

capability lls

To enable the use of the Link-Local Signalling (LLS) data block in originated OSPF packets and reenable OSPF nonstop forwarding (NSF) awareness, use the **capability lls** command in router configuration mode. To disable LLS and OSPF NSF awareness, use the **no** form of this command.

capability lls

no capability lls

Syntax Description This command has no arguments or keywords.

Defaults LLS is enabled.

Command Modes Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

You might want to disable NSF awareness by disabling the use of the LLS data block in originated OSPF packets. You might want to disable NSF awareness if the router has no applications using LLS.

If NSF is configured and you try to disable LLS, you will receive the error message, “OSPF Non-Stop Forwarding (NSF) must be disabled first.”

If LLS is disabled and you try to configure NSF, you will receive the error message, “OSPF Link-Local Signaling (LLS) capability must be enabled first.”

Examples

The following example disables LLS support and OSPF NSF awareness:

```
router ospf 2
 no capability lls
```

capability vrf-lite

To suppress the Provider Edge (PE) specific checks on a router when the OSPF process is associated with the VRF, use the **capability vrf-lite** command in router configuration mode. To restore the checks, use the **no** form of this command.

capability vrf-lite

no capability vrf-lite

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled. PE specific checks are performed if the process is associated with VRF command modes.

Command Modes

Router configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)B	This command was integrated into Cisco IOS Release 12.2(8)B.

Usage Guidelines

This command works only if the OSPF process is associated with the VRF.

When the OSPF process is associated with the VRF, several checks are performed when link-state advertisements (LSAs) are received. PE checks are needed to prevent loops when the PE is performing a mutual redistribution between OSPF and BGP interfaces.

Type-3 LSA received	The DN bit is checked. If the DN bit is set, the Type-3 LSA is not considered during the SPF calculation.
Type-5 or -7 LSA received	If the Tag in the LSA is equal to the VPN-tag, the Type-5 or-7 LSA is not considered during the SPF calculation.

In some situations, performing PE checks might not be desirable. The concept of VRFs can be used on a router that is not a PE router (that is, a router that is not running BGP). With the **capability vrf-lite** command, the checks can be turned off to allow correct population of the VRF routing table with routes to IP prefixes.

Examples

This example shows a router configured with multi-VRF.

```
router ospf 100 vrf grc
  capability vrf-lite
```

clear bgp nsap

To clear and then reset Connectionless Network Service (CLNS) network service access point (NSAP) Border Gateway Protocol (BGP) sessions, use the **clear bgp nsap** command in privileged EXEC mode.

```
clear bgp nsap { * | as-number | ip-address } [soft] [in | out]
```

Syntax Description

*	Clears and then resets all current BGP sessions.
<i>as-number</i>	Clears and then resets BGP sessions for BGP neighbors within the specified autonomous system.
<i>ip-address</i>	Clears the TCP connection to the specified BGP neighbor and removes all routes learned from the connection from the BGP table. The TCP connections are then reset.
soft	(Optional) Soft reset. Allows routing tables to be reconfigured and activated without clearing the BGP session.
in out	(Optional) Triggers inbound or outbound soft reconfiguration. If the in or out option is not specified, both inbound and outbound soft reset are triggered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **clear bgp nsap** command is similar to the **clear ip bgp** command, except that it is NSAP address family-specific.

Use of the **clear bgp nsap** command allows a reset of the neighbor sessions with varying degrees of severity, depending on the specified keywords and arguments.

Use the ***** keyword to reset all neighbor sessions. The software will clear and then reset the neighbor connections. Use this form of the command in the following situations:

- BGP timer specification change
- BGP administrative distance changes

Use the **soft out** keywords to clear and reset only the outbound neighbor connections. Inbound neighbor sessions will not be reset. Use this form of the command in the following situations:

- Additions or changes are made to the BGP-related access lists
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Use the **in** keyword to clear only the inbound neighbor connections. Outbound neighbor sessions will not be reset. Use this form of the command in the following situations:

- BGP-related access lists change or get additions
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Examples

The following example clears the inbound session with the neighbor 172.20.16.6 without the outbound session being reset:

```
Router# clear bgp nsap 172.20.16.6 in
```

The following example clears the outbound session with the neighbors in autonomous system 65000 without the inbound session being reset:

```
Router# clear bgp nsap 65000 soft out
```

Related Commands

Command	Description
show bgp nsap	Displays entries in the BGP routing table for the NSAP address family.

clear bgp nsap dampening

To clear Border Gateway Protocol (BGP) route dampening information for the network service access point (NSAP) address family and unsuppress the suppressed routes, use the **clear bgp nsap dampening** command in privileged EXEC mode.

```
clear bgp nsap dampening [nsap-prefix]
```

Syntax Description

<i>nsap-prefix</i>	(Optional) NSAP prefix about which to clear dampening information. This argument can be up to 20 octets long.
--------------------	---

Defaults

When the *nsap-prefix* argument is not specified, the **clear bgp nsap dampening** command clears route dampening information for the entire BGP routing table for the NSAP address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **clear bgp nsap dampening** command is similar to the **clear ip bgp dampening** command, except that it is specific to the NSAP address family.

Examples

The following example clears route dampening information about the route to NSAP prefix 49.6001 and unsuppresses its suppressed routes:

```
Router# clear bgp nsap dampening 49.6001
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show bgp nsap dampened-paths	Displays BGP dampened routes for the NSAP address family.

clear bgp nsap external

To clear all external Border Gateway Protocol (BGP) peers for the network service access point (NSAP) address family, use the **clear bgp nsap external** command in privileged EXEC mode.

```
clear bgp nsap external [soft] [in | out]
```

Syntax Description

soft	(Optional) Soft reset. Does not reset the session.
in out	(Optional) Triggers inbound or outbound soft reconfiguration. If the in or out option is not specified, both inbound and outbound soft reset are triggered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **clear bgp nsap external** command is similar to the **clear ip bgp external** command, except that it is specific to the NSAP address family.

Examples

The following example clears the inbound session with external BGP peers without the outbound session being reset:

```
Router# clear bgp nsap external soft in
```

Related Commands

Command	Description
clear bgp nsap	Resets an NSAP BGP connection by dropping all neighbor sessions.

clear bgp nsap flap-statistics

To clear Border Gateway Protocol (BGP) flap statistics for the network service access point (NSAP) address family, use the **clear bgp nsap flap-statistics** command in privileged EXEC mode.

clear bgp nsap flap-statistics [*nsap-prefix*] [**regexp** *regexp* | **filter-list** *access-list-number*]

Syntax Description		
<i>nsap-prefix</i>	(Optional) NSAP prefix about which to clear dampening information. This argument can be up to 20 octets long.	
regexp <i>regexp</i>	(Optional) Clears flap statistics for all the paths that match the regular expression.	
filter-list <i>access-list-number</i>	(Optional) Clears flap statistics for all the paths that pass the access list. The acceptable access list number range is from 1 to 199.	

Defaults

No statistics are cleared.

If no arguments or keywords are specified, the software clears flap statistics for all routes.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **clear bgp nsap flap-statistics** command is similar to the **clear ip bgp flap-statistics** command, except that it is specific to the NSAP address family.

The flap statistics for a route are also cleared when an NSAP BGP peer is reset. Although the reset withdraws the route, no penalty is applied in this instance even though route flap dampening is enabled.

Examples

The following example clears all of the flap statistics for paths that pass access list 3:

```
Router# clear bgp nsap flap-statistics filter-list 3
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show bgp nsap flap-statistics	Displays BGP flap statistics for the NSAP address family.

clear bgp nsap peer-group

To clear the Border Gateway Protocol (BGP) TCP connections to all members of a BGP peer group for the network service access point (NSAP) address family, use the **clear bgp nsap peer-group** command in privileged EXEC mode.

```
clear bgp nsap peer-group peer-group-name
```

Syntax Description	<i>peer-group-name</i> Name of the NSAP BGP peer group.
---------------------------	---

Defaults	No BGP TCP connections are cleared.
-----------------	-------------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines	The clear bgp nsap peer-group command is similar to the clear ip bgp peer-group command, except that it is specific to the NSAP address family.
-------------------------	---

Examples	The following example shows the BGP TCP connections being cleared for all members of the NSAP BGP peer group named internal:
-----------------	--

```
Router# clear bgp nsap peer-group internal
```

Related Commands	Command	Description
	neighbor peer-group (assigning members)	Configures a BGP neighbor to be a member of a peer group.

clear ip bgp

To reset a BGP connection using BGP soft reconfiguration, use the **clear ip bgp** command in privileged EXEC mode at the system prompt.

```
clear ip bgp { * | neighbor-address | peer-group-name } [soft [in | out]]
```

Syntax Description		
*		Specifies that all current BGP sessions will be reset.
<i>neighbor-address</i>		Specifies that only the identified BGP neighbor will be reset.
<i>peer-group-name</i>		Specifies that the specified BGP peer group will be reset.
soft		(Optional) Soft reset. Does not reset the session.
in out		(Optional) Triggers inbound or outbound soft reconfiguration. If the in or out option is not specified, both inbound and outbound soft reset is triggered.

