

D

data-character-bits

- Description:** Sets the number of data bits available for characters for all sessions on the specified vty lines. There is no **no** version.
- Syntax:** data-character bits { 7 | 8 }
- 7 – 7 data bits per character; this setting supports only characters in the standard ASCII set
 - 8 – 8 data bits per character; default setting, supports the full set of 8-bit international characters
- Mode(s):** Line Configuration

dead-interval

- Description:** Sets the time period that the OSPF router waits without seeing hello packets from a remote neighbor before declaring the neighbor to be down. The **no** version restores the default value.
- Syntax:** dead-interval *deadInterval*
no dead-interval
- *deadInterval* – number in the range 1–65535 seconds; default value is 40 seconds
- Mode(s):** Remote Neighbor Configuration

deadtime

- Description:** Use to configure the amount of time (in minutes) that a server is marked as unavailable if a request times out for the configured retry count. If a server fails to answer a request, it is marked “unavailable” by the system. The system does not send requests to the server for the configured time. The **no** version restores the default value, 0, turning off the deadtime mechanism.
- Syntax:** deadtime *recovery*
no deadtime
- *recovery* – amount of time that a server is marked as unavailable in the range 0–30 (minutes). The default is 0.
- Mode(s):** Radius Configuration

debug ip bgp

Description: Shows information on the selected variable. The **no** version disables the display.

Syntax:

```
debug ip bgp [ in | out ] [ peerAddress [ peerAddressMask ] ]
[ bgpLog ] [ import ] [ router routerName ]
[ filtering-router filteringRouterName ] [ accessClassName ]
[ route-map mapName ] [ severity { severityValue | severityNumber } ]
[ verbosity verbosityLevel ] [ secondary ]

no debug ip bgp [ in | out ] [ peerAddress [ peerAddressMask ] ]
[ bgpLog ] [ import ] [ router routerName ]
[ filtering-router filteringRouterName ] [ accessClassName ]
[ route-map mapName ]
```

- in – displays information for inbound events
- out – displays information for outbound events
- peerAddress – IP address of BGP peer for which information is displayed
- peerAddressMask – network mask of BGP peer for which information is displayed
- bgpLog – BGP log of interest; one of the following options:
 - › dampening – BGP dampening event; route is suppressed or no longer suppressed by route-flap dampening
 - › events – BGP finite state machine events and transitions
 - › keepalives – BGP keepalive message events
 - › updates – BGP routing table update events
 - › vpnv4 – BGP VPNv4 NLRI events
- import – displays BGP import processing events; appears only if you specify the **vpn4** keyword
- routerName – name of the virtual router that owns the BGP router for which information is being displayed
- filteringRouterName – name of the virtual router that owns the access class and route map parameters
- accessClassName – name of an access list to filter output
- mapName – name of a route map to filter output
- severity – specifies the minimum severity of the log messages displayed for the selected category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7; the lower the number, the higher the priority:
 - › emergency or 0 – system unusable
 - › alert or 1 – immediate action needed

- › critical *or 2* – critical condition exists
- › error *or 3* – error condition
- › warning *or 4* – warning condition
- › notice *or 5* – normal but significant condition
- › info *or 6* – informational message
- › debug *or 7* – debug message
- *verbosityLevel* – verbosity of the log category's messages; can be any of the following:
 - › low – terse
 - › medium – moderate detail
 - › high – verbose
- secondary – indicates that the specified filter conditions for the log are imposed in addition to any that were previously specified; if omitted, the specified filter conditions replace any that were previously specified

Mode(s): Privileged Exec

debug ip mbgp

Description: Shows information on the selected variable. The **no** version disables the display.

