

E-F-G-H Commands

e3-scramble

Description: Enables scrambling of the ATM cell payload on an E3 interface. E3 scrambling assists clock recovery on the receiving end of the interface. The **no** version disables scrambling.

Syntax: [no] e3-scramble

Mode(s): Controller Configuration

enable

Description: Enters Privileged Exec mode at the specified privilege level. There is no **no** version.

Syntax: enable [*level*]

- *level* – one of the following privilege levels; the default is 10
 - › 0 – allows the user to execute the **help**, **enable**, **disable**, and **exit** commands
 - › 1 – allows the user to execute commands in User Exec mode plus commands at level 0
 - › 5 – allows the user to execute Privileged Exec show commands plus the commands at levels 1 and 0
 - › 10 – allows the user to execute all commands except support commands, which may be provided by Juniper Networks Customer Service
 - › 15 – allows the user to execute support commands

Mode(s): User Exec

enable password

Description: Sets a password to control access to certain types of commands. The **no** version removes the password requirement.

Syntax: enable password [level *securityLevel*] [*passwordType*] *passwordText*
no enable password [level *securityLevel*]

- *securityLevel* – the security level for which you want to set the password; the default is 5
 - › 0 – allows the user to execute the **help**, **enable**, **disable**, and **exit** commands
 - › 1 – allows the user to execute commands in User Exec mode plus commands at level 0
 - › 5 – allows the user to execute Privileged Exec **show** commands plus the commands at levels 1 and 0; this is the default level
 - › 10 – allows the user to execute all commands except support commands, which may be provided by Juniper Networks Customer Service
 - › 15 – allows the user to execute support commands
- *passwordType*:
 - › 0 – specifies that an unencrypted password follows; this is the default
 - › 7 – specifies that an encrypted password follows
- *passwordText* – password, either encrypted or unencrypted, depending on the password type



Note: *On your system, all passwords are stored as encrypted passwords.*

Mode(s): Global Configuration

enable proxy authenticate

Description: Configures proxy authenticate for a remote host. The **no** version removes proxy authenticate configuration from the remote host.

Syntax: [no] enable proxy authenticate

Mode(s): L2TP Destination Profile Host Configuration

enable secret

Description: Sets a secret to control access to certain types of commands. The **no** version removes the secret requirement.

Syntax: enable secret [level *securityLevel*] [*secretType*] *secretText*
no enable secret [*securityLevel*]

- *securityLevel* – the security level for which you want to set the secret; the default is 5
 - › 0 – allows the user to execute the **help**, **enable**, **disable**, and **exit** commands
 - › 1 – allows the user to execute commands in User Exec mode plus commands at level 0
 - › 5 – allows the user to execute Privileged Exec **show** commands plus the commands at levels 1 and 0; this is the default level
 - › 10 – allows the user to execute all commands except support commands, which may be provided by Juniper Networks Customer Service
 - › 15 – allows the user to execute support commands
- *secretType*:
 - › 0 – specifies that an unencrypted secret follows; this is the default
 - › 7 – specifies that an encrypted secret follows
- *secretText* – secret, either encrypted or unencrypted, depending on the secret type



Note: *On your system, all secrets are stored as encrypted secrets.*

Mode(s): Global Configuration

encapsulation bridge1483

Description: Configures bridged Ethernet as the encapsulation method on an interface. The **no** version removes bridged Ethernet as the encapsulation method on the interface.

Syntax: [no] encapsulation bridge1483

Mode(s): Interface Configuration, Subinterface Configuration

encapsulation hdlc

- Description:** Enables Cisco HDLC encapsulation. The **no** version disables Cisco HDLC on an interface.
- Syntax:** [no] encapsulation hdlc
- Mode(s):** Interface Configuration, Subinterface Configuration

encapsulation ietf

- Description:** Enables Frame Relay or Multilink Frame Relay encapsulation. The **no** version removes Frame Relay or Multilink Frame Relay configuration from an interface.
- Syntax:** encapsulation { frame-relay | mlframe-relay } ietf
no encapsulation { frame-relay | mlframe-relay }
- Mode(s):** Interface Configuration