Defaults No reset is initiated.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(6)T	The dynamic inbound soft reset capability was added.
	12.0(2)S	The dynamic inbound soft reset capability was added.

Usage Guidelines You can reset inbound routing table updates dynamically or by generating new updates using stored update information. Using stored update information required additional memory for storing the updates.

To reset inbound routing table updates dynamically, all BGP routers must support the route refresh capability. To determine whether a BGP router supports this capability, use the [show ip bgp neighbors](#) command. If a router supports the route refresh capability, the following message is displayed:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp** { * | *address* | *peer-group-name* } **in** command. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the [neighbor soft-reconfiguration inbound](#) command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Examples

The following example clears the inbound session with the neighbor 10.108.1.1 without resetting the session:

```
Router# clear ip bgp 10.108.1.1 soft in
```

The following example clears the outbound session with the peer group named corp without resetting the session:

```
Router# clear ip bgp corp soft out
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp	Displays entries in the BGP routing table.

clear ip bgp dampening

To clear BGP route dampening information and unsuppress the suppressed routes, use the **clear ip bgp dampening** command in privileged EXEC mode.

```
clear ip bgp dampening [ip-address network-mask]
```

Syntax Description	<i>ip-address</i>	(Optional) IP address of the network about which to clear dampening information.
	<i>network-mask</i>	(Optional) Network mask applied to the <i>ip-address</i> argument.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	11.0	This command was introduced.

Examples

The following example clears route dampening information about the route to network 192.168.0.0 and unsuppresses its suppressed routes. When the address and mask arguments are not specified, the **clear ip bgp dampening** command clears route dampening information for the entire BGP routing table.

```
Router# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

Related Commands	Command	Description
	bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
	show ip bgp dampened-paths	Displays BGP dampened routes.

clear ip bgp external

To clear external Border Gateway Protocol (eBGP) peers, use the **clear ip bgp external** command in privileged EXEC mode.

```
clear ip bgp external [in | out]
```

```
clear ip bgp external [soft [in | out]]
```

```
clear ip bgp external {ipv4 | ipv6} {multicast | unicast} [in | out | soft]
```

```
clear ip bgp external [vpn4 unicast] {in | out | soft}
```

Syntax Description		
in out	(Optional)	Triggers inbound or outbound soft reconfiguration.
soft	(Optional)	Triggers soft reconfiguration.
ipv4 ipv6 vpn4	(Optional)	Triggers reset of IPv4, IPv6, or VPNn4 address family session.
multicast	(Optional)	Triggers reset of IPv4 or IPv6 multicast address family session.
unicast	(Optional)	Triggers reset of IPv4, IPv6, or VPNv4 unicast family session.

Defaults A reset is not initiated.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(2)S	This command was introduced.

Usage Guidelines Using the **clear ip bgp external** command without the **soft** keyword will reset the session.

Examples The following examples clear an inbound session with the eBGP peers:

```
Router# clear ip bgp external in
```

or

```
clear ip bgp external soft in
```

The following example clears an outbound address family IPv4 multicast session with the eBGP peers:

```
Router# clear ip bgp external ipv4 multicast out
```

Related Commands	Command	Description
	clear ip bgp	Resets a BGP connection or session.

■ clear ip bgp external

neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp	Displays entries in the BGP routing table.

clear ip bgp flap-statistics

To clear BGP flap statistics, use the **clear ip bgp flap-statistics** command in privileged EXEC mode.

```
clear ip bgp flap-statistics [{regexp regexp} | {filter-list list-name} | {ip-address network-mask}]
```

```
clear ip bgp [ip-address] flap-statistics
```

Syntax Description

<i>ip-address</i>	(Optional) Clears flap statistics for a single entry at this IP address. If this argument is placed before flap-statistics , the router clears flap statistics for all paths from the neighbor at this address.
regexp <i>regexp</i>	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list <i>list-name</i>	(Optional) Clears flap statistics for all the paths that pass the access list.
<i>network-mask</i>	(Optional) Network mask applied to the <i>ip-address</i> argument.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

If no arguments or keywords are specified, the router will clear BGP flap statistics for all routes. The flap statistics for a route are also cleared when a BGP peer is reset. Although the reset withdraws the route, no penalty is applied in this instance even though route flap dampening is enabled.

Examples

The following example clears all of the flap statistics for paths that pass filter list 3:

```
Router# clear ip bgp flap-statistics filter-list 3
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.

clear ip bgp peer-group

To clear all the members of a BGP peer group, use the **clear ip bgp peer-group** command in privileged EXEC mode.

clear ip bgp peer-group *tag*

Syntax Description	<i>tag</i>	Name of the BGP peer group to clear.
--------------------	------------	--------------------------------------

Defaults	No BGP peer group members are cleared.
----------	--

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	11.0	This command was introduced.

Examples	The following example clears all members from the BGP peer group named internal:
----------	--

```
Router# clear ip bgp peer-group internal
```

Related Commands	Command	Description
	neighbor peer-group (assigning members)	Configures a BGP neighbor to be a member of a peer group.

clear ip eigrp neighbors

To delete entries from the neighbor table, use the **clear ip eigrp neighbors** command in EXEC mode.

clear ip eigrp neighbors [*ip-address* | *interface-type interface-number*]

Syntax Description		
<i>ip-address</i>	(Optional)	Address of the neighbor.
<i>interface-type</i> <i>interface-number</i>	(Optional)	Interface type and number. Specifying these arguments removes the specified interface type from the neighbor table that all entries learned via this interface.

Command Modes	
	EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following example removes the neighbor whose address is 172.16.8.3:

```
Router# clear ip eigrp neighbors 172.16.8.3
```

Related Commands	Command	Description
	show ip eigrp interfaces	Displays information about interfaces configured for EIGRP.

clear ip eigrp vrf neighbor

To clear neighbor entries of the specified Enhanced Interior Gateway Routing Protocol (EIGRP) virtual routing and forwarding instance (VRF) from the Routing Information Base (RIB), use the **clear ip eigrp vrf command** in **privileged EXEC** mode.

```
clear ip eigrp vrf {vrf-name as-number} neighbor [interface-number]
```

Syntax Description

<i>vrf-name</i>	Specifies the name of the VRF whose EIGRP neighbors will be cleared. The * keyword can be used as a wild card to specify all VRFs
<i>as-number</i>	Specifies the autonomous system number of the VRF whose neighbors will be cleared.
<i>interface-number</i>	(optional) Specifies the interface that VRF neighbors were learned through. The exact interface is specified by interface number with the <i>interface-number</i> argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into 12.2(15)T.

Examples

The following example clears EIGRP neighbors reached through the VRF named VRF-RED in autonomous system 101:

```
clear ip eigrp vrf VRF-RED 101 neighbor
```

The following example clears EIGRP neighbors reached through the VRF named VRF-GREEN in autonomous-system 101 learned through Ethernet interface 0/0:

```
clear ip eigrp vrf VRF-RED 101 neighbor ethernet 0/0
```

Related Commands

Command	Description
show ip eigrp vrf interfaces	Displays EIGRP interfaces that are defined under the specified VRF.
show ip eigrp vrf neighbors	Displays neighbors discovered by EIGRP that carry VRF information.
show ip eigrp vrf topology	Displays VRF entries in the EIGRP topology table.
show ip eigrp vrf traffic	Displays EIGRP VRF traffic statistics.
show ip route vrf	Displays routing protocol information that is associated with a VRF.

clear ip ospf

To clear redistribution based on the OSPF routing process ID, use the **clear ip ospf** command in privileged EXEC mode.

```
clear ip ospf [pid] {process | redistribution | counters [neighbor [neighbor-interface]
[neighbor-id]}}
```

Syntax Description

<i>pid</i>	(Optional) Process ID.
process	Reset OSPF process.
redistribution	Clear OSPF route redistribution.
counters	OSPF counters.
neighbor	(Optional) Neighbor statistics per interface.
<i>neighbor-interface</i>	(Optional) Neighbor interface.
<i>neighbor-id</i>	(Optional) Neighbor ID.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use the *pid* argument to clear only one OSPF process. If the *pid* argument is not specified, all OSPF processes are cleared.

Examples

The following example clears all OSPF processes:

```
clear ip ospf process
```

clear ip prefix-list

To reset the hit count of the prefix list entries, use the **clear ip prefix-list** command in privileged EXEC mode.