Syntax: debug ip mbgp [in | out] [*peerAddress* [*peerAddressMask*]]
 [*bgpLog*] [import] [router *routerName*]
 [filtering-router *filteringRouterName*] [*accessClassName*]
 [route-map *mapName*] [severity { *severityValue* | *severityNumber* }]
 [verbosity *verbosityLevel*] [secondary]

no debug ip mbgp [in | out] [*peerAddress* [*peerAddressMask*]]
 [*bgpLog*] [import] [router *routerName*]
 [filtering-router *filteringRouterName*] [*accessClassName*]
 [route-map *mapName*]

- in – displays information for inbound events
- out – displays information for outbound events
- *peerAddress* – IP address of BGP peer for which information is displayed
- *peerAddressMask* – network mask of BGP peer for which information is displayed
- *bgpLog* – BGP log of interest; one of the following options:
 - › dampening – BGP dampening event; route is suppressed or no longer suppressed by route-flap dampening
 - › events – BGP finite state machine events and transitions
 - › keepalives – BGP keepalive message events
 - › updates – BGP routing table update events
 - › vpv4 – BGP VPNv4 NLRI events
- import – displays BGP import processing events; appears only if you specify the **vpnv4** keyword
- *routerName* – name of the virtual router that owns the BGP router for which information is being displayed
- *filteringRouterName* – name of the virtual router that owns the access class and route map parameters
- *accessClassName* – name of an access list to filter output
- *mapName* – name of a route map to filter output
- severity – specifies the minimum severity of the log messages displayed for the selected category. See the **debug ip bgp** command.
- *verbosityLevel* – verbosity of the log category's messages. See the **debug ip bgp** command.

- secondary – indicates that the specified filter conditions for the log are imposed in addition to any that were previously specified; if omitted, the specified filter conditions replace any that were previously specified

Mode(s): Privileged Exec

debug ip ospf

Description: Shows information on the selected variable. The **no** version disables the display.

Syntax: debug ip ospf *ospfLog* [severity { *severityValue* | *severityNumber* }]
[verbosity *verbosityLevel*]

no debug ip ospf *ospfLog*

- *ospfLog* – OSPF log of interest; one of the following options:
 - › adj – OSPF adjacency events
 - › elect-dr – OSPF designated router election
 - › events – OSPF general events
 - › lsa – OSPF link state advertisements events
 - › neighbor – OSPF neighbor state machine
 - › packets-rcvd – OSPF packets received
 - › packets-sent – OSPF packets sent
 - › route – OSPF route events
 - › spf – all OSPF shortest path first calculation events
 - › spf-ext – OSPF shortest path first external route calculation events
 - › spf-inter – OSPF shortest path first interarea route calculation events
 - › spf-intra – OSPF shortest path first intra-area route calculation events
- severity – specifies the minimum severity of the log messages displayed for the selected category. See the **debug ip bgp** command.
- *verbosityLevel* – verbosity of the log category's messages. See the **debug ip bgp** command.

Mode(s): Privileged Exec

debug ip pim

Description: Shows information on the selected variable. The **no** version disables the display.

Syntax: The syntax differs for PIM Dense Mode and PIm Sparse Mode.

PIM Dense Mode:

```
debug ip pim { pimLog [ severity { severityValue | severityNumber } ]
[ verbosity verbosityLevel ] |
switchState groupAddress sourceAddress |
dense-mode { on | off } }
```

PIM Sparse Mode:

```
debug ip pim { pimLog [ severity { severityValue | severityNumber } ]
[ verbosity verbosityLevel ] |
switchState groupAddress sourceAddress |
sparse-mode { on | off | sg-state [ group groupAddress
[ source sourceAddress ] | rp rpAddress ] [ count ] } }
```

no debug ip pim *pimLog*

- *pimLog* – PIM log of interest; one of the following options:
 - › autoRp-rcvd – autoRP packets received
 - › autoRP-sent – autoRP packets sent
 - › engineering – PIM engineering
 - › hellos-rcvd – PIM hello messages received
 - › hellos-sent – PIM hello messages sent
 - › packets – PIM packets received and sent
 - › packets-rcvd – PIM packets received
 - › packets-sent – PIM packets sent
- *severity* – specifies the minimum severity of the log messages displayed for the selected category. See the **debug ip bgp** command.
- *verbosityLevel* – verbosity of the log category's messages. See the **debug ip bgp** command.
- *switchState* – switches from one type of tree to another
 - › rpt-switch – switch from a shortest path tree to a shared path tree
 - › spt-switch – switch from a shared path tree to a shortest path tree

