



## accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the **accept-lifetime** command in key chain key configuration mode. To revert to the default value, use the **no** form of this command.

**accept-lifetime** *start-time* { **infinite** | *end-time* | **duration** *seconds* }

**no accept-lifetime** [*start-time* { **infinite** | *end-time* | **duration** *seconds* }]

### Syntax Description

<i>start-time</i>	Beginning time that the key specified by the <b>key</b> command is valid to be received. The syntax can be either of the following:  <i>hh:mm:ss</i> <i>Month</i> <i>date</i> <i>year</i> <i>hh:mm:ss</i> <i>date</i> <i>Month</i> <i>year</i>  <i>hh</i> —hours <i>mm</i> —minutes <i>ss</i> —seconds <i>Month</i> —first three letters of the month <i>date</i> —date (1-31) <i>year</i> —year (four digits)  The default start time and the earliest acceptable date is January 1, 1993.
<b>infinite</b>	Key is valid to be received from the <i>start-time</i> value on.
<i>end-time</i>	Key is valid to be received from the <i>start-time</i> value until the <i>end-time</i> value. The syntax is the same as that for the <i>start-time</i> value. The <i>end-time</i> value must be after the <i>start-time</i> value. The default end time is an infinite time period.
<b>duration</b> <i>seconds</i>	Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

### Defaults

Forever (the starting time is January 1, 1993, and ending time is infinite)

### Command Modes

Key chain key configuration

**Command History**

Release	Modification
11.1	This command was introduced.

**Usage Guidelines**

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration seconds**.

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you assign a lifetime to a key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

**Examples**

The following example configures a key chain called trees. The key named chestnut will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named birch will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
interface ethernet 0
 ip rip authentication key-chain trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string birch
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

**Related Commands**

Command	Description
<a href="#">key</a>	Identifies an authentication key on a key chain.
<a href="#">key chain</a>	Enables authentication for routing protocols.
<a href="#">key-string (authentication)</a>	Specifies the authentication string for a key.
<a href="#">send-lifetime</a>	Sets the time period during which an authentication key on a key chain is valid to be sent.
<a href="#">show key chain</a>	Displays authentication key information.

# address-family ipv4 (BGP)

To enter address family configuration mode to configure a routing session using standard IP Version 4 address prefixes, use the **address-family ipv4** command in router configuration mode. To exit address family configuration mode and remove the IPv4 address family configuration from the running configuration, use the **no** form of this command.

**address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]

**no address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]

Syntax Description		
	<b>multicast</b>	(Optional) Specifies IP Version 4 multicast address prefixes.
	<b>unicast</b>	(Optional) Specifies IP Version 4 unicast address prefixes.
	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with subsequent IP Version 4 address family configuration mode commands.

## Defaults

Unicast prefix support is enabled by default when this command is entered without any optional keywords.



### Note

Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

## Command Modes

Router configuration

## Command History

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

## Usage Guidelines

The **address-family ipv4** command replaces the **match nlri** and **set nlri** commands.

The **address-family ipv4** command places the router in address family configuration mode (prompt: `(config-router-af)#`), from which you can configure routing sessions that use standard IP Version 4 address prefixes.

To leave address family configuration mode and return to router configuration mode without removing the existing configuration, enter the **exit-address-family** command.

## Examples

The following example places the router in address family configuration mode for the IP Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)#
```

### Multicast Example

The following example places the router in address family configuration mode and specifies only multicast address prefixes for the IP Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 multicast
Router(config-router-af)#
```

### Unicast Example

The following example places the router in address family configuration mode and specifies unicast address prefixes for the IP Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)#
```

### VRF Example

The following example places the router in address family configuration mode and specifies **cisco** as the name of the VRF instance to associate with subsequent IP Version 4 address family configuration mode commands:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 vrf cisco
Router(config-router-af)#
```



#### Note

Use this form of the command, which specifies a VRF, only to configure routing exchanges between provider edge (PE) and customer edge (CE) devices.

#### Related Commands

Command	Description
<a href="#">address-family ipv6</a>	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
<a href="#">address-family nsap</a>	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use CLNS prefixes.
<a href="#">address-family vpnv4</a>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
<a href="#">bgp default ipv4-unicast</a>	Enables the IPv4 unicast address family on all neighbors.
<a href="#">neighbor activate</a>	Enables the exchange of information with a BGP neighboring router.

## address-family ipv4 (EIGRP)

To enter IPv4 address family configuration mode to configure an Enhanced Interior Gateway Routing Protocol (EIGRP) Virtual Private Network (VPN), use the **address-family ipv4** command in address family configuration mode. To remove the address family from the EIGRP configuration, use the **no** form of this command.

```
address-family ipv4 [unicast] [vrf vrf-name]
```

```
no address-family ipv4 [unicast] [vrf vrf-name]
```

Syntax Description		
	<b>unicast</b>	(Optional) Specifies the unicast subaddress family.
	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name of the VRF.

**Defaults** A default VRF is automatically created when this command is entered without the **vrf** keyword.

**Command Modes** Address family configuration

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.

**Usage Guidelines** The **address-family ipv4** command is used to configure IPv4 address family sessions under EIGRP. To leave address family configuration mode without removing the address family configuration, use the **exit-address-family** command.

EIGRP VPNs can be configured only under IPv4 address family configuration mode. A virtual routing and forwarding instance (VRF) and route distinguisher must be defined before the address family session can be created.

A single EIGRP routing process can support multiple VRFs. The number of VRFs that can be configured is limited by only available system resources on the router, which is determined by the number of VRFs, running processes, and available memory. However, only a single VRF can be supported by each VPN, and redistribution between different VRFs is not supported.

