes to route maps or access lists that affect how routes are redistributed to IS-IS.
- Example

  host1#**clear ip isis redistribution**

- There is no **no** version.

disable-dynamic-redistribute

- Use to halt the dynamic redistribution of routes that are initiated by changes to a route map.
- Dynamic redistribution is enabled by default.
- Example

  host1(config-router)#**disable-dynamic-redistribute**

- Use the **no** version to reenable dynamic redistribution.

redistribute

- Use to redistribute routes from other routing protocols in the routing table to IS-IS. IS-IS advertises these routes as level 1 only, level 2 only, or both. Level 2 only is the default.
- To redistribute IPv6 routes, you must issue the command from within the IS-IS IPv6 address family.
- The default is no source protocol defined for redistribution.

- This command can accomplish the same results as the **passive-interface** command by redistributing a connected route to level 1.
- Optionally, you can specify a route map and use it to set a route tag for routes redistributed to IS-IS.
- Example 1—Redistributing static IP routes with a route map

  host1(config-router)#**redistribute static ip route-map 10**

- Example 2—Redistributing IPv6 routes from OSPF into IS-IS level 1 and level 2

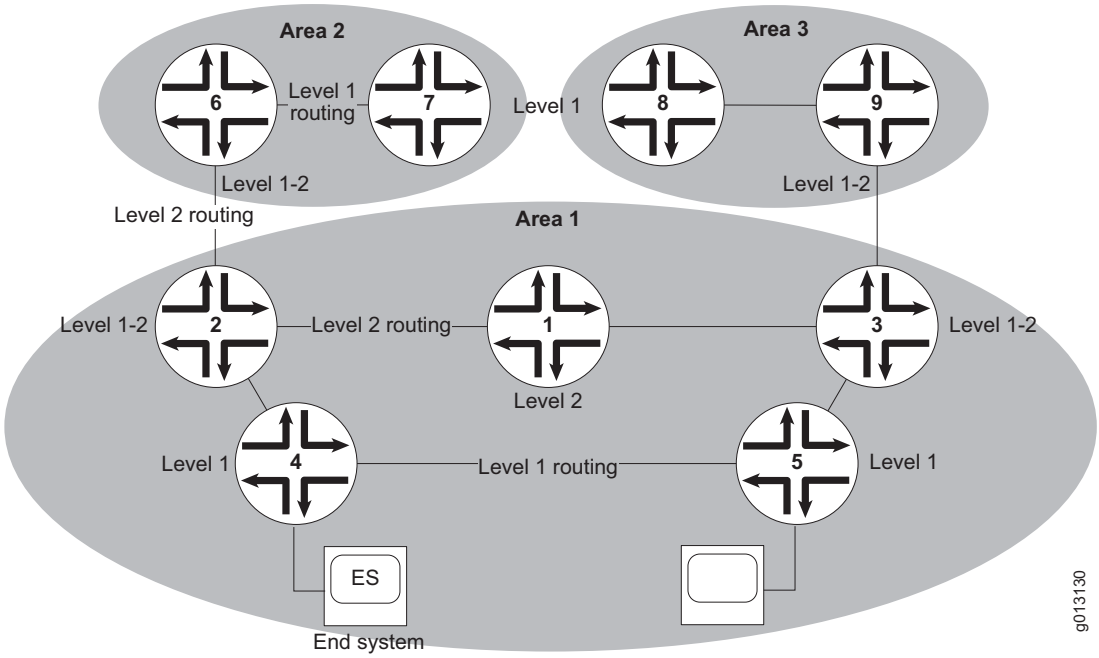
  host1(config-router-af)#**redistribute ospf level-1-2**

- Use the **no** version to disable redistribution.

Redistributing Routes Between Levels

The two-level routing hierarchy of IS-IS can lead to suboptimal path selection in certain situations. Because a level 1 router by default has knowledge only of level 1 routes, traffic from a level 1 router to a router in another area passes through the nearest level 1-2 router as its next hop. Consider the topology shown in Figure 20.

Figure 20: Example of Level 1 and Level 2 Routing



In this example, Router 4 in Area 1 considers Router 2 to be its next hop for interarea traffic, and Router 5 considers Router 3 to be its next hop for interarea traffic. Traffic from Router 4 to Router 8 passes through Router 2, requiring a total of five hops to the destination: Routers 2, 1, 3, 9, and 8. Similarly, five hops are required for traffic from Router 5 to Router 7.

Neither of these paths is optimal. For example, it would be shorter for traffic from Router 4 to take the four-hop path: Routers 5, 3, 9, and 8.

You can configure IS-IS to redistribute routes between the routing levels; this is sometimes known as route leaking between levels. The **redistribute isis ip** command enables you to specify a route filter (an access list) and the direction of leakage, as shown in the following example:

```
host1(config)#access-list leakList permit ip 100.0.0.0 0.255.255.255 any
host1(config)#router isis 1
host1(config-router)#redistribute isis ip level-1 into level-2 distribute-list leakList
host1(config-router)#redistribute isis ip level-2 into level-1 distribute-list leakList
```

When you issue the **redistribute isis ip** command and include the **route-map** keyword, you can use the map to set a route tag for a route redistributed from one IS-IS level to another. Make sure the route map you specify includes the **set tag** command that defines a tag value for the IS-IS routes to be redistributed. For details about configuring and using route maps, see *Route Maps* in *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*.

To redistribute IPv6 routes from one IS-IS level to another, use the **redistribute isis** command from within the IS-IS IPv6 address family.

redistribute isis

- Use to redistribute IS-IS IPv6 routes from level 1 to level 2 or from level 2 to level 1.
- Use the **route-map** keyword to specify the route map to be applied. You can use the route map to set a route tag for redistributed routes.
- Example

  host1(config-router-af)#**redistribute isis level-1 into level-2**

- Use the **no** version to stop redistribution of IPv6 routes between the specified levels.

redistribute isis ip

- Use to redistribute IS-IS IP routes from level 1 to level 2 or from level 2 to level 1.
- Specify one of the following:
  - Use the **distribute-list** keyword to specify the IP access list used to filter routes between levels. Issue the **access list** command to create a route filter to apply to the redistribution.
  - Use the **route-map** keyword to specify the route map to be applied. You can use the route map to set a route tag for redistributed routes.
- Example 1—Redistributes IS-IS IP routes between levels, filtered by an access list.

  host1(config-router)#**redistribute isis ip level-1 into level-2 distribute-list leakList**

- Example 2—Redistributes IS-IS IP routes between levels, filtered by a route map.

  host1(config-router)#**redistribute isis ip level-2 into level-1 route-map boston01**

- Use the **no** version to stop redistribution of IP routes between the specified levels.

Controlling Granularity of Routing Information

You can force the distribution of level 2 routing information to level 1 routers in other areas to improve the quality of the resulting routes, but at the cost of reduced scalability.

distribute-domain-wide

- Use to increase the granularity of routing information within a domain.
- Domainwide prefix distribution enables a routing domain running with both level 1 and level 2 IS-IS routers to distribute IP prefixes from level 2 to level 1 between areas.
- The major advantage for using domainwide prefix distribution is to improve the quality of the resulting routes within a domain by distributing more specific information.
- The major disadvantage of using domainwide prefix distribution is that it affects the scalability of IS-IS. When used, it increases the number of prefixes throughout the domain, causing increased memory consumption, transmission requirements, and computation requirements throughout the domain.
- A trade-off decision must be made between scalability and optimality.
- Issue this command from within the IS-IS IPv6 address family to increase the granularity of IPv6 routing information within a domain.
- Example

  host1(config-router)#**distribute-domain-wide**

- Use the **no** version to halt the distribution of routes from level 2 to level 1.

Configuring a Global Default Metric

You can use the **metric** command to specify a global default metric that applies to all active IS-IS interfaces. This command enables you to avoid configuring the desired metric on each active interface individually when you want all IS-IS interfaces to have the same metric, but a different value than the individual default of 10. The global default metric applies to both level 1 and level 2 interfaces unless you restrict it to one level.

If you have configured a nondefault metric on any IS-IS interface with the **isis metric** command, that value overrides the global default metric.

Reference bandwidth takes precedence over both individual and global default metrics. If you have configured a reference bandwidth, the **metric** command has no effect on interface metrics,

You can use the following commands to verify configuration of the global default metric:

- **show configuration**
- **show clns interface**
- **show clns protocol**
- **show isis database detail**

metric

- Use to apply the same default metric value to all active IS-IS interfaces. The command affects both IPv4 and IPv6 interfaces.
- Specify whether the command applies to level 1 or level 2 interfaces. If you do not specify a level, then the metric is applied to both level 1 and level 2 interfaces.
- Example

  host1(config-router)#**metric 50 level-1**

- Use the **no** version to remove the global default value. This restores the default value of 10 to all active IS-IS interfaces except for interfaces that have been individually configured with another metric value.

Configuring Metric Type

Extensions to IS-IS traffic engineering enable the use of bigger metrics. You can specify whether your router accepts, generates, or accepts and generates only old-style metrics, only new-style metrics, or both.

metric-style narrow

- Use to specify that the router generates and accepts only old-style TLV tuples.
- *Old-style TLVs* refers to TLVs having metrics with a narrow (six-bit) field with a value in the range 0–63. *New-style TLVs* refers to TLVs having metrics with a wider field, as provided for in current extensions to IS-IS traffic engineering.
- Use the **transition** option to *accept* old-style and new-style metrics; only old-style metrics are *generated*.
- Specify whether the command applies to level 1, level 2, or both.
- Example

  host1(config-router)#**metric-style narrow level-2**

- Use the **no** version to restore the default, which is to generate and accept only old-style TLVs with narrow (six-bit) metric fields.

metric-style transition

- Use to specify that the router generates and accepts both old-style and new-style TLV tuples.
- *Old style* refers to TLVs having metrics with a narrow (six-bit) field with a value in the range 0–63. *New style* refers to TLVs having metrics with a wider field, as provided for in current extensions to IS-IS traffic engineering.
- Specify whether the command applies to level 1, level 2, or both.
- Example

  host1(config-router)#**metric-style transition level-1**

- Issuing this command results in more resource usage than issuing the **metric-style narrow** or **metric-style wide** commands.
- Use the **no** version to restore the default, which is to generate and accept only old-style TLVs with narrow (six-bit) metric fields.

metric-style wide

- Use to specify that the router generates and accepts only new-style TLV tuples.
- *Old style* refers to TLVs having metrics with a narrow (six-bit) field with a value in the range 0–63. *New style* refers to TLVs having metrics with a wider field, as provided for in current extensions to IS-IS traffic engineering.
- Use the **transition** option to *accept* old-style and new-style metrics; only new-style metrics are *generated*.
- Specify whether the command applies to level 1, level 2, or both.
- Before you set a route tag for an IS-IS interface, you must issue the **metric-style wide** command to configure the router to generate and accept TLV type 135, which is a new-style tuple that contains the route tag.
- Example

  host1(config-router)#**metric-style wide level-1-2**

- Use the **no** version to restore the default, which is to generate and accept only old-style TLVs with narrow (six-bit) metric fields.

Setting the Administrative Distance

You can indicate the dependability of a routing information source by configuring the administrative distance for learned routes.

distance ip

- Use to configure the administrative distance for IS-IS learned routes.
- The distance indicates the dependability of a routing information source. A higher relative value indicates lower dependability. Preference is always given to the routes with smaller values.
- Select a value in the range 1–255. A value of 255 means discard the route.
- Example

  host1(config-router)#**distance ip 50**

- Use the **no** version to restore the default value, 115.

Configuring Default Routes

You can specify a default route within IS-IS routing domains. You can also suppress the installation of a default route to level 1-2 routers by level 1 routers.