- *groupAddress* – IP address of the multicast group
- *sourceAddress* – IP address of the multicast source
- *on* – turns on the specified PIM mode on all virtual routers
- *off* – turns off the specified PIM mode on all virtual routers
- *sg-state* – displays information about the relationship between a source, multicast group, and RP router
- *rp* – displays information about the relationships between sources, groups, and the specified RP router
- *rpAddress* – address of the RP router
- *count* – displays one of the following
 - › (with no optional keywords) number of relationships between a source, multicast group, and RP router
 - › (with the **group** keyword) number of sources associated with the multicast group for PIM SM
 - › (with the **source** and **group** keywords) number of source-group pairs for PIM SM
 - › (with the **rp** keyword) number of source-group pairs associated with the RP router for PIM SM

Mode(s): Privileged Exec

debug ip rip

Description: Shows information on the selected variable. The **no** version disables the display.

Syntax: debug ip rip *ripLog* [severity { *severityValue* | *severityNumber* }]
[verbosity *verbosityLevel*]

no debug ip rip *ripLog*

- *ripLog* – RIP log of interest; one of the following options:
 - › *events* – general RIP events, such as removing RIP from an interface or creating the RIP process
 - › *route* – events associated with two RIP routers exchanging routes
- *severity* – specifies the minimum severity of the log messages displayed for the selected category. See the **debug ip bgp** command.
- *verbosityLevel* – verbosity of the log category's messages. See the **debug ip bgp** command.

Mode(s): Privileged Exec

debug isis

Description: Displays debug-related information about selected IS-IS log parameters. This command manipulates the same log as the Global Configuration **log** commands. The **no** version disables debugging display.

Syntax: debug isis *isisLog* [severity { *severityValue* | *severityNumber* }]
[verbosity *verbosityLevel*]

no debug isis *isisLog*

- *isisLog* – IS-IS log of interest; one of the following options:
 - › adj-packets – IS-IS adjacency-related packets, such as hello packets sent and IS-IS received adjacencies going up and down
 - › mpls traffic-eng advertisements – MPLS traffic-engineering agent advertisements
 - › mpls traffic-eng agents – MPLS traffic-engineering agents
 - › snp-packets – IS-IS CSNPs/PSNPs
 - › spf-events – shortest path first events
 - › spf-statistics – SPF timing and statistic data
 - › spf-triggers – SPF triggering events
 - › update-packets – update-related packets
- severity – specifies the minimum severity of the log messages displayed for the selected category. See the **debug ip bgp** command.
- *verbosityLevel* – verbosity of the log category's messages. See the **debug ip bgp** command.

Mode(s): Privileged Exec

default-fields peer

- Description:** Specifies the fields that will appear by default in the output of a subsequently issued **show ip bgp summary** command.
- Syntax:** [no] default-fields peer *fieldOptions*
- *fieldOptions* – field(s) to be displayed, in the format all | [intro | last-reset-reason | messages-received | messages-sent | peer-type | prefixes-received | remote-as | state | times-up | up-down-time | updates-received | updates-sent]*
 - › all – all available information; not recommended, as this information for each network does not fit on a single line and is difficult to read
 - › intro – introductory information about the state of various BGP attributes; this information is displayed only if you specify this keyword
 - › last-reset-reason – reason for most recent reset
 - › messages-received – total number of messages received from the peer
 - › messages-sent – total number of messages sent to the peer
 - › peer-type – type of BGP peer: internal, external, or confederation
 - › prefixes-received – number of unique prefixes received from the peer
 - › remote-as – the remote AS number of the peer
 - › state – state of the BGP session
 - › times-up – number of times the session has been established
 - › up-down-time – how long the session has been up or down
 - › updates-received – number of update messages received from the peer
 - › updates-sent – number of update messages sent to the peer
 - › * – indicates that one or more parameters can be repeated multiple times in a list in the command line
- Mode(s):** Router Configuration

default-fields route

Description: Specifies the fields that will appear by default in the output of any subsequently issued **show ip bgp** command that displays routes (except for the **show ip bgp summary** command).