MPLS VPN support between PE and CE routers is configured only on PE routers that provide VPN services over the service provider backbone. The customer site does not require any changes to equipment or configurations to support the EIGRP VPN. A metric must be configured for routes to be advertised to the CE router. The metric can be configured using the **redistribute (IP)** command or configured with the **default-metric (EIGRP)** command.

**Examples**

The following example, starting in Global configuration mode, configures an IPv4 address family session for the VRF named RED:

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 1:1
Router(config-vrf)# exit
Router(config)# router eigrp 1
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# autonomous-system 101
Router(config-router-af)# network 172.16.0.0
Router(config-router-af)# default-metric 10000 100 255 1 1500
Router(config-router-af)# exit-address-family
```

**Related Commands**

Command	Description
<a href="#">default-metric (EIGRP)</a>	Sets metric for EIGRP.
<a href="#">exit-address-family</a>	Exits from address family configuration mode.
<a href="#">network (EIGRP)</a>	Specifies a list of networks for the EIGRP routing process.
<a href="#">redistribute (IP)</a>	Redistributes routes from one routing domain into another routing domain.

# address-family nsap

To enter address family configuration mode to configure Connectionless Network Service (CLNS)-specific parameters for Border Gateway Protocol (BGP) routing sessions, use the **address-family nsap** command in router configuration mode. To exit address family configuration mode and remove the CLNS address family configuration from the running configuration, use the **no** form of this command.

**address-family nsap [unicast]**

**no address-family nsap [unicast]**

<b>Syntax Description</b>	<b>unicast</b> (Optional) Specifies network service access point (NSAP) unicast address prefixes.
---------------------------	---

**Defaults** Unicast prefix support is enabled by default when this command is entered without any optional keywords.



**Note**

Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

**Command Modes** Router configuration

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

**Usage Guidelines** The **address-family nsap** command enters address family configuration mode (prompt: `config-router-af`)#, from which you can configure routing sessions that use standard NSAP address prefixes; you must enter NSAP address family configuration mode to configure BGP for CLNS prefixes. To leave address family configuration mode and return to router configuration mode without removing the existing configuration, enter the **exit-address-family** command.

**Examples** The following example enters NSAP address family configuration mode under BGP:

```
Router(config)# router bgp 50000
Router(config-router)# address-family nsap
Router(config-router-af)#
```

Related Commands	Command	Description
	<a href="#">address-family ipv4 (BGP)</a>	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
	<a href="#">address-family ipv6</a>	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
	<a href="#">address-family vpnv4</a>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
	<a href="#">bgp default ipv4-unicast</a>	Enables the IPv4 unicast address family on all neighbors.
	<a href="#">neighbor activate</a>	Enables the exchange of information with a BGP neighboring router.

## address-family vpnv4

To enter address family configuration mode to configure a routing session using Virtual Private Network (VPN) Version 4 address prefixes, use the **address-family vpnv4** command in router configuration mode. To exit address family configuration mode and remove the VPNv4 address family configuration from the running configuration, use the **no** form of this command.

**address-family vpnv4 [unicast]**

**no address-family vpnv4 [unicast]**

<b>Syntax Description</b>	<b>unicast</b> (Optional) Specifies VPN Version 4 unicast address prefixes.
---------------------------	---

<b>Defaults</b>	Unicast prefix support is enabled by default when this command is entered without any optional keywords.
-----------------	--



**Note**

Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

<b>Command Modes</b>	Router configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)T	This command was introduced.

<b>Usage Guidelines</b>	<p>The <b>address-family vpnv4</b> command replaces the <b>match nlri</b> and <b>set nlri</b> commands.</p> <p>The <b>address-family vpnv4</b> command places the router in address family configuration mode (prompt: <code>config-router-af</code>), from which you can configure routing sessions that use VPN Version 4 address prefixes.</p> <p>To leave address family configuration mode and return to router configuration mode without removing the existing configuration, enter the <b>exit-address-family</b> command.</p>
-------------------------	--

<b>Examples</b>	The following example places the router in address family configuration mode for the VPN Version 4 address family:
-----------------	--

```
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4
Router(config-router-af)#
```

The following example places the router in address family configuration mode for the unicast VPN Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4 unicast
Router(config-router-af)#
```

Related Commands	Command	Description
	<a href="#">address-family ipv4 (BGP)</a>	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
	<a href="#">address-family ipv6</a>	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
	<a href="#">address-family nsap</a>	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use CLNS prefixes.
	<a href="#">neighbor activate</a>	Enables the exchange of information with a BGP neighboring router.

# advertise-passive-only

To configure IS-IS to advertise only prefixes that belong to passive interfaces, use the **advertise-passive-only** command in router configuration mode. To remove the restriction, use the **no** form of this command.

**advertise-passive-only**

**no advertise-passive-only**

**Syntax Description** This command has no arguments or keywords.

**Defaults** This command has no default behavior.

**Command Modes** Router configuration

Command History	Release	Modification
	12.0(22)S	This command was introduced.
	12.3(2)T	This command was integrated.

**Usage Guidelines** This command is an IS-IS mechanism to exclude IP prefixes of connected networks from LSP advertisements, thereby reducing IS-IS convergence time.

Configuring this command per IS-IS instance is a scalable solution to reduce IS-IS convergence time because fewer prefixes will be advertised in the router nonpseudonode LSP.

This command relies on the fact that when enabling IS-IS on a loopback interface, you usually configure the loopback as passive (to prevent sending unnecessary hello packets out through it because there is no chance of finding a neighbor behind it). Thus, if you want to advertise only the loopback and if it has already been configured as passive, configuring the **advertise-passive-only** command per IS-IS instance would prevent the overpopulation of the routing tables.

An alternative to this command is the **no isis advertise-prefix** command. The **no isis advertise-prefix** command is a small-scale solution because it is configured per interface.

