

Contents

IS-IS commands	1
address-family ipv4	1
area-authentication send-only	1
area-authentication-mode	2
auto-cost enable	3
bandwidth-reference	4
circuit-cost	5
cost-style	6
default-route-advertise	7
display isis	8
display isis event-log graceful-restart	9
display isis event-log lsp	10
display isis event-log non-stop-routing	11
display isis event-log spf	12
display isis graceful-restart status	18
display isis interface	20
display isis lsdb	23
display isis lsdb statistics	27
display isis name-table	28
display isis non-stop-routing status	29
display isis packet	30
display isis peer	37
display isis redistribute	40
display isis route	41
display isis spf-tree	44
display isis statistics	50
display osi	52
display osi statistics	54
distribute bgp-ls	55
domain-authentication send-only	56
domain-authentication-mode	56
fast-reroute	58
filter-policy export	59
filter-policy import	60
flash-flood	61
graceful-restart	62
graceful-restart suppress-sa	62
graceful-restart t1	63
graceful-restart t2	64
graceful-restart t3	65
ignore-att	66
import-route	66
import-route isis level-1 into level-2	68
import-route isis level-2 into level-1	69
import-route limit	70
isis	71
isis authentication send-only	71
isis authentication-mode	72
isis bfd enable	74
isis circuit-level	74
isis circuit-type p2p	75
isis cost	76
isis dis-name	77
isis dis-priority	77
isis enable	78
isis fast-reroute lfa-backup exclude	79
isis mib-binding	79

isis prefix-suppression.....	80
isis primary-path-detect bfd.....	80
isis silent.....	81
isis small-hello.....	82
isis tag.....	82
isis timer csnp.....	83
isis timer hello.....	84
isis timer holding-multiplier.....	84
isis timer lsp.....	85
isis timer retransmit.....	86
is-level.....	87
is-name.....	87
is-name map.....	88
ispf enable.....	89
log-peer-change.....	89
lsp-fragments-extend.....	90
lsp-length originate.....	91
lsp-length receive.....	91
maximum load-balancing.....	92
network-entity.....	92
non-stop-routing.....	93
pic.....	94
preference.....	94
prefix-priority.....	95
reset isis all.....	96
reset isis event-log graceful-restart.....	96
reset isis event-log lsp.....	97
reset isis event-log non-stop-routing.....	97
reset isis event-log spf.....	98
reset isis packet.....	98
reset isis peer.....	99
reset osi statistics.....	99
set-att.....	100
set-overload.....	100
snmp context-name.....	101
snmp-agent trap enable isis.....	102
summary.....	103
timer lsp-generation.....	104
timer lsp-max-age.....	105
timer lsp-refresh.....	106
timer spf.....	106
virtual-system.....	107

IS-IS commands

address-family ipv4

Use **address-family ipv4** to create the IS-IS IPv4 address family and enter its view.

Use **undo address-family ipv4** to delete the IS-IS IPv4 address family and all configurations in the view.

Syntax

```
address-family ipv4 [ unicast ]  
undo address-family ipv4 [ unicast ]
```

Default

No IS-IS IPv4 address family exists.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

unicast: Specifies the unicast address family (the default).

Examples

```
# Create the IS-IS IPv4 address family and enter its view.  
<Sysname> system-view  
[Sysname] isis 100  
[Sysname-isis-100] address-family ipv4  
[Sysname-isis-100-ipv4]
```

area-authentication send-only

Use **area-authentication send-only** to configure IS-IS not to check the authentication information in the received Level-1 packets, including LSPs, CSNPs, and PSNPs.

Use **undo area-authentication send-only** to restore the default.

Syntax

```
area-authentication send-only  
undo area-authentication send-only
```

Default

When area authentication mode and key are configured, a Level-1 or Level-1-2 router checks the authentication information in the received packets.

Views

IS-IS view

Predefined user roles

network-admin

Usage guidelines

When area authentication mode and key are configured, a Level-1 or Level-1-2 router adds the key in the specified mode into transmitted Level-1 packets (including LSPs, CSNPs, and PSNPs). It also checks the key in the received Level-1 packets.

To prevent packet exchange failure in case of an authentication key change, configure IS-IS not to check the authentication information in the received packets.

Examples

```
# Configure IS-IS not to check the authentication information in the received packets.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] area-authentication send-only
```

Related commands

area-authentication-mode
domain-authentication send-only
isis authentication send-only

area-authentication-mode

Use **area-authentication-mode** to specify an area authentication mode and a key.

Use **undo area-authentication-mode** to restore the default.

Syntax

```
area-authentication-mode { { gca key-id { hmac-sha-1 | hmac-sha-224 | hmac-sha-256 |  
hmac-sha-384 | hmac-sha-512 } [ nonstandard ] | md5 | simple } { cipher | plain } string |  
keychain keychain-name } [ ip | osi ]  
undo area-authentication-mode
```

Default

No area authentication mode or key is configured.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

gca: Specifies the Generic Cryptographic Authentication (GCA) mode.

key-id: Uniquely identifies an SA in the range of 1 to 65535. The sender inserts the Key ID into the authentication TLV, and the receiver authenticates the packet by using the SA that is selected based on the Key ID.

hmac-sha-1: Specifies the HMAC-SHA-1 algorithm.

hmac-sha-224: Specifies the HMAC-SHA-224 algorithm.

hmac-sha-256: Specifies the HMAC-SHA-256 algorithm.

hmac-sha-384: Specifies the HMAC-SHA-384 algorithm.

hmac-sha-512: Specifies the HMAC-SHA-512 algorithm.

nonstandard: Specifies the nonstandard GCA mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

ip: Checks IP-related fields in LSPs.

osi: Checks OSI-related fields in LSPs.

Usage guidelines

Area authentication enables IS-IS to discard routes from untrusted routers.

The key in the specified mode is inserted into all outbound Level-1 packets (LSP, CSNP, and PSNP) and is used to authenticate inbound Level-1 packets.

IS-IS keychain authentication can operate correctly only when the keys in the keychain use the HMAC-MD5 authentication algorithm.

- Before IS-IS sends a Level-1 packet, it uses the valid send key obtained from the keychain to authenticate the packet. If no valid send key exists or the valid send key does not use the HMAC-MD5 algorithm, the authentication fails and the packet does not contain authentication information.
- After IS-IS receives a Level-1 packet, it uses a valid accept key obtained from the keychain to authenticate the packet. If no valid accept key exists or all valid accept keys fail to authenticate the packet, the authentication fails and the packet is discarded.

Routers in an area must have the same authentication mode and key.

If neither **ip** nor **osi** is specified, OSI-related fields are checked.

When you specify the GCA mode, follow these guidelines:

- If you do not specify the **nonstandard** keyword, the device can communicate only with devices that use the GCA mode.
- If you specify the **nonstandard** keyword, the device can communicate only with devices that use the nonstandard GCA mode.

Examples

```
# Set the area authentication mode to simple, and set the plaintext key to 123456.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] area-authentication-mode simple plain 123456
```

Related commands

area-authentication send-only

domain-authentication-mode

isis authentication-mode

auto-cost enable

Use **auto-cost enable** to enable automatic link cost calculation.

Use **undo auto-cost enable** to disable automatic link cost calculation.

Syntax

auto-cost enable

undo auto-cost enable

Default

Automatic link cost calculation is disabled.

Views

IS-IS view

Predefined user roles

network-admin

Usage guidelines

After automatic link cost calculation is enabled, the link cost is automatically calculated based on the bandwidth reference value of an interface. When the **cost-style** is **wide** or **wide-compatible**, the cost value of an interface is calculated by using the following formula: Cost = (Reference bandwidth value / Link bandwidth) × 10. For other cost styles, [Table 1](#) applies.

Table 1 Automatic cost calculation scheme for cost styles other than wide and wide-compatible

Interface bandwidth	Cost
≤10 Mbps	60
≤100 Mbps	50
≤155 Mbps	40
≤622 Mbps	30
≤2500 Mbps	20
>2500 Mbps	10

Examples

```
# Enable automatic link cost calculation for IS-IS process 1.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] auto-cost enable
```

Related commands

bandwidth-reference

cost-style

isis cost

bandwidth-reference

Use **bandwidth-reference** to set the bandwidth reference value for automatic link cost calculation.

Use **undo bandwidth-reference** to restore the default.

Syntax

bandwidth-reference *value*

undo bandwidth-reference

Default

The bandwidth reference value is 100 Mbps.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

value: Specifies the bandwidth reference value in the range of 1 to 2147483648 Mbps.

Examples

```
# Set the bandwidth reference of IS-IS process 1 to 200 Mbps.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] bandwidth-reference 200
```

Related commands

auto-cost enable

isis cost

circuit-cost

Use **circuit-cost** to set a global IS-IS link cost.

Use **undo circuit-cost** to remove the configuration.

Syntax

```
circuit-cost cost-value [ level-1 | level-2 ]
```

```
undo circuit-cost [ level-1 | level-2 ]
```

Default

No global link cost is configured.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

cost-value: Specifies the link cost value. The value range varies by cost style.

- For styles **narrow**, **narrow-compatible**, and **compatible**, the cost value is in the range of 0 to 63.
- For styles **wide** and **wide-compatible**, the cost value is in the range of 0 to 16777215.

level-1: Applies the link cost to Level-1.

level-2: Applies the link cost to Level-2.

Usage guidelines

If no level is specified, the specified cost applies to both Level-1 and Level-2.

Examples

```
# Set the global Level-1 link cost to 11 for IS-IS process 1.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] circuit-cost 11 level-1
```

Related commands

cost-style
isis cost

cost-style

Use **cost-style** to set a cost style.

Use **undo cost-style** to restore the default.

Syntax

```
cost-style { narrow | wide | wide-compatible | { compatible | narrow-compatible }  
[ relax-spf-limit ] }  
undo cost-style
```

Default

The IS-IS cost style is **narrow**.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

narrow: Receives and sends only narrow cost style packets. The narrow cost is in the range of 0 to 63.

wide: Receives and sends only wide cost style packets. The wide cost is in the range of 0 to 16777215.

compatible: Receives and sends both wide and narrow cost style packets.

narrow-compatible: Receives both narrow and wide cost style packets, but sends only narrow cost style packets.

wide-compatible: Receives both narrow and wide cost style packets, but sends only wide cost style packets.

relax-spf-limit: Allows receiving routes with a cost greater than 1023. If you do not specify this keyword, routes with a cost bigger than 1023 will be discarded. This keyword is available only when **compatible** or **narrow-compatible** is used.

Examples

```
# Configure the router to send only narrow cost style packets, but receive both narrow and wide cost style packets.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] cost-style narrow-compatible
```

Related commands

circuit-cost

isis cost

default-route-advertise

Use **default-route-advertise** to advertise a default route of 0.0.0.0/0.

Use **undo default-route-advertise** to restore the default.

Syntax

default-route-advertise [**avoid-learning** | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

undo default-route-advertise

Default

Default route advertisement is disabled.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

avoid-learning: Avoids learning the default route received in LSPs or generated by using the ATT bit to avoid routing loops.

level-1: Advertises a Level-1 default route.

level-1-2: Advertises both Level-1 and Level-2 default routes.

level-2: Advertises a Level-2 default route.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies the tag value for the default route, in the range of 1 to 4294967295.

Usage guidelines

If no level is specified, a Level-2 default route is advertised.

The Level-1 default route is advertised to other routers in the same area, and the Level-2 default route is advertised to all the Level-2 and Level-1-2 routers.

You can use a routing policy to specify a level for the default route. The **apply isis level-1** command in routing policy view can generate a Level-1 default route. The **apply isis level-2** command in routing policy view can generate a Level-2 default route. The **apply isis level-1-2** command in routing policy view can generate both a Level-1 default route and Level-2 default route.

The tag value specified in the routing policy takes precedence over the tag value specified in this command.

Examples

Configure IS-IS process 1 to advertise a Level-2 default route.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] default-route-advertise
```

display isis

Use **display isis** to display configuration information for an IS-IS process.

Syntax

```
display isis [ process-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays configuration information for all IS-IS processes.

Examples

```
# Display IS-IS configuration information.
```

```
<Sysname> display isis
```

```
IS-IS(1) Protocol Information

Network entity           : 10.0000.0000.0001.00
IS level                 : level-1-2
Cost style               : Wide
Fast reroute             : Disabled
Preference               : 15
LSP length receive      : 1497
LSP length originate
  level-1                 : 1497
  level-2                 : 1497
Maximum imported routes : 1000
Timers
  LSP-max-age            : 1200
  LSP-refresh            : 900
  SPF intervals          : 5 50 200
IPv6 enabled
  Fast reroute           : Disabled
  Preference             : 15
  Maximum imported routes : 1000
  SPF intervals          : 5 50 200
```

Table 2 Command output

Field	Description
Network entity	Network entity name.
IS level	IS-IS routing level.
Cost style	Cost style.

Field	Description
Fast reroute	IS-IS FRR status: <ul style="list-style-type: none"> • Disabled—IS-IS FRR is disabled. • LFA—IS-IS FRR automatically calculates a backup next hop. • Route-policy—IS-IS FRR specifies a backup next hop by using a routing policy.
Preference	IS-IS route preference.
LSP length receive	Maximum LSP that can be received.
LSP length originate	Maximum LSP that can be generated.
Maximum imported routes	Maximum number of redistributed Level-1/Level-2 IPv4/IPv6 routes.
Timers	Timers: <ul style="list-style-type: none"> • LSP-max-age—Maximum life period of LSPs. • LSP-refresh—Refresh interval of LSPs. • SPF intervals—Interval between SPF calculations.
IPv6 enabled	IPv6 is enabled.

display isis event-log graceful-restart

Use **display isis event-log graceful-restart** to display IS-IS GR log information.

Syntax

display isis event-log graceful-restart slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its ID.

Examples

Display IS-IS GR log information for the specified slot.

```
<Sysname> display isis event-log graceful-restart slot 1
IS-IS loginfo :
Sep 18 08:48:24 2015 slot 1 Process 1 enter GR restarting phase(Initialization).
Sep 18 08:48:24 2015 slot 1 Process 1 enter GR phase (LSDB synchronization).
Sep 18 08:48:24 2015 slot 1 Process 1 enter GR phase (TE tunnel prepare).
Sep 18 08:48:24 2015 slot 1 Process 1 enter GR phase (First SPF computation).
Sep 18 08:48:25 2015 slot 1 Process 1 enter GR phase (Redistribution).
Sep 18 08:48:25 2015 slot 1 Process 1 enter GR phase (Second SPF computation).
Sep 18 08:48:25 2015 slot 1 Process 1 enter GR phase (LSP stability).
Sep 18 08:48:25 2015 slot 1 Process 1 enter GR phase (LSP generation).
Sep 18 08:48:25 2015 slot 1 Process 1 enter GR phase (Finish).
```

Table 3 Command output

Field	Description
GR phase	GR phase: <ul style="list-style-type: none"> • Initialization. • LSDB synchronization. • TE tunnel prepare—Preparing for TE tunnel computation. • First SPF computation. • Redistribution. • Second SPF computation. • LSP stability—Ready to generate LSPs. • LSP generation. • Finish.

display isis event-log lsp

Use **display isis event-log lsp** to display IS-IS LSP log information.

Syntax

```
display isis event-log lsp [ level-1 | level-2 ] * [ process-id ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

level-1: Displays Level-1 LSP log information.

level-2: Displays Level-2 LSP log information.

process-id: Specifies a process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSP log information for all IS-IS processes.

Usage guidelines

If you do not specify a level, the command displays both Level-1 and Level-2 LSP log information.

Examples

```
# Display IS-IS LSP log information.
```

```
<Sysname> display isis event-log lsp
```

```
LSP Log for IS-IS(1)
```

```
-----
```

```
Level-1 LSP Log
```

```
-----
```

```
Date          Time          LSPID          Seq Num      Event
```

```
-----
```

```

2015-11-06 11:10:45 1111.1111.1111.00-00 0x0000019c LSP received
2015-11-06 09:26:40 1111.1111.1111.01-00 0x00000111 Purged LSP received
2015-11-06 09:26:28 2222.2222.2222.00-00 0x00000181 LSP generated
2015-11-06 09:26:21 2222.2222.2222.00-00 0x00000180 Purged LSP generated

```

Level-2 SPF Log

```

Date          Time          LSPID          Seq Num      Event
-----
2015-11-06 11:10:45 1111.1111.1111.00-00 0x0000090d LSP received
2015-11-06 09:26:41 1111.1111.1111.01-00 0x00000101 Purged LSP received
2015-11-06 09:26:27 2222.2222.2222.00-00 0x00000171 LSP generated
2015-11-06 09:26:20 2222.2222.2222.00-00 0x00000170 Purged LSP generated

```

Table 4 Command output

Field	Description
Date	Date of the LSP change.
Time	Time of the LSP change.
LSPID	LSP ID.
Seq Num	LSP sequence number.
Event	LSP change event: <ul style="list-style-type: none"> • LSP received. • Purged LSP received. • LSP generated. • Purged LSP generated.

Related commands

reset isis event-log lsp

display isis event-log non-stop-routing

Use **display isis event-log non-stop-routing** to display IS-IS NSR log information.

Syntax

display isis event-log non-stop-routing slot *slot-number*

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

slot *slot-number*. Specifies an IRF member device by its ID.

Examples

Display IS-IS NSR log information for the specified slot.

```

<Sysname> display isis event-log non-stop-routing slot 1
IS-IS loginfo :
Sep 18 10:20:44 2015 slot 1 Enter HA Block status
Sep 18 10:20:44 2015 slot 1 Exit HA Block status
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (Initialization).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (Smooth).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (TE tunnel prepare).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (First SPF computation).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (Redistribution).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (Second SPF computation).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (LSP stability).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (LSP generation).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (Finish).
Sep 18 10:24:00 2015 slot 1 Process 100 NSR complete.

```

Table 5 Command output

Field	Description
NSR phase	NSR phase: <ul style="list-style-type: none"> • Initialization. • Smooth. • TE tunnel prepare—Preparing for TE tunnel computation. • First SPF computation. • Redistribution. • Second SPF computation. • LSP stability—Ready to generate LSPs. • LSP generation. • Finish.

display isis event-log spf

Use **display isis event-log spf** to display IS-IS route calculation log information.

Syntax

```
display isis event-log spf [ ipv4 ] [ [ level-1 | level-2 ] | verbose ] * [ process-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4: Displays IS-IS IPv4 route calculation log information. If you do not specify this keyword, the command displays IS-IS IPv4 route calculation log information for the public network.

level-1: Displays Level-1 route calculation log information.

level-2: Displays Level-2 route calculation log information.

verbose: Displays detailed route calculation log information. If you do not specify this keyword, the command displays brief route calculation log information.

process-id: Specifies a process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays route calculation log information for all IS-IS processes.

Usage guidelines

If you do not specify a level, the command displays both Level-1 and Level-2 route calculation log information.