```
clear ip prefix-list [prefix-list-name] [network/length]
```

Syntax Description		
<i>prefix-list-name</i>	(Optional) The name of the prefix list from which the hit count is to be cleared.	
<i>network/length</i>	(Optional) The network number and length (in bits) of the network mask. The slash mark is required.	

Defaults Does not clear the hit count.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0	This command was introduced.

Usage Guidelines The hit count is a value indicating the number of matches to a specific prefix list entry.

Examples The following example clears the hit count from the prefix list entries for the prefix list named `first_list` that match the network mask `10.0.0.0/8`:

```
Router# clear ip prefix-list first_list 10.0.0.0/8
```

Related Commands	Command	Description
	distribute-list in (IP)	Filters networks received in updates.
	distribute-list out (IP)	Suppresses networks from being advertised in updates.
	ip prefix-list	Creates an entry in a prefix list.
	ip prefix-list description	Adds a text description of a prefix list.
	ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
	redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
	show ip bgp regexp	Displays information about a prefix list or prefix list entries.

compatible rfc1583

To restore the method used to calculate summary route costs per RFC 1583, use the **compatible rfc1583** command in router configuration mode. To disable RFC 1583 compatibility, use the **no** form of this command.

compatible rfc1583

no compatible rfc1583

Syntax Description

This command has no arguments or keywords.

Defaults

Compatible with RFC 1583.

Command Modes

Router configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

This command is backward compatible with Cisco IOS Release 12.0.

To minimize the chance of routing loops, all OSPF routers in an OSPF routing domain should have RFC compatibility set identically.

Because of the introduction of RFC 2328, OSPF Version 2, the method used to calculate summary route costs has changed. Use the **no compatible rfc1583** command to enable the calculation method used per RFC 2328.

Examples

The following example specifies that the router process is compatible with RFC 1583:

```
router ospf 1
  compatible rfc1583
!
```

dampening

To configure a router to automatically dampen a flapping interface, use the **dampening** command in interface configuration mode. To disable automatic route dampening, use the **no** form of this command.

dampening [*half-life-period reuse-threshold*] [*suppress-threshold max-suppress-time* [*restart-penalty*]]

no dampening

Syntax Description

<i>half-life-period</i>	(optional) Time (in seconds) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period expires. The range of the half-life period is from 1 to 30 seconds. The default time is 5 seconds.
<i>reuse-threshold</i>	(optional) Reuse value based on the number of penalties. When the accumulated penalty decreases enough to fall below this value, the route is unsuppressed. The range of the reuse value is from 1 to 20000; the default is 1000.
<i>suppress-threshold</i>	(optional) Value of the accumulated penalty that triggers the router to dampen a flapping interface. A route is suppressed when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
<i>max-suppress-time</i>	(optional) Maximum time (in seconds) a route can be suppressed. The range is from 1 to 20000; the default is four times the <i>half-life-period</i> value. If the <i>half-life-period</i> value is allowed to default, the maximum suppress time defaults to 20 seconds.
<i>restart-penalty</i>	(optional) Penalty to applied to the interface when it comes up for the first time after the router reloads. The configurable range is from 1 to 20000 penalties. The default is 2000 penalties. This argument is not required for any other configurations.

Defaults

This command is disabled by default. To manually configure the timer for the *restart-penalty* argument, the value for all arguments must be manually entered.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The IP Event Dampening feature will function on a subinterface but cannot be configured on only the subinterface. Only the primary interface can be configured with this feature, and all the subinterfaces are subject to the same dampening configuration.

When an interface is dampened, the interface is dampened to both IP and Connectionless Network Services (CLNS) routing equally. The interface is dampened to both IP and CLNS because integrated routing protocols like Intermediate System-to-Intermediate System (IS-IS), IP, and CLNS routing protocols are closely interconnected, so it is impossible to apply dampening separately.

This occurs because for integrated protocols like Intermediate System-to-Intermediate System (IS-IS), IP, and CLNS routing are closely interconnected, so it is impossible to apply dampening separately.

Copying a dampening configuration from virtual templates to virtual access interfaces is not supported because dampening has limited usefulness to existing applications using virtual templates. Virtual access interfaces are released when an interface flaps, and new connections and virtual access interfaces are acquired when the interface comes up and is made available to the network. Because dampening states are attached to the interface, the dampening states would not survive an interface flap.

If this command is applied to an interface that already has dampening configured, all dampening states are reset and the accumulated penalty will be set to 0. If the interface has been dampened, the accumulated penalty will fall into the reuse threshold range, and the dampened interface will be made available to the network. The flap counts, however, are retained.

Examples

The following example sets the half life to 30 seconds, the reuse threshold to 1500, the suppress threshold to 10000, and the maximum suppress time to 120 seconds:

```
interface Ethernet 0/0
 dampening 30 1500 10000 120
```

The following example configures the router to apply a penalty of 500 on Ethernet interface 0/0 when the interface comes up for the first time after the router is reloaded:

```
interface Ethernet 0/0
 dampening 5 500 1000 20 500
```

Related Commands

Command	Description
clear counters	Clears the interface counters.
show dampening interface	Displays a summary of interface dampening.
show interface dampening	Displays a summary of the dampening parameters and status.

default-information

To control the candidate default routing information or Enhanced Interior Gateway Routing Protocol (EIGRP) processes, use the **default-information** command in router configuration mode. To suppress EIGRP candidate information in incoming or outbound updates, use the **no default-information in** command.

default-information {**allowed** {**in** | **out**} | **in** | **out**} [*acl-number* | *acl-name*]

no default-information {**allowed** {**in** | **out**} | **in** | **out**}

Syntax Description

allowed	Configures EIGRP to accept default routing information.
in	Configures EIGRP to accept exterior or default routing information.
out	Configures EIGRP to advertise external routing information.
<i>acl-number</i>	(Optional) Standard access list number from 1 to 99 or an expanded standard access list from 1300 to 1999.
<i>acl-name</i>	(Optional) Named standard access list.

Defaults

Normally, exterior routes are always accepted and default information is passed between EIGRP processes when redistribution occurs.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>access-list-number</i> and <i>access-list-name</i> arguments were added.

Usage Guidelines

The default network of 0.0.0.0 used by Routing Information Protocol (RIP) can be redistributed by EIGRP.

Examples

The following example allows exterior or default routes to be received by an EIGRP peer in autonomous system 23:

```
router eigrp 23
 default-information in
```

default-information originate (RIP)

To generate a default route into Routing Information Protocol (RIP), use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

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

```
no default-information originate
```

Syntax Description	route-map <i>map-name</i> (Optional) Routing process will generate the default route if the route map is satisfied.
---------------------------	--

Defaults	This command is disabled by default.
-----------------	--------------------------------------

Command Modes	Router configuration
----------------------	----------------------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	The route map referenced in the default-information originate command cannot use an extended access list; it can use a standard access list.
-------------------------	---

Examples	The following example originates a default route (0.0.0.0/0) over a certain interface when 172.68.0.0/16 is present. Applying a condition (in this case a route map) to determine when the default route is originated is called “conditional default origination.”
-----------------	---

```
router rip
  version 2
  network 172.68.16.0
  default-information originate route-map condition
!
  route-map condition permit 10
  match ip address 10
  set interface s1/0
!
access-list 10 permit 172.68.16.0 0.0.0.255
!
```

default-information originate (BGP)

To control the redistribution of a protocol or network into the BGP, use the **default-information originate** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

default-information originate

no default-information originate

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Address family configuration
Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(7)T	Address family configuration mode was added.

Usage Guidelines The **default-information originate** command should be used if the network operator needs to control the redistribution of default routes. Using the **default-information originate** command in BGP is similar to using the **network** command. However, to achieve the same result as configuring the **network** command with the route 0.0.0.0, the **default-information originate** command requires an explicit redistribution of the route 0.0.0.0. The **network** command requires only that route 0.0.0.0 is specified in the Interior Gateway Protocol (IGP) routing table. For this reason, the **network** command is preferred for redistributing default routes and protocols into BGP.

Examples The following address family configuration mode example configures BGP to redistribute OSPF into BGP:

```
router bgp 164
  address-family ipv4 unicast
  default-information originate
  redistribute ospf 109
```

The following router configuration mode example configures BGP to redistribute OSPF into BGP:

```
router bgp 164
  default-information originate
  redistribute ospf 109
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

default-information originate (IS-IS)

To generate a default route into an IS-IS routing domain, use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

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

no default-information originate [**route-map** *map-name*]

Syntax Description	route-map <i>map-name</i> (Optional) Routing process will generate the default route if the route map is satisfied.
---------------------------	--

Defaults	This command is disabled by default.
-----------------	--------------------------------------

Command Modes	Router configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines If a router configured with this command has a route to 0.0.0.0 in the routing table, IS-IS will originate an advertisement for 0.0.0.0 in its link-state packets (LSPs).

Without a route map, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the attached-bit (ATT) in Level 1 LSPs.

A route map can be used for two purposes:

- Make the router generate default in its Level 1 LSPs.
- Advertise 0/0 conditionally.

With a **match ip address** *standard-access-list* command, you can specify one or more IP routes that must exist before the router will advertise 0/0.

Examples The following example forces the software to generate a default external route into an IS-IS domain:

```
router isis
! BGP routes will be distributed into IS-IS
redistribute bgp 120
! access list 2 is applied to outgoing routing updates
distribute-list 2 out
default-information originate
! access list 2 defined as giving access to network 10.105.0.0
access-list 2 permit 10.105.0.0 0.0.255.255
```

Related Commands	Command	Description
	redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
	show isis database	Displays the IS-IS link-state database.

default-information originate (OSPF)

To generate a default external route into an OSPF routing domain, use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

```
default-information originate [always] [metric metric-value] [metric-type type-value]
  [route-map map-name]
```

```
no default-information originate [always] [metric metric-value] [metric-type type-value]
  [route-map map-name]
```

Syntax Description		
always	(Optional) Always advertises the default route regardless of whether the software has a default route.	
metric <i>metric-value</i>	(Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 1. The value used is specific to the protocol.	
metric-type <i>type-value</i>	(Optional) External link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values: 1—Type 1 external route 2—Type 2 external route The default is type 2 external route.	
route-map <i>map-name</i>	(Optional) Routing process will generate the default route if the route map is satisfied.	