**Examples** The following example uses the **advertise-passive-only** command, which affects the IS-IS instance, and thereby prevents advertising the IP network of Ethernet interface 0. Only the IP address of loopback interface 0 is advertised.

```
!
interface loopback 0
 ip address 192.168.10.1 255.255.255.255
 no ip directed-broadcast
!
!
interface Ethernet0
 ip address 192.168.20.1 255.255.255.0
```

```

no ip directed-broadcast
ip router isis
!.
!.
!.
!
router isis
  passive-interface Loopback0
  net 47.0004.004d.0001.0001.0c11.1111.00
  advertise-passive-only
  log-adjacency-changes
!
```

**Related Commands**

Command	Description
<a href="#">isis advertise-prefix</a>	Allows the advertising of IP prefixes of connected networks in LSP advertisements per IS-IS interface.
<b>passive-interface</b>	Suppresses the sending of routing updates through the specified interface.

# aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) or multiprotocol BGP (mBGP) database, use the **aggregate-address** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

```
aggregate-address address mask [as-set] [summary-only] [suppress-map map-name]
[advertise-map map-name] [attribute-map map-name]
```

```
no aggregate-address address mask [as-set] [summary-only] [suppress-map map-name]
[advertise-map map-name] [attribute-map map-name]
```

Syntax Description		
<i>address</i>		Aggregate address.
<i>mask</i>		Aggregate mask.
<b>as-set</b>		(Optional) Generates autonomous system set path information.
<b>summary-only</b>		(Optional) Filters all more-specific routes from updates.
<b>suppress-map</b> <i>map-name</i>		(Optional) Name of the route map used to select the routes to be suppressed.
<b>advertise-map</b> <i>map-name</i>		(Optional) Name of the route map used to select the routes to create AS_SET origin communities.
<b>attribute-map</b> <i>map-name</i>		(Optional) Name of the route map used to set the attribute of the aggregate route.

**Defaults** The atomic aggregate attribute is set automatically when an aggregate route is created with this command unless the **as-set** keyword is specified.

**Command Modes** Address family configuration  
Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	11.1(20)CC	The <b>nlri unicast</b> , <b>nlri multicast</b> , and <b>nlri unicast multicast</b> keywords were added.
	12.0(2)S	The <b>nlri unicast</b> , <b>nlri multicast</b> , and <b>nlri unicast multicast</b> keywords were added.
	12.0(7)T	The <b>nlri unicast</b> , <b>nlri multicast</b> , and <b>nlri unicast multicast</b> keywords were removed.
		Address family configuration mode support was added.

## Usage Guidelines

You can implement aggregate routing in BGP and mBGP either by redistributing an aggregate route into BGP or mBGP, or by using the conditional aggregate routing feature.

Using the **aggregate-address** command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix which matches the aggregate must exist in the RIB.) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the **as-set** keyword.)

Using the **as-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS\_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the **aggregate-address** command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the **summary-only** keyword not only creates the aggregate route (for example, 192.\*.\*.\*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the **suppress-map** keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the **match** clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Using the **advertise-map** keyword selects specific routes that will be used to build different components of the aggregate route, such as AS\_SET or community. This form of the **aggregate-address** command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS\_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS\_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists **match** clauses are supported.

Using the **attribute-map** keyword allows attributes of the aggregate route to be changed. This form of the **aggregate-address** command is useful when one of the routes forming the AS\_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

## Examples

### AS-Set Example

In the following example, an aggregate BGP address is created in router configuration mode. The path advertised for this route will be an AS\_SET consisting of all elements contained in all paths that are being summarized.

```
Router(config)# router bgp 50000
Router(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set
```

### Summary-Only Example

In the following example, an aggregate BGP address is created in address family configuration mode and applied to the multicast database (SAFI) under the IP Version 4 address family. Because the **summary-only** keyword is configured, more-specific routes are filtered from updates.

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 multicast
Router(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

### Conditional Aggregation Example

In the following example, a route map called MAP-ONE is created to match on an as-path access list. The path advertised for this route will be an AS\_SET consisting of elements contained in paths that are matched in the route map.

```
Router(config)# ip as-path access-list 1 deny ^1234_
Router(config)# ip as-path access-list 1 permit .*
Router(config)# !
Router(config)# route-map MAP-ONE
Router(config-route-map)# match ip as-path 1
Router(config-route-map)# exit
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 as-set advertise-map
MAP-ONE
Router(config-router-af)# end
```

### Related Commands

Command	Description
<a href="#">address-family ipv4 (BGP)</a>	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.
<a href="#">ip as-path access-list</a>	Defines a BGP autonomous system path access list.
<a href="#">match ip address</a>	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
<a href="#">neighbor distribute-list</a>	Distribute BGP neighbor information in an access list.
<a href="#">route-map (IP)</a>	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

# area authentication

To enable authentication for an OSPF area, use the **area authentication** command in router configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the **no** form of this command.

**area** *area-id* **authentication** [**message-digest**]

**no area** *area-id* **authentication** [**message-digest**]

## Syntax Description

<i>area-id</i>	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
<b>message-digest</b>	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the <i>area-id</i> argument.

## Defaults

Type 0 authentication (no authentication)

## Command Modes

Router configuration

## Command History

Release	Modification
10.0	This command was introduced.
11.0	The <b>message-digest</b> keyword was added.

## Usage Guidelines

Specifying authentication for an area sets the authentication to Type 1 (simple password) as specified in RFC 1247. If this command is not included in the configuration file, authentication of Type 0 (no authentication) is assumed.

The authentication type must be the same for all routers and access servers in an area. The authentication password for all OSPF routers on a network must be the same if they are to communicate with each other via OSPF. Use the **ip ospf authentication-key** interface command to specify this password.

