

A Commands

aaa accounting acct-stop on-aaa-failure

- Description:** Configures AAA to send an Acct-Stop message if a user fails AAA, but RADIUS grants access. The **no** version returns the parameter to the default of enable.
- Syntax:** aaa accounting acct-stop on-aaa-failure { enable | disable }
no aaa accounting acct-stop on-aaa-failure
- Mode(s):** Global Configuration

aaa accounting acct-stop on-access-deny

- Description:** Issues an Acct-Stop message if RADIUS denies access. The **no** version returns the parameter to the default of disable.
- Syntax:** aaa accounting acct-stop on-access-deny { enable | disable }
no aaa accounting acct-stop on-access-deny
- Mode(s):** Global Configuration

aaa accounting duplication

- Description:** Sends duplicate accounting records to the accounting server of a different virtual router. The **no** version disables the feature.
- Syntax:** aaa accounting duplication *routerName*
no aaa accounting duplication
- *routerName* – virtual router name
- Mode(s):** Global Configuration

aaa accounting interval

- Description:** Specifies the accounting interval. The **no** version sets the value to 0, which turns off interim accounting.
- Syntax:** aaa accounting interval *period*
no aaa accounting interval
- *period* – accounting interval in minutes in the range 10–1080, which sets the time period between accounting updates
- Mode(s):** Global Configuration

aaa accounting ppp default

- Description:** Specifies the default accounting protocol for PPP. The **no** version produces the same result as specifying the **radius** value.
- Syntax:** aaa accounting ppp default *accountor* [*accountors*]*
no aaa accounting ppp default
- *accountor* – specifies the accounting method:
 - › radius – uses RADIUS for the accounting method
 - › none – disables accounting
 - * – indicates that one or more parameters can be repeated multiple times in a list in the command line
- Mode(s):** Global Configuration

aaa authentication enable default

- Description:** Allows privilege determination to be authenticated through the authenticator(s) you specify. This authentication is applied to vty users. The **no** version removes the authentication settings.
- Syntax:** `aaa authentication enable default [authenticator] [authenticators] *`
`no aaa authentication enable default`
- *authenticator* – specifies the authentication method
 - *authenticators*
 - › *radius* – use RADIUS authentication
 - › *line* – use the line password
 - › *tacacs+* – use TACACS+ authentication
 - › *none* – use no authentication
 - › *enable* – use the enable password
 - › * – indicates that one or more parameters can be repeated multiple times in a list in the command line
- Mode(s):** Global Configuration

aaa authentication login

- Description:** Creates an authentication list and the criteria for login. This authentication is applied to vty users.
- Syntax:** `aaa authentication login authListName authenticator [authenticators]*`
`no aaa authentication login authListName`
- *authListName* – specifies an existing authentication list name (created using the **login authentication** command); a string of 1–32 characters
 - *authenticator* – specifies the authentication method
 - *authenticators*
 - › *line* – use the line password for authentication
 - › *none* – use no authentication
 - › *radius* – use RADIUS authentication
 - › *tacacs+* – use TACACS+ authentication
 - * – indicates that one or more parameters can be repeated multiple times in a list in the command line
- Mode(s):** Global Configuration

aaa authentication ppp default

- Description:** Specifies the default authentication protocol for PPP and DHCP clients. The **no** version produces the same result as specifying the **radius** value.
- Syntax:** aaa authentication ppp default *authenticator* [*authenticators*]*
no aaa authentication ppp default
- *authenticator* – authentication method:
 - › radius – uses RADIUS for authentication
 - › none – means authentication is off, allowing all users access
 - * – indicates that one or more parameters can be repeated multiple times in a list in the command line
- Mode(s):** Global Configuration

aaa delimiter

- Description:** Specifies delimiters for the domain and realm names. You can specify up to eight delimiters each for domain and realm names. The **no** version restores the default value.
- Syntax:** aaa delimiter { domainName | realmName } *delimiters*
no aaa delimiter { domainName | realmName }
- domainName – allows you to set delimiters for the domain name
 - realmName – allows you to set delimiters for the realm name
 - *delimiters* – either the domain or realm delimiter(s). You can specify up to eight characters.
 - › The default domain name delimiter is @.
 - › The default realm name delimiter is NULL (no character). In this case, realm parsing is disabled (having no delimiter disables realm parsing).
- Mode(s):** Global Configuration


aaa dns

- Description:** Specifies the IP address of the primary DNS name server. The **no** version sets the corresponding address to 0.
- Syntax:** `aaa dns { primary | secondary } ipAddress`
`no aaa dns { primary | secondary }`
- `primary` – specifies the primary DNS name server
 - `secondary` – specifies the secondary DNS name server
 - `ipAddress` – IP address of the name server
- Mode(s):** Global Configuration

aaa domain-map

- Description:** Maps a user domain name to a virtual router. When you specify only the domain name, the command sets the mode to Domain Map Configuration. The **no** version deletes the map entry.
- Syntax:** `aaa domain-map domainName [routerName [loopback interfaceNumber]]`
`no aaa domain-map domainName`
- `domainName` – a user domain name; specify the domain name `none` to assign users without domains to a specific virtual router.
 - `routerName` – a router name associated with the domain name
 - `loopback` – specifies the loopback interface
 - `interfaceNumber` – interface number in the range 0–32000
- Mode(s):** Global Configuration

aaa duplicate-address-check

- Description:** Allows you to enable or disable routing table address lookup or duplicate address check. There is no **no** version.
- Syntax:** `aaa duplicate-address-check { enable | disable }`
-  **Note:** To use this command, you must have a B-RAS license. Run the **license b-ras** command and enter your password.
- Mode(s):** Global Configuration

aaa new-model

- Description:** Specifies AAA authentication for Telnet sessions. The **no** version restores simple authentication (login and password).
- Syntax:** [no] aaa new-model
- Mode(s):** Global Configuration

aaa parse-order

- Description:** Specifies the order in which the system searches for a domain name. It either searches for realm and then domain, or it searches for domain and then realm. The **no** version returns the parse order to the default of searching for realm first.
- Syntax:** aaa parse-order { domain-first | realm-first }
no aaa parse-order
- domain-first – causes the system to search for a domain name starting with the right-most character. When the system reaches a delimiter, it uses anything to the right of the delimiter as the domain name.
 - realm-first – causes the system to search for a domain name starting with the left-most character. When the system reaches a delimiter, it uses anything to the left of the delimiter as the domain name.
- Mode(s):** Global Configuration

aaa profile

- Description:** Creates a new AAA profile to allow mapping to AAA services.
- Syntax:** aaa profile *profileName*
- *profileName* – profile name of up to 32 characters
- Mode(s):** AAA Profile Configuration

aaa subscriber limit per-port

- Description:** Sets the maximum number of active subscribers permitted on the specified port. The **no** version returns the limit to the default, 0 (zero).
- Syntax:** aaa subscriber limit per-port *interfaceValue* *limitValue*
no aaa subscriber limit per-port *interfaceValue*
- *interfaceValue* – location of the interface in the slot/port format
 - *limitValue* – maximum number of subscribers. The default is 0 (zero), which means there is no limit on the number of subscribers.
- Mode(s):** Global Configuration

aaa subscriber limit per-vr

- Description:** Sets the maximum number of active subscribers permitted on the virtual router. The **no** version returns the limit to the default, 0 (zero).
- Syntax:** aaa subscriber limit per-vr *limitValue*
no aaa subscriber limit per-vr
- *limitValue* – maximum number of subscribers. The default is 0 (zero), which means there is no limit on the number of subscribers.
- Mode(s):** Global Configuration

aaa timeout

- Description:** Sets either the default idle or session timeout for B-RAS PPP users. The **no** version deletes either the idle or session timeout.
- Syntax:** aaa timeout { idle *idleTimeout* | session *sessionTimeout* }
no aaa timeout { idle | session }
- *idleTimeout* – in seconds: 300, 7200
 - *sessionTimeout* – in seconds: 60–2678400 (that is, a minimum of 1 minute to a maximum of 31 days)
- Mode(s):** Global Configuration