encapsulation mlppp

- Description:** Configures MLPPP as the encapsulation method on an individual interface. Creates an MLPPP link interface, also known as an MLPPP bundle member. The **no** version disables MLPPP on an interface.
- Syntax:** [no] encapsulation mlppp
- Mode(s):** Interface Configuration, Subinterface Configuration

encapsulation ppp

- Description:** Configures PPP as the encapsulation method for the interface. The **no** version disables PPP on an interface.
- Syntax:** [no] encapsulation ppp
- Mode(s):** Interface Configuration, Subinterface Configuration

encapsulation pppoe

- Description:** Configures PPPoE as the encapsulation method for the interface. The **no** version disables PPPoE on an interface.
- Syntax:** [no] encapsulation pppoe
- encapsulation – configure pppoe encapsulation
- Mode(s):** Interface Configuration, Subinterface Configuration

encapsulation smds-trunk

- Description:** Configures SMDS trunk as the encapsulation method for the interface. SMDS trunk encapsulation allows SMDS traffic to be sent over a GRE tunnel or a HSSI interface. The **no** version disables SMDS trunk encapsulation on an interface.
- Syntax:** [no] encapsulation smds-trunk
- Mode(s):** Interface Configuration

encapsulation vlan

- Description:** Configures VLAN as the encapsulation method for the interface. The **no** version disables VLAN on an interface.
- Syntax:** [no] encapsulation vlan
- Mode(s):** Interface Configuration, Subinterface Configuration

encryption

- Description:** Sets the encryption algorithm to use in the IKE policy. The **no** version restores the default, 3DES.
- Syntax:** encryption des | 3des
no encryption
- des – specifies 56-bit DES-CBC as the encryption algorithm
 - 3des – specifies 168-bit 3DES-CBC as the encryption algorithm
- Mode(s):** ISAKMP Policy Configuration

end

- Description:** Exits Global Configuration mode or any of the Configuration submodes and returns to the User Exec mode. There is no **no** version.
- Syntax:** end
- Mode(s):** Global Configuration

erase secrets

Description: Removes all CLI passwords or secrets. Execute before pressing the NMI button on the SRP module. There is no **no** version.



Note: If you enter the **service unattended password-recovery** command, the behavior of the **erase secrets** command changes. The **erase secrets** command will not take any parameters and will not be available through a vty session until you enter **no service unattended password-recovery**.

Syntax: erase secrets *seconds*

- *seconds* – number of seconds in the range 1–60 to allow for the operation

Mode(s): User Exec

ethernet description

Description: Adds a text description to a non-SRP Fast Ethernet or Gigabit Ethernet interface. The **no** version removes the description from the interface.

Syntax: ethernet description *name*

no ethernet description

- *name* – string of up to 15 characters

Mode(s): Interface Configuration

exceeded-action

Description: Sets the action for packets not conforming to the committed rate and committed burst size, and not conforming to the peak rate and peak burst size. The **no** version restores the default value, **drop**.

Syntax: [no] exceeded-action { drop | transmit | mark *markVal* }

- drop – drop the packet
- transmit – transmit the packet
- *markVal* – mark value for the packet in the range 0–255

Mode(s): Rate Limit Profile Configuration

exceeded-fraction

- Description:** Sets the percentage of the total queue length that can be occupied before dropping exceeded packets. The **no** version returns the exceeded fraction to its default setting.
- Syntax:** exceeded-fraction *exceededFraction*
no exceeded-fraction
- *exceededFraction* – percentage range 0–100; default is 25
- Mode(s):** Queue Profile Configuration

exceeded-length

- Description:** Sets minimum and maximum constraints for the queue's exceeded lengths. The **no** version removes constraints on the queue's exceeded length.
- Syntax:** exceeded-length *minimumExceededLength* [*maximumExceededLength*]
no exceeded-length
- *minimumExceededLength* – range 0–1073741824
 - *maximumExceededLength* – range 0–1073741824
- Mode(s):** Queue Profile Configuration