Optionally, when you issue the **default-information originate** command and specify a route map, you can use the map to set a route tag for the default route. Make sure the route map you specify includes the **set tag** command, which defines a tag value for the default route within the IS-IS domain. For details about configuring and using route maps, see *Route Maps* in *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*.

default-information originate

- Use to generate a default route into an IS-IS routing domain.
- When you specify a route map with this command and the router has a route to 0.0.0.0 in the routing table, IS-IS originates an advertisement for 0.0.0.0 in its LSPs.
- When you do not specify a route map, the default route is advertised only in level 2 LSPs.
- If you specify a route map, you can use the map to set a route tag for the default route.
- For level 1 routing, look for the closest level 1-2 router to find the default route. The closest level 1-2 router is found by looking at the attach bit (ATT) in level 1 LSPs.
- The default value is disabled.
- Example1

  host1(config-router)#**default-information originate**

- Example 2

  host1(config-router)#**default-information originate route-map map3**

- Use the **no** version to disable the command.

suppress-default

- Use to prevent level 1 routers from automatically installing a default route to a level 1-2 router in order to reach destinations outside the area.
- Suppresses the level 1-2 router from indicating to level 1 routers that it can reach other areas. Consequently, the level 1 routers do not consider the level 1-2 router to be the nearest attached level 2 router and do not install default routes to it.
- This command is useful, for example, if you issue the distribute-domain-wide command, which causes the level 2 routes to be leaked into the level 1 area. The level 1 routers then have knowledge of the routes outside the area and will not need to rely on the nearest attached level 2 router for any unknown destination.
- Example

  host1(config-router)#**suppress-default**

- Use the **no** version to disable suppression of default routes.

Setting Router Type

You can specify whether the router behaves as an IS-IS station router, area router, or both.

is-type

- Use to configure the router to act as either a station router (level 1), an area router (level 2), or as both a station router and an area router (level-1-2).
- Always configure the type of IS-IS router.
- Level-1-2 is the default.
- Example

  host1(config-router)#**is-type level-2-only**

- Use the **no** version to restore the default value, level-1-2.

Summarizing Routes

You can summarize routes redistributed into IS-IS or within IS-IS by creating aggregate addresses for the routes. Use the **summary-address** command for IP routes and the **summary-prefix** command for IPv6 routes.

Optionally, you can set a route tag for an IS-IS aggregate (summary) address by including the **tag** keyword and a numeric tag value in the command.

summary-address
summary-prefix

- Use to create aggregate addresses of routes that are redistributed from other protocols in the routing table or distributed between level 1 and level 2 by a summary address. This process is called *route summarization*.
- A single summary address includes groups of addresses for a given level.
- Use the **summary-address** command for IP routes. Use the **summary-prefix** command for IPv6 routes.
- The metric value is used when the router advertises the summary address. When the metric value is not used, the value of the lowest cost route (the default) is used.
- This command reduces the size of the neighbor's routing table and improves stability because a summary advertisement depends on many more specific routes.
- A disadvantage of summary addresses is that other routes might have less information to calculate the optimal routing table for all individual destinations.
- Use the optional **tag** keyword to specify a tag value for an IS-IS summary address. The tag value must be a number in the range 1–4294967295.
- Example 1—For IP routes

  host1(config-router)#**summary-address 10.2.0.82 255.255.0.0 level-1-2 tag 34**

- Example 2—For IPv6 routes

  host1(config-router-af)#**summary-prefix 2001:2000::0/8 level-1 metric 10 tag 100**

- Use the **no** version to restore the default, the value of the lowest-cost route.

Avoiding Transient Black Holes

When you start or reload a transit router that is running both IS-IS and BGP, the router is temporarily unavailable to the routing domain. Other routers in that routing domain must select alternative paths to destinations that used the transit router. When the transit router becomes available again, the other routers soon select it again as the optimal path to those destinations.

The other routers select the transit router again before it has loaded the complete BGP routing table. Because the transit router does not yet have all the reachability information that is needed to reach some external destinations, traffic to destinations that were not learned by means of the IGP is dropped until the transit router has complete external reachability information again. This condition is known as a *transient black hole*.

You can use the overload bit to avoid these black holes. When the overload bit is set in the LSP header, other routers in the domain do not include the transit router in their SPF calculations and thus do not use that router for traffic forwarding.

When the transit router boots, it begins establishing adjacencies with its neighbors. As soon as it establishes an adjacency, it creates (or updates) its LSP, sets the overload bit in the LSP header, and transmits the LSP with the current neighbor information. By sending the updated LSP with the overload bit set immediately after forming the first adjacency, IS-IS reduces the convergence time across the network.

If IS-IS waits for all adjacencies to be up before it sends the updated LSP with the overload bit set, the other routers in the domain still have the transit router's old LSP and continue to forward transit traffic to the transit router until all adjacencies are formed. That traffic is lost.

Waiting for BGP Convergence

When BGP converges, the transit router again has the reachability information it needs to forward traffic to destinations that are not directly connected. Typically, you then want the transit router to clear the overload bit in its LSP and retransmit the LSP to inform the other routers in the domain that they can use it as a transit router.

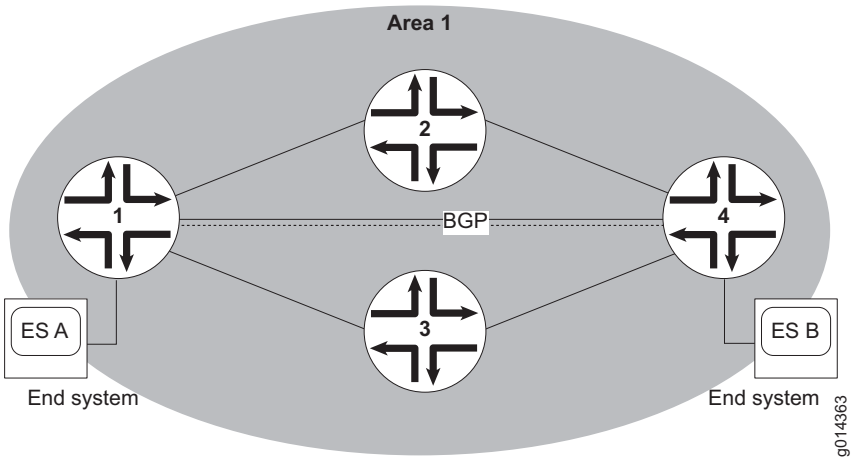
BGP is assumed to have converged when all of the following conditions have been met:

- 90 percent of BGP peers have reached an established state,
- The transit router has received an end-of-rib marker from all IBGP peers that advertise the graceful-restart capability.
- The average rate of learning new routes has dropped to a low level.

Example Topology

Figure 21 shows a sample topology where source end system A is communicating with destination end system B through routers 1, 2, 3, and 4.

Figure 21: Transit Router Topology



The transit routers, 2 and 3, learn the route to B from BGP. In a steady state environment, the BGP routing tables are synchronized on all the transit routers.

Suppose the traffic forwarding path is currently A –> 1 –> 2 –> 4 –> B. If transit router 2 goes down, the network converges to the alternative path, A –> 1 –> 3 –> 4 –> B. Because transit router 3 already had synchronized its BGP routing tables, traffic forwarding continues without delay.

When transit router 2 reloads, it establishes adjacencies with routers 1 and 4, and sends out its LSP advertising its neighbors. While router 2 begins to synchronize its BGP routes, the network reconverges to the original path of A –> 1 –> 2 –> 4 –> B. Traffic from A to B is forwarded to router 2. Typically, BGP has not converged by then, so router 2 does not have the BGP route that it needs to forward the traffic, and drops the packets, resulting in a black hole until the BGP convergence is complete.

You can avoid this black hole by configuring the overload bit for the transit router. In this circumstance, router 2 sends out its LSP with the overload bit set in its header as soon as it reloads, before it establishes all adjacencies. The bit set in the header indicates to all the routers in the domain that router 2 is overloaded and not to use it to carry transit traffic. The forwarding path continues to be the alternative path, A –> 1 –> 3 –> 4 –> B, even after router 2 reloads.

When BGP convergence is complete at router 2, router 2 sends out a new LSP with the overload bit cleared. The other routers then include router 2 in their SPF calculations and revert to the original path, of A –> 1 –> 2 –> 4 –> B.

Suppression for IS-IS Graceful Restart

When graceful restart is configured on the transit router, the black hole avoidance feature is suppressed.

Configuration

You can configure the transit router to set the overload bit when it reloads and to then wait for a specified interval before it clears the bit and retransmits its LSP. More commonly, and to avoid the transient black holes, you configure the transit router to wait for BGP to converge, and specify an interval it waits after convergence before it clears the bit and retransmits its LSP.

set-overload-bit

- Use to configure the router to set the overload bit in the header of its nonpseudonode LSPs.
- While the overload bit is set, other routers in the domain do not include this router in their shortest-path-first (SPF) calculations. Consequently, the other routers do not detect any paths through this router and do not forward traffic through this router. However, IP prefixes directly connected to this router are still reachable. When the bit is cleared, the router is again included in SPF calculations.
- You can set the overload bit for a number of reasons, including the following:
  - To prevent traffic through the router from disappearing into transient black holes.
  - To reduce routing table inaccuracies caused by router problems such as memory shortage.
  - To prevent real traffic from flowing through a router to an IS-IS network, such as might be the case for a test router connected to a production network.
- Use the **on-startup** keyword to set the overload bit when the router reboots and to specify a period in seconds that IS-IS waits after the reboot before it clears the overload bit.
- Use the **on-startup wait-for-bgp** keywords to instruct IS-IS to set the overload bit when the router reboots and then wait until BGP has completed convergence after the reload before IS-IS clears the overload bit. You can specify a maximum interval that IS-IS waits for BGP notification. When that interval passes, IS-IS clears the overload bit. If you do not specify an interval, IS-IS waits a default 600 seconds and then clears the overload bit.
- If you issue the **on-startup** keyword but do not issue the **wait-for-bgp** keyword, then you must specify the number of seconds that IS-IS waits after a reload before clearing the overload bit.
- If you issue both the **on-startup** keyword and the **wait-for-bgp** keyword, you cannot specify a time interval for **on-startup** but can optionally do so for **wait-for-bgp**.
- By default, the overload bit is not set.

- Example 1

  host1(config-router)#**set-overload-bit**

- Example 2

  host1(config-router)#**set-overload-bit on-startup 900**

- Example 3

  host1(config-router)#**set-overload-bit on-startup wait-for-bgp 450**

- Use the **no** version to disable the setting.

Ignoring LSP Errors

You can configure the router to ignore rather than purge LSPs received with errors.

ignore-lsp-errors

- Use to enable your router to ignore rather than purge IS-IS LSPs that are received with internal checksum errors.
- Under normal conditions, the IS-IS protocol definition requires that received LSPs with incorrect data link checksums are to be purged by the receiver. This causes the LSP initiator to regenerate LSPs. If a network link causes data corruption while still delivering LSPs with correct data link checksums, a continuous cycle of regenerating and purging LSPs may result. This can render the network nonfunctional. Enabling this command prevents this continuous cycle from occurring because LSPs are ignored rather than purged.
- Example

  host1(config-router)#**ignore-lsp-errors**

- Use the **no** version to disable the function.

Logging Adjacency State Changes

You can configure the router to log messages that track when adjacencies change state between up and down.

log-adjacency-changes

- Use to generate log messages that track IS-IS adjacency state changes (up or down).
- The default is not to log adjacency state changes.
- Recommended for monitoring large networks.
- The system logs messages by using the router error message facility.
- Specify the minimum severity (0–7) or verbosity (low, medium, high) of this log category's messages.

- You can also use the **system log** command to generate the desired log messages.
- Example

  host1(config-router)#**log-adjacency-changes severity 3 verbosity low**

- Use the **no** version to disable the function.