Examples

Display brief IS-IS route calculation log information.

```
<Sysname> display isis event-log spf
```

```
SPF Log for IS-IS(1)
-----

Level-1 SPF Log
-----

Date          Time          Duration      Count      Trigger event
-----
2015-09-07 11:10:45 0              4          Interface metric changed
2015-09-07 09:26:40 0              4          LSP updated
2015-09-07 09:26:28 0              2          DIS changed
2015-09-07 09:26:21 0.001         2          LSP updated
2015-09-07 09:26:07 0.001         3          Direct route changed

Level-2 SPF Log
-----

Date          Time          Duration      Count      Trigger event
-----
2015-09-07 11:10:45 0              4          Interface metric changed
2015-09-07 09:26:40 0              4          LSP updated
2015-09-07 09:26:28 0              2          DIS changed
2015-09-07 09:26:21 0              2          LSP updated
2015-09-07 09:26:07 0              3          Direct route changed
```

Display detailed IS-IS route calculation log information.

```
<Sysname> display isis event-log spf verbose
```

```
SPF Log for IS-IS(1)
-----

Level-1 SPF Log
-----

Log date      : 2015-09-07 11:10:45
Log key       : 5
Trigger count : 4
Trigger event : Interface metric changed
SPF details   :
Phase         Duration      Description
```

TE tunnel ADJ	0	TE SPF nodes: 0
Topology	0	SPF nodes: 3
BSPF	0	Candidate NBRs: 1
LFA	0	LFA SPF nodes: 1
Area	0	Area addresses: 1
PRC	0	Add: 0 modify: 1 delete: 0
		Last 10 routes:
		1.1.1.0/24
Route summary	0	Summary route nodes: 0
Total	0	

Log date : 2015-09-07 09:26:40

Log key : 4

Trigger count : 4

Trigger event : LSP updated

SPF details :

Phase	Duration	Description
TE tunnel ADJ	0	TE SPF nodes: 0
Topology	0	SPF nodes: 3
BSPF	0	Candidate NBRs: 1
LFA	0	LFA SPF nodes: 1
Area	0	Area addresses: 1
PRC	0	Add: 0 modify: 0 delete: 0
Route summary	0	Summary route nodes: 0
Total	0	

Log date : 2015-09-07 09:26:28

Log key : 3

Trigger count : 2

Trigger event : DIS changed

SPF details :

Phase	Duration	Description
TE tunnel ADJ	0	TE SPF nodes: 0
Topology	0	SPF links changed: 1
BSPF	0	Candidate NBRs: 0
LFA	0	LFA SPF nodes: 0
Area	0	Area addresses: 0
PRC	0	Add: 0 modify: 0 delete: 0
Route summary	0	Summary route nodes: 0
Total	0	

Log date : 2015-09-07 09:26:21

Log key : 2

Trigger count : 2

Trigger event : LSP updated

SPF details :

Phase	Duration	Description
TE tunnel ADJ	0	TE SPF nodes: 0

Topology	0	SPF nodes: 0
BSPF	0	Candidate NBRs: 0
LFA	0	LFA SPF nodes: 0
Area	0	Area addresses: 1
PRC	0.001	Add: 0 modify: 0 delete: 0
Route summary	0	Summary route nodes: 0
Total	0.001	

Log date : 2015-09-07 09:26:07
 Log key : 1
 Trigger count : 3
 Trigger event : Direct route changed

SPF details :

Phase	Duration	Description
TE tunnel ADJ	0	TE SPF nodes: 0
Topology	0	SPF nodes: 0
BSPF	0	Candidate NBRs: 0
LFA	0	LFA SPF nodes: 0
Area	0	Area addresses: 1
PRC	0.001	Add: 1 modify: 0 delete: 0
		Last 10 routes:
		1.1.1.0/24
Route summary	0	Summary route nodes: 0
Total	0.001	

Level-2 SPF Log

Log date : 2015-09-07 11:10:45
 Log key : 5
 Trigger count : 4
 Trigger event : Interface metric changed

SPF details :

Phase	Duration	Description
TE tunnel ADJ	0	TE SPF nodes: 0
Topology	0	SPF nodes: 3
BSPF	0	Candidate NBRs: 1
LFA	0	LFA SPF nodes: 1
Area	0	Area addresses: 1
PRC	0	Add: 0 modify: 0 delete: 0
Route summary	0	Summary route nodes: 0
Total	0	

Log date : 2015-09-07 09:26:40
 Log key : 4
 Trigger count : 4
 Trigger event : LSP updated

SPF details :

Phase	Duration	Description
TE tunnel ADJ	0	TE SPF nodes: 0
Topology	0	SPF nodes: 3
BSPF	0	Candidate NBRs: 1
LFA	0	LFA SPF nodes: 1
Area	0	Area addresses: 1
PRC	0	Add: 0 modify: 0 delete: 0
Route summary	0	Summary route nodes: 0
Total	0	

Log date : 2015-09-07 09:26:28

Log key : 3

Trigger count : 2

Trigger event : DIS changed

SPF details :

Phase	Duration	Description
TE tunnel ADJ	0	TE SPF nodes: 0
Topology	0	SPF links changed: 1
BSPF	0	Candidate NBRs: 0
LFA	0	LFA SPF nodes: 0
Area	0	Area addresses: 0
PRC	0	Add: 0 modify: 0 delete: 0
Route summary	0	Summary route nodes: 0
Total	0	

Log date : 2015-09-07 09:26:21

Log key : 2

Trigger count : 2

Trigger event : LSP updated

SPF details :

Phase	Duration	Description
TE tunnel ADJ	0	TE SPF nodes: 0
Topology	0	SPF nodes: 0
BSPF	0	Candidate NBRs: 0
LFA	0	LFA SPF nodes: 0
Area	0	Area addresses: 1
PRC	0	Add: 0 modify: 0 delete: 0
Route summary	0	Summary route nodes: 0
Total	0	

Log date : 2015-09-07 09:26:07

Log key : 1

Trigger count : 3

Trigger event : Direct route changed

SPF details :

Phase	Duration	Description
TE tunnel ADJ	0	TE SPF nodes: 0
Topology	0	SPF nodes: 0

```

BSPF          0          Candidate NBRs: 0
LFA           0          LFA SPF nodes: 0
Area          0          Area addresses: 1
PRC           0          Add: 0 modify: 0 delete: 0
Route summary 0          Summary route nodes: 0
Total         0

```

Table 6 Command output

Field	Description
Date	Start date of route calculation.
Time	Start time of route calculation.
Duration	Route calculation duration in seconds. The value is accurate to six decimal places.
Count	Number of events that trigger the current route calculation.
Trigger event	<p>Type of the most recent event that triggers route calculation:</p> <ul style="list-style-type: none"> • NextHop changed. • DIS changed. • Interface metric changed. • SPF link changed. • Default route changed. • Summary route changed. • TE tunnel updated. • TE tunnel metric changed. • IPv6 mode changed. • FRR configuration changed. • Prefix priority configuration changed. • Route preference changed. • ISPF configuration changed. • Import filter policy changed. • ECMP configuration changed. • PIC configuration changed. • Interface LFA exclude changed. • ATT configuration changed. • GR/NSR first SPF. • GR over. • T3 timeout. • Direct route changed. • Logic interface changed. • Route leakage configuration changed. • NSR over. • Entered overload state. • Exited overload state. • Area address changed. • Route policy changed. • Redistributed route updated. • LSP updated. • MT disabled. • MT enabled. • TE tunnel configuration changed. • TE tunnel destination changed.

Field	Description
	<ul style="list-style-type: none"> RIB smooth.
Log date	Generation time of the route calculation logs.
Log key	Route calculation log key.
Trigger count	Number of events that trigger the current route calculation.
SPF details	Detailed information about the route calculation phases.
Phase	Route calculation phase: <ul style="list-style-type: none"> TE tunnel ADJ—TE tunnel adjacency calculation. Topology—Topology calculation. BSPF—Backup SPF calculation. LFA—LFA calculation. Area—Area calculation. PRC—Prefix calculation. Route summary—Route summarization calculation.
Description	Route calculation phase description: <ul style="list-style-type: none"> TE SPF nodes—Number of SPF nodes for TE tunnel adjacency calculation. SPF nodes—Number of SPF nodes for topology calculation. Candidate NBRs—Number of candidate neighbors. LFA SPF nodes—Number of SPF nodes for LFA calculation. Area addresses—Number of area addresses. Add, modify, and delete—Prefix calculation summary. Last 10 routes—10 routes that are most recently calculated. Summary route nodes—Number of summarized routes.
Total	Total duration time of all route calculation phases.

Related commands

`reset isis event-log spf`

display isis graceful-restart status

Use `display isis graceful-restart status` to display IS-IS GR state.

Syntax

`display isis graceful-restart status [level-1 | level-2] [process-id]`

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

level-1: Displays the IS-IS Level-1 GR state.

level-2: Displays the IS-IS Level-2 GR state.

process-id: Specifies a process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays GR state of all IS-IS processes.

Examples

Display IS-IS GR state.

```
<Sysname> display isis graceful-restart status
```

```

Restart information for IS-IS(1)
-----
Restart status: COMPLETE
Restart phase: Finish
Restart t1: 3, count 10; Restart t2: 60; Restart t3: 300
SA Bit: supported

```

```

Level-1 restart information
-----
Total number of interfaces: 1
Number of waiting LSPs: 0

```

```

Level-2 restart information
-----
Total number of interfaces: 1
Number of waiting LSPs: 0

```

Table 7 Command output

Field	Description
Restart status	Current GR state: <ul style="list-style-type: none"> • RESTARTING—In this state, forwarding can be ensured. • STARTING—In this state, forwarding cannot be ensured. • COMPLETE—GR is completed.
Restart phase	Current Restart phase: <ul style="list-style-type: none"> • Initialization. • LSDB synchronization. • First SPF computation. • Redistribution. • Second SPF computation. • LSP stability—Ready to generate LSPs. • LSP generation. • Finish.
Restart t1	T1 timer, in seconds.
count	Number of T1 timer expirations.
Restart t2	T2 timer, in seconds.
Restart t3	T3 timer, in seconds.
SA Bit	Whether SA is supported.
Total number of interfaces	Total number of IS-IS interfaces.
Number of waiting LSPs	Number of LSPs not obtained by the GR restarter from GR helpers during LSDB synchronization.

display isis interface

Use **display isis interface** to display IS-IS interface information.

Syntax

```
display isis interface [ [ interface-type interface-number ] [ verbose ] | statistics ] [ process-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Displays information for a specified IS-IS interface. If you do not specify this argument, the command displays information about all interfaces.

verbose: Displays detailed information about an interface. If you do not specify this keyword, the command displays brief information about an interface.

statistics: Displays IS-IS interface statistics.

process-id: Displays IS-IS interface information for an IS-IS process specified by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays interface information for all IS-IS processes.

Examples

Display brief IS-IS interface information.

```
<Sysname> display isis interface
```

```
Interface information for IS-IS(1)
```

```
-----
```

```
Interface: Vlan-interface100
```

Index	IPv4 state	IPv6 state	Circuit ID	MTU	Type	DIS
00001	Up	Down	1	1497	L1/L2	No/No

Display detailed IS-IS interface information.

```
<Sysname> display isis interface verbose
```

```
Interface information for IS-IS(1)
```

```
-----
```

```
Interface: Vlan-interface100
```

Index	IPv4 state	IPv6 state	Circuit ID	MTU	Type	DIS
00001	Up	Down	1	1497	L1/L2	No/No
SNPA address			: 000c-29e8-1bd5			
IP address			: 192.168.220.10			
Secondary IP address(es)			:			
IPv6 link-local address			:			
Extended circuit ID			: 1			
CSNP timer value			L1	10	L2	10
Hello timer value			: 10			

```

Hello multiplier value      :          3
LSP timer value           : L12      33
LSP transmit-throttle count : L12      5
Cost                      : L1       100  L2       100
IPv6 cost                 : L1       10   L2       10
Priority                   : L1       64   L2       64
Retransmit timer value    : L12      5
LDP state                  : L1      Init  L2      No-LDP
LDP sync state            : L1      Init  L2      Achieved
MPLS TE status            : L1 Disabled L2      Disabled
IPv4 BFD                   : Disabled
IPv6 BFD                   : Disabled
IPv4 FRR LFA backup       : Enabled
IPv6 FRR LFA backup       : Enabled
IPv4 prefix suppression   : Disabled
IPv6 prefix suppression   : Disabled
IPv4 tag                   : 1
IPv6 tag                   : 4294967295
IPv4 primary path detection mode: BFD ctrl
IPv6 primary path detection mode: BFD ctrl

```

Table 8 Command output

Field	Description
Interface	Interface type and number.
Index	Interface index.
IPv4 state	IPv4 state.
IPv6 state	IPv6 state.
CircuitID	Circuit ID.
MTU	Interface MTU.
Type	Interface link adjacency type.
DIS	Indicates whether the interface is elected as the Level-1/Level-2 DIS. In a P2P network, this field displays a hyphen (-) because DIS election is not performed.
SNPA address	Subnet access point address.
IP address	Primary IP address.
Secondary IP address(es)	Secondary IP addresses.
IPv6 link-local address	IPv6 link local address.
Extended circuit ID	Extended circuit ID for a P2P link.
CSNP timer value	Interval for sending CSNP packets.
Hello timer value	Interval for sending Hello packets.
Hello multiplier value	Number of invalid Hello packets.
LSP timer value	Minimum interval for sending LSP packets.
LSP transmit-throttle count	Number of LSP packets sent each time.

Field	Description
Cost	Cost of the interface.
IPv6 cost	IPv6 link cost of the interface.
Priority	DIS priority.
Retransmit timer value	Retransmission interval for LSPs on a P2P link.
MPLS TE status	MPLS TE status: Enabled or Disabled .
LDP state	LDP state: <ul style="list-style-type: none"> • Init—LDP is not reported. • No-LDP—LDP is not configured. • Not ready—LDP session is not established. • Ready—LDP session is established.
LDP sync state	LDP synchronization state: <ul style="list-style-type: none"> • Init—Initialized. • Achieved—Synchronized. • Max cost—Maintain the maximum cost.
IPv4 BFD	Whether BFD for IS-IS is enabled: <ul style="list-style-type: none"> • Disabled. • Enabled.
IPv6 BFD	Whether BFD for IPv6 IS-IS is enabled: <ul style="list-style-type: none"> • Disabled. • Enabled.
IPv4 FRR LFA backup	Whether LFA calculation is enabled for IPv4 FRR: <ul style="list-style-type: none"> • Disabled. • Enabled.
IPv6 FRR LFA backup	Whether LFA calculation is enabled for IPv6 FRR: <ul style="list-style-type: none"> • Disabled. • Enabled.
IPv4 prefix suppression	Whether IPv4 IS-IS prefix suppression is enabled: <ul style="list-style-type: none"> • Disabled. • Enabled.
IPv6 prefix suppression	Whether IPv6 IS-IS prefix suppression is enabled: <ul style="list-style-type: none"> • Disabled. • Enabled.
IPv4 tag	IPv4 tag value of the interface.
IPv6 tag	IPv6 tag value of the interface.
IPv4 primary path detection mode	IPv4 primary path detection mode: <ul style="list-style-type: none"> • BFD ctrl—BFD control packet mode. • BFD echo—BFD echo packet mode.
IPv6 primary path detection mode	IPv6 primary path detection mode: <ul style="list-style-type: none"> • BFD ctrl—BFD control packet mode. • BFD echo—BFD echo packet mode.

Display IS-IS interface statistics.

```
<Sysname> display isis interface statistics
```

```

Interface statistics information for IS-IS(1)
-----
Type          IPv4 up/down          IPv6 up/down
LAN           1/0                   0/0
P2P           0/0                   0/0

```

Table 9 Command output

Field	Description
Type	Network type of the interface: <ul style="list-style-type: none"> LAN—Broadcast network. P2P—Point-to-point network.
IPv4 up	Number of IS-IS interfaces in up state.
IPv4 down	Number of IS-IS interfaces in down state.
IPv6 up	Number of IS-ISv6 interfaces in up state.
IPv6 down	Number of IS-ISv6 interfaces in down state.

display isis lsdb

Use **display isis lsdb** to display IS-IS LSDB information.

Syntax

```

display isis lsdb [ [ level-1 | level-2 ] | local ] [ [ lsp-id lspid | lsp-name lspname ] | verbose ] *
[ process-id ]

```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

level-1: Displays the level-1 LSDB.

level-2: Displays the level-2 LSDB.

local: Displays LSP information generated locally.

lsp-id *lspid*: Specifies an LSP ID, in the form of *sysID.Pseudo ID-fragment num*, where *sysID* represents the originating node or pseudo node. *Pseudo ID* is separated by a dot from *sysID* and by a hyphen from *fragment num*.

lsp-name *lspname*: Specifies the LSP name, in the form of *Symbolic name.Pseudo ID-fragment num*, where *Pseudo ID* is separated by a dot from *Symbolic name* and by a hyphen from *fragment num*. If the Pseudo ID is 0, specify the LSP name in the form *Symbolic name-fragment num*.

verbose: Displays LSDB detailed information. If you do not specify this keyword, the command displays brief information about LSDB.

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSDBs for all IS-IS processes.

Usage guidelines

If no level is specified, the command displays both Level-1 and Level-2 LSDB information.

Examples

Display brief Level-1 LSDB information.

```
<Sysname> display isis lsdb level-1
```

```
Database information for IS-IS(1)
-----

Level-1 Link State Database
-----

LSPID                Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-----
0000.0000.0001.00-00* 0x00000087  0xf846       1152          183    0/0/0
0000.0000.0003.00-00 0x00000005  0x4bee       520           177    0/0/0
0000.0000.0003.00-01 0x00000004  0x7245       520           45     0/0/0
0000.0000.0011.00-00 0x0000000b  0xcdf6       815           183    0/0/0
```

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

Display detailed Level-1 LSDB information.