exception dump

- Description:** Specifies the location from and to which the system should transfer a core dump file. The **no** version disables the command.
- Syntax:** exception dump { except-srp | srp-only } { local | *ipAddress* [*directoryName*] }
no exception dump
- *except-srp* – generates core dump for all non-SRP modules
 - *srp-only* – generates core dump for only the SRP modules
 - *local* – nonvolatile storage memory
 - *ipAddress* – IP address of the server to which the system will transfer the core dump file
 - *directoryName* – name of the directory on the server to which the system will transfer the core dump file
- Mode(s):** Global Configuration

exception gateway

- Description:** Specifies the gateway through which the system sends the core dump file to the remote FTP server. There is no **no** version.
- Syntax:** exception gateway *ipAddress*
- *ipAddress* – IP address of the gateway
- Mode(s):** Global Configuration

exception protocol ftp

- Description:** Specifies the username and password for FTP access to a host where you transferred a core dump file. The **no** version restores the defaults.
- Syntax:** exception protocol ftp
[[*algorithmType*] *userName* [[*algorithmType*] *password*]]
no exception protocol
- *algorithmType* – type of user name or password
 - › 0 – unencrypted password, the default.
 - › 8 – encrypted password
 - *userName* – username required to access the FTP server; the default username is anonymous
 - *password* – password required to access the FTP server; the default is no password
- Mode(s):** Global Configuration

exception source

- Description:** Specifies the IP address and mask of the system interface over which you want to send the core dump file to the remote FTP server. There is no **no** version.
- Syntax:** exception source *ipAddress ipAddressMask*
- *ipAddress* – IP address of the interface
 - *ipAddressMask* – optionally add the IP address mask of the interface
- Mode(s):** Global Configuration

excess-burst

- Description:** Sets amount of bandwidth allocated to accommodate a packet in progress when the rate is in excess of the burst.
- Syntax:** [no] excess-burst [*size*]
- *size* – the amount of bandwidth allocated; in the range 0–4294967295
- Mode(s):** Rate Limit Profile Configuration

exclude-subsystem

- Description:** Excludes subsystem files from being copied when you copy a software release to the system. The **no** version removes the exclusion for a specified subsystem file or all subsystem files.
- Syntax:** exclude-subsystem *subsystemName*
 no exclude-subsystem [*subsystemName*]
- *subsystemName* – name of the subsystem file to be excluded
- Mode(s):** Global Configuration

exec-banner

- Description:** Controls display of an exec banner (configured with the **banner** command) on a particular line after user authentication (if any) and before the first prompt of a CLI session. The **no** version disables the banner.
- Syntax:** [no] exec-banner
- Mode(s):** Line Configuration

exec-timeout

- Description:** Sets the time interval that the console or vty line waits for expected user input. The **no** version restores the default value, which is no time limit.
- Syntax:** exec-timeout *minutes* [*seconds*]
 no exec-timeout
- *minutes* – number of minutes for the time limit
 - *seconds* – number of seconds in addition to the minutes for the time limit
- Mode(s):** Line Configuration

exit

- Description:** Exits the current command mode. There is no **no** version.
- Syntax:** exit
- Mode(s):** All modes

exit-address-family

- Description:** Exits from Address Family Configuration mode and returns to Router Configuration mode. There is no **no** version.
- Syntax:** exit-address-family
- Mode(s):** Address Family Configuration

exit-remote-neighbor

- Description:** Exits from Remote Neighbor Configuration mode and returns to Router Configuration mode. There is no **no** version.
- Syntax:** exit-remote-neighbor
- Mode(s):** Remote Neighbor Configuration

export map

- Description:** Associates a route map with a VRF to filter routes exported by the VRF. The **no** version disables the application of the route map to exported routes.
- Syntax:** [no] export map *routeMap*
- *routeMap* – name of a route map
- Mode(s):** VRF Configuration