Configuring LSP Parameters

You can specify the following parameters for LSPs:

- Maximum transmission unit (MTU)
- Transmission rate
- Generation rate
- Maximum lifetime

lsp-gen-interval

- Use to set the minimum interval rate that LSPs are generated on a per-LSP basis.
- You can set an interval value in the range 0–120 seconds.
- The default interval value is 5 seconds. When a link is changing state at a high rate, the default value limits the signaling of the changing state to once every 5 seconds. Because the generation of an LSP may cause all routers in the area to perform the SPF calculation, controlling this interval can have an areawide effect.
- When you raise this interval, you reduce the load on the network imposed by a rapidly changing link.
- Example

  host1(config-router)#**lsp-gen-interval level-2 30**

- Use the **no** version to restore the default value, 5.

lsp-mtu

- Use to specify the MTU LSP size in bytes. The size must be less than or equal to the smallest MTU of any link in the area.
- Use this command to limit the size of LSPs generated by this router only. The router can receive LSPs of any size up to the maximum.
- You can set the value in the range 128–9180.
- The default LSP MTU value is 1497.
- When a very large amount of information is generated by a single router, we recommend that you increase the LSP MTU. However, the default MTU is usually sufficient.

- If the MTU of a link is lowered to less than 1500 bytes, the LSP MTU must be lowered accordingly on each router in the network. If this is not done, routing may become unpredictable.
- Example

  host1(config-router)#**lsp-mtu 1500**

- Use the **no** version to restore the default value, 1497.

lsp-refresh-interval

- Use to set the LSP rate at which locally generated LSPs are periodically transmitted.
- The refresh interval determines the rate at which the router software periodically transmits the route topology information that it originates. These transmissions refresh the link-state information, reaffirming that the router is still up and that the link-state information in the LSP is still valid.
- You can set the interval rate in the range 1–65535 seconds; the default is 900 seconds.
- LSPs must be periodically refreshed before their lifetimes expire. The refresh interval must be less than the LSP lifetime specified by **max-lsp-lifetime**.
- In the unlikely event that link stage database corruption is undetected, reducing the refresh interval reduces the amount of time that the corruption can persist.
- Increasing the interval reduces the link utilization caused by the flooding of refreshed packets.
- Example

  host1(config-router)#**lsp-refresh-interval 1000**

- Use the **no** version to restore the default value, 900 seconds.

max-lsp-lifetime

- Use to set the maximum time that LSPs persist without being refreshed.
- You can select a maximum time in the range 1–65535 seconds.
- The default value is 1200 seconds (20 minutes).
- You might need to adjust the maximum LSP lifetime if you change the LSP refresh interval with the **lsp-refresh-interval** command. The maximum LSP lifetime must be greater than the LSP refresh interval.
- Example

  host1(config-router)#**max-lsp-lifetime 1500**

- Use the **no** version to restore the default value, 1200 seconds.

Specifying the SPF Interval

You can configure how often the router performs the shortest-path-first (SPF) calculation. IS-IS runs SPF calculations in response to any change in its link-state database. Because SPF calculation is processor intensive, increasing the SPF interval reduces the processor load of the router, but can slow down the rate of convergence.

Topology changes in a network cause all routers involved in the change to regenerate their LSDB and flood new LSPs throughout the network. Therefore, a router that receives a new LSP is likely to receive more LSPs in the following seconds. An immediate response to a given change is going to miss the subsequent topology changes and spend CPU time. When many changes are taking place, a slower response to each change makes more sense.

IS-IS enables the router to respond quickly to an isolated network event, but to slow the response exponentially when many triggering events are taking place in rapid succession. SPF calculations are performed at exponentially increasing intervals until the maximum interval set by the **spf-interval** command is reached.

The first SPF calculation is performed immediately when the LDSB changes. If another calculation-triggering event occurs, the router waits 1 second before performing the SPF calculation. If another event occurs, the router waits 2 seconds before performing the SPF calculation. The interval between a triggering event and the corresponding SPF calculation continues to increase exponentially: 4 seconds, 8 seconds, 16 seconds, and so on. When the maximum configured interval is reached, the interval reverts back to immediate response mode for the next triggering event.

If no calculation-triggering network events have occurred by the end of any given back-off interval, the router reverts back to immediate response mode.

spf-interval

- Use to set the maximum interval between SPF calculations.
- You can select an interval value in the range 0–120 seconds.
- The default value is 5 seconds.
- If you do not specify **level-1** or **level-2**, the interval applies to both level 1 and level 2.
- SPF calculations are performed only when the topology of the area changes. They are not performed when external routes change.
- Example

  host1(config-router)#**spf-interval level-2 30**

- Use the **no** version to restore the default value, 5 seconds.

Defining the SPF Route Calculation Level

The IS-IS protocol uses the Dijkstra algorithm to compute IP node metrics when a change occurs within the IS-IS network. This calculation results in the IS-IS router containing a shortest-path tree (SPT) that maps the shortest path to each node in the IS-IS network.

By default, the router uses a partial route calculation (PRC) SPF to determine the next hop (when required). This partial computation occurs when the router receives link-state PDUs (LSPs) with only changes relating to IP prefixes (for example, the addition of a new IP prefix, change in attributes of an existing IP prefix, or the removal of an existing IP prefix).

Because changes in IP prefixes happen more frequently than other events, using the PRC SPF results in faster IS-IS convergence and saves router resources. However, you can also specify that the router always use full SPF, recalculating the entire SPT, when resolving any IS-IS state changes.

full-spf-always

- Use to enable and disable full SPF calculations for IS-IS network changes.
- Example

  host1(config-router)#**full-spf-always**

- Use the **no** version to restore partial route calculation (PRC) mode for SPF calculations.

Setting CLNS Parameters

You can specify transmission rates for ES and IS hello packets, the period for which the router considers ES and IS hello packets to be valid, and name-to-network service access point mappings.

clns configuration-time

- Use to specify the rate (in seconds) at which ES hello and IS hello packets are sent.
- The hello packet recipient creates an adjacency entry for the router that sent it. If the next hello packet is not received within the specified interval, the adjacency times out, and the adjacent node is determined to be unreachable.
- In most cases, leave these parameters at their default value, which is 10 seconds.
- Example

  host1(config)#**clns configuration-time 240**

- Use the **no** version to restore the default value, 10 seconds.

clns holding-time

- Use to enable sender of an ES hello or IS hello packet to specify the length of time you consider the information in these packets to be valid.
- In most cases, leave these parameters at their default value, which is 30 seconds.
- Example

  host1(config)#**clns holding-time 900**

- Use the **no** version to restore the default value, 30 seconds.

clns host

- Use to define a name-to-NSAP mapping that can then be used with commands requiring NSAPs.
- The default is that no mapping is defined.
- The assigned NSAP name is displayed, where applicable, in **show** commands.
- The first character can be either a letter or a number.
- This command is generated after all other CLNS commands when the configuration file is parsed. As a result, the NVRAM version of the configuration cannot be edited to specifically change the address defined in the original **clns host** command. You must specifically change any commands that refer to the original address. This affects commands that accept names, such as the **net** command.
- Enables dynamic resolution of hostnames to system IDs (within the NSAP address). The hostname mapping is sent in the LSPs within the Dynamic Hostname type-length-value (TLV type 137). Display the TLV by issuing the **show isis database detail** command.
- Use the **show hosts** command to display the mapping.
- Example

  host1(config)#**clns host**

- Use the **no** version to restore the default state of no mapping defined.

Setting the Maximum Parallel Routes

You can configure how many parallel routes IS-IS supports to a destination.

maximum-paths

- Use to control the maximum number of parallel routes IS-IS can support.
- You can select a number of routes (or paths) in the range 1–16.
- The default number for IS-IS is 4 paths.
- Example

  host1(config-router)#**maximum-paths 12**

- Use the **no** version to restore the default value, 4.

Configuring a Virtual Multiaccess Network

You can specify that interfaces within a given mesh group act as a virtual multiaccess network.

isis mesh-group

- Use when you want interfaces in the same mesh group to act as a virtual multiaccess network.
- LSPs seen on one interface in a mesh group are not flooded to another interface in the same mesh group.
- Example

  host1(config-if)#**isis mesh-group blocked**

- Use the **no** version to disable the feature.

Configuring Table Maps

You can use the **table-map** command to apply a specified route map as a policy filter on an IS-IS route before the route is installed in the routing table. The route map you apply must contain one or more **set** commands to modify route attributes.

table-map

- Use to apply a policy to modify distance, level, metric, metric type, origin, preference, route type, or tag values of IS-IS routes about to be added to the IP routing table.
- The router applies the new route map to all routes currently in the forwarding table and those about to be installed in the forwarding table.
- If any previously redistributed routes are changed as a result of applying the route map, the router redistributes these routes again with the changes caused by the route map.
- The router removes from the forwarding table any old routes that are now disallowed by the specified route map.
- Issue the command from the IS-IS IPv6 address family to apply a specified route map as a policy filter on an IS-IS IPv6 route before the route is installed in the routing table. IS-IS IPv6 supports only a single table map.
- Example

  The following commands apply a policy (route map) named metricTypeExt to modify the metric type of IS-IS routes configured with a route tag value of 33.

  host1(config)#**route-map metricTypeExt permit 5**
  host1(config-route-map)#**match tag 33**
  host1(config-route-map)#**set metric-type external**
  host1(config-route-map)#**exit**
  host1(config)#**router isis marketing**
  host1(config-router)#**table-map metricTypeExt**
  host1(config-router)#**exit**
  host1(config)#**exit**

- Use the **no** version to halt application of the route map.

Configuring Graceful Restart

To enable IS-IS graceful restart (also known as nonstop forwarding, or NSF) on the router, you must first issue the **nsf ietf** command (in Router Configuration mode). You can then configure one or more optional timing parameters for graceful restart on the router.

To enable IS-IS graceful restart and configure optional graceful restart parameters:

1. Specify a previously configured IS-IS routing process to access Router Configuration mode. (For information about enabling IS-IS on the router, see *Enabling IS-IS for IP Routing* on page 326.)

   host1(config)#**router isis engineering**
   host1(config-router)#

2. Enable the IS-IS graceful restart mechanism for the router.

   host1(config-router)#**nsf ietf**

3. (Optional) Configure one or more of the following timing parameters for the restarting router:

   - Set the maximum time in seconds that the router waits before completing the restart process.

     host1(config-router)#**nsf interface wait 30**

   - Set the time interval in seconds between restart requests sent by the router.

     host1(config-router)#**nsf t1 interval 60**

   - Set the number of times that the router resends unacknowledged restart requests.

     host1(config-router)#**nsf t1 retry-times 3**

   - Set the maximum time in seconds that the router waits for the LSP database to synchronize. You must configure this parameter separately for each IS-IS level at which the router operates.

     host1(config-router)#**nsf t2 level-1 70**
     host1(config-router)#**nsf t2 level-2 50**

   - Set the maximum time in seconds that the restarting router waits before setting the overload bit to indicate that the graceful restart operation has failed. You can use either of the following methods:

     - Set the wait time manually to the specified number of seconds.

       host1(config-router)#**nsf t3 manual 80**

     - Specify that router obtain the wait time from neighboring IS-IS routers to which it has active adjacencies.

       host1(config-router)#**nsf t3 adjacency**

4. (Optional) Issue the **show isis nsf** command from Privileged Exec mode to verify the graceful restart configuration.

   ```
   host1(config-router)#exit
   host1(config)#exit
   host1#show isis nsf
   ```

   For more information about monitoring graceful restart, see the **show isis nsf** command description in *Monitoring IS-IS Parameters* on page 373 and the **show clns neighbors detail** command description in *Displaying CLNS* on page 385.

nsf ietf

- Use to enable the IS-IS graceful restart mechanism on the router.
- Graceful restart, which is also known as nonstop forwarding (NSF), allows an IS-IS router to restart with minimal routing disruption to the network.
- Example

  ```
  host1(config-router)#nsf ietf
  ```

- Use the **no** version to restore the default state for IS-IS graceful restart on the router, disabled.

nsf interface wait

- Use to specify the maximum amount of time, in seconds, that an IS-IS process on a restarting router waits for all interfaces with IS-IS adjacencies to come up before completing the restart process.
- You can specify a value in the range 5–120 seconds.
- Example

  ```
  host1(config-router)#nsf interface wait 45
  ```

- Use the **no** version to restore the default maximum wait time, 10 seconds.

nsf t1

- Use to specify either the interval between IS-IS restart requests sent by the router or the number of times that the router resends unacknowledged restart requests.
- Use the **interval** keyword to specify the number of seconds, in the range 5–120, between restart requests sent by the router on a particular IS-IS interface to neighboring IS-IS routers in the network.
- Use the **retry-times** keyword to specify the number of times, in the range 1–3, that the router tries to resend unacknowledged restart requests.
- The restarting router stops sending restart requests after it receives an acknowledgment.