```
<Sysname> display isis lsdb level-1 verbose
```

```
Database information for IS-IS(1)
-----

Level-1 Link State Database
-----

LSPID                Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-----
0000.0000.0001.00-00* 0x00000080  0x73f        1185          183    0/0/0
Source              0000.0000.0001.00
NLPID               IPv4
Area address 10
IPv4 address 192.168.220.10
MT ID               0000 (-/-)
MT ID               0002 (-/-)
MT ID               0006 (-/-)
+NBR ID
0000.0000.0011.00          Cost: 100
Admin group: 0x00000000
Physical bandwidth: 12500000 bytes/sec
Reservable bandwidth: 0 bytes/sec
Unreserved bandwidth for each TE class:
TE class 0: 0 bytes/sec      TE class 1: 0 bytes/sec
TE class 2: 0 bytes/sec      TE class 3: 0 bytes/sec
TE class 4: 0 bytes/sec      TE class 5: 0 bytes/sec
TE class 6: 0 bytes/sec      TE class 7: 0 bytes/sec
TE class 8: 0 bytes/sec      TE class 9: 0 bytes/sec
```

```

    TE class 10: 0 bytes/sec          TE class 11: 0 bytes/sec
    TE class 12: 0 bytes/sec          TE class 13: 0 bytes/sec
    TE class 14: 0 bytes/sec          TE class 15: 0 bytes/sec
TE cost: 10
Bandwidth constraint model: Prestandard DS-TE RDM
Bandwidth constraints:
    BC[0]      : 0 bytes/sec          BC[1]      : 0 bytes/sec
Neighbor IP address: 192.168.220.30
Interface IP address: 192.168.220.10
IPv6 unicast NBR ID
    6464.6464.6464.01                Cost: 10          MT ID: 2
MT NBR ID
    6464.6464.6464.01                Cost: 10          MT ID: 6
+IP-Extended
    192.168.220.0  255.255.255.0      Cost: 100
IPv4 unicast
    1.1.1.1          255.255.255.255  Cost: 0          MT ID: 6
IPv4 unicast
    10.10.10.0       255.255.255.0    Cost: 10         MT ID: 6
IPv6 unicast
    1::1::1/128      Cost: 0          MT ID: 2
IPv6 unicast
    10::10::/64      Cost: 10         MT ID: 2
Router ID  1.1.1.1

0000.0000.0003.00-00  0x00000005  0x4bee      887          177          0/0/0
Source      0000.0000.0003.00
NLPID      IPv4
Area address 10
IPv4 address 10.10.10.10
IPv4 address 192.168.220.20
+NBR ID
    0000.0000.0001.00                Cost: 10
Admin group: 0x00000000
Physical bandwidth: 12500000 bytes/sec
Reservable bandwidth: 0 bytes/sec
Unreserved bandwidth for each TE class:
    TE class 0: 0 bytes/sec          TE class 1: 0 bytes/sec
    TE class 2: 0 bytes/sec          TE class 3: 0 bytes/sec
    TE class 4: 0 bytes/sec          TE class 5: 0 bytes/sec
    TE class 6: 0 bytes/sec          TE class 7: 0 bytes/sec
    TE class 8: 0 bytes/sec          TE class 9: 0 bytes/sec
    TE class 10: 0 bytes/sec         TE class 11: 0 bytes/sec
    TE class 12: 0 bytes/sec         TE class 13: 0 bytes/sec
    TE class 14: 0 bytes/sec         TE class 15: 0 bytes/sec
TE cost: 10
Bandwidth constraint model: Prestandard DS-TE RDM
Bandwidth constraints:

```

```

BC[0]: 0 bytes/sec
BC[1]: 0 bytes/sec
Interface IP address: 192.168.220.20
Neighbor IP address: 192.168.220.10
Router ID 3.3.3.3

0000.0000.0003.00-01 0x00000004 0x7245 887 45 0/0/0
Source 0000.0000.0003.00
+IP-Extended
10.10.10.0 255.255.255.0 Cost: 10
+IP-Extended
192.168.220.0 255.255.255.0 Cost: 10

```

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

Table 10 Command output

Field	Description
LSPID	LSP ID.
Seq Num	LSP sequence number.
Checksum	LSP checksum.
Holdtime	LSP lifetime, which decreases as time elapses.
Length	LSP length.
ATT/P/OL	<ul style="list-style-type: none"> • ATT—Attach bit. • P—Partition bit. • OL—Overload bit. 1 means the LSP bit is set and 0 means the LSP bit is not set.
Source	System ID of the originating router.
HOST NAME	Dynamic host name of the originating router.
ORG ID	Original system ID of the virtual system of the originating router.
NLPID	Network layer protocol the originating router runs.
Area address	Area address of the originating router.
IPv4 address	IP address of the originating router's IS-IS interface.
IPv6 address	IPv6 address of the originating router's IS-ISv6 interface.
MT ID 0000 (-/-) MT ID 0002 (-/-) MT ID 0006 (-/-)	Topology supported by the originating router (0/0/0 indicates ATT/P/OL): <ul style="list-style-type: none"> • 0000—Base topology. • 0002—IPv6 unicast topology. • 0006—IPv4 unicast topology. • (-/-)—Attach bit/overload bit.
NBR ID	Neighbor ID of the originating router.
MT NBR ID	IPv4 unicast topology neighbor information about the originating router.
IPv6 unicast NBR ID	IPv6 unicast neighbor information about the originating router.
Admin group	Link management group attribute.
Interface IP address	IP address of the interface connected to the remote end.

Field	Description
Neighbor IP address	Neighbor interface IP address.
Physical bandwidth	Physical bandwidth.
Reservable bandwidth	Reserved bandwidth.
Unreserved bandwidth for each TE class	Available bandwidth reserved for each TE class.
TE class	Available bandwidth for each of the 8 or 16 TE classes.
TE cost	TE cost.
Bandwidth constraint model	Bandwidth constraint model: <ul style="list-style-type: none"> • Prestandard DS-TE RDM. • IETF DS-TE RDM. • IETF DS-TE MAM.
BC	Bandwidth constraint value. The Prestandard model supports 2 BCs, and the IETF modes support a maximum of 8 BCs.
Router ID	Router ID.
IP-Internal	Internal IP address and mask of the originating router.
IP-External	External IP address and mask of the originating router.
IP-Extended	Extended IP address and mask of the originating router.
Cost	Cost.
Auth	Authentication information of the originating router.
IPv6	Internal IPv6 address and prefix of the originating router.
IPv6-Ext	External IPv6 address and prefix of the originating router.
IPv4 unicast	IPv4 unicast reachability information about the originating router.
IPv6 unicast	Internal IPv6 unicast reachability information about the originating router.
IPv6 unicast-ext	External IPv6 unicast reachability information about the originating router.

display isis lsdb statistics

Use **display isis lsdb statistics** to display IS-IS LSDB statistics.

Syntax

```
display isis lsdb statistics [ level-1 | level-2 ] [ process-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

level-1: Displays Level-1 LSDB statistics.

level-2: Displays Level-2 LSDB statistics.

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSDB statistics for all IS-IS processes.

Usage guidelines

If you do not specify a level, the command displays both Level-1 and Level-2 LSDB statistics.

Examples

Display IS-IS LSDB statistics.

```
<Sysname> display isis lsdb statistics
```

```
Database Statistics information for IS-IS(1)
-----

Level-1 LSDB Statistics
-----

LSP source ID                                     LSP count
-----
Total                                             333
1111.1111.1111.00                                1
2222.2222.2222.00                                256
2222.2222.2222.01                                1
bbbb.bbbb.0001.00                                75

Level-2 LSDB Statistics
-----

LSP source ID                                     LSP count
-----
Total                                             663
1111.1111.1111.00                                256
2222.2222.2222.00                                256
2222.2222.2222.01                                1
aaaa.aaaa.0001.00                                75
bbbb.bbbb.0001.00                                75
```

Table 11 Command output

Field	Description
LSP count	Number of LSPs generated by a source.
Total	Number of LSPs generated by all sources.

Related commands

display isis lsdb

display isis name-table

Use **display isis name-table** to display the host name-to-system ID mapping table.

Syntax

display isis name-table [*process-id*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

process-id: Displays the host name to system ID mapping table for an IS-IS process specified by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the host name to system ID mapping table for all IS-IS processes.

Examples

Display the IS-IS host name to system ID mapping table.

```
<Sysname> display isis name-table
                        Name table information for IS-IS(1)
                        -----
System ID              Hostname                Type           Level
6789.0000.0001        RUTA                      DYNAMIC        Level-1
6789.0000.0001        RUTA                      DYNAMIC        Level-2
0000.0000.0041        RUTB                      STATIC         Level-1
0000.0000.0041        RUTB                      STATIC         Level-2
6789.0000.0001.01    DIS-A                    DYNAMIC        Level-1
0000.0000.0041.01    DIS-B                    DYNAMIC        Level-2
```

Table 12 Command output

Field	Description
System ID	System ID.
Hostname	Host name.
Type	Mapping type: <ul style="list-style-type: none">• STATIC.• DYNAMIC.
Level	Level on which the system ID-to-host name mapping takes effect: Level-1 or Level-2.

display isis non-stop-routing status

Use **display isis non-stop-routing status** to display IS-IS NSR status.

Syntax

display isis non-stop-routing status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IS-IS NSR status.

```
<Sysname> display isis non-stop-routing status
```

```
Nonstop Routing information for IS-IS(1)
-----
NSR phase: Finish
```

Table 13 Command output

Field	Description
NSR phase	NSR phase: <ul style="list-style-type: none">• Initialization.• Smooth.• First SPF computation.• Redistribution.• Second SPF computation.• LSP stability—Ready to generate LSPs.• LSP generation.• Finish.

display isis packet

Use **display isis packet** to display IS-IS packet statistics.

Syntax

```
display isis packet { csnp | hello | lsp | psnp } by-interface [ verbose ] [ interface-type  
interface-number ] [ process-id ]
```

```
display isis packet { csnp | hello | lsp | psnp } [ verbose ] [ process-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

csnp: Displays CSNP packet statistics.

hello: Displays hello packet statistics.

lsp: Displays LSP packet statistics.

psnp: Displays PSNP packet statistics.

by-interface: Displays packet statistics on a per-interface basis.

verbose: Displays detailed packet statistics.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this option, the command displays IS-IS packet statistics for all interfaces.

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays packet statistics for all IS-IS processes.

Examples

Display detailed hello packet statistics on a per-interface basis.

<Sysname> display isis packet hello by-interface verbose

```
                Hello packet information for IS-IS(1)
                -----

Interface:  Vlan-interfaces10
Total output packets : 0          Total output error packets : 0
Total input packets  : 0          Total input error packets  : 0

Input packets with errors
  Bad packet length      : 0          Bad header length          : 0
  Jumbo packet           : 0          Bad protocol description   : 0
  Bad protocol ID       : 0          Bad protocol version      : 0
  Unknown packet type   : 0          Bad max area count        : 0
  Bad system ID length  : 0          Bad circuit type          : 0
  Bad auth TLV: 0       : 0          Bad area address TLV      : 0
  Auth failure          : 0          Excessive area addresses  : 0
  Bad NBR TLV          : 0          Excessive auth TLVs      : 0
  Excessive IF Addr TLVs: 0         Excessive IF addresses   : 0
  Bad IF address TLV   : 0          Duplicate system ID       : 0
  Bad TLV length        : 0          Bad IP address            : 0
  Duplicate IP address  : 0          Mismatched area address   : 0
  Mismatched protocol  : 0          Mismatched network type  : 0
  Bad IPv6 address TLV : 0          Bad IPv6 address          : 0
  Duplicate IPv6 address: 0         Bad MT ID TLV             : 0
  SNPA conflict (LAN)  : 0          Excessive NBR SNPAs (LAN) : 0
  Mismatched level (LAN): 0         Bad 3-Way option TLV (P2P) : 0
  No common MT ID (P2P) : 0         Bad circuit ID (P2P)     : 0
```

Display detailed hello packet statistics.

<Sysname> display isis packet hello verbose

```
                Hello packet information for IS-IS(1)
                -----

Total output packets : 0          Total output error packets : 0
Total input packets  : 0          Total input error packets  : 0

Input packets with errors
  Bad packet length      : 0          Bad header length          : 0
  Jumbo packet           : 0          Bad protocol description   : 0
  Bad protocol ID       : 0          Bad protocol version      : 0
  Unknown packet type   : 0          Bad max area count        : 0
  Bad system ID length  : 0          Bad circuit type          : 0
  Bad auth TLV          : 0          Bad area address TLV      : 0
  Auth failure          : 0          Excessive area addresses  : 0
  Bad NBR TLV          : 0          Excessive auth TLVs      : 0
```

Excessive IF Addr TLVs	: 0	Excessive IF addresses	: 0
Bad IF address TLV	: 0	Duplicate system ID	: 0
Bad TLV length	: 0	Bad IP address	: 0
Duplicate IP address	: 0	Mismatched area address	: 0
Mismatched protocol	: 0	Mismatched network type	: 0
Bad IPv6 address TLV	: 0	Bad IPv6 address	: 0
Duplicate IPv6 address	: 0	Bad MT ID TLV	: 0
SNPA conflict (LAN)	: 0	Excessive NBR SNPAs (LAN)	: 0
Mismatched level (LAN)	: 0	Bad 3-Way option TLV (P2P)	: 0
No common MT ID (P2P)	: 0	Bad circuit ID (P2P)	: 0

Table 14 Command output

Field	Description
Input packets with errors	<p>Statistics for packets with the following errors:</p> <ul style="list-style-type: none"> • Bad packet length—Invalid packet length. • Bad header length—Invalid header length. • Jumbo packet—The packet length exceeds the buffer size or the interface MTU. • Bad protocol description—Invalid protocol description. • Bad protocol ID—Invalid protocol identifier. • Bad protocol version—Invalid protocol version. • Unknown packet type—Unknown packet type. • Bad max area count—Invalid maximum number of area addresses. • Bad system ID length—Invalid system ID length. • Bad circuit type—Invalid interface type. • Bad auth TLV—Invalid authentication TLV. • Bad area address TLV—Invalid area address TLV. • Auth failure—Authentication failure. • Excessive area addresses—Excessive area addresses. • Bad NBR TLV—Invalid neighbor TLV. • Excessive auth TLVs—Excessive authentication TLVs. • Excessive IF Addr TLVs—Excessive interface address TLVs. • Excessive IF addresses—Excessive interface addresses. • Bad IF address TLV—Invalid interface address TLV. • Duplicate system ID—Duplicate system IDs. • Bad TLV length—Invalid TLV length. • Bad IP address—The IP address does not belong to the same network as the local interface address. • Duplicate IP address—Duplicate IP addresses. • Mismatched area address—Mismatched area addresses. • Mismatched protocol—Mismatched protocols. • Mismatched network type—Mismatched network types. • Bad IPv6 address TLV—Invalid IPv6 address TLV. • Bad IPv6 address—Invalid IPv6 address. • Duplicate IPv6 address—Duplicate IPv6 addresses. • SNPA conflict (LAN)—SNPA conflict. • Excessive NBR SNPAs (LAN)—Excessive neighbor SNPAs. • Mismatched level (LAN)—Mismatched levels. • Bad 3-Way option TLV (P2P)—Invalid three-way handshake information. • Bad circuit ID (P2P)—Invalid circuit ID.

Display detailed LSP packet statistics on a per-interface basis.

<Sysname> display isis packet lsp by-interface verbose

LSP packet information for IS-IS(1)

Interface: Vlan-interfaces10

Total output packets : 0 Total output error packets : 0

Total input packets : 0 Total input error packets : 0

Input packets with errors

Bad packet length	: 0	Bad header length	: 0
Jumbo packet	: 0	SNPA conflict (LAN)	: 0
Smaller than header	: 0	Bad protocol description	: 0
Bad protocol ID	: 0	Bad protocol version	: 0
Unknown packet type	: 0	Bad max area count	: 0
No active NBR	: 0	Bad system ID length	: 0
Mismatched level	: 0	Illegal IS type	: 0
Sequence number is 0	: 0	Checksum is 0	: 0
Incorrect checksum	: 0	Bad TLV length	: 0
Mismatched protocol	: 0	Bad auth TLV	: 0
Auth failure	: 0	Excessive auth TLVs	: 0
Bad NBR TLV	: 0	Bad extended IS TLV	: 0
Bad IF address TLV	: 0	Bad IPv6 IF address TLV	: 0
Bad alias TLV	: 0	Bad IP reachability TLV	: 0
Bad MT IS TLV	: 0	Bad area address TLV	: 0
Bad MT ID TLV	: 0	Bad MT IP TLV	: 0
Bad MT IPv6 TLV	: 0	Bad IPv6 reachability TLV	: 0
Bad router ID TLV	: 0		

Display detailed LSP packet statistics.

<Sysname> display isis packet lsp verbose

LSP packet information for IS-IS(1)

Total output packets : 0 Total output error packets : 0

Total input packets : 0 Total input error packets : 0

Input packets with errors

Bad packet length	: 0	Bad header length	: 0
Jumbo packet	: 0	SNPA conflict (LAN)	: 0
Smaller than header	: 0	Bad protocol description	: 0
Bad protocol ID	: 0	Bad protocol version	: 0
Unknown packet type	: 0	Bad max area count	: 0
No active NBR	: 0	Bad system ID length	: 0
Mismatched level	: 0	Illegal IS type	: 0
Sequence number is 0	: 0	Checksum is 0	: 0

```

Incorrect checksum      : 0          Bad TLV length          : 0
Mismatched protocol    : 0          Bad auth TLV           : 0
Auth failure           : 0          Excessive auth TLVs    : 0
Bad NBR TLV           : 0          Bad extended IS TLV    : 0
Bad IF address TLV     : 0          Bad IPv6 IF address TLV : 0
Bad alias TLV          : 0          Bad IP reachability TLV : 0
Bad MT IS TLV          : 0          Bad area address TLV   : 0
Bad MT ID TLV          : 0          Bad MT IP TLV           : 0
Bad MT IPv6 TLV        : 0          Bad IPv6 reachability TLV : 0
Bad router ID TLV      : 0

```

Table 15 Command output

Field	Description
Input packets with errors	<p>Statistics for packets with the following errors:</p> <ul style="list-style-type: none"> • Bad packet length—Invalid packet length. • Bad header length—Invalid header length. • Jumbo packet—The packet length exceeds the maximum length of packets that can be received. • SNPA conflict (LAN)—SNPA conflict. • Smaller than header—The packet length is smaller than the fixed header length. • Bad protocol description—Invalid protocol description. • Bad protocol ID—Invalid protocol identifier. • Bad protocol version—Invalid protocol version. • Unknown packet type—Unknown packet type. • Bad max area count—Invalid maximum number of area addresses. • No active NBR—The packet is from an unknown neighbor. • Bad system ID length—Invalid system ID length. • Mismatched level—Mismatched levels. • Illegal IS type—Invalid IS type. • Sequence number is 0—The sequence number is 0. • Checksum is 0—The checksum is 0. • Incorrect checksum—Incorrect checksum. • Bad TLV length—Invalid TLV length. • Mismatched protocol—Mismatched protocols. • Bad auth TLV—Invalid authentication TLV. • Auth failure—Authentication failure. • Excessive auth TLVs—Excessive authentication TLVs. • Bad NBR TLV—Invalid neighbor TLV. • Bad extended IS TLV—Invalid extended IS TLV. • Bad IF address TLV—Invalid interface address TLV. • Bad IPv6 IF address TLV—Invalid IPv6 interface address TLV. • Bad alias TLV—Invalid alias TLV. • Bad IP reachability TLV—Invalid IP reachability TLV. • Bad area address TLV—Invalid area address TLV. • Bad MT IPv6 TLV—Invalid IPv6 topology TLV. • Bad IPv6 reachability TLV—Invalid IPv6 reachability TLV. • Bad router ID TLV—Invalid router ID TLV.

Display detailed CSNP packet statistics on a per-interface basis.

```
<Sysname> display isis packet csnp by-interface verbose
```

CSNP packet information for IS-IS(1)

```
Interface: Vlan-interface10
Total output packets : 0          Total output error packets : 0
Total input packets  : 0          Total input error packets  : 0
```

```
Input packets with errors
Bad packet length  : 0          Bad header length      : 0
Jumbo packet      : 0          SNPA conflict (LAN)    : 0
Smaller than header: 0          Bad protocol description: 0
Bad protocol ID   : 0          Bad protocol version   : 0
Unknown packet type: 0          Bad max area count     : 0
No active NBR     : 0          Bad system ID length   : 0
Mismatched level  : 0          Bad TLV length         : 0
Auth failure      : 0          Bad auth TLV           : 0
Bad LSP TLV length: 0          Excessive auth TLVs    : 0
Excessive LSPs    : 0          Bad LSP ID             : 0
```

Display detailed CSNP packet statistics.

<Sysname> display isis packet csnp verbose

CSNP packet information for IS-IS(1)

```
Total output packets : 0          Total output error packets : 0
Total input packets  : 0          Total input error packets  : 0
```

```
Input packets with errors
Bad packet length  : 0          Bad header length      : 0
Jumbo packet      : 0          SNPA conflict (LAN)    : 0
Smaller than header: 0          Bad protocol description: 0
Bad protocol ID   : 0          Bad protocol version   : 0
Unknown packet type: 0          Bad max area count     : 0
No active NBR     : 0          Bad system ID length   : 0
Mismatched level  : 0          Bad TLV length         : 0
Auth failure      : 0          Bad auth TLV           : 0
Bad LSP TLV length: 0          Excessive auth TLVs    : 0
Excessive LSPs    : 0          Bad LSP ID             : 0
```

Table 16 Command output

Field	Description
Input packets with errors	<p>Statistics for packets with the following errors:</p> <ul style="list-style-type: none"> • Bad packet length—Invalid packet length. • Bad header length—Invalid header length. • Jumbo packet—The packet length exceeds the maximum length of packets that can be received. • SNPA conflict (LAN)—SNPA conflict. • Smaller than header—The packet length is smaller than the fixed

Field	Description
	header length. <ul style="list-style-type: none"> • Bad protocol description—Invalid protocol description. • Bad protocol ID—Invalid protocol identifier. • Bad protocol version—Invalid protocol version. • Unknown packet type—Unknown packet type. • Bad max area count—Invalid maximum number of area addresses. • No active NBR—The packet is from an unknown neighbor. • Bad system ID length—Invalid system ID length. • Mismatched level—Mismatched levels. • Bad TLV length—Invalid TLV length. • Auth failure—Authentication failure. • Bad auth TLV—Invalid authentication TLV. • Bad LSP TLV length—Invalid LSP TLV length. • Excessive auth TLVs—Excessive authentication TLVs. • Excessive LSPs—Excessive LSPs. • Bad LSP ID—Invalid LSP ID.

Display detailed PSNP packet statistics on a per-interface basis.