If you enable MD5 authentication with the **message-digest** keyword, you must configure a password with the **ip ospf message-digest-key** interface command.

To remove the authentication specification for an area, use the **no** form of this command with the **authentication** keyword.



### Note

To remove the specified area from the software configuration, use the **no area area-id** command (with no other keywords). That is, the **no area area-id** command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

## Examples

The following example mandates authentication for areas 0 and 10.0.0.0 of OSPF routing process 201. Authentication keys are also provided.

```

interface ethernet 0
 ip address 192.168.251.201 255.255.255.0
 ip ospf authentication-key adcdefgh
!
interface ethernet 1
 ip address 10.56.0.201 255.255.0.0
 ip ospf authentication-key ijklmnop
!
router ospf 201
 network 10.0.0.0 0.255.255.255 area 10.0.0.0
 network 192.168.0.0 0.0.255.255 area 0
 area 10.0.0.0 authentication
 area 0 authentication

```

### Related Commands

Command	Description
<a href="#">area default-cost</a>	Specifies a cost for the default summary route sent into a stub area.
<a href="#">area stub</a>	Defines an area as a stub area.
<a href="#">ip ospf authentication-key</a>	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
<a href="#">ip ospf message-digest-key</a>	Enables OSPF MD5 authentication.

# area default-cost

To specify a cost for the default summary route sent into a stub or not so stubby area (NSSA), use the **area default-cost** command in router configuration mode. To remove the assigned default route cost, use the **no** form of this command.

**area** *area-id* **default-cost** *cost*

**no area** *area-id* **default-cost** *cost*

## Syntax Description

<i>area-id</i>	Identifier for the stub or NSSA. The identifier can be specified as either a decimal value or as an IP address.
<i>cost</i>	Cost for the default summary route used for a stub or NSSA. The acceptable value is a 24-bit number.

## Defaults

*cost*: 1

## Command Modes

Router configuration

## Command History

Release	Modification
10.0	This command was introduced.

## Usage Guidelines

The command is used only on an Area Border Router (ABR) attached to a stub or NSSA.

There are two stub area router configuration commands: the **stub** and **default-cost** options of the **area** command. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **stub** option of the **area** command. Use the **default-cost** option only on an ABR attached to the stub area. The **default-cost** option provides the metric for the summary default route generated by the ABR into the stub area.



### Note

To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

## Examples

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
interface ethernet 0
 ip address 10.56.0.201 255.255.0.0
!
router ospf 201
 network 10.0.0.0 0.255.255.255 area 10.0.0.0
 area 10.0.0.0 stub
 area 10.0.0.0 default-cost 20
```

Related Commands	Command	Description
	<a href="#">area authentication</a>	Enables authentication for an OSPF area.
	<a href="#">area stub</a>	Defines an area as a stub area.

# area filter-list

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR), use the **area filter-list** command in router configuration mode. To change or cancel the filter, use the **no** form of this command.

```
area {area-id} filter-list prefix {prefix-list-name in | out}
```

```
no area {area-id} filter-list prefix {prefix-list-name in | out}
```

## Syntax Description

<i>area-id</i>	Identifier of the area for which filtering is configured. The identifier can be specified as either a decimal value or an IP address.
<i>prefix</i>	Indicates that a prefix list is used.
<i>prefix-list-name</i>	Name of a prefix list.
<b>in</b>	Prefix list applied to prefixes advertised to the specified area from other areas.
<b>out</b>	Prefix list applied to prefixes advertised out of the specified area to other areas.

## Defaults

This command has no default behavior.

## Command Modes

Router configuration

## Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

## Usage Guidelines

With this feature enabled in the “in” direction, all type 3 LSAs originated by the ABR to this area, based on information from all other areas, are filtered by the prefix list. Type 3 LSAs that were originated as a result of the **area range** command in another area are treated like any other type 3 LSA that was originated individually. Any prefix that does not match an entry in the prefix list is implicitly denied.

With this feature enabled in the “out” direction, all type 3 LSAs advertised by the ABR, based on information from this area to all other areas, are filtered by the prefix list. If the **area range** command has been configured for this area, type 3 LSAs that correspond to the area range are sent to all other areas, only if at least one prefix in the area range matches an entry in the prefix list.

If all specific prefixes are denied by the prefix list, type 3 LSAs that correspond to the **area range** command will not be sent to any other area. Prefixes that are not permitted by the prefix list are implicitly denied.

## Examples

The following example filters prefixes that are sent from all other areas to area 1:

```
area 1 filter-list prefix AREA_1 in
```

Related Commands	Command	Description
	<a href="#">area range</a>	Consolidates and summarizes routes at an area boundary.

## area nssa

To configure an area as a not-so-stubby area (NSSA), use the **area nssa** command in router configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command.

```
area area-id nssa [no-redistribution] [default-information-originate [metric] [metric-type]]
[no-summary]
```

```
no area area-id nssa [no-redistribution] [default-information-originate [metric] [metric-type]]
[no-summary]
```

### Syntax Description

<i>area-id</i>	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
<b>no-redistribution</b>	(Optional) Used when the router is an NSSA Area Border Router (ABR) and you want the <b>redistribute</b> command to import routes only into the normal areas, but not into the NSSA area.
<b>default-information-originate</b>	(Optional) Used to generate a Type 7 default into the NSSA area. This keyword takes effect only on NSSA ABR or NSSA Autonomous System Boundary Router (ASBR).
<b>metric</b>	(Optional) OSPF default metric.
<b>metric-type</b>	(Optional) OSPF metric type for default routes.
<b>no-summary</b>	(Optional) Allows an area to be a not-so-stubby area but not have summary routes injected into it.

### Defaults

No NSSA area is defined.

### Command Modes

Router configuration

### Command History

Release	Modification
10.0	This command was introduced.

### Usage Guidelines

To remove the specified area from the software configuration, use the **no area area-id** command (with no other keywords). That is, the **no area area-id** command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

### Examples

The following example makes area 1 an NSSA area:

```
router ospf 1
 redistribute rip subnets
 network 172.19.92.0 0.0.0.255 area 1
 area 1 nssa
```

# area nssa translate

To configure an area as a not-so-stubby area (NSSA) and configure the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature, use the **area nssa translate** command in router configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command.