- Example 1

  host1(config-router)#**nsf t1 interval 90**

- Example 2

  host1(config-router)#**nsf t1 retry-times 2**

- Use the **no** version to restore the default time interval, 5 seconds, or the default number of retry attempts, 1.

nsf t2

- Use to specify the maximum amount of time, in seconds, that a restarting router waits for the LSP database to synchronize.
- You must configure independent instances of the T2 timer for each IS-IS level at which the router operates. This requirement means that for a level 1-2 router, you must issue this command twice: first to configure the timer for level 1, and a second time to configure it for level 2.
- Use either the **level-1** keyword to set the T2 wait time for level 1 routing, or the **level-2** keyword to set the wait time for level 2 routing.
- You can specify a value in the range 5–120 seconds for each level.
- Example—Configures the T2 wait time for a level 1-2 IS-IS router

  host1(config-router)#**nsf t2 level-1 70**
  host1(config-router)#**nsf t2 level-2 50**

- Use the **no** version to restore the default T2 wait time, 30 seconds.

nsf t3

- Use to specify the maximum amount of time, in seconds, that the restarting router waits before setting the overload bit.
- The restarting router sets the overload bit to indicate that the LSP database has not been synchronized and the IS-IS graceful restart operation has failed.
- You must use one of the following methods to set the T3 wait time:
  - Use the **manual** keyword and a value in the range 5–120 seconds to set the T3 wait time manually.
  - Use the **adjacency** keyword to specify that the restarting router should obtain its T3 wait time from neighboring IS-IS routers that have active adjacencies to this router. This option sets the wait time to the minimum of the remaining times specified in the restart TLVs contained in the hello packets that the router receives from its neighbors.
- Example1

  host1(config-router)#**nsf t3 manual 120**

- Example 2

  host1(config-router)#**nsf t3 adjacency**

- Use the **no** version to restore the default T3 wait time, 30 seconds.

Summary Example

```
host1(config)#router isis floor12
host1(config-router)#net 47.0010.0000.0000.0000.0001.0001.1111.1111.1111.00
host1(config-router)#exit
host1(config)#interface atm 0/1
host1(config-if)#ip router isis floor12 tag 24
host1(config-if)#isis mesh-group blocked
host1(config-if)#exit
host1(config)#interface atm 1/0
host1(config-if)#ip router isis floor12
host1(config-router)#distribute-domain-wide
host1(config-router)#distance 100 ip
host1(config-router)#default-information originate route-map 9
host1(config-router)#is-type level-1-2
host1(config-router)#summary-address 10.2.0.82 255.255.0.0 level-1-2 tag 90
host1(config-router)#set-overload-bit on-startup wait-for-bgp 450
host1(config-router)#ignore-lsp-errors
host1(config-router)#log-adjacency-changes
host1(config-router)#lsp-mtu 1500
host1(config-router)#lsp-refresh-interval 1000
host1(config-router)#lsp-gen-interval level-2 30
host1(config-router)#max-lsp-lifetime 1500
host1(config-router)#spf-interval level-2 30
host1(config-router)#maximum-paths 16
host1(config-router)#redistribute static ip route-map 5
host1(config-router)#nsf ietf
host1(config-router)#nsf t2 level-1 70
host1(config-router)#nsf t2 level-2 50
host1(config-router)#nsf t3 adjacency
host1(config-router)#exit
host1(config)#clns configuration-time 120
host1(config)#clns holding-time 600
```

Configuring IS-IS for MPLS

IS-IS has several commands to provide support for MPLS. See *JUNOSe BGP and MPLS Configuration Guide, Chapter 2, Configuring MPLS*, for a detailed discussion of MPLS. If you configure your tunnel with the **tunnel mpls autoroute announce isis** command, MPLS attempts to register the tunnel endpoint with IS-IS. You must enable this registration with IS-IS by issuing the **mpls traffic-eng** command.

When you configure a node as the downstream endpoint of an LSP, you must provide a stable interface as the router ID for the endpoint. Typically you select a loopback interface because of its inherent stability. Use the **mpls traffic-eng router-id** command to specify the router ID.

By default, IS-IS always uses the MPLS tunnel to reach the MPLS endpoint. Best paths determined by IS-IS SPF calculations are not considered. You can enable the consideration of best paths by issuing the **mpls spf-use-any-best-path** command. As a result, IS-IS considers metrics for IGP paths and the tunnel metric, and might forward traffic along a best path, through the MPLS tunnel, or both.

Several **show** commands enable monitoring of MPLS information. See *Monitoring IS-IS* on page 372 for more information.

MPLS traffic engineering requires that IS-IS generate the new-style TLVs that enable wider metrics. Use the **metric-style wide** command to generate the new-style TLVs. If you are using some IS-IS routers that still do not understand the new-style TLVs, use the **metric-style transition** command. See *Extensions for Traffic Engineering* on page 317 and *Configuring Global IS-IS Parameters* on page 342 for detailed information about using the **metric-style** commands.

mpls spf-use-any-best-path

- Use to enable SPF calculations to consider the IGP (IS-IS) best paths as well as the MPLS tunnel for forwarding traffic to the MPLS endpoint.
- By default, the MPLS tunnel is always selected for traffic to the tunnel endpoint; IGP paths are not considered. For traffic beyond the endpoint, the tunnel is considered equally with any other path.
- Example

  host1(config-router)#**mpls spf-use-any-best-path**

- Use the **no** version to disable the use of IGP best paths.

mpls traffic-eng

- Use to enable flooding of MPLS traffic engineering link information into the specified IS-IS level. Flooding is disabled by default.
- Example

  host1(config-router)#**mpls traffic-eng level-1**

- Use the **no** version to disable flooding.

mpls traffic-eng router-id

- Use to specify a very stable interface to be used as a router ID for MPLS traffic engineering. Typically you specify a loopback interface to provide the greatest stability, because this is flooded to all nodes. The interface acts as the destination node for tunnels originating at other nodes.
- Example

  host1(config-router)#**mpls traffic-eng router-id loopback 0**

- Use the **no** version to remove the interface as a router ID.

Using IS-IS Routes for Multicast RPF Checks

You can use the **ip route-type** command to specify whether IS-IS routes are available for only unicast forwarding protocols or only multicast reverse-path forwarding (RPF) checks. Routes available for unicast forwarding appear in the unicast view of the routing table, whereas routes available for multicast RPF checks appear in the multicast view of the routing table.

ip route-type

- Use to specify whether IS-IS routes are available only for unicast forwarding, only for multicast reverse-path forwarding checks, or for both.
- Use the **show ip route** command to view the routes available for unicast forwarding.
- Use the **show ip rpf-routes** command to view the routes available for multicast reverse path forwarding checks.
- By default, IS-IS routes are available for both unicast forwarding and multicast reverse path forwarding checks.
- Example

  host1(config)#**router isis**
  host1(config-router)#**ip route-type unicast**

- Use the **no** version to restore the default value, both.

Configuring the BFD Protocol for IS-IS

The **isis bfd-liveness-detection** command configures the Bidirectional Forwarding Detection (BFD) protocol for IS-IS. The BFD protocol uses control packets and shorter detection time limits to more rapidly detect failures in a network. Also, because they are adjustable, you can modify the BDF timers for more or less aggressive failure detection.

When you issue the **isis bfd-liveness-detection** command on an IS-IS peer, the peer establishes BFD liveness detection with all BFD-enabled IS-IS peers. When the local peer receives an update from a remote IS-IS peer—if BFD is enabled and if the session is not already present—the local peer attempts to create a BFD session to the remote peer.

Each adjacent pair of peers negotiates an acceptable transmit interval for BFD packets. The negotiated value can be different on each peer. Each peer then calculates a BFD liveness detection interval. When a peer does not receive a BFD packet within the detection interval, it declares the BFD session to be down and purges all routes learned from the remote peer.

NOTE: Before the router can use the **isis bfd-liveness-detection** command, you must specify a BFD license key. To view an already configured license, use the **show license bfd** command.

For general information about configuring and monitoring the BFD protocol, see *JUNOSe IP Services Configuration Guide, Chapter 5, Configuring BFD*.

isis bfd-liveness-detection

- Use to enable BFD (bidirectional forwarding detection) and define BFD values to more quickly detect IS-IS data path failures.
- The peers in an IS-IS adjacency use the configured values to negotiate the actual transmit intervals for BFD packets.
  - You can use the **minimum-transmit-interval** keyword to specify the interval at which the local peer proposes to transmit BFD control packets to the remote peer. The default value is 300 milliseconds.
  - You can use the **minimum-receive-interval** keyword to specify the minimum interval at which the local peer must receive BFD control packets from the remote peer. The default value is 300 milliseconds.
  - You can use the **minimum-interval** keyword to specify the same value for both of those intervals. Configuring a minimum interval has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value. The default value is 300 milliseconds.
- You can use the **multiplier** keyword to specify the detection multiplier value. The calculated BFD liveness detection interval can be different on each peer. The multiplier value is roughly equivalent to the number of packets that can be missed before the BFD session is declared to be down. The default value is 3.
- For details on liveness detection negotiation, see *Negotiation of the BFD Liveness Detection Interval* section in *JUNOSe IP Services Configuration Guide, Chapter 5, Configuring BFD*.
- You can change the BFD liveness detection parameters at any time without stopping or restarting the existing session; BFD automatically adjusts to the new parameter value. However, no changes to BFD parameters take place until the values resynchronize with each peer.
- Example

  host1(config)#**isis bfd-liveness-detection minimum-interval 800**

- Use the **no** version to disable BFD on the IS-IS interface.

Disabling the IS-IS Protocol

The **protocol shutdown** command disables the IS-IS protocol but does not remove any IS-IS configuration. In addition, even though the router does not participate in IS-IS routing after you issue the **protocol shutdown** command, you can continue to configure IS-IS.

Issuing the **protocol shutdown** command:

- Clears the LSP database
- Removes all IS-IS routes in the routing information database (RIB)
- Deletes all adjacencies with the IS-IS instance

NOTE: Rebooting the router does not affect the state of the IS-IS protocol.

protocol shutdown

- Use to disable the IS-IS protocol without removing the IS-IS configuration.
- Example

  host1(config-router)#**protocol shutdown**

- Use the **no** version to reenable the IS-IS protocol.

Monitoring IS-IS

The CLI has commands available for monitoring IS-IS parameters and CLNS parameters.

System Event Logs

To troubleshoot and monitor IP, use the following system event logs:

- isisAdjChange—IS-IS adjacency up or down events
- isisAdjPackets—IS-IS adjacency hello packets
- isisBfdEvents—IS-IS interactions with BFD
- isisChecksumErr—IS-IS checksum errors
- isisGeneral—IS-IS system notifications
- isisHelloGeneral—IS-IS system notifications
- isisHelloPackets—IS-IS hello packets
- isisipv6Log—IS-IS IPv6 notifications
- isisLdpEvents—IS-IS interactions with LDP
- isisLocalUpdate—IS-IS local LSP packets
- isisMplsTeAdvertisements—IS-IS MPLS traffic engineering advertisements
- isisMplsTeEvents—IS-IS MPLS traffic engineering
- isisNsfEvents—IS-IS nonstop forwarding events during warm starts
- isisProtocolErr—IS-IS protocol errors
- isisSnpPackets—IS-IS complete sequence numbers PDU (CSNP) and partial sequence numbers PDU (PSNP) packets
- isisSpfEvents—IS-IS Shortest Path First (SPF)

- isisSpfStatistics—IS-IS SPF timing and statistic data
- isisSpfTriggers—IS-IS SPF triggering
- isisUpdate Packets—IS-IS LSP packets sent or received

For more information about using event logs, see the *JUNOSe System Event Logging Reference Guide*.