fabric-strict-priority

- Description:** Specifies strict priority scheduling for queues in the traffic class in the fabric. The **no** version deletes the strict priority setting.
- Syntax:** [no] fabric-strict-priority
- Mode(s):** Traffic Class Configuration

fabric-weight

- Description:** Specifies the relative weight for queues in the traffic class in the fabric. The **no** version sets the fabric weight to the default value.
- Syntax:** fabric-weight *weight*
no fabric-weight
- *weight* – range 1–63; default is 8
- Mode(s):** Traffic Class Configuration

fdl

- Description:** Specifies the facility data link standard used by a CT1 interface. The **no** version restores the default, none.
- Syntax:** fdl { ansi | att | all | none }
no fdl [ansi | att | all]
- ansi – specifies ANSI T1.403 Standard for extended superframe FDL exchange support
 - att – specifies AT&T Technical Reference 54016 for extended superframe FDL exchange support
 - all – specifies both the AT&T and ANSI mode for extended superframe FDL exchange support
 - none – removes the current FDL mode settings
- Mode(s):** Controller Configuration

fdl carrier

- Description:** Specifies that an CT1 interface is used in the carrier environment. The **no** version restores the default situation, in which an interface does not operate in the carrier environment.
- Syntax:** [no] fdl carrier
- Mode(s):** Controller Configuration

fdl string

- Description:** Defines an FDL message on a T1 interface as defined in the ANSI T1.403 specification. Currently, FDL strings can only be configured locally. The **no** version restores the default value to the specified FDL message or to all FDL messages.
- Syntax:** `fdl string { eic eicValue | fic ficValue | lic licValue | unit unitValue | pfi pfiValue | port portValue | generator generatorValue }`
`no fdl string { eic | fic | lic | unit | pfi | port | generator }`
- *eicValue* – equipment identification code; 1–10 characters; default is the null value
 - *licValue* – line identification code; 1–10 characters; default is the null value
 - *ficValue* – frame identification code; 1–10 characters; default is the null value
 - *unitValue* – unit identification code; 1–6 characters; default is the null value.
 - *pfiValue* – facility identification code to send in the FDL path message; 1–38 characters; default is the null value.
 - *portValue* – equipment port number to send in the FDL idle signal message; 1–38 characters; default is the null value.
 - *generatorValue* – generator number to send in the FDL test signal message; 1–38 characters; default is the null value.
- Mode(s):** Controller Configuration

fdl transmit

- Description:** Configures the system to send the specified type of FDL message on the T1 interface. The **no** version stops the system from sending the specified type of FDL message or all FDL messages.
- Syntax:** `[no] fdl transmit { path-id | idle-signal | test-signal }`
`no fdl transmit`
- *path-id* – transmits a path identification message every second
 - *idle-signal* – transmits an idle signal every 10 seconds
 - *test-signal* – transmits a test signal every 10 seconds
- Mode(s):** Controller Configuration

filter

- Description:** Defines a policy rule that drops all packets conforming to the specified classifier control list. If you do not specify a classifier control list, the system selects all packets from the interface associated with this policy list for this rule. Use the **suspend** keyword to suspend a filter rule temporarily. The **no** version removes the rule from the policy list.
- Syntax:** [no] [suspend] filter [classifier-group *clac/Name*] [precedence *precValue*]
- **suspend** – suspend the policy rule
 - *clac/Name* – classifier control list used to classify packets for this filter policy
 - *precValue* – precedence of this rule in relation to other rules within this set
- Mode(s):** Policy Configuration

flash-disk duplicate

- Description:** Copies the contents of NVS on the primary SRP module to another NVS card. There is no **no** version.
- Syntax:** flash-disk duplicate
- Mode(s):** Boot
- To access the Boot mode from the local console:
- 1 At the Privileged Exec prompt, type the **reload** command. Information on the reloading process appears.
 - 2 When the *countdown* begins, press the <M+B> key combination.
- This puts the CLI in Boot mode (:boot## prompt). If you do not press the <M+B> key combination, the reloading process continues and returns the CLI to the normal User Exec mode.