Syntax: [no] default-fields route *fieldOptions*

- *fieldOptions* – field(s) to be displayed, in the format all | [afi | aggregator | as-path | atomic-aggregate | best | clusters | communities | extended-communities | imported | intro | label | loc-pref | med | next-hop | next-hop-cost | origin | originator-id | peer | peer-type | rd | safi | unknown-types | weight]*
 - › all – all available information; not recommended, as this information for each network does not fit on a single line and is difficult to read
 - › afi – address family identifier
 - › aggregator – AS number and IP address of aggregator
 - › as-path – AS path through which this route has been advertised
 - › atomic-aggregate – whether the atomic aggregate attribute is present
 - › best – whether this is the best route for the prefix
 - › clusters – list of cluster IDs through which the route has been advertised
 - › communities – community number associated with the route
 - › extended-communities – extended community
 - › imported – whether the route was imported
 - › intro – introductory information about the state of various BGP attributes; this information is displayed only if you specify this keyword
 - › label – MPLS label
 - › loc-pref – local preference for the route
 - › med – multiexit discriminator for the route
 - › next-hop – IP address of the next router that is used when forwarding a packet to the destination network
 - › next-hop-cost – whether the indirect next hop of the route is unreachable, if not, displays IGP cost to the indirect next hop
 - › peer – IP address of BGP peer from which route was learned
 - › peer-type – type of BGP peer: internal, external, or confederation
 - › origin – origin of the route
 - › originator-id – router ID of the router in the local AS that originated the route
 - › rd – route distinguisher
 - › safi – subsequent address family identifier

- › unknown-types – attribute codes for unknown path attributes
- › weight – weight of the route
- › * – indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode(s): Router Configuration

default-information originate

Description: Enables BGP to advertise a default route (0.0.0.0/0) if the default route exists in the IP routing table. If the default route does not exist, you must configure it using the **ip route** command.

For IS-IS, OSPF, and RIP, configures a default route for the distribution of default information into the respective routing domain. IS-IS creates the default route (0.0.0.0/0) if it does not exist in the IP routing table. OSPF and RIP do not create the default route unless you use the **always** option.

For all protocols, the **no** version disables advertisement of the default route. The syntax varies with the protocol.

Syntax: For BGP:

[no] default-information originate

For IS-IS:

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

For RIP:

[no] default-information originate [always | route-map *mapTag*]

For OSPF:

[no] default-information originate [always | metric *metricValue* | metric-type 1 | metric-type 2 | route-map *mapTag*]*

- *mapTag* – name of route map used to import the default route; string of up to 32 characters
- always – creates the default route, so that it is always advertised
- *metricValue* – sets the metric for the default route; a value ranging from 0–4294967295
- metric-type 1 – sets the default route’s metric type to OSPF external type 1
- metric-type 2 – sets the default route’s metric type to OSPF external type 2
- * – 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

default-metric

- Description:** Configures RIP to use this metric when advertising routes on all subsequently created interfaces. The **no** version restores the default value, 0.
- Syntax:** [no] default-metric *metricValue* [*interfaceType* *interfaceSpecifier*]
- *metricValue* – metric to apply to routes, a value ranging from 1–16
 - *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):** Router Configuration

default-router

- Description:** Specifies the IP address of the router that the subscriber's computer will use for traffic destined for locations beyond the local subnet. The **no** version removes the association between the address pool and the router.
- Syntax:** default-router *ipAddressPrimary* [*ipAddressSecondary*]
no default-router
- *ipAddressPrimary* – IP address of preferred router
 - *ipAddressSecondary* – IP address of secondary router
- Mode(s):** Pool Configuration