```
area area-id nssa translate type7 suppress-fa
```

```
no area area-id nssa translate type7 suppress-fa
```

Syntax Description		
	<i>area-id</i>	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
	<b>translate</b>	Translates one type of LSA to another type of LSA. This keyword takes effect only on an NSSA ABR or NSSA Autonomous System Boundary Router (ASBR).
	<b>type7</b>	Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.
	<b>suppress-fa</b>	Suppresses the forwarding address of the Type-7 LSAs from being placed in the Type-5 LSAs. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.

**Defaults** No translation occurs.

**Command Modes** Router configuration

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

**Usage Guidelines** To configure the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature, configure the **translate type7 suppress-fa** keywords. Consider the following caution.



**Caution**

Configuring the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes the router to be noncompliant with RFC 1587. Also, suboptimal routing might result because there might be better paths to reach the destination's forwarding address. This feature should not be configured without careful consideration and not until the network topology is understood.

If the **translate** keyword is used in addition to the **no-redistribution** or **default-information originate** keywords, two separate lines for the **area nssa** command appear in the configuration file for ease of readability. For example, if **area 6 nssa no-redistribution translate type7 suppress-fa** is configured, the following lines would appear in the configuration file:

```
router ospf 1
 area 6 nssa no-redistribution
 area 6 nssa translate type7 suppress-fa
```

To remove the specified area from the software configuration, use the **no area *area-id*** command (with no other keywords). That is, the **no area *area-id*** command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

---

### Examples

The following example causes OSPF to translate Type-7 LSAs from area 1 to Type-5 LSAs, but not place the Type-7 forwarding address into the Type-5 LSAs. OSPF places 0.0.0.0 as the forwarding address in the Type-5 LSAs.

```
router ospf 2
 network 172.19.92.0 0.0.0.255 area 1
 area 1 nssa translate type7 suppress-fa
```

## area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no** form of this command.

```
area area-id range ip-address ip-address-mask [advertise | not-advertise] [cost cost]
```

```
no area area-id range ip-address ip-address-mask [advertise | not-advertise] [cost cost]
```

Syntax Description		
<i>area-id</i>	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix.	
<i>ip-address</i>	IP address.	
<i>ip-address-mask</i>	IP address mask.	
<b>advertise</b>	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).	
<b>not-advertise</b>	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.	
<b>cost</b> <i>cost</i>	(Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215.	

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

**Command Modes** Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(24)S	The <b>cost</b> keyword and <i>cost</i> argument were added.
	12.2(15)T	The <b>cost</b> keyword and <i>cost</i> argument were added.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines** The **area range** command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*.

Multiple **area** router configuration commands specifying the **range** option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

**Note**

To remove the specified area from the software configuration, use the **no area *area-id*** command (with no other keywords). That is, the **no area *area-id*** command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

**Examples**

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
interface ethernet 0
 ip address 192.168.110.201 255.255.255.0
!
interface ethernet 1
 ip address 192.168.120.201 255.255.255.0
!
router ospf 201
 network 192.168.110.0 0.0.0.255 area 0
 area 10.0.0.0 range 10.0.0.0 255.0.0.0
 area 0 range 192.168.110.0 255.255.0.0
```

**Related Commands**

Command	Description
<b>area range (IPv6)</b>	Consolidates and summarizes routes at an area boundary in an IPv6 network.

## area sham-link cost

To configure a sham-link interface on a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) backbone, use the **area sham-link cost** command in global configuration mode. To remove the sham-link, use the **no** form of this command.

**area** *area-id* **sham-link** *source-address destination-address cost number*

**no area** *area-id* **sham-link** *source-address destination-address cost number*

### Syntax Description

<i>area-id</i>	ID number of the Open Shortest Path First (OSPF) area assigned to the sham-link. Valid values: numeric value or valid IP address. There is no default.
<i>source-address</i>	IP address of the source PE router in the format: <i>ip-address [mask]</i> .
<i>destination-address</i>	IP address of the destination PE route in the format: <i>ip-address [mask]</i> .
<i>number</i>	OSPF cost to send IP packets over the sham-link interface. The range of this value is from 1 to 65535.

### Defaults

No default behavior or values.

### Command Modes

Global configuration

### Command History

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

### Usage Guidelines

In the MPLS VPN environment, several VPN client sites can be connected in the same OSPF area. If these sites are connected over a backdoor link in addition to the VPN backbone, all traffic passes over the backdoor link instead of over the VPN backbone. OSPF always selects intra-area routes over interarea (external) routes.

To correct this default OSPF behavior in an MPLS VPN, use the **area sham-link cost** command to configure a sham-link between two PEs to connect the sites through the MPLS VPN backbone. A sham-link represents an intra-area (unnumbered point-to-point) connection between PEs. All other routers in the area use the sham-link to calculate intra-area shortest path first (SPF) routes to the remote site.

Configure the source and destination addresses of the sham-link as a host route mask (255.255.255.255) on the PE routers that serve as the endpoints of the sham-link. The source and destination IP addresses must belong to the VRF and be advertised by Border Gateway Protocol (BGP) to remote PE routers. The sham-link endpoint addresses should not be advertised by OSPF.