Monitoring IS-IS Parameters

You can monitor the IS-IS link-state database and IS-IS debug information. Use the commands in this section to:

- Display router information.
- Display information about SPF calculations.
- Monitor IS-IS summary address information.
- Display debug information.
- Display host.
- Display information about MPLS tunnels.
- Clear adjacencies.
- Display paths to intermediate systems.
- Display information about the settings for IS-IS graceful restart.

You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. See *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface*, for details.

clear isis adjacency

- Use to remove entries from the adjacency database.
- Specify a hostname or the system ID of a neighbor to clear only adjacencies with that neighbor.
- Specify no options to remove all adjacencies from the database.
- Example

  host1#**clear isis adjacency**

- There is no **no** version.

debug isis

- Use to obtain debug-related information about certain parameters.
- This command manipulates the same log as the Global Configuration **log** commands.
- You can select from these parameters:
  - **adj-packets**—IS-IS adjacency-related packets
  - **mpls traffic-eng advertisements**—MPLS traffic-engineering agent advertisements
  - **mpls traffic-eng agents**—MPLS traffic-engineering agents
  - **snp-packets**—IS-IS CSNP/PSNP packets
  - **spf-events** —IS-IS Shortest Path First events
  - **spf-statistics**—IS-IS SPF timing and statistic data
  - **spf-triggers**—IS-IS SPF triggering events
  - **update-packets**—IS-IS update-related packets
- Example

  host1#**debug isis adj-packets**

- Use the **no** version to disable debugging display.

show hosts

- Use to display the name-to-NSAP mappings defined with the **clns host** command.
- Field descriptions
  - Static Host Table
    - name—Name assigned to the host
    - ip address—Host IP address
    - type—Type of host
    - username—Username necessary to access the host
    - password—Password necessary to access the host
  - Clns Host Alias Table
    - name—Name of the host alias
    - area address—Area address of the host alias
    - system ID—Six-byte value of the host alias
    - type—Type of host alias
- Example

```
host1:abc#show hosts
Static Host Table
-----------------
name   ip address   type   username    password
----   ----------   ----   ---------   --------
jkk    10.10.0.73   ftp    anonymous   null
```

```
Clns Host Alias Table
---------------------
name  area address                       system ID         type
----- ------------------------------- ----------------- ------
fred  47.0005.80FF.F800.0000.0001.0001 0000.0000.0011.00 static
karen 47.0005.80FF.F800.0000.0001.0001 0000.0000.0012.00 static
```

show isis database

- Use to display IS-IS link-state database information.
- Request specific **show isis database** statistics by selecting from these options:
  - *lspid*—Link-state protocol ID in form xxxx.xxxx.xxxx.yy-zz
  - *hostname*—Link-state database information for the specified hostname
  - **detail**—Detailed link-state database information; if this option is not specified, a summary display is provided
  - **l1**—Level 1 routing link-state database
  - **l2** —Level 2 routing link-state database
  - **level-1**—Level 1 routing link-state database
  - **level-2**—Level 2 routing link-state database
- Each option can be entered in an arbitrary string within a single command entry.
- Field descriptions
  - LSPID—LSP identifier
  - LSP Seq Num—Sequence number for the LSP. Enables other routers to determine if they have received the latest information from source.
  - LSP Checksum—Checksum of the LSP packet
  - LSP Holdtime—Number of seconds that the LSP remains valid
  - ATT—Attach bit; indicates that the router is a level 2 router and can reach other areas
  - P—P bit; detects whether intermediate system is capable of area partition repair
  - OL—Overload bit; determines whether intermediate system is congested
  - Area Address—Area addresses that can be reached from the router
  - NLPID—ISO network layer protocol identifier
  - IP Address—IP address of the interface
  - Hostname—Hostname of the router
  - Router ID—ID configured on the router
  - Metric —Metric that indicates either of the following costs:
    - Cost of adjacency between the originating router and the advertised neighbor
    - Cost between the advertising router and the advertised destination

- IPv4 Interface Address—Address of the interface
- IPv4 Neighbor Address—Address of a neighbor
- Maximum link bandwidth—Bandwidth capacity of the link in bits per second
- Reservable link bandwidth—Amount of bandwidth reservable on the link (whether reserved or not)
- Unreserved bandwidth—Amount of bandwidth available for reservation on the link
- TE default metric—Traffic engineering default metric value
- Tag value(s)—Route tag assigned to the IS-IS interface, if configured

- Example 1

```
host1#show isis database
IS-IS Level-1 Link State Database
LSPID LSP    Seq Num     LSP Checksum LSP Holdtime ATT/P/OL
0000.0000.004E.00-00  0x000013F5   0x8BAA 1198         0/0/0
0000.0000.3333.00-00* 0x0000020F   0xEA1E 1199         0/0/0
0000.0000.3333.02-00  0x00000007   0x8C30 1199         0/0/0
0000.0000.7500.00-00  0x0000308D   0x5EDF 1198         0/0/0
0090.1A00.B000.00-00  0x00000011   0xB082 1195         1/0/0
0090.1A00.C000.00-00  0x0000005F   0x9860 1196         0/0/0

IS-IS Level-2 Link State Database
LSPID LSP    Seq Num     LSP Checksum LSP Holdtime ATT/P/OL
0000.0000.004E.00-00  0x00001355   0x0DA7 1198         0/0/0
0000.0000.3333.00-00* 0x00000257   0x566B 1199         0/0/0
0000.0000.3333.02-00  0x00000007   0x8C30 1199         0/0/0
0000.0000.7500.00-00  0x00003315   0x3627 1198         0/0/0
0010.7B36.5FF7.00-00  0x00000BAF   0x187A 1183         0/0/0
0090.1A00.B000.00-00  0x00000016   0xD624 1195         1/0/0
0090.1A00.C000.00-00  0x00000071   0x9358 1196        0/0/0
```

- Example 2

```
host1#show isis database detail
LSPID LSP    Seq Num     LSP Checksum LSP Holdtime ATT/P/OL
boston.00-00*0x000001160x4760 6551/0/0
  Area Address: 47.0005.80FF.F800.0000.0000.0004
  NLPID:       0x81 0xcc
  IP Address:  10.1.1.1
  Hostname: boston
  Router ID:  10.1.1.1
  Metric: 10 IS newyork.00
    IPv4 Interface Address:  10.1.1.1
    IPv4 Neighbor Address:   10.1.1.2
  Metric: 10 IS washington.00
    IPv4 Interface Address:  10.1.3.1
    IPv4 Neighbor Address:   10.1.3.3
  Metric: 10 IP 192.168.1.0/24
  Metric: 10 IP 10.1.1.0/24  tag value(s):   11
  Metric: 10 IP 10.1.3.0/24
  Metric: 20 IP 10.1.2.0/24  tag value(s):   22
```

- Example 3

```
host1#show isis database verbose
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
zion.00-00*           0x00000011   0xBFAD        487           0/0/0
  Area Address: 47.0005.80FF.F800.0000.0000.0003
  NLPID:       0x81 0xcc
  IP Address:  222.9.1.1
  Hostname: zion
  Router ID:  222.9.1.1
  Metric: 0  ES 2220.0900.1001
  Metric: 10 IS london.00
        Administrative group:  0
        IPv4 Interface Address:  221.1.1.1
        IPv4 Neighbor Address:   221.1.1.2
        Maximum link bandwidth:  50000
        Reservable link bandwidth:  50000
        Unreserved bandwidth:
          Priority 0:  50000
          Priority 1:  50000
          Priority 2:  50000
          Priority 3:  50000
          Priority 4:  30000
          Priority 5:  30000
          Priority 6:  30000
          Priority 7:  30000
        TE default metric:  0
  Metric: 10 IS london.00
        Administrative group:  0
        IPv4 Interface Address:  221.1.6.1
        IPv4 Neighbor Address:   221.1.6.2
        Maximum link bandwidth:  50000
        Reservable link bandwidth:  50000
        Unreserved bandwidth:
          Priority 0:  50000
          Priority 1:  50000
          Priority 2:  50000
          Priority 3:  50000
          Priority 4:  30000
          Priority 5:  30000
          Priority 6:  30000
          Priority 7:  30000
        TE default metric:  0
  Metric: 10 IS paris.00
        Administrative group:  0
        IPv4 Interface Address:  221.1.4.1
        IPv4 Neighbor Address:   221.1.4.4
        Maximum link bandwidth:  0
        Reservable link bandwidth:  0
        Unreserved bandwidth:
          Priority 0:  0
          Priority 1:  0
          Priority 2:  0
          Priority 3:  0
          Priority 4:  0
          Priority 5:  0
          Priority 6:  0
          Priority 7:  0
        TE default metric:  0
```

```
  Metric: 10 IP 221.1.1.0/24
  Metric: 10 IP 221.1.6.0/24
  Metric: 10 IP 221.1.4.0/24
  Metric: 0 IP 222.9.1.1/32
```

- Example 4

```
host1#show isis database Getafix:v2
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
Getafix:v2.00-00*     0x00000001   0xEB53        1097          0/0/0

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
Getafix:v2.00-00*     0x00000001   0x456D        1097          0/0/0
```

- Example 5

```
host1#show isis database Getafix:v2 detail
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
Getafix:v2.00-00*     0x00000001   0xEB53        967           0/0/0
  Area Address: 22
  NLPID:       0x81 0xcc
  IP Address:  1.1.1.2
  Hostname: Getafix:v2
  Metric: 10 IS Getafix:v2.01
  Metric: 0  ES Getafix:v2
  Metric: 10 IP 1.1.1.0 255.255.255.0

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
Getafix:v2.00-00*     0x00000001   0x456D        967           0/0/0
  Area Address: 22
  NLPID:       0x81 0xcc
  IP Address:  1.1.1.2
  Hostname: Getafix:v2
  Metric: 10 IS Getafix:v2.01
  Metric: 10 IP 1.1.1.0 255.255.255.0
```

- Example 6—For IS-IS IPv6 configuration

```
host1:2#show isis database detail
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
host1:1.00-00          0x00000005   0x0E39        930           0/0/0
  Area Address: 49.0001
  NLPID:       0x81 0xcc
  IP Address:  4.4.4.1
  Hostname: host1:1
  Metric: 0  ES host1:1
  Metric: 10 IS host1:2.00
  Metric: 10 IS host1:2.00
  Metric: 10 IP 4.4.4.0/24
  Metric: 10 IP 20.0.0.0/24
  Metric: 10 IPv6 Internal Up 1:1:1:101::/64
host1:2.00-00*         0x00000004   0xC558        735           0/0/0
  Area Address: 49.0001
  NLPID:       0x81 0xcc
  IP Address:  9.9.9.9
  Hostname: host1:2
  Metric: 0  ES host1:2
  Metric: 10 IS host1:1.00
  Metric: 10 IS host1:3.00
```

```
Metric: 10 IS host1:1.00
Metric: 10 IS host1:3.00
Metric: 10 IP 4.4.4.0/24
Metric: 10 IP 20.0.0.0/24
Metric: 10 IP 40.0.0.0/24
Metric: 10 IP 30.0.0.0/24
Metric: 10 IPv6 Internal Up 1:1:1:102::/64
```

show isis mpls adjacency-log

- Use to display a log of the last 20 IS-IS adjacency changes.
- Field descriptions
  - When—Amount of time since recording the log entry
  - Neighbor ID—Identifier for the neighbor
  - IP Address—IP address of the neighbor
  - Interface—Interface from which neighbor was learned
  - Status—Adjacency status, Up or Down
  - Level—IS-IS routing level
- Example

```
host1#show isis mpls adjacency-log
IS-IS MPLS TE log
When      Neighbor ID        IP Address   Interface Status  Level
02:25:47  2220.0900.2002.00  221.1.1.2    at2/0.1   Up      L1
02:25:47  2220.0900.2002.00  221.1.6.2    at2/0.6   Up      L1
02:25:47  2220.0900.4004.00  221.1.4.4    at2/1.5   Up      L1
```

show isis mpls advertisements

- Use to display the last record flooded from MPLS.
- Field descriptions
  - System ID—Name or system ID of the MPLS tail-end (destination) router
  - Router ID—Router ID for the router
  - Link Count—Number of links that MPLS advertises
  - Neighbor System ID—Identifier of the remote system in an area
  - Administrative group—TLV administrative group or color assigned to the link
  - Interface IP address—IP address of the interface
  - Neighbor IP Address—IP address of the neighbor
  - Maximum link bandwidth—Bandwidth capacity of the link in bits per second
  - Reservable link bandwidth—Amount of bandwidth reservable on the link (whether reserved or not)
  - Unreserved bandwidth—Amount of bandwidth available for reservation on the link
  - TE default metric—Traffic engineering default metric value
  - Affinity Bits—Attributes flooded for the link