delete

- Description:** Deletes a directory or file in nonvolatile storage. There is no **no** version.
- Syntax:** delete *filename* | directory *directoryName* [force]
- *filename* – name of the local file you are deleting (for example, system1.cnf)
 - *directoryName* – path of a directory
 - force – forces deletion of directory even if it is not empty
- Mode(s):** Boot, User Exec, Privileged Exec

description

- Description:** In Interface Configuration mode, adds a text description to an IP interface. In VRF Configuration mode, adds a text description to the VRF. The **no** version removes the description from the interface or VRF.
- Syntax:** description *name*
no description
- *name* – string of up to 256 characters in Interface Configuration mode; string of up to 80 characters in VRF Configuration mode
- Mode(s):** Interface Configuration, VRF Configuration

dir

- Description:** Displays information about the files in nonvolatile storage, including name, size, date created, and whether they are in use. There is no **no** version.
- Syntax:** dir [*path*] [short]
- *path* – path to a specific directory
 - short – limits display to file name and creation date
- Mode(s):** User Exec, Privileged Exec

disable

Description:	<p>When used from Privileged Exec mode, exits Privileged Exec mode and returns to User Exec mode.</p> <p>When used from Router Configuration or Interface Configuration mode in the context of a DVMRP configuration, disables DVMRP on the virtual router or interface. The no version reenables DVMRP on the virtual router or interface.</p> <p>When used from Router Configuration mode in the context of a RIP configuration, disables RIP on the virtual router. The no version enables RIP processing on the virtual router.</p>
Syntax:	<p>To return to User Exec mode:</p> <pre>disable [level]</pre> <ul style="list-style-type: none"> • <i>level</i> – one of the following privilege levels; the default is 10 <ul style="list-style-type: none"> › 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 <p>DVMRP, RIP:</p> <pre>[no] disable</pre>
Mode(s):	Privileged Exec, Router Configuration (DVMRP or RIP), Interface Configuration (DVMRP only)

disable-autosync

Description:	Halts automatic synchronization between the primary and standby SRP modules. The no version restores the default situation, in which automatic synchronization runs as a background process every 5 minutes.
Syntax:	<pre>[no] disable-autosync</pre>
Mode(s):	Global Configuration

disable-dynamic-redistribute

- Description:** Halts the dynamic redistribution of routes that are initiated by changes to a route map. Supported by DVMRP, BGP, IS-IS, OSPF, and RIP. The **no** version reenables dynamic redistribution of routes.
- Syntax:** [no] disable-dynamic-redistribute
- Mode(s):** Address Family Configuration, Router Configuration

disable proxy lcp

- Description:** Disables the proxy LCP parameter for the remote host. The **no** version enables the proxy LCP parameter for the remote host.
- Syntax:** [no] disable proxy lcp
- Mode(s):** L2TP Destination Profile Host Configuration

disable-switch-on-error

- Description:** Prevents the redundant SRP module from taking over if the primary SRP module experiences a software failure or if you push the reset button on the primary SRP module. Issue the **sync** command immediately before you issue this command. The **no** version restores the default situation, in which the redundant SRP module takes over if the primary SRP module experiences a failure.
- Syntax:** [no] disable-switch-on-error
- Mode(s):** Global Configuration

disconnect ssh

- Description:** Terminates an active SSH session. Use the **show ip ssh** command to determine the session identifier for the session to terminate. There is no **no** version.
- Syntax:** disconnect ssh { vty *vtyId* | *sessionId* }
- *vtyId* – virtual terminal identifier for VTY where the SSH session resides; use the **show users** command to determine the identifier
 - *sessionId* – identifier for the session to be terminated
- Mode(s):** Privileged Exec

distance

Description: Defines an administrative distance for RIP or OSPF routes. A distance of 255 prevents the route from being installed in the routing table. The **no** version either negates a command or restores the command's defaults.