flash-disk initialize

- Description:** Performs a low-level format of NVS. There is no **no** version.
- Syntax:** flash-disk initialize [no-format]
- **no-format** – erases all files but does not format NVS
- Mode(s):** Boot
- To access the Boot mode from the local console:
- 1 At the Privileged Exec prompt, type the **reload** command. Information on the reloading process appears.
 - 2 When the *countdown* begins, press the <M+B> key combination.
- This puts the CLI in Boot mode (:boot## prompt). If you do not press the <M+B> key combination, the reloading process continues and returns the CLI to the normal User Exec mode.

flash-disk scan

Description: Scans NVS on the primary SRP module to detect corrupt sectors, deletes files and directories that contain corrupt sectors, fixes errors associated with unused sectors. There is no **no** version.

Syntax: flash-disk scan [repair]

Mode(s): Boot

To access the Boot mode from the local console:

- 1 At the Privileged Exec prompt, type the **reload** command. Information on the reloading process appears.
- 2 When the *countdown* begins, press the <M+B> key combination.

This puts the CLI in Boot mode (:boot## prompt). If you do not press the <M+B> key combination, the reloading process continues and returns the CLI to the normal User Exec mode.

forward

Description: Defines a rule that forwards all packets conforming to the specified classifier control list. If you do not specify a classifier control list, the system selects all packets from the interface associated with this policy list for this rule. Use the **suspend** keyword to suspend a forward rule temporarily. The **no** version removes the rule from the policy list.

Syntax: [no] [suspend] forward [classifier-group *clacName*]
[precedence *precValue*]

- *suspend* – suspend a policy rule
- *clacName* – classifier control list used to classify packets for this filter policy
- *precValue* – precedence of this rule in relation to other rules within this set

Mode(s): Policy Configuration

frame-relay class

Description: Associates a map class with a subinterface. The **no** version removes the association between the map class and the subinterface.

Syntax: [no] frame-relay class *mapName*

- *mapName* – name of the map class; use up to 64 characters

Mode(s): Subinterface Configuration

frame-relay description

- Description:** Assigns a text description or alias to a Frame Relay major interface or subinterface. The **no** version removes the description or alias.
- Syntax:** frame-relay description *name*
no frame-relay description
- *name* – text description or alias for the Frame Relay interface or subinterface; up to 64 characters
- Mode(s):** Interface Configuration, Subinterface Configuration

frame-relay fragment

- Description:** Configures fragmentation and reassembly for the map class created with the **map-class frame-relay** command. The **no** version stops fragmentation and/or reassembly on the subinterface.
- Syntax:** frame-relay fragment [[*fragmentSize*] [fragmentation-only] | reassembly-only]
no frame-relay fragment
- *fragmentSize* – maximum payload size of a fragment in bytes; a number in the range 16–8188; default value is 52
 - fragmentation-only – specifies fragmentation only
 - reassembly-only – specifies reassembly only
- Mode(s):** Map Class Configuration

frame-relay interface-dlci ietf

- Description:** Assigns a data-link connection identifier to a specified Frame Relay subinterface on the router or access server. The DLCI number identifies a virtual circuit. The **no** version removes this assignment.
- Syntax:** frame-relay interface-dlci *dlci* ietf
no frame-relay interface-dlci *dlci*
- *dlci* – DLCI number to be used on the specified subinterface to identify a virtual circuit in the range 16–1007
- Mode(s):** Subinterface Configuration

frame-relay intf-type

- Description:** Configures a Frame Relay interface type. The **no** version restores the default value, DTE.
- Syntax:** frame-relay intf-type *type*
no frame-relay intf-type
- *type* – one of the following interface types:
 - › dce – router is connected to user DTE equipment
 - › dte – router is connected to a Frame Relay network; the default
 - › nni – router connects two Frame Relay networks
- Mode(s):** Interface Configuration