```
<Sysname> display isis packet psnp by-interface verbose
```

```

PSNP packet information for IS-IS(1)
-----

Interface: Vlan-interface10
Total output packets : 0          Total output error packets : 0
Total input packets  : 0          Total input error packets  : 0

Input packets with errors
Bad packet length   : 0          Bad header length         : 0
Jumbo packet       : 0          SNPA conflict (LAN)      : 0
Smaller than header: 0          Bad protocol description: 0
Bad protocol ID    : 0          Bad protocol version     : 0
Unknown packet type: 0          Bad max area count       : 0
No active NBR     : 0          Bad system ID length     : 0
Mismatched level  : 0          Bad TLV length           : 0
Auth failure      : 0          Bad auth TLV             : 0
Bad LSP TLV length: 0          Excessive auth TLVs     : 0
Excessive LSPs   : 0          Bad LSP ID               : 0

```

Display detailed PSNP packet statistics.

```
<Sysname> display isis packet psnp verbose
```

```

PSNP packet information for IS-IS(1)
-----

Total output packets : 0          Total output error packets : 0
Total input packets  : 0          Total input error packets  : 0

Input packets with errors

```

```

Bad packet length      : 0          Bad header length      : 0
Jumbo packet          : 0          SNPA conflict (LAN)    : 0
Smaller than header   : 0          Bad protocol description : 0
Bad protocol ID       : 0          Bad protocol version   : 0
Unknown packet type   : 0          Bad max area count     : 0
No active NBR         : 0          Bad system ID length   : 0
Mismatched level      : 0          Bad TLV length         : 0
Auth failure          : 0          Bad auth TLV           : 0
Bad LSP TLV length    : 0          Excessive auth TLVs    : 0
Excessive LSPs       : 0          Bad LSP ID             : 0

```

Table 17 Command output

Field	Description
Input packets with errors	<p>Statistics for packets with the following errors:</p> <ul style="list-style-type: none"> • Bad packet length—Invalid packet length. • Bad header length—Invalid header length. • Jumbo packet—The packet length exceeds the maximum length of packets that can be received. • SNPA conflict (LAN)—SNPA conflict. • Smaller than header—The packet length is smaller than the fixed header length. • Bad protocol description—Invalid protocol description. • Bad protocol ID—Invalid protocol identifier. • Bad protocol version—Invalid protocol version. • Unknown packet type—Unknown packet type. • Bad max area count—Invalid maximum number of area addresses. • No active NBR—The packet is from an unknown neighbor. • Bad system ID length—Invalid system ID length. • Mismatched level—Mismatched levels. • Bad TLV length—Invalid TLV length. • Auth failure—Authentication failure. • Bad auth TLV—Invalid authentication TLV. • Bad LSP TLV length—Invalid LSP TLV length. • Excessive auth TLVs—Excessive authentication TLVs. • Excessive LSPs—Excessive LSPs. • Bad LSP ID—Invalid LSP ID.

Related commands

`reset isis packet`

display isis peer

Use `display isis peer` to display IS-IS neighbor information.

Syntax

`display isis peer [statistics | verbose] [process-id]`

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

statistics: Displays IS-IS neighbor statistics.

verbose: Displays detailed IS-IS neighbor information. If you do not specify this keyword, the command displays brief IS-IS neighbor information.

process-id: Displays IS-IS neighbor information for an IS-IS process specified by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays neighbor information for all IS-IS processes.

Examples

Display brief IS-IS neighbor information.

```
<Sysname> display isis peer
```

```
Peer information for IS-IS(1)
-----

System ID: 0000.0000.0001
Interface: Vlan100          Circuit Id: 0000.0000.0001.01
State: Up      HoldTime: 27s   Type: L1(L1L2)      PRI: 64

System ID: 0000.0000.0001
Interface: Vlan100          Circuit Id: 0000.0000.0001.01
State: Up      HoldTime: 27s   Type: L2(L1L2)      PRI: 64
```

Display detailed IS-IS neighbor information.

```
<Sysname> display isis peer verbose
```

```
Peer information for IS-IS(1)
-----

System ID: 0000.1111.2222
Interface: Vlan100          Circuit Id: 0000.1111.2222.01
State: Up      Holdtime: 6s    Type: L1(L1L2)      PRI: 64
Area address(es): 49
Peer IP address(es): 12.0.0.2
Peer local circuit ID: 1
Peer circuit SNPA address: 000c-293b-c4be
Uptime: 00:05:07
Adj protocol: IPv4
Adj P2P three-way handshake: No
Graceful Restart capable
  Restarting signal: No
  Suppress adjacency advertisement: No
Local topology:
  0
Remote topology:
  0  2
```

```

System ID: 0000.0000.0002
Interface: Vlan101          Circuit Id: 001
State: Up      HoldTime: 27s      Type: L1L2      PRI: --
Area address(es): 49
Peer IP address(es): 192.168.220.30
Peer local circuit ID: 1
Peer circuit SNPA address: 000c-29fd-ed69
Uptime: 00:05:07
Adj protocol: IPv4
Adj P2P three-way handshake: Yes
    Peer extended circuit ID: 2
Graceful Restart capable
    Restarting signal: No
    Suppress adjacency advertisement: No

```

Table 18 Command output

Field	Description
System ID	System ID of the neighbor.
Interface	Interface connecting to the neighbor.
Circuit Id	Circuit ID.
State	Circuit state.
HoldTime	Within the holdtime, if no hellos are received from the neighbor, the neighbor is considered down. If a hello is received, the holdtime is reset to the initial value.
Type	Circuit type: <ul style="list-style-type: none"> • L1—Means the circuit type is Level-1 and the neighbor is a Level-1 router. • L2—Means the circuit type is Level-2 and the neighbor is a Level-2 router. • L1(L1L2)—Means the circuit type is Level-1 and the neighbor is a Level-1-2 router. • L2(L1L2)—Means the circuit type is Level-2 and the neighbor is a Level-1-2 router.
PRI	DIS priority of the neighbor.
Area Address(es)	Area address of the neighbor.
Peer IP Address(es)	IP address of the neighbor.
Uptime	Time elapsed since the neighbor relationship was formed.
Adj Protocol	Adjacency protocol: IPv4 or IPv6.
Peer local circuit ID	Circuit ID of the neighbor.
Peer circuit SNPA address	SNPA address of the neighbor.
Adj P2P three-way handshake	Indicates whether the neighbor supports P2P three-way handshake.
Peer extended circuit ID	Extended circuit ID of the neighbor interface. This field is available when the neighbor supports three-way handshake.
Graceful Restart capable	The neighbor has the GR helper capability.

Field	Description
Restarting signal	RR flag.
Suppress adjacency advertisement	SA flag.
Local topology	List of topologies supported by the local interface.
Remote topology	List of topologies supported by the neighbor interface.

Display IS-IS neighbor statistics.

```
<Sysname> display isis peer statistics
```

```

Peer Statistics information for IS-IS(1)
-----
Type          IPv4 Up/Init          IPv6 Up/Init
LAN Level-1   1/0                   0/0
LAN Level-2   1/0                   0/0
P2P           0/0                   0/0

```

Table 19 Command output

Field	Description
Type	Neighbor type: <ul style="list-style-type: none"> LAN Level-1—Number of Level-1 neighbors whose network type is broadcast. LAN Level-2—Number of Level-2 neighbors whose network type is broadcast. P2P—Number of neighbors whose network type is P2P.
IPv4 Up	Number of IPv4 neighbors in up state.
IPv4 Init	Number of IPv4 neighbors in init state.
IPv6 Up	Number of IPv6 neighbors in up state.
IPv6 Init	Number of IPv6 neighbors in init state.

display isis redistribute

Use **display isis redistribute** to display the redistributed IS-IS routing information.

Syntax

```
display isis redistribute [ ipv4 [ ip-address mask-length ] ] [ level-1 | level-2 ] [ process-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4: Displays the redistributed IPv4 routing information (the default).

ip-address mask-length: Specifies the destination IP address and mask length.

process-id: Specifies the IS-IS process by its ID in the range of 1 to 65535.

level-1: Displays the IS-IS Level-1 routing information.

level-2: Displays the IS-IS Level-2 routing information.

Usage guidelines

If you do not specify an IS-IS level, this command displays both Level-1 and Level-2 routing information.

Examples

Display redistributed IPv4 routing information.

```
<Sysname> display isis redistribute 1
```

```
Route information for IS-IS(1)
-----

Level-1 IPv4 Redistribute Table
-----

Type IPv4 Destination      IntCost  ExtCost  Tag      State
-----
D     192.168.30.0/24        0        0        0        Active
D     11.11.11.11/32         0        0        0
D     10.10.10.0/24          0        0        0
```

Table 20 Command output

Field	Description
Route information for IS-IS(1)	IS-IS process of the redistributed routing information.
Level-1 IPv4 Redistribute Table	Redistributed IPv4 routing information of IS-IS Level-1.
Level-2 IPv4 Redistribute Table	Redistributed IPv4 routing information of IS-IS Level-2.
Type	Redistributed route type.
IPv4 Destination	IPv4 destination address.
IntCost	Internal cost of the route.
ExtCost	External cost of the route.
Tag	Tag value.
State	Indicates whether the route is valid.

display isis route

Use **display isis route** to display IS-IS IPv4 routing information.

Syntax

```
display isis route [ ipv4 [ ip-address mask-length ] ] [ [ level-1 | level-2 ] ] verbose ] * [ process-id ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

ipv4: Displays IS-IS IPv4 routing information (the default).

ip-address mask-length: Displays IS-IS IPv4 routing information for the specified IP address. The *mask-length* argument is in the range of 0 to 32.

verbose: Displays detailed IS-IS IPv4 routing information. If you do not specify this keyword, the command displays brief IS-IS IPv4 routing information

process-id: Displays IS-IS IPv4 routing information for an IS-IS process specified by its ID in the range of 1 to 65535. If you do not specify an IS-IS process, this command displays routing information for all IS-IS processes.

level-1: Displays Level-1 IS-IS routes.

level-2: Displays Level-2 IS-IS routes.

Usage guidelines

If you do not specify a level, this command displays both Level-1 and Level-2 routing information.

Examples

Display brief IS-IS IPv4 routing information.

```
<Sysname> display isis route
```

```
Route information for IS-IS(1)
-----

Level-1 IPv4 Forwarding Table
-----

IPv4 Destination      IntCost      ExtCost      ExitInterface      NextHop      Flags
-----
8.8.8.0/24            10           NULL         Vlan100            Direct       D/L/-
9.9.9.0/24            20           NULL         Vlan100            8.8.8.5     R/L/-
```

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down bit set

```
Level-2 IPv4 Forwarding Table
-----

IPv4 Destination      IntCost      ExtCost      ExitInterface      NextHop      Flags
-----
8.8.8.0/24            10           NULL         NULL                NULL         D/L/-
```

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down bit set

Table 21 Command output

Field	Description
Route information for IS-IS(1)	Route information for IS-IS process 1.

Field	Description
Level-1 IPv4 Forwarding Table	IS-IS IPv4 routing information for Level-1.
Level-2 IPv4 Forwarding Table	IS-IS IPv4 routing information for Level-2.
IPv4 Destination	IPv4 destination address.
IntCost	Internal cost.
ExtCost	External cost.
ExitInterface	Output interface.
NextHop	Next hop.
Flags	Routing state flag: <ul style="list-style-type: none"> • D—Direct route. • R—The route has been added into the routing table. • L—The route has been advertised in an LSP. • U—Penetration flag. Setting it to UP can prevent an LSP sent from L2 to L1 from being sent back to L2.

Display detailed IS-IS IPv4 routing information.

```
<Sysname> display isis route verbose
```

```

                                Route information for IS-IS(1)
                                -----

                                Level-1 IPv4 Forwarding Table
                                -----

IPv4 Dest : 8.8.8.0/24           Int. Cost : 10           Ext. Cost : NULL
Admin Tag : -                   Src Count  : 2           Flag       : D/L/-
NextHop   :                     Interface   :                     ExitIndex  :
    Direct                               Vlan100      0x00000000
Nib ID    : 0x0

IPv4 Dest : 9.9.9.0/24           Int. Cost : 20           Ext. Cost : NULL
Admin Tag : -                   Src Count  : 1           Flag       : R/L/-
NextHop   :                     Interface   :                     ExitIndex  :
    8.8.8.5                             Vlan100      0x00000003
Nib ID    : 0x0

```

```
Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down bit set
```

```

                                Level-2 IPv4 Forwarding Table
                                -----

IPv4 Dest : 8.8.8.0/24           Int. Cost : 10           Ext. Cost : NULL
Admin Tag : -                   Src Count  : 2           Flag       : D/L/-

```

```
Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down bit set
```

Table 22 Command output

Field	Description
Route information for IS-IS(1)	Route information for IS-IS process 1.
Level-1 IPv4 Forwarding Table	IS-IS IPv4 routing information for Level-1.
Level-2 IPv4 Forwarding Table	IS-IS IPv4 routing information for Level-2.
IPV4 Dest	IPv4 destination.
Int. Cost	Internal cost.
Ext. Cost	External cost.
Admin Tag	Tag.
Src Count	Count of advertising sources.
Flag	Route state flag: <ul style="list-style-type: none"> • R—The route has been installed into the routing table. • L—The route has been flooded in an LSP. • U—Route leaking flag. Setting it to UP can prevent an LSP sent from L2 to L1 from being sent back to L2.
Next Hop	Next hop.
Interface	Output interface.
ExitIndex	Index of the output interface.
Nib ID	ID assigned by the routing management module (next hop index).

display isis spf-tree

Use **display isis spf-tree** to display IS-IS IPv4 SPF tree information.

Syntax

```
display isis spf-tree [ ipv4 ] [ [ level-1 | level-2 ] | verbose ] * [ process-id ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

ipv4: Displays IS-IS IPv4 SPF tree information. If you do not specify this keyword, the command displays IS-IS IPv4 SPF tree information.

level-1: Displays Level-1 IS-IS SPF tree information. If you do not specify a level, the command displays both Level-1 and Level-2 SPF tree information.

level-2: Displays Level-2 SPF tree information. If you do not specify a level, the command displays both Level-1 and Level-2 SPF tree information.

verbose: Displays detailed IS-IS SPF tree information. If you do not specify this keyword, the command displays brief IS-IS SPF tree information.

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays SPF tree information for all IS-IS processes.

Examples

Display brief IS-IS IPv4 SPF tree information.

```
<Sysname> display isis spf-tree
```

Shortest Path Tree for IS-IS(1)

Flags: S-Node is on SPF tree T-Node is on tent list
O-Node is overload R-Node is directly reachable
I-Node or Link is isolated D-Node or Link is to be deleted
C-Neighbor is child P-Neighbor is parent
V-Link is involved N-Link is a new path
L-Link is on change list U-Protocol usage is changed
H-NextHop is changed

Level-1 Shortest Path Tree

SpfNode	NodeFlag	SpfLink	LinkCost	LinkFlag
0000.0000.0032.00	S/-/-/-/-/-	-->0000.0000.0032.01	10	-/-/C/-/-/-/-/-
		-->0000.0000.0064.00	10	-/-/C/-/-/-/-/-
0000.0000.0032.01	S/-/-/R/-/-	-->0000.0000.0064.00	0	-/-/C/-/-/-/-/-
		-->0000.0000.0032.00	0	-/-/-/P/-/-/-/-/-
0000.0000.0064.00	S/-/-/R/-/-	-->0000.0000.0032.00	10	-/-/-/P/-/-/-/-/-
		-->0000.0000.0032.01	10	-/-/-/P/-/-/-/-/-

Level-2 Shortest Path Tree

SpfNode	NodeFlag	SpfLink	LinkCost	LinkFlag
0000.0000.0032.00	S/-/-/-/-/-	-->0000.0000.0032.01	10	-/-/C/-/-/-/-/-
		-->0000.0000.0064.00	10	-/-/C/-/-/-/-/-
0000.0000.0032.01	S/-/-/R/-/-	-->0000.0000.0064.00	0	-/-/C/-/-/-/-/-
		-->0000.0000.0032.00	0	-/-/-/P/-/-/-/-/-
0000.0000.0064.00	S/-/-/R/-/-	-->0000.0000.0032.00	10	-/-/-/P/-/-/-/-/-
		-->0000.0000.0032.01	10	-/-/-/P/-/-/-/-/-

Display detailed IS-IS IPv4 SPF tree information.

```
<Sysname> display isis spf-tree verbose
```

Shortest Path Tree for IS-IS(1)

```

-----
Flags: S-Node is on SPF tree      T-Node is on tent list
      O-Node is overload          R-Node is directly reachable
      I-Node or Link is isolated  D-Node or Link is to be deleted
      C-Neighbor is child         P-Neighbor is parent
      V-Link is involved          N-Link is a new path
      L-Link is on change list    U-Protocol usage is changed
      H-Nexthop is changed

```

Level-1 Shortest Path Tree

```

-----
SpfNode      : 0000.0000.0001.00
Distance     : 0
TE distance  : 0
NodeFlag     : S/-/-/-/-/-
RelayNibID   : 0x0
TE tunnel count: 0
Nexthop count : 0
SpfLink count : 1
-->0000.0000.0004.04
  LinkCost    : 10
  LinkNewCost : 10
  LinkFlag    : -/-/C/-/-/-/-/-/-
  LinkSrcCnt  : 1
    Type      : Adjacent   Interface: N/A
    Cost      : 10         Nexthop   : N/A

SpfNode      : 0000.0000.0004.00
Distance     : 10
Te Distance  : 10
NodeFlag     : S/-/-/-/-/-
RelayNibID   : 0x14000000
TE tunnel count: 1
  Destination: 4.4.4.4      Interface  : Tun0
  TE cost     : 10          Final cost : 10
  Add nexthop: YES         Add TLV   : YES
Nexthop count : 2
  Neighbor    : 0000.0000.0004.00  Interface  : Tun0
  Nexthop     : 4.4.4.4
  BkNeighbor  : N/A           BkInterface: N/A
  BkNexthop   : N/A
  Neighbor    : 0000.0000.0004.00  Interface  : Vlan50
  Nexthop     : 1.1.1.3
  BkNeighbor  : N/A           BkInterface: N/A
  BkNexthop   : N/A
SpfLink count : 1

```

```

-->0000.0000.0004.04
  LinkCost      : 10
  LinkNewCost   : 10
  LinkFlag      : -/-/P/-/-/-/-
  LinkSrcCnt    : 1
    Type        : Remote      Interface: N/A
    Cost         : 10          Nexthop   : N/A
    AdvMtID     : 0

```

```

SpfNode        : 0000.0000.0004.04
Distance       : 10
TE distance    : 10
NodeFlag       : S/-/R/-/-
RelayNibID     : 0x1400001
TE tunnel count: 0
Nexthop count  : 0
SpfLink count  : 2

```

```

-->0000.0000.0001.00
  LinkCost      : 0
  LinkNewCost   : 0
  LinkFlag      : -/-/P/-/-/-/-
  LinkSrcCnt    : 1
    Type        : Remote      Interface: N/A
    Cost         : 0          Nexthop   : N/A