Syntax: The options available vary depending on your routing protocol context; that is, on whether you are configuring OSPF or RIP.

OSPF:

```
[ no ] distance { weight | ospf { external distExt | inter-area disInter | intra-area disIntra } [ external distExt | inter-area distInter | intra-area distIntra ]* }
```

- *distance* – weight applied to OSPF routes
- *weight* – value assigned to OSPF routes that are added to the IP routing table; a number in the range 1–255
- *ospf* – OSPF routes
- *distExt* – distance for external type 5 and type 7 routes; a number in the range 1–255
- *disInter* – distance for interarea routes; a number in the range 1–255
- *disIntra* – distance for intra-area routes; a number in the range 1–255
- * – indicates that one or more parameters can be repeated multiple times in a list in the command line

RIP:

```
[ no ] distance weight
```

- *weight* – administrative distance assigned to RIP routes added to the IP routing table in the range 0–255; the default is 120

Mode(s): Router Configuration

distance bgp

- Description:** Sets the administrative distances for BGP routes. A distance of 255 prevents the route from being installed in the routing table. The **no** version restores the default values.
- Syntax:** distance bgp *externalDistance internalDistance localDistance*
no distance bgp [*externalDistance* [*internalDistance* [*localDistance*]]]
- *externalDistance* – administrative distance for routes external to the AS in the range 1–255; the default is 20
 - *internalDistance* – administrative distance for routes internal to the AS in the range 1–255; the default is 200
 - *localDistance* – administrative distance for local (redistributed) routes in the range 1–255; the default is 200
- Mode(s):** Address Family Configuration, Router Configuration

distance ip

- Description:** Sets the administrative distance for IS-IS routes that are inserted into the IP routing table. A distance of 255 prevents the route from being installed in the routing table. The **no** version restores the default value of 115.
- Syntax:** [no] distance *weight* ip
- *weight* – administrative distance assigned to IS-IS routes added to the IP routing table in the range 1–255
- Mode(s):** Router Configuration

distribute-domain-wide

- Description:** Increases the granularity of routing information within an IS-IS domain by allowing routes to be distributed from level 2 to level 1. This results in more accurate routing between level 1 areas. The **no** version disables command.
- Syntax:** [no] distribute-domain-wide
- Mode(s):** Router Configuration

distribute-list

Description: Specifies the distribute list, an access list applied to incoming or outgoing RIP route updates. In Remote Neighbor Configuration mode, applies only to a RIP remote-neighbor interface. The **no** version removes the distribute list. An IP access list acts as a filter; refer to the **access-list** command for details.

Syntax: In Router Configuration mode:

```
[ no ] distribute-list accessListNumber { in | out }  
[ interfaceType interfaceSpecifier ]
```

In Remote Neighbor Configuration mode:

```
[ no ] distribute-list accessListName { in | out }
```

- *accessListName* – name of the access list
- in – applies the access list to incoming route updates
- out – applies the access list to outgoing route updates
- *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): Router Configuration, Remote Neighbor Configuration

dns-server

Description: Assigns a DNS server to an address pool. The **no** version removes the association between the address pool and the DNS server.

Syntax: dns-server *ipAddressPrimary* [*ipAddressSecondary*]

no dns-server

- *ipAddressPrimary* – IP address of preferred DNS server
- *ipAddressSecondary* – IP address of secondary DNS server