aaa tunnel assignment-id-format

- Description:** Sets the format for the tunnel assignment ID.
- Syntax:** aaa tunnel assignment-id-format { assignmentId | client-server-id }
- assignmentId – configures the format to be assignmentId only
 - client-server-id – configures the format to be a combination of clientAuthId + serverAuthId + assignmentId
- Mode(s):** Global Configuration

aaa tunnel client-name

- Description:** Specifies the default tunnel client name. If the tunnel client name is not included in the tunnel attributes that are returned from the domain map or authentication server, the system uses the default name. The **no** version deletes the client name.
- Syntax:** aaa tunnel client-name *name*
no aaa tunnel client-name
- *name* – default tunnel client name; a string of up to 32 characters
- Mode(s):** Global Configuration

aaa tunnel ignore

- Description:** Specifies whether or not the tunnel peer's NAS-Port [5] and NAS-Port-Type [61] attributes should be used. The **no** version negates the command or restores the default of enable.
- Syntax:** aaa tunnel ignore { nas-port | nas-port-type } { enable | disable }
no aaa tunnel ignore { nas-port | nas-port-type }
- nas-port – configures the tunnel peer's supplied nas-port value
 - nas-port-type – configures the tunnel peer's supplied nas-port-type value
- Mode(s):** Global Configuration

aaa tunnel password

- Description:** Specifies the default tunnel password. If the tunnel password is not included in the tunnel attributes that are returned from the domain map or authentication server, the system uses the default password. The **no** version deletes the password.
- Syntax:** aaa tunnel password *name*
no aaa tunnel password
- *name* – default tunnel password; a string of up to 32 characters
- Mode(s):** Global Configuration

aaa wins

- Description:** Specifies the IP address of the WINS name server. The **no** version sets the corresponding address to 0.
- Syntax:** aaa wins { primary | secondary } *ipAddress*
no aaa wins { primary | secondary }
- primary – specifies the primary WINS name server
 - secondary – specifies the secondary WINS name server
 - *ipAddress* – IP address of the name server
- Mode(s):** Global Configuration

access-class in

- Description:** Restricts incoming connections between a particular virtual terminal line and the addresses in an access list. The **no** version removes access restrictions.
- Syntax:** access-class *listName* in
no access-class [*listName*] in
- *listName* – name of the access list
- Mode(s):** Line Configuration

access-list

Description: Defines a standard or extended IP access list. The extended access list enables you to specify a destination address or host, precedence, and type of service. Imposes an implicit last rule of “deny ip any any” to deny all routes that do not match previous rules in the access list. The **no** version removes the IP access list, the specified entry in an access list, or the log for a specified entry.

Syntax: Standard IP access list:

```
access-list accessListName { permit | deny } { srcIP srcWildlp | [ host ]
srcIPHost | any } [ log ]
```

```
no access-list accessListName [ { permit | deny } { srcIP srcWildlp | [ host ]
srcIPHost | any } [ log ] ]
```

Extended IP access list:

```
access-list accessListName { permit | deny } ip { srcIP srcWildlp |
host srcIPHost | any } { dstIP dstWildlp | host dstIPHost | any }
[ precedence preced ] [ tos typeOServ ] [ log ]
```

```
no access-list accessListName [ { permit | deny } ip { srcIP srcWildlp | host
srcIPHost | any } { dstIP dstWildlp | host dstIPHost | any } [ log ] ]
```

- *accessListName* – string of up to 32 alphanumeric characters
- permit – permits access if the conditions are matched
- deny – denies access if the conditions are matched
- *srcIP* – source IP address from which the packet is being sent
- *srcWildlp* – wildcard mask IP address
- *srcIPHost* – source host IP address; assumes a wildcard mask of 0
- any – creates an address of 0.0.0.0 with a wildcard mask of 255.255.255.255
- *dstIP* – destination IP address
- *dstWildlp* – wildcard mask IP address for destination
- *dstIPHost* – destination host IP address to which the packet is being sent
- *preced* – number from 1 to the access list maximum that indicates the precedence level to which packets are filtered
- *typeOServ* – number from 1 to the access list maximum that indicates the type of service to which packets are filtered
- log – logs an Info event into the ipAccessList log whenever the access-list rule is matched

Mode(s): Global Configuration

address

Description: From Domain Map Tunnel Configuration mode, sets the tunnel endpoint address of an L2TP or L2F tunnel. The **no** version removes the address of the tunnel.

From Interface Configuration or Subinterface Configuration mode, configures RIP to run on the interface specified by the IP address or on an unnumbered interface. Uses the default values: send version is RIP version 1, receive version is RIP version 1 and version 2, authentication is not enabled. The **no** version deletes the RIP interface. Use the **address** commands to configure RIP attributes on the network.

Syntax: To set the tunnel endpoint address:

```
address serverAddress
```

```
no address
```

- *serverAddress* – the IP address of the LNS or home gateway endpoint

To configure RIP:

```
[ no ] address { ipAddress | unnumbered interfaceType interfaceSpecifier }
```

- *ipAddress* – address of IP interface where RIP will be run
- unnumbered – specifies that RIP will be run on an unnumbered interface
 - › *interfaceType* – interface type; see *Interface Types and Specifiers in About This Guide*
 - › *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers in About This Guide*

Mode(s): Interface Configuration (RIP), Subinterface Configuration (RIP), Domain Map Tunnel Configuration

address area

Description: Creates an interface on which OSPF runs in the specified area, on top of the IP interface at the specified IP address. Uses the default values. The **no** version deletes OSPF interfaces. If the OSPF network was previously specified with the **network area** command, the OSPF interface already exists, and you do not need to use this command, unless you want to change the area of the OSPF interface to an area different from the one specified by the **network area** command.

Syntax: [no] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* }
area { *areald* | *arealdInt* }

- *ipAddress* – IP address of the interface on which OSPF will be run
- unnumbered – configures OSPF on an unnumbered interface
- *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- *areald* – OSPF area ID in IP address format
- *arealdInt* – OSPF area ID as a decimal value in the range 1–4294967295



Note: Before you issue this command, you must first configure an interface with the IP address specified by *ipAddress* or an interface configured as *unnumbered*.



Note: You must issue this command before issuing any other OSPF **address** command.

Mode(s): Router Configuration

address authentication key

- Description:** Specifies the password for text authentication and the key for MD5 authentication. The **no** version clears the key for the interface. Supported only in RIP version 2. Authentication is disabled by default.
- Syntax:**
- ```
address { ipAddress | unnumbered interfaceType interfaceSpecifier }
authentication key [0 | 8] authkey
```
- ```
no address [ ipAddress | unnumbered interfaceType interfaceSpecifier ]  
authentication key
```
- *ipAddress* – address of IP interface where RIP will be run
 - unnumbered – specifies that RIP will be run on an unnumbered interface
 - *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
 - *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
 - 0 – indicates the *authKey* is entered in unencrypted form (plaintext); this is the default option
 - 8 – indicates the *authKey* is entered in encrypted form (ciphertext)
 - *authkey* – password sent with RIP messages or the key used to encrypt/decrypt RIP messages, depending on the authentication mode set for this interface.
- Mode(s):** Interface Configuration, Subinterface Configuration

address authentication-key

Description: Assigns a password used by neighboring routers that are using OSPF simple password authentication. The **no** version deletes the password.

Syntax: [no] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* } authentication-key [0 | 8] *authKey*

- *ipAddress* – OSPF interface address previously specified with the **address** command
- unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
- *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- 0 – indicates the *authKey* is entered in unencrypted form (plaintext); this is the default option
- 8 – indicates the *authKey* is entered in encrypted form (ciphertext)
- *authKey* – password, a continuous string of characters up to 8 characters in length



Note: You must issue the **address area** command before issuing this command.

Mode(s): Router Configuration

address authentication message-digest

Description: Specifies that MD5 authentication is used for the OSPF interface. The **no** version sets authentication for the interface to none, but leaves any configured MD5 key intact.

Syntax: [no] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* }
authentication message-digest

- *ipAddress* – OSPF interface address previously specified with the **address** command
- unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
- *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*



Note: You must issue the **address area** command before issuing this command.