Defaults This command is disabled by default.

Command Modes Router configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Whenever you use the **redistribute** or the **default-information** router configuration command to redistribute routes into an OSPF routing domain, the Cisco IOS software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

When you use this command for the OSPF process, the default network must reside in the routing table, and you must satisfy the **route-map** *map-name* keyword and argument. Use the **default-information originate always route-map** *map-name* form of the command when you do not want the dependency on the default network in the routing table.

Examples

The following example specifies a metric of 100 for the default route redistributed into the OSPF routing domain and an external metric type of Type 1:

```
router ospf 109
 redistribute eigrp 108 metric 100 subnets
 default-information originate metric 100 metric-type 1
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

default-metric (BGP)

To set a default metric for routes redistributed into Border Gateway Protocol (BGP), use the **default-metric** command in address family or router configuration mode. To remove the configured value and return BGP to default operation, use the **no** form of this command.

default-metric *number*

no default-metric *number*

Syntax Description

<i>number</i>	Default metric value applied to the redistributed route. The range of values for this argument is from 1 to 4294967295.
---------------	---

Defaults

The following is default behavior if this command is not configured or if the **no** form of this command is entered:

- The metric of redistributed interior gateway protocol (IGP) routes is set to a value that is equal to the interior BGP (iBGP) metric.
- The metric of redistributed connected and static routes is set to 0.

When this command is enabled, the metric for redistributed connected routes is set to 0.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode support was added.

Usage Guidelines

The **default-metric** command is used to set the metric value for routes redistributed into BGP with the **redistribute** command. A default metric can be configured to solve the problem of redistributing routes with incompatible metrics. Assigning the default metric will allow redistribution to occur.

This value is the Multi Exit Discriminator (MED) that is evaluated by BGP during the best path selection process. The MED is a non-transitive value that is processed only within the local autonomous system and adjacent autonomous systems. The default metric is not set if the received route has a MED value.



Note

When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

Examples

In the following example, a metric of 1024 is set for routes redistributed into BGP from OSPF:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)# default-metric 1024
Router(config-router-af)# redistribute ospf 10
Router(config-router-af)# end
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

default-metric (EIGRP)

To set metrics for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **default-metric** command in router configuration mode. To remove the metric value and restore the default state, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

Syntax Description

<i>bandwidth</i>	Minimum bandwidth of the route in kilobits per second. It can be from 1 to 4294967295.
<i>delay</i>	Route delay in tens of microseconds. It can be 1 or any positive number that is a multiple of 39.1 nanoseconds.
<i>reliability</i>	Likelihood of successful packet transmission expressed as a number between 0 and 255. The value 255 means 100 percent reliability; 0 means no reliability.
<i>loading</i>	Effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).
<i>mtu</i>	Minimum maximum transmission unit (MTU) size of the route in bytes. It can be from 1 to 65535.

Defaults

Only connected routes can be redistributed without a default metric. The metric of redistributed connected routes is set to 0.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	Address family support was added in Cisco IOS Release 12.0(22)S.
12.0(15)T	Address family support was added in Cisco IOS Release 12.2(15)T

Usage Guidelines

A default metric is required to redistribute a protocol into EIGRP, unless you use the **redistribute** command. You do not need default metrics to redistributed EIGRP into itself.



Note

The **default-metric** command does not affect EIGRP-to-EIGRP distribution. To configure EIGRP-to-EIGRP distribution, use route maps.

Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values. Keeping the same metrics is supported only when redistributing from EIGRP, or static routes.

When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

Examples

The following example takes redistributed Routing Information Protocol (RIP) metrics and translates them into EIGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
router eigrp 109
 network 172.16.0.0
 redistribute rip
 default-metric 1000 100 250 100 1500
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

default-metric (OSPF)

To set default metric values for the OSPF routing protocol, use the **default-metric** command in router configuration mode. To return to the default state, use the **no** form of this command.

default-metric *metric-value*

no default-metric *metric-value*

Syntax Description	<i>metric-value</i>	Default metric value appropriate for the specified routing protocol.
--------------------	---------------------	--

Defaults	Built-in, automatic metric translations, as appropriate for each routing protocol. The metric of redistributed connected and static routes is set to 0.
----------	---

Command Modes	Router configuration
---------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.
------------------	--



Note

When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

Examples	The following example shows a router in autonomous system 109 using both the Routing Information Protocol (RIP) and the OSPF routing protocols. The example advertises OSPF-derived routes using RIP and assigns the Internal Gateway Protocol (IGP)-derived routes a RIP metric of 10.
----------	---

```
router rip
 default-metric 10
 redistribute ospf 109
```

Related Commands	Command	Description
	redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

default-metric (RIP)

To set default metric values for Routing Information Protocol (RIP), use the **default-metric** command in router configuration mode. To return to the default state, use the **no** form of this command.

default-metric *number-value*

no default-metric [*number-value*]

Syntax Description

<i>number-value</i>	Default metric value.
---------------------	-----------------------

Defaults

Built-in, automatic metric translations, as appropriate for each routing protocol. The metric of redistributed connected and static routes is set to 0.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.



Note

When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

Examples

The following example shows a router in autonomous system 109 using both the RIP and the Open Shortest Path First (OSPF) routing protocols. The example advertises OSPF-derived routes using RIP and assigns the OSPF-derived routes a RIP metric of 10.

```
router rip
 default-metric 10
 redistribute ospf 109
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

discard-route

To reinstall either an external or internal discard route that was previously removed, use the **discard-route** command in router configuration mode. To remove either an external or internal discard route, use the **no** form of this command.

discard-route [external | internal]

no discard-route [external | internal]

Syntax Description

external	(Optional) Reinstalls the discard route entry for redistributed summarized routes on an Autonomous System Boundary Router (ASBR).
internal	(Optional) Reinstalls the discard-route entry for summarized internal routes on the Area Border Router (ABR).

Defaults

External and internal discard route entries are installed.

Command Modes

Router configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

External and internal discard route entries are installed in routing tables by default. During route summarization, routing loops may occur when data is sent to a nonexisting network that appears to be a part of the summary, and the router performing the summarization has a less specific route (pointing back to the sending router) for this network in its routing table. To prevent the routing loop, a discard route entry is installed in the routing table of the ABR or ASBR.

If for any reason you do not want to use the external or internal discard route, remove the discard route by entering the **no discard-route** command with either the external or internal keyword.

Examples

The following display shows the discard route functionality installed by default. When external or internal routes are summarized, a summary route to Null0 will appear in the router output from the **show ip route** command. See the router output lines that appear in bold font:

```
Router# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

```

Gateway of last resort is not set

      172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
C       172.16.0.128/25 is directly connected, Loopback1
O       172.16.0.0/24 is a summary, 00:00:14, Null0
C       172.16.0.0/25 is directly connected, Loopback0
      172.31.0.0/24 is variably subnetted, 3 subnets, 2 masks
C       172.31.0.128/25 is directly connected, Loopback3
O       172.31.0.0/24 is a summary, 00:00:02, Null0
C       172.31.0.0/25 is directly connected, Loopback2
C       192.168.0.0/24 is directly connected, Ethernet0/0

```

```
RouterB# show ip route ospf
```

```

      172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
O       172.16.0.0/24 is a summary, 00:00:29, Null0
      172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
O       201.0.0.0/24 is a summary, 00:00:17, Null0

```

When the **no discard-route** command with the **internal** keyword is entered, notice the following route change, indicated by the router output lines that appear in bold font:

```
RouterB# configure terminal
```

```

Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)# router ospf 1
RouterB(config-router)# no discard-route internal
RouterB(config-router)#end

```

```
RouterB# show ip route ospf
```

```

      172.31.0.0/24 is variably subnetted, 3 subnets, 2 masks
O       172.16.0.0/24 is a summary, 00:04:14, Null0

```

Next, the **no discard-route** command with the **external** keyword is entered to remove the external discard route entry:

```
RouterB# configure terminal
```

```

Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)# router ospf 1
RouterB(config-router)# no discard-route external
RouterB(config-router)# end

```

The following router output from the **show running-config** command confirms that both the external and internal discard routes have been removed from the routing table of RouterB. See the router output lines that appear in bold font:

```
RouterB# show running-config
```

```

Building configuration...