```

```

-->0000.0000.0004.00
  LinkCost      : 0
  LinkNewCost   : 0
  LinkFlag      : -/-/C/-/-/-/-/-
  LinkSrcCnt    : 1
    Type        : Remote      Interface: Vlan50
    Cost         : 0          Nexthop   : 1.1.1.3

```

Level-2 Shortest Path Tree

```

SpfNode        : 0000.0000.0001.00
Distance       : 0
TE distance    : 0
NodeFlag       : S/-/---/-
RelayNibID     : 0x0
TE tunnel count: 0
Nexthop count  : 0
SpfLink count  : 1

```

```

-->0000.0000.0004.04
  LinkCost      : 10
  LinkNewCost   : 10
  LinkFlag      : -/-/C/-/-/-/-/-
  LinkSrcCnt    : 1

```

```

        Type      : Adjacent   Interface: N/A
        Cost       : 10         Nexthop   : N/A

SpfNode      : 0000.0000.0004.00
Distance     : 10
TE distance  : 10
NodeFlag     : S/-/-/-/-/-
RelayNibID   : 0x0
TE tunnel count: 1
  Destination: 4.4.4.4           Interface  : Tun0
  TE cost     : 10               Final cost : 10
  Add nexthop: YES              Add TLV    : YES
Nexthop count : 2
  Neighbor    : 0000.0000.0004.00 Interface  : Tun0
  Nexthop     : 4.4.4.4
  BkNeighbor  : N/A             BkInterface: N/A
  BkNexthop   : N/A
  Neighbor    : 0000.0000.0004.00 Interface  : Vlan50
  Nexthop     : 1.1.1.3
  BkNeighbor  : N/A             BkInterface: N/A
  BkNexthop   : N/A
SpfLink count : 1
-->0000.0000.0004.04
  LinkCost    : 10
  LinkNewCost : 10
  LinkFlag    : -/-/-/P/-/-/-/-/-
  LinkSrcCnt  : 1
    Type      : Remote         Interface: N/A
    Cost      : 10             Nexthop   : N/A
    AdvMtID   : 0

SpfNode      : 0000.0000.0004.04
Distance     : 10
TE distance  : 10
NodeFlag     : S/-/-/R/-/-
RelayNibID   : 0x0
TE tunnel count: 0
Nexthop count : 0
SpfLink count : 2
-->0000.0000.0001.00
  LinkCost    : 0
  LinkNewCost : 0
  LinkFlag    : -/-/-/P/-/-/-/-/-
  LinkSrcCnt  : 1
    Type      : Remote         Interface: N/A
    Cost      : 0             Nexthop   : N/A
-->0000.0000.0004.00
  LinkCost    : 0

```

```

LinkNewCost : 0
LinkFlag    : -/-/C/-/-/-/-/-/-
LinkSrcCnt  : 1
    Type    : Remote      Interface: Vlan50
    Cost    : 0           Nexthop   : 1.1.1.3

```

Table 23 Command output

Field	Description
SpfNode	ID of the topology node.
Distance	Shortest distance from the root node to the local node.
TE distance	Shortest distance from the root node to the local node (including tunnel links). If tunnel is not configured, TE distance equals to Distance.
NodeFlag	Node flag: <ul style="list-style-type: none"> • S—The node is on the SPF tree. • T—The node is on the tent list. • O—The node is overloaded. • R—The node is directly connected. • I—The node is isolated. • D—The node is to be deleted.
RelayNibID	Next hop ID of the node after route recursion.
TE tunnel count	Number of tunnels destined to this node.
Destination	Destination router.
TE cost	IGP cost of the TE tunnel.
Final cost	Final cost of the TE tunnel.
Nexthop count	Next hop count.
Nexthop	Primary next hop of the node or the link advertising source.
AdvMtlID	Topology from which the routing information is learned: <ul style="list-style-type: none"> • 0—Base topology. • 6-4094—Other topologies.
Interface	Primary output interface of the node or the link advertising source.
BkNexthop	Backup next hop.
BkInterface	Backup output interface.
Neighbor	ID of the primary next hop neighbor.
BkNeighbor	ID of the backup next hop neighbor.
SpfLink	Topology link.
SpfLink count	Number of topology links.
LinkCost	Link cost.
LinkNewCost	New link cost.
LinkFlag	Link flag: <ul style="list-style-type: none"> • I—The link is isolated. • D—The link is to be deleted. • C—The neighbor is a child node. • P—The neighbor is the parent node. • V—The link is involved.

Field	Description
	<ul style="list-style-type: none"> • N—The link is a new path. • L—The link is on the change list. • U—The protocol usage of the link is changed. • H—The next hop of the link is changed.
LinkSrcCnt	Number of link advertising sources.
Type	Type of the link advertising source: <ul style="list-style-type: none"> • Adjacent—The link advertising source is a local neighbor. • Remote—The link advertising source is advertised by a remote node in an LSP.
Cost	Cost of the link advertising source.

display isis statistics

Use **display isis statistics** to display IS-IS statistics.

Syntax

```
display isis statistics [ ipv4 ] [ level-1 | level-1-2 | level-2 ] [ process-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4: Displays IS-IS IPv4 statistics. If you do not specify this option, the command displays both IPv4 and IPv6 statistics.

level-1: Displays IS-IS Level-1 statistics.

level-1-2: Displays IS-IS Level-1-2 statistics.

level-2: Displays IS-IS Level-2 statistics.

process-id: Displays statistics for an IS-IS process specified by its ID in the range of 1 to 65535. If you do not specify an IS-IS process, this command displays the statistics for all IS-IS processes.

Usage guidelines

If you do not specify a level, this command displays both Level-1 and Level-2 routing information.

Examples

```
# Display IS-IS statistics.
```

```
<Sysname> display isis statistics
```

```
Statistics information for IS-IS(1)
```

```
-----
```

```
Level-1 Statistics
```

```
-----
```

```
MTR (base)
```

Learnt routes information:

Total IPv4 Learnt Routes in IPv4 Routing Table: 1

Imported routes information:

IPv4 Imported Routes:

Static:	0	Direct:	0
ISIS:	0	BGP:	0
RIP:	0	OSPF:	0
Total Number:	0		

MTR(base)

Learnt routes information:

Total IPv6 Learnt Routes in IPv6 Routing Table: 0

Imported routes information:

IPv6 Imported Routes:

Static:	0	Direct:	0
ISISv6:	0	BGP4+:	0
RIPng:	0	OSPFv3:	0
Total Number:	0		

Lsp information:

LSP Source ID:	No. of used LSPs
7777.8888.1111	001

Level-2 Statistics

MTR(base)

Learnt routes information:

Total IPv4 Learnt Routes in IPv4 Routing Table: 0

Imported routes information:

IPv4 Imported Routes:

Static:	0	Direct:	0
ISIS:	0	BGP:	0
RIP:	0	OSPF:	0
Total Number:	0		

MTR(base)

Learnt routes information:

Total IPv6 Learnt Routes in IPv6 Routing Table: 0

Imported routes information:

IPv6 Imported Routes:

```

Static: 0      Direct: 0
ISISv6: 0     BGP4+: 0
RIPng: 0      OSPFv3: 0
Total Number: 0
    
```

Lsp information:

```

LSP Source ID:      No. of used LSPs
7777.8888.1111     001
    
```

Table 24 Command output

Field	Description
Statistics information for IS-IS(<i>processid</i>)	Statistics for the IS-IS process.
Level-1 Statistics	Level-1 statistics.
Level-2 Statistics	Level-2 statistics.
MTR(<i>topo-name</i>)	MTR topology. base represents the base topology.
Learnt routes information	<ul style="list-style-type: none"> Total IPv4 Learnt Routes in IPv4 Routing Table—Number of learned IPv4 routes. Total IPv6 Learnt Routes in IPv6 Routing Table—Number of learned IPv6 routes.
IPv4 Imported Routes	Numbers of different types of redistributed IPv4 routes, including static, direct, IS-IS, BGP, RIP, and OSPF routes.
IPv6 Imported Routes	Numbers of different types of redistributed IPv6 routes, including static, direct, IS-ISv6, BGP4+, RIPng, and OSPFv3 routes.
Lsp information	LSP information: <ul style="list-style-type: none"> LSP Source ID—ID of the source system. No. of used LSPs—Number of used LSPs.

display osi

Use **display osi** to display OSI connection information.

Syntax

```
display osi [ slot slot-number ]
```

Views

Any view

Predefined user roles

```

network-admin
network-operator
    
```

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays OSI connection information for all member devices.

Examples

```
# Display OSI connection information.
```

```
<Sysname> display osi
Total OSI socket number: 2
```

```
Location: slot 0
Creator: isisd[1539]
State: N/A
Options: SO_FILTER
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 1048576 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 262144 / 512 / N/A
Type: 2
Enabled interfaces:
  Vlan-interface100
    MAC address: 0180-c200-0014
```

```
Location: slot 0
Creator: isisd[1539]
State: N/A
Options: SO_FILTER
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 1048576 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 262144 / 512 / N/A
Type: 2
Enabled interfaces:
  Vlan-interface100
    MAC address: 0180-c200-0014
```

Table 25 Command output

Field	Description
Total OSI socket number	Total number of OSI sockets.
Creator	Name of the socket creator. The process ID of the creator is displayed in the square brackets.
State	This field always displays N/A .
Options	Socket options: <ul style="list-style-type: none"> SO_FILTER—Filter option is configured. N/A—No option is configured.
Error	Number of errors that affect the socket session.
Receiving buffer(cc/hiwat/lowat/drop/state)	Receiving buffer information, including the current used space, maximum space, minimum space, number of dropped packets, and status.
Sending buffer(cc/hiwat/lowat/state)	Sending buffer information, including the current used space, maximum space, minimum space, and status.
Type	Type 2 socket, corresponding to unreliable connectionless-oriented transport layer protocols.
Enabled interfaces	Input interfaces and matched multicast MAC addresses. Only packets received from Ethernet link-layer interfaces need to match the multicast MAC addresses.

display osi statistics

Use **display osi statistics** to display OSI packet statistics.

Syntax

display osi statistics [*slot slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays OSI packet statistics for all member devices.

Examples

Display OSI packet statistics.

```
<Sysname> display osi statistics
```

Received packets:

Total: 35

Relay received: 35

Relay forwarded: 35

Invalid service slot: 0

No matched socket: 0

Not delivered, input socket full: 0

Sent packets:

Total: 19

Relay forwarded: 19

Relay received: 19

Failed: 0

Table 26 Command output

Field	Description
Received packets	<p>Statistics of received packets:</p> <ul style="list-style-type: none">• Total—Total number of received link layer packets.• Relay received—Number of inbound packets on LPUs relayed from other cards. This count is not included in the total count of received packets.• Relay forwarded—Number of inbound packets relayed to LPUs.• Invalid service slot—Number of discarded packets due to unavailable LPUs.• No matched socket—Number of discarded packets due to mismatches in input interfaces, MAC addresses, or connection filter criteria.• Not delivered, input socket full—Number of undelivered packets due to a socket receiving buffer overflow.

Field	Description
Sent packets	Statistics of sent packets: <ul style="list-style-type: none"> • Total—Total number of packets that IS-IS sent over OSI connections. • Relay forwarded—Number of outbound packets relayed to the cards that hosts the output interfaces. This count is not included in the total count of sent packets. • Relay received—Number of outbound packets on the cards that hosts the output interfaces. These packets are relayed from other cards. • Failed—Number of packets failed to be sent.

Related commands

`reset osi statistics`

distribute bgp-ls

Use **distribute bgp-ls** to advertise IS-IS link state information to BGP.

Use **undo distribute bgp-ls** to restore the default.

Syntax

distribute bgp-ls [instance-id *id*] [level-1 | level-2]

undo distribute bgp-ls [level-1 | level-2]

Default

The device does not advertise IS-IS link state information to BGP.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

instance-id *id*: Specifies an instance by its ID in the range of 0 to 65535. If you do not specify this option, the command advertises IS-IS link state information of instance 0 to BGP.

level-1: Advertises the Level-1 IS-IS link state information to BGP.

level-2: Advertises the Level-2 IS-IS link state information to BGP.

Usage guidelines

After the device advertises IS-IS link state information to BGP, BGP can advertise the information for intended applications.

If multiple IS-IS processes have the same instance ID and link state information, only the link state information of the IS-IS process with the smallest process ID is advertised.

To advertise the same link state information of different IS-IS processes to BGP, specify different instance IDs for the IS-IS processes.

If you do not specify a level for the **distribute bgp-ls** command, both Level-1 and Level-2 IS-IS link state information are advertised to BGP.

If you do not specify a level for the **undo distribute bgp-ls** command, neither Level-1 nor Level-2 IS-IS link state information can be advertised to BGP.

Examples

```
# Advertise link state information of IS-IS process 1 to BGP.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] distribute bgp-ls
```

domain-authentication send-only

Use **domain-authentication send-only** to configure IS-IS not to check the authentication information in the received Level-2 packets, including LSPs, CSNPs, and PSNPs.

Use **undo domain-authentication send-only** to restore the default.

Syntax

domain-authentication send-only

undo domain-authentication send-only

Default

When domain authentication mode and key are configured, a Level-2 or Level-1-2 router checks the authentication information in the received packets.

Views

IS-IS view

Predefined user roles

network-admin

Usage guidelines

When domain authentication mode and key are configured, a Level-2 or Level-1-2 router adds the key in the specified mode into transmitted Level-2 packets (including LSPs, CSNPs, and PSNPs). It also checks the key in the received Level-2 packets.

To prevent packet exchange failure in case of an authentication key change, configure IS-IS not to check the authentication information in the received packets.

Examples

```
# Configure IS-IS not to check the authentication information in the received packets.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] domain-authentication send-only
```

Related commands

area-authentication send-only

domain-authentication-mode

isis authentication send-only

domain-authentication-mode

Use **domain-authentication-mode** to specify the routing domain authentication mode and a key.

Use **undo domain-authentication-mode** to restore the default.

Syntax

```
domain-authentication-mode { { gca key-id { hmac-sha-1 | hmac-sha-224 | hmac-sha-256 | hmac-sha-384 | hmac-sha-512 } [ nonstandard ] | md5 | simple } { cipher | plain } string | keychain keychain-name } [ ip | osi ]
```

```
undo domain-authentication-mode
```

Default

No routing domain authentication mode or key is configured.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

gca: Specifies the GCA mode.

key-id: Uniquely identifies an SA in the range of 1 to 65535. The sender inserts the Key ID into the authentication TLV, and the receiver authenticates the packet by using the SA that is selected based on the Key ID.

hmac-sha-1: Specifies the HMAC-SHA-1 algorithm.

hmac-sha-224: Specifies the HMAC-SHA-224 algorithm.

hmac-sha-256: Specifies the HMAC-SHA-256 algorithm.

hmac-sha-384: Specifies the HMAC-SHA-384 algorithm.

hmac-sha-512: Specifies the HMAC-SHA-512 algorithm.

nonstandard: Specifies the nonstandard GCA authentication mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

ip: Checks IP-related fields in LSPs.

osi: Checks OSI-related fields in LSPs.

Usage guidelines

The configured key in the specified mode is inserted into all outgoing Level-2 packets (LSP, CSNP, and PSNP) and is used for authenticating the incoming Level-2 packets.

IS-IS keychain authentication can operate correctly only when the keys in the keychain use the HMAC-MD5 authentication algorithm.

- Before IS-IS sends a Level-2 packet, it uses the valid send key obtained from the keychain to authenticate the packet. If no valid send key exists or the valid send key does not use the HMAC-MD5 algorithm, the authentication fails and the packet does not contain the authentication information.

- After IS-IS receives a Level-2 packet, it uses a valid accept key obtained from the keychain to authenticate the packet. If no valid accept key exists or all valid accept keys fail to authenticate the packet, the authentication fails and the packet is discarded.

All the backbone routers must have the same authentication mode and key.

If neither **ip** nor **osi** is specified, the OSI-related fields in LSPs are checked.

When you specify the GCA mode, follow these guidelines:

- If you do not specify the **nonstandard** keyword, the device can communicate only with devices that use the GCA mode.
- If you specify the **nonstandard** keyword, the device can communicate only with devices that use the nonstandard GCA mode.

Examples

```
# Set the routing domain authentication mode to simple, and set the plaintext key to 123456.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] domain-authentication-mode plain 123456
```

Related commands

area-authentication-mode

domain-authentication send-only

isis authentication-mode

fast-reroute

Use **fast-reroute** to configure IS-IS FRR.

Use **undo fast-reroute** to disable IS-IS FRR.

Syntax

```
fast-reroute { lfa | route-policy route-policy-name }
```

```
undo fast-reroute { lfa | route-policy }
```

Default

IS-IS FRR is disabled.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

lfa: Calculates a backup next hop through Loop Free Alternate (LFA) calculation for all routes.

route-policy *route-policy-name*: Uses the specified routing policy to designate a backup next hop. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

The LFA calculation of FRR and IS-IS TE are mutually exclusive.

Example

```
# Enable FRR for IS-IS process 1 and configure IS-IS FRR to calculate a backup next hop through LFA calculation for all routes.
```

```

<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] fast-reroute lfa

```

filter-policy export

Use **filter-policy export** to configure IS-IS to filter redistributed routes.

Use **undo filter-policy export** to remove the configuration.

Syntax

```

filter-policy { ipv4-acl-number | prefix-list prefix-list-name | route-policy route-policy-name }
export [ protocol [ process-id ] ]

undo filter-policy export [ protocol [ process-id ] ]

```

Default

IS-IS does not filter redistributed routes.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

prefix-list *prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes by destination address.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes.

protocol: Filters routes redistributed from the specified routing protocol. If no protocol is specified, the command filters all redistributed routes.

process-id: Specifies a process by its ID in the range of 1 to 65535. This argument is available only when the protocol is **isis**, **ospf**, or **rip**. The default process ID is 1.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard destination dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter redistributed routes.

```

<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255

```

```

[Sysname-acl-ipv4-basic-2000] quit
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] filter-policy 2000 export

# Configure advanced ACL 3000 to permit only route 113.0.0.0/16 to pass. Use advanced ACL 3000
to filter redistributed routes.