Mode(s): Router Configuration

address authentication mode

- Description:** Specifies the type of authentication used on this interface. The **no** version removes authentication from the interface. Supported only in RIP version 2. Authentication is disabled by default.
- Syntax:**
- ```
address { ipAddress | unnumbered interfaceType interfaceSpecifier }
authentication mode { text | md5 keyID }

no address [ipAddress | unnumbered interfaceType interfaceSpecifier]
authentication mode
```
- *ipAddress* – address of IP interface where RIP will be run
  - unnumbered – specifies RIP will be run on an unnumbered interface
  - *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
  - *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
  - text – simple text password is sent with each RIP message. If the password is not possessed by neighbors, the message is rejected.
  - md5 – MD5 message-digest algorithms are used to encrypt and compress the RIP message.
  - *keyID* – number identifying the MD5 key. Neighbors must share the MD5 key to decrypt the message and encrypt the response.
- Mode(s):** Interface Configuration, Subinterface Configuration

## address authentication-none

---

**Description:** Specifies that no authentication is to be used for the OSPF interface. The **no** version has no effect.

**Syntax:** [ no ] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* } authentication-none

- *ipAddress* – OSPF interface address previously specified with the **address** command
- unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
- *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*



**Note:** You must issue the **address area** command before issuing this command.

**Mode(s):** Router Configuration

## address cost

---

**Description:** Specifies a cost metric for an OSPF interface. Used in the calculation of the SPF routing table. The **no** version resets the path cost to the default.

**Syntax:** [ no ] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* } cost *intfCost*

- *ipAddress* – OSPF interface address previously specified with the **address** command
- unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
- *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- *intfCost* – link state metric cost; a number in the range 0–65535; default value is 10



**Note:** You must issue the **address area** command before issuing this command.

**Mode(s):** Router Configuration

## address dead-interval

---

**Description:** Sets the time period that the system's neighbors should wait without seeing hello packets from the system before they declare the router to be down. The **no** version resets the dead interval to its default.

**Syntax:** [ no ] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* }  
dead-interval *deadInterval*

- *ipAddress* – OSPF interface address previously specified with the **address** command
- unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
- *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- *deadInterval* – number in the range 1–65535 seconds; default value is 40 seconds



**Note:** You must issue the **address area** command before issuing this command.

**Mode(s):** Router Configuration

## address-family

---

**Description:** For BGP, configures the router or a specific VRF to exchange IPv4 addresses in unicast, multicast, or VPN mode by creating the specified address family. The **no** version removes the address family.

For RIP, configures RIP in a specific VRF to exchange IPv4 addresses. The **no** version removes the address family.

**Syntax:** For BGP:

```
[no] address-family { ipv4 [multicast | unicast | unicast vrf vrfName |
vrf vrfName] | vpnv4 [unicast] }
```

For RIP:

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

- **ipv4** – sessions that carry standard IPv4 address prefixes (default)
- **multicast** – specifies multicast prefixes
- **unicast** – specifies unicast prefixes (default)
- **vrfName** – name of the VRF; string of 1–32 alphanumeric characters
- **vpnv4** – sessions that carry customer VPN-IPv4 prefixes, each of which has been made globally unique by adding an 8-byte route distinguisher

**Mode(s):** Router Configuration

## address hello-interval

---

**Description:** Specifies the interval between hello packets that the router sends on the interface. The **no** version resets the hello interval to its default.

**Syntax:** [ no ] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* }  
hello-interval *helloInterval*

- **ipAddress** – OSPF interface address previously specified with the **address** command
- **unnumbered** – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
- **interfaceType** – interface type; see *Interface Types and Specifiers* in *About This Guide*
- **interfaceSpecifier** – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- **helloInterval** – number in the range 1–65535 seconds; default value is 10 seconds



**Note:** You must issue the **address area** command before issuing this command.

**Mode(s):** Router Configuration

## address message-digest-key md5

**Description:** Enables OSPF MD5 authentication and configures the MD5 key. The **no** version deletes an MD5 key.

**Syntax:** address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* }  
 message-digest-key *keyID* md5 [ 0 | 8 ] *msgDigestKey*

no address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* }  
 message-digest-key *keyID*

- *ipAddress* – OSPF interface address previously specified with the **address** command
- unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
- *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- *keyID* – key identifier in the range 1–255
- md5 – specifies use of the MD5 algorithm
- 0 – indicates that the *msgDigestKey* is entered in unencrypted form (plaintext); this is the default option
- 8 – indicates that the *msgDigestKey* is entered in encrypted form (ciphertext)
- *msgDigestKey* – OSPF password; a continuous string of up to 16 alphanumeric characters.



**Note:** If all the MD5 keys have been deleted, the authentication type is still MD5, but you need to configure MD5 keys.



**Note:** To disable MD5 authentication for the interface, use the **address authentication-none** command.



**Note:** You must issue the **address area** command before issuing this command.

**Mode(s):** Router Configuration

address network

---

- Description:** Configures the OSPF network type for the specified interface to something other than the default for the network medium. The **no** version restores the default value for the medium.
- Syntax:**
- ```
address { ipAddress | unnumbered interfaceType interfaceSpecifier }  
network { broadcast | non-broadcast | point-to-point }  
  
no address { ipAddress | unnumbered interfaceType interfaceSpecifier }  
network
```
- *ipAddress* – OSPF interface address previously specified with the **address** command
 - unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
 - *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
 - broadcast – sets network type to broadcast
 - non-broadcast – sets network type to NBMA
 - point-to-point – sets network type to point-to-point



Note: You must issue the **address area** command before issuing this command.

Mode(s): Router Configuration

address passive-interface

Description: Disables the transmission of routing updates on an interface. OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain. The **no** version reenables the transmission of routing updates.

Syntax: [no] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* }
passive-interface

- *ipAddress* – OSPF interface address previously specified with the **address** command
- unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
- *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*



Note: You must issue the **address area** command before issuing this command.

Mode(s): Router Configuration

address-pool-name

Description: Specifies an address pool name to associate with the domain name being configured. The **no** version removes the pool name.

Syntax: address-pool-name *poolName*
no address-pool-name

- *poolName* – name of the pool to associate with the domain name

Mode(s): Domain Map Configuration

address priority

Description: Sets the router priority. Used in determining the designated router for the particular network. This designation only applies to multi-access networks. Every broadcast and nonbroadcast multiaccess network has a designated router. The **no** version restores the default value.

Syntax: [no] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* }
priority *intfPriority*

- *ipAddress* – OSPF interface address previously specified with the **address** command
- unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
- *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- *intfPriority* – priority value, an 8-bit number in the range 1–255; default value is 1



Note: You must issue the **address area** command before issuing this command.

Mode(s): Router Configuration

address receive version

Description: Restricts the RIP version that the system can receive on an interface. The **no** version sets the interface back to the default value, receiving both RIP version 1 and version 2.

Syntax: address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* } receive version { 1 | 2 | 1 2 | 2 1 | off }

no address [*ipAddress* | unnumbered *interfaceType interfaceSpecifier*] receive version

- *ipAddress* – address of IP interface where RIP will be run
- unnumbered – specifies that RIP will be run on an unnumbered interface
- *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- 1 – specifies RIP version 1 only
- 2 – specifies RIP version 2 only
- 1 2 – specifies RIP version 1 and version 2; the default value
- 2 1 – specifies RIP version 2 and version 1
- off – turns reception off

Mode(s): Interface Configuration, Subinterface Configuration

address retransmit-interval

- Description:** Specifies the time between LSA retransmissions for the interface when an acknowledgment for the LSA is not received. The **no** version restores the default value.
- Syntax:** [no] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* }
retransmit-interval *retransInterval*
- *ipAddress* – OSPF interface address previously specified with the **address** command
 - unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
 - *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
 - *retransInterval* – number in the range 0–3600 seconds; default value is 5 seconds



Note: You must issue the **address area** command before issuing this command.