frame-relay keepalive

- Description:** Enables the LMI mechanism for serial lines using Frame Relay encapsulation. The **no** version disables this capability. The keepalive command is similar to the **frame-relay lmi-t391dte** command.
- Syntax:** frame-relay keepalive [*seconds*]
no frame-relay keepalive
- *seconds* – number in the range 5–30; default is 10 seconds; defines the keepalive interval; the interval must be set, and the value on the DTE should be less than the value set on the DCE
- Mode(s):** Interface Configuration

frame-relay lmi-n391dte

- Description:** Sets the full-status polling counter (N391) on a DTE interface. The **no** version restores the default value, assuming an LMI has been configured.
- Syntax:** frame-relay lmi-n391dte *keepExchanges*
no frame-relay lmi-n391dte
- *keepExchanges* – number in the range 1– 255; default is 6; number of keep exchanges to be done before requesting a full-status message. If you specify a value of 1, you receive full-status messages only.
- Mode(s):** Interface Configuration

frame-relay lmi-n392dce

- Description:** Sets the error threshold counter (N392) on a DCE interface. The **no** version removes current setting and sets the default.
- Syntax:** frame-relay lmi-n392dce *threshold*
no frame-relay lmi-n392dce
- *threshold* – positive number in the range 1– 10; number of errors that will place the interface in an operationally down state; the default is 2 errors
- Mode(s):** Interface Configuration

frame-relay lmi-n392dte

- Description:** Sets the error threshold counter (N392) on a DTE interface. The **no** version removes current setting and sets the default.
- Syntax:** frame-relay lmi-n392dte *threshold*
no frame-relay lmi-n392dte
- *threshold* – positive number in the range 1–10; number of errors that will place the interface in an operationally down state; the default is 3 errors
- Mode(s):** Interface Configuration

frame-relay lmi-n393dce

- Description:** Sets the monitored events count (N393) on a DCE interface. The **no** version removes current setting and sets the default.
- Syntax:** frame-relay lmi-n393dce *events*
no frame-relay lmi-n393dce
- *events* – number in the range 1–10 events; specifies the diagnostic window used to verify link integrity; the default is 2 events (The detection of N392 errors within the window of N393 samples places the interface in an operationally down state.)
- Mode(s):** Interface Configuration

frame-relay lmi-n393dte

- Description:** Sets the monitored event count (N393) on a DTE interface. The **no** version removes current setting and sets the default.
- Syntax:** frame-relay lmi-n393dte *events*
no frame-relay lmi-n393dte
- *events* – number in the range 1–10 events; the default is 4 events; specifies the diagnostic window used to verify link integrity (The detection of N392 errors within the window of N393 samples places the interface in an operationally down state)
- Mode(s):** Interface Configuration

frame-relay lmi-t391dte

- Description:** Sets the link integrity verification polling timer (T391) on a DTE interface. The **no** version removes the current setting and sets the default.
- Syntax:** frame-relay lmi-t391dte *seconds*
no frame-relay lmi-t391dte
- *seconds* – number in the range 5–30 seconds; specifies the interval in seconds between status inquiries issued by the DTE; the default is 10 seconds
- Mode(s):** Interface Configuration

frame-relay lmi-t392dce

- Description:** Sets the polling verification timer (T392) on a DCE interface. The **no** version removes current setting and sets the default.
- Syntax:** frame-relay lmi-t392dce *seconds*
no frame-relay lmi-t392dce
- *seconds* – number in the range 5–30 seconds; specifies the expected interval in seconds between status inquiries issued by the DTE equipment; the default is 15 seconds
- Mode(s):** Interface Configuration

frame-relay lmi-type

Description: Selects the LMI type. The **no** version restores the default value.

Syntax: frame-relay lmi-type *type*

no frame-relay lmi-type

- *type* – one of the following types:
 - › ansi – ANSI T1.617 Annex D
 - › cisco – original Group of Four specification developed by DEC, Northern Telecom, Stratacom, and Cisco
 - › q933a – ITU-T Q.933 Annex A
 - › none – no management interface is used

Mode(s): Interface Configuration

framing

Description: Specifies the framing mode used by a CE1, CT1, E3, or T3 interfaces. Available modes vary by the type of interface. The **no** version restores the default for that interface.