<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] isis 1
[Sysname-isis 1] address-family ipv4
[Sysname-isis-1-ipv4] filter-policy 3000 export

```

Related commands

display isis route

filter-policy import

Use **filter-policy import** to configure IS-IS to filter routes calculated using received LSPs.

Use **undo filter-policy import** to restore the default.

Syntax

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* }
import

undo filter-policy import

Default

IS-IS does not filter routes calculated using received LSPs.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999 to filter routes calculated using received LSPs.

prefix-list *prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes calculated using received LSPs by destination address.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr* *sour-wildcard* command.

- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard destination dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter routes calculated using received LSPs.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] filter-policy 2000 import
```

Use advanced ACL 3000 to filter routes calculated using received LSPs and install only route 113.0.0.0/16 to the IP routing table.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] isis 1
[Sysname-isis 1] address-family ipv4
[Sysname-isis-1-ipv4] filter-policy 3000 import
```

Related commands

display ip routing-table

flash-flood

Use **flash-flood** to enable IS-IS LSP flash flooding.

Use **undo flash-flood** to disable IS-IS LSP flash flooding.

Syntax

flash-flood [**flood-count** *flooding-count* | **max-timer-interval** *flooding-interval* | [**level-1** | **level-2**]]
*

undo flash-flood [**level-1** | **level-2**]

Default

IS-IS LSP flash flooding is disabled.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

flood-count *flooding-count*. Specifies the maximum number of LSPs to be flooded before the next SPF calculation, in the range of 1 to 15. The default is 5.

max-timer-interval *flooding-interval*: Specifies the delay of the flash flooding, in the range of 10 to 50000 milliseconds. The default is 10.

level-1: Enables flash flooding for **level-1**.

level-2: Enables flash flooding for **level-2**.

Usage guidelines

If no level is specified, the command enables IS-IS LSP flash flooding for both Level-1 and Level-2.

Examples

```
# Enable fast flooding, and set the maximum LSPs to be sent to 10 and the delay time to 100 milliseconds.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] flash-flood flood-count 10 max-timer-interval 100
```

graceful-restart

Use **graceful-restart** to enable IS-IS GR.

Use **undo graceful-restart** to disable IS-IS GR.

Syntax

graceful-restart

undo graceful-restart

Default

IS-IS GR is disabled.

Views

IS-IS view

Predefined user roles

network-admin

Usage guidelines

IS-IS GR and IS-IS NSR are mutually exclusive. Therefore, do not configure the **graceful-restart** command and the **non-stop-routing** command at the same time.

Examples

```
# Enable GR for IS-IS process 1.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart
```

Related commands

graceful-restart suppress-sa

graceful-restart suppress-sa

Use **graceful-restart suppress-sa** to suppress the Suppress-Advertisement (SA) bit during restart.

Use **undo graceful-restart suppress-sa** to restore the default.

Syntax

```
graceful-restart suppress-sa
undo graceful-restart suppress-sa
```

Default

The SA bit is set during restart.

Views

IS-IS view

Predefined user roles

network-admin

Usage guidelines

Suppressing the SA bit is mainly for avoiding black hole route. If a router starts or reboots without keeping the local forwarding table, sending packets to the router might result in severe packet loss. To avoid this, you can set the SA bit of the hello packet sent by the GR restarter to 1. Upon receiving such hello packets, the GR helpers will not advertise the GR restarter through LSP.

Examples

```
# Suppress the SA bit during graceful restart.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart suppress-sa
```

Related commands

graceful-restart

graceful-restart t1

Use **graceful-restart t1** to set the T1 timer.

Use **undo graceful-restart t1** to restore the default.

Syntax

```
graceful-restart t1 seconds count count
undo graceful-restart t1
```

Default

The T1 timer is 3 seconds and can expire 10 times.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

seconds: Specifies the T1 timer in the range of 3 to 10 seconds.

count: Specifies the number of times that the T1 timer can expire, in the range of 1 to 20.

Usage guidelines

The T1 timer specifies the number of times that GR restarter can send a Restart TLV with the RR bit set. After restart, the GR restarter sends a Restart TLV with the RR bit set to its neighbor. If the

restarting router receives a Restart TLV with the RA set from its neighbor before the T1 timer expires, the GR process starts. Otherwise, the GR process fails.

To avoid GR failure, follow these guidelines when you set the GR timers:

- The product of the T1 timer and the number of times that the T1 timer can expire must be smaller than the T2 timer.
- The T2 timer must be smaller than the T3 timer.

Examples

```
# Set the T1 timer of IS-IS process 1 to 5 seconds, and the expiration times to 5.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart t1 5 count 5
```

Related commands

graceful-restart
graceful-restart t2
graceful-restart t3

graceful-restart t2

Use **graceful-restart t2** to set the T2 timer.

Use **undo graceful-restart t2** to restore the default.

Syntax

graceful-restart t2 *seconds*
undo graceful-restart t2

Default

The T2 timer is 60 seconds.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

seconds: Specifies the T2 timer in the range of 30 to 65535 seconds.

Usage guidelines

The T2 timer specifies the LSDB synchronization interval. Each LSDB has a T2 timer. The Level-1-2 router has two T2 timers: a Level-1 timer and a Level-2 timer. If the LSDBs have not achieved synchronization before the two timers expire, the GR process fails.

To avoid GR failure, follow these guidelines when you set the GR timers:

- The product of the T1 timer and the number of times that the T1 timer can expire must be smaller than the T2 timer.
- The T2 timer must be smaller than the T3 timer.

Examples

```
# Set the T2 timer of IS-IS process 1 to 50 seconds.
<Sysname> system-view
```

```
[Sysname] isis 1
[Sysname-isis-1] graceful-restart t2 50
```

Related commands

```
graceful-restart
graceful-restart t1
graceful-restart t3
```

graceful-restart t3

Use **graceful-restart t3** to set the T3 timer.

Use **undo graceful-restart t3** to restore the default.

Syntax

```
graceful-restart t3 seconds
undo graceful-restart t3
```

Default

The T3 timer is 300 seconds.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

seconds: Specifies the T3 timer in the range of 300 to 65535 seconds.

Usage guidelines

The T3 timer specifies the GR interval. The GR interval is set as the holdtime in hello PDUs. Within the interval, the neighbors maintain their adjacency with the GR restarter. If the GR process has not completed within the holdtime, the neighbors tear down the neighbor relationship and the GR process fails.

To avoid GR failure, follow these guidelines when you set the GR timers:

- The product of the T1 timer and the number of times that the T1 timer can expire must be smaller than the T2 timer.
- The T2 timer must be smaller than the T3 timer.

Examples

```
# Set the T3 timer of IS-IS process 1 to 500 seconds.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart t3 500
```

Related commands

```
graceful-restart
graceful-restart t1
graceful-restart t2
```

ignore-att

Use **ignore-att** to configure IS-IS not to calculate the default route through the ATT bit.

Use **undo ignore-att** to restore the default.

Syntax

ignore-att

undo ignore-att

Default

IS-IS calculates the default route through the ATT bit.

Views

IS-IS view

Predefined user roles

network-admin

Examples

Configure IS-IS not to calculate the default route through the ATT bit.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ignore-att
```

import-route

Use **import-route** to redistribute routes from another routing protocol or another IS-IS process.

Use **undo import-route** to remove the redistribution.

Syntax

import-route bgp [*as-number*] [**allow-ibgp**] [**cost** *cost-value* | **cost-type** { **external** | **internal** } | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

import-route bgp [*as-number*] [**allow-ibgp**] **inherit-cost** [[**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

import-route { **direct** | **static** } [**cost** *cost-value* | **cost-type** { **external** | **internal** }] [[**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

import-route { **direct** | **static** } **inherit-cost** [[**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

import-route { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **cost-type** { **external** | **internal** }] [[**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

import-route { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] **inherit-cost** [**allow-direct** | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route { **bgp** | **direct** | { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] | **static** }

Default

IS-IS does not redistribute routes from other routing protocols or processes.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

bgp: Redistributes BGP routes.

bgp4+: Redistributes IPv6 BGP routes.

as-number: Specifies an AS by its number in the range of 1 to 4294967295. If you do not specify this argument, the command redistributes all IPv4 EBGp routes. As a best practice, specify an AS to prevent the system from redistributing excessive routes.

direct: Redistributes direct routes.

isis: Redistributes IS-IS routes.

isisv6: Redistributes IPv6 IS-IS routes.

ospf: Redistributes OSPF routes.

ospfv3: Redistributes OSPFv3 routes.

rip: Redistributes RIP routes.

ripng: Redistributes RIPng routes.

process-id: Specifies a process by its ID in the range of 1 to 65535.

all-processes: Redistributes routes from all the processes of the specified routing protocol.

allow-ibgp: Allows redistribution of IBGP routes. The **import-route bgp** command redistributes only EBGp routes. The **import-route bgp allow-ibgp** command redistributes both EBGp and IBGP routes. Because this command might cause routing loops, use it with caution.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy route-policy-name** option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost cost-value: Specifies a cost for redistributed routes, which is in the range of 0 to 4261412864.

- For the styles of **narrow**, **narrow-compatible**, and **compatible**, the cost is in the range of 0 to 63.
- For the styles of **wide** and **wide-compatible**, the cost is in the range of 0 to 4261412864.

cost-type { external | internal }: Specifies the cost type. The **internal** type indicates internal routes, and the **external** type indicates external routes. If **external** is specified, the cost of a redistributed route is added by 64 to make internal routes take priority over external routes. The type is **external** by default. The keywords are available only when the cost type is **narrow**, **narrow-compatible**, or **compatible**.

inherit-cost: Uses the original cost of redistributed routes. This keyword is available in Release 2612P01 and later.

level-1: Redistributes routes into the Level-1 routing table.

level-1-2: Redistributes routes into both Level-1 and Level-2 routing tables.

level-2: Redistributes routes into the Level-2 routing table. If no level is specified, the routes are redistributed into the Level-2 routing table by default.

route-policy route-policy-name: Redistributes only routes matching the specified routing policy. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag tag: Specifies a tag value for marking redistributed routes, in the range of 1 to 4294967295.

Usage guidelines

IS-IS takes all the redistributed routes as external routes to destinations outside the IS-IS routing domain.

The effective cost varies by cost style. For the styles of **narrow**, **narrow-compatible**, and **compatible**, the cost is in the range of 0 to 63. If the cost is more than 63, 63 is used. For the style of wide or wide-compatible, the configured value is the effective value.

This **import-route** command cannot redistribute default routes. The command redistributes only active routes. To display route state information, use the **display ip routing-table protocol** command.

If you do not specify the **cost** or **inherit-cost** keyword, the cost of a redistributed route is 0.

The **undo import-route protocol all-processes** command removes only the configuration made by the **import-route protocol all-processes** command, instead of the configuration made by the **import-route protocol process-id** command.

Examples

Redistribute static routes into IS-IS, and set the cost for redistributed routes to 15.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] import-route static cost 15
```

Related commands

import-route limit

import-route isis level-1 into level-2

Use **import-route isis level-1 into level-2** to enable route advertisement from Level-1 to Level-2.

Use **undo import-route isis level-1 into level-2** to disable route advertisement from Level-1 to Level-2.

Syntax

import-route isis level-1 into level-2 [**filter-policy** { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *

undo import-route isis level-1 into level-2

Default

Route advertisement from Level-1 to Level-2 is enabled.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

filter-policy: Specifies a filtering policy.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999 to filter routes from Level-1 to Level-2.

prefix-list *prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes from Level-1 to Level-2 by destination address.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter routes from Level-1 to Level-2.

tag *tag*: Specifies a tag for marking redistributed routes, in the range of 1 to 4294967295.

Usage guidelines

If a routing policy is used, the routing policy must be specified in the **import-route isis level-1 into level-2** command to filter routes from Level-1 to Level-2. Other routing policies specified for route reception and redistribution do not affect the route leaking.

If a filtering policy is configured, only Level-1 routes not filtered out can be advertised into the Level-2 area.

Examples

```
# Enable route advertisement from Level-1 to Level-2.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] import-route isis level-1 into level-2
```

Related commands

import-route

import-route isis level-1 into level-2

import-route isis level-2 into level-1

Use **import-route isis level-2 into level-1** to enable route advertisement from Level-2 to Level-1.

Use **undo import-route isis level-2 into level-1** to restore the default.

Syntax

import-route isis level-2 into level-1 [**filter-policy** { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *

undo import-route isis level-2 into level-1

Default

Route advertisement from Level-2 to Level-1 is disabled.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

filter-policy: Specifies a filtering policy.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999 to filter routes from Level-2 to Level-1.

prefix-list *prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes from Level-2 to Level-1 by destination address.

route-policy *route-policy-name*: Uses the specified routing policy to filter routes from Level-2 to Level-1. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for marking redistributed routes, in the range of 1 to 4294967295.

Usage guidelines

If a routing policy is used, the routing policy must be specified in the **import-route isis level-2 into level-1** command to filter routes from Level-2 to Level-1. Other routing policies specified for route reception and redistribution does not affect the route leaking.

If a filtering policy is configured, only Level-2 routes not filtered out can be advertised into the Level-1 area.

Examples

```
# Enable route advertisement from Level-2 to Level-1.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] import-route isis level-2 into level-1
```

Related commands

import-route

import-route isis level-1 into level-2

import-route limit

Use **import-route limit** to configure the maximum number of redistributed Level 1/Level 2 IPv4 routes.

Use **undo import-route limit** to restore the default.

Syntax

import-route limit *number*

undo import-route limit

Default

The maximum number of redistributed Level 1/Level 2 IPv4 routes is not configured.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of redistributed Level 1/Level 2 IPv4 routes. The value range for this argument is 1 to N, and N equals the maximum number of routes allowed in the IPv4 routing table.

Usage guidelines

You can use the **hardware-resource switch-mode** and **hardware-resource routing-mode ipv6-128** commands to set the maximum number of routes allowed in the IPv4 routing table. For more information about the **hardware-resource switch-mode** command, see device management configuration in *Fundamentals Configuration Guide*.

Examples

```
# Configure IS-IS process 1 to redistribute up to 1000 Level 1/Level 2 IPv4 routes.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
```

```
[Sysname-isis-1-ipv4] import-route limit 1000
```

Related commands

hardware-resource routing-mode ipv6-128

hardware-resource switch-mode (*Fundamentals Command Reference*)

import-route

isis

Use **isis** to enable IS-IS and enter IS-IS view.

Use **undo isis** to disable IS-IS.

Syntax

```
isis [ process-id ] [ vpn-instance vpn-instance-name ]
```

```
undo isis [ process-id ]
```

Default

IS-IS is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. The default is 1.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the IS-IS process runs on the public network.

Examples

```
# Enable IS-IS process 1 and set the system ID to 0000.0000.0002 and area ID to 01.0001.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] network-entity 01.0001.0000.0000.0002.00
```

Related commands

isis enable

network-entity

isis authentication send-only

Use **isis authentication send-only** to configure an IS-IS interface not to check the authentication information in the received hello packets.

Use **undo isis authentication send-only** to remove the configuration.

Syntax

```
isis authentication send-only [ level-1 | level-2 ]
```

```
undo isis authentication send-only [ level-1 | level-2 ]
```

Default

When interface authentication mode and key are configured, an IS-IS interface checks the authentication information in the received packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

level-1: Configures IS-IS not to check the authentication information in the received Level-1 hello packets.

level-2: Configures IS-IS not to check the authentication information in the received Level-2 hello packets.

Usage guidelines

When peer authentication mode and key are configured, an IS-IS interface adds the key in the specified mode into transmitted hello packets. It also checks the key in the received hello packets.

To prevent packet exchange failure in case of an authentication key change, configure the IS-IS interface not to check the authentication information in the received packets.

Examples

Configure VLAN-interface 10 not to check the authentication information in the received Level-1 hello packets.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 10
```

```
[Sysname-Vlan-interface10] isis authentication send-only level-1
```

Related commands

area-authentication send-only

domain-authentication send-only

isis authentication-mode

isis authentication-mode

Use **isis authentication-mode** to specify the neighbor relationship authentication mode and a key.

Use **undo isis authentication-mode** to remove the configuration.

Syntax

```
isis authentication-mode { { gca key-id { hmac-sha-1 | hmac-sha-224 | hmac-sha-256 | hmac-sha-384 | hmac-sha-512 } [ nonstandard ] | md5 | simple } { cipher | plain } string | keychain keychain-name } [ level-1 | level-2 ] [ ip | osi ]
```

```
undo isis authentication-mode [ level-1 | level-2 ]
```

Default

No neighbor relationship authentication mode or key is configured.

Views

Interface view

Predefined user roles

network-admin

Parameters

gca: Specifies the GCA mode.

key-id: Uniquely identifies an SA in the range of 1 to 65535. The sender inserts the Key ID into the authentication TLV, and the receiver authenticates the packet by using the SA that is selected based on the Key ID.

hmac-sha-1: Specifies the HMAC-SHA-1 algorithm.

hmac-sha-224: Specifies the HMAC-SHA-224 algorithm.

hmac-sha-256: Specifies the HMAC-SHA-256 algorithm.

hmac-sha-384: Specifies the HMAC-SHA-384 algorithm.

hmac-sha-512: Specifies the HMAC-SHA-512 algorithm.

nonstandard: Specifies the nonstandard GCA mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

level-1: Configures the key for Level-1.

level-2: Configures the key for Level-2.

ip: Checks IP-related fields in LSPs and SNPs.

osi: Checks OSI-related fields in LSPs and SNPs.

Usage guidelines

The key in the specified mode is inserted into all outbound hello packets and is used for authenticating inbound hello packets. Only if the authentication succeeds can the neighbor relationship be formed.

IS-IS keychain authentication can operate correctly only when the keys in the keychain use the HMAC-MD5 authentication algorithm.

- Before IS-IS sends a Hello packet, it uses the valid send key obtained from the keychain to authenticate the packet. If no valid send key exists or the valid send key does not use the HMAC-MD5 algorithm, the authentication fails and the packet does not contain the authentication information.
- After IS-IS receives a Hello packet, it uses a valid accept key obtained from the keychain to authenticate the packet. If no valid accept key exists or all valid accept keys fail to authenticate the packet, the authentication fails and the packet is discarded.

The **level-1** and **level-2** keywords are configurable on an interface that has had IS-IS enabled with the **isis enable** command.

If you configure a key without specifying a level, the key applies to both Level-1 and Level-2.

For two routers to become neighbors, the authentication mode and key at both ends must be identical.

If neither **ip** nor **osi** is specified, the OSI-related fields in LSPs are checked.

When you specify the GCA mode, follow these guidelines:

- If you do not specify the **nonstandard** keyword, the device can communicate only with devices that use the GCA mode.
- If you specify the **nonstandard** keyword, the device can communicate only with devices that use the nonstandard GCA mode.

Examples

```
# On VLAN-interface 10, set the authentication mode to simple, and set the plaintext key to 123456.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis authentication-mode simple plain 123456
```

Related commands

area-authentication-mode
domain authentication-mode
isis authentication send-only

isis bfd enable

Use **isis bfd enable** to enable BFD.
 Use **undo isis bfd enable** to disable BFD.

Syntax

isis bfd enable
undo isis bfd enable

Default

IS-IS BFD is disabled.

Views

Interface view

Predefined user roles

network-admin

Examples

```
# Enable BFD for IS-IS on VLAN-interface 11.
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] isis enable
[Sysname-Vlan-interface11] isis bfd enable
```

isis circuit-level

Use **isis circuit-level** to set the circuit level for the interface.
 Use **undo isis circuit-level** to restore the default.

Syntax

isis circuit-level [level-1 | level-1-2 | level-2]
undo isis circuit-level

Default

An interface can establish either the Level-1 or Level-2 adjacency.

Views

Interface view

Predefined user roles

network-admin

Parameters

level-1: Sets the circuit level to Level-1.

level-1-2: Sets the circuit level to Level-1-2.

level-2: Sets the circuit level to Level-2.

Usage guidelines

For a Level-1 (Level-2) router, the circuit level can only be Level-1 (Level-2). For a Level-1-2 router, you must specify a circuit level for a specific interface to form only the specified level neighbor relationship.