Mode(s): Router Configuration

address send version

- Description:** Restricts the RIP version that the system can send on an interface. The **no** version sets the interface back to the default value, sending only RIP version 1.
- Syntax:** address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* } send version { 1 | 2 | 1 2 | 2 1 | off }
- no address [*ipAddress* | unnumbered *interfaceType interfaceSpecifier*] send version
- *ipAddress* – address of IP interface where RIP will be run
 - unnumbered – specifies that RIP will be run on an unnumbered interface
 - *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
 - *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
 - 1 – specifies RIP version 1 only
 - 2 – specifies RIP version 2 only
 - 1 2 – specifies RIP version 1 and version 2
 - 2 1 – specifies RIP version 2 and version 1
 - off – turns reception off
- Mode(s):** Interface Configuration, Subinterface Configuration

address transmit-delay

- Description:** Sets the estimated time it takes to transmit a link state update packet on the interface. The **no** version restores the default value.
- Syntax:** [no] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* } transmit-delay *transmDelay*
- *ipAddress* – OSPF interface address previously specified with the **address** command
 - unnumbered – indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
 - *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
 - *transmDelay* – link state transmit delay, a number in the range 0–3600 seconds; default value is 1 second



Note: You must issue the **address area** command before issuing this command.

Mode(s): Router Configuration

aggregate-address

- Description:** Creates an aggregate entry in a BGP routing table. The **no** version removes the aggregate.
- Syntax:** [no] aggregate-address *address mask* [as-set | summary-only | attribute-map *attributeMapTag* | advertise-map *advertiseMapTag* | suppress-map *suppressMapName*]*
- *address* – aggregate IP address
 - *mask* – aggregate IP mask
 - as-set – if the **as-set** option is not specified, the path attributes of the aggregate route are set in the same way as locally originated routes, except that the `atomic_aggregate` and `aggregator` attributes are added. If the **as-set** option is used, the path attributes of the aggregate route are determined by combining the path attributes of the aggregated routes as described in RFC 1771. If the **as-set** option is used, the path attributes of the aggregate route may change whenever one of the aggregated routes changes, causing the aggregate route to be readvertised.
 - summary-only – filters all more specific routes from updates. **summary-only** not only creates the aggregate route but also suppresses advertisements of more-specific routes to all neighbors. If you only want to suppress advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific route leaks out, all BGP speakers will prefer that route over the less-specific aggregate you are generating (using longest-match routing). Alternatively, you can use the **suppress-map** keyword to suppress specific routes
 - *attributeMapTag* – string of up to 32 characters that identifies the route map used to set the attributes of the aggregate route
 - *advertiseMapTag* – string of up to 32 characters that identifies the route map used to set the routes to create AS-SET origin communities in the range
 - *suppressMapName* – string of up to 32 characters that identifies a route map that filters routes to be suppressed
 - * – indicates that one or more parameters can be repeated multiple times in a list in the command line
- Mode(s):** Address Family Configuration, Router Configuration

aggressive-mode

- Description:** Allows aggressive mode negotiation for the tunnel. The **no** version restores the default, main mode.
- Syntax:** [no] aggressive-mode
- Mode(s):** ISAKMP Policy Configuration

allow

- Description:** Specifies the domain names that are to be allowed access to AAA authentication. The **no** version negates the command.
- Syntax:** [no] allow *domainName*
- *domainName* – name of the domain; maximum of 64 characters
- Mode(s):** AAA Profile Configuration

append-after

- Description:** Add a next hop after a particular index in the MPLS explicit path. The sequence numbers for existing hops after the index adjust automatically. There is no **no** version.
- Syntax:** append-after *indexNumber* next-address *ipAddress* [mask *ipMask*] [loose]
- *index* – number of a node in an ordered set of abstract nodes
 - *ipAddress* – address of the next hop
 - *ipMask* – [not currently used] mask for the next adjacent address
 - loose – indicates the node is not necessarily directly connected (adjacent) to the previous node in the path. If loose is not configured, the configuration defaults to strict. Strict indicates that the node is directly connected to the previous node.
- Mode(s):** Explicit Path Configuration

aps force

- Description:** Forces the specified interface to be replaced by the inactive interface in an APS/MSP group. The no version allows the specified interface to resume operation.
- Syntax:** aps force *channelNumber*
no aps force [*channelNumber*]
- channelNumber* – number that identifies the working or protect interface. The number of the working interface is the same as the number of the corresponding active port on the I/O module. If there are *n* active ports on the I/O module, working interfaces are identified by the numbers 0 to *n*-1. Protect interfaces are identified by the numbers of the corresponding working interfaces plus *n*. For example, if the working interface has the number 0, and there is one active port on the I/O module, the corresponding protect interface has the number 1.
- Mode(s):** Controller Configuration

aps group

Description:	Assigns an interface to an APS/MSP group.
Syntax:	aps group <i>groupName</i> no aps group <ul style="list-style-type: none"> • <i>groupName</i>— name of the APS/MSP group to which the active and standby interfaces belong; up to 32 characters in length
Mode(s):	Controller Configuration

aps lockout

Description:	Prevents the working interface from switching to the protect interface. The no version restores the default situation, in which the working interface can switch to the protect interface.
Syntax:	aps lockout [<i>channelNumber</i>] no aps lockout <i>channelNumber</i> – number that identifies the working interface. The number of the working interface is the same as the number of the corresponding active port on the I/O module.
Mode(s):	Controller Configuration

aps manual

Description:	Forces the working interface to switch to the protect interface, unless a request of equal or higher priority exists. The no version allows the specified working interface to resume the active role.
Syntax:	aps manual <i>channelNumber</i> no aps manual [<i>channelNumber</i>] <i>channelNumber</i> – number that identifies the working or protect interface. The number of the working interface is the same as the number of the corresponding active port on the I/O module. If there are <i>n</i> active ports on the I/O module, working interfaces are identified by the numbers 0 to <i>n</i> -1. Protect interfaces are identified by the numbers of the corresponding working interfaces plus <i>n</i> . For example, if the working interface has the number 0, and there is one active port on the I/O module, the corresponding protect interface has the number 1.
Syntax:	Controller Configuration

aps protect

- Description:** Configures an interface as a protect interface. The **no** version removes the relationship between the protect interface and the active interface.
- Syntax:** aps protect [*channelNumber*]
 no aps protect

channelNumber – number that identifies the working interface. The number of the working interface is the same as the number of the corresponding active port on the I/O module.
- Mode(s):** Controller Configuration

aps revert

- Description:** Configures the APS/MSP group to operate in revertive mode. The **no** version restores the default setting, non-revertive mode.
- Syntax:** aps revert *minutes*
 no aps revert
- *minutes* – number of minutes in the range 5–12 at which the interface resumes the active role after that interface becomes available
- Mode(s):** Controller Configuration

aps unidirectional

- Description:** Configures the APS/MSP group to operate in unidirectional mode, the default setting. The **no** version configures the APS/MSP group to operate in bidirectional mode.
- Syntax:** aps unidirectional
 no aps unidirectional
- Mode(s):** Controller Configuration

aps working

- Description:** Configures an interface as a working interface. The **no** version removes the configuration.
- Syntax:** `aps working [channelNumber]`
`no aps working`
channelNumber – number that identifies the working interface. The number of the working interface is the same as the number of the corresponding active port on the I/O module.
- Mode(s):** Controller Configuration

area

- Description:** This command has only a **no** version. See the **no area** command for a complete description and syntax.

area-authentication-key

- Description:** Assigns a password used by neighboring routers for authentication of IS-IS level 1 LSPs, CSNPs, and PSNPs. The **no** version deletes the password.
- Syntax:** `[no] area-authentication-key [0 | 8] authKey`
`no area-authentication-key`
- 0 – indicates the *authKey* is entered in unencrypted form (plaintext); this is the default option
 - 8 – indicates the *authKey* is entered in encrypted form (ciphertext)
 - *authKey* – password, a continuous string of characters up to 8 characters in length
- Mode(s):** Router Configuration

area default-cost

- Description:** Specifies a cost for the default summary route sent into a stub area. A stub area is an OSPF area that carries a default route, intra-area routes, and interarea routes, but does not carry external routes. You cannot configure virtual links across a stub area. Stub areas cannot contain an ASBR. The **no** version removes the configured default route cost.
- Syntax:**
- ```
area { areald | arealdInt } default-cost defaultCost
no area { areald | arealdInt } default-cost
```
- *areald* – OSPF area ID in IP address format
  - *arealdInt* – OSPF area ID as a decimal value 0–4294967295
  - *defaultCost* – stub area's advertised external route cost (cost metric); an integer in the range 0–16777215
- Mode(s):** Router Configuration

## area-message-digest-key

**Description:** Specifies an HMAC MD5 key that the system uses to create a secure, encrypted message digest of each IS-IS level 1 packet (LSPs, CSNPs, and PSNPs). The digest is inserted into the packet from which it is created. Using this algorithm for area routers protects against unauthorized routers injecting false routing information into your network. You can specify when the system will start (default is the current time) and stop (default is never) accepting packets that include a digest made with this key. You can specify when the system will start (default is the current time plus 2 minutes) and stop (default is never) generating packets that include a digest made with this key. The **no** version deletes the key specified by the key-id.