### Examples

The following example shows how to configure a sham-link between two PE routers in an MPLS VPN backbone by using the **area sham-link cost** command on each router:

```
Router1(config)# interface loopback 55
Router1(config-if)# ip vrf forwarding v1
Router1(config-if)# ip address 10.0.0.1 255.255.255.255
!
Router1(config)# router ospf 2 vrf v1
Router1(config-if)# log-adjacency-changes
Router1(config-if)# area 120 sham-link 10.0.0.1 10.44.0.1 cost 1
Router1(config-if)# redistribute bgp 1 subnets
Router1(config-if)# network 10.2.0.1 255.255.255.255 area 1
Router1(config-if)# network 10.120.0.0 0.255.255.255 area 120
Router1(config-if)# network 10.140.0.0 0.255.255.255 area 120
!
Router2(config)# interface loopback 44
Router2(config-if)# ip vrf forwarding v1
Router2(config-if)# ip address 172.16.0.1 255.255.255.255
!
Router2(config)# router ospf 2 vrf v1
Router2(config-if)# log-adjacency-changes
Router2(config-if)# area 120 sham-link 10.44.0.1 10.0.0.1 cost 1
Router2(config-if)# redistribute bgp 1 subnets
Router2(config-if)# network 10.2.0.1 255.255.255.255 area 1
Router2(config-if)# network 10.120.0.0 0.255.255.255 area 120
Router2(config-if)# network 10.140.0.0 0.255.255.255 area 120
!
```

# area stub

To define an area as a stub area, use the **area stub** command in router configuration mode. To disable this function, use the **no** form of this command.

**area** *area-id* **stub** [**no-summary**]

**no area** *area-id* **stub** [**no-summary**]

Syntax Description	
<i>area-id</i>	Identifier for the stub area; either a decimal value or an IP address.
<b>no-summary</b>	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

**Defaults** No stub area is defined.

**Command Modes** Router configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** You must configure the **area stub** command on all routers and access servers in the stub area. Use the **area** router configuration command with the **default-cost** keyword to specify the cost of a default internal router sent into a stub area by an ABR.

There are two stub area router configuration commands: the **stub** and **default-cost** options of the **area** router configuration command. In all routers attached to the stub area, the area should be configured as a stub area using the **stub** keyword of the **area** command. Use the **default-cost** keyword only on an ABR attached to the stub area. The **default-cost** keyword provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the **no-summary** keyword on the ABR to prevent it from sending summary LSAs (LSA type 3) into the stub area.



**Note**

To remove the specified area from the software configuration, use the **no area area-id** command (with no other keywords). That is, the **no area area-id** command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

**Examples** The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
interface ethernet 0
 ip address 10.56.0.201 255.255.0.0
 !
router ospf 201
```

```
network 10.0.0.0 0.255.255.255 area 10.0.0.0
area 10.0.0.0 stub
area 10.0.0.0 default-cost 20
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">area authentication</a>	Enables authentication for an OSPF area.
<a href="#">area default-cost</a>	Specifies a cost for the default summary route sent into a stub area.

## area virtual-link

To define an OSPF virtual link, use the **area virtual-link** command in router configuration mode with the optional parameters. To remove a virtual link, use the **no** form of this command.

```
area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds]
[transmit-delay seconds] [dead-interval seconds]
```

```
no area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds]
[transmit-delay seconds] [dead-interval seconds]
```

```
no area area-id
```

Syntax Description	
<i>area-id</i>	Area ID assigned to the transit area for the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default.
<i>router-id</i>	Router ID associated with the virtual link neighbor. The router ID appears in the <b>show ip ospf</b> display. There is no default.
<b>hello-interval</b> <i>seconds</i>	(Optional) Time (in seconds) between the hello packets that the Cisco IOS software sends on an interface. Unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers attached to a common network. The default is 10 seconds.
<b>retransmit-interval</b> <i>seconds</i>	(Optional) Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. Expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. The default is 5 seconds.
<b>transmit-delay</b> <i>seconds</i>	(Optional) Estimated time (in seconds) required to send a link-state update packet on the interface. Integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. The default value is 1 second.
<b>dead-interval</b> <i>seconds</i>	(Optional) Time (in seconds) that hello packets are not seen before a neighbor declares the router down. Unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.

### Defaults

*area-id*: No area ID is predefined.  
*router-id*: No router ID is predefined.  
**hello-interval** *seconds*: 10 seconds  
**retransmit-interval** *seconds*: 5 seconds  
**transmit-delay** *seconds*: 1 second  
**dead-interval** *seconds*: 40 seconds

### Command Modes

Router configuration

**Command History**

Release	Modification
10.0	This command was introduced.
12.0(24)S	Support for IPv6 was added.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.

**Usage Guidelines**

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue.

The setting of the retransmit interval should be conservative, or needless retransmissions will result. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

To configure a virtual link in OSPF for IPv6, you must use a router ID instead of an address. In OSPF for IPv6, the virtual link takes the router ID rather than the IPv6 prefix of the remote router.



**Note**

For a virtual link to be properly configured, each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID. To see the router ID, use the **show ip ospf command** in EXEC mode.



**Note**

To remove the specified area from the software configuration, use the **no area area-id** command (with no other keywords). That is, the **no area area-id** command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

**Examples**

The following example establishes a virtual link with default values for all optional parameters:

```
ipv6 router ospf 1
 log-adjacency-changes
 area 1 virtual-link 192.168.255.1
```

The following example establishes a virtual link in OSPF for IPv6:

```
ipv6 router ospf 1
 log-adjacency-changes
 area 1 virtual-link 192.168.255.1 hello-interval 5
```

# area-password

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

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

**no area-password** [*password*]

Syntax Description	
<i>password</i>	Password you assign.
<b>authenticate snp</b>	(Optional) Causes the system to insert the password into sequence number PDUs (SNPs).
<b>validate</b>	(Optional) Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
<b>send-only</b>	(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 area password is defined, and area password authentication is disabled.