Examples

VLAN-interface 10 is connected to a non-backbone router in the same area. Set the circuit level of VLAN-interface 10 to Level-1 to prevent sending and receiving Level-2 Hello packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable
[Sysname-Vlan-interface10] isis circuit-level level-1
```

Related commands

is-level

isis circuit-type p2p

Use **isis circuit-type p2p** to set the network type of an interface to P2P.

Use **undo isis circuit-type** to restore the default.

Syntax

isis circuit-type p2p

undo isis circuit-type

Default

The network type of an interface varies by physical media. (The network type of a VLAN interface is broadcast.)

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Use this command only on a broadcast network with two attached routers.

Interfaces with different network types operate differently. For example, broadcast interfaces must elect a DIS and flood CSNP packets to synchronize the LSDBs. P2P interfaces do not need to elect a DIS, and use a different LSDB synchronization mechanism.

If only two routers exist on a broadcast network, set the network type of attached interfaces to P2P to avoid DIS election and CSNP flooding. This saves network bandwidth and speeds up network convergence.

Examples

```
# Set the network type of VLAN-interface 10 to P2P.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable
[Sysname-Vlan-interface10] isis circuit-type p2p
```

isis cost

Use **isis cost** to set the IS-IS cost for an interface.

Use **undo isis cost** to remove the configuration.

Syntax

isis cost *cost-value* [**level-1** | **level-2**]

undo isis cost [**level-1** | **level-2**]

Default

No IS-IS cost is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

cost-value: Specifies an IS-IS cost in the range of 1 to 16777215.

level-1: Applies the cost to Level-1.

level-2: Applies the cost to Level-2.

Usage guidelines

If neither **level-1** nor **level-2** is included, the cost applies to both **level-1** and **level-2**.

Examples

```
# Set the Level-2 IS-IS cost to 5 for VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis cost 5 level-2
```

Related commands

auto-cost enable

bandwidth-reference

isis dis-name

Use **isis dis-name** to configure a name for a DIS to represent the pseudo node on a broadcast network.

Use **undo isis dis-name** to restore the default.

Syntax

isis dis-name *symbolic-name*

undo isis dis-name

Default

No name is configured for the DIS.

Views

Interface view

Predefined user roles

network-admin

Parameters

symbolic-name: Specifies a DIS name, a case-insensitive string of 1 to 64 characters.

Usage guidelines

This command takes effect only on routers that have dynamic system ID to host name mapping enabled. This command does not take effect on Point-to-Point interfaces.

Examples

```
# Set the DIS name to LOCALAREA.
```

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 10
```

```
[Sysname-Vlan-interface10] isis dis-name LOCALAREA
```

Related commands

display isis name-table

is-name

isis dis-priority

Use **isis dis-priority** to specify a DIS priority at a specified level for an interface.

Use **undo isis dis-priority** to remove the configuration.

Syntax

isis dis-priority *priority* [**level-1** | **level-2**]

undo isis dis-priority [**level-1** | **level-2**]

Default

The priority of Level-1 and Level-2 is 64.

Views

Interface view

Predefined user roles

network-admin

Parameters

priority: Specifies a DIS priority in the range of 0 to 127.

level-1: Applies the DIS priority to Level-1.

level-2: Applies the DIS priority to Level-2.

Usage guidelines

On an IS-IS broadcast network, a router must be elected as the DIS at each routing level. Specify a DIS priority at a level for an interface. The greater the interface's priority is, the more likelihood it becomes the DIS. If multiple routers in the broadcast network have the same highest DIS priority, the router with the highest Subnetwork Point of Attachment (SNPA) address becomes the DIS. SNPA addresses are MAC addresses on a broadcast network.

IS-IS has no backup DIS. The router with a priority of 0 can also participate in DIS election.

If neither **level-1** nor **level-2** is specified, the DIS priority applies to both Level-1 and Level-2.

Examples

```
# Set the Level-2 DIS priority to 127 for VLAN-interface 10.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis dis-priority 127 level-2
```

isis enable

Use **isis enable** to enable an IS-IS process on an interface.

Use **undo isis enable** to disable IS-IS.

Syntax

```
isis enable [ process-id ]
```

```
undo isis enable
```

Default

No IS-IS process is enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. The default is 1.

Examples

```
# Enable IS-IS process 1 globally and enable it on VLAN-interface 10.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable 1
```

Related commands

isis

network-entity

isis fast-reroute lfa-backup exclude

Use **isis fast-reroute lfa-backup exclude** to disable LFA calculation on an interface.

Use **undo isis fast-reroute lfa-backup exclude** to restore the default.

Syntax

isis fast-reroute lfa-backup exclude

undo isis fast-reroute lfa-backup exclude

Default

LFA calculation is enabled on an interface, and the interface can be elected as a backup interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

When this command is configured, the interface does not participate in the LFA calculation, and cannot be elected as a backup interface.

Examples

```
# Disable LFA calculation on VLAN-interface 10.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable 1
[Sysname-Vlan-interface10] isis fast-reroute lfa-backup exclude
```

Related commands

fast-reroute

isis mib-binding

Use **isis mib-binding** to bind an IS-IS process to MIB.

Use **undo isis mib-binding** to restore the default.

Syntax

isis mib-binding *process-id*

undo isis mib-binding

Default

MIB operation is bound to the IS-IS process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535.

Usage guidelines

If the specified process ID does not exist, the MIB binding configuration fails.

Deleting an IS-IS process bound to MIB operation deletes the MIB binding configuration. MIB operation is bound to the IS-IS process with the smallest process ID.

Examples

```
# Bind IS-IS process 100 to MIB.
<Sysname> system-view
[Sysname] isis mib-binding 100
```

isis prefix-suppression

Use **isis prefix-suppression** to enable prefix suppression on an interface.

Use **undo isis prefix-suppression** to disable prefix suppression on an interface.

Syntax

isis prefix-suppression

undo isis prefix-suppression

Default

Prefix suppression is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Use this command to disable an interface from advertising its prefix in LSPs. This enhances network security by preventing IP routing to the interval nodes and speeds up network convergence.

This command is also applicable to the secondary IP address of the interface.

Examples

```
# Enable prefix suppression on VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis prefix-suppression
```

isis primary-path-detect bfd

Use **isis primary-path-detect bfd** to enable BFD for IS-IS FRR or IS-IS PIC.

Use **undo isis primary-path-detect bfd** to disable BFD for IS-IS FRR or IS-IS PIC.

Syntax

isis primary-path-detect bfd { ctrl | echo }

undo isis primary-path-detect bfd

Default

BFD is disabled for IS-IS FRR or IS-IS PIC.

Views

Interface view

Predefined user roles

network-admin

Parameters

ctrl: Specifies the BFD control packet mode.

echo: Specifies the BFD echo packet mode.

Usage guidelines

This command enables IS-IS FRR or IS-IS PIC to use BFD to detect primary link failures.

Examples

Enable BFD control packet mode for IS-IS FRR on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] fast-reroute lfa
[Sysname-isis-1-ipv4] quit
[Sysname-isis-1] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis primary-path-detect bfd ctrl
```

Enable BFD echo packet mode for IS-IS PIC on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] pic additional-path-always
[Sysname-isis-1] quit
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interfacell] isis primary-path-detect bfd echo
```

isis silent

Use **isis silent** to disable the interface from sending and receiving IS-IS packets.

Use **undo isis silent** to restore the default.

Syntax

isis silent

undo isis silent

Default

An interface can send and receive IS-IS packets.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command is not available in loopback interface view.

Examples

```
# Disable VLAN-interface 10 from sending and receiving IS-IS packets.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis silent
```

isis small-hello

Use **isis small-hello** to configure the interface to send small hello packets without CLVs.

Use **undo isis small-hello** to restore the default.

Syntax

isis small-hello

undo isis small-hello

Default

An interface sends standard hello packets.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command is not available in loopback interface view.

Examples

```
# Configure VLAN-interface 10 to send small Hello packets.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis small-hello
```

isis tag

Use **isis tag** to configure the tag value for an interface.

Use **undo isis tag** to restore the default.

Syntax

isis tag *tag*

undo isis tag

Default

The interface is not configured with a tag value.

Views

Interface view

Predefined user roles

network-admin

Parameters

tag: Specifies the tag value in the range of 1 to 4294967295.

Usage guidelines

When IS-IS advertises an IP prefix with a tag value, it adds the tag to the IP reachability information TLV if the link cost style is **wide**, **wide-compatible**, or **compatible**.

Examples

```
# Configure the tag value for VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis tag 4294967295
```

isis timer csnp

Use **isis timer csnp** to set on the DIS of a broadcast network the interval for sending CSNP packets.

Use **undo isis timer csnp** to remove the configuration.

Syntax

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

undo isis timer csnp [**level-1** | **level-2**]

Default

The default CSNP interval is 10 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies on the DIS of a broadcast network the interval for sending CSNP packets. The value range is 1 to 600 seconds.

level-1: Applies the interval to Level-1.

level-2: Applies the interval to Level-2.

Usage guidelines

On a broadcast network, this command only applies to the DIS, because the DIS sends CSNP packets periodically for LSDB synchronization.

If no level is specified, the CSNP interval applies to both Level-1 and Level-2.

Examples

```
# Configure Level-2 CSNP packets to be sent every 15 seconds over VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer csnp 15 level-2
```

isis timer hello

Use **isis timer hello** to set the interval for sending hello packets.

Use **undo isis timer hello** to remove the configuration.

Syntax

isis timer hello *seconds* [**level-1** | **level-2**]

undo isis timer hello [**level-1** | **level-2**]

Default

The hello interval is 10 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the interval for sending hello packets, in the range of 3 to 255 seconds.

level-1: Specifies the interval for sending Level-1 hello packets.

level-2: Specifies the interval for sending Level-2 hello packets.

Usage guidelines

If a neighbor does not receive any hello packets from the router within the advertised hold time, it considers the router down and recalculates the routes. The hold time is the hello multiplier multiplied by the hello interval.

Level-1 and Level-2 hello packets are sent independently on a broadcast network, so you need to specify an interval for each level. On a P2P link, Level-1 and Level-2 packets are both sent in P2P hello packets, and you need not specify an interval for each level.

You can configure the **level-1** and **level-2** keywords only on broadcast interfaces. Before you configure the **level-1** or **level-2** keyword, enable IS-IS on the interface.

The shorter the interval, the more system resources will be occupied.

If no level is specified, the hello interval applies to both Level-1 and Level-2.

Examples

```
# Configure Level-2 hello packets to be sent every 20 seconds over VLAN-interface 10.
```

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 10
```

```
[Sysname-Vlan-interface10] isis timer hello 20 level-2
```

Related commands

isis timer holding-multiplier

isis timer holding-multiplier

Use **isis timer holding-multiplier** to set the IS-IS hello multiplier.

Use **undo isis timer holding-multiplier** to remove the configuration.

Syntax

isis timer holding-multiplier *value* [**level-1** | **level-2**]

undo isis timer holding-multiplier [level-1 | level-2]

Default

The default IS-IS hello multiplier is 3.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the number of hello intervals, in the range of 3 to 1000.

level-1: Applies the number to the Level-1 IS-IS neighbor.

level-2: Applies the number to the Level-2 IS-IS neighbor.

Usage guidelines

The hello multiplier is the number of hello packets a neighbor must miss before declaring the router is down.

If a neighbor does not receive any hello packets from the router within the advertised hold time, it considers the router down and recalculates the routes. The hold time is the hello multiplier multiplied by the hello interval.

Level-1 and Level-2 hello packets are sent independently on a broadcast network, so you need to specify a hello multiplier for each level. On a P2P link, Level-1 and Level-2 packets are both sent in P2P hello packets, and you need not specify Level-1 or Level-2.

You can configure the **level-1** and **level-2** keywords only on broadcast interfaces. Before you configure the **level-1** or **level-2** keyword, enable IS-IS on the interface.

If no level is specified, the hello multiplier applies to both Level-1 and Level-2.

The value of hello multiplier multiplied by hello interval cannot be more than 65535.

Examples

Set the hello multiplier to 6 for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer holding-multiplier 6
```

Related commands

isis timer hello

isis timer lsp

Use **isis timer lsp** to set the minimum interval for sending LSPs on the interface and specify the maximum number of LSPs that can be sent per time.

Use **undo isis timer lsp** to restore the default.

Syntax

isis timer lsp *time* [**count** *count*]

undo isis timer lsp

Default

The minimum interval for sending LSPs on the interface is 33 milliseconds, and the maximum number of LSPs that can be sent at a time is 5.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the minimum interval for sending link-state packets, in the range of 1 to 1000 milliseconds.

count: Specifies the maximum number of link-state packets to be sent at one time, in the range of 1 to 1000.

Usage guidelines

If a change occurs in the LSDB, IS-IS advertises the changed LSP to neighbors. You can specify the minimum interval for sending these LSPs to control the amount of LSPs on the network.

Examples

```
# Set the interval to 500 milliseconds for sending LSPs on VLAN-interface 10.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer lsp 500
```

Related commands

isis timer retransmit

isis timer retransmit

Use **isis timer retransmit** to configure the interval for retransmitting LSP packets over a point-to-point link.

Use **undo isis timer retransmit** to restore the default.

Syntax

isis timer retransmit *seconds*

undo isis timer retransmit

Default

The retransmission interval on a P2P link is 5 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the interval for retransmitting LSP packets, in the range of 1 to 300 seconds.

Usage guidelines

On a P2P link, IS-IS requires an advertised LSP be acknowledged. If no acknowledgment is received within a configurable interval, IS-IS will retransmit the LSP.

You do not need to use this command over a broadcast link where CSNPs are periodically broadcast to implement LSDB synchronization.

Examples

```
# Set the LSP retransmission interval on a P2P link to 50 seconds for VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis circuit-type p2p
[Sysname-Vlan-interface10] isis timer retransmit 50
```

Related commands

isis circuit-type p2p

isis timer lsp

is-level

Use **is-level** to specify the IS level.

Use **undo is-level** to restore the default.

Syntax

is-level { level-1 | level-1-2 | level-2 }

undo is-level

Default

The IS level is **level-1-2**.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

level-1: Specifies Level-1, which means IS-IS only calculates intra-area routes and maintains the Level-1 LSDB.

level-1-2: Specifies Level-1-2, which means IS-IS calculates routes and maintains the LSDBs for both Level-1 and Level-2.

level-2: Specifies Level-2, which means IS-IS calculates routes and maintains the LSDB for Level-2 only.

Usage guidelines

If only one area exists, configure all the routers as either Level-1 or Level-2, because the routers do not need to maintain two identical LSDBs at the same time.

If the only area is an IP network, configure all the routers as Level-2 for scalability.

Examples

```
# Set the IS level to Level-1 for IS-IS process 1.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] is-level level-1
```

is-name

Use **is-name** to specify a host name for the IS and enable dynamic system ID to hostname mapping.

Use **undo is-name** to disable dynamic system ID to hostname mapping.

Syntax

is-name *sys-name*

undo is-name

Default

Dynamic system ID to hostname mapping is disabled, and no host name is configured for the IS.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

sys-name: Specifies a host name for the local IS, a case-insensitive string of 1 to 64 characters.

Usage guidelines

To display the host name rather than the system ID of an IS by using the **display isis lsdb** command, first enable dynamic system ID to hostname mapping.

Examples

Configure a host name for the local IS.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] is-name RUTA
```

Related commands

display isis name-table

is-name map

Use **is-name map** to configure a system ID to host name mapping for a remote IS.

Use **undo is-name map** to remove the mapping.

Syntax

is-name map *sys-id map-sys-name*

undo is-name map *sys-id*

Default

No system ID to host name mapping is configured for a remote IS.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

sys-id: Specifies the system ID or pseudonode ID of a remote IS.

map-sys-name: Specifies a host name for the remote IS, a case-insensitive string of 1 to 64 characters.

Usage guidelines

Each remote IS system ID corresponds to only one name.

Examples

```
# Map the host name RUTB to the system ID 0000.0000.0041 of the remote IS.  
<Sysname> system-view  
[Sysname] isis 1  
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB
```

Related commands

display isis name-table

ispf enable

Use **ispf enable** to enable IS-IS incremental SPF (ISPF).

Use **undo ispf enable** to disable IS-IS ISPF.

Syntax

ispf enable

undo ispf enable

Default

IS-IS ISPF is enabled.

Views

IS-IS view

Predefined user roles

network-admin

Usage guidelines

When a network topology is changed, ISPF recomputes only the affected part of the SPT, instead of the entire SPT.

Examples

```
# Enable IS-IS ISPF.  
<Sysname> system-view  
[Sysname] isis 1  
[Sysname-isis-1] ispf enable
```

log-peer-change

Use **log-peer-change** to enable the logging of neighbor state changes.

Use **undo log-peer-change** to disable the logging.

Syntax

log-peer-change

undo log-peer-change

Default

The logging of IS-IS neighbor state changes is enabled.

Views

IS-IS view

Predefined user roles

network-admin

Usage guidelines

This command enables sending logs about IS-IS neighbor state changes to the information center. For IS-IS neighbor state change logs to be sent correctly, you must also configure the information center parameters on the device. For more information about information center, see the network management and monitoring configuration guide for the device.

Examples

```
# Disable the logging of IS-IS neighbor state changes.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] undo log-peer-change
```

lsp-fragments-extend

Use **lsp-fragments-extend** to enable LSP fragment extension for a level.

Use **undo lsp-fragments-extend** to restore the default.

Syntax

```
lsp-fragments-extend [ level-1 | level-1-2 | level-2 ]
undo lsp-fragments-extend
```

Default

LSP fragment extension is disabled.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

level-1: Applies the fragment extension to Level-1 LSPs.

level-1-2: Applies the fragment extension to both Level-1 and Level-2 LSPs.

level-2: Applies the fragment extension to Level-2 LSPs.

Usage guidelines

If no level is specified, the command enables LSP fragment extension for both Level-1 and Level-2.

Examples

```
# Enable LSP fragment extension for Level-2.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] lsp-fragments-extend level-2
```

Isp-length originate

Use **Isp-length originate** to configure the maximum size of generated Level-1 or Level-2 LSPs.

Use **undo Isp-length originate** to remove the configuration.

Syntax

Isp-length originate *size* [**level-1** | **level-2**]

undo Isp-length originate [**level-1** | **level-2**]

Default

The maximum size of generated Level-1 and Level-2 LSPs is 1497 bytes.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum size of LSP packets, in the range of 512 to 16384 bytes.

level-1: Applies the size to Level-1 LSP packets.

level-2: Applies the size to Level-2 LSP packets.

Usage guidelines

If neither Level-1 nor Level-2 is specified in the command, the configured maximum size applies to the current IS-IS level.

Examples

```
# Set the maximum size of the generated Level-2 LSPs to 1024 bytes.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] lsp-length originate 1024 level-2
```

Isp-length receive

Use **Isp-length receive** to configure the maximum size of received LSPs.

Use **undo Isp-length receive** to restore the default.

Syntax

Isp-length receive *size*

undo Isp-length receive

Default

The maximum size of received LSPs is 1497 bytes.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum size of received LSPs, in the range of 512 to 16384 bytes.

Examples

```
# Configure the maximum size of received LSPs to 1024 bytes.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] lsp-length receive 1024
```

maximum load-balancing

Use **maximum load-balancing** to configure the maximum number of ECMP routes for load balancing.

Use **undo maximum load-balancing** to restore the default.

Syntax

```
maximum load-balancing number
undo maximum load-balancing
```

Default

The maximum number of IS-IS ECMP routes equals the maximum number of ECMP routes supported by the system.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of ECMP routes. The value of 1 indicates that IS-IS does not perform load balancing. The value range for the *number* argument depends on the **max-ecmp-num** command. If you use the **max-ecmp-num** command to configure the maximum number of ECMP routes supported by the system as *m* and reboot the device, the value range for the *number* argument becomes 1 to *m*.

Examples

```
# Set the maximum number of ECMP routes to 2.
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] address-family ipv4
[Sysname-isis-100-ipv4] maximum load-balancing 2
```

Related commands

max-ecmp-num

network-entity

Use **network-entity** to configure the Network Entity Title (NET) for an IS-IS process.

Use **undo network-entity** to delete a NET.

Syntax