Syntax: framing *framingType*

no framing

- *framingType* – one of the following framing types:

CE1 module

› crc4 – default; CRC4 frame

› no-crc4 – disables CRC4 framing

CT1 module

› esf – default; extended superframe; sets the HDLC idle code to 0x7E

› sf – superframe; sets the HDLC idle code to 0xFF

E3-FRAME module

› g751 – default; G.751 compliant frame

› g832 – G.832 compliant frame

E3-ATM module

› g751adm – G.751 ATM direct mapping

› g751plcp – default; G.751 PLCP mapping

› g832adm – G.832 ATM direct mapping

T3 module

› c-bit – default; specifies c-bit parity framing

› m23 – specifies M23 multiplexer framing

Mode(s): Controller Configuration

frequency

Description: Sets the time interval between RTR operations. The **no** version restores the default value.

Syntax: frequency *frequencyValue*

no frequency

- *frequencyValue* – number of seconds between RTR operations; for both types (echo and pathEcho), the default is 60 seconds

Mode(s): RTR Configuration

ftp-server enable

- Description:** Enables the FTP server and monitors the FTP port for attempts to connect to the FTP server. The **no** version terminates the current FTP sessions and disables the FTP server.
- Syntax:** [no] ftp-server enable
- Mode(s):** Global Configuration

group

- Description:** From QoS Profile Configuration mode, specifies that a group scheduler node be configured for each interface of the given interface type. The **no** version removes this rule from the QoS profile.
- From ISAKMP Policy Configuration mode, assigns a Diffie-Hellman group to the IKE policy. The **no** version restores the default, 1024-bit Diffie-Hellman group.
- Syntax:** To specify a group scheduler node for QoS:
- [no] *interfaceType* group *groupName* scheduler-profile *schedulerProfileName*
- *interfaceType* – one of the following interface types for which groups should be configured: **atm**, **ethernet**, **serial**, **server-port**
 - *groupName* – name of the traffic class group
 - *schedulerProfileName* – name of the scheduler profile
- To Specify a Diffie-Hellman group:
- group { 1 | 2 | 5 }
- no group
- 1 – specifies the 768-bit group
 - 2 – specifies the 1024-bit group
 - 5 – specifies the 1536-bit group
- Mode(s):** QoS Profile Configuration, ISAKMP Policy Configuration

halt

Description: Stops operation on both SRP modules or on the specified SRP module. There is no **no** version.



Caution: *To prevent corruption of NVS, issue this command before you remove or power down an SRP module.*

Syntax: The syntax of the command depends on whether you enter it in Boot mode or Privileged Exec mode.

Boot Mode:
halt

Privileged Exec Mode:
halt [force | primary [force] | standby [force]]

- force – prompts the user to confirm that the system should stop operation if the SRP modules are in certain states, such as writing configuration data to NVS, that could lead to loss of configuration data or corruption of NVS.
- primary – stop operation on primary SRP module only
- standby – stop operation on standby SRP module only

Mode(s): Boot, Privileged Exec

To access the Boot mode from the local console:

- 1 At the Privileged Exec prompt, type the **reload** command. Information on the reloading process appears.
- 2 When the *countdown* begins, press the <M+B> key combination.

This puts the CLI in Boot mode (:boot## prompt). If you do not press the <M+B> key combination, the reloading process continues and returns the CLI to the normal User Exec mode.

hash

Description: Sets the hash algorithm in an IKE policy. The **no** version restores the default, SHA-1.