**Syntax:** area-message-digest-key *keyId* hmac-md5 [ 0 | 8 ] *key*  
 [ start-accept *startAcceptTime* [ { *startAcceptMonth* *startAcceptDay* |  
*startAcceptDay* *startAcceptMonth* } *startAcceptYear* ] ]  
 [ start-generate *startGenTime* [ { *startGenMonth* *startGenDay* | *startGenDay*  
*startGenMonth* } *startGenYear* ] ]  
 [ stop-accept { never | *stopAcceptTime* [ { *stopAcceptMonth* *stopAcceptDay* |  
*stopAcceptDay* *stopAcceptMonth* } *stopAcceptYear* ] } ]  
 [ stop-generate { never | *stopGenTime* [ { *stopGenMonth* *stopGenDay* |  
*stopGenDay* *stopGenMonth* } *stopGenYear* ] } ]

no area-message-digest-key *keyId*

- *keyId* – integer from 1 to 255 that is a unique identifier for the secret key, sent with the message digest in the packet.
- 0 – indicates *key* is entered in unencrypted form (plaintext); default option
- 8 – indicates the *key* is entered in encrypted form (ciphertext)
- *key* – string of up to 20 alphanumeric characters; secret key used by the HMAC MD5 algorithm to generate the message digest
- *startAcceptTime*, *startAcceptMonth*, *startAcceptDay*, *startAcceptYear* – time, month, day, year that the system will start accepting packets created with this password. Use military time format *HH:MM[:SS]*.
- *startGenTime*, *startGenMonth*, *startGenDay*, *startGenYear* – time, month, day, year that the system will start inserting this password into packets. Use military time format *HH:MM[:SS]*.
- never – indicates the system never stops accepting or generating packets; overrides previously specified stop times and keeps using the authentication key in sending and receiving PDUs with the corresponding authentication indefinitely

- *stopAcceptTime*, *stopAcceptMonth*, *stopAcceptDay*, *stopAcceptYear* – time, month, day, year that the system will stop accepting packets created with this password. Use military time format *HH:MM[:SS]*.
- *stopGenTime*, *stopGenMonth*, *stopGenDay*, *stopGenYear* – time, month, day, year that the system will stop inserting this password into packets. Use military time format *HH:MM[:SS]*.

**Mode(s):** Router Configuration

## area nssa

---

**Description:** Configures an area as an NSSA and controls generation of type 7 default LSAs. NSSAs are similar to stub areas but have the additional capability of importing AS external routes in a limited fashion. The **no** version removes the specified option for default-information-originate, removes default-information-originate, or removes the NSSA designation from the area.

**Syntax:** [ no ] area { *areald* | *arealdInt* } nssa [ default-information-originate [ always | metric *absoluteValue* | metric-type 1 | metric-type 2 | route-map *mapTag* ]\* ]

- *areald* – OSPF area ID in IP address format
- *arealdInt* – OSPF area ID as a decimal value in the range 0–4294967295
- default-information-originate – causes the generation of a type 7 default LSA if a default route exists in the routing table.
- always – creates the default route if it doesn't exist
- *absoluteValue* – metric applied to the generated type 7 default LSAs; ranges from 0–429496729
- metric-type 1 – cost of the external routes is equal to the sum of all internal costs and the external cost
- metric-type 2 – cost of the external routes is equal to the external cost alone; this is the OSPF default
- *mapTag* – string of up to 32 alphanumeric characters that specifies a route map applied to the generated type 7 default LSAs
- \* – indicates that one or more parameters can be repeated multiple times in a list in the command line

**Mode(s):** Router Configuration

## area range

---

**Description:** Aggregates the routes at an area boundary. By default, the range of configured networks is advertised in type 3 (summary) LSAs. The **no** version disables this function.

**Syntax:** [ no ] area { *areald* | *arealdInt* } range *ipAddress mask* [ do-not-advertise ]

- *areald* – OSPF area ID in IP address format
- *arealdInt* – OSPF area ID as a decimal value in the range 0–4294967295
- *ipAddress* – IP address to match
- *mask* – IP address mask
- do-not-advertise – specifies that the range of configured networks is not advertised

**Mode(s):** Router Configuration

## area stub

---

**Description:** Defines an area as a stub area. A stub area is an OSPF area that carries a default route, intra-area routes, and interarea routes, but does not carry AS external routes. This reduces the size of the area's OSPF database and decreases memory usage for external routers in the stub area. The **no** version disables this function.

**Syntax:** [ no ] area { *areald* | *arealdInt* } stub

- *areald* – OSPF area ID in IP address format
- *arealdInt* – OSPF area ID as a decimal value in the range 0–4294967295

**Mode(s):** Router Configuration

## area virtual-link

---

**Description:** Defines an OSPF virtual link. The **no** version removes the virtual link.

**Syntax:** [ no ] area { *areald* | *arealdInt* } virtual-link *ipAddress*

- *areald* – OSPF area ID in IP address format
- *arealdInt* – OSPF area ID as a decimal value in the range 0–4294967295
- *ipAddress* – IP address associated with the virtual link neighbor

**Mode(s):** Router Configuration

---

## area virtual-link authentication-key

---

- Description:** Configures simple password (type 1) authentication for OSPF virtual links. The **no** version removes the password.
- Syntax:** [ no ] area { *areaID* | *arealdInt* } virtual-link *ipAddress* authentication-key [ 0 | 8 ] *line*
- *areald* – OSPF area ID in IP address format
  - *arealdInt* – OSPF area ID as a decimal value in the range 0–4294967295
  - *ipAddress* – IP address of the virtual link neighbor
  - 0 – indicates that the *line* is entered in unencrypted form (plaintext); this is the default option
  - 8 – indicates that the *line* is entered in encrypted form (ciphertext)
  - *line* – password to be used by neighbors. All neighboring routers on the same network must have the same password. The password can be a continuous string of up to 16 alphanumeric characters.
- Mode(s):** Router Configuration

---

## area virtual-link authentication message-digest

---

- Description:** Specifies that MD5 authentication is used for the virtual link. The **no** version sets the authentication for the virtual link to none, but leaves any configured MD5 key intact.
- Syntax:** [ no ] area { *areaID* | *arealdInt* } virtual-link *ipAddress* authentication message-digest
- *areald* – OSPF area ID in IP address format
  - *arealdInt* – OSPF area ID as a decimal value in the range 0–4294967295
  - *ipAddress* – IP address of the virtual link neighbor
- Mode(s):** Router Configuration

---

## area virtual-link authentication-none

---

- Description:** Specifies that no authentication is to be used for the virtual link. The **no** version has no effect.
- Syntax:** [ no ] area { *areald* | *arealdInt* } virtual-link *ipAddress* authentication-none
- *areald* – OSPF area ID in IP address format
  - *arealdInt* – OSPF area ID as a decimal value in the range 0–4294967295
  - *ipAddress* – IP address of the virtual link neighbor
- Mode(s):** Router Configuration

## area virtual-link dead-interval

---

**Description:** Defines an OSPF virtual link and the time interval allowed for detecting a dead router. The **no** version removes the virtual link's dead interval.