- Example

```
host1#show isis mpls advertisements
System ID: zion.00
  Router ID:  222.9.1.1
    Link[1]
      Neighbor System ID: london.00
        Administrative group:  0
        IPv4 Interface Address:  221.1.1.1
        IPv4 Neighbor Address:   221.1.1.2
        Maximum link bandwidth:  50000
        Reservable link bandwidth:  50000
        Unreserved bandwidth:
          Priority 0:  50000
          Priority 1:  50000
          Priority 2:  50000
          Priority 3:  50000
          Priority 4:  30000
          Priority 5:  30000
          Priority 6:  30000
          Priority 7:  30000
        TE default metric:  0
    Link[2]
      Neighbor System ID: london.00
        Administrative group:  0
        IPv4 Interface Address:  221.1.6.1
        IPv4 Neighbor Address:   221.1.6.2
        Maximum link bandwidth:  50000
        Reservable link bandwidth:  50000
        Unreserved bandwidth:
          Priority 0:  50000
          Priority 1:  50000
          Priority 2:  50000
          Priority 3:  50000
          Priority 4:  30000
          Priority 5:  30000
          Priority 6:  30000
          Priority 7:  30000
        TE default metric:  0
    Link[3]
      Neighbor System ID: paris.00
        Administrative group:  0
        IPv4 Interface Address:  221.1.4.1
        IPv4 Neighbor Address:   221.1.4.4
        Maximum link bandwidth:  0
        Reservable link bandwidth:  0
        Unreserved bandwidth:
          Priority 0:  0
          Priority 1:  0
          Priority 2:  0
          Priority 3:  0
          Priority 4:  0
          Priority 5:  0
          Priority 6:  0
          Priority 7:  0
        TE default metric:  0
```

show isis mpls tunnel

- Use to display information about tunnels used in the calculation of IS-IS next hops.
- Field descriptions
  - System Id—Name or system ID of the MPLS tail-end (destination) router
  - Tunnel Name—Name of the MPLS tunnel interface
  - Nexthop—Destination IP address of the MPLS tunnel
  - Metric —Metric of the MPLS tunnel
  - Mode—Metric mode, either absolute or relative
- Example

```
host1#show isis mpls tunnel
System Id         Tunnel Name   Nexthop    Metric    Mode
dakota-router1.00 Tunnel1       2.2.2.2    -3        Relative
                  Tunnel2       2.2.2.2    11        Absolute
jersey-router2.00 Tunnel3       3.3.3.3    -1        Relative
                  Tunnel4       3.3.3.3
```

show isis nsf

- Use to display information about the configured and operational settings on the router for IS-IS graceful restart, which is also known as nonstop forwarding (NSF).
- Field descriptions
  - Configured Timer Values—Displays the following values configured for IS-IS graceful restart on the router, as described in *Configuring Graceful Restart* on page 365*:*
    - Graceful Restart—Setting for IS-IS graceful restart on the router: Enabled or Disabled
    - T3 Timer—Method by which the restarting router obtains the T3 wait time: Manual or Derive from adjacency
    - T3 Timeout Value—Maximum time, in seconds, that the restarting router waits before setting the overload bit to indicate that IS-IS graceful restart has failed
    - T2 Timeout Value—Maximum time for IS-IS level 1 routing and level 2 routing, in seconds, that the restarting router waits for the LSP database to synchronize
    - T1 Timeout Value—Time interval, in seconds, between IS-IS restart requests sent by the restarting router on this interface to neighboring routers
    - T1 Retry Count—Number of times the restarting router resends unacknowledged restart requests on this interface at the specified interval
    - Adj. Wait Time—Maximum time, in seconds, that an IS-IS process on the restarting router waits for all interfaces with IS-IS adjacencies to come up before completing the restart process

- Operation Timer Values—Displays the following currently remaining timer settings, in seconds, for IS-IS graceful restart during the restart process:
  - T3 Timer—Remaining time before the restarting router sets the overload bit to indicate that graceful restart has failed
  - T2 Timeout Value—Remaining time for level 1 routing and level 2 routing that the restarting router waits for the LSP database to synchronize
  - Adj. Wait Time—Remaining time that the restarting router waits for all adjacencies to come up before completing the restart process
  - Restart Ack Recv Adj Count—Number of neighboring IS-IS routers for level 1 routing and level 2 routing that have acknowledged the restart requests sent by the router
  - LAN If DIS Wait Count—Number of interfaces on which the restarting router is waiting to receive election of the designated intermediate system (DIS)
  - Restart CSNP Adj Recv Count—Number of adjacencies for level 1 routing and level 2 routing that have sent complete sequence number PDUs (CSNPs) to provide information about LSP database synchronization
  - Local LSP Wait Count—Number of level 1 and level 2 LSPs for which the restarting router is awaiting complete synchronization

- Example

```
host1#show isis nsf
Configured Timer Values
-----------------------
 Graceful Restart           : Enabled
 T3 Timer                   : Manual
 T3 Timeout Value           : 80
 T2 Timeout Value           : 70(level-1)
                              70(level-2)
 T1 Timeout Value           : 60
 T1 Retry Count             : 3
 Adj. Wait Time             : 30

Operation Timer Values
----------------------
 T3 Timer                   : 0
 T2 Timeout Value           : 0(level-1)
                              0(level-2)
 Adj. Wait Time             : 0
 Restart Ack Recv Adj Count : 0(level-1)
                              0(level-2)
 LAN If DIS Wait Count      : 0
 Restart CSNP Adj Recv Count: 0(level-1)
                              0(level-2)
 Local LSP Wait Count       : 0(level-1)
                              0(level-2)
```

show isis spf-log

- Use to display how often and why the router has run a full SPF calculation.
- Field descriptions
  - When—Amount of time since a full SPF calculation took place, given in hours:minutes:seconds. The previous 20 calculations are logged.
  - Duration—Number of seconds to complete this SPF run. The elapsed time is in actual clock time, not CPU time.
  - First Trigger LSP—Whenever a full SPF calculation is triggered by a new LSP, the LSP ID is stored in the router
  - SpfType—Type of SPF run
  - Triggers—List of causes that triggered the SPF calculation
- Example 1

```
host1#show isis spf-log
Level 1 SPF log
When     Duration      First Trigger LSP    SpfType  Triggers
00:01:45 0.000         0000.0000.0000.00-00 Full     LSP Add
00:01:36 0.000         0000.0000.0000.00-00 Full     LSP Add
00:01:31 0.000         0000.0101.0101.00-00 Full     LSP Add
00:00:08 0.000         0000.0101.0101.00-00 PRC      LSP Sequence Update
```

- Example 2

```
host1#show isis spf-log detail
Level 1 SPF log
When     Duration      First Trigger LSP    SpfType  Triggers
00:01:53 0.000         0000.0000.0000.00-00 Full     LSP Add
  RTupdt 0.000
  RtLeak 0.000
00:01:44 0.000         0000.0000.0000.00-00 Full     LSP Add
  RTupdt 0.000
  RtLeak 0.000
00:01:39 0.000         0000.0101.0101.00-00 Full     LSP Add
  RTupdt 0.000
  RtLeak 0.000
00:00:16 0.000         0000.0101.0101.00-00 PRC      LSP Sequence Update
  RTupdt 0.000
  RtLeak 0.000
```

show isis summary-addresses

- Use to display the status of IS-IS aggregate addresses.
- Field descriptions
  - Address—Aggregate addresses advertised by summarization process
  - Mask—IP subnet masks used for the summary routes
  - Level—Level for which multiple groups of addresses can be summarized
  - Metric—Metric used to advertise the summary
  - State—State of the summary address
  - Prefix—IPv6 prefix
  - Tag—Number in the range 1–4294967295 that identifies the route tag assigned to the IS-IS IPv6 interface

- Example 1—For IS-IS IP addresses

```
host1#show isis summary-addresses
Address       Mask          Level       Metric   State
--------      ----------    ---------   ------   -------
3.0.0.0       255.0.0.0     LEVEL-1     0        ENABLED
4.0.0.0       255.0.0.0     LEVEL-1-2   5        ENABLED
```

- Example 2—For IS-IS IPv6 addresses

```
host1#show isis summary-addresses
Prefix          Level            Metric         Tag     State
------------    -------------    ----------     ------  -------
2008::0/8       LEVEL-2          0              100     ENABLED
```

show isis topology

- Use to display the paths to all intermediate systems or specific types of intermediate systems.
- Field descriptions
  - System ID—Name or system ID of the intermediate system
  - Metric—Metric of the path to the intermediate system
  - Next Hop—Destination IP address of the intermediate system
  - Interface—Interface from which neighbor was learned
  - SNPA—Subnetwork point of attachment; for a LAN circuit, it is the MAC address; not meaningful for a point-to-point circuit.
- Example

```
host1#show isis topology level-1
              IS-IS paths for level-1 routers
              -------------------------------
  System-ID   Metric    Next Hop       Intf      SNPA
------------- ------   -------------  --------   ----
barcelona:vr2  10      barcelona:vr2  at2/0.12
```

undebug isis

- Use to cancel the display of information about a selected event.
- The same IS-IS variables can be designated as in the **debug isis** command.
- Example

  host1#**undebug isis adj-packets**

- There is no **no** version.