Current configuration : 1114 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
.
.
.

```

discard-route

```
router ospf 1
  log-adjacency-changes
  no discard-route external
  no discard-route internal
  area 1 range 172.16.0.0 255.255.255.0
  summary-address 172.31.0.0 255.255.255.0
  redistribute rip subnets
  network 192.168.0.0 0.0.0.255 area 0
  network 172.16.0.0 0.0.0.255 area 1
!
```

Related Commands

Command	Description
show ip route	Displays the current state of the routing table.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

distance (IP)

To define an administrative distance, use the **distance** command in router configuration mode. To remove a distance definition, use the **no** form of this command.

distance {*ip-address* {*wildcard-mask*}} [*ip-standard-list*] [*ip-extended-list*]

no distance {*ip-address* {*wildcard-mask*}} [*ip-standard-list*] [*ip-extended-list*]

Syntax Description

<i>ip-address</i>	IP address in four-part, dotted notation.
<i>wildcard-mask</i>	Wildcard mask in four-part, dotted decimal format. A bit set to 1 in the <i>wildcard-mask</i> argument instructs the software to ignore the corresponding bit in the address value.
<i>ip-standard-list</i> <i>ip-extended-list</i>	(Optional) Number or name of a standard or extended IP access list to be applied to incoming routing updates.

Defaults

For more information on default administrative distance, see “Usage Guidelines.”

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>access-list-number</i> <i>name</i> argument was added.
11.3	The <i>access-list-number</i> <i>name</i> argument was removed.
11.3	The ip keyword was removed.
12.0	The <i>ip-standard-list</i> and <i>ip-extended-list</i> arguments were added.

Usage Guidelines

[Table 2](#) lists default administrative distances.

Table 2 Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (eBGP)	20
Internal EIGRP	90
Open Shortest Path First (OSPF)	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120

Table 2 Default Administrative Distances (continued)

Route Source	Default Distance
EIGRP external route	170
Internal BGP	200
Unknown	255

Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored.

When the optional access list number is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows filtering of networks according to the IP address of the router supplying the routing information. This option could be used, as an example, to filter out possibly incorrect routing information from routers not under your administrative control.

The order in which you enter **distance** commands can affect the assigned administrative distances in unexpected ways (see the “Examples” section for further clarification).

For BGP, the **distance** command sets the administrative distance of the External BGP (EBGP) route.

The **show ip protocols EXEC** command displays the default administrative distance for a specified routing process.

Always set the administrative distance from the least to the most specific network.

**Note**

The weight of a route can no longer be set with the **distance** command. To set the weight for a route, use a route-map.

Examples

In the following example, the **router eigrp** global configuration command sets up EIGRP routing in autonomous system number 109. The **network** router configuration commands specify EIGRP routing on networks 192.168.7.0 and 172.16.0.0. The first **distance** router configuration command sets the default administrative distance to 255, which instructs the Cisco IOS software to ignore all routing updates from routers for which an explicit distance has not been set. The second **distance** command sets the administrative distance for all routers on the Class C network 192.168.7.0 to 90. The third **distance** command sets the administrative distance for the router with the address 172.16.1.3 to 120.

```
router eigrp 109
 network 192.168.7.0
 network 172.16.0.0
 distance 255
 distance 90 192.168.7.0 0.0.0.255
 distance 120 172.16.1.3 0.0.0.0
```

In the following example, the set distance is from the least to the most specific network:

```
router eigrp 100
 network 10.0.0.0
 distance 22 10.0.0.0
 distance 33 10.11.0.0 0.0.255.255
 distance 44 10.11.12.0 0.0.0.255
```

**Note**

In this example, adding distance 255 to the end of the list would override the distance values for all networks within the range specified in the example. The result is that the distance values are set to 255.

Related Commands

Command	Description
<code>distance bgp</code>	Allows the use of external, internal, and local administrative distances that could be a better route to a node.

distance bgp

To allow the use of external, internal, and local administrative distances that could be a better route than other external, internal, or local routes to a node, use the **distance bgp** command in address family or router configuration mode. To return to the default values, use the **no** form of this command.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Syntax Description

<i>external-distance</i>	Administrative distance for BGP external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Acceptable values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.
<i>internal-distance</i>	Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.
<i>local-distance</i>	Administrative distance for BGP local routes. Local routes are those networks listed with a network router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

Defaults

external-distance: 20
internal-distance: 200
local-distance: 200

Command Modes

Address family configuration
 Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.

**Caution**

Changing the administrative distance of BGP internal routes is considered dangerous and is not recommended. One problem that can arise is the accumulation of routing table inconsistencies, which can break routing.

The **distance bgp** command replaces the **distance mbgp** command.

Examples

In the following router configuration mode example, internal routes are known to be preferable to those learned through the Interior Gateway Protocol (IGP), so the administrative distance values are set accordingly:

```
router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 distance bgp 20 20 200
```

In the following address family configuration mode example, internal routes are known to be preferable to those learned through IGP, so the administrative distance values are set accordingly:

```
router bgp 109
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 address family ipv4 multicast
 network 10.108.0.0
 distance bgp 20 20 200
 neighbor 192.168.6.6 activate
 neighbor 172.16.1.1 activate
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.

distance eigrp

To allow the use of two administrative distances—internal and external—that could be a better route to a node, use the **distance eigrp** command in router configuration mode. To reset these values to their defaults, use the **no** form of this command.

distance eigrp *internal-distance external-distance*

no distance eigrp

Syntax Description

<i>internal-distance</i>	Administrative distance for Enhanced Interior Gateway Routing Protocol (EIGRP) internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255.
<i>external-distance</i>	Administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. The distance can be a value from 1 to 255.

Defaults

internal-distance: 90
external-distance: 170

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Use the **distance eigrp** command if another protocol is known to be able to provide a better route to a node than was actually learned via external EIGRP, or if some internal routes should really be preferred by EIGRP.

[Table 3](#) lists the default administrative distances.

Table 3 Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP summary route	5

Table 3 Default Administrative Distances (continued)

Route Source	Default Distance
External BGP	20
Internal EIGRP	90
Open Shortest Path First (OSPF)	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
EIGRP external route	170
Internal Border Gateway Protocol (BGP)	200
Unknown	255

To display the default administrative distance for a specified routing process, use the **show ip protocols EXEC** command.

Examples

In the following example, the **router eigrp** global configuration command sets up EIGRP routing in autonomous system number 109. The **network** router configuration commands specify EIGRP routing on networks 192.168.7.0 and 172.16.0.0. The **distance eigrp** command sets the administrative distance of all EIGRP internal routes to 80 and all EIGRP external routes to 130.

```
Router(config)# router eigrp 109
Router(config-router)# network 192.168.7.0
Router(config-router)# network 172.16.0.0
Router(config-router)# distance eigrp 80 130
```

Related Commands

Command	Description
show ip protocols	Displays the parameters and current state of the active routing protocol process.

distance ospf

To define OSPF route administrative distances based on route type, use the **distance ospf** command in router configuration mode. To restore the default value, use the **no** form of this command.

distance ospf {[intra-area *dist1*] [inter-area *dist2*] [external *dist3*]}

no distance ospf

Syntax Description

intra-area <i>dist1</i>	(Optional) Sets the distance for all routes within an area. The default value is 110.
inter-area <i>dist2</i>	(Optional) Sets the distance for all routes from one area to another area. The default value is 110.
external <i>dist3</i>	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. The default value is 110.

Defaults

dist1: 110
dist2: 110
dist3: 110

Command Modes

Router configuration

Command History

Release	Modification
11.1(14)	This command was introduced.

Usage Guidelines

You must specify at least one of the keyword-argument pairs.

This command performs the same function as the **distance** command used with an access list. However, the **distance ospf** command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.

A common reason to use the **distance ospf** command is when you have multiple OSPF processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

Examples

The following example changes the external distance to 200, making the route less reliable:

Router A Configuration

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

Router B Configuration

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

Related Commands

Command	Description
distance (IP)	Defines an administrative distance.

distribute-list in (BGP)

To filter routes or networks received in incoming Border Gateway Protocol (BGP) updates, use the **distribute-list in** command in router configuration mode. To delete the distribute list and remove it from the running configuration file, use the **no** form of this command.

distribute-list {*acl-number* | **prefix** *list-name*} **in**

no distribute-list {*acl-number* | **prefix** *list-name*} **in**

Syntax Description

<i>acl-number</i>	IP access list number. The access list defines which networks are to be received and which are to be suppressed in routing updates.
prefix <i>list-name</i>	Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching prefixes in the prefix list.



Note

Interface type and number arguments may be displayed in the CLI depending on the installed version of Cisco IOS software. However, the interface arguments are not support in any software release.

Defaults

If this command is configured without a predefined access list, the distribute list will default to permitting all traffic.

Command Modes

Router configuration



Note

The **distribute-list in** command can be entered in address family configuration mode. However, address family configuration is not recommended and not supported.

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>acl-number</i> arguments was added.
12.0	The prefix <i>list-name</i> argument was added.

Usage Guidelines

The **distribute-list in** command is used to filter incoming BGP updates. An access list must be defined prior to configuration of this command. In addition to access lists, prefix list can be used to filter based upon the prefix length, making it possible to filter either on the prefix list, the gateway, or both for incoming updates. The session must be reset with the **clear ip bgp** command before the distribute list will take effect. To suppress networks from being advertised in updates, use the **distribute-list out** command.

**Note**

We recommend that you use IP prefix lists (configured with the **ip prefix-list** command in global configuration mode) instead of distribute lists. IP prefix lists provide improved performance and are simpler to configure. Distribute list configuration will be removed from the CLI at a future date.