**Syntax:** [ no ] area { *areaID* | *areaIDInt* } virtual-link *ipAddress* dead-interval *deadInterval*

- *areaID* – OSPF area ID in IP address format
- *areaIDInt* – OSPF area ID as a decimal value in the range 0–4294967295
- *ipAddress* – IP address of the virtual link neighbor
- *deadInterval* – integer in the range 1–8192 seconds

**Mode(s):** Router Configuration

## area virtual-link hello-interval

---

**Description:** Defines an OSPF virtual link and the time between the hello packets. The hello interval value must be the same for both ends of the virtual link. The **no** version removes the virtual link's hello interval.

**Syntax:** [ no ] area { *areaID* | *areaIDInt* } virtual-link *ipAddress* hello-interval *helloInterval*

- *areaID* – OSPF area ID in IP address format.
- *areaIDInt* – OSPF area ID as a decimal value in the range 0–4294967295
- *ipAddress* – IP address associated with the virtual link neighbor
- *helloInterval* – integer in the range 1–8192 seconds

**Mode(s):** Router Configuration

## area virtual-link message-digest-key md5

---

**Description:** Enables MD5 authentication and configures MD5 keys for virtual links. The **no** version deletes MD5 keys.

**Syntax:** `area { areald | arealdInt } virtual-link ipAddress message-digest-key md5Keyld md5 [ 0 | 8 ] msgDigestKey`

`no area { areald | arealdInt } virtual-link ipAddress message-digest-key md5Keyld`

- *areald* – OSPF area ID in IP address format
- *arealdInt* – OSPF area ID as a decimal value in the range 0–4294967295
- *ipAddress* – IP address of the virtual link neighbor
- *md5Keyld* – key identifier in the range 1–255
- 0 – indicates that the *msgDigestKey* is entered in unencrypted form (plaintext); this is the default option
- 8 – indicates that the *msgDigestKey* is entered in encrypted form (ciphertext)
- *msgDigestKey* – password to be used by neighbors. All neighboring routers on the same network must have the same password. The password can be a continuous string of up to 16 alphanumeric characters.



**Note:** *If you delete all the MD5 keys, the authentication type for the virtual link is still MD5, but you need to configure MD5 keys.*



**Note:** *To disable MD5 authentication for the virtual link, use the `area virtual-link authentication-none` command.*

**Mode(s):** Router Configuration

## area virtual-link retransmit-interval

---

**Description:** Defines an OSPF virtual link and the time between link state advertisement retransmissions for the adjacency belonging to the virtual link. The **no** version removes the virtual link's retransmit interval.

**Syntax:** `[ no ] area { areald | arealdInt } virtual-link ipAddress retransmit-interval retransmInterval`

- *areald* – OSPF area ID in IP address format.
- *arealdInt* – OSPF area ID as a decimal value in the range 0–4294967295
- *ipAddress* – IP address of the virtual link neighbor
- *retransmInterval* – LSA retransmit interval; an integer in the range 1–8192 seconds

**Mode(s):** Router Configuration

## area virtual-link transmit-delay

---

- Description:** Defines an OSPF virtual link and the estimated time it takes to transmit a link state update packet on the virtual link. The **no** version removes the virtual link's transmit delay.
- Syntax:** [ no ] area { *areald* | *arealdInt* } virtual-link *ipAddress* transmit-delay *transmDelay*
- *areald* – OSPF area ID in IP address format
  - *arealdInt* – OSPF area ID as a decimal value in the range 0–4294967295
  - *ipAddress* – IP address associated with the virtual link neighbor
  - *transmDelay* – LSA transmit delay; an integer in the range 1–8192 seconds
- Mode(s):** Router Configuration

## arp

---

- Description:** Adds a permanent entry in the ARP cache. The **no** version removes an entry from the ARP cache. This command applies only on an Ethernet or bridged Ethernet interface.
- Syntax:** [ no ] arp [ vrf *vrfName* ] *ipAddress* { *interfaceType interfaceSpecifier* [ *macAddress* [ validate ] ] | *macAddress* }
- *vrfName* – name of the VRF to which the command applies; string of 1–32 alphanumeric characters
  - *ipAddress* – IP address in 32-bit dotted-decimal format corresponding to the local data link address
  - *interfaceType* – interface type; see *Interface Types and Specifiers* in *About This Guide*
  - *interfaceSpecifier* – particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
  - *macAddress* – MAC address of the interface
  - *validate* – allows the inclusion of MAC validation entries
- Mode(s):** Global Configuration

## arp timeout

---

**Description:** Specifies how long an entry remains in the ARP cache. You can set the ARP timeout only on bridged Ethernet and Fast Ethernet interfaces on the FE-2 module. You cannot set the timeout on the SRP module. The default value is 21600 seconds (6 hours). Use the **show config** command to display the current value. The **no** version restores the default value.

**Syntax:** arp timeout *timeoutVal*  
no arp timeout

- *timeoutVal* – time in seconds that an entry remains in the ARP cache

**Mode(s):** Interface Configuration

## atm

---

**Description:** The system supports the configuration of traffic-shaping parameters for PPPoA via domain-based parameters and RADIUS. The **no** version removes the ATM traffic-shaping configuration.

**Syntax:** atm { ubr | ubrpcr *pcr* | nrtvbr *pcr scr mbs* | cbr *pcr* }  
no atm

- ubr – sets the traffic category to unspecified bit rate
- ubrpcr – sets the traffic category to unspecified bit rate with peak cell rate
- *pcr* – peak cell rate
- nrtvbr – sets the traffic category to non-real time variable bit rate
- *scr* – sustained cell rate
- *mbs* – maximum burst size
- cbr – sets the traffic category to constant bit rate

**Mode(s):** Domain Map Configuration

## atm aal5 description

---

**Description:** Assigns a text description or alias to an ATM AAL5 interface. The **no** version removes the text description or alias. Use the **show atm subinterface** command to display the text description. The atm description is pushed out to RADIUS during authentication/accounting.

**Syntax:** atm aal5 description *name*  
no atm aal5 description

- *name* – alias for the AAL5 interface; up to 32 characters

**Mode(s):** Interface Configuration

---

## atm aal5 shutdown

---

- Description:** Sets the administrative state of an ATM AAL5 interface to disabled. The **no** version enables a disabled interface.
- Syntax:** [ no ] atm aal5 shutdown
- Mode(s):** Interface Configuration

---

## atm aal5 snmp trap link-status

---

- Description:** Enables SNMP link status traps on the AAL5 layer on a per-interface basis. The **no** version disables the traps.
- Syntax:** [ no ] atm aal5 snmp trap link-status
- Mode(s):** Interface Configuration

---

## atm atm1483 description

---

- Description:** Assigns a text description or alias to an ATM 1483 interface. The **no** version removes the text description or alias. Use the **show atm aal5 interface** to display the text description. The atm description is pushed out to RADIUS during authentication/accounting.
- Syntax:** atm atm1483 description *name*  
no atm atm1483 description
- *name* – alias for the atm atm1483 interface; up to 15 characters
- Mode(s):** Subinterface Configuration

---

## atm atm1483 mtu

---

- Description:** Sets the MTU size for an ATM 1483 subinterface. The **no** version restores the default MTU size of 9180.
- Syntax:** atm atm1483 mtu *size*  
no atm atm1483 mtu
- *size* – maximum number of packet transmissions permitted on an ATM 1483 subinterface; the valid range is 256–9180. The default is 9180.
- Mode(s):** Subinterface Configuration

---

## atm atm1483 shutdown

---

- Description:** Sets the administrative state of an ATM 1483 subinterface to disabled. The **no** version enables a disabled subinterface.
- Syntax:** [ no ] atm atm1483 shutdown
- Mode(s):** Subinterface Configuration

---

## atm atm1483 snmp trap link-status

---

- Description:** Enables SNMP link status traps on the ATM1483 layer. The **no** version disables the traps.
- Syntax:** [ no ] atm atm1483 snmp trap link-status
- Mode(s):** Subinterface Configuration

---

## atm auto-configuration

---

- Description:** Enables auto configuration of ILMI. Auto configuration is enabled by default. The **no** version disables auto configuration and sets the ILMI parameters to the UNI version configured using the **atm uni-version** command, which has a default value of UNI 4.0. Entering the **atm auto-configuration** command overrides any previous configuration of the **atm uni-version** command.
- Syntax:** [ no ] atm auto-configuration
- Mode(s):** Interface Configuration

---

## atm cac

---

- Description:** Enables CAC on the ATM interface. If the subscription limit or UBR weight parameters are set to zero, the system uses the effective port bandwidth as the subscription bandwidth. The effective bandwidth varies according to line module. The **no** version disables CAC on the interface.
- Syntax:** [ no ] atm cac [ *subscriptionBandwidth* ] [ubr *ubrWeight* ]
- *subscriptionBandwidth* – maximum allowable bandwidth on this port in the range 0–2147482647 kbps; the default value is 0
  - *ubrWeight* – bandwidth associated with UBR and UBR-PCR connections in the range is 0–2147482647 kbps; the default value is 0



**Note:** If you modify one of these parameters after CAC is enabled, you must modify both parameters. Otherwise, the parameter not specified reverts to its default value.