Displaying CLNS

You can display the following information related to the CLNS protocol:

- CLNS information about interfaces
- Information about router adjacencies
- Information about ES and IS neighbors
- Protocol-specific information for each routing process
- Information about CLNS packets
- Global CLNS configurations

You can set a statistics baseline for CLNS using the **baseline clns** command.

baseline clns

- Use to set a statistics baseline for CLNS.
- The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the optional *interface-specifier* parameter to specify an interface; otherwise the command sets a baseline for all interfaces.
- You cannot set a baseline for groups of interfaces.
- When baselining is requested, the time since the last baseline was set is displayed in days, hours, minutes, and seconds.
- Use the optional **delta** keyword with the **show clns traffic** command to specify that baselined statistics are to be shown.
- Example

```
host1#show clns traffic detail
IS-IS: Baseline last set 0 days, 0 hours, 1 minutes, 41 seconds
IS-IS: Corrupted LSPs: 0
IS-IS: L1 LSP Database Overloads: 0
IS-IS: L2 LSP Database Overloads: 0
IS-IS: Area Addresses Dropped: 0
IS-IS: Attempts to Exceed Max Sequence: 0
IS-IS: Sequence Numbers Skipped: 6
IS-IS: Own LSPs Purged: 1
IS-IS: System ID Length Mismatches: 0
IS-IS: Maximum Area Mismatches: 0

Interface: atm2/1.3
IS-IS: Baseline last set 0 days, 0 hours, 1 minutes, 43 seconds
IS-IS: Protocol PDUs (in/out): 32/36
IS-IS: Init Failures: 0
IS-IS: Adjacencies Changes: 1
IS-IS: Adjacencies Rejected: 0
IS-IS: Bad LSPs: 0
IS-IS: Level-1 Designated IS Changes: 0
IS-IS: Level-2 Designated IS Changes: 0
IS-IS: Invalid 9542s: 0
host1#baseline clns atm 2/1.3
```

```
host1#show clns traffic detail delta
IS-IS: Baseline last set 0 days, 0 hours, 2 minutes, 27 seconds
IS-IS: Corrupted LSPs: 0
IS-IS: L1 LSP Database Overloads: 0
IS-IS: L2 LSP Database Overloads: 0
IS-IS: Area Addresses Dropped: 0
IS-IS: Attempts to Exceed Max Sequence: 0
IS-IS: Sequence Numbers Skipped: 6
IS-IS: Own LSPs Purged: 1
IS-IS: System ID Length Mismatches: 0
IS-IS: Maximum Area Mismatches: 0

Interface: atm2/1.3
IS-IS: Baseline last set 0 days, 0 hours, 0 minutes, 8 seconds
IS-IS: Protocol PDUs (in/out): 2/1
IS-IS: Init Failures: 0
IS-IS: Adjacencies Changes: 0
IS-IS: Adjacencies Rejected: 0
IS-IS: Bad LSPs: 0
IS-IS: Level-1 Designated IS Changes: 0
IS-IS: Level-2 Designated IS Changes: 0
IS-IS: Invalid 9542s: 0
```

- There is no **no** version.

clear isis database

- Use to delete all entries from the IS-IS link-state database, or only the entries associated with the specified neighbor.
- Field descriptions
  - LSPID—LSP identifier
  - LSP Seq Num—Sequence number for the LSP. Enables other routers to determine if they have received the latest information from source.
  - LSP Checksum—Checksum of the LSP packet
  - LSP Holdtime—Number of seconds that the LSP remains valid
  - ATT—Attach bit; indicates that the router is a level 2 router and can reach other areas
  - P—P bit; detects whether intermediate system is capable of area partition repair
  - OL—Overload bit; determines whether intermediate system is congested
- Example

```
host1#show isis database
IS-IS Level-1 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
rtr1.00-00*    0x00000009   0x568F        1188          0/0/0
rtrtwo.00-00   0x00000005   0xEC9B        444           0/0/0

IS-IS Level-2 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
rtr1.00-00*    0x00000010   0xF630        1193          0/0/0
rtrtwo.00-00   0x0000000C   0xF8DA        1188          0/0/0
```

```
host1#clear isis database
host1#show isis database
IS-IS Level-1 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL

IS-IS Level-2 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
```

- There is no **no** version.

show clns

- Use to display global CLNS information about the router.
- Field descriptions
  - Interfaces Enabled for CLNS—Number of interfaces that have the CLNS routing protocol enabled
  - Configuration Timer—Interval (in seconds) after which the router sends out IS hello packets
  - Default Holding Timer—Length of time (in seconds) that hello packets are remembered
  - Packet Lifetime—Default value used in packets sourced by this router
  - Intermediate system operation enabled (forwarding allowed)—Indicates whether this router is configured to be an ES or an IS
  - IS-IS Level-1-2 Router—Shows whether IS-IS is running in this router, gives tag information, and shows whether it is running level 1 or level 1-2
  - Routing for Area—ISO (NSAP) address for the network
  - Distribute domain wide enabled—Indicates whether distribute-domain-wide is enabled
  - Area Authentication—Displays the following fields if area authentication is enabled:
    - PSNP/CSNP PDU authentication enabled—Indicates whether authentication of level 1 PSNP packets and/or level 1 CSNP packets has been enabled by means of the **area-authentication** command
    - Key-id—Numeric identifier for the authentication key
    - Type—Type of authentication: hmac-md5 or password; an asterisk after the type indicates that the key is active
    - Start Accept—Date and time that the router starts accepting packets created with this password
    - Start Generate—Date and time that the router starts inserting this password into packets
    - Stop Accept—Date and time that the router stops accepting packets created with this password
    - Stop Generate—Date and time that the router stops inserting this password into packets

- Domain Authentication—Displays the following fields if domain authentication is enabled:
  - PSNP/CSNP PDU authentication enabled—Indicates whether authentication of level 2 PSNP packets and/or level 1 CSNP packets has been enabled by means of the **domain-authentication** command
  - Key-id—Numeric identifier for the authentication key
  - Type—Type of authentication: hmac-md5 or password; an asterisk after the type indicates that the key is active
  - Start Accept—Date and time that the router starts accepting packets created with this password
  - Start Generate—Date and time that the router starts inserting this password into packets
  - Stop Accept—Date and time that the router stops accepting packets created with this password
  - Stop Generate—Date and time that the router stops inserting this password into packets

- Use the **es-neighbors** keyword to display information for IS-IS end-system adjacencies or the **is-neighbors** keyword to display information for IS-IS intermediate-system adjacencies. Neighbor entries are sorted according to the area in which they are located. The following fields are displayed when any of these keywords is used:
  - System Id—Six-byte value of router
  - Interface—Interface on which the router was discovered
  - State—Adjacency state, either Up or Init
    - Up—Believes that the ES or IS is reachable
    - Init—Router is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent.
  - Type—Level 1, level 2, and level 1-2 type adjacencies
    - L1—Router adjacency for level 1 routing only
    - L1L2—Router adjacency for level 1 and level 2 routing
    - L2—Router adjacency for level 2 only
  - Priority—IS-IS priority that the respective neighbor is advertising. The highest-priority neighbor becomes the designated IS-IS router for the interface.
  - Circuit Id—Neighbor's idea of what the designated IS-IS router is for the interface
- Add the **detail** keyword to display area addresses and IP addresses.
- Example 1—For IS-IS IP configuration

```
host1#show clns
Global CLNS Information:
  3 Interfaces Enabled for CLNS
  NET: 47.0005.80FF.F800.0000.0001.0001.0000.0000.3333.00
  Configuration Timer: 10, Default Holding Timer: 30, Packet Lifetime: 1200
  Intermediate system operation enabled
```

```
  IS-IS level-1-2 Router: testnet
    Routing for Area: 47.0005.80FF.F800.0000.0001.0001
  Distribution domain wide enabled
  Area Authentication:
  PSNP PDU authentication enabled
    Key-id:   1 Type: hmac-md5
      Start Accept:   FRI JAN 14 09:57:41 2000
      Start Generate: FRI JAN 14 09:59:41 2000
      Stop Accept:    0
      Stop Generate:  0
  Domain Authentication:
  PSNP PDU authentication enabled
  CSNP PDU authentication enabled
    Key-id:   1 Type: hmac-md5*
      Start Accept:   WED JAN 12 19:01:52 2000
      Start Generate: WED JAN 12 19:03:52 2000
      Stop Accept:    0
      Stop Generate:  0
```

- Example 2—For IS-IS IPv6 configuration

```
host1:2#show clns
Global CLNS Information:
  3 Interfaces Enabled for CLNS
  NET: 49.0001.0040.0400.4002.00
  Configuration Timer: 10, Default Holding Timer: 30, Packet Lifetime: 30
  Intermediate system operation enabled
  IS-IS level-1-2 Router:
    Routing for Area: 49.0001
Ip route-type both
```

- Example 3—For IS-IS adjacencies

```
host1#show clns is-neighbors
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.7500 atm2/0.111    up     L1L2 127        0000.0000.0000.00
```

- Example 4—For detailed information on IS-IS adjacencies

```
host1#show clns is-neighbors detail
System Id      Interface  State Type Priority  Circuit Id
0000.0000.7500 atm2/0.111 up    L1L2 127       0000.0000.0000.00
  Area Address(es): 47.0005.80FF.F800.0000.0001.0001
  Ip Address(es):   172.30.245.33
```

show clns interface

- Use to display CLNS-specific information about each interface.
- Field descriptions
  - interface—Status of interface
  - line protocol—Status of the line protocol, up or down
  - Checksums—Status of checksum, enabled or disabled
  - MTU—Maximum transmission size for a packet on this interface
  - Encapsulation—Encapsulation used by CLNP packets on this interface
  - Next ESH/ISH—When the next ES hello or IS hello is sent on this interface
  - Routing Protocol—One or more areas that this interface is in. In most cases, an interface is in only one area.

  - Circuit type—Whether the interface has been configured for local routing (level-1), area routing (level-2), or local and area routing (level-1-2)
  - Interface number—Number of the interface
  - local circuit ID—Local circuit ID of the interface
  - Authentication Level-1—If area authentication is enabled, lists key-id, type of authentication, start and stop accept times, and start and stop generate times for the key. An asterisk after the type indicates the key is active.
  - Authentication Level-2—If domain authentication is enabled, lists key-id, type of authentication, start and stop accept times, and start and stop generate times for the key. An asterisk after the type indicates the key is active.
  - Level 1 and level 2 metrics—Metric value for each level
  - DIS priority—DIS priority value assigned to the IS-IS router at each level
  - Priority—Priority value assigned to the IS-IS router at each level
  - Circuit ID—Circuit ID of the IS-IS router at each level
  - Number of active level 1 and level 2 adjacencies—Number of adjacencies active at each level
  - Designated IS—Name of the designated IS-IS router at each level
  - Next IS-IS LAN level Hello—Amount of time (in seconds) before the next IS-IS LAN level 1 or level 2 hello message occurs
  - BFD—State of BFD for IS-IS, enabled or disabled
  - Mesh Group—Status of the mesh group, Active or Inactive
  - LDP-IGP Synchronization—Status of synchronization, Achieved or Pending; supported only for OSPFv2
- When you specify the **brief** keyword, the output includes the following fields.
  - interface—Name of the interface
  - state—State of the interface, up or down
  - level—Configured interface level, level-1, level-2, or level-1-2
  - DIS(L-1)—Level-1 designated intermediate system (DIS) in a multiaccess network
  - DIS(L-2)—Level-2 designated intermediate system (DIS) in a multiaccess network
  - l1/l2 Metric—Metric for the interface
- Example 1

```
host1#show clns interface
FastEthernet4/1 is up, line protocol is up
  Checksums Enabled, MTU 1500, Encapsulation SNAP
  Next ESH/ISH is 5 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x10, local circuit ID 0x1
    Level-1 Metric: 10, DIS Priority: 0, Priority: 64,
            Circuit ID: 0000.0000.0000.01
         Designated IS: Getafix:v2.01 (us)
    Number of active level-1 adjacencies: 0
```

```
        Level-2 Metric: 10, DIS Priority: 0, Priority: 64,
                Circuit ID: 0000.0000.0000.01
             Designated IS: Getafix:v1.01 (Not Us)
        Number of active level-2 adjacencies: 1
        Next IS-IS LAN Level-1 Hello in 7 seconds
        Next IS-IS LAN Level-2 Hello in 6 seconds
        BFD disabled
        Mesh Group Inactive
                     LDP is configured through LDP autoconfig
                     LDP-IGP Synchronization: Achieved
```

- Example 2

```
host1#show clns interface brief
                          Clns Intf brief Table
                          ---------------------

                                                                          l1/l2
   interface      state     level        DIS(L-1)         DIS(L-2)      Metric
---------------   -----   ---------   --------------   --------------   ------
loopback1         up      level-1-2   Point to Point   Point to Point   10/10
ATM3/1.1          up      level-1-2   Point to Point   Point to Point   10/10
FastEthernet1/1   up      level-1-2   nemo:2.03        nemo:2.03        10/10
3 interfaces up in 3 interfaces
```

show clns neighbors

- Use to display information about ES and IS neighbors.
- Use the **detail** keyword to display area addresses, IP addresses, and the ES or IS neighbor's graceful restart capability and restarting state.
- Field descriptions
  - System Id—Six-byte value of router
  - SNPA—Subnetwork point of attachment, which is the data link address; not meaningful for a point-to-point circuit
  - Interface—Interface the router was learned from
  - State—State of the ES or IS
    - Init—Router is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent.
    - Up—ES or IS is considered reachable
  - Holdtime(rem)—Remaining number of seconds before this adjacency entry times out
  - Type—One of the following adjacency types:
    - ES—End-system adjacency either discovered by means of the ES-IS protocol or statically configured
    - IS—Router adjacency either discovered by means of the ES-IS protocol or statically configured
    - L1—Router adjacency for level 1 routing only
    - L1L2—Router adjacency for level 1 and level 2 routing
    - L2—Router adjacency for level 2 only