Mode(s): Pool Configuration

domain-authentication-key

- Description:** Assigns a password for authentication of IS-IS level 2 LSPs, CSNPs, and PSNPs. The **no** version deletes the password.
- Syntax:** domain-authentication-key [0 | 8] *authKey*
no domain-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):** Router Configuration

domain-id

- Description:** Sets the OSPF domain ID for an OSPF VRF on a PE. The **no** version restores the default value.
- Syntax:** domain-id *domainIdAddress* | *domainId*
no domain-id
- *domainIdAddress* – OSPF domain ID in IP address format; default is the IP address of the OSPF router configured in the VRF
 - *domainId* – OSPF domain ID as an integer value in the range 0–4294967295; default is 0
- Mode(s):** Router Configuration

domain-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 2 packet (LSPs, CSNPs, and PSNPs). The digest is inserted into the packet from which it is created. Using this algorithm for domain 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: domain-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 domain-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 – the *key* is entered in unencrypted form (plaintext); this is the default option
- 8 – 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 – the system never stops accepting or generating packets; overrides previously specified stop times.
- *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

domain-name

- Description:** Specifies a domain name that can be returned to the subscriber of an address pool if requested. The **no** version removes the association between the address pool and the domain name.
- Syntax:** domain-name *domainName*
no domain-name
- *domainName* – name of the domain
- Mode(s):** Pool Configuration

domain-tag

- Description:** Sets the VPN route tag for an OSPF VRF on a PE to prevent routing loops back into the VPN. The **no** version restores the default value.
- Syntax:** domain-tag *routeTag*
no domain-tag
- *routeTag* – number identifying the VPN route tag in the range 0–4294967295
- Mode(s):** Router Configuration

ds3-scramble

- Description:** Enables scrambling of the ATM cell payload on a T3 interface. DS3 scrambling assists clock recovery on the receiving end of the interface. The **no** version disables cell scrambling.
- Syntax:** [no] ds3-scramble
- Mode(s):** Controller Configuration

dsr-detect

- Description:** Requires that a DSR signal be detected on the line for a user to log into the console. DSR is carried on pin 6 of the SRP module's RS-232 (DB-9) connector. The DSR input must be connected to the DSR output of a modem or the DTR output of another DTE device, such as a terminal server, that supports this signal. If a session is in progress and the DSR signal is lost, the user is logged out automatically. The **no** version restores the default of no DSR required.
- Syntax:** [no] dsr-detect
- Mode(s):** Privileged Exec

dsu bandwidth

Description: Sets the speed for the fractional T3 lines. The **no** version clears the bandwidth. If you issue this command, be sure to issue the **dsu mode** and **scramble** commands. Similarly, if you issue the **no** version, be sure to issue the **no dsu mode** and **no scramble** commands; otherwise, the interface may drop packets unexpectedly.

Syntax: dsu bandwidth *bandwidthValue*
no dsu bandwidth

- bandwidth – sets a fractional bandwidth
- *bandwidthValue* – value of the fractional bandwidth in the range 22–44210 Kbps. The system offers a set of speeds in increments that depend on the DSU mode you specify. The actual speed of the fractional T3 lines will be the value closest to the fractional bandwidth you specify.

Mode(s): Controller Configuration

dsu mode

Description: Sets the DSU mode for the lines. The **no** version clears the dsu mode. If you issue this command, be sure to issue the **dsu bandwidth** and **scramble** commands. Similarly, if you issue the **no** version, be sure to issue the **no dsu bandwidth** and **no scramble** commands; otherwise, the interface may drop packets unexpectedly.

Syntax: dsu mode 0 | 2
no dsu mode

- 0 – Digital Link mode
- 2 – Larscom mode

Mode(s): Controller Configuration

duplex

Description: Specifies the duplex mode for an Ethernet interface. The **no** version specifies the default value, **automatically negotiate**. This command works in conjunction with the **speed** command; if you set or accept the **automatically negotiate** setting for either duplex mode or speed, the system negotiates both parameters with the remote device. This command is not available for the Ethernet interface on the SRP module.

Syntax: duplex *duplexMode*
no duplex

- *duplexMode* – one of the following the duplex options
 - › automatically negotiate – specifies that the system negotiates duplex mode with the remote device
 - › full – specifies that the system uses full duplex on an FE or GE interface
 - › half – specifies that the system uses half duplex on an FE interface; this value is not valid for GE interfaces

Mode(s): Interface Configuration