Syntax: hash sha | md5
no hash

- sha – specifies SHA-1 (HMAC variant) as the hash algorithm
- md5 – specifies MD5 (HMAC variant) as the hash algorithm

Mode(s): ISAKMP Policy Configuration

hdlc down-when-looped

- Description:** Enables loopback detection on a Cisco HDLC interface. Loopback detection is disabled by default. The **no** version disables loopback detection.
- Syntax:** [no] hdlc down-when-looped
- Mode(s):** Interface Configuration, Subinterface Configuration

hdlc keepalive

- Description:** Specifies a keepalive value. The keepalive mechanism tracks the health of the connection. The **no** version turns off the keepalive feature.
- Syntax:** hdlc keepalive [*seconds*]
no hdlc keepalive
- *seconds* – keepalive timeout period in the range 0–6553 seconds. The default is 10. A value of zero (0) turns off the keepalive feature.
- Mode(s):** Interface Configuration, Subinterface Configuration

hdlc shutdown

- Description:** Stops or restarts a Cisco HDLC session. The **no** version restarts a Cisco HDLC session.
- Syntax:** [no] hdlc shutdown
- Mode(s):** Interface Configuration, Subinterface Configuration

hello hold-time

- Description:** Configures the MPLS hold time, the period that a sending LSR maintains a record of hello messages from the receiving LSR without receipt of another hello from that LSR. The **no** version restores the default value of 0.
- Syntax:** hello hold-time *holdTime*
no hello hold-time
- *holdTime* – a number in the range 0–65535; a value of 0 indicates 15 seconds for link hellos and 45 seconds for targeted hellos; a value of 65535 indicates an infinite hold time
- Mode(s):** LDP Profile Configuration

hello-interval

- Description:** Specifies the interval between hello packets that the router sends on the OSPF remote-neighbor interface. The **no** version restores the default value.
- Syntax:** hello-interval *helloInterval*
no hello-interval
- *helloInterval* – a number in the range 1–65535 seconds; default value is 10 seconds
- Mode(s):** Remote Neighbor Configuration

help

- Description:** Displays basic information on the Help system. There is no **no** version.
- Syntax:** help
- Mode(s):** All modes

hops-of-statistics-kept

- Description:** Sets the number of hops to keep statistics for an entry. The **no** version restores the default value.
- Syntax:** hops-of-statistics-kept [*hopsKeptValue*]
no hops-of-statistics-kept
- *hopsKeptValue* – number of hops for which statistics are collected for a particular *pathEcho* type; the default is 16 for a *pathEcho* entry and 1 for an *echo* entry; if you omit this option, all hops found are recorded




Note: *The only types your system supports are the pathEcho and the echo.*

- Mode(s):** RTR Configuration

host

- Description:** Adds or modifies an entry to the host table. The **no** version removes the specified host.
- Syntax:** `host hostname ipAddress [ftp [[algorithmType] userName [[algorithmType] password]]]`
`no host hostname`
- *hostname* – hostname to add or modify; up to 20 characters
 - *ipAddress* – IP address of the host
 - *ftp* – specifies that the host is an FTP server
 - *algorithmType* – type of username or password
 - › 0 – unencrypted password, the default.
 - › 8 – encrypted password
 - *userName* – username used to access an FTP server (but not an NFS server); defaults to **anonymous**
 - *password* – password used to access an FTP server (but not an NFS server); defaults to **null**
- Mode(s):** Global Configuration

hostname

- Description:** Sets the name for the system in Global Configuration mode; this hostname subsequently appears in the system CLI prompt. The **no** version removes the hostname from the system.
-  **Note:** *In Domain Map Tunnel Configuration mode, this command has been deprecated in favor of the **client-name** command. See the **client-name** command.*
- Syntax:** `hostname hostname`
`no hostname`
- *hostname* – string of up to 64 characters (no spaces)
- Mode(s):** Global Configuration, Domain Map Tunnel Configuration (deprecated)

hssi force-dte-acknowledge

Description: Provides compatibility with DCE devices that wait for the DTE side to set the acknowledge bit first. Issue this command if the HSSI interface is configured as DTE, both sides of the connection are correctly configured, and the link does not come up. The **no** version prevents the HSSI interface from sending acknowledgment signals when in DTE mode.

Syntax: [no] hssi force-dte-acknowledge

Mode(s): Interface Configuration

hssi internal-clock

Description: Enable the internal clock for DCE mode on a HSSI interface. The **no** version disables the internal clock for DCE mode on a HSSI interface.

Syntax: [no] hssi internal-clock

Mode(s): Interface Configuration