**Command Modes** Router configuration

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

**Usage Guidelines** Using the **area-password** command on all routers in an area will prevent unauthorized routers from injecting false routing information into the link-state database.

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

This password is inserted in Level 1 (station router level) PDU link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNP).

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 area authentication password and specifies that the password be inserted in SNPs and checked in SNPs that the system receives:

```
router isis
 area-password track authenticate snp validate
```

Related Commands	Command	Description
	<a href="#">domain-password</a>	Configures the IS-IS routing domain authentication password.
	<a href="#">isis password</a>	Configures the authentication password for an interface.

# authentication key-chain

To enable authentication for IS-IS, use the **authentication key-chain** command in router configuration mode. To disable such authentication, use the **no** form of this command.

**authentication key-chain** *name-of-chain* [**level-1** | **level-2**]

**no authentication key-chain** *name-of-chain* [**level-1** | **level-2**]

Syntax Description		
	<i>name-of-chain</i>	Enables authentication and specifies the group of keys that are valid.
	<b>level-1</b>	(Optional) Enables authentication for Level 1 packets only.
	<b>level-2</b>	(Optional) Enables authentication for Level 2 packets only.

**Defaults** No key chain authentication is provided for IS-IS packets at the router level.

**Command Modes** Router configuration

Command History	Release	Modification
	12.0(21)ST	This command was introduced.

**Usage Guidelines**

If no key chain is configured with the **key chain** command, no key chain authentication is performed. Key chain authentication could apply to clear text authentication or MD5 authentication. The mode is determined by the **authentication mode command**.

Only one authentication key chain is applied to IS-IS at one time. That is, if you configure a second **authentication key-chain** command, the first is overridden.

If neither the **level-1** nor **level-2** keyword is configured, the chain applies to both levels.

You can specify authentication for an individual IS-IS interface by using the **isis authentication key-chain** command.

**Examples** The following example configures IS-IS to accept and send any key belonging to the key chain named cities:

```
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode md5 level-1
 authentication key-chain cities level-1
```

Related Commands	Command	Description
	<a href="#">authentication mode</a>	Specifies the type of authentication used in IS-IS packets for the IS-IS instance.
	<a href="#">isis authentication key-chain</a>	Enables authentication for an IS-IS interface.
	<a href="#">key chain</a>	Enables authentication for routing protocols.

# authentication mode

To specify the type of authentication used in IS-IS packets for the IS-IS instance, use the **authentication mode** command in router configuration mode. To restore clear text authentication, use the **no** form of this command.

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

**no authentication mode**

Syntax Description	md5	Message Digest 5 (MD5) authentication.
	text	Clear text authentication.
	level-1	(Optional) Enables the specified authentication for Level 1 packets only.
	level-2	(Optional) Enables the specified authentication for Level 2 packets only.

**Defaults** No authentication is provided for IS-IS packets at the router level by use of this command, although clear text (plain text) authentication could be configured by other means, such as the **area-password** command or the **domain-password** command.

**Command Modes** Router configuration

Command History	Release	Modification
	12.0(21)ST	This command was introduced.

**Usage Guidelines** If neither the **level-1** nor **level-2** keyword is configured, the mode applies to both levels.

You can specify the type of authentication and the level to which it applies for a single IS-IS interface, rather than per IS-IS instance, by using the **isis authentication mode** command.

If you had clear text authentication configured by using the **area-password** or **domain-password** command, the **authentication mode** command overrides both of those commands.

If you configure the **authentication mode** command and subsequently try to configure the **area-password** or **domain-password** command, you will not be allowed to do so. If you truly want to configure clear text authentication using the **area-password** or **domain-password** command, you must use the **no authentication mode** command first.

**Examples** The following example configures for the IS-IS instance that MD5 authentication is performed on Level 1 packets:

```
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode md5 level-1
 authentication key-chain cities level-1
```

Related Commands	Command	Description
	<a href="#">area-password</a>	Configures the IS-IS area authentication password.
	<a href="#">authentication key-chain</a>	Enables authentication for IS-IS packets and specifies the set of keys that can be used on an interface.
	<a href="#">domain-password</a>	Configures the IS-IS routing domain authentication password.
	<a href="#">isis authentication mode</a>	Specifies the type of authentication used for an ISIS interface.
	<a href="#">key chain</a>	Enables authentication for routing protocols.

# authentication send-only

To specify for the IS-IS instance that authentication is performed only on IS-IS packets being sent (not received), use the **authentication send-only** command in router configuration mode. To configure for the IS-IS instance that if authentication is configured at the router level, such authentication be performed on packets being sent and received, use the **no** form of this command.

**authentication send-only [level-1 | level-2]**

**no authentication send-only**

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

**Defaults** If authentication is configured at the router level, it applies to IS-IS packets being sent and received.

**Command Modes** Router configuration

Command History	Release	Modification
	12.0(21)ST	This command was introduced.

**Usage Guidelines** Use this command before configuring the authentication mode and authentication key chain so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all of the routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then specify the **no authentication send-only** command to disable the send-only feature.

If neither the **level-1** nor **level-2** keyword is configured, the send-only feature applies to both levels.

This command could apply to clear text authentication or MD5 authentication. The mode is determined by the **authentication mode** command.