- Mode(s):** Interface Configuration

## atm clock internal

---

- Description:** Causes the ATM interface to generate the transmit clock internally. The **no** version causes ATM interfaces to recover the clock from the received signal. If the internal clock is chosen and no internal source is specified, then the internal clock source is taken from the line module.
- Syntax:** [ no ] atm clock internal [ *internalSource* ]
- *internalSource* – one of the following:
    - › module – specify that the internal clock is from the line module
    - › chassis – specify that the internal clock is from the configured system clock
- Mode(s):** Interface Configuration

## atm description

---

- Description:** Assigns a text description or alias to the interface. The **no** version removes the text description or alias. The **show atm interface** command displays the text description. The description is pushed out to RADIUS during authentication/accounting.
- Syntax:** atm description *name*  
no atm description
- *name* – alias for the atm interface; up to 32 characters
- Mode(s):** Interface Configuration

## atm esi-address

---

- Description:** Specifies an ATM ESI address for the subinterface. The **no** version removes the ESI address.
- Syntax:** atm esi-address *esiAddress*  
no atm esi-address
- *esiAddress* – end system ID portion of the ATM NSAP address in the format xxxxxxxxxxxx.xx
- Mode(s):** Subinterface Configuration

## atm framing

---

- Description:** Configures T3 or E3 framing on an ATM interface. The **no** version returns framing to the default. For a T3 interface, the default is cbitplcp. For an E3 interface, the default is g751plcp.
- Syntax:** atm framing *framingType*  
no atm framing
- *framingType* – one of the following:
    - › cbitadm – c-bit with ATM direct mapping for a DS3 (T3) interface
    - › cbitplcp – c-bit with PLCP framing for a DS3 (T3) interface (default for T3)
    - › g832adm – G.832 ATM direct mapping for an E3 interface
    - › g751adm – G.751 ATM direct mapping for an E3 interface
    - › g751plcp – G.751 PLCP mapping for an E3 interface (default for E3)
    - › m23adm – M23 ATM direct mapping for a DS3 (T3) interface
    - › m23plcp – M23 with PLCP framing for a DS3 (T3)
- Mode(s):** Interface Configuration

## atm ilmi-enable

---

- Description:** Enables ILMI on the interface. The **no** version removes the ILMI PVC.
- Syntax:** [ no ] atm ilmi-enable
- Mode(s):** Interface Configuration

## atm ilmi-keepalive

---

- Description:** Enables generation of ILMI keepalive messages on the system. The **no** version disables the generation of keepalive messages. Enabling generation of keepalive messages has an effect on the operational state of the ATM interface.
- Syntax:** [ no ] atm ilmi-keepalive [ *seconds* ]
- *seconds* – number in the range 0–4294967295; the interval in seconds between two consecutive ILMI keepalive requests
- Mode(s):** Interface Configuration

## atm lbo

- Description:** Specifies the cable length (line build-out) for the ATM T3 or E3 interface. The length of cable determines power requirements. The **no** version restores the default value.
- Syntax:** atm lbo { long | short }  
no atm lbo
- short – a cable length in the range 0–225 feet (the default)
  - long – a cable length in the range 255–450 feet
- Mode(s):** Interface Configuration

## atm oam

- Description:** Configures F4 OAM on an interface or circuit. The **no** version deletes F4 OAM circuits.
- Syntax:** atm oam [ vpi ] [ [ seg-loopback | end-loopback [ loopback-timer *time* ] ]  
[ cc { source | sink | both } ] ]  
no atm oam [ vpi ] [ [ seg-loopback | end-loopback [ loopback-timer *time* ] ] ]



**Note:** If you do not specify any options, both end-to-end and segment loopback are enabled on all VPIs on the interface.

- vpi – VPI on which you want to enable F4 OAM. If you do not specify a VPI, F4 OAM flow is enabled on all VPIs on the interface.
- seg-loopback – enables F4 segment OAM
- end-loopback – enables F4 end-to-end OAM
- loopback-timer – to generate F4 loopback cells on the VPI, you must configure the loopback timer; you can set the loopback timer only for end-to-end loopback
- time – time interval in the range 0–600 seconds between transmissions of F4 loopback cells. This value is a multiple of 20 and is based on the number of circuits with VC integrity enabled. The values are 20 seconds for 1–1999 circuits, 40 seconds for 2000–3999 circuits, 60 seconds for 4000–5999 circuits, and so on. These values are used regardless of the setting of this parameter.
- cc – enables CC cells on the PVC; you can enable CC cells only on data circuits, not on control circuits, such as ILMI or signaling circuits
- sink – enables this VC as a sink point (cell receiver)
- source – enables this VC as the source point (cell generator)
- both – enables this VC as both a sink point and a source point

- Mode(s):** Interface Configuration, Subinterface Configuration

## atm oam flush

---

- Description:** Indicates that all OAM cells received on an interface should be ignored. OAM performs fault management and performance management functions on an ATM interface. The **no** version disables the feature.
- Syntax:** [ no ] atm oam flush [ alarm-cells ]
- alarm-cells – causes the system to ignore only AIS and RDI cells and to accept all other OAM cells
- Mode(s):** Interface Configuration

## atm oam loopback-location

---

- Description:** Sets the location ID of the ATM interface. The **no** version returns the loopback location to the default setting of all 1s (ones).
- Syntax:** atm oam loopback-location *locationID*  
[ no ] atm oam loopback-location
- *locationID* – value of the four-octet long location ID of the ATM interface
- Mode(s):** Interface Configuration, Subinterface Configuration

## atm pvc

- Description:** Creates a PVC on an ATM interface. The **no** version removes the specified PVC.
- Syntax:**
- ```
atm pvc vcd vpi vci { encapsulation } [ { cbr cbr } | { peak [ average burst
[ rt ] ] ] [ oam [ seconds | cc [ segment | end-to-end ] { source | sink | both } ] ]
[ inArp [ minutes ] ]
```
- ```
no atm pvc vcd
```
- *vcd* – virtual circuit descriptor that is an identifier for the VC in other commands; the range is 1–2147483647
  - *vpi* – virtual path identifier of this PVC. The allowable numeric range depends on the line module capabilities and current configuration. The VPI and VCI cannot both be set to 0; if one is 0, the other cannot be 0.
  - *vci* – virtual circuit identifier of this PVC. The allowable numeric range depends on the line module capabilities and current configuration. The VPI and VCI cannot both be set to 0; if one is 0, the other cannot be 0.
  - *encapsulation* – one of the following:
    - › aal5snap – LLC encapsulated circuit; LLC/SNAP precedes the protocol datagram
    - › aal5mux ip – VC-based multiplexed circuit used for IP only
    - › aal5autoconfig – enables autodetection of the 1483 encapsulation (LLC/SNAP or VC multiplexed)
    - › ilmi – integrated local management interface encapsulation
    - › qsaal – Q.2931 signalling
  - *peak* – PCR in Kbps
  - *average* – average rate in Kbps; also referred to as SCR
  - *burst* – length in cells of the burst.; also referred to as MBS
  - *rt* – selects VBR-RT as the service type; the default type is VBR-NRT. You can select *rt* only if you set the *peak*, *average*, and *burst* parameters.
  - *cbr* – constant bit rate in Kbps
  - *oam* – enable generation of OAM F5 loopback cells on this circuit. This option enables VC integrity features that have an effect on the operational state of the ATM PVC.
  - *seconds* - time interval in seconds between transmissions of OAM F5 end-to-end loopback cells for VC connectivity verification. This value is a multiple of 20 and is based on the number of circuits with VC integrity

enabled. The values are: 20 seconds for 1–1999 circuits, 40 seconds for 2000–3999 circuits, 60 seconds for 4000–5999 circuits, and so on. These values are used regardless of the setting of this parameter.