```
network-entity net
```

undo network-entity *net*

Default

No NET is configured.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

net. Specifies a NET as a dotted hexadecimal string in the X...X.XXXX....XXXX.00 format. The X...X segment represents the area address, the XXXX....XXXX segment represents the system ID, and the 00 segment is the SEL.

Usage guidelines

A NET is a special NSAP address with the SEL being 0. The length of the NET is in the range of 8 to 20 bytes.

A NET comprises the following parts:

- **Area ID**—With a length of 1 to 13 bytes.
- **System ID**—A system ID uniquely identifies a host or router in the area and has a fixed 6-byte length.
- **SEL**—It has a value of 0 and a fixed 1-byte length.

For example, a NET of ab.cdef.1234.5678.9abc.00 specifies the area ID ab.cdef, the system ID 1234.5678.9abc, and the SEL 00.

Examples

```
# Set the NET to 10.0001.1010.1020.1030.00, of which 10.0001 is the area ID and 1010.1020.1030 is the system ID.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
```

Related commands

isis

isis enable

non-stop-routing

Use **non-stop-routing** to enable IS-IS NSR.

Use **undo non-stop-routing** to disable IS-IS NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

IS-IS NSR is disabled.

Views

IS-IS view

Predefined user roles

network-admin

Usage guidelines

IS-IS NSR takes effect on a per-process basis. As a best practice, enable NSR for each IS-IS process.

IS-IS NSR and IS-IS GR are mutually exclusive. Therefore, do not configure the **non-stop-routing** command and the **graceful-restart** command at the same time.

Examples

```
# Enable NSR for IS-IS process 1.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] non-stop-routing
```

pic

Use **pic** to enable IS-IS PIC.

Use **undo pic** to disable IS-IS PIC.

Syntax

```
pic [ additional-path-always ]
undo pic
```

Default

IS-IS PIC is enabled.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

additional-path-always: Allows the indirect suboptimal route as the backup route.

Usage guidelines

Prefix Independent Convergence (PIC) enables the device to speed up network convergence by ignoring the number of prefixes. PIC applies only to indirect routes.

When both IS-IS PIC and IS-IS FRR are configured, only IS-IS FRR takes effect.

Examples

```
# Configure IS-IS PIC to support the indirect suboptimal route as the backup route.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] pic additional-path-always
```

preference

Use **preference** to configure the preference for IS-IS.

Use **undo preference** to restore the default.

Syntax

```
preference { preference | route-policy route-policy-name } *  
undo preference
```

Default

IS-IS preference is 15.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

preference: Specifies an IS-IS protocol preference in the range of 1 to 255.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to assign a priority to the matching routes.

Usage guidelines

If multiple routing protocols find routes to the same destination, the route found by the routing protocol with the highest preference is selected as the optimal route.

If a routing policy is specified in this command, the preference set by the routing policy applies to the matching routes. Other routes use the preference set by the **preference** command.

Examples

```
# Set the preference for IS-IS to 25.  
<Sysname> system-view  
[Sysname] isis 1  
[Sysname-isis-1] address-family ipv4  
[Sysname-isis-1-ipv4] preference 25
```

prefix-priority

Use **prefix-priority** to assign convergence priorities to specific IS-IS routes.

Use **undo prefix-priority** to remove the configuration.

Syntax

```
prefix-priority { critical | high | medium } { prefix-list prefix-list-name | tag tag-value }  
prefix-priority route-policy route-policy-name  
undo prefix-priority { critical | high | medium } [ prefix-list | tag ]  
undo prefix-priority route-policy
```

Default

IS-IS routes have the lowest convergence priority.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

critical: Specifies the highest convergence priority.

high: Specifies the high convergence priority.

medium: Specifies the medium convergence priority.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters.

tag *tag-value*: Specifies a tag value in the range of 1 to 4294967295.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

The higher the convergence priority, the faster the convergence speed.

IS-IS host routes have a medium convergence priority.

Examples

Assign the high convergence priority to IS-IS routes permitted by IP prefix list **standtest**.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] prefix-priority high prefix-list standtest
```

reset isis all

Use **reset isis all** to clear all IS-IS data structure information.

Syntax

reset isis all [*process-id*] [**graceful-restart**]

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535 to clear the data structure information for an IS-IS process.

graceful-restart: Recovers the data through graceful restart after the data is cleared.

Usage guidelines

If no IS-IS process is specified, the command clears data structure information for all IS-IS processes.

Use this command when LSPs must be updated immediately.

Examples

Clear all IS-IS data structure information.

```
<Sysname> reset isis all
```

reset isis event-log graceful-restart

Use **reset isis event-log graceful-restart** to clear IS-IS GR log information.

Syntax

reset isis event-log graceful-restart slot *slot-number*

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*. Specifies an IRF member device by its ID.

Examples

```
# Clear IS-IS GR log information.
<Sysname> reset isis event-log graceful-restart
# Clear IS-IS GR log information for the specified slot.
<Sysname> reset isis event-log graceful-restart slot 1
```

reset isis event-log lsp

Use **reset isis event-log lsp** to clear IS-IS LSP log information.

Syntax

reset isis event-log lsp [*process-id*]

Views

User view

Predefined user roles

network-admin

Parameters

process-id. Specifies an IS-IS process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears LSP log information for all IS-IS processes.

Examples

```
# Clear LSP log information for IS-IS process 1.
<Sysname> reset isis event-log lsp 1
```

Related commands

display isis event-log lsp

reset isis event-log non-stop-routing

Use **reset isis event-log non-stop-routing** to clear IS-IS NSR log information.

Syntax

reset isis event-log non-stop-routing slot *slot-number*

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID.

Examples

```
# Clear IS-IS NSR log information for the specified slot.
<Sysname> reset isis event-log non-stop-routing slot 1
```

reset isis event-log spf

Use **reset isis event-log spf** to clear IS-IS route calculation log information.

Syntax

```
reset isis event-log spf [ process-id ]
```

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears route calculation log information for all IS-IS processes.

Examples

```
# Clear route calculation log information for IS-IS process 1.
<Sysname> reset isis event-log spf 1
```

Related commands

display isis event-log spf

reset isis packet

Use **reset isis packet** to clear IS-IS packet statistics.

Syntax

```
reset isis packet [ csnp | hello | lsp | psnp ] [ interface-type interface-number ] [ process-id ]
```

Views

User view

Predefined user roles

network-admin

Parameters

csnp: Clears CSNP packet statistics.

hello: Clears hello packet statistics.

lsp: Clears LSP packet statistics.

psnp: Clears PSNP packet statistics.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this option, the command clears IS-IS packet statistics for all interfaces.

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears IS-IS packet statistics for all IS-IS processes.

Examples

```
# Clear IS-IS packet statistics for all IS-IS processes.  
<Sysname> reset isis packet
```

Related commands

display isis packet

reset isis peer

Use **reset isis peer** to clear data structure information for a specified IS-IS neighbor.

Syntax

```
reset isis peer system-id [ process-id ]
```

Views

User view

Predefined user roles

network-admin

Parameters

system-id: Specifies an IS-IS neighbor by its system ID.

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535 to clear data structure information for the neighbor in the specified IS-IS process.

Usage guidelines

Use this command when you re-establish an IS-IS neighbor relationship.

Examples

```
# Clear the data structure information of the neighbor with the system ID 0000.0c11.1111.  
<Sysname> reset isis peer 0000.0c11.1111
```

reset osi statistics

Use **reset osi statistics** to clear OSI packet statistics.

Syntax

```
reset osi statistics
```

Views

User view

Predefined user roles

network-admin

Usage guidelines

To obtain OSI packet statistics from the specified time point, first clear the existing statistics.

Examples

```
# Clear OSI packet statistics.  
<Sysname> reset osi statistics
```

Related commands

display osi statistics

set-att

Use **set-att** to set the ATT bit of Level-1 LSPs.

Use **undo set-att** to restore the default.

Syntax

```
set-att { always | never }
```

```
undo set-att
```

Default

The ATT bit is not set for Level-1 LSPs.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

always: Sets the ATT bit of Level-1 LSPs.

never: Keeps the ATT bit of Level-1 LSPs not set.

Examples

```
# Set the ATT bit of Level-1 LSPs.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] set-att always
```

set-overload

Use **set-overload** to set the overload bit.

Use **undo set-overload** to restore the default.

Syntax

```
set-overload [ on-startup [ [ start-from-nbr system-id [ timeout1 [ nbr-timeout ] ] ] | timeout2 |
wait-for-bgp [ timeout3 ] ] ] [ allow { external | interlevel } * ]
```

```
undo set-overload
```

Default

The overload bit is not set.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

on-startup: Sets the overload bit upon system startup.

start-from-nbr system-id [timeout1 [nbr-timeout]]: Starts the *nbr-timeout* timer when the router begins to establish the neighbor relationship with the neighbor after system startup. If the neighbor relationship is formed within the *nbr-timeout* interval, IS-IS keeps the overload bit set. If not, the bit is

cleared. IS-IS keeps the overload bit set within the *timeout1* interval after the neighbor relationship is formed within the *nbr-timeout* interval.

- *system-id*—Specifies the neighbor.
- *timeout1*—The *timeout1* interval is in the range of 5 to 86400 seconds, and the default is 600 seconds.
- *nbr-timeout*—The timer has an interval from 5 to 86400 seconds. The default is 1200 seconds.

timeout2: Sets the overload bit within the *timeout2* interval after system startup. The interval is in the range of 5 to 86400 seconds, and the default is 600 seconds.

wait-for-bgp [*timeout3*]: Starts the *timeout3* timer for BGP convergence after system startup. If BGP is not converged within the *timeout3* interval, IS-IS clears the overload bit. The value range for the *timeout3* argument is 5 to 86400 seconds, and the default is 600 seconds.

allow: Allows advertising address prefixes. By default, no address prefixes are allowed to be advertised when the overload bit is set.

external: Allows advertising IP address prefixes redistributed from other routing protocols with the **allow** keyword specified.

interlevel: Allows advertising IP address prefixes learned from different IS-IS levels with the **allow** keyword specified.

Usage guidelines

If the **on-startup** keyword is not specified, the command sets the overload bit immediately until the **undo set-overload** command is executed.

If the **on-startup** keyword is specified, IS-IS sets the overload bit upon system startup and keeps it set within the *timeout2* interval.

Examples

```
# Set overload flag on the current router.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] set-overload
```

snmp context-name

Use **snmp context-name** to set the context name for the SNMP object for managing IS-IS.

Use **undo snmp context-name** to restore the default.

Syntax

```
snmp context-name context-name
undo snmp context-name
```

Default

No context name is set for the SNMP object for managing IS-IS.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

context-name: Specifies a context name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

TRILL shares the standard IS-IS MIB with IS-IS. The standard IS-IS MIB provides only single-instance MIB objects. For SNMP to correctly identify TRILL's management information in the standard IS-IS MIB, you must configure a unique context for TRILL.

Context is a method introduced to SNMPv3 for multiple-instance management. For SNMPv1/v2c, you must specify a community name as a context name for protocol identification.

Examples

```
# Configure the context name as isis for the SNMP object for managing IS-IS process 1.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] snmp context-name isis
```

snmp-agent trap enable isis

Use **snmp-agent trap enable isis** to enable IS-IS SNMP notifications.

Use **undo snmp-agent trap enable isis** to disable IS-IS SNMP notifications.

Syntax

snmp-agent trap enable isis [**adjacency-state-change** | **area-mismatch** | **authentication** | **authentication-type** | **buffsize-mismatch** | **id-length-mismatch** | **lsdboverload-state-change** | **lsp-corrupt** | **lsp-parse-error** | **lsp-size-exceeded** | **manual-address-drop** | **max-seq-exceeded** | **maxarea-mismatch** | **own-lsp-purge** | **protocol-support** | **rejected-adjacency** | **skip-sequence-number** | **version-skew**] *

undo snmp-agent trap enable isis [**adjacency-state-change** | **area-mismatch** | **authentication** | **authentication-type** | **buffsize-mismatch** | **id-length-mismatch** | **lsdboverload-state-change** | **lsp-corrupt** | **lsp-parse-error** | **lsp-size-exceeded** | **manual-address-drop** | **max-seq-exceeded** | **maxarea-mismatch** | **own-lsp-purge** | **protocol-support** | **rejected-adjacency** | **skip-sequence-number** | **version-skew**] *

Default

IS-IS SNMP notifications are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

adjacency-state-change: Specifies notifications about IS-IS adjacency status changes.

area-mismatch: Specifies notifications about area address mismatches between hello packets.

authentication: Specifies notifications about authentication failures of IS-IS packets.

authentication-type: Specifies notifications about authentication type errors of IS-IS packets.

buffsize-mismatch: Specifies notifications about buffer size mismatches for LSPs.

id-length-mismatch: Specifies notifications about system ID length mismatches of IS-IS packets.

lsdboverload-state-change: Specifies notifications about LSDB overload state changes.

lsp-corrupt: Specifies notifications about LSP checksum errors in the LSDB.

lsp-parse-error: Specifies notifications about LSP packet parse failures.

lsp-size-exceeded: Specifies notifications about propagation failures caused by oversized LSPs.

manual-address-drop: Specifies notifications about manually configured area addresses that have been dropped.

max-seq-exceeded: Specifies notifications about attempts to exceed the maximum LSP sequence number.

maxarea-mismatch: Specifies notifications about maximum area address mismatches of hello packets.

own-lsp-purge: Specifies notifications about attempts to remove the local LSP.

protocol-support: Specifies notifications about supported-protocol mismatches.

rejected-adjacency: Specifies notifications about adjacency creation failures.

skip-sequence-number: Specifies notifications about LSP sequence number duplications.

version-skew: Specifies notifications about hello packet version mismatches.

Usage guidelines

If you do not specify a notification, this command enables all IS-IS SNMP notifications.

If no IS-IS process exists, the configuration is not allowed.

This function does not take effect if all configured IS-IS processes are deleted.

Examples

```
# Disable IS-IS SNMP notifications.
<Sysname> system-view
[Sysname] undo snmp-agent trap enable isis
```

summary

Use **summary** to configure a summary route.

Use **undo summary** to remove a summary route.

Syntax

```
summary ip-address { mask-length | mask } [ avoid-feedback | generate_null0_route ] [ level-1 | level-1-2 | level-2 ] | tag tag ] *
```

```
undo summary ip-address { mask-length | mask } [ level-1 | level-1-2 | level-2 ]
```

Default

No summary route is configured.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IP address of the summary route.

mask-length: Specifies the mask length of the summary route, in the range of 0 to 32.

mask: Specifies the mask of the destination IP address, in dotted decimal notation.

avoid-feedback: Avoids learning summary routes by route calculation.

generate_null0_route: Generates the Null 0 route to avoid routing loops.

level-1: Summarizes only the routes redistributed to Level-1.

level-1-2: Summarizes the routes redistributed to both Level-1 and Level-2.

level-2: Summarizes only the routes redistributed to Level-2.

tag tag: Specifies a management tag in the range of 1 to 4294967295.

Usage guidelines

To reduce the size of the routing table, as well as the size of LSP and LSDB generated by the router, summarize multiple contiguous networks into a single network. You can summarize native IS-IS routes and redistributed routes. After summarization, the cost of the summary route is the smallest cost of the summarized routes.

If no level is specified, only **level-2** routes are summarized.

The router summarizes only routes generated from local LSPs.

Examples

Configure a summary route of 202.0.0.0/8.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] summary 202.0.0.0 255.0.0.0
```

timer lsp-generation

Use **timer lsp-generation** to set the LSP generation interval.

Use **undo timer lsp-generation** to remove the configuration.

Syntax

timer lsp-generation *maximum-interval* [*minimum-interval* [*incremental-interval*]] [**level-1** | **level-2**]

undo timer lsp-generation [**level-1** | **level-2**]

Default

The maximum interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum interval in the range of 1 to 120 seconds.

minimum-interval: Specifies the minimum interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the incremental interval in the range of 10 to 60000 milliseconds.

level-1: Applies the intervals to Level-1.

level-2: Applies the intervals to Level-2. If no level is specified, the specified intervals apply to both Level-1 and Level-2.

Usage guidelines

By adjusting the LSP generation interval, you can prevent bandwidth and router resources from being over consumed due to frequent topology changes.

If you specify only the *maximum-interval* argument, the LSP generation interval is *maximum-interval*.

If you do not specify the *incremental-interval* argument, the LSP generation interval is in the range of *minimum-interval* to *maximum-interval*.

If you specify the *incremental-interval* argument, the LSP generation interval is as follows:

- When network changes are not frequent, the *minimum-interval* is adopted.
- If network changes are frequent, the LSP generation interval increases by *incremental-interval* $\times 2^{n-2}$ (n is the number of calculation times) each time a generation occurs until the *maximum-interval* is reached.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

```
# Set the maximum interval, minimum interval, and incremental interval to 10 seconds, 100 milliseconds, and 200 milliseconds, respectively.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1]timer lsp-generation 10 100 200
```

timer lsp-max-age

Use **timer lsp-max-age** to set the LSP maximum age in the LSDB.

Use **undo timer lsp-max-age** to restore the default.

Syntax

```
timer lsp-max-age seconds
```

```
undo timer lsp-max-age
```

Default

The LSP maximum age is 1200 seconds.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

seconds: Specifies the LSP maximum aging time in the range of 1 to 65535 seconds.

Usage guidelines

Each LSP has an age that decreases in the LSDB. Any LSP with an age of 0 is deleted from the LSDB. You can adjust the age value based on the scale of a network.

Examples

```
# Set the maximum LSP age to 1500 seconds.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] timer lsp-max-age 1500
```

Related commands

```
timer lsp-refresh
```

timer lsp-refresh

Use **timer lsp-refresh** to set the LSP refresh interval.

Use **undo timer lsp-refresh** to restore the default.

Syntax

timer lsp-refresh *seconds*

undo timer lsp-refresh

Default

The default LSP refresh interval is 900 seconds.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

seconds: Specifies the LSP refresh interval in the range of 1 to 65534 seconds.

Usage guidelines

Each router refreshes its LSPs at a configurable interval and sends them to other routers to achieve the following purposes:

- Prevent valid routes from aging out.
- Synchronize LSPs in the network.

A smaller refresh interval speeds up network convergence but consumes more bandwidth.

To refresh LSPs before they are aged out, the interval configured by the **timer lsp-refresh** command must be smaller than that configured by the **timer lsp-max-age** command.

Examples

```
# Set the LSP refresh interval to 1500 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] timer lsp-refresh 1500
```

Related commands

timer lsp-max-age

timer spf

Use **timer spf** to set the SPF calculation interval.

Use **undo timer spf** to restore the default.

Syntax

timer spf *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo timer spf

Default

The maximum interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum SPF calculation interval in the range of 1 to 120 seconds.

minimum-interval: Specifies the minimum SPF calculation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the incremental SPF calculation interval in the range of 10 to 60000 milliseconds.

Usage guidelines

Based on the LSDB, an IS-IS router uses the SPF algorithm to calculate a shortest path tree with itself being the root, and uses the shortest path tree to determine the next hop to a destination network. By adjusting the SPF calculation interval, you can prevent bandwidth and router resources from being overused due to frequent topology changes.

When network changes are not frequent, the *minimum-interval* is adopted. If network changes become frequent, the SPF calculation interval increases by the *incremental-interval* each time a generation happens until the *maximum-interval* is reached.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum interval to 10 seconds, the minimum interval to 100 milliseconds, and the incremental interval to 300 milliseconds, respectively.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] timer spf 10 100 300
```

virtual-system

Use **virtual-system** to configure a virtual system ID for the IS-IS process.

Use **undo virtual-system** to remove a virtual system ID.

Syntax

virtual-system *virtual-system-id*

undo virtual-system *virtual-system-id*

Default

No virtual system ID is configured.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

virtual-system-id: Specifies a virtual system ID for the IS-IS process.

Examples

Set a virtual system ID of 2222.2222.2222 for IS-IS process 1.

```
<Sysname> system-view  
[Sysname] isis 1  
[Sysname-isis-1] virtual-system 2222.2222.2222
```