**Examples** The following example configures IS-IS Level 1 packets to use clear text authentication on packets being sent (not received):

```
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication send-only level-1
 authentication mode text level-1
 authentication key-chain cities level-1
```

Related Commands	Command	Description
	<a href="#">authentication key-chain</a>	Enables authentication for IS-IS packets and specifies the set of keys that can be used on an interface.
	<a href="#">authentication mode</a>	Specifies the type of authentication used in IS-IS packets for the IS-IS instance.
	<a href="#">key chain</a>	Enables authentication for routing protocols.

# auto-cost

To control how OSPF calculates default metrics for the interface, use the **auto-cost** command in router configuration mode. To assign cost based only on the interface type, use the **no** form of this command.

**auto-cost reference-bandwidth** *ref-bw*

**no auto-cost reference-bandwidth**

<b>Syntax Description</b>	<b>reference-bandwidth</b> <i>ref-bw</i> Rate in Mbps (bandwidth). The range is from 1 to 4294967; the default is 100.
---------------------------	--

<b>Defaults</b>	100 Mbps
-----------------	----------

<b>Command Modes</b>	Router configuration
----------------------	----------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.2</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	11.2	This command was introduced.
Release	Modification				
11.2	This command was introduced.				

**Usage Guidelines**

In Cisco IOS Release 10.3 and later releases, by default OSPF will calculate the OSPF metric for an interface according to the bandwidth of the interface. For example, a 64K link will get a metric of 1562, and a T1 link will have a metric of 64.

The OSPF metric is calculated as the *ref-bw* value divided by the *bandwidth*, with *ref-bw* equal to 10<sup>8</sup> by default, and *bandwidth* determined by the **bandwidth (interface)** command. The calculation gives FDDI a metric of 1.

If you have multiple links with high bandwidth (such as FDDI or ATM), you might want to use a larger number to differentiate the cost on those links.

The value set by the **ip ospf cost** command overrides the cost resulting from the **auto-cost** command.

**Examples**

The following example changes the cost of the FDDI link to 10, while the gigabit Ethernet link remains at a cost of 1. Thus, the link costs are differentiated.

```
router ospf 1
 auto-cost reference-bandwidth 1000
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><a href="#">ip ospf cost</a></td> <td>Explicitly specifies the cost of sending a packet on an interface.</td> </tr> </tbody> </table>	Command	Description	<a href="#">ip ospf cost</a>	Explicitly specifies the cost of sending a packet on an interface.
Command	Description				
<a href="#">ip ospf cost</a>	Explicitly specifies the cost of sending a packet on an interface.				

# auto-summary (BGP)

To configure automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in address family or router configuration mode. To disable automatic summarization and send subprefix routing information across classful network boundaries, use the **no** form of this command.

**auto-summary**

**no auto-summary**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Automatic summarization is disabled by default (the software sends subprefix routing information across classful network boundaries).

BGP automatically summarizes to classful network boundaries when this command is enabled.

**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.
	12.2(8)T	Command default behavior changed to disabled.

**Usage Guidelines** Route summarization is used to reduce the amount of routing information in the routing tables. By default, BGP does not accept subnets redistributed from an Interior Gateway Protocol (IGP). To allow Cisco IOS Software to create summary subprefixes to the classful network boundary when crossing classful network boundaries, use the **auto-summary** command. To advertise and carry subnet routes in BGP when automatic summarization is enabled, use an explicit **network** command statement to advertise the subnet.

**Examples** In the following example, automatic summarization is enabled for IPv4 address family prefixes:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)# auto-summary
```

Related Commands	Command	Description
	<a href="#">address-family ipv4 (BGP)</a>	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.
	<a href="#">address-family vpnv4</a>	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.

# auto-summary (EIGRP)

To allow automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in router configuration mode. To disable this function and send subprefix routing information across classful network boundaries, use the **no** form of this command.

**auto-summary**

**no auto-summary**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The behavior of this command is disabled by default (the software sends subprefix routing information across classful network boundaries).

**Command Modes** Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(8)T	Command default behavior changed to disabled.

**Usage Guidelines** Route summarization reduces the amount of routing information in the routing tables.

By default, Border Gateway Protocol (BGP) does not accept subnets redistributed from an Interior Gateway Protocol (IGP). To allow the software to create summary subprefixes to the classful network boundary when crossing classful network boundaries, use the **auto-summary** command.

To advertise and carry subnet routes in BGP, use an explicit **network** command because automatic summarization is disabled by default. If you have not entered a **network** command, you will not advertise network routes for networks with subnet routes unless they contain a summary route.

Enhanced Interior Gateway Routing Protocol (EIGRP) summary routes are given an administrative distance value of 5. You cannot configure this value.

Routing Information Protocol (RIP) Version 1 always uses automatic summarization. If you are using RIP Version 2, you can turn off automatic summarization by specifying the **no auto-summary** command. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is off, subnets are advertised.

**Examples** The following example enables automatic summarization for EIGRP process 109:

```
router eigrp 109
  auto-summary
```

Related Commands	Command	Description
	<a href="#">ip summary-address eigrp</a>	Configures a summary aggregate address for a specified interface.

# auto-summary (RIP)

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in router configuration mode. To disable this function and send subprefix routing information across classful network boundaries, use the **no** form of this command.

**auto-summary**

**no auto-summary**

---

## Syntax Description

This command has no arguments or keywords.

---

## Defaults

Enabled (the software summarizes subprefixes to the classful network boundary when crossing classful network boundaries).

---

## Command Modes

Router configuration

---

## Command History

Release	Modification
10.0	This command was introduced.

---

## Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables.

RIP Version 1 always uses automatic summarization. If you are using RIP Version 2, you can turn off automatic summarization by specifying the **no auto-summary** command. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is off, subnets are advertised.

---

## Examples

In the following example, network numbers are not summarized automatically:

```
router rip
version 2
no auto-summary
```