**Note**

Prefix lists and access lists are mutually exclusive when configuring a distribute list. We recommend that you do not use both the *prefix-list* and *access-list-name* arguments with the **distribute-list in** command.

Examples

In the following example, a prefix list and distribute list are defined to configure the BGP routing process to accept traffic from only network 192.168.1.0 and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
Router(config)# ip prefix-list RED deny 0.0.0.0/0 le 32
Router(config)# ip prefix-list RED permit 10.108.0.0/16
Router(config)# ip prefix-list RED permit 192.168.1.0/24
Router(config)# !
Router(config)# router bgp 50000
Router(config-router)# network 10.108.0.0
Router(config-router)# distribute-list prefix RED in
Router(config-router)# end
Router# clear ip bgp in
```

In the following example, an access list and a distribute list are defined to configure the BGP routing process to accept traffic from only network 192.168.1.0 and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
Router(config)# access-list 1 permit 192.168.1.0
Router(config)# access-list 1 permit 10.108.0.0
Router(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Router(config)# !
Router(config)# router bgp 50000
Router(config-router)# network 10.108.0.0
Router(config-router)# distribute-list 1 in
Router(config-router)# end
Router# clear ip bgp in
```

Related Commands

Command	Description
access-list	Defines an IP access list.
clear ip bgp	Resets a BGP connection or session.
distribute-list out (BGP)	Suppresses networks from being advertised in outbound BGP updates.
ip prefix-list	Creates an entry in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list in (IP)

To filter networks received in updates, use the **distribute-list in** command in router configuration mode. To change or cancel the filter, use the **no** form of this command.

distribute-list [*access-list-number* | *name*] | [**route-map** *map-tag*] **in** [*interface-type* | *interface-number*]

no distribute-list [*access-list-number* | *name*] | [**route-map** *map-tag*] **in** [*interface-type* | *interface-number*]

Syntax Description

<i>access-list-number</i> <i>name</i>	(Optional) Standard IP access list number or name. The list defines which networks are to be received and which are to be suppressed in routing updates.
route-map <i>map-tag</i>	(Optional) Name of the route map that defines which networks are to be installed in the routing table and which are to be filtered from the routing table. This argument is supported by OSPF only.
in	Applies the access list to incoming routing updates.
<i>interface-type</i>	(Optional) Interface type. The <i>interface-type</i> argument cannot be used in address family configuration mode.
<i>interface-number</i>	(Optional) Interface number on which the access list should be applied to incoming updates. If no interface is specified, the access list will be applied to all incoming updates. The <i>interface type</i> and <i>number</i> arguments can apply if you specify an access list, not a route map. The <i>interface-number</i> argument cannot be used in address family configuration mode.

Defaults

This command is disabled by default.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>access-list-name</i> , <i>type</i> , and <i>number</i> arguments were added.
12.0(7)T	Address family configuration mode was added.
12.0(24)S	The route-map <i>map-tag</i> keyword and argument were added.

Usage Guidelines

This command must specify either an access list or a map-tag name of a route map. The route map is supported for OSPF filtering only.

The *interface-type* and *interface-number* arguments cannot be used in address family configuration mode.

OSPF routes cannot be filtered from entering the OSPF database. If you use this command for OSPF, it only filters routes from the routing table; it does not prevent link-state packets from being propagated.

If a route map is specified, the route map can be based on the following **match** options:

- **match interface**
- **match ip address**
- **match ip next-hop**
- **match ip route-source**
- **match metric**
- **match route-type**
- **match tag**

Configure the route map before specifying it in the **distribute-list in** command.

Examples

In the following example, the EIGRP routing process accepts only two networks—network 0.0.0.0 and network 10.108.0.0:

```
access-list 1 permit 0.0.0.0
access-list 1 permit 10.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router eigrp
 network 10.108.0.0
 distribute-list 1 in
```

In the following example, OSPF external LSAs have a tag. The value of the tag is examined before the prefix is installed in the routing table. All OSPF external prefixes that have the tag value of 777 are filtered (prevented from being installed in the routing table). The permit statement with sequence number 20 has no match conditions, and there are no other route-map statements after sequence number 20, so all other conditions are permitted.

```
route-map tag-filter deny 10
 match tag 777
route-map tag-filter permit 20
!
router ospf 1
 router-id 10.0.0.2
 log-adjacency-changes
 network 172.16.2.1 0.0.0.255 area 0
 distribute-list route-map tag-filter in
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list out (BGP)

To suppress networks from being advertised in outbound Border Gateway Protocol (BGP) updates, use the **distribute-list out** command in router configuration mode. To delete the distribute list and remove it from the running configuration file, use the **no** form of this command.

distribute-list *acl-number* | **prefix** *list-name* **out** [*protocol process-number* | **connected** | **static**]

no distribute-list *acl-number* | **prefix** *list-name* **out** [*protocol process-number* | **connected** | **static**]

Syntax Description

<i>acl-number</i>	IP access list number. The access list defines which networks are to be received and which are to be suppressed in routing updates.
prefix <i>list-name</i>	Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching prefixes in the prefix list.
<i>protocol process-number</i>	Specifies the routing protocol to apply the distribution list. BGP, EIGRP, OSPF, and RIP are supported. The process number is entered for all routing protocols, except RIP. The process number is a value from 1 to 65535.
connected	Specifies peers and networks learned through connected routes.
static	Specifies peers and networks learned through static routes.



Note

Interface type and number arguments may be displayed in the CLI depending on the installed version of Cisco IOS software. However, the interface arguments are not support in any software release.

Defaults

If this command is configured without a predefined access list, the distribute list will default to permitting all traffic.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>acl-number</i> argument was added.
12.0	The prefix <i>list-name</i> argument was added.

Usage Guidelines

The **distribute-list out** command is used to filter outbound BGP updates. An access list must be defined prior to configuration of this command. In addition to access lists, prefix list can be used to filter based upon the prefix length, making it possible to filter either on the prefix list, the gateway, or both for incoming updates. The session must be reset with the **clear ip bgp** command before the distribute list will take effect. To filter routes that are received in inbound updates, use the **distribute-list in** command.

Entering a *protocol* and/or *process-number* arguments causes the distribute list to be applied to only routes derived from the specified routing process. Addresses not specified in the distribute-list command will not be advertised in outgoing routing updates after a distribute list is configured.

**Note**

We recommend that you use IP prefix lists (configured with the **ip prefix-list** command in global configuration mode) instead of distribute lists. IP prefix lists provide improved performance and are simpler to configure. Distribute list configuration will be removed from the CLI at a future date.

**Note**

Prefix lists and access lists are mutually exclusive when configuring distribute lists. We recommend that you do not use both the *prefix-list* and *access-list-name* arguments with the **distribute-list out** command.

Examples

In the following example, an access list and a distribute list are defined to configure the BGP routing process to advertise only network 192.168.0.0. An outbound route refresh is initiated to activate the distribute-list.

```
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Router(config)# !
Router(config)# router bgp 50000
Router(config-router)# distribute-list 1 out
Router(config-router)# end
Router# clear ip bgp out
```

Related Commands

Command	Description
access-list	Defines an IP access list.
clear ip bgp	Resets a BGP connection or session.
distribute-list in (BGP)	Filters routes and networks received in updates.
ip prefix-list	Creates an entry in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list out (IP)

To suppress networks from being advertised in updates, use the **distribute-list out** command in router configuration mode. To cancel this function, use the **no** form of this command.

```
distribute-list {access-list-number | access-list-name} out [interface-name | routing-process | as-number]
```

```
no distribute-list {access-list-number | access-list-name} out [interface-name | routing-process | as-number]
```

Syntax Description

<i>access-list-number</i> <i>access-list-name</i>	Standard IP access list number or name. The list defines which networks are to be sent and which are to be suppressed in routing updates.
out	Applies the access list to outgoing routing updates.
<i>interface-name</i>	(Optional) Name of a particular interface. The <i>interface-name</i> argument cannot be used in address family configuration mode.
<i>routing-process</i>	(Optional) Name of a particular routing process, or the static or connected keyword.
<i>as-number</i>	(Optional) Autonomous system number.

Defaults

This command is disabled by default.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>access-list-name</i> argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

When networks are redistributed, a routing process name can be specified as an optional trailing argument to the **distribute-list** command. Specifying this option causes the access list to be applied to only those routes derived from the specified routing process. After the process-specific access list is applied, any access list specified by a **distribute-list** command without a process name argument will be applied. Addresses not specified in the **distribute-list** command will not be advertised in outgoing routing updates.

The *interface-name* argument cannot be used in address family configuration mode.



Note

To filter networks received in updates, use the **distribute-list in** command.

Examples

The following example would cause only one network to be advertised by a RIP routing process, network 10.108.0.0:

```
access-list 1 permit 10.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router rip
 network 10.108.0.0
 distribute-list 1 out
```

The following example applies access list 1 to outgoing routing updates and enables Enhanced Interior Gateway Routing Protocol (EIGRP) on Ethernet interface 0. Only network 10.10.101.0 will be advertised in outgoing EIGRP routing updates.