- `inarp` – enables Inverse ARP
- `minutes` – InARP refresh rate in minutes; 15 minutes is the default



**Note:** *The optional peak, average, and burst parameters configure traffic-shaping parameters for the circuit. The allowable traffic-shaping features and range specifications depend on the line module capabilities.*

- `cc` – enables CC cells on the PVC; you can enable CC cells only on data circuits, not on control circuits, such as ILMI or signaling circuits
- `segment` – opens an OAM CC segment cell flow
- `end-to-end` – opens an OAM CC end-to-end cell flow
- `sink` – enables this VC as a sink point (cell receiver)
- `source` – enables this VC as the source point (cell generator)
- `both` – enables this VC as both a sink point and a source point

**Mode(s):** Interface Configuration, Subinterface Configuration

## atm shutdown

---

**Description:** Administratively disables an ATM interface. The **no** version enables a disabled interface.

**Syntax:** [ no ] atm shutdown

**Mode(s):** Interface Configuration

## atm snmp trap link-status

---

**Description:** Enables SNMP link status traps on the ATM layer on a per-interface basis. The **no** version disables the traps.

**Syntax:** [ no ] atm snmp trap link-status

**Mode(s):** Interface Configuration

## atm sonet stm-1

---

**Description:** Sets the mode of operation on the physical interface to SDH STM-1. The **no** version restores the default value, SONET STS-3c operation.

**Syntax:** [ no ] atm sonet stm-1

**Mode(s):** Interface Configuration

## atm svc

**Description:** Defines an SVC on an ATM subinterface. The system will attempt to set up an SVC to the destination address with the requested traffic parameters and encapsulation. The **no** version removes the specified SVC definition.

**Syntax:** atm svc nsap *nsapAddress* [ { *encapsulation* } [ { *cbr cbr* } | *peak* [ *average burst* [ *rt* ] ] ] ]

no [ atm ] svc [ nsap *nsapAddress* ]

- *nsapAddress* – destination address in the format

$$\underbrace{XX}_{2} \cdot \underbrace{XXXXXXXXXXXXXXXXXXXXXXXXXXXX}_{24} \cdot \underbrace{XXXXXXXXXXXX}_{12} \cdot \underbrace{XX}_{2}$$

- *encapsulation* – one of the following:
  - › aal5snap – LLC encapsulated circuit; LLC/SNAP precedes the protocol datagram
  - › aal5mux ip – VC-based multiplexed circuit used for IP only
- *cbr* – constant bit rate in Kbps
- *peak* – PCR in Kbps
- *average* – average rate in Kbps; also referred to as SCR
- *burst* – length in cells of the burst.; also referred to as MBS
- *rt* – selects VBR-RT as the service type

**Mode(s):** Subinterface Configuration

## atm uni-version

**Description:** Specifies the UNI version the interface should use. There is no **no** version.

**Syntax:** atm uni-version *versionNumber*

- *versionNumber* – UNI version number: 3.0, 3.1, or 4.0

**Mode(s):** Interface Configuration

## atm vc-per-vp

---

**Description:** Configures the number of virtual circuits per virtual path. This command controls the VPI and VCI range on the ATM interface. The allowable configuration range depends on the line module. The system will not execute the command if any virtual circuits are open on the interface. The **no** version restores the default.



**Note:** *The minimum number of VCs per VP is 4096 for OC3-4 modules and 1024 for UT3a modules. If you enter a value that is below the minimum, the system uses the minimum value.*

**Syntax:** atm vc-per-vp [ *vcCount* ]  
no atm vc-per-vp

- *vcCount* – number of virtual circuits per virtual path

**Mode(s):** Interface Configuration

## atm vp-tunnel

---

**Description:** Defines a virtual path tunnel and configures the rate of traffic flow within the tunnel. The **no** version removes the restriction.

**Syntax:** atm vp-tunnel *vpi* [ *cbr* ] *kbps*  
no atm vp-tunnel *vpi*

- *vpi* – number in the range 0–255; virtual path identifier of this PVC
- *cbr* – specifies the service class as constant bit rate
- *kbps* – tunnel rate for a virtual path. The aggregate to this traffic from all circuits configured in the tunnel is held to the specified rate. Certain line modules may have minimum rates for VP tunnels.

**Mode(s):** Interface Configuration

## authentication

---

**Description:** Specifies the authentication method to use in the IKE policy. The **no** version restores the default, preshared keys.

**Syntax:** authentication { pre-share }  
no authentication

- pre-share – specifies preshared keys as the authentication method

**Mode(s):** ISAKMP Policy Configuration

## authentication key

---

- Description:** Specifies the password for text authentication and the key for MD5 authentication for RIP remote-neighbor interface. The **no** version clears the key for the interface. Supported only in RIP version 2. Authentication is disabled by default.
- Syntax:** authentication key [ 0 | 8 ] *authkey*  
no authentication key
- 0 – the *authKey* is entered in unencrypted form (plaintext); this is the default option
  - 8 – the *authKey* is entered in encrypted form (ciphertext)
  - *authkey* – specifies the password sent with RIP messages or the key used to encrypt/decrypt RIP messages, depending on the authentication mode set for this remote-neighbor interface.
- Mode(s):** Remote Neighbor Configuration

## authentication-key

---

- Description:** Enables simple password authentication and assigns a password used by OSPF remote neighbors. The **no** version deletes the password.
- Syntax:** authentication-key [ 0 | 8 ] *authKey*  
no authentication-key
- 0 – the *authKey* is entered in unencrypted form (plaintext); this is the default option
  - 8 – the *authKey* is entered in encrypted form (ciphertext)
  - *authKey* – a password, a continuous string of characters up to 8 characters in length
- Mode(s):** Remote Neighbor Configuration

## authentication message-digest

---

- Description:** Specifies that MD5 authentication is used for the OSPF remote-neighbor interface. There is no **no** version.
- Syntax:** authentication message-digest
- Mode(s):** Remote Neighbor Configuration

## authentication mode

---

- Description:** Specifies the type of authentication used on the RIP remote-neighbor interface. The **no** version removes authentication from the interface. Supported only in RIP version 2. Authentication is disabled by default.
- Syntax:** authentication mode { text | md5 *keyID* }  
no authentication mode
- text – a simple text password is sent with each RIP message. If the password is not possessed by remote neighbors, the message is rejected.
  - md5 – MD5 message-digest algorithms are used to encrypt and compress the RIP message.
  - *keyID* – number identifying the MD5 key in the range 1–255. Remote neighbors must share the MD5 key to decrypt the message and encrypt the response.
- Mode(s):** Remote Neighbor Configuration

## authentication-none

---

- Description:** Specifies that no authentication is to be used for the OSPF remote-neighbor interface. There is no **no** version.
- Syntax:** authentication-none
- Mode(s):** Remote Neighbor Configuration

## auto-configure

---

- Description:** Specifies the type(s) of dynamic encapsulations that will be accepted or detected by the static ATM 1483 interface. The command may be entered repeatedly in ATM subinterface mode.
- Syntax:** [ no ] auto-configure *upperInterfaceType*
- *upperInterfaceType* – dynamic encapsulation type: **bridgedEthernet**, **ip**, **ppp**, **pppoe**
- Mode(s):** Interface Configuration, Subinterface Configuration

## automatic-virtual-link

---

- Description:** Enables or disables automatic virtual link configuration. The **no** version disables an automatic virtual link.
- Syntax:** [ no ] automatic-virtual-link
- Mode(s):** Router Configuration

## auto-summary

---

**Description:** Reenables the automatic summarization of routes redistributed into BGP to their natural network masks. Automatic summarization is enabled by default. The **no** version disables automatic summarization.

**Syntax:** [ no ] auto-summary

**Mode(s):** Address Family Configuration, Router Configuration