- Proto—Protocol through which the adjacency was learned. Valid protocol sources include ES-IS, IS-IS, and Static.
- Area Address(es)—Area addresses of the ES or IS
- Ip Address(es)—IP addresses of the ES or IS
- Graceful Restart Capable—Whether graceful restart is enabled (yes) or disabled (no) on the ES or IS
- Neighbor Restarting—Whether the ES or IS is currently restarting: yes or no
- BFD session—State of any BFD session for this neighbor

- Example 1—For IS-IS IP configuration

```
host1#show clns neighbors detail
System Id       SNPA   Interface   State   Holdtime(rem)   Type   Proto
1111.1111.1111         A5/0.1      up      30(29)          L1L2   IS-IS
Area Address(es): 11.1111.1111.1111.1111.1111.1111
Ip Address(es): 172.100.11.1
Graceful Restart Capable: yes
Neighbor Restarting: yes
BFD session is not-up
```

- Example 2—For IS-IS IPv6 configuration

```
host1:2#show clns neighbors detail
System Id      SNPA                Interface   State  Holdtime(rem) Type Proto
host1:1         0090.1A41.081A      F1/1        up     30(25)        L1   IS-IS
  Area Address(es): 49.0001
  Ip Address(es):   4.4.4.1
  Graceful Restart Capable: no
  Neighbor Restarting: no
host1:3         0090.1A41.081C      F1/1        up     30(27)        L1   IS-IS
  Area Address(es): 49.0001
  Ip Address(es):   4.4.4.3
  Graceful Restart Capable: no
Neighbor Restarting: no
```

show clns protocol

- Use to display protocol-specific information about a routing process.
- Field descriptions
  - IS-IS Router—IS-IS router name
  - System ID—Six-byte value of router
  - IS-Type—Routing level (level 1, level 2, or both) that is enabled on the router
  - Manual area addresses—Configured area addresses
  - Routing for area address(es)—Identified for level 1 routing processes. For level 2 routing processes, lists the domain address.
  - Interfaces supported by IS-IS—Interfaces and type
  - Distance—Configured distance value
  - Redistributing—Protocols being redistributed into IS-IS

- Example

```
host1:2#show clns protocol
IS-IS Router:
  System Id: 0040.0400.4002.00  IS-Type: level-1-2
  Operational State: Up
  Manual area address(es):
        49.0001
  Routing for area address(es):
        49.0001
  Interfaces supported by IS-IS:
        loopback1 - IP
        FastEthernet1/1 - IP,IPv6
        ATM3/1.1 - IP, IPv6
  Distance: 115
  Redistributing:
        static
```

show clns traffic

- Use to display all CLNS packets the router sees.
- Use the optional **delta** keyword to specify that baselined statistics are to be shown.
- Field descriptions
  - IS-IS: Baseline last set—Time since the baseline was set
  - IS-IS: Corrupted LSPs—Number of LSPs received with errors
  - IS-IS: L1 LSP Database Overloads—Number of overloads in level 1
  - IS-IS: L2 LSP Database Overloads—Number of overloads in level 2
  - IS-IS: Area Addresses Dropped—Number of area addresses that the router dropped
  - IS-IS: Attempts to Exceed Max Sequence—Number of sequence wraps over maximum
  - IS-IS: Sequence Numbers Skipped—Number of LSPs received out of order
  - IS-IS: Own LSPs Purged—Number of LSPs deleted
  - IS-IS: Other LSPs Purged—Number of received LSPs deleted
  - IS-IS: System ID Length Mismatches—Number of unmatched system ID lengths
  - IS-IS: Maximum Area Mismatches—Number of rejected hellos due to area mismatches
  - IS-IS: Area/Domain Authentication Failures—Number of authentication failures on received level 1 and level 2 LSP/SNPs
  - IS-IS: Level-1 LSPs Sent Rcvd Dropped—Number of level 1 LSPs sent, received, and dropped
  - IS-IS: Level-2 LSPs Sent Rcvd Dropped—Number of level 2 LSPs sent, received, and dropped
  - IS-IS: LSP checksum errors received—Number of LSP checksum errors received

- When you specify an interface, reports include the following additional fields:
  - Interface—IS-IS interface for which details are displayed
  - IS-IS: Protocol PDUs (in/out)—Number of packets in/out on interface
  - IS-IS: Init Failures—Number of rejected hellos on interface
  - IS-IS: Adjacencies Changes—Number of times adjacencies have transitioned from down to up
  - IS-IS: Adjacencies Rejected—Number of times hellos are rejected because of an incompatibility
  - IS-IS: Bad LSPs—Number of LSPs received with errors
  - IS-IS: Level-1 Designated IS Changes—Number of times the level 1 designated router has changed
  - IS-IS: Level-2 Designated IS Changes—Number of times the level 2 designated router has changed
  - IS-IS: Invalid 9542s—Number of rejected ES hello packets
  - IS-IS: Malformed PDUs received—Number of malformed packets received
  - IS-IS: Authentication Failures—Number of authentication failures on received level 1 and level 2 hello packets
- When you specify the **detail** keyword, the output includes the following additional fields that show packet statistics and LSP statistics. The hello, CSNP, and PSNP statistics are shown only when you issue the **detail** keyword. When the interface is Ethernet, L1 and L2 hello counts are displayed; otherwise the point-to-point hello count is displayed.
  - IS-IS: Level-1 Hellos (in/out/dropped)—Number of level 1 hellos received, sent, and dropped
  - IS-IS: Level-2 Hellos (in/out/dropped)—Number of level 2 hellos received, sent, and dropped
  - IS-IS: Level-1 CSNPs (in/out)—Number of level 1 CSNPs received and sent on the interface
  - IS-IS: Level-2 CSNPs (in/out)—Number of level 2 CSNPs received and sent on the interface
  - IS-IS: Level-1 PSNPs (in/out)—Number of level 1 PSNPs received and sent on the interface
  - IS-IS: Level-2 PSNPs (in/out)—Number of level 2 PSNPs received and sent on the interface
  - IS-IS: LSP Retransmissions—Number of LSPs retransmitted on the interface
- Example 1

```
host1#show clns traffic
IS-IS: Baseline last set 0 days, 21 hours, 12 minutes, 15 seconds
IS-IS: Corrupted LSPs: 0
IS-IS: L1 LSP Database Overloads: 0
IS-IS: L2 LSP Database Overloads: 0
IS-IS: Area Addresses Dropped: 0
IS-IS: Attempts to Exceed Max Sequence: 0
IS-IS: Sequence Numbers Skipped: 5
IS-IS: Own LSPs Purged: 0
```

```
IS-IS: Other LSPs Purged: 0
IS-IS: System ID Length Mismatches: 0
IS-IS: Maximum Area Mismatches: 0
IS-IS: Area/Domain Authentication Failures: 0
IS-IS: Level-1 LSPs Sent: 1 Rcvd: 6769 Dropped: 6769
IS-IS: Level-2 LSPs Sent: 1 Rcvd: 6769 Dropped: 6769
IS-IS: LSP checksum errors received: 0
```

- Example 2

```
host1#show clns traffic fastEthernet 4/0 detail
Interface: FastEthernet4/0
IS-IS: Baseline last set 5 days, 0 hours, 3 minutes, 31 seconds
IS-IS: Protocol PDUs (in/out): 10421/5862
IS-IS: Level-1 Hellos (in/out/dropped): 610046/610456/0
IS-IS: Level-2 Hellos (in/out/dropped): 610046/610456/0
IS-IS: Level-1 CSNPs (in/out): 0/0
IS-IS: Level-2 CSNPs (in/out): 0/0
IS-IS: Level-1 PSNPs (in/out): 0/0
IS-IS: Level-2 PSNPs (in/out): 0/0
IS-IS: Init Failures: 0
IS-IS: Adjacencies Changes: 1
IS-IS: Adjacencies Rejected: 0
IS-IS: Bad LSPs: 0
IS-IS: LSP Retransmissions: 0
IS-IS: Level-1 Designated IS Changes: 1
IS-IS: Level-2 Designated IS Changes: 1
IS-IS: Invalid 9542s: 0
IS-IS: Malformed PDU received: 0
IS-IS: Authentication Failures: 0
```

- Example 3

```
host1#show clns traffic detail
IS-IS: Baseline last set 5 days, 0 hours, 3 minutes, 31 seconds
IS-IS: Corrupted LSPs: 0
IS-IS: L1 LSP Database Overloads: 0
IS-IS: L2 LSP Database Overloads: 0
IS-IS: Area Addresses Dropped: 0
IS-IS: Attempts to Exceed Max Sequence: 0
IS-IS: Sequence Numbers Skipped: 0
IS-IS: Own LSPs Purged: 0
IS-IS: Other LSPs Purged: 0
IS-IS: System ID Length Mismatches: 0
IS-IS: Maximum Area Mismatches: 0
IS-IS: Area/Domain Authentication Failures: 0
IS-IS: Level-1 LSPs Sent: 1 Rcvd: 6769 Dropped: 6769
IS-IS: Level-2 LSPs Sent: 1 Rcvd: 6769 Dropped: 6769
IS-IS: LSP checksum errors received: 0

Interface: FastEthernet4/0
IS-IS: Baseline last set 5 days, 0 hours, 3 minutes, 31 seconds
IS-IS: Protocol PDUs (in/out): 10421/5862
IS-IS: Level-1 Hellos (in/out/dropped): 610046/610456/0
IS-IS: Level-2 Hellos (in/out/dropped): 610046/610456/0
IS-IS: Level-1 CSNPs (in/out): 0/0
IS-IS: Level-2 CSNPs (in/out): 0/0
IS-IS: Level-1 PSNPs (in/out):0/0
IS-IS: Level-2 PSNPs (in/out):0/0
IS-IS: Init Failures: 0
IS-IS: Adjacencies Changes: 1
IS-IS: Adjacencies Rejected: 0
IS-IS: Bad LSPs: 0
```

```
IS-IS: LSP Retransmissions: 0
IS-IS: Level-1 Designated IS Changes: 1
IS-IS: Level-2 Designated IS Changes: 1
IS-IS: Invalid 9542s: 0
IS-IS: Malformed PDU received: 0
IS-IS: Authentication Failures: 0

Interface: FastEthernet4/1
IS-IS: Baseline last set 5 days, 0 hours, 3 minutes, 31 seconds
IS-IS: Protocol PDUs (in/out): 10421/5862
IS-IS: Level-1 Hellos (in/out/dropped): 609946/610056/0
IS-IS: Level-2 Hellos (in/out/dropped): 609946/610056/0
IS-IS: Level-1 CSNPs (in/out): 0/0
IS-IS: Level-2 CSNPs (in/out): 0/0
IS-IS: Level-1 PSNPs (in/out):0/0
IS-IS: Level-2 PSNPs (in/out):0/0
IS-IS: Init Failures: 0
IS-IS: Adjacencies Changes: 1
IS-IS: Adjacencies Rejected: 0
IS-IS: Bad LSPs: 0
IS-IS: LSP Retransmissions: 0
IS-IS: Level-1 Designated IS Changes: 1
IS-IS: Level-2 Designated IS Changes: 1
IS-IS: Invalid 9542s: 0
IS-IS: Malformed PDU received: 0
IS-IS: Authentication Failures: 0
```