```
router isis
 redistribute ospf 109
 distribute-list 1 out
interface Ethernet 0
 ip router eigrp 100
access-list 1 permit 10.10.101.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
distribute-list in (IP)	Filters networks received in updates.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

domain-password

To configure the IS-IS routing domain authentication password, use the **domain-password** command in router configuration mode. To disable a password, use the **no** form of this command.

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

no domain-password [*password*]

Syntax Description

<i>password</i>	Password you assign.
authenticate snp	(Optional) Causes the system to insert the password into SNP protocol data units (PDUs).
validate	(Optional) Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
send-only	(Optional) Causes the system only to insert the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

Defaults

No domain password is specified and no authentication is enabled for exchange of Level 2 routing information.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(21)ST	The authenticate snp , validate , and send-only keywords were added.

Usage Guidelines

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

This password is inserted in Level 2 (area router level) PDU link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

If you do not specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, then the IS-IS routing protocol does not insert the password into SNPs.

Examples

The following example assigns an authentication password to the routing domain and specifies that the password be inserted in SNPs and checked in SNPs that the system receives:

```
router isis
 domain-password users2j45 authenticate snp validate
```

Related Commands

Command	Description
area-password	Configures the IS-IS area authentication password.
isis password	Configures the authentication password for an interface.

domain-tag

To set the Open Shortest Path First (OSPF) domain tag value for Type-5 or Type-7 link-state advertisements (LSAs) when OSPF is used as a protocol between a provider edge (PE) router and customer edge (CE) router, use the **domain-tag** command in router configuration mode. To reinstate the default tag value, use the **no** form of this command.

domain-tag *tag-value*

no domain-tag *tag-value*

Syntax Description

<i>tag-value</i>	Tag value. A 32-bit value entered in decimal format. The default value is calculated based on the Border Gateway Protocol (BGP) autonomous system (AS) number of the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) backbone. The four highest bits are set to 1101 according to RFC 1745. The lowest 16 bits map the BGP AS number of the MPLS VPN backbone. If a user specifies the <i>tag-value</i> , the value does not have to follow any particular format.
------------------	---

Defaults

The default value is calculated based on the BGP autonomous system number of the MPLS VPN backbone. The four highest bits are set to 1101 according to RFC 1745. The lowest 16 bits map the BGP autonomous system number of the MPLS VPN backbone.

Command Modes

Router configuration

Command History

Release	Modification
12.1(7)	The command was introduced.
12.1(7)E	The command was integrated into Cisco IOS Release 12.1(7)E.
12.1(7)EC	The command was integrated into Cisco IOS Release 12.1(7)EC.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(2)B	The command was integrated into Cisco IOS Release 12.2(4)B.
12.2(14)S	The command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

When OSPF is used between a PE router and a CE router, BGP routes that come from the MPLS backbone are redistributed to OSPF. These redistributed routes can be announced in Type-3, Type-5, or Type-7 LSAs. If the redistribution of the BGP routes results in Type-5 or Type-7 LSAs, the External Route Tag will be set to the value of the tag. If another PE router receives a Type-5 or Type-7 LSA with an External Route Tag equal to the set tag value, it will ignore the LSA, therefore preventing the redistributed routes that originated from the MPLS backbone from returning via some other location on the MPLS backbone.

Examples

The following example configures the tag value 777:

```
Router(config)# router ospf 10 vrf grc
Router(config-router)# domain-tag 777
```

The **show ip ospf database** command is entered to verify that the tag value 777 has been applied to the External Route Tag:

```
Router# show ospf database external 192.168.50.1

          OSPF Router with ID (192.168.239.66) (Process ID 10)

          Type-5 AS External Link States

LS age: 18
Options: (No TOS-capability, DC)
S Type: AS External Link
Link State ID: 192.168.238.1 (External Network Number )
Advertising Router: 192.168.239.66
LS Seq Number: 80000002
Checksum: 0xDAB0
Length: 36
Network Mask: /32
  Metric Type: 2 (Larger than any link state path)
  TOS: 0
  Metric: 1
  Forward Address: 0.0.0.0
  External Route Tag: 777
.
.
.

          OSPF Router with ID (198.168.237.56) (Process ID 1)
```

Related Commands

Command	Description
show ospf database	Displays lists of information related to the OSPF database for a specific router.

eigrp log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the **eigrp log-neighbor-changes** command in router configuration mode. To disable the logging of changes in EIGRP neighbor adjacencies, use the **no** form of this command.

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

Syntax Description This command has no arguments or keywords.

Defaults Adjacency changes are logged.

Command Modes Router configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines This command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems. Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the **no** form of this command.

Examples The following configuration disables logging of neighbor changes for EIGRP process 209:

```
router eigrp 209
 no eigrp log-neighbor-changes
```

The following configuration enables logging of neighbor changes for EIGRP process 209:

```
router eigrp 209
 eigrp log-neighbor-changes
```

eigrp log-neighbor-warnings

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **eigrp log-neighbor-warnings** command in router configuration mode. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

Syntax Description	<i>seconds</i>	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range of seconds is from 1 to 65535.
---------------------------	----------------	--

Defaults Neighbor warning messages are logged.

Command Modes Router configuration

Command History	Release	Modification
	12.0(5)	This command was introduced.

Usage Guidelines When neighbor warning messages occur, they are logged by default. With this command, you can disable and enable neighbor warning messages, and configure the interval between repeated neighbor warning messages.

Examples The following command will log neighbor warning messages for EIGRP process 209 and repeat the warning messages in 5-minute (300 seconds) intervals:

```
router eigrp 209
  eigrp log-neighbor-warnings 300
```

eigrp router-id

To set the router ID used by Enhanced Interior Gateway Routing Protocol (EIGRP) when communicating with its neighbors, use the **eigrp router-id** command in router configuration mode. To remove the configured router ID, use the **no** form of this command.

eigrp router-id *ip-address*

no eigrp router-id *ip-address*

Syntax Description

<i>ip-address</i>	Router ID in dotted decimal notation.
-------------------	---------------------------------------

Defaults

EIGRP automatically selects an IP address to use as the router ID when an EIGRP process is started. The highest local IP address is selected and loopback interfaces are preferred. The router ID is not changed unless the EIGRP process is removed with the **no router eigrp** command or if the router ID is manually configured with the **eigrp router-id** command.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

The router ID is used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. The router ID can be configured with any IP address with two exceptions; 0.0.0.0 and 255.255.255.255 are not legal values and cannot be entered. A unique value should be configured for each router.

Examples

The following command will set a fixed router ID:

```
router eigrp 209
 eigrp router-id 172.16.1.3
```

eigrp stub

To configure a router as a stub using Enhanced Interior Gateway Routing Protocol (EIGRP), use the **eigrp stub** command in router configuration mode. To disable the EIGRP stub routing feature, use the **no** form of this command.

eigrp stub [**receive-only** | **connected** | **static** | **summary** | **redistributed**]

no eigrp stub [**receive-only** | **connected** | **static** | **summary** | **redistributed**]

Syntax Description

receive-only	(Optional) Sets the router as a receive-only neighbor.
connected	(Optional) Advertises connected routes.
static	(Optional) Advertises static routes.
summary	(Optional) Advertises summary routes.
redistributed	(Optional) Advertises redistributed routes from other protocols and autonomous systems.

Defaults

Stub routing is not enabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S.
12.2	Keyword redistributed was added.

Usage Guidelines

Use the **eigrp stub** command to configure a router as a stub where the router directs all IP traffic to a distribution router.

The **eigrp stub** command can be modified with several options, and these options can be used in any combination except for the **receive-only** keyword. The **receive-only** keyword will restrict the router from sharing any of its routes with any other router in that EIGRP autonomous system, and the **receive-only** keyword will not permit any other option to be specified because it prevents any type of route from being sent. The four other optional keywords (**connected**, **static**, **summary**, and **redistributed**) can be used in any combination but cannot be used with the **receive-only** keyword.

If any of these four keywords is used with the **eigrp stub** command, only the route types specified by the particular keyword(s) will be sent. Route types specified by the non-used keyword(s) will not be sent.

The **connected** keyword permits the EIGRP Stub Routing feature to send connected routes. If the connected routes are not covered by a network statement, it may be necessary to redistribute connected routes with the **redistribute connected** command under the EIGRP process. This option is enabled by default.

The **static** keyword permits the EIGRP Stub Routing feature to send static routes. Without the configuration of this option, EIGRP will not send any static routes, including internal static routes that normally would be automatically redistributed. It will still be necessary to redistribute static routes with the **redistribute static** command.

The **summary** keyword permits the EIGRP Stub Routing feature to send summary routes. Summary routes can be created manually with the **summary address** command or automatically at a major network border router with the **auto-summary** command enabled. This option is enabled by default.

The **redistributed** keyword permits the EIGRP Stub Routing feature to send other routing protocols and autonomous systems. Without the configuration of this option, EIGRP will not advertise redistributed routes.

**Note**

Multi-access interfaces, such as ATM, Ethernet, Frame Relay, ISDN PRI, and X.25, are supported by the EIGRP Stub Routing feature only when all routers on that interface, except the hub, are configured as stub routers.

Examples

In the following example, the **eigrp stub** command is used to configure the router as a stub that advertises connected and summary routes:

```
router eigrp 1
network 10.0.0.0
eigrp stub
```

In the following example, the **eigrp stub** command is issued with the **connected** and **static** keywords to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
router eigrp 1
network 10.0.0.0
eigrp stub connected static
```

In the following example, the **eigrp stub** command is issued with the **receive-only** keyword to configure the router as a receive-only neighbor (connected, summary, and static routes will not be sent):

```
router eigrp 1
network 10.0.0.0 eigrp
eigrp stub receive-only
```

In the following example, the **eigrp stub** command is issued with the **redistributed** keyword to configure the router to advertise other protocols and autonomous systems:

```
router eigrp 1
network 10.0.0.0 eigrp
eigrp stub redistributed
```

exit-address-family

To exit from address family configuration mode, use the **exit-address-family** command in address family configuration mode.

exit-address-family

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Address family configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.0(22)S	EIGRP support was added.
	12.2(15)T	EIGRP support was added.

Usage Guidelines This command can be abbreviated to **exit**.

Examples The following example shows how to exit address family configuration mode:

```
(config-router-af)# exit-address-family
```

Related Commands	Command	Description
	address-family ipv4 (EIGRP)	Enters address family configuration mode for EIGRP.

export map

To configure an export route map for a VRF, use the **export map** command in VRF configuration mode.

export map *route-map*

Syntax Description	<i>route-map</i>	Specifies the route map to be used as an export route map for the VRF.
---------------------------	------------------	--

Defaults This command has no default behavior.

Command Modes VRF configuration mode

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use an export route map when an application requires finer control over the routes that are exported out of a VRF than the control that is provided by import and export extended communities configured for the importing and exporting VRFs.

The **export map** command associates a route map with the specified VRF. You can use a route map to filter routes that are eligible for export out of a VRF, based on the route target extended community attributes of the route.

Only one export route map per VRF is supported.

Examples The following example shows how to configure an export route map for a VRF:

```
Router(config)# ip vrf vrf_red
Router(config-vrf)# export map blue_export_map
```

Related Commands	Command	Description
	import map	Configures an import route map for a VRF.
	ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
	ip vrf	Configures a VRF routing table.
	route-target	Creates a route-target extended community for a VRF.
	show ip vrf	Displays the set of defined VRFs and associated interfaces.

flash-update-threshold

To suppress regularly scheduled flash updates, use the **flash-update-threshold** command in router configuration mode. To return to the default state, use the **no** form of this command.

flash-update-threshold *seconds*

no flash-update-threshold

Syntax Description	<i>seconds</i>	The time interval in seconds for which the suppression of flash updates can be configured. The range is from 1 to 30 seconds.
---------------------------	----------------	---

Defaults	This command is disabled by default.
-----------------	--------------------------------------

Command Modes	Router configuration
----------------------	----------------------

Command History	Release	Modification
	12.0	This command was introduced.

Usage Guidelines	This command suppresses flash updates when the arrival of a regularly scheduled update matches the number of seconds that is configured with the <i>seconds</i> argument. The range of seconds that can be configured is from 0 to 30 seconds. If the number of seconds matches the number of seconds or is less than the number seconds that is configured with the <i>seconds</i> argument, the flash update is suppressed. If the number of seconds until the flash update arrives exceeds the number of seconds that is configured with the <i>seconds</i> argument, the flash update is not suppressed. The regular scheduled interval for flash updates and the configuration of the suppression of flash updates can be verified with the show ip protocol command.
-------------------------	---

Examples	The following example configures a router to suppress a regularly scheduled flash update if the update is due in 10 seconds or less:
-----------------	--

```
router rip
 flash-update-threshold 10
```

Related Commands	Command	Description
	show ip protocols	Displays the parameters and current state of the active routing protocol process.

hello padding

To reenable IS-IS hello padding at the router level, enter the **hello padding** command in router configuration mode. To disable IS-IS hello padding, use the **no** form of this command.

hello padding

no hello padding

Syntax Description This command has no arguments or keywords.

Defaults IS-IS hello padding is enabled.

Command Modes Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)S	This command was integrated into Cisco IOS Release 12.0(5)S.

Usage Guidelines

Intermediate System-to-Intermediate System (IS-IS) hellos are padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

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

To disable hello padding for all interfaces on a router for the IS-IS routing process, enter the **no hello padding** command in router configuration mode. To selectively disable hello padding for a specific interface, enter the **no isis hello padding** command in interface configuration mode.

Examples

In the following example the **no hello padding** command is used to turn off hello padding at the router level:

```
Router(config)# router isis
Router(config-router)# no hello padding
Router(config-router)# end
```

The **show clns interfaces** command is entered to show that hello padding has been turned off at router level:

```
Router# show clns interface e0/0

Ethernet0/0 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
```

```

ERPDUs enabled, min. interval 10 msec.
CLNS fast switching enabled
CLNS SSE switching disabled
DEC compatibility mode OFF for this interface
Next ESH/ISH in 4 seconds
Routing Protocol: IS-IS
  Circuit Type: level-1-2
  Interface number 0x0, local circuit ID 0x1
  Level-1 Metric: 10, Priority: 64, Circuit ID: Router_B.01
  Level-1 IPv6 Metric: 10
  Number of active level-1 adjacencies: 1
  Level-2 Metric: 10, Priority: 64, Circuit ID: Router_B.01
  Level-2 IPv6 Metric: 10
  Number of active level-2 adjacencies: 1
  Next IS-IS LAN Level-1 Hello in 6 seconds
! No hello padding
  Next IS-IS LAN Level-2 Hello in 2 seconds
! No hello padding

```

When the **debug isis adj packets** command is entered, the output will show the IS-IS hello protocol data unit (PDU) length when a hello packet has been sent to or received from an IS-IS adjacency. In the following example the IS-IS hello PDU length is 1497:

```

Router# debug isis adj packets e0/0

IS-IS Adjacency related packets debugging is on
Router_A#
*Oct 11 18:04:17.455: ISIS-Adj: Sending L1 LAN IIH on Ethernet0/0, length 55
*Oct 11 18:04:19.075: ISIS-Adj: Rec L2 IIH from aabb.cc00.6600 (Ethernet0/0), cir type
L1L2, cir id 0000.0000.000B.01, length 1497

```

Related Commands

Command	Description
isis hello padding	Reenables IS-IS hello padding at the interface level.
debug isis adj packets	Displays information on all adjacency-related activity such as hello packets sent and received and IS-IS adjacencies going up and down.
show clns interface	Lists the CLNS-specific information about each interface.

hostname dynamic

To enable IS-IS dynamic hostname capability on the router, use the **hostname dynamic** command in router configuration mode. To disable the dynamic hostname feature, use the **no** form of this command.

hostname dynamic

no hostname dynamic

Syntax Description This command has no arguments or keywords.

Command Default The dynamic hostname feature is enabled by default.

Command Modes Router configuration

Command History	Release	Modification
	12.0	This command was introduced.
	12.0S	This command was integrated into Cisco IOS Release 12.0(S).

Usage Guidelines In the IS-IS routing domain, the system ID is used to represent each router. The system ID is part of the network entity title (NET) that is configured for each IS-IS router. For example, a router with a configured NET of 49.0001.0023.0003.000a.00 has a system ID of 0023.0003.000a. Router-name-to-system-ID mapping is difficult for network administrators to remember during maintenance and troubleshooting on the routers. Entering the **show isis hostname** command displays the entries in the system-ID-to-router-name mapping table.

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

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



Note

Locally defined mappings are always preferred over dynamically learned mappings. If you have already configured the **clns host** command to overwrite network advertised name mappings from LSPs, the **clns host** command will take precedence over the dynamic hostname feature.

Examples

The following example changes the hostname from Router to RouterA and assigns the NET 49.0001.0000.0000.000b.00 to RouterA. The dynamic hostname feature is disabled by entering the **no dynamic hostname** command. The dynamic hostname feature is then reenabled by entering the **dynamic hostname** command.

```
Router> enable
Router# configure terminal
Router(config)# hostname RouterA
RouterA(config)# router isis CompanyA
RouterA(config-router)# net 49.0001.0000.0000.000b.00
RouterA(config-router)# hostname dynamic
RouterA(config-router)# end
```

Entering the **show isis hostname** command displays the dynamic host mapping table. The * symbol signifies that this is the hostname for the local router. The dynamic host mapping table confirms that system ID 0000.0000.000B belongs to a router with the dynamic hostname RouterA. This router is running the IS-IS process named CompanyA.

```
Router# show isis hostname

Level System ID      Dynamic Hostname      (CompanyA)
* 0000.0000.000B RouterA
```

Related Commands

Command	Description
clns host	Defines a name-to-NSAP mapping that can then be used with commands that require NSAPs.
hostname	Specifies or modifies the hostname for the network server.
net	Configures an IS-IS NET for a CLNS or IS-IS routing process.
show isis hostname	Displays the entries of the dynamic